Dr.Tom Shinder's Configuring

ISA Server 2004

Dr. Thomas W. Shinder
Debra Littlejohn Shinder

SYNGRESS

Эта *книга посвящается:*

как всегда нашим семьям: детям (Крису и Кники), братьям (Ричу и Д) и родителям, включая тех, кого уже нет с *нами;*

нашим друзьям, многие из которых также и наши коллеги;

нашим кошкам, которые прохаживались по нашим клавиатурам, спали на столах и помогали сохранять веру в конечный результат в течение долгого процесса написания этой книги.

Наравне с другими мы посвящаем эту книгу друг другу. Не так много людей имеет возможность работать со своими близкими, проводить 24 часа изо дня в день в компании друг друга и получать от этого удовольствие. Мы благодарны судьбе за этот редкий дар.

ISA Server 2004

Томас В. Шиндер
Дебра Л. Шиндер

«Русская **Редакция»** **«БХВ-ПетерОург»**

2005

УДК 681.3.06 ББК
32.973.81-018.2 Ш62

Шин$_д$ ер **Т., Шиндер** Д.

Ш62 ISA Server 2004: Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция»; СПб.: «БХВ-Петербург», 2006. — 1088 стр.: ил.

ISBN 5-7502-0272-0 («Русская Редакция»)

ISBN 5-94157-746-X («БХВ-Петербург»)

Структура книги позволяет использовать ее как в качестве справочника, включающего отдельные, не зависящие друг от друга разделы инструкций, так и для изучения продукта «шаг за шагом», начиная с терминологии и основных понятий и заканчивая практическими вопросами. В книге представлена эволюция брандмауэров компании Microsoft от Proxy 1.0 лo ISA Server 2004. Подробно рассмотрены: современный рынок брандмауэров и серверов кэширования, функциональные возможности **ISA** Server 2004, конфигурация сетей с использованием ISA Server 2004, типы клиентов и способы их настройки, установка и конфигурирование ISA Server 2004. Даны советы по повышению скорости доступа в Интернет и основы сетевой безопасности.

Для системных администраторов

УДК 6S1.3.06
ББК32.973.81-018.2

Лицензия ИД № О242S от 24.07.00. Подписано в печать 02 11.05.
Формат 70x100V$_{ie}$. Печать офсетная. Усл. леч. л. 87,72.
Тираж 3000 экз. Заказ Nt4388 «БХВ-Петербург»,
194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП «Типография «Наука» 199034,
Санкт-Петербург, 9 линия, 12

ISBN 1-931836-19-1(англ.)
ISBN 5-7502-0272-0
(«Русская Редакция»)
ISBN 5-94157-746-X
(«БХВ-Петербург»)

Благодарности

Издательство «Syngress» хотело бы выразить благодарность людям, чьи доброта и поддержка сделали возможным появление этой книги.

В настоящее время книги издательства «Syngress» распространяются в Соединенных Штатах и Канаде O'Reilly Media, Inc. Эту корпорацию отличают необыкновенный энтузиазм и высокие этические принципы, и нам хотелось бы поблагодарить ее сотрудников, потративших много сил и времени на представление книг издательства «Syngress» на рынке: Тима О'Рейли (Tim O'Reilly), Лауру Болдуин (Laura Baldwin), Марка Брокеринга (Mark Brokering), Майка Леонарда (Mike Leonard), Донну Селенко (Donna Selenko), Бонни Шихан (Bonnie Sheehan), Синди Дэвис (Cindy Davis), Гранта Киккерта (Grant Kikkert), Опол Мацутаро (Opol Matsutaro), Стива Хэзелвуда (Steve Hazelwood), Марка Вилсона (Mark Wilson), Рика Брауна (Rick Brown), Лесли Бекер (Leslie Becker), Джил Лотроп (Jill Lothrop), Тима Хинтона (Tim Hinton), Кайла Харта (Kyle Hart), Сару Виндж (Sara Winge), C. J. Rayhill, Питера Пардо (Peter Pardo), Лесли Кранделл (Leslie Crandell), Валери Доу (Valerie Dow), Регину Аджио (Regina Aggio), Паскаля Хоншера (Pascal Honscher), Престона Пола (Preston Paull), Сьюзан Томпсон (Susan Thompson), Брюса Стюарта (Bruce Stewart), Лауру Шмайер (Laura Schmier), Сью Виллинг (Sue Willing), Марка Джекобсена (Mark Jacobsen), Бетси Валижевски (Betsy Waliszewski), Дона Манна (Dawn Mann), Катрин Барре (Kathryn Barrett), Джона Чодаки (John Chodacki) и Роба Буллингтона (Rob Bullington). Сердечная благодарность Айлин Берг (Aileen Berg) — работать с вами очень приятно.

Мы признательны невероятно напряженно работавшей группе сотрудников из издательства Elsevier Science, включающей Джонатана Банкелла (Jonathan Bunkell), Яна Сигера (Ian Seager), Данкана Энрайта, (Duncan Enright), Дэвида Бертона (David Burton), Розанну Рамачиотти (Rosanna Ramacciotti), Роберта Файебразе (Robert Fairbrother), Мигеля Санчеса (Miguel Sanchez), Клауса Берана (Klaus Beran), Эмму Вайет (Emma Wyatt), Рози Мосс (Rosie Moss), Криса Хоссака (Chris Hossack), Марка Ханта (Mark Hunt) и Кристу Леппико (Krista Leppiko) и убедившей нас в том, что наше видение проблемы соответсвует обще при нятому.

Мы благодарим Дэвида Бакленда (David Buckland), Мэри Чиен (Marie Chieng), Люси Чон (Lucy Chong), Лесли Лим (Leslie Lim), Одри Ган (Audrey Gan), Пан Аи Хуа (Pang Ai Hua) и Джозефа Чаня (Joseph Chan) из STP Distributors за энтузиазм, проявленный при получении наших книг.

Мы выражаем благодарность Квону Сун Джуну (Kwon Sung June) из Acorn Publishing за его поддержку.

Мы выражаем глубокую признательность Дэвиду Скопу (David Scott), Трише Вайлден (Tricia Wilden), Марилле Берджис (Marilla Burgess), Аннетте Скотт (Annette Scott), Эндрю Свафферу (Andrew Swaffer), Стефану О'Донахью (Stephen O'Donoghue), Беку Лоу (Bec Lowe) и Марку Лэнгли (Mark Langley) из компании Woodslane за распространение наших книг в Австралии, Новой Зеландии, Папуа-Новой Гвинее, Фиджи Тонга, Соломоновых островах и островах Кука.

Мы также благодарны Винстону Лиму (Winston Lim) из компании Global Publishing за помощь и поддержку в распространении книг издательства «Syngress» на Филиппинах.

Об авторах

Томас В. Шиндер, доктор медицинских наук (Thomas W. Shinder, MD), — сертифицированный инженер по системам корпорации Microsoft (Microsoft Certified Systems Engineer, MCSE), награжденный званием MVP (Microsoft Most Valuable Professional — свидетельство, выдаваемое корпорацией Microsoft членам компьютерного сообщества (Microsoft Most Valuable Professional), за его работу с ISA Server, известен в сообществе специалистов по брандмауэрам как один из главных экспертов по брандмауэру ISA Server. Том получал консультации в главных компаниях и организациях, таких как Microsoft, Xerox, Lucent Technologies, FINA Oil, Hewlett-Packard и Департамент энергетики США (U. S. Department of Energy).

Том занимался практической медициной в Орегоне, Техасе и Арканзасе, прежде чем решил начать новую карьеру, увлекшись компьютерными технологиями вскоре после женитьбы на Дебре Литтлджон Шиндер в середине 1990-х. Супруги организовали совместную компанию TACteam (Trainers, Authors, and Consultants) (Преподаватели, авторы и консультанты), в которой они обучают основам компьютерных технологий и разрабатывают обучающие программы, пишут книги, статьи, официальные отчеты (whitepapers) и документацию для корпоративных продуктов и подготавливают материалы по маркетингу, помогают малым и большим коммерческим фирмам в реализации и распространении технологических решений.

Том *в* соавторстве с Деб написал такие бестселлеры, как Configuring ISA Server 2000 (Настройка ISA Server 2000) (Syngress, ISBN 1 -928994-29-6), Dr. Tom Shinder's ISA Server and Beyond (ISA Server д-ра Тома Шиндера и то, что находится за брандмауэром) (Syngress, ISBN 1-931836-66-3), and Troubleshooting Windows 2000 TCP/IP (Локализация неисправностей Windows 2000 TCP/IP) (Syngress, ISBN 1-928994-11-3). Он принимал участие в написании нескольких книг, посвященных подготовке к экзаменам на получение сертификата MCSE по операционным системам Windows 2000 и Windows 2003, и написал сотни статей о серверах под управлением Windows для различных книжных и электронных издательств.

Том — главный «нарушитель спокойствия» на сайте ISAserver.org (www.isaserver.org), отвечающий на сотни вопросов в неделю в дискуссионных форумах, и ведущий сотрудник, обеспечивающий информационное наполнение сайта.

Дебра Литтлджон Шиндер (Debra Littlejohn Shinder) — сертифицированный инженер по системам корпорации Microsoft (MCSE), награждена званием MVP в области серверной безопасности. В прошлом она — офицер полиции и преподаватель уголовного судопроизводства уровня колледжа (college level criminal justice instructor), этим и объясняется ее интерес к компьютерной безопасности и компьютерным преступлениям. Она — автор нескольких книг о компьютерных операционных системах, сетях и безопасности. К ним относятся Scene of the Cybercrime: Computer Forensics Handbook (Арена киберпреступления: юридический справочник в области компьютерных технологий) (Syngress, ISBN 1-931836-65-5) и Computer

Networking Essentials (Основы организации компьютерных сетей) (Cisco Press). Дебра написала в соавторстве с мужем, д-ром Томасом Шиндером, такие бестселлеры, как Configuring ISA Server 2000 (Настройка ISA Server 2000) (Syngress, ISBN 1-928994-29-6), Dr. Tom Shinder's ISA Server and Beyond (ISA Server д-ра Тома Шиндера и то, что находится за брандмауэром) (Syngress, ISBN 1-931836-66-3) и Troubleshooting Windows 2000 TCP/IP (Локализация неисправностей Windows 2000 TCP/IP) (Syrgress, ISBN 1-928994-11-3).

Кроме того, Деб — технический и научный редактор и соавтор более 15 книг, посвященных подготовке к экзаменам на получение сертификата MCSE по операционным системам Windows 2000 и Windows 2003, экзамену на получение сертификата CompTIA Security-*- и сертификации TruSecure's ICSA (International Computer Security Assosiation, Международная ассоциация компьютерной безопасности). В недавнем прошлом она редактировала Brainbuzz A+ Hardware News, а в настоящее время редактирует Sunbelt Software's WinXP News (www.winxpnews.com). Ее статьи регулярно публикуются на сайтах TechRepublic's TechProGuild и Windowsecurity.com, а также в печатных журналах, таких как Windows IT Pro Magazine (в прошлом Windows & .NET). Дебра — автор обучающих программ, корпоративных отчетов (whitepapers), материалов по маркетингу и технической документации для корпораций Microsoft, DigitalThink, Sunbelt Software, CNET и других. В настоящее время она специализируется на вопросах безопасности и разработках корпорации Microsoft.

Деб и Том живут в районе Dallas-Ft Worth и время от времени читают курсы по организации компьютерных сетей и компьютерной безопасности в истфилдском колледже (Eastfield College).

Технический редактор

Мартин Грасдол (Martin Grasdal) MCSE+I, MCT, CNE (Certified NetWare Engineer, дипломированный инженер по сетевым программным средствам), CNI, CT^{T}, A+ Мартин, независимый консультант с десятилетним опытом работы в компьютерной индустрии, обладает практическими знаниями в области организации компьютерных сетей и управления в сфере компьютерных технологий. Он получил сертификат MCT (Microsoft Certified trainer, сертифицированный преподаватель Microsoft) в 1995 г., а MCSE — в 1996 г. Его знания и опыт как специалиста по сетевым технологиям включают работу с такими программными продуктами, как NetWare, Lotus Notes, Windows NT, Windows 2000, Windows 2003, Exchange Server, IIS, ISA Server и др. В настоящее время Мартин активно работает как консультант, автор и редактор. В последнее время в качестве консультанта он сотрудничал по контракту с корпорацией Microsoft в качестве технического специалиста программы MCP (Master Control Program, главная программа управления) над проектами, связанными с серверными технологиями. Мартин живет в г. Эдмонтоне штата Альберта в Канаде (Edmonton, Alberta, Canada) с женой Кати (Cathy) и двумя сыновьями.

От авторов,

Деб и Тома Шиндеров

ISA Server занимал большое место в нашей жизни в течение последних четырех лет. Это наша третья книга о быстро развивающихся технических разработках брандмауэров и серверов кэширования корпорации Microsoft, и мы более чем когда-либо воодушевлены ее новым воплощением, сервером ISA Server 2004.

Мы знакомы с ним с момента его появления, у нас была возможность проверить вносимые изменения, дополнения и улучшения на этапах альфа и бета-тестирования программного обеспечения.

Этот книга — плод не только наших совместных усилий, но и усилий команды. Множество людей принимало участие в ее создании и без них книга не была бы написана.

Мы глубоко признательны разработчикам ISA Server из корпорации Microsoft за вовлечение нас в процесс разработки ISA, его документирования и продвижения на рынке. В особенности мы хотим поблагодарить сотрудников в Редмонде, Далласе и Шарлот: Майка Нэша (Mike Nash), Стива Брауна (Steve Brown), Тони Бейли (Tony Bailey), Джозефа Ландеса (Joseph Landes), Жози Фонтане (Josue Fontanez), Маркуса Шмидта (Marcus Schmidt), Рису Колеман (Risa Coleman), Марка Мортимера (Mark Mortimer), Реда Джонстона (Red Johnston), Дейва Гарднера (Dave Gardner), Джоула Слосса (Joel Sloss), Джулию Полк (Julia Polk), Стива Райли (Steve Riley), Зака Гатта (Zach Gutt), Майка Чаня (Mike Chan), Сюзан Колберер (Suzanne Kalberer), Келли Мондлоч (Kelly Mondloch), Алана Вуда (Alan Wood), Клинта Денхэма (Clint Denham), Элен Пратер (Ellen Prater), Скотта Джайлса (Scott Jiles), Сибелл Нуперт (Sibylle Haupert), Эми Логан (Amy Logan), Ари Фручтера (Ari Fruchter), Ронен Боази (Ronen Boazi), Барклая Неира (Barclay Neira), Бена Гутерсона (Ben Guterson), Колин Лит (Colin Lyth,) Эрика Розенкранца (Eric Rosencrantz), Джан Шанахан (Jan Shanahan), Джима Эдвардса (Jim Edwards) и Вальтера Бойда (Walter Boyd), а также Джоуэн Веттерн Qoern Wettern) и Роналда Бикелара (Ronald Beekelaar) за их помощь и поддержку.

Мы также хотим поблагодарить группу ISA в Израиле: Ави Натана (Avi Nathan), АдинуХагеге (Adina Hagege), Керен Мастер (Keren Master), Рона Мондри (RonMondri), Итаи Гринберга (Itai Greenberg), Йоси Сайлеса (Yossi Siles), Сигалит Бар (Sigalit Bar), Натана Бигмана (Nathan Bigman), Линду Лиор (Linda Lior), Нету Амит (Neta Amit), Амит Финкельштейн (Amit Finkelstein), Меир Шмоуеэли (Meir Shmouely), Нира Бен Зви (Nir Ben Zvi), Офер Дубровски (Opher Dubrovsky), Орен Трутнер (Oren Trutner), Йигал Эдери (Yigal Edery), Зива Мадора (Ziv Mador), Раз Горен (Raz Goren), Мооли Беери (Mooly Beeri), Нира Калива (Nir Caliv), Зива Каспи (Ziv Caspi), Гергори Бершански (Gergory Bershansky), Ариэля Каца (Ariel Katz), Дана Бар-Лева (Dan Bar-Lev), Макса Урицки (Max Uritsky), Ронен Баренбоим (Ronen Barenboim), Нира Михайлович (Nir Michalowitz) и Ури Бараша (Uri Barash).

Спасибо поставщикам оборудования, давшим нам возможность поработать с их устройствами, ориентированными на ISA Server: Джону Кертису (John Curtis,) .Джону Амаралу (John Amaral), Майку Друару (Mike Druar), Кевину Мерфи (Kevin Murphy), Эрике Баттен (Erika Batten), Бонни Андерсон (Bonnie Anderson) и Марку Родену (Mark Roden) из компании Network Engines, Абдулу Ажану (Abdul Azhan) из RimApp, Марку Семандени (Marc Semadeni) из Hewlett Packard и Йон Тье Линь (Y^{on}g T^{h}y^{e} Lin) and Йон Пин Линь (Yong Ping Lin) из Celestix.

Мы хотим выразить признательность техническому редактору Мартину Грасдолу (Martin Grasdal) за его кропотливую и тщательную проверку работоспособности каждой предложенной нами процедуры, корректности и завершенности всех наших описаний и инструкций и смысловой ясности текста, даже тех его частей, которые писались нами в конце восемнадцатичасового рабочего дня, когда мы старались сохранить остатки здравого смысла и рассудка с помощью лишь силы воли и многочисленных чашек кофе. Мы также признательны нашему корректору Эдвине Левис (Edwina Lewis), воевавшей с терминологией, находившей орлиным глазом наши опечатки и при этом остававшейся доброй и неунывающей даже тогда, когда мы становились слегка несдержанными.

Мы хотим поблагодарить Стефана Четкути (Stephen Chetcuti) и Шона Батгейга (Sean Buttgieg), сотрудников сайтов Isaserver.org (www.isaserver.org) и Windowsecurity.com (www.windowsecurity.com), предоставивших нам возможность на форумах рекламировать как ISA Server, так и эту книгу, благодаря чему мы узнали о других фанатах ISA Server, разбросанных по всему миру.

Большое спасибо Джону Шисли (John Sheesley) из Tech Republic/TechProGuild (www.techproguild.com), поместившему серию наших статей об ISA Server 2004, и Эми Айзенберг (Amy Eisenberg) и Патриции Колби (Patricia Colby) из журнала Windows IT Pro Magazine (ранее Windows & .NET), который представлял ряд наших статей об ISA Server 2004.

Мы хотим отдать дань уважения всем специалистам по ISA Server, обладающим званием MVP, чьи идеи и помощь в процессе написания книги были бесценны: Крису Грегоги (Chris Gregory), Каи Вилки (Kai Wilke), Стефану Поусилу (Stefaan Pouseele), Джейсону Балларду (Jason Ballard), Баду Ратлифу (Bud Ratliff), Кристиану Гроебнеру (Christian Groebner), Дайетер Рочер (Dieter Rauscher), Фредерику Исноуфу (Frederic Esnouf), Джесперу Ханно (Jesper Hanno), Филиппу Матону (Philippe Mathon), Фил Винделл (Phil Windell), Славу Пидгорному (Slav Pidgorny), Абрахаму Мартинез Фернандес (Abraham Martinez Fernandez).

Кроме того, особые благодарности тем, кто обеспечивал и сопровождал программу MVP: Джерри Брайенту Q^{err}y Bryant), Эмили Фрит (Emily Freet), Джейни Кларк (Janni Clark) и Джону Эдди (John Eddy).

Мы также хотим поблагодарить участников групп новостей, посвященных ISA Server, списков рассылок и досок объявлений (message boards), чьи вопросы ини-

циировали многие сценарии в этой книге, и всех остальных, так или иначе оказавшим нам помощь. В частности мы выражаем благодарность Джону Толмачеву (John Tolmachoff), Джефри Мартину (Jeffrey Martin), Эми Бабинчак (Amy Babinchak), Стиву Моффату (Steve Moffat), Грегу Малхолланду (Greg Mulholland), Шону Квилману (Shawn Quillman), Джозефу Кравитцу (Joseph Kravitz), Тьяго де Авиз (Tiago de Aviz), Дэвиду Фаринику (David Farinic), Аману Беди (Aman Bedi), Биллу Стюарту (Bill Stewart), AWJ (Al), Сюзан Бредли (Susan Bradley) и многим-многим другим. Спасибо друзья!

Особую благодарность мы выражаем Джиму Харрисону (Jim Harrison). Он работает в группе тестирования (QA team) ISA Server корпорации Microsoft и поддерживает исключительный Web-сайт: www.isatools.org. Многие из нас пропали бы без программных средств Джима и его постоянного подталкивания к совершенствованию приобретенных нами профессиональных навыков сетевых специалистов и администраторов брандмауэров.

Все, кого мы уже упомянули, способствовали планированию и созданию этой книги, а любые ошибки и упущения целиком ложатся на наши плечи. Мы старались выполнить работу аккуратно и по возможности без ошибок, но совершенство — скорее цель, чем достижимый результат. Если мы забыли упомянуть кого-либо, пожалуйста, примите наши искреннейшие извинения (завершающий этап работы над рукописью был, мягко говоря, лихорадочным) и дайте нам знать об этом, чтобы можно было исправить этот промах в следующем издании книги.

В заключение мы хотим выразить особую благодарность сотрудникам издательства «Syngress», подтолкнувших нас к созданию этой книги, проявившим необыкновенное терпение и понимание при плавном переносе сроков окончания работы и поверившим в нас с самого начала: Эндрю Вильямсу (Andrew Williams), нашему издателю, и Джейме Квигли (Jaime Quigley), нашему редактору. Друзья, верите вы или нет, но в конце концов мы сделали это!

От издателя

Издательство Syngress было основано в 1997 г. Своей главной целью оно видит издание оригинальных авторских книг в отличие от «поточного» производства литературы. С тех пор с издательством начали сотрудничать многие выдающиеся авторы, первые среди которых — Дебра Литтлджон Шиндер (Debra Littlejohn Shinder) и Томас Шиндер (Thomas Shinder).

Они работают в издательстве в качестве редакторов, авторов, вдохновителей, консультантов и иногда критиков. Они всегда готовы к работе и подготовке к изданию самых лучших книг. С их помощью мы узнали очень много нового.

В своей работе они всегда придерживаются строгих этических норм, подобно полицейским и врачам (Дебра — полицейский, а Том — врач). В своей работе они всегда стремятся к высшему качеству, потому что в книге указываются их имена.

Но что особенно важно, они сочетают в себе фундаментальные технические познания со страстью к обучению других. Это редкое соединение качеств позволяет им помогать в работе более чем 250 000 ИТ-профессионалов.

Мы благодарим вас от всего сердца.

Крис Уильяме (Chis Williams), Президент и основатель издательства

Амаретт Педерсен (Amorette Pedersen), Вице-президент отдела маркетинга, основатель издательства

Эндрю Уильяме (Andrew Williams),
Издатель Syngress Publishing
Декабрь 2004 г.

Оглавление

Глава 1

Эволюция брандмауэра: от Proxy 1.0 до ISA 2004

Основные темы главы:

- **О чем эта книга и для кого предназначена**
- **Безопасность: восходящая звезда**
- **Брандмауэры: стражи у ворот**
- **ISA Server: от прокси-сервера до полнофункционального брандмауэра**

О чем эта книга и для кого предназначена

Наша первая книга о ISA Server «Configuring ISA Server 2000: Building Firewalls for Windows 2000» (Syngress Publishing, 2001, ISBN 1-928994-29-6) была посвящена первой попытке корпорации Microsoft создать сетевой брандмауэр уровня предприятия. Как чаще всего бывает при первой попытке, ISA 2000 стал опытным образцом как для Microsoft, так и для пользователей.

Microsoft обеспечила ISA 2000 развитую многоуровневую функциональность, намного превосходящую традиционный брандмауэр с фильтрацией пакетов, а также снабдила его такими «излишествами», как обнаружение и предупреждение вторжений (Intrusion Detection/Intrusion Prevention, IDS/I DP) и Web-кэширование — функции, которые многие другие производители брандмауэров не включают вообще или поставляют в виде добавочных модулей или отдельных продуктов за отдельную плату.

ISA Server неизбежно сравнивали с другими популярными брандмауэрами, такими как Firewall-1 /VPN-1 от Checkpoint и PIX от Cisco, а также с недорогими средствами обеспечения безопасности от таких производителей, как NetScreen, Watchguard, SonicWall, Symantec и многих других, заполнивших рынок за последние несколько лет. И хотя ISA Server выдержал это сравнение, администраторы ISA вскоре приступили к созданию «перечней пожеланий», включавших в себя характеристики и функции, которые могли сделать его еще лучше.

> ПРИМЕЧАНИЕ Некоторые могут возразить, что «перечни пожеланий» пользователей в некоторых случаях приводили к добавлению ненужных или бесполезных свойств, а также к исключению полезных свойств. По сообщению разработчиков, некоторые функции, например шлюз H.323, входившие в ISA Server 2000, были исключены из ISA 2004 из-за того, что пользователи не проявили к ним интереса. С другой стороны, ISA 2004 включает в себя возможность перенаправления трафика со всех портов на внешний сервер («all-port forwarding»), потому что на этом настояли пользователи брандмауэров низшей ценовой категории, включающих в себя эту функцию.

Как и в случае любого программного обеспечения, нужно было устранить некоторые шероховатости. Поскольку сфера обеспечения безопасности стала более сложной и появились новые типы угроз, возникла необходимость в новых технологиях и в улучшении уже существующих. Поэтому корпорация Microsoft приступила к созданию новой версии ISA Server, которая должна была включить множество функций по просьбам пользователей, стать проще в использовании и эффективнее в обеспечении безопасности.

Некоторые изменения в ISA Server 2004 оказались настолько радикальными, что Microsoft серьезно подумывала о том, чтобы полностью изменить название программного продукта, но в итоге все же пришла к решению оставить название «Internet Security and Acceleration Server» (ISA Server), чтобы не потерять пользователей предыдущей версии

и избежать путаницы на рынке программных продуктов. Брандмауэр ISA Server 2004 стал основательным всеобъемлющим средством обеспечения безопасности, служащим различным целям в разнообразных сетевых конфигурациях.

О чем эта книга

Написание книги о ISA Server 2000 так же, как и работа с самим программным продуктом, помогло нам изучить этот продукт. После того, как книга была написана, мы продолжили работу с ISA Server и столкнулись с новыми вопросами (и новыми ответами). От читателей были получены ценные отзывы о том, что еще они хотели бы прочитать в книге. Мы учли все это при подготовке плана этой книги, посвященной ISA Server 2004.

> СОВЕТ Многие читатели просили нас предоставить побольше основ предмета, поэтому более опытные читатели, а также пользователи, имеющие конкретные вопросы или столкнувшиеся с конкретными проблемами, могут пропустить первые несколько глав и сразу перейти к описанию принципов работы ISA Server 2004.

Структура книги дает возможность легко найти конкретные советы о том, как действовать в определенных ситуациях, или способы устранения возникших при использовании ISA Server 2004 проблем. Добавлены многочисленные советы и примечания, помогающие в практической работе с ISA Server 2004, справочная информация о других темах, с которыми можно столкнуться при работе с ISA Server 2004, а также включено множество диаграмм и скриншотов.

От главы к главе

Данную книгу можно использовать в качестве справочника, включающего отдельные, не зависящие друг от друга разделы инструкций. Логический порядок изложения материала предназначен для тех, кто изучает данную книгу постепенно, шаг за шагом, начиная с терминологии и основных понятий и переходя к практическим вопросам.

Глава 1. Эволюция брандмауэра: от Proxy 1.0 до ISA 2004

Глава 1 начинается с раздела под названием «Безопасность: восходящая звезда», который представляет собой обзор новой, выдающейся роли безопасности в новом тысячелетии. В разделе «Безопасность: какое отношение к ней имеет корпорация Microsoft?» мы обсудим новую стратегию корпорации Microsoft, нацеленную на обеспечение безопасности как первоочередного приоритета, в рамках ее инициативы по обеспечению безопасности использования компьютеров — Trustworthy Computing Initiative. Затем мы изучим лучшие способы обеспечения сохранности ваших ценностей (как в физическом, так и в электронном виде) в разделе «Безопасность: многоуровневый подход».

В разделе «Брандмауэры: стражи у ворот» мы подробнее рассмотрим роль брандмауэра, историю и философию современных брандмауэров, а также различия между разнообразными моделями брандмауэров (хост-модель по сравнению с сетевой, аппаратная модель по сравнению с программной). Затем мы рассмотрим функциональные возможности современных брандмауэров и эволюцию брандмауэров от простых прокси с фильтрацией пакетов до всеобъемлющих средств обеспечения безопасности.

Заключительный раздел «ISA Server: от прокси-сервера к полнофункциональному брандмауэру» посвящен теме остальной части книги — ISA Server. Мы рассмотрим, как корпорация Microsoft вышла на рынок средств обеспечения безопасности, начиная с появления MS Proxy Server — предвестника ISA Server и заканчивая появлением ISA Server 2004. Мы обсудим, какую роль может сыграть для вас и вашей компании этот программный продукт, как можно получить два программных продукта по цене одного и как работать с кэшированием. Мы также порассуждаем о будущем ISA Server и о тенденции интегрирования функций обеспечения безопасности в программные продукты, которая прослеживается в продукции корпорации Microsoft.

Глава 2. Изучение функциональных возможностей ISA Server 2004

В этой главе подробно рассмотрены основные функции ISA Server 2004: перешедшие из ISA Server 2000 и новые или улучшенные, а также функции, входившие в ISA Server 2000, но опущенные в новой версии.

В начале мы сосредоточимся на функциях ISA Server 2000, которые были улучшены или расширены, например: администрирование VPN, проверка подлинности пользователя, правила брандмауэра, пользовательские и групповые политики доступа, мастер публикации OWA (Outlook Web Access, Web-доступ с помощью Outlook) и безопасные Web-публикации, поддержка FTP (File Transfer Protocol, протокол передачи файлов), правила кэширования, средство контроля сообщений SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты), улучшенные механизмы ведения журналов и создания отчетов, а также усовершенствованный графический интерфейс.

Кроме того мы подробно рассмотрим многочисленные новые функции ISA Server 2004, в том числе возможность работы с несколькими сетями, изолирование VPN-подключений и другие новые функции, имеющие отношение кVPN, группам пользователей брандмауэра, настраиваемые определения протоколов и расширенная поддержка протоколов, делегирование базовой проверки подлинности, поддержка проверки подлинности SecurID для клиентов Web-прокси, формы, созданные брандмауэром (проверка подлинности на основе форм), публикация серверов с помощью протокола поддержки туннельного режима PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол), использование протокола SSL (Secure Sockets Layer, протокол защищенных сокетов) для VPN-подключения к службам

терминалов, принудительное шифрование для обеспечения безопасности Exchange RPC (Remote Procedure Call, удаленный вызов процедуры) соединений, улучшенная фильтрация протокола ШТР, преобразование ссылок и новые функции мониторинга и отчетности.

Глава 3. Рейтинг брандмауэров и место в нем ISA Server 2004

По многочисленным просьбам читателей мы уделим целую главу обсуждению рынка брандмауэров 2004 и того, как выдерживает конкуренцию ISA Server 2004, рассмотрим современный рынок брандмауэров и серверов кэширования и используем различные критерии сравнения, в том числе:

- процедуры лицензирования, начальные расходы и полную себестоимость работы программного продукта (административный персонал, контакты со службой поддержки, покупка дополнительных возможностей и устройств и расходы по обновлению программного обеспечения);
- спецификации;
- функции брандмауэра и IDS/IDP;
- VPN функции;
- функции по Web-кэшированию;
- сертификация.

Мы рассмотрим, как в различных брандмауэрах реализованы фильтрация потоков данных приложений, аппаратные и системные требования, VPN функции, возможности и вопросы лицензирования клиентов, возможности взаимодействия с другими программными продуктами и интеграции с другими сетевыми компонентами, например с Exchange, SharePoint, Active Directory, с операционными системами сторонних разработчиков, а также интерфейс и простоту их использования.

Мы сравним ISA Server 2004 со следующими наиболее популярными брандмауэрами и/или средствами кэширования:

- программный продукт Checkpoint NG и устройства от Nokia (которые работают с Checkpoint);
- брандмауэр Cisco PIX / устройства VPN;
- NetScreen / брандмауэр Juniper Networks / устройства VPN;
- брандмауэр SonicWall / устройства VPN;
- брандмауэр Symantec / устройства и программное обеспечение VPN;
- брандмауэр Watchguard / устройства VPN;
- свободно распространяемое программное обеспечение брандмауэра на основе Linux;
- брандмауэр BlueCoat / VPN / устройства кэширования;
- продукты для кэширования от Novell Volera;
- свободно распространяемое программное обеспечение для кэширования от Squid.

Мы рассмотрим сильные и слабые стороны каждого из этих продуктов по сравнению с ISA Server 2004 и также обсудим, как можно эффективно использовать ISA Server 2004 вместе с брандмауэрами сторонних разработчиков, чтобы обеспечить многоуровневую безопасность как по внутреннему, так и по внешнему периметру сети.

Глава 4. Конфигурация сетей в среде ISA Server 2004 и подготовка сетевой инфраструктуры

Одна из наиболее распространенных проблем, с которыми приходилось сталкиваться при поиске неисправностей в работе ISA Server 2000, — недостаток соответствующей поддерживающей инфраструктуры. Мы предвидим, что схожие проблемы возникнут и при работе с ISA Server 2004, если *до* установки брандмауэра ISA Server 2004 на компьютере не будет обеспечена соответствующая поддерживающая сетевая инфраструктура.

В этой главе мы обсудим ряд основных вопросов, связанных с сетевой инфраструктурой:

- понятие сетевой модели ISA Server 2004;
- настройка таблицы маршрутизации на брандмауэре ISA Server 2004;
- поддержка протокола DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) для брандмауэра и клиентов ISA Server 2004;
- я поддержка службы WINS (Windows Internet Naming Service, служба имен Интернета для Windows) для брандмауэра и клиентов ISA Server 2004;
- поддержка службы DNS (Domain Name System, служба имен доменов) для бранд мауэра и клиентов ISA Server 2004;
- поддержка службы встроенного пространства имен RADIUS (Remote Authenti cation Dial-In User Service, служба аутентификации удаленного дозванивающе гося пользователя) для брандмауэра и клиентов ISA Server 2004;
- поддержка служб сертификации для брандмауэра и клиентов ISA Server 2004.

В этой главе мы рассмотрим каждый из сетевых сервисов, обеспечивающих поддержку брандмауэра ISA Server 2004 и хостов, подключающихся через брандмауэр ISA Server 2004. Кроме того, мы обсудим понятия сетей, сетевых конфигураций, сетевых отношений и контроля доступа между сетями с точки зрения ISA Server 2004. Мы также рассмотрим конфигурацию «сеть внутри сети», способы разрешения возникающих в такой конфигурации проблем с помощью ISA Server 2004 и настройки внутреннего сетевого маршрутизатора.

Глава 5. Типы клиентов ISA Server 2004 и автоматизация настройки клиентов

В этой главе рассматриваются три типа сетевых клиентов ISA 2004:

- клиент SecureNAT;
- клиент брандмауэра;
- клиент Web-прокси.

Эти типы клиентов работают по-разному, позволяя клиентскому компьютеру получить доступ к Интернету или другой внешней сети через сервер ISA. Мы подробно объясним механизм работы всех типов клиентов. У каждого из них есть свои преимущества и недостатки, а выбор «лучшего» клиента зависит от ряда факторов, включая операционную систему клиента, протоколы, к которым должен иметь доступ клиентский компьютер, а также нужно ли (и позволяют ли политики или обстоятельства) установить дополнительное программное обеспечение на клиентские компьютеры. Мы предоставим вам необходимую информацию для принятия правильного решения о том, какой тип клиента должен использоваться в конкретной ситуации.

Затем мы представим вам пошаговые инструкции по настройке каждого типа клиентов и дадим конкретные рекомендации для каждого типа. Мы рассмотрим общие проблемы, возникающие при работе с различными типами клиентов, например вопросы разрешения имен и проблемы петель (loopback) с помощью ISA сервера, применяя расщепленную инфраструктуру DNS.

Поскольку ручная установка и конфигурирование большого числа клиентов **в** рамках предприятия может стать утомительным занятием, мы также приводим инструкции по автоматизации процесса инициализации клиента, чтобы снизить расходы на администрирование. В этом разделе мы рассмотрим различные способы автоматизации конфигурирования клиентов Web-прокси и брандмауэров, включая:

- конфигурирование серверов DHCP для поддержки авто обнаружения клиентов Web-прокси и брандмауэров;
- конфигурирование серверов DNS для поддержки автообнаружения клиентов Web-прокси и брандмауэров;
- автоматизация настройки клиента Web-прокси с групповой политикой;
- автоматизация настройки клиента Web-прокси с помощью инструмента IEAK (Internet Explorer Administration Kit, набор администрирования Internet Explorer).

Вы узнаете, как автоматизировать процесс установки программного обеспечения для клиента брандмауэра при помощи установки и управления программным обеспечением, основанным на групповой политике, или путем создания и применения сценария установки по умолчанию. Мы также обсудим использование сервера SMS (System Management Server, сервер управления системами) для реализации программного обеспечения клиента брандмауэра.

Глава 6. Установка и конфигурирование брандмауэра ISA

Эта глава начинается с пошаговых инструкций по установке ISA Server в двух различных возможных конфигурациях:

я Установка ISA 2004 на групповом сервере Если ISA Server должна играть роль брандмауэра, выполняя исключительно функции брандмауэра или выступая в качестве и брандмауэра, и сервера кэширования, то он должен быть установлен на компьютере с несколькими сетевыми адаптерами;

■ **Установка ISA 2004 на сервере с одним сетевым адаптером** В отличие от ISA 2000, в ISA 2004 больше нет режима установки, при котором задаются только функции кэширования, однако при установке программы на сервер с единственным сетевым подключением вы получите тот же самый результат, поскольку сервер с одним сетевым адаптером не может использоваться в качестве брандмауэра

ISA Server 2004 работает на компьютерах с установленной операционной системой Windows 2000 Server или Windows Server 2003. Мы обсудим некоторые различия в функциональности программы в зависимости от используемой операционной системы и укажем, на какие моменты нужно обратить внимание в процессе установки, чтобы позднее избежать возможных проблем.

Таблицы локальных адресов LAT (Local Address Table), применяемой в ISA Server 2000, больше нет, поэтому можно установить несколько сетевых интерфейсов, чтобы создать несколько внутренних сетей (воспользовавшись новой возможностью ISA Server 2004 по поддержке нескольких сетей), в дополнение к общему или частному диапазону адресов демилитаризованной зоны (Demilitarized Zone, DMZ). Некая подсеть, отделенная межсетевыми экранами от публичных и/или корпоративных сетей. — *Примеч. пер.).* В этой главе мы обсудим, как это сделать.

ISA Server 2004 включает набор сетевых шаблонов, облегчающих начинающим администраторам брандмауэра ISA Server 2004 начало работы. Мы изучим такие шаблоны брандмауэров, как внешний брандмауэр, пограничный брандмауэр, внутренний брандмауэр, брандмауэр с тремя интерфейсами и демилитаризованной зоной, брандмауэр с одним интерфейсом, и посмотрим, как они могут помочь администратору брандмауэра ISA Server 2004 работать с простыми и сложными сетевыми настройками. Мы также рассмотрим новый графический пользовательский интерфейс и его использование для выполнения стандартных административных задач.

Мы рассмотрим вопросы модернизации программы: обновление ISA Server 2000 до ISA Server 2004, обновление для Microsoft Proxy Server 2.0, которая требует предварительное обновление до ISA Server 2000 и лишь затем до ISA Server 2004. Здесь же будут рассмотрены различия в установке стандартной и промышленной версии программы.

Наконец, в этой главе содержатся базовые сведения о том, как начать работу с ISA Server 2004, и инструкции по созданию временной свободной политики доступа, которая позволит вам убедиться, что после установки ISA Server работает корректно.

СОВЕТ Вероятнее всего, простота использования ISA Server 2004 в сети предприятия будет обеспечена, если вы предварительно протестируете работу программы в смоделированной среде; это позволит вам определить, как ISA Server 2004 будет взаимодействовать со службами и приложениями вашей сети. Использование программ создания виртуальной среды, такой как Virtual PC или VMWare корпорации Microsoft, является наиболее рентабельным способом моделирования промышленной полнофункциональной сети без необходимости инвестиций в дополнительные аппаратные средства.

Глава 7. Создание и применение политики доступа в брандмауэре ISA Server 2004

В отличие от ISA Server 2000, брандмауэр ISA Server 2004 использует унифицированный набор правил, обрабатывающий правила доступа и правила **публикации** сверху вниз. Вам больше не нужно гадать, какое правило активно на данный момент, как это приходилось делать при использовании ISA Server 2000. Теперь вы знаете, что запрос будет обрабатывать первое правило из списка, соответствующее параметрам запроса на соединение.

Правила доступа ISA Server 2004 контролируют трафик на основе ряда параметров, наиболее важными из которых являются: источник, пункт назначения, протокол и пользователь. Однако вы можете произвести настройку каждого правила так, чтобы оно применялось в определенное время суток, к определенной группе пользователей и/или к конкретному серверу. Вы можете использовать правила доступа, чтобы заблокировать сайты, файлы, всплывающие элементы или одноранговые приложения. Правила доступа ISA Server 2004 предоставляют вам возможность полностью контролировать то, какие соединения разрешены (и не разрешены) через брандмауэр ISA.

Одно из основных усовершенствований ISA Server 2004 — возможность назначения практически любого элемента правила в мастере создания правил доступа. В ISA Server 2000 было невозможно **непосредственно** задавать элементы политик; часто администратор брандмауэра ISA Server 2000 начинал создавать правило протокола, забыв, что необходимое определение протокола еще не создано.

В этой главе мы обсудим, как работают правила доступа ISA Server 2004 и как их настроить для того, чтобы контролировать доступ через брандмауэр. Кроме того, мы обсудим методики, необходимые для заблаговременного задания элементов политик, и покажем, как использовать набор инструментов правил доступа для облегчения создания правил доступа. Мы приведем конкретные примеры-, как разрешить и запретить обмен мгновенными сообщениями Instant Messaging (IM) и одноранговыми приложениями типа P2P (Peer-to-Peer), как разрешить доступ к удаленным серверам Exchange и другие.

Глава 8. Публикация сетевых служб в Интернете с помощью ISA Server 2004

Публикация сетевых служб позволяет открыть доступ к серверам и службам вашей корпоративной сети другим пользователям через Интернет и из других не внушающих доверия мест. Задача состоит в том, чтобы предоставить удаленный доступ к вашим сетевым серверам и службам без ущерба безопасности. ISA Server 2004 — сложный и настраиваемый брандмауэр, осуществляющий фильтрацию потока данных на уровне приложения — сможет быстро разобраться с теми, кто пытается незаконно атаковать ваши серверы.

В этой главе мы обсудим правила Web-публикации и публикации серверов. Правила Web-публикации обеспечивают наивысший уровень безопасности, доступный для публикуемых Web-сервисов, что объясняется их уникальной возможностью — создавать мост SSL-SSL и делегировать базовую проверку подлинности. Кроме того, фильтр протокола HTTP позволяет контролировать практически каждый аспект обмена данными протокола HTTP, происходящего через брандмауэр; фильтр блокирует любые подозрительные или опасные соединения до того, как они попадут на опубликованный Web-сайт.

Правила публикации серверов могут использоваться для того, чтобы разрешить доступ для данных протоколов HTTP (если вы не хотите применять правило Web-публикации, вы можете использовать правило публикации серверов), HTTPS (HyperText Transmission Protocol Secure, протокол защищенной передачи гипертекстов), FTP, NNTP (Network News Transfer Protocol, сетевой протокол передачи новостей), SMTP, POP3 (Post Office Protocol v. 3, почтовый протокол), 1MAP4 (Internet Message Access Protocol, протокол доступа к сообщениям в сети Интернет), VNC (Voice Numerical Control, система числового управления с речевым вводом команд), для любых компьютеров, терминальных служб и т. д. Кроме того, за брандмауэром ISA Server 2004 вы можете публиковать серверы VPN с помощью протокола PPT.P и встроенной поддержки туннельного режима L2TP/IPSec. Вы можете опубликовать любой протокол, основанный на TCP/UDP (User Data Protocol, пользовательский протокол данных).

В этой главе мы рассмотрим понятия и пошаговые процедуры, необходимые для публикации любой сетевой службы с помощью правил Web-публикации и правил публикации серверов, которые покажут вам, как публиковать все популярные интернет-протоколы, а также некоторые менее распространенные службы, используя стандартные конфигурации и клиент брандмауэра на публикуемом сервере.

Глава 9. VPN-соединения удаленного доступа и конфигурации «узел-в-узел» в брандмауэре ISA Server 2004

Наверное, наиболее интересная и мощная новая функция, добавленная в брандмауэр ISA Server 2004, — существенно улучшенная функциональность VPN-сервера и шлюза. В ISA Server 2000 была возможность настройки брандмауэра для выполнения роли VPN-сервера и VPN-шлюза, но VPN-подключения не были подвластны политике брандмауэра. В ISA Server 2004, напротив, VPN-подключения удаленного доступа и между шлюзами починяются политике брандмауэра так же, как и любое другое соединение, осуществляемое через брандмауэр ISA Server 2004.

Функции брандмауэра ISA Server 2004, имеющие отношение к VPN, позволяют контролировать ресурсы, с которыми устанавливают соединение клиенты VPN, с точки зрения пользовательских и групповых правил. Например, если необходимо, чтобы группа пользователей при подключении к VPN могла устанавливать соединение только с сервером Exchange, используя безопасный протокол Exchange RPC

через клиент Outlook 2002, то можно создать политику брандмауэра, ограничивающую доступ этой группы только сервером Exchange при условии использования протоколов, необходимых для установления соединения с применением клиента Outlook MAPI (Messaging Application Programming Interface, интерфейс прикладного программирования электронной почты).

Теперь брандмауэр ISA Server 2004 может устанавливать VPN-подключения между шлюзами, используя туннельный режим IPSec. Это позволяет устанавливать соединение между брандмауэром ISA Server 2004 и VPN-шлюзами сторонних разработчиков, например с помощью брандмауэра ISA Server 2004 филиала можно легко установить соединение с сервером или концентратором VPN от сторонних разработчиков в главном офисе. Однако если нужно использовать брандмауэры ISA Server 2004 в качестве VPN-шлюзов как в главном офисе, так и в филиалах, то можно извлечь пользу из того, что применение L2TP/IPSec в качестве VPN-протокола «узел-в-узел» обеспечит более высокий уровень безопасности.

В этой главе мы рассмотрим понятия и пошаговые инструкции, необходимые для того, чтобы сделать брандмауэр ISA Server 2004 сервером удаленного доступа (Remote Access Server, RAS) для VPN и VPN-шлюзом (который применяется для VPN-подключений «узел-в-узел»). Это включает в себя установление соединения с VPN-шлюзами сторонних разработчиков и касается конкретных случаев публикации серверов виртуальной частной сети за брандмауэром ISA Server 2004 с помощью протокола PPTP и туннельного режима L2TP/IPSec. Также рассмотрим обеспечение исходящего доступа для клиентов виртуальной частной сети, использующих решения PPTP, L2TP/IPSec NAT-T (Network Address Translation, преобразование сетевых адресов) и IPSec NAT-T сторонних разработчиков.

Глава 10. Динамическая фильтрация и фильтрация на уровне приложений в брандмауэре ISA Server 2004

Брандмауэр ISA способен выполнять как динамическую фильтрацию пакетов, так и их динамическую проверку на уровне приложений. Набор параметров динамической фильтрации брандмауэра ISA позволяет причислить его к классу брандмауэров с динамической фильтрацией на сетевом уровне, а также к классу аппаратных брандмауэров, выполняющих подобную фильтрацию на сетевом и транспортном уровнях. В этой главе будут обсуждаться фильтры приложений и Web-фильтры.

Глава 11. Повышение скорости доступа в Интернет с помощью функции кэширования ISA Server 2004

Одно из наиболее важных конкурентных преимуществ ISA Server 2004 — программа представляет собой не только брандмауэр, сервер и шлюз виртуальной частной сети, но также является сервером Web-кэширования. Компонент Web-кэширования дает возможность ускорить доступ к Интернету пользователей вашей корпоративной сети и потенциально уменьшить общее использование полосы пропускания на всех ваших интернет-каналах связи.

В этой главе мы рассмотрим понятия и пошаговые процедуры, необходимые для настройки брандмауэра ISA Server 2004 в качестве сервера Web-кэширования. Вы узнаете, какие настройки **нужны** для оптимизации производительности Web-кэширования и как настроить цепочку Web-прокси для повышения производительности работы в Интернете пользователей из филиала и уменьшения общего использования канала связи между филиалом и главным офисом.

Глава 12. Применение ISA Server 2004 для наблюдения, ведения журналов и создания отчетов

ISA Server 2004 Enterprise Edition включает ряд новейших средств управления и мониторинга, расширяющих набор функций стандартной версии. Помимо управления и мониторинга на локальном компьютере, ISA Server 2004 Enterprise Edition включает инструменты, позволяющие использовать массивы брандмауэров ISA Server 2004 и групп брандмауэров, применяемых на предприятии.

Приложение. Основы сетевой безопасности

Для того чтобы понять, что делает брандмауэр и как работают различные функции брандмауэра, необходимо иметь представление о стеке протоколов TCP/IP и о том, каким образом злоумышленники с помощью наиболее распространенных типов вторжений и атак используют характеристики этих протоколов на различных уровнях эталонной модели OSI (Open Systems Interconnect, взаимодействие открытых систем) и сетевой модели DoD (Department of Defense, Министерство обороны).

В Приложении рассматриваются основные понятия сетевой безопасности. Дополнительный материал предназначен для тех, кто хочет освежить свои знания об уязвимых местах корпоративных сетей. Часть этого материала была взята из книги «Configuring ISA Server 2000», это будет особенно полезно для тех, кто не читал эту книгу.

Для кого предназначена эта книга

Эта книга предназначена для тех, кто хочет узнать, что такое ISA Server 2004, чем эта программа отличается от ISA Server 2000, а также от брандмауэров и программ кэширования сторонних разработчиков и как извлечь из этой программы **максимальную** пользу для защиты сети и улучшения производительности работы с Интернетом внутренних **и** внешних пользователей организации.

Эта книга не предназначена для подготовки к экзаменам или для использования в качестве учебника. Хотя она содержит полезную информацию и пошаговые упражнения, которые помогут читателям лучше ознакомиться с ISA Server 2004, и может выступать в роли дополнительного материала для подготовки к сдаче экзамена MCSA/MCSE (Microsoft Certified Systems Administrator, дипломированный администратор по системам корпорации Microsoft/Microsoft Certified Systems Engineer, дипломированный инженер по системам корпорации Microsoft), но цель этой книги состоит в том,

чтобы рассмотреть реальные **ситуации,** возникающие в работе при установке, конфигурировании, управлении и поиске неисправностей этой программы.

Инструменты и ловушки

Сертификационный экзамен 70-350 корпорации Microsoft

Ко времени написания данной книги сертификационный экзамен 70-350 корпорации Microsoft под названием *Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2004* (Установка, конфигурирование и администрирование ISA Server 2004 корпорации Microsoft) еще не был написан и его основные темы еще не были известны. Информация об этом экзамене представена на обучающем Web-сайте корпорации Microsoft www.microsoft.com/learn ing/mcpexams/defau lt. asp.

Тем, кто хочет заранее приступить к подготовке к экзамену по ISA Server 2004, лучше начать с руководства по подготовке к экзамену 70-277 под названием *Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition* (Установка, конфигурирование и администрирование ISA Server 2000, Enterprise Edition). Во время написания данной книги экзамен 70-277 не только считался факультативным для получения сертификата MCSA и MCSE, но также представлял собой наиболее важный экзамен по средствам обеспечения безопасности для получения сертификата MCSA и MCSE в сфере обеспечения безопасности. Ожидается, что экзамен 70-350 также будет относиться к сертифицированию специалистов в области средств безопасности.

При подготовке к любому современному экзамену корпорации Microsoft важнее всего перейти к непосредственной работе с программой во всем многообразии практических ситуаций в сети. Лучший способ подробно ознакомиться с интерфейсом, понятиями и административными задачами, которые необходимо знать, чтобы правильно ответить на вопросы экзамена, состоит в том, чтобы ежедневно работать с ISA Server 2004 в домашней сети, *в* сети предприятия или в виртуальной сети.

В основном данная книга основана на наших экспериментах и ошибках (мы тоже иногда кричали «Эврика!»), в процессе работы с ISA Server 2004. Эту книгу мы адресуем опытным сетевым администраторам Windows, которые хотят обеспечить безопасность своих сетей и увеличить скорость доступа к Интернету для своих пользователей, не уделяя этому все свое время; тем, кто учится программированию, перекомпиляции ядер или работе с новым синтаксисом команд; тем, кто хочет найти решение в области обеспечения безопасности, которое будет взаимодействовать с их контроллерами доменов Windows и серверами Microsoft типа Exchange и SharePoint. Эта книга адресована и опытным администраторам ISA Server 2000, и тем, кто

совсем не знаком с брандмауэрами, и тем, кто отказался от использования брандмауэров сторонних производителей.

Эта книга по своей сущности является монологом: авторы излагают свои мысли читателю. Однако все наши книги основаны на вопросах и комментариях читателей, и мы не закроем тему после того, как книга будет напечатана и окажется на книжных полках. Напротив, это всего лишь начало, и ваши отзывы помогут нам в написании следующей книги, статьи или курса. С нами можно связаться через Web-сайт www.syngress.com. Много дополнительной и обновленной информации о ISA Server 2004 можно найти на Web-сайте www.isaserver.org и на нашем Web-сайте www.msfirewall.org.

Безопасность: восходящая звезда

С наступлением нового тысячелетия в компьютерной индустрии, как и в большинстве других областей жизни, акцент сместился на новый злободневный вопрос: безопасность. Происходящие в мире события заставил и нас осознать, что мы живем в гораздо более опасное время, чем могли себе представить. Нет ничего неожиданного в том, что первое появление корпорации Microsoft на рынке брандмауэров произошло в 2000 году, когда она анонсировала свой первый полнофункциональный брандмауэр под названием Internet Acceleration and Security Server (ISA, сервер защищенного быстрого доступа к сети Интернет).

С тех пор крупнейший производитель программного обеспечения в мире продолжает укреплять свои позиции, создавая программные продукты, обладающие определенным набором функций и возможностей и обеспечивающие защиту от взломщиков, которые как будто прячутся за каждым виртуальным углом.

Как мы уже говорили в нашей первой книге об ISA Server, качественное решение в области обеспечения безопасности должно предотвращать различные типы угроз безопасности. В плане по обеспечению безопасности должна предусматриваться защита всех или нескольких из перечисленных далее пунктов:

- конфиденциальность особо секретных данных;
- целостность данных разной степени секретности;
- доступность данных разной степени секретности;
- проверка источника происхождения данных;
- работоспособность сети (защита от злонамеренной порчи системных файлов со стороны вирусов и в результате прямого вторжения).

Угрозы безопасности можно разделить на две категории: внутренние и внешние. DoS-атака (Denial-of-Service, отказ от обслуживания), инициированная взломщиком с удаленного компьютера, является внешней угрозой безопасности. Непреднамеренное удаление важных файлов сотрудником компании на рабочем месте является внутренней угрозой. Хотя главная функция брандмауэра в обеспечении защиты

от внешних угроз (проникновений в вашу ЛВС — локальную вычислительную сеть — из Интернета), ISA Server также позволяет вам установить ограничение исходящего сетевого трафика, обеспечивая защиту от некоторых (разумеется, не ото всех) внутренних угроз безопасности.

В данной главе мы рассмотрим, как развивался ISA Server вместе с развитием самой компьютерной **индустрии.** Чтобы получить разностороннее представление о том, что представляет собой ISA Server и откуда он возник, нам нужно вернуться в те времена, когда у Билла Гейтса еще не зародилась идея создания подобной программы, и посмотреть, как корпорация Microsoft рассматривала вопрос безопасности (и как эти взгляды менялись) с момента появления Windows и до наших дней.

Безопасность: какое отношение к ней имеет корпорация Microsoft?

Пользователи операционных систем (ОС) сторонних разработчиков утверждают, что на самом деле программные продукты корпорации Microsoft не могут обеспечить безопасность. Как и многие другие мифы, этот тоже основан на фактах, правда уже устаревших. Операционная система Windows, в отличие от UNIX, была изначально рассчитана на применение на отдельных ПК, а не в сети. В таком случае функции обеспечения безопасности имеют меньшее значение, а на первый план выходит удобство для пользователя.

Краткая история возникновения Windows

Акцент на удобстве для пользователей принес Windows популярность сначала как операционной системе для настольных компьютеров, а затем для серверов. Прочие операционные системы, например Macintosh от Apple и современная ОС X, основанная на UNIX, а также различные дистрибутивы от Linux, предназначены для конкретных групп пользователей, и даже более старые операционные системы типа MS-DOS и OS/2 по-прежнему используются в некоторых бизнес-средах. Однако операционная система Windows имеет больше различных установок. Большинство новых ПК поставляются производителями аппаратного обеспечения с предустановленной последней версией Windows. Это означает, что большинство пользователей знакомы с интерфейсом Windows. То, что именно этот интерфейс пользователи хотят видеть на своих компьютерах, подтверждается тем, что большинство популярных графических оболочек настольных компьютеров для UNIX/Linux, например KDE, делают эти операционные системы внешне похожими на Windows.

В начале 1990-х гг. большинство бизнесменов отдавали предпочтение программному обеспечению для сервера NetWare от Novell, а университеты и интернет-провайдеры обычно использовали в качестве сетевого программного обеспечения UNIX. К концу 1990-х гг. ОС Windows NT практически полностью вытеснила NetWare с рынка.

Также в 1990-х гг. коммерциализация Интернета и его последующая доступность для частных и бизнес-пользователей по низким ценам изменили компьютерную индустрию. Персональные компьютеры больше не использовались исключительно как отдельные машины для создания текстовых документов, выполнения вычислений или игр. Теперь большинство домашних и офисных компьютеров подключены к глобальной сети напрямую или через ЛВС (Local Area Network, LAN). Популярность Интернета для поиска информации, обмена сообщениями по электронной почте или живого общения в чатах, «Web-серфинга» и сетевых игр также привели к увеличению числа домашних ЛВС, многие из которых были созданы специально для обеспечения совместного доступа к Интернету.

Новый акцент на безопасности

По мере развития компьютерной индустрии от изолированных компьютеров к взаимодействию между ними менялась и Windows. Компьютерные сети должны обеспечивать доступность данных, но природа компьютерных сетей также требует введения ограничений на доступность данных. Корпорация Microsoft поздно пришла на рынок средств обеспечения безопасности, так же как она запоздала с применением идеи подключения к Интернету. Однако, когда уровень угрозы повысился и важность обеспечения безопасности стала очевидной, каждая последующая операционная система Windows стала включать в себя все больше функций, предназначенных для защиты самой себя и своих данных от неавторизованного доступа и атак.

Это перемещение акцента со свойств и функциональности на безопасность произошло не внезапно. Корпорация Microsoft, как и другие разработчики программного обеспечения, на своем опыте поняла важность обеспечения безопасности для нее самой и для ее клиентов. В 2001 г. большой урон серверам Windows нанесли черви Code Red и Nimba, и это активизировало разработчиков. Вскоре после этого корпорация представила новую концепцию надежной вычислительной техники.

Программы корпорации Microsoft имели преимущества по сравнению с программами других производителей, и это было основным фактором успеха на фоне конкурентов. К примеру, Microsoft, благодаря публикации своих API (Application Programming Interface, программный интерфейс приложения) дала возможность писать приложения, которые могли взаимодействовать с их операционной системой. (Написать модуль NLM — NetWare Loadable Module, загружаемый модуль системы NetWare — для операционной системы NetWare было гораздо сложнее.) По мере того, как корпорация Microsoft добивалась все больших успехов, усиливалась и враждебность по отношению к ней — API и другие зацепки стали использоваться взломщиками.

Инициатива по созданию надежной вычислительной техники

В вопросах обеспечения безопасности так же, как и в вопросах соединения с Интернетом, наблюдается следующее: если Microsoft решает разработать некоторую

концепцию, то все ведущие специалисты и работники корпорация вкладывают в достижение поставленной цели все свои знания. Выступив с инициативой надежности вычислительной техники, корпорация Microsoft признала обеспечение безопасности своей первоочередной задачей. Современные операционные системы Windows включают многообразные встроенные средства обеспечения безопасности. Службы, которые могут быть особенно уязвимыми с точки зрения безопасности, например IIS (Internet Information Server, информационный сервер Интернета), отключаются и блокируются по умолчанию. Корпорация также уделила внимание разработке и улучшению программных продуктов, предназначенных для обеспечения конкретных аспектов безопасности, включая сервер MIIS (Microsoft Identity and Integration Server, сервер интеграции и управления Microsoft), анализатор MBSA (Microsoft Baseline Security Analyser, сканер системы на установленные заплаты от Microsoft), службы SUS (Software Update Services, службы обновления программного обеспечения) и, конечно, ISA Server.

ПРИМЕЧАНИЕ Службы SUS будут переименованы в WUS (Windows Update Services, службы обновления Windows), этот новый программный продукт находился в процессе бета-тестирования в момент написания данной книги.

Инициатива по созданию надежной вычислительной техники включает в себя трехступенчатую систему безопасности (SD* Security Framework), компоненты которой приведены в табл. 1.1.

Табл. 1.1. Трехступенчатая система безопасности

Компонент системы безопасности	Реализация компонента
Безопасность, обеспечиваемая при разработке (Secure by Design)	Программисты проходят обучение по вопросам обеспечения безопасности. Код пересматривается с точки зрения безопасности. Процесс разработки программного обеспечения включает моделирование угроз, и в код встраиваются средства обеспечения безопасности
Безопасность при применении настроек по умолчанию (Secure by Default)	Программное обеспечение сконфигурировано таким образом, что его применение наиболее безопасно при использовании настроек по умолчанию, при которых все службы и функции, уязвимые с точки зрения безопасности, блокируются или отключаются по умолчанию
Безопасность в применении (Secure by Deployment)	Инструменты обеспечения безопасности предоставляются бесплатно для оказания помощи администраторам в мониторинге и решении вопросов безопасности. Автоматическое обновление обеспечивает более простую и широко распространенную установку средств по обеспечению и усилению безопасности

ПРИМЕЧАНИЕ Позже в систему был добавлен четвертый компонент — взаимодействие с потребителями, т. е. двухсторонний процесс общения: корпорация учитывает пожелания потребителей в вопросах безопасности и распространяет информацию о безопасности среди потребителей и широкой аудитории.

Корпорация Microsoft также делает упор на безопасности в своих взаимоотношениях со сторонними разработчиками, партнерами и потребителями. На Web-сайте Microsoft было размещено сообщение о том, что в период с февраля по июнь 2004 г. корпорация планирует организовать обучение по вопросам безопасности более чем для четверти миллиона своих потребителей; эта акция была осуществлена в виде ряда тренингов по безопасности, проводимых в разных городах. Они провели маркетинговую кампанию, суть которой заключалась в том, чтобы лучше познакомить пользователей своих программных продуктов — как рядовых, так и корпоративных — с вопросами безопасности. Выпущен служебный пакет программ Service Pack 2 для Windows XP, решающий многие проблемы безопасности, корпорация выделила миллионы долларов на распространение этого компакт-диска.

Помимо исправления ошибок в коде, связанных с обеспечением безопасности, служебные пакеты программ включают также изменения в интерфейсе и объяснения, которые помогут конечным пользователям получить более ясное представление о последствиях конкретных действий для безопасности. Например, были изменены предупреждения и функции Authenticode (кода проверки подлинности) для устранения сбоев при установке кода ActiveX. Это решает проблему программного обеспечения, которое неоднократно просит пользователя установить его, в результате чего многие пользователи в итоге сдаются и от безысходности нажимают клавишу «Yes» (Да).

В сертификационный экзамен MCSE/MCSA включен тест на специалиста в области обеспечения безопасности, а экзамен 70-298 под названием *Designing Security for a Microsoft Windows Server 2003 Network* (Разработка систем безопасности для сети на основе Microsoft Windows Server 2003) является основным экзаменом в области разработки в рамках Server 2003 MCSE.

Роль ISA Server 2004 в инициативе Microsoft по обеспечению безопасности

Модернизированная программа ISA Server 2000, представляющая собой улучшенный брандмауэр, является логическим продолжением работы корпорации по осуществлению своей инициативы в обеспечении безопасности. В качестве примера нового акцента на безопасности можно привести тот факт, что Билл Гейтс обратил особое внимание на демонстрацию бета-версии ISA Server 2004 в своем основном докладе на компьютерной выставке COMDEX в ноябре 2003 г.

С помощью ISA 2004 Microsoft рассчитывает выйти на один уровень с крупнейшими игроками на рынке промышленных брандмауэров, Checkpoint и Cisco, и конкурировать с массой готовых к непосредственному использованию брандмау-

эров и устройств VPN низшего ценового диапазона производства NetScreen, WatchGuard, SonicWall и др. Чтобы удовлетворить потребности малого и среднего бизнеса, а также пользователей на предприятиях, ISA 2004 (как и ISA 2000) поставляется в двух видах — Standard Edition и Enterprise Edition — с широким набором функций, который легко масштабируется и беспрепятственно взаимодействует с другими сетевыми программными продуктами от Microsoft (операционные системы Windows для сервера и клиента, серверы Exchange, SharePoint, SQL и др.).

Безопасность: подход, основанный на политике

Департамент полиции был бы бесполезен, если бы не было законов, исполнение которых он должен обеспечивать. Точно так же брандмауэр и другие средства обеспечения безопасности не принесут пользы для вашей сети, если у вас нет правил и руководящих принципов, выполнение которых они должны обеспечивать.

Информация, имеющая критически важное значение для компании, включая финансовые данные, данные о персонале, покупателях и коммерческие тайны, хранится виртуально в одном месте: в сети предприятия. Это делает информацию уязвимой для неавторизованного доступа и случайного или преднамеренного повреждения как изнутри, так и извне (если локальная сеть подключена к Интернету, как большинство других локальных сетей). Реализация мер по обеспечению безопасности должна быть основана на плане, в котором учитываются все потребности организации в защите. Выполнение плана должно осуществляться в соответствии с правилами и руководящими принципами — *политиками*. Средством обеспечения этих политик является брандмауэр.

Что такое политика безопасности?

Политика безопасности — письменный документ, определяющий подход организации к безопасности или определенной сфере безопасности (в данном случае это компьютерная и сетевая безопасность) и устанавливающий набор правил, которым необходимо следовать при реализации философии безопасности организации.

> ПРИМЕЧАНИЕ Руководящие принципы обычно выступают в роли рекомендованных процедур, а не жестких правил. Они могут дополнять, но не замещать политики.

Организации могут устанавливать как устные правила, так и выпускать документы различных типов, связанные с вопросами безопасности.

Стандарты и спецификации безопасности

Стандарты и спецификации в общем случае являются требованиями, которые должны быть удовлетворены при реализации методов обеспечения безопасности системы; они могут быть использованы для измерения или оценки общей надежности, совместимости или других характеристик системы. Например, правительство

США создало критерии, определенные в книгах *Department of Defense Trusted Computer System Evaluation Criteria* (Критерии оценки надежных компьютерных систем Министерства обороны) (также называемая «оранжевой книгой») и *Trusted Network Interpretation ofTCSEC* (Trusted Computer System Evaluation Criteria, критерии оценки пригодности компьютерных систем) (Интерпретация надежных компьютерных сетей TCSEC) («красная» книга), для оценки реализации обеспечения безопасности. Подобные системы оценки есть и в других странах. Международная организация по стандартизации (International Organization for Standardization, ISO) выпустила стандарт ISO 17799 — международный признанный набор лучших методов организации ИТ-безопасности. Ваша политика безопасности может включать в себя те или иные конкретные стандарты или политики.

Оценка потребностей в обеспечении безопасности

Нет и не может быть универсальной политики ИТ-безопасности, одинаково пригодной для всех организаций. Потребности в обеспечении безопасности различаются в зависимости от следующих моментов:

- факторы риска;
- осознаваемый и реальный уровень угрозы;
- уязвимые места в организации;
- философия организации (открытая система против закрытой);
- юридические вопросы;
- доступные денежные средства.

Важно внимательно проанализировать все эти факторы при разработке политики, которая обеспечит как надлежащую защиту, так и необходимый уровень до>лупа.

Функции обеспечения безопасности теперь встраиваются в программное обеспечение операционных систем; Windows NT/2000/XP и Windows Server 2003 включают в себя многочисленные функции обеспечения безопасности. Создано огромное количество как аппаратных, так и программных средств обеспечения ИТ-безопасности. Проводится обучение по вопросам безопасности, существуют множественные сертификаты по безопасности, а также ИТ-профессионалы, которые ко всему этому стремятся.

Это важные составляющие общего плана организации по обеспечению безопасности, но их недостаточно. Для эффективного взаимодействия всех этих частей требуется еще одно — всеобъемлющая политика безопасности.

Определение сфер ответственности

Чтобы точно оценить потребности в обеспечении безопасности, необходимо изучить инфраструктуру компании, рабочие процессы и методы и привлечь к этому персонал всех уровней организации из как можно большего числа ее отделов. В идеале эти задачи выполняются тщательно отобранной комиссией, которая включает в себя, как минимум, представителей руководства, ИТ-персонал и юридичес-

кого представителя компании. Каждый член комиссии должен отвечать за определенную сферу работы, следует назначать сроки выполнения каждой задачи. Разработка политики безопасности включают в себя следующие шаги:

- анализ факторов риска;
- оценка угроз и уровней угроз;
- анализ уязвимых мест организации и сети;
- анализ философии организации;
- анализ юридических факторов;
- анализ стоимостных факторов;
- оценка решений по обеспечению безопасности.

Анализ факторов риска

Прежде чем комиссия по разработке политик безопасности начнет создавать политики, она должна определить природу и уровень риска для безопасности организации. Традиционно анализ риска включает в себя:

- определение брешей, которые могут возникнуть в системе защиты организации;
- определение вероятности появления каждого типа бреши;
- определение размеров убытков в случае возникновения бреши (для каждого типа бреши).

Такой анализ называется *количественным анализом риска*.

Инструменты и ловушки

Формула для количественного анализа риска

Стандартная промышленная формула количественного анализа риска такова:

ALE = SLE x ARO, или

Ожидаемая величина убытков в годовом исчислении (Annualized Loss Expectancy, ALE) = Размер однократного убытка (Single Loss Exposure, SLE) x Частота убытков в годовом исчислении (Annualized Rate of Occurrence, ARO).

Параметр SLE — произведение номинальной стоимости активов и фактора подверженности убыткам. Например, фактор риска того, что массированная вирусная атака происходит как минимум раз в год и что до уничтожения вируса будет заражено как минимум 60% компьютеров в сети, составляет 80%. Далее представьте, что стоимость удаления вируса с рабочих станций составляет примерно $60 за одну станцию (исходя из почасовой оплаты работы), а у вас есть 500 рабочих станций. Тогда SLE составит 500 Ч 60 x 0,6 = 118 000. ALE тогда составит 18 000 x 0,8 (ARO) = $14 400.

В этом примере не учитывается стоимость утраченных данных и вложенного труда, поэтому реальные расходы еще больше.

Качественный анализ риска не учитывает вероятность, а сосредоточен на потенциальных угрозах и характеристиках системы/сети, которые делают ее уязвимой для этих угроз. Также разрабатываются методы предотвращения и снижения вероятности возникновения брешей, определяющие, когда возникают бреши, уменьшения убытков и восстанавления урона в случае, если брешь все же возникнет.

Существуют инструменты анализа риска, помогающие определить угрозы и уязвимые места, оценить уровень угрозы, ее влияние на организацию и рекомендуемые решения. В качестве примера можно привести консультанта по рискам COBRA от C&A Systems Security Ltd. Этот метод используется крупнейшими корпорациями и правительственными организациями.

Анализ риска необходим, потому что:

- сточки зрения ИТ-профессионалов, тщательный анализ риска — это первый и, пожалуй, наиболее важный шаг в оправдании перед руководством расходов на осуществление необходимых мер безопасности;
- с точки зрения коммерческого директора, документ об анализе риска обеспе чивает надежную объективную основу для принятия решений, имеющих отно шение к бюджету и к персоналу;
- сбор данных во время проведения анализа риска заставляет как ИТ-персонал, так и руководство признать наличие угроз и уязвимых мест, о которых они, возможно, не знали раньше или на которые они могли раньше не обращать внимания;
- анализ риска позволяет организации сосредоточить свои ресурсы на устране нии существующих угроз и уязвимых мест и не тратить время и средства на меры, которые не принесут пользы.

Поскольку в процесс анализа риска вовлечен весь персонал организации, то анализ риска может повысить осведомленность сотрудников по вопросам безопасности и сделать так, чтобы каждый, использующий компьютеры и сеть, отвечал за соблюдение соответствующих мер безопасности. Это основной принцип предотвращения правонарушений.

Оценка угроз и уровней угроз

Словарь определяет *угрозу {threat)* как «вероятность того, что кто-либо или что-либо причинит вред». Раздел анализа риска по оценке угрозы должен включать в себя:

- источники потенциальных угроз;
- природу потенциальных угроз;
- вероятность возникновения каждого типа потенциальной угрозы;
- предполагаемое влияние каждого типа потенциальной угрозы.

Источники потенциальных угроз можно разделить на внутренние и внешние. Хотя многие политики безопасности сосредоточены на угрозе бреши в системе безопасности извне (из Интернета), в действительности многие организации об-

наруживают, что наиболее крупные потенциальные убытки исходят изнутри — умышленные или непреднамеренные действия сотрудников, подрядчиков и тех, у кого есть законный доступ к сети. При выполнении оценки угрозы нужно учитывать обе категории угроз.

При дальнейшем определении источников угрозы оценочная комиссия должна определить, *кто* и *что* может представлять угрозу для сети. Например, к людям, представляющим угрозу, относится большинство типов виртуальных преступников, о которых мы поговорим в главе 3, например:

- случайные взломщики, которыми движет желание поразвлечься, доказать себе, что они могут проникнуть в сеть, или посоревноваться с другими взломщиками;
- похитители информации, объектом которых является организации, точнее, информация; эта категория включает промышленный шпионаж;
- люди, движимые эмоциями, например желающие отомстить бывшие сотрудни ки, деловые конкуренты, которые хотят нанести урон компании в ведении дел, или люди, затаившие злобу на компанию, ее сотрудников или отрасль промыш ленности, в которой она работает;
- люди, которые нечаянно или по неосторожности причиняют вред или приво дят к утрате данных (чаще всего это внутренняя угроза, например непреднаме ренное удаление важных файлов с сервера в результате «эксперимента» работ ника).

Природа возможных угроз в этом равенстве выражается переменной *«что»*. Любая из вышеперечисленных категорий людей может инициировать угрозу, имеющую одну или несколько характерных черт:

- неавторизованный доступ к данным;
- неавторизованное разглашение информации;
- разрушение данных;
- изменение или порча данных;
- заражение вирусами, червями или троянскими конями;
- отказ или прерывание обслуживания, перегрузка или замедление работы сети.

ПРИМЕЧАНИЕ В программе тщательной оценки угроз не должны быть упущены такие угрозы, как пожар, наводнение, отключение электроэнергии, а также угрозы, исходящие от людей.

Следующим шагом в анализе угроз является оценка вероятности возникновения угрозы каждого из типов. Высокая вероятность означает, что представляющее угрозу событие скорее произойдет, чем не произойдет, например подобные случаи уже происходили в прошлом. Средняя вероятность означает, что представляющее угрозу событие может произойти, а может и нет. Низкая вероятность означает, что событие, представляющее угрозу, вряд ли случится, хотя оно возможно. Наконец, оценочная комиссия должна определить возможное влияние на организацию лю-

бого события, представляющего потенциальную угрозу. Приведем несколько примеров.

- Если бы была уничтожена база данных клиентов компании, как это повлияло бы на продажи и выписку счетов?
- Если бы компьютерная сеть компании вышла из строя на один день, во сколько бы это обошлось компании в материальном и нематериальном выражении, например потери в продажах или производительности труда?
- Если бы база данных **клиентов** компании была предана огласке, каковы были бы потенциальные потери компании с учетом судебных процессов, отказов клиентов работать с компанией и других выплат, уменьшающих прибыль ком пании?

После того, как ответы на эти вопросы определены, довольно просто создать матрицу оценки угрозы, которая позволит представить эту информацию *Е* перспективе и поможет комиссии по разработке политики безопасности сосредоточить политики безопасности компании на тех сферах угроз, которые наиболее вероятны и имеют наиболее существенные последствия.

Анализ слабых мест в системе защиты организации и сети

Технически слабые места в системе защиты сети — это те характеристики или особенности **конфигурации,** которые могут быть использованы злоумышленником для получения неавторизованного доступа к вашей сети или неправомерного использования вашей сети и ее ресурсов. Слабые места в системе защиты сети часто называют *дырами в системе защиты.* Дыры в системе защиты должны быть определены в процессе разработки политики безопасности. Эти слабые места в системе защиты могут быть обусловлены программными характеристиками или настройками (некорректными настройками) операционной системы, служебным протоколом или приложением. В качестве примеров можно привести следующие:

- код операционной системы, позволяющий хакерам получить доступ к файлу, путь к которому содержит определенные зарезервированные слова, и вызвать, пол ную остановку компьютера;
- ненужные открытые порты TCP/UDP, которые могут использоваться хакерами для проникновения или получения информации о системе;
- пользование интернет-браузером языка JavaScript, что позволяет вредоносно му коду исполнять нежелательные команды.

Соединения сети с Интернетом и другими сетями очевидно влияют на ее уязвимость. Информация в сети, подключенной к Интернету по высокоскоростной линии 24 часа в сутки 7 дней в неделю, более уязвима, чем в сети, лишь иногда устанавливающей внешние соединения. Сеть, в которой возможны различные внешние соединения, например на нескольких различных компьютерах есть модемы и телефонные линии, повышает собственную уязвимость для внешних атак. Особого внимания заслуживают коммутируемые модемные соединения (dial-up) Хотя

dial-up соединение менее открыто для вторжений, чем постоянное соединение по выделенной линии, потому что имеет меньшую продолжительность, что уменьшает возможность вторжений, и еще потому что соединению обычно присваивается динамический IP-адрес, что затрудняет задачу злоумышленника установить его местонахождение в различных случаях; тем не менее установка модемов и телефонных линий на рабочих станциях в сети может подвергать безопасность сильному риску.

При неправильной настройке компьютер с dial-up подключением к Интернету, который также имеет кабельное соединение с внутренней сетью, может играть роль маршрутизатора, что позволяет злоумышленникам получать доступ извне не только к самой рабочей станции, подключенной к модему, но и к другим компьютерам в локальной сети. Единственная причина разрешения установки модемов на отдельных рабочих станциях состоит в необходимости установки dial-up соединения с другими частными сетями. Более безопасный способ — убрать модемы и сделать так, чтобы пользователи устанавливали VPN-соединения с другой частной сетью через интернет-соединение локальной сети. Лучшая политика безопасности заключается в том, чтобы во внутренней сети было как можно меньше внешних подключений и чтобы на этих точках (по *периметру сети)* осуществлялся контроль доступа.

> ПРИМЕЧАНИЕ Программные средства сторонних разработчиков, известные как сканеры слабых мест в системе защиты, предназначены для того, чтобы обнаружить слабые места в системе защиты сети при помощи базы данных известных слабых мест, которые подвергаются атакам, и проверке вашей сети на наличие этих слабых мест.

Слабые места в системе защиты организации — это области и данные, открытые для угрозы или нанесения вреда при совершении атаки. Для определения этих слабых мест комиссия по разработке политики безопасности должна сначала оценить активы, которые могут быть подвержены типам угроз, определенных ранее. Например:

- финансовые документы компании;
- профессиональные тайны;
- информация о сотрудниках;
- м информация о покупателях/клиентах;
- частная переписка;
- интеллектуальная собственность;
- документы по стратегии бизнеса и маркетинга;
- целостность сети;
- системные и программные файлы.

Существует ряд факторов, которые нужно учесть при оценке слабых мест в системе защиты, в том числе тип информации, проходящей по сети организации. Уяз-

вимости особо секретных данных, таких как профессиональные тайны, или незаменимых, таких как авторские произведения, должен быть присвоен высший приоритет. На степень уязвимости также влияет размер организации и сети. Чем больше людей имеет доступ к сети, тем выше вероятность того, что среди них окажется тот, кто захочет нанести вред.

Анализ организационных факторов

Следующий шаг оценки потребностей в обеспечении безопасности состоит в определении философии руководства организации в вопросе равновесия между безопасностью и доступностью. Эти две характеристики являются несовместимыми — чем выше одна, тем ниже другая. Философия организации определяет, какое равновесие безопасности и доступности будет применяться в этой конкретной сети (что обусловит ее политики безопасности).

В некоторых компаниях принят высоко структурированный, формальный стиль управления. Работники должны соблюдать строгую субординацию, а информация обычно распространяется по принципу «кому нужно знать». Правительственные организации, особенно имеющие отношение к исполнению законов, например полиция и следственные органы, часто имеют такую же философию. Иногда такую модель называют *полувоенной.*

Другие компании, особенно работающие в творческих сферах и в других областях, мало подверженных контролю со стороны государства, построены на противоположном принципе: все сотрудники должны располагать как можно большим количеством информации, менеджеры должны выступать в роли лидеров группы, а не властных начальников, ограничения на действия работника должны накладываться, только если это необходимо для эффективности и производительности организации. Эту модель иногда называют *«одна большая счастливая семья»* Творческий подход здесь ценится больше, чем «следование букве», а удовлетворение от работы считается важным аспектом повышения производительности труда работника.

С точки зрения управления бизнесом, эти две диаметрально противополэжные модели называются *теория x* (традиционная полувоенная модель) и *теория Y* (современная модель, ориентированная на команду). Хотя существует огромное количество других моделей управления, которые стали популярными в последнее время, например управление целью (Management by Objective, MBO) и управление, ориентированное на общее качество (Total Quality Management, TQM), стиль управления в каждой компании представляет собой нечто промежуточное между теорией X и теорией Y. Модель управления основана на личном представлении топ-менеджеров компании о том, какими должны быть отношения между руководителями и работниками.

Модель управления может иметь сильное влияние на то, что является приемлемым, а что неприемлемым при планировании системы безопасности сети. Политика безопасности, основанная на принципе «запретить любой доступ», которая

считается приемлемой в организации с управлением по теории X, может столкнуться со столь сильным возмущением и недовольством сотрудников в компании с управлением по теории Y, что это создаст проблемы в работе организации. Специалисты, создающие политики безопасности, должны учитывать атмосферу в компании как часть планирования безопасности. Если существуют серьезные причины для принятия жестких мер по обеспечению безопасности в компании с управлением по теории Y, то, вероятно, следует оправдать эти ограничения перед руководством и представить работникам, в то время как те же самые ограничения скорее всего будут безоговорочно приняты в более традиционной организации.

Анализ юридических факторов

Требования к безопасности зависят не только от пожеланий руководства компании, они могут быть продиктованы уголовным и гражданским законодательством в конкретной области юрисдикции. Если сфера деятельности компании регулируется государством, или информация в ее сети подпадает под действие законов по обеспечению секретности, или же договоры компании запрещают раскрытие информации в сети компании, то эти юридические факторы должны учитываться при разработке политик безопасности.

Повреждение и защита

Когда безопасность является обязательной

В Соединенных Штатах, как и во многих других странах, существуют законы по обеспечению секретности в определенных отраслях, влияющие на план и политики безопасности организации. Например, закон об отчетности по страхованию здоровья (Health Insurance Portability and Accountability Act, HIPAA) предписывает хранение и передачу в электронном виде информации о пациентах и требует, чтобы врачи и другие работники здравоохранения соблюдали определенные стандарты безопасности, уведомляли пациентов о принятых мерах по защите их личной информации и документировали каждый случай разглашения информации о пациенте третьим лицам (за некоторыми исключениями). Вся работа в области здравоохранения должна была соответствовать этому закону с апреля 2003 г. Нарушение положений этого закона может стать причиной наложения штрафных санкций от $100 (за нарушение) до $250 000 и до 10 лет тюрьмы в случае преднамеренного разглашения информации о пациенте с целью ее продажи, передачи третьим лицам или использования для достижения личных, коммерческих целей или со злым умыслом.

Данный закон является федеральным; в некоторых штатах также есть законы, которые обеспечивают еще более жесткую защиту личной информации в сфере здравоохранения.

(см. след. стр.)

> В других отраслях тоже есть подобные законы. Например, так называемый закон Gramm-Leach-Bliley (GLB) устанавливает ограничения для финансовых учреждений относительно разглашения личной информации клиента, за нарушение этого закона также предусмотрены наказания.

Важно обеспечить **защиту** вашей компании от обязательств, которые она должна будет понести в случае, если ее сотрудники или третьи лица, использующие ее сеть, нарушат законы. Поэтому очень важно, чтобы в комиссию по разработке политики безопасности входил один или несколько юристов, хорошо знакомых с соответствующим законодательством (например, с законом о защите информации Data Protection Act в Великобритании, законом об авторских правах Digital Millenium Copyright Act в США) и осведомленных об условиях договоров компании с ее партнерами, поставщиками, клиентами и т. д.

Оценка факторов стоимости

Наконец, оценка потребностей в обеспечении безопасности должна учитывать денежную стоимость обеспечения повышенных мер безопасности. Определение доступных средств для модернизации системы безопасности заставит комиссию по разработке политик провести различие между потребностями и желаниями организации в обеспечении безопасности. При этом полезным может оказаться количественный анализ риска, поскольку для определения соотношения цена/польза он основывается на поддающихся контролю данных.

Фактор стоимости также может заставить комиссию расставить приоритеты различных потребностей в безопасности так, чтобы основное внимание уделялось угрозам, имеющим наибольшую вероятность, чтобы наиболее важные данные: были защищены и чтобы прежде всего была обеспечена защита наиболее явных слабых мест в системе защиты.

Оценка решений по обеспечению безопасности

После того, как компания определила и закрепила в документах свои потребности в безопасности и установила рабочий бюджет для реализации этих потребностей, можно оценить решения и определить, какое или какие из них удовле творя ют эти потребности с учетом имеющегося бюджета. Решения в области обеспечения сетевой безопасности можно в общем разделить на три обширные категории: решения, основанные на политиках, аппаратные решения и программные решения.

Решения, основанные на политиках

Большинство мер по обеспечению безопасности, основанных на аппаратном и программном обеспечении, включают в себя политики и указания по их применению, но есть и много мер по обеспечению безопасности, состоящих только из политик. Например:

- политики, которые запрещают пользователям передавать другим свои пароли;
- политики, которые обязывают пользователей блокировать свои рабочие стан ции, когда они выходят из-за стола;
- политики, которые обязывают пользователей получать разрешение, прежде чем устанавливать любое программное обеспечение на своем компьютере;
- политики, которые запрещают пользователям разрешать третьим лицам пользо ваться их компьютером после того, как они выполнили его загрузку.

Разумеется, во многих случаях политики накладываются и при использовании программных и аппаратных средств защиты. Например, политика, запрещающая пользователям выключать компьютер, может быть наложена с помощью настройки групповой политики (Group Policy) в объекте политики локальной безопасности (Local Security policy object). Политика, требующая, чтобы пользователи меняли свои пароли каждые 30 дней, может быть создана, если настроить срок действия паролей.

Аппаратные решения

Решения по обеспечению безопасности, основанные на аппаратном обеспечении, включают добавление некоего физического устройства типа специализированного брандмауэра для обеспечения защиты сети или устройства для чтения смарт-карт для аутентификации при загрузке. К аппаратным решениям также относится удаление с настольных компьютеров CD-приводов и накопителей на гибких дисках для предотвращения несанкционированного копирования файлов или заражения вирусами. Прочие аппаратные средства обеспечения безопасности включают:

- устройства фиксации нажатия клавиш для мониторинга использования компью тера;
- аппаратные маркеры для хранения ключей безопасности;
- шифровальные аппаратные устройства для разгрузки процессора по выполне нию операций шифрования;
- биометрические устройства аутентификации, например сканеры отпечатков пальцев или сетчатки глаза.

Аппаратные решения могут быть дороже программных, но они имеют несколько преимуществ: меньше разглашается информация, имеющая отношение к безопасности (секретные ключи), аппаратное обеспечение более устойчиво к действиям злоумышленников, чем программное. Также аппаратные решения часто обеспечивают более высокую производительность.

Программные решения

Программные решения включают системы обнаружения вторжений, программы фильтрации пакетов/каналов/данных уровня приложения, программы аудита, а также пакеты программных брандмауэров типа ISA Server от корпорации Microsoft, который сочетает в себе эти функции. Есть и другие программные решения по обес-

печению безопасности: антивирусные программы, например от Symantec и McAfee, программы-шпионы, отслеживающие, как используются компьютеры (выключая программы-анализаторы пакетов, которые фиксируют и анализируют сетевой трафик) и пакеты управления сетью, включающие функции обеспечения безопасности. К этой категории также можно отнести заплаты к операционным системам и приложениям, которые закрывают бреши в системе безопасности.

Таким образом, брандмауэры являются лишь одним из многих способов, разработанных для реализации ваших политик безопасности. Это приводит нас к понятию *многоуровневой безопасности.*

Безопасность: многоуровневый подход

Определение понятия безопасность (из словаря American Heritage Dictionary): «Б*езопасность — это свобода от риска или опасности, надежность».* Возможно, это определение по отношению к компьютерной и сетевой безопасности является дезориентирующим, поскольку оно подразумевает такую степень защиты, которая, в сущности, невозможна в современной компьютерной среде, ориентированной на множество соединений.

Поэтому этот же словарь приводит еще одно определение специально для вычислительной техники: *«Уровень, до которого программа или устройство защищено от неавторизованного применения».* В этом определении подразумевается, что цели безопасности и доступности — двух главных ориентиров для многих сетевых администраторов — являются по самой своей природе диаметрально противоположными. Чем более доступна информация, тем менее она безопасна; чем сильнее вы ее охраняете, тем больше вы затрудняете к ней доступ. Любой план по обеспечению безопасности является попыткой установить равновесие между этими двумя параметрами. Первый шаг состоит в уточнении того, *что* нуждается в защите и до какой степени. Поскольку не все данные являются в равной мере ценными, некоторые данные требуют более надежной защиты, чем остальные. Это приводит нас к концепции необходимости установления нескольких уровней безопасности. Многоуровневая безопасность — это широкое понятие, относящееся не только к информационной, но и к физической безопасности. Термин «всесторонняя защита» используется специалистами по информационным технологиям для описания этого понятия применительно к защите компьютеров и сетей, хотя первоначально этот термин использовался военными. В следующих разделах мы рассмотрим важность многоуровневой безопасности и решений по обеспечению всесторонней защиты.

Важность многоуровневой безопасности

Эффективный план по обеспечению безопасности не основывается только на одной технологии или одном решении, напротив, он характеризуется многоуровневым подходом. Сравните это с мерами по обеспечению физической безопасности бизнеса; большинство компаний не ограничиваются замками на офисах, чтобы

избежать нападений воров, они также устанавливают защиту по периметру (забор), возможно, применяют дополнительные внешние средства защиты (охранников или сторожевых псов, внешнюю и внутреннюю сигнализацию), а для защиты особо ценных вещей еще и внутренние средства защиты (сейфы). Такой же многоуровневой должна быть защита в области информационных технологий. Например:

- брандмауэры на точках входа в сеть (и по возможности демилитаризованные зоны или экранированная подсеть между ЛВС и сетевым интерфейсом, подклю ченным к Интернету), функционирующие как защита по периметру;
- защита паролей на локальных компьютерах, требующая проверки подлиннос ти пользователя при загрузке, чтобы неавторизованные пользователи не могли войти в компьютер;
- набор настроек доступа на каждом из сетевых ресурсов, чтобы ограничить до ступ тех, кто уже в сети (вошел в сеть);
- шифрование данных, передаваемых по сети Или хранящихся на диске, чтобы защитить наиболее ценную и секретную информацию;
- серверы, маршрутизаторы и концентраторы должны быть расположены в за крытых помещениях, чтобы предотвратить хищения данных со стороны тех, кто имеет физический доступ.

С точки зрения многоуровневого подхода, разбита на уровни должна быть не только система безопасности, но и весь подход к вопросам безопасности в организации. То есть безопасность должна быть сосредоточена на технологиях, рабочих процессах и людях. Например, к многоуровневой безопасности относится наличие хороших политик безопасности и их выполнение, отлаженный механизм приема новых сотрудников и обучение пользователей.

Несколько линий обороны

Поскольку в больших сетях более одной точки "входа», сами брандмауэры могут наиболее эффективно использоваться на нескольких уровнях сети предприятия. Возвращаясь к аналогии с физической безопасностью, при защите вашего дома или офиса от воров вы установите несколько периметров защиты. Внешний периметр вы можете обозначить забором, окружающим вашу собственность. Внутренний периметр создают стены вашего дома или офисного здания.

Точно так же в крупной сети брандмауэры размещены вдоль границы (там, где сеть компании подключается к Интернету). Отделы или подсети могут использовать брандмауэры для создания внутренних периметров и для защиты внутренних серверов и клиентских компьютеров от других отделов или подсетей в сети компании.

Несколько брандмауэров могут использоваться для выполнения различных функций. В нашем примере у вас есть забор, который не пускает посторонних в ваш двор. У вас еще может **быть** злая собака, которая выполняет защиту на этом же уровне

(защищает внешний периметр), но собака, в отличие от забора, может решать, кого пропускать во двор, а кого нет. Собака может узнать членов вашей семьи и друзей, часто заходящих к вам во двор, и разрешит им пройти, а если к забору подойдет незнакомый человек, она будет лаять и рычать.

Брандмауэры с фильтрацией пакетов выполняют роль забора. Они мало интеллектуальны. Их фильтрация происходит на основе простых критериев, содержащихся в заголовках пакетов. Брандмауэр с фильтрацией данных уровня приложения, который помещают «за забором» (за брандмауэром с фильтрацией пакетов) является более интеллектуальным. Так же, как собака, которая может определить характерные отличительные черты того, кто пытается войти к вам во двор, чтобы решить, друг это или незнакомец, фильтры на уровне приложения могут анализировать содержимое пакетов данных, чтобы определить, содержатся ли в них опасные коды.

Использование брандмауэров на разных уровнях или совместное применение различных типов брандмауэров для выполнения разнообразных задач сильно повышает эффективность вашего плана по обеспечению безопасности. Мы обсудим разные типы брандмауэров (с фильтрацией пакетов, каналов, данных на уровне приложения) более подробно в разделе «Брандмауэры: свойства и функции».

Брандмауэры: стражи у ворот

На Web-сайте координационного центра CERT (Computer Emergency Response Team, группа компьютерной «скорой помощи») содержатся данные, согласно которым число известных брешей в системах безопасности ежегодно возрастает на 50—100%. Хакеры создают все более изощренные инструменты для атак, чтобы автоматизировать процесс атаки, тем самым уменьшая уровень технической оснащенности, необходимой для организации атак на сети. Начинающим хакерам не нужно обладать знаниями в области программирования, чтобы атаковать ваши серверы и сети, но широкий доступ к таким инструментам превращает начинающих хакеров в растущую и серьезную угрозу. Можно предположить, что с течением времени ситуация только ухудшится. Из-за наличия постоянно нарастающей угрозы каждая сеть или отдельный компьютер, имеющий соединение с Интернетом, должен иметь защиту от хакерских атак, вирусов и нежелательной электронной почты (спама).

В то время, как вероятность атак возрастает, компании и частные лица все больше и больше рассчитывают на быстрые и безопасные коммуникации. У них должна быть возможность осуществлять поиск в Интернете, отправлять через Интернет сообщения сотрудникам, поставщикам и партнерам и получать доступ к сетям своей компании из дома или командировки по удаленному dial-up соединению или через виртуальную частную сеть. Все это должно быть безопасным и не идти в ущерб производительности.

Брандмауэр обеспечивает необходимую современным компаниям защиту путем фильтрации входящих и исходящих пакетов и блокирования тех из них, которые

не авторизованы, так, чтобы они не могли проникнуть в сеть. Многие производители брандмауэров расширяют функциональность своих продуктов путем добавления таких свойств, как VPN-шлюзы и прокси-серверы Web-кэширования. Эти объединенные продукты, часто называемые комплексными решениями в области безопасности и часто входящие в состав готовых к непосредственному использованию аппаратных средств, обеспечивают защиту от атак, в то же время предоставляя безопасный удаленный VPN-доступ и ускоряя доступ к Интернету.

Брандмауэр создает пункт, через который должны пройти все данные при переходе из одной сети или компьютера в другой. Программное обеспечение брандмауэра способно анализировать, создавать журналы событий и блокировать конкретные пакеты, основываясь на критериях, заданных администраторами, например размер пакета, адрес источника и даже тип файла или содержимое данных файла.

Брандмауэры: история и философия

Термин «брандмауэр» (firewall) появился задолго до возникновения компьютерных сетей. Он использовался для обозначения огнеупорной преграды, предотвращающей распространение огня из одной части строения или автомобиля в другую. Для профессионалов в области компьютерных сетей брандмауэр — это программа (устанавливаемая на обычном компьютере или выделенном аппаратном устройстве), которая способна блокировать нежелательные сетевые пакеты, например пакеты, содержащие атаки, вирусы или нежелательную коммерческую почту. Брандмауэр выступает в роли преграды, которая препятствует проходу этих пакетов из Интернета или другой сети в локальную сеть. В случае «персональных брандмауэров» (которые также называют брандмауэрами, основанными на хосте) обеспечивается защита локального компьютера, особенно если он напрямую подключен к Интернету через модем или широкополосное соединение.

В начале своего развития компьютерные сети были закрытыми системами, соединены были только компьютеры в пределах одного здания или небольшой географической области. Однако вскоре сети выросли и стали более сложными, а компьютеры, находящиеся в географически удаленных областях, могли взаимодействовать друг с другом по глобальным сетевым каналам. Первой попыткой создания такой большой сети была сеть ARPANET, *в* которую входил ограниченный круг правительственной элиты и компьютерных пользователей университета. В итоге она расширилась и стала Интернетом. В 1990-х гг. доступ в Интернет стал проще и дешевле. Появились коммерческие интернет-провайдеры, предоставляющие владельцам компьютеров доступ в Интернет прямо из дома по разумным ценам. Вскоре коммерческие и частные пользователи по всему миру, раньше не знакомые друг с другом, получили возможность общаться. Электронная коммерция стала популярным способом покупки товаров и услуг, а банковские операции и другие финансовые услуги, оказываемые в онлайновом режиме, сделали очевидной необходимость в защитных механизмах.

Один из первых интернет-вирусов, червь Morris, поразил компьютеры нескольких крупнейших учебных заведений в 1988 г. Это заставило компании и отдельных пользователей Интернета осознать опасность, которую представляет собой информационный доступ в сеть извне. Вскоре необходимость привела к изобретению брандмауэра.

Первыми брандмауэрами были маршрутизаторы. Маршрутизатор соединяет между собой две сети и является логическим местом в сети для создания ^контрольной точки», в которой пакеты анализируются и на основании этого блокируются или пропускаются дальше. Эти первые брандмауэры, основанные на маршрутизаторах, были больше ориентированы на проверку входящих, а не исходящих данных. Маршрутизаторы разделяли сети на сегменты, называемые подсетями, например различные отделы компании или университета. Это имеет несколько преимуществ, одно из которых состоит в том, что сбои в одном сегменте не повлияют на компьютеры в других сегментах. Вскоре появились IP-маршрутизаторы с функциями фильтрования, предназначенные для того, чтобы не допустить проникновения в сеть злоумышленников или пользователей, не имеющих права доступа. По современным стандартам эти брандмауэры были очень недоразвитыми. Они могли блокировать и пропускать пакеты только на основании их IP-адреса или номеров порта TCP/UDP. У них не было возможности проанализировать содержимое данных, поскольку они работали на сетевом уровне сетевой модели OSI.

«Хост-бастион» — это шлюз, предназначенный специально для защиты внутренней сети от внешних атак. Один из первых коммерческих брандмауэров этого типа, в котором применялись фильтры и шлюзы уровня приложения (прокси уровня приложения), был создан компанией DEC (Digital Equipment Corporation) в начале 1990-х гг. В 1993 г. компания TIS (Trusted Information System) выпустила свободно распространяемый брандмауэр под названием Firewall Toolkit (FWTK), затем промышленный брандмауэр Gauntlet, основанный на том же коде. Компания Checkpoint вышла на рынок брандмауэров в 1994 г., выпустив программу Firewall-1 (FW-1). Это был первый популярный брандмауэр с удобным графическим интерфейсом, позже он был использован компанией Nokia в качестве основы для создания брандмауэров-устройств.

С течением времени сетевые атаки становились все более изощренными, а сетевые протоколы все более многочисленными и сложными. Это способствовало развитию брандмауэров от простых маршрутизаторов с фильтрацией пакетов до выделенных многоуровневых устройств обеспечения безопасности.

Брандмауэры: основы архитектуры

Брандмауэры можно классифицировать несколькими различными способами: по производителю/торговой марке, по функциям или по моделям. В следующих разделах мы рассмотрим несколько важных элементов архитектуры брандмауэров:

- модели на базе аппаратного/программного обеспечения;
- брандмауэры на базе хоста/брандмауэры сетевого уровня.

Модели на базе аппаратного/программного обеспечения

Первый аспект архитектуры брандмауэра, который мы рассмотрим, это физическая архитектура: брандмауэры бывают программными и аппаратными. Эта терминология стандартная, но не совсем точная. Все брандмауэры состоят как из программных, так и из аппаратных элементов. Настоящее различие зависит от того, как данный брандмауэр позиционируется на рынке. «Программные брандмауэры» продают как программные приложения, которые можно установить на стандартную операционную систему и аппаратную платформу. «Аппаратные брандмауэры» продают как «комплексную сделку», когда программное обеспечение брандмауэра предварительно установлено на конкретную аппаратную платформу, часто со специализированной операционной системой, предназначенной именно для работы с данным брандмауэром.

Брандмауэр на базе аппаратного обеспечения

Аппаратный брандмауэр приобретается как единый модуль: аппаратное обеспечение (часто называемое устройством) с предварительно установленным программным обеспечением брандмауэра. Большинство аппаратных брандмауэров работает на базе специализированных операционных систем, разработанных именно для программного обеспечения брандмауэра, хотя на некоторых устройствах брандмауэры работают под Linux или BSD. Специализированные операционные системы не включают в себя многие сетевые службы, которые есть в обычных операционных системах. Преимуществом, с точки зрения обеспечения безопасности, считается то, что операционная система уже «подогнана» под конкретный брандмауэр и не уязвима для некоторых атак, предпринимаемых по отношению к обычным операционным системам.

Устройство — это самодостаточный модуль, предназначенный для конкретной цели. Некоторые устройства служат нескольким целям, производители их часто называют «устройствами обеспечения безопасности», чтобы отличить от «брандмауэров-устройств». Многие устройства включают в себя функции VPN-шлюзов наряду с брандмауэром, а некоторые также включают такие функции как Web-кэширование. Некоторые производители предлагают различные аппаратные компоненты (называемые лезвиями безопасности), подключаемые *к* брандмауэру. Например, модуль ГОР от NetScreen подключается к их блоку брандмауэра.

Некоторые брандмауэры-устройства в сущности являются компьютерами,, имея тот же тип жесткого диска, памяти и других компонентов стандартного компьютера. Другие называются монолитными (solid-state), поскольку в них практически нет съемных частей. В них применяется флэш-память и нет жестких дисков. Поскольку вместо механических дисков, ограниченных необходимостью физически вра-

щаться, используются высокоскоростные монолитные схемы, монолитные устройства хранения обеспечивают более высокую скорость работы.

Специализированная интегральная схема ASIC является микросхемой, созданной для контроля функций конкретного приложения. В брандмауэрах на базе ASIC применяется микросхема, разработанная для брандмауэров-приложений.

Аппаратные брандмауэры имеют и достоинства, и недостатки. Монолитная технология и использование оптимизированных операционных систем без каких-либо лишних сервисов позволяет обеспечить высокую производительность. Монолитная технология также гарантирует большую надежность, поскольку в ней отсутствуют точки для механического выхода из строя, как в брандмауэрах, основанных на жестких дисках.

Однако аппаратные брандмауэры менее адаптивны и их сложнее модернизировать. Поскольку микросхемы ASIC вошли в массовое производство, а также учитывая стоимость доработки и перепроектирования аппаратного обеспечения, внесение изменений в такие устройства с учетом новых угроз требует больше **времени.** Производителям этих устройств сложно идти в ногу с ростом вычислительной мощности компьютера. Использование стандартного компьютера с установленным программным брандмауэром всегда обходится дешевле, чем устройство с аналогичными вычислительной мощностью и памятью. Кроме того, программные брандмауэры гораздо проще интегрировать с другими сетевыми устройствами, в которых применяются те же технологии, что и в брандмауэре. Специализированные операционные системы, используемые в брандмауэрах на базе ASIC, затрудняют добавление новых программ.

Еще одно преимущество технологии ASIC (алгоритмы шифрования для VPN и SSL встроены в микросхему) нивелируется тем фактом, что Intel начала встраивать алгоритмы шифрования в свои обычные микросхемы, которые могут использоваться программными брандмауэрами.

И наконец, динамический характер и сложность алгоритмов, используемых для глубинной фильтрации уровня приложения, делают ее менее подходящей для технологии ASIC. Сравнения производительности показали, что программные брандмауэры имеют преимущество в производительности и надежности по сравнению с брандмауэрами, основанными на ASIC.

Брандмауэры на базе программного обеспечения

Так называемый «программный брандмауэр» — это брандмауэр, который позиционируется на рынке как программный продукт, устанавливаемый на базе одной или нескольких различных операционных систем и аппаратных платформ. ISA Server 2004 — это программный брандмауэр, который можно установить на компьютере с операционной системой Windows 2000 Server или Windows Server 2003.

Некоторые брандмауэры позиционируются одновременно как программные продукты и как предустановленные на аппаратных устройствах брандмауэры. Checkpoint NG — это программный брандмауэр, который может быть установлен на компьютере с операционной системой Windows NT или 2000 или Linux, на Solaris от Sun или на AIX разновидности UNIX от IBM. Этот брандмауэр также является основой для устройств безопасности от Nokia.

ПРИМЕЧАНИЕ Предполагается, что ISA Server 2004, помимо продажи в качестве программного брандмауэра, будет поставляться предварительно установленным на устройствах, пригодных для немедленной эксплуатации. В момент написания данной книги некоторые производители аппаратного обеспечения уже создали устройства, основанные на ISA, или вели переговоры с корпорацией Microsoft на получение лицензии для этого. У авторов данной книги была возможность произвести бета-тестирование некоторых из этих устройств, и два из них работают в нашей сети.

Главный момент состоит в том, что вы покупаете эти брандмауэры как программный продукт и устанавливаете их на подходящую операционную систему, которая может выполнять и другие функции помимо обеспечения работы программного брандмауэра.

Как и аппаратный брандмауэр, программный брандмауэр имеет свои достоинства и недостатки. Поскольку программный брандмауэр обычно работает на стандартной сетевой операционной системе типа Windows, UNIX/Linux или Solaris, то у вас, возможно, уже есть система, в которой вы можете его установить, тем самым сэкономив на стоимости аппаратного обеспечения.

Обычно конфигурация и управление являются простыми, поскольку программное обеспечение работает на базе операционной системы, знакомой администратору. Еще одно важное преимущество состоит в возможности легко модернизировать аппаратную базу. Вы можете дополнительно установить новый процессор или больший объем памяти, что обойдется относительно недорого. Вы также можете полностью заменить блок и установить программу в новой системе (если это разрешено лицензионным соглашением).

Еще одно преимущество состоит в том, что во многих случаях вы можете скачать демонстрационную версию программного брандмауэра и испытать его перед покупкой (только попытайтесь попросить у производителя аппаратного обеспечения устройство для того, чтобы опробовать его; вам откажут, если только вы не высоко привилегированный покупатель).

Программные брандмауэры также имеют свои недостатки. Обычно они работают медленнее, чем аппаратные брандмауэры, и поскольку они работают на базе стандартных операционных систем, эти операционные системы без правильно заданных настроек безопасности могут быть более уязвимыми для атак, чем специализированные операционные системы.

Модели на основе хоста и модели сетевого уровня

Еще один способ классификации брандмауэров зависит от того, предназначен ли он для работы на отдельном хосте-компьютер е или должен обеспечивать защиту группы компьютеров, всей сети или подсети. Это различие определяет разграничение брандмауэров на основе хоста и брандмауэров сетевого уровня.

Брандмауэр на основе хоста

Более распространенное маркетинговое название дешевого брандмауэра на основе хоста — персональный брандмауэр. Персональный брандмауэр устанавливается на рабочей станции или портативном компьютере, чтобы обеспечить его защиту от наиболее распространенных сетевых атак. Цена персональных брандмауэров обычно не превышает $100, также существует много бесплатно распространяемых персональных брандмауэров. Операционные системы Windows XP и Windows Server 2003 имеют встроенный персональный брандмауэр Internet Connection Firewall (IFC).

Простой брандмауэр на основе хоста блокирует входящие пакеты, основываясь на IP-адресе источника или назначения и номере порта, используя заранее настроенные правила, учитывающие нормальное поведение установленных приложений и компонентов операционной системы. Более сложные версии также могут фильтровать пакеты, основываясь на их содержимом (см. раздел «Многоуровневая фильтрация» далее в этой главе).

Любой компьютер, имеющий прямое подключение к Интернету без брандмауэра сетевого уровня, должен иметь брандмауэр, основанный на хосте. Это относится практически ко всем компьютерам, подключаемым к Интернету по аналоговому модемному соединению, а также к компьютерам, имеющим прямые широкополосные подключения (кроме тех случаев, когда широкополосный «модем» или «маршрутизатор» имеет работающее встроенное программное обеспечение брандмауэра).

Политики многих компаний требуют, чтобы на любом компьютере, подключенном к их сетям по удаленному доступу dial-up или через VPN, был установлен и активирован персональный брандмауэр, Это необходимо для того, чтобы предотвратить распространение интернет-атак от удаленных клиентов в корпоративную сеть. Именно брандмауэр уровня корпоративной сети обычно и реализует эти политики.

Брандмауэр сетевого уровня

Брандмауэры сетевого уровня, как следует из их названия, защищают всю сеть или всю подсеть, а не отдельные компьютеры. Брандмауэр сетевого уровня — это специально выделенный компьютер или устройство, на котором выполняется программное обеспечение брандмауэра, а также, возможно, связанные программы, или «модули», например кэширования или обнаружения/предотвращения вторжений, и

сетевое антивирусное программное обеспечение. Добавить эти дополнительные функции можно двумя способами:

- **On box (все на одном компьютере)** Дополнительные функции или встроены в программное приложение брандмауэра, или устанавливаются на том же компьютере в виде отдельных программ.
- **Off box (на разных компьютерах)** Дополнительные функции реализованы на отдельных компьютерах, которые работают совместно с компьютером или устройством с брандмауэром.

Возможность организации виртуальных частных сетей и обнаружения вторжений интегрированы в большинство брандмауэров сетевого уровня. Кэширование, антивирусная программа и другие дополнительные возможности могут быть интегрированными в программное обеспечение брандмауэра (например, ISA Server), могут быть установлены в виде дополнительных программ на том же компьютере (например, Checkpoint) или могут реализовываться в виде отдельных компьютеров или устройств (например, Cisco PIX).

Брандмауэры сетевого уровня намного дороже персональных брандмауэров, что объясняется их большей сложностью и расширенной функциональностью. Брандмауэры сетевого уровня предназначены для работы с гораздо большими объемами трафика и поддерживают больше протоколов и одновременных соединений, чем персональный брандмауэр. В большинстве из них используются сложные инструменты управления: удаленное администрирование, централизованное администрирование нескольких брандмауэров и настраиваемый мониторинг, ведение отчетов и создание журналов. Брандмауэры сетевого уровня могут быть как сравнительно простыми «пограничными» брандмауэрами и работать в качестве единственного брандмауэра в сети, так и промышленными брандмауэрами, объединенными в иерархическую структуру для обеспечения многоуровневой защиты от пакетного уровня до уровня приложения или выравнивания нагрузки в группе брандмауэров на одном уровне сети.

Брандмауэры: свойства и функции

Для осуществления своей основной функции — защиты сети — современные брандмауэры используют многочисленные сложные методы.

- **Первая линия защиты** от **сетевых атак** Помимо блокирования пакетов, поступающих с определенных IP-адресов, из конкретных доменов или с конкретных адресов электронной почты, эффективный брандмауэр должен распознавать «подписи» или конкретные характеристики пакетов, содержащих наиболее распространенные типы сетевых атак, таких как DoS-атака или IP-спуфинг (фальсификация адреса источника в IP-пакете). Это функция системы обнаружения/предотвращения вторжений (IDS/IPS) брандмауэра.

- **Первая линия защиты от вирусов и спама** Эффективный брандмауэр дол жен распознавать вирусы, черви, троянские кони и другие вредоносные коды, пред назначенные для нанесения урона компьютерным программам или данным в вашей сети, пересылки данных третьим лицам без уведомления вас об этом или без ва шего согласия и/или использования системы вашей сети в качестве посредника (зомби) для инициирования атак на другие удаленные компьютеры.
- **Инструмент для судебного разбирательства «постфактум»** Основная роль брандмауэра — предотвращение вторжения в сеть атакующих, злонамеренных кодов или неавторизованных пользователей, но он также выполняет важную вто ричную роль в качестве инструмента судебного разбирательства после того, как была зафиксирована атака или попытка атаки. Современный брандмауэр осна щен системой ведения журнала и создания отчетов для обеспечения аудита системы безопасности.

ПРИМЕЧАНИЕ Хороший брандмауэр является эффективным средством нейтрализации многих типов брешей в системе безопасности, но ни один брандмауэр не может гарантировать стопроцентную безопасность вашей сети. Хакеры всегда имеют возможность создать бреши в системе безопасности сети, например с помощью социотехники, которая позволяет обойти защиту, обеспечиваемую брандмауэром. Поэтому важен настоящий многоуровневый подход к безопасности, в том числе обучение пользователей, разработка политик и правил для сотрудников компании и т. д.

Перечислим некоторые важные функции, входящие в современные брандмауэры:

- многоуровневая фильтрация;
- VPN-шлюзы;
- обнаружение и предотвращение вторжений;
- защита от вирусов;
- Web-кэширование;
- современные инструменты управления.

В последующих разделах мы обсудим каждую из них подробнее.

Многоуровневая фильтрация

Существует три основных типа брандмауэров, в зависимости от того, на каком уровне брандмауэр осуществляет фильтрацию. Ранние брандмауэры фильтровали только на одном уровне, обычно пакетном. Большинство современных брандмауэров использует многоуровневую фильтрацию, что обеспечивает большую безопасность. Многоуровневый брандмауэр выполняет два и более уровней фильтрации из приведенных далее:

- фильтрация пакетов;
- фильтрация уровня канала;
- фильтрация уровня приложения.

Эти три уровня фильтрации и их связь с сетевой моделью OSI (см. рис. 1.1) более подробно обсуждаются в следующих разделах.

ПРИМЕЧАНИЕ Модель OSI была разработана Международной организацией по стандартизации в качестве многоуровневой модели для использования производителями сетевого программного и аппаратного обеспечения для лучшей совместимости между их продуктами. Дополнительная информация: www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm.

Рис. 1.1. Три уровня фильтрации в сетевых моделях OSI

Фильтрация пакетов

Первыми брандмауэрами были брандмауэры с фильтрацией пакетов, работающие на сетевом уровне модели OSI. Они анализируют заголовки пакетов, содержащих IP-адреса и свойства пакета, и блокируют или пропускают трафик через брандмауэр на основе полученной информации. Брандмауэр с фильтрацией пакетов использует одну из трех технологий:

- *статическая фильтрация пакетов:* правила устанавливаются вручную, а конкретные порты остаются открытыми или закрытыми до тех пор, пока они не будут закрыты или открыты вручную;
- *динамическая фильтрация пакетов:* более интеллектуальная фильтрация, при которой правила изменяются динамически, основываясь на событиях или условиях; порты открываются, только когда это необходимо, а затем закрываются;
- *фильтрация с отслеживанием состояний соединений:* используется таблица для сохранения состояний соединения в сессиях и пакеты проходят в последовательности, определенной политиками фильтра.

ПРИМЕЧАНИЕ Проверка с *отслеживанием состояния соединения* (stateful inspection), или динамическая проверка, — это технология осуществления более глубокого анализа информации, содержащейся в пакетах (вплоть до уровня приложения); последующие решения принимаются на основании предшествующего анализа пакетов.

Фильтрация уровня канала

Брандмауэр с фильтрацией уровня канала, или шлюз канального уровня, работает на транспортном и сеансовом уровнях модели OSI. Он исследует информацию квитирования протокола TCP, пересылаемую между компьютерами, для определения легитимности сеансового запроса.

Фильтры уровня канала работают на более высоком уровне модели OSI — на транспортном уровне (уровень хост-хост модели DoD). Фильтры уровня канала ограничивают доступ на основе хост-машин (а не пользователей), обрабатывая информацию в заголовках пакетов TCP и UDP. Это позволяет администраторам создавать фильтры, например запрещающие любому, использующему компьютер A, получать доступ с помощью FTP на компьютер B.

При использовании фильтров уровня канала контроль доступа основан на потоках данных TCP или диаграммах UDP. Фильтры уровня канала могут работать на основании статусных флагов TCP и UDP и информации упорядочивания, кроме адресов источника и назначения и номеров портов. Фильтрация уровня канала позволяет администраторам анализировать сеансы, а не каналы. Сеанс рассматривается как аналог соединения, но в действительности сеанс может состоять более чем из одного соединения. Сеансы устанавливаются только в ответ на запрос пользователя, что обеспечивает дополнительную безопасность.

Фильтры уровня канала не ограничивают доступ, основываясь на информации о пользователе; они также не могут интерпретировать значение пакетов. То есть они не могут различить команды **GET** и **PUT,** посылаемые программным приложением. Для этого используется фильтрация уровня приложения.

Фильтрация уровня приложения

Фильтрация уровня приложения (Application-layer filtering, ALF) осуществляется прикладными шлюзами, которые также называются прикладными прокси. Брандмауэры с фильтрацией уровня приложения работают на уровне приложения модели OSI и могут анализировать содержимое данных, например адрес URL, содержащийся в HTTP-сообщении, или команду, содержащуюся в FTP-сообщении.

Иногда эффективнее бывает фильтрация пакетов, основанная на информации, содержащейся в самих данных. Фильтры пакетов и фильтры уровня канала не используют содержимое информационного потока при принятии решений о фильтрации, но это можно сделать с помощью фильтрации уровня приложения. Фильтр уровня приложения работает на верхнем уровне сетевой модели — уровне прило-

жения. Фильтры уровня приложения могут использовать информацию из заголовка пакета, а также содержимого данных и информации о пользователе.

Администраторы могут использовать фильтрацию уровня приложения для контроля доступа на основе идентичности пользователя и/или на основе конкретной задачи, которую пытается осуществить пользователь. В фильтрах уровня приложения можно установить правила на основе отдаваемых приложением команд. Например, администратор может запретить конкретному пользователю скачивать файлы на конкретный компьютер с помощью FTP или разрешить пользователю размещать файлы через FTP на том же самом компьютере. Это возможно, потому что в зависимости от того, получает ли пользователь файлы с сервера или размещает их там, используются различные команды.

Многие эксперты в области брандмауэров считают прикладные шлюзы наиболее безопасными среди всех технологий фильтрации, потому что используемые в них критерии охватывают больший диапазон, чем другие методы. Иногда хакеры пишут вредоносные программы, в которых используется адрес порта авторизованного приложения, например порта 53 (адрес службы DNS). Фильтр пакетов или фильтр уровня канала не смогут распознать, что это фальсифицированный DNS-запрос или ответ, и пропустят его. Фильтр уровня приложения способен проанализировать содержимое пакета и определить, что его не следует пропускать.

Но в этом типе фильтрации также есть свои недостатки. Самая большая проблема состоит в том, что для каждой службы Интернета должен быть определен отдельный прикладной шлюз, поддерживаемый брандмауэром, а это создает дополнительную работу по конфигурированию. Однако это слабое место одновременно является и преимуществом, поскольку оно увеличивает безопасность брандмауэра. Поскольку шлюз для каждой службы должен быть активирован, администратор не может случайно разрешить службы, представляющие угрозу для сети. Фильтрация уровня приложения является наиболее сложным уровнем фильтрации, осуществляемой брандмауэром, и особенно полезна при защите сети от особых типов атак, например злонамеренных SMTP-команд или попыток проникнуть на локальные DNS-серверы.

Еще одним недостатком фильтрации уровня приложения является низкая производительность. Фильтрация уровня приложения является медленной, потому что анализируются данные внутри пакетов. Следовательно, брандмауэр с фильтрацией уровня приложения не рекомендуется размещать по периметру сети, если есть быстрые входящие соединения, например OC-3. Напротив, там должны быть установлены простые и быстрые брандмауэры с фильтрацией пакетов, а фильтрация уровня приложения должна осуществляться далее, ближе к самому приложению.

VPN-шлюз

Большинство современных брандмауэров включают интегрированные VPN-шлюзы, позволяющие удаленным пользователям соединяться с VPN-сервером или со всей внутренней сетью через «туннель» виртуальной частной сети, который проходит

через общедоступный Интернет, либо обеспечивающие безопасное соединение через Интернет между двумя локальными сетями, расположенными в различных местах. Эти два типа VPN называют клиент-серверными VPN-подключениями и VPN-подключениями «узел-в-узел».

Клиент-серверное VPN-подключение

Клиент-серверное VPN-подключение используется, когда удаленные компьютеры (работающих дома или находящихся в командировке пользователей) подключаются к ЛВС компании, сначала установив соединение с Интернетом, а затем используя клиентское программное обеспечение VPN, туннельный протокол VPN (типа PPTP или L2TP), чтобы установить соединение с ЛВС компании, которая также подключена к Интернету. Поскольку данные, передаваемые по этому «туннелю», зашифрованы (с использованием таких протоколов, как MPPE или IPSec), то соединение также является конфиденциальным.

VPN-подключение «узел-в-узел»

VPN-подключение «узел-в-узел» используется для соединения между собой целых сетей. Как и в случае клиент-серверных VPN-подключений, обе стороны «виртуальной сети» должны быть подключены к Интернету. При этом используются те же самые туннелирование и протоколы шифрования. Различие между ними состоит в том, что при VPN-подключении «узел-в-узел» на обоих концах соединения имеется по шлюзу (в отличие от отдельного клиентского компьютера на одном конце соединения). Некоторые брандмауэры поддерживают только VPN-подключения «узел-в-узел».

Поддержка VPN в ISA Server

ISA Server 2004 поддерживает следующие VPN-протоколы:

- сквозной туннельный протокол (PPTP);
- **туннельный** протокол второго уровня/IPSec (L2TP/IPSec);
- туннельный режим IPSec.

Протоколы PPTP и L2TP/IPSec можно применять как для соединений удаленного доступа, так и для VPN-подключений «узел-в-узел».

Туннельный режим IPSec используется только для обеспечения совместимости с VPN-серверами сторонних разработчиков. Его не следует применять, если соединения «узел-в-узел» устанавливаются между брандмауэром ISA Server 2004 и другим продуктом VPN от Microsoft (Windows 2000/Windows Server 2003 RRAS или ISA Server 2000).

Функция VPN в ISA Server 2004 поддерживает оба типа VPN-подключений: клиент-серверное (также называемое VPN-подключением удаленного доступа) и «узел-в-узел».

VPN-подключение удаленного доступа позволяет отдельным компьютерам, настроенным как VPN-клиенты, выполнять соединение с брандмауэром ISA Server 2004

и получать доступ к ресурсам корпоративной сети. Клиенты VPN-подключения удаленного доступа могут использовать протоколы VPN PPTP или L2TP/IPSec. Расширенные механизмы проверки подлинности типа сертификатов SecurID, RADIUS, EAP/TLS, биометрических и других методов поддерживаются VPN-сервером удаленного доступа ISA Server 2004.

VPN-подключения «узел-в-узел» позволяют брандмауэру ISA Server 2004 устанавливать соединение с другим VPN-сервером и объединять друг с другом целые сети через Интернет. VPN-подключения «узел-в-узел» позволяют организациям отказаться от дорогих выделенных линий, что ведет к существенному сокращению расходов.

Основное конкурентное преимущество ISA Server 2004 состоит в том, что политики доступа брандмауэра применяются к VPN-подключениям удаленного доступа и «узел-в-узел». В отличие от брандмауэров сторонних разработчиков, разрешающих полный доступ клиентов VPN к корпоративной сети, VPN-соединения в ISA Server 2004 регулируются политиками доступа брандмауэра. Это позволяет администратору брандмауэра ISA Server 2004 устанавливать контроль ограничения доступа по VPN-соединениям для каждого пользователя. Когда пользователь устанавливает VPN-соединение с брандмауэром ISA Server 2004, он может получить доступ только к тем ресурсам, которые необходимы ему для выполнения его работы. Все остальные сетевые ресурсы будут ему не доступны.

Все операционные системы Windows включают в себя программное обеспечение для клиента VPN Windows. Перечислим некоторые преимущества использования клиента VPN Windows:

- отсутствие необходимости устанавливать программное обеспечение от сторонних разработчиков;
- отсутствие необходимости устранять неисправности совместимости между программным обеспечением клиента VPN от сторонних разработчиков и операционной системой Windows;
- упрощенная конфигурация и применение клиента VPN с помощью набора инструментов CMAK (Connection Manager Administration Kit);
- поддержка RFC (Requests for Comments, Запросы на комментарии) стандарта Интернета IPSec NAT Traversal, разработанного IETF (Internet Engineering Task Force, проблемная группа проектирования Интернета).

ISA Server 2004 также включает функции обеспечения безопасности VPN типа изолирования VPN-подключений, которое мы обсудим в главе 2.

Обнаружение и предупреждение вторжений

Многие брандмауэры (включая ISA Server) имеют систему обнаружения вторжений IDS, способную распознать попытку атаки определенного типа и выполнить заранее заданные действия.

Система обнаружения вторжений может распознавать множество различных распространенных форм сетевых вторжений, таких как сканирование портов, LAND-атаки (Local Area Network Directory, каталог локальной сети), Ping of Death, бомбы UDP, атаки типа out-of-band (OOB или WinNuke) и т. д. Также в брандмауэры могут быть встроены специализированные фильтры обнаружения вторжений, такие как фильтр обнаружения вторжений по протоколу POP, который анализирует почтовый трафик POP-протокола, чтобы избежать переполнений буфера POP, или фильтр обнаружения вторжений по DNS, который можно настроить на поиск атаки переполнения имени хоста DNS или атаки превышения длины.

ISA Server 2004 включает набор фильтров для обнаружения вторжения, которые имеют лицензию от IIS. Эти фильтры обнаружения вторжения сосредоточены на обнаружении и блокировании атак на сетевом уровне. Кроме того, ISA Server 2004 включает в себя фильтры обнаружения вторжения, которые обнаруживают и блокируют атаки уровня приложения.

ISA Server 2004 может обнаруживать следующие вторжения или атаки:

- Windows out-of-band (OOB или WinNuke);
- Land;
- Ping of Death;
- IP half scan;
- бомбы UDP;
- сканирование портов;
- переполнение имени хоста DNS (host name overflow);
- превышение длины DNS (length overflow);
- перемещение зоны DNS (zone transfer);
- переполнения буфера POP3;
- переполнения буфера SMTP.

При обнаружении брандмауэром ISA Server 2004 одной из этих атак предпринимаются следующие действия:

- в журнал событий ISA Server 2004 записывается предупреждение;
- службы ISA Server 2004 могут быть остановлены или перезапущены;
- может быть выполнена административная команда;
- на пейджер или ящик электронной почты администратора может быть отправлено сообщение.

К сожалению, система обнаружения вторжений, встроенная в ISA Server 2004, не является настраиваемой, и вы не сможете создать ваши собственные записи о вторжениях. Для расширения набора функций по обнаружению вторжений могут использоваться приложения от сторонних разработчиков, например системы IDS интернет-безопасности Real Secure.

Web-кэширование

ISA Server — это один из немногих популярных брандмауэров (другой — BlueCoat), сочетающий в себе брандмауэр и функцию Web-кэширования. Многие производители брандмауэров предлагают добавочный модуль (Checkpoint), отдельное аппаратное устройство (Cisco) или использование решений по кэшированию от сторонних разработчиков вместе с их брандмауэрами.

В большинстве организаций, имеющих доступ в Интернет, объем Web-трафика постоянно растет. Во многих случаях пользователи (или множество пользователей одной организации) постоянно посещают одни и те же Web-сайты и просматривают одни и те же страницы. В то же время общий объем сетевого и интернет-трафика неуклонно растет, иногда достигая почти предельных пропускных возможностей канала интернет-соединения.

Web-кэширование предоставляет способ уменьшения сетевого трафика как для Web-запросов, исходящих от ваших внутренних пользователей к Web-серверу, так и Web-запросов, поступающих от внешних пользователей на Web-серверы вашей внутренней сети.

Дальше мы обсудим следующие методики кэширования:

- прямое кэширование (forward caching);
- обратное кэширование (reverse caching);
- распределенное кэширование (distributed caching);
- иерархическое кэширование (hierarchical caching).

Прямое кэширование

Некоторые интернет-провайдеры назначают пользователям плату за использование каналов соединения на основе степени загрузки. Одним из способов снижения расходования пропускной способности интернет-соединения является хранение часто посещаемых Web-сайтов и страниц в локальной сети, где к ним могут получить доступ внутренние пользователи, не обращаясь на сервер в Интернете. Это прямое Web-кэш ирование, его дополнительное преимущество в том, что внутренние пользователи могут быстрее получить доступ к нужным ресурсам, потому что они обращаются к Web-объектам (страницам, графике, звуковым файлам и т. д.) по быстрому соединению по локальной сети, обычно на скорости 100 Мбит/с и выше, в отличие от более медленного интернет-соединения на скорости около 1,5 Мбит/с.

Обратное кэширование

Обратное кэширование уменьшает трафик по внутренней сети и повышает скорость доступа для внешних пользователей, если компания имеет свои собственные Web-сайты. В этом случае часто запрашиваемые объекты на внутренних Web-серверах кэшируются на периметре сети на прокси-сервере, чтобы уменьшить нагрузку на Web-серверы.

Распределенное кэширование

Несколько серверов Web-кэширования могут быть использованы вместе для обеспечения более эффективного кэширования. Как следует из названия, распределенное кэширование распределяет кэшированные Web-объекты на двух или нескольких серверах кэширования (рис. 1.2). Эти серверы находятся на одном уровне сети.

Рис. 1.2. Использование нескольких серверов на одном уровне сети при распределенном кэшировании

Иерархическое кэширование

Иерархическое кэширование является еще одним способом использования нескольких серверов Web-кэширования. Серверы кэширования размещаются на разных уровнях сети. Серверы кэширования восходящего потока взаимодействуют с прокси нисходящего потока. Например, сервер кэширования устанавливается в каждом филиале. Эти серверы взаимодействуют с кэширующим массивом в главном офисе (рис. 1.3).

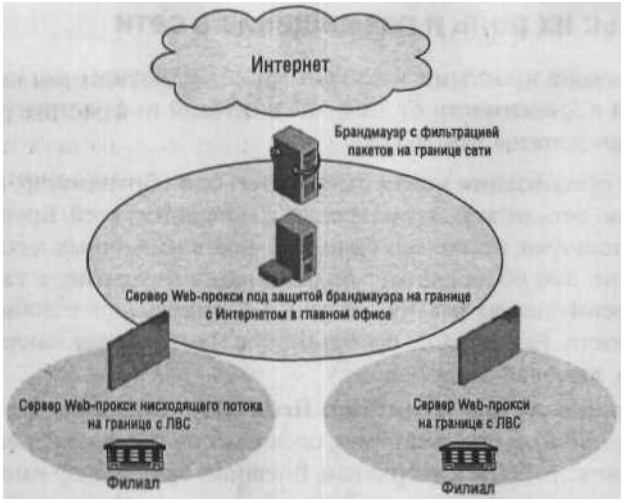


Рис. 1.3. Использование нескольких серверов Web-прокси на различных уровнях при иерархическом кэшировании

Иерархическое кэширование использует полосу пропускания эффективнее, чем распределенное кэширование. Однако при распределенном кэшировании к объему свободного дискового пространства предъявляются меньшие требования. Лучшими являются гибридные схемы кэширования (см. рис. 1.4), сочетающие в себе распределенное и иерархическое кэширование. Это повышает производительность и эффективность.

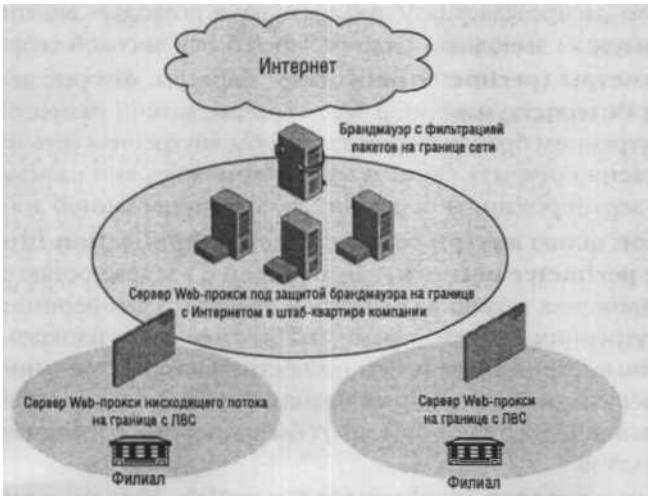


Рис. 1.4. Сочетание распределенного и иерархического методов кэширования при гибридном кэшировании

Брандмауэры: их роль и размещение в сети

Брандмауэры бывают простыми и сложными. Брандмауэры могут играть в сети несколько ролей в зависимости от того, где в сетевой инфраструктуре они размещаются и что они должны там делать.

В небольшой организации может быть только один брандмауэр, который защищает внутреннюю сеть от атак, приходящих из внешних сетей. Крупные организации обычно используют несколько брандмауэров в различных местах и с разными назначениями. Это обеспечивает более полное покрытие, а также позволяет использовать преимущества различных типов брандмауэров и добиваться лучшей производительности. Размещение брандмауэров в сети может накладывать на них различные роли, включая следующие:

- **Внешние брандмауэры (front-end firewalls)** Внешний брандмауэр также называется граничным брандмауэром, поскольку он помещается на границе внут ренней сети между ЛВС и Интернетом. Внешний брандмауэр имеет одно соеди нение с корпоративной сетью, а другое напрямую **с** Интернетом Все данные, поступающие в корпоративную сеть и исходящие из нее, должны быть прове рены брандмауэром и проанализированы его фильтрами, прежде чем они бу дут заблокированы или пропущены в сеть или из нее.
- **Внутренние брандмауэры (back-end firewalls)** Внутренний брандмауэр также размещается на границе внутренней сети, но не на границе с Интернетом, позади одного или нескольких брандмауэров. Обычно внешний брандмауэр(-ы) выполняет(-ют) фильтрацию пакетов, затем пропущенные пакеты должны прой ти через внутренний брандмауэр, осуществляющий фильтрацию на уровне при ложения. Это распределяет рабочую нагрузку и позволяет внешним и внутрен ним брандмауэрам выполнять свою работу с более высокой скоростью.
- **Сети-периметры (perimeter networks)** Серверы, которые должны быть до ступны для Интернета, например Web-серверы, можно разместить между вне шним и внутренним брандмауэром так, чтобы внутренняя сеть не была для них непосредственно открыта. Область между брандмауэрами называется сетью-пе риметром, экранированной сетью или демилитаризованной зоной (DMZ).
- **Прикладной шлюз внутри сети-периметра (application-filtering gateway within the perimeter network)** Брандмауэр с возможностью фильтрации на уровне приложения можно разместить в пределах сети-периметра между вне шним и внутренним брандмауэрами, чтобы уменьшить площадь атаки и обес печить очень высокий уровень безопасности. Поскольку он снимает груз филь трации содержимого с граничных брандмауэров, их производительность воз растает. Граничные брандмауэры могут быть простыми брандмауэрами с филь трацией пакетов.
- **Брандмауэры отделов (department firewalls)** Брандмауэры могут приме няться в пределах внутренней сети для защиты отдельных подсетей. Это обес-

печивает защиту конкретных отделов или других подразделений сети не только от атак из Интернета, но и из других отделов или подразделений. В данном случае брандмауэр размещается между подсетью отдела и остальной частью внутренней сети.

- **Брандмауэры филиалов (branch office firewalls)** Филиалы, подключенные к более крупной внутренней сети, например через VPN-подключения «узел-в-узел», должны быть защищены брандмауэром на границе их собственного со единения с Интернетом.
- **Дистанционные брандмауэры (telecommuter firewalls)** Удаленные пользо ватели, например надомные работники или сотрудники в командировке, кото рые соединяются с корпоративной сетью через VPN-подключение удаленного доступа, должны иметь защиту на своих компьютерах. Эту защиту можно обес печить с помощью персонального брандмауэра или простых недорогих уст ройств-брандмауэров, разработанных для этой цели.
- **Брандмауэры от различных производителей (multiple firewall configu ration)** могут работать совместно в конфигурациях с несколькими брандмау эрами. Для обеспечения эффективной защиты брандмауэры должны быть соз даны так, чтобы взаимодействовать друг с другом, с сетевой операционной си стемой и прикладными серверами, используемыми в сети.

Размещение брандмауэров и их роли более подробно рассматриваются в главе 4.

ISA Server: от прокси-сервера до полнофункционального брандмауэра

ISA Server претерпел длительное развитие, становясь все функциональнее и наконец превратившись в универсальное решение в области безопасности. Происхождение ISA Server связано с MS Proxy Server. Менее чем за десятилетие этот продукт превратился в нечто совершенно другое.

Предвестник ISA: MS Proxy Server

Прокси-серверы известны уже довольно давно. ISA Server является прокси-сервером, но он также представляет из себя нечто гораздо большее. Термин «прокси» первоначально означал «того, кто получил право действовать в интересах другого». Это слово используется в английском языке в выражении «брак по доверенности» (marriage by proxy), означающем, что подставное лицо выступает в роли одной из сторон, таким образом брачная церемония может состояться даже в отсутствие жениха (реже, невесты).

Прокси-серверы названы так потому, что они, подобно тому злополучному подставному лицу, которое говорит: «Согласен», когда на самом деле согласен кто-то другой, выступают в роли посредника и разрешают произойти какому-либо собы-

тию между двумя системами, которые должны оставаться отдельными (в данном случае сетевому соединению).

Прокси-серверы «вклиниваются» между компьютерами в ЛВС и компьютерами внешней сети. Еще одним хорошим примером будет привратник, который сгоит у входа в поместье и проверяет всех входящих, чтобы убедиться, что они есть в списке приглашенных. Прокси может спрятать компьютеры в ЛВС от посторонних. Другим в Интернете виден только IP-адрес прокси-сервера; внутренние компьютеры используют свои собственные IP-адреса (не передаваемые по Интернету), которые не видны с другой стороны прокси.

На самом деле прокси также может выступать в роли тюремщика, который не только следит за тем, чтобы входили лишь те, у кого есть на это право, но и за тем, чтобы выйти могли только те, у кого есть разрешение. Так же как и охранник сверяется со своим списком, прежде чем впустить или выпустить кого-либо, прокси *фильтрует* исходящие и входящие данные в соответствии с заранее заданными критериями. В таком случае прокси ведет себя как брандмауэр.

Начало: MS Proxy Server

Корпорация Microsoft в ноябре 1996 г. выпустила свою первую версию прокси-сервера, включающую несколько уникальных функций, например Winsock прокси, которая позволяла использовать приложения, не поддерживавшиеся традиционными прокси-серверами.

Но, к сожалению, в версии 1.0 был ряд существенных ограничений, в том числе отсутствие резервирования, которые помешали ей стать популярной в области кэширования и безопасности для крупных промышленных сетей. В то время как конкурирующие продукты, например прокси-сервер от Netscape, использовали распределенное кэширование на нескольких серверах для обеспечения отказоустойчивости, в первой версии прокси от Microsoft не было такой функции. Казалось, что прокси от Microsoft был лучше приспособлен для небольших сетей и для тех сетей, ь которых кэширование и функции безопасности являлись менее критичными.

Вопросу резервирования было уделено внимание во второй версии Proxy Server, Microsoft даже превзошла достижения Netscape, введя понятие *массивов* прокси-сервера. Массив — это группа из двух и более прокси-серверов, работающих как зеркальные отображения друг друга и функционирующих как единое целое под общим именем. Во второй версии появилась возможность объединять несколько прокси вместе для лучшего выравнивания нагрузки; корпорация Microsoft разработала новый протокол — CARP (Cache Array Routing Protocol, протокол маршрутизации между кэш-серверами) для обмена данными между прокси-серверами.

ПРИМЕЧАНИЕ CARP является патентованным (принадлежащим только Microsoft) протоколом. Он используется для управления многочисленными Web-запросами пользователей в массиве прокси-серверов. Протокол ЮР (Internet

Cache Protocol, протокол интернет-кэширования) — это сходный протокол, используемый производителями других решений в области прокси, например Border Manager от Novell. Хотя по функциональности CARP и ICP похожи, они используют разные алгоритмы хэширования. Протокол CARP имеет некоторые преимущества по сравнению с ЮР, особенно с точки зрения производительности, поскольку протокол CARP не обменивается сообщениями-запросами между серверами, как ICP. Кроме того, с помощью протокола CARP удается избежать ненужного резервирования содержания на серверах в массиве. Для применения протокола CARP с целью выравнивания нагрузки требуется установка промышленной версии ISA Server 2004.

Для того, чтобы внести изменения в настройки на все серверы массива, была добавлена автоматическая синхронизация. Были расширены возможности кэширования — теперь они включали в себя кэширование по протоколу FTP и HTTP. Все эти службы было легко настроить.

Также новой в версии 2 была функция *обратного прокси,* которая позволяла публиковать Web-содержимое с защищенных Web-серверов. На одном прокси-сервере можно было опубликовать множество Web-сайтов с помощью поддержки нескольких интерфейсов. Кроме того, во второй версии был добавлен обратный хостинг (reverse hosting) (при котором прокси сервер слушает и отвечает на входящие Web-запросы за многочисленные серверы, стоящие позади него), а также возможность публиковать другие службы через *связывание серверов* (server binding).

Proxy Server от корпорации Microsoft получил высокие оценки за легкость установки и настройки по сравнению с конкурирующими продуктами. Во вторую версию был также добавлен интегрированный административный модуль для IIS 4.0 под названием консоль управления Microsoft (Microsoft Management Console, MMC), которая предоставляла администраторам удобный и мощный способ управления отдельным или несколькими прокси-серверами.

Первый настоящий брандмауэр корпорации Microsoft: ISA Server 2000

Третья реализация Microsoft Proxy Server получила совершенно новое название, потому что она включала в себя ряд усовершенствований, которые превосходили определение прокси-сервера. ISA Server 2000 был впервые выпущен в начале нового тысячелетия и был полнофункциональным брандмауэром с возможностью кэширования и дальнейшего улучшения.

ПРИМЕЧАНИЕ Что является брандмауэром, а что нет — это вопрос соглашения среди специалистов по сетевой безопасности. Все согласны с тем, что брандмауэры — это программы (или группы программ), которые расположены у входа в сеть, и с тем, что они защищают ресурсы этой внутренней сети от вторжений извне. Национальный институт стандартов и технологии (National Institute of Standards and Technology, NIST) в документе SP-800-10 определя-

ет брандмауэр как *подход* к безопасности, помогающий реализовать более масштабную политику безопасности путем создания защиты по периметру, через которую должен проходить весь входящий и исходящий трафик, тем самым контролируя доступ в/из защищенной сети или узла.

Некоторые производители используют более широкое определение брандмауэра, которое включает прокси-серверы. С учетом этого корпорация Microsoft позиционировала Proxy Server 2.0 как брандмауэр, хотя некоторые эксперты в области безопасности оспаривали это и утверждали, что для того, чтобы удовлетворять стандарту брандмауэра, продукт должен быть не просто маршрутизатором, хост-бастионом или другим устройством обеспечения безопасности. Этим утверждается требование, состоящее в том, что для того, чтобы считаться брандмауэром, продукт должен быть основан на политиках.

Помимо многоуровневых функций брандмауэра (фильтрация пакетов, фильтрация уровня канала и фильтрация уровня приложения), в ISA Server 2000 имеются и такие новые или улучшенные функции:

- **Встроенная поддержка виртуальных частных сетей (VPN)** ISA Server может использоваться либо для установления удаленного VPN-подключения между клиентом и шлюзом, либо для создания VPN-туннеля от сервера к серверу.
- **Встроенная поддержка Active Directory (AD)** Политики доступа и инфор мация о конфигурации сервера ISA интегрированы в Windows 2000 Active: Direc tory для более простого и безопасного администрирования.
- **Обнаружение вторжений** может быть настроено так, что буд>т отсылаться предупреждения, если/когда на вашу сеть совершается попытка определенного типа атаки, например кто-то извне пытается просканировать ваши порты.
- **Поддержка SecureNAT (Secure Network Address Translation, безопасное преобразование сетевых адресов)** Наращиваемая архитектура NAT, реали зованная в ISA, обеспечивает безопасное соединение для клиентов, у которых не установлено клиентское программное обеспечение для брандмауэра, вклю чая клиенты Macintosh и UNIX и других операционных систем сторонних раз работчиков, которые работают с протоколом TCP/IP.
- **Распределение полосы пропускания,** выделяемой конкретному пользова телю, соединению, клиенту или пункту назначения, может происходить под кон тролем правил качества обслуживания, которые создает администратор для оп тимизации сетевого трафика.
- **Безопасная публикация серверов** Внутренние серверы могут стать доступ ными для конкретных клиентов, в то время как эти серверы защищены от неавторизованного доступа.

- **Управление на уровне предприятия** ISA, как и Windows 2000, рассчитан на большую масштабируемость и ориентирован на рынок для предприятий боль ше, чем предыдущие продукты от Microsoft. ISA дает вам возможность назначить политики уровня предприятия, а также политики уровня массива, а управление массивами ISA легко сделать централизованным.
- **Мониторинг и создание отчетов** Программа ISA Server позволяет вам вес ти мониторинг ее производительности и создавать подробные журналы безо пасности и доступа, а также графические отчеты. Создание отчетов может производиться по расписанию, а удаленное управление позволяет администра торам контролировать использование и производительность сервера ISA с уда ленного места.
- **Сканирование содержимого e-mail сообщений** ISA Server позволяет скани ровать содержимое e-mail сообщений по ключевым словам, что дает возможность администраторам обеспечивать выполнение строгих политик безопасности.
- **Служба поддержки протокола H.323** позволяет использовать программное обеспечение для проведения видеоконференций, например Microsoft NetMeeting, через прокси и функции директории NetMeeting (которые заменяют некоторые функции ILS).
- **Усовершенствованное программное обеспечение** может использоваться для потоковых мультимедиа, включая разбиение потока в режиме реального вре мени (live stream splitting) и кэширование содержимого Windows Media (при ис пользовании Windows Media Server).

Обновленный и улучшенный: ISA Server 2004

Со своего появления ISA Server 2000 медленно, но верно повышал свою долю на рынке по сравнению с конкурентами. По сообщению IDC (Internet Data Center, центр обработки данных), рост продаж корпорации Microsoft и ее доли на рынке брандмауэров был одним из наиболее быстрых в 2002/2003 гг. Однако многие пользователи ISA составляли «списки пожеланий» с указанием функций и улучшений, которые они хотели бы видеть в следующей версии. В ответ команда разработки ISA корпорации Microsoft приложила значительные усилия для того, чтобы создать более удобный и интуитивно понятный графический интерфейс, обеспечив лучшую поддержку основных функций типа VPN, более гибкие и полные политики, поддержку нескольких сетей и простоту настройки.

В ISA Server 2004 было добавлено много новых функций, а другие функции были улучшены; был полностью **исправлен** интерфейс, что сильно повысило функциональность, особенно на уровне предприятия. В табл. 1.2 показаны некоторые функции, которые были добавлены в ISA 2004. Более подробно мы обсудим их в главе *2*.

Табл. 1.2. Новые функции ISA Server 2004

Новая функция	Ее возможности
Поддержка нескольких сетей	Позволяет вам настроить более одной сети, каждая из которых имеет определенные отношения с остальными сетями. Вы можете определить политики доступа для сетей. В отличие от ISA Server 2000, когда весь сетевой трафик проверялся в соответствии с таблицей локальных адресов (local address table, LAT), вклю чающей адреса только локальной сети, в ISA Server 2004 вы можете применять функции брандмауэра по обеспечению безопасности к трафику между любыми сетями или объектами сети
Сетевые политики	Новые **функции** поддержки нескольких сетей в ISA Server 2004 позволяют вам защитить вашу сеть от внутренних и внешних угроз безопасности путем ограничения соединений между клиентами даже в пределах вашей организации. Работа с несколькими сетями обеспечивает поддержку сложной сети-пер и метра (также называемой демилитаризованной зоной, DMZ, или экранированной подсетью), что позволяет вам настроить способ получения клиентами в различных сетях доступа к сети-пер и метру. Политика доступа между сетями затем может основываться на уникальной зоне безопасности, представленной каждой сетью Вы можете использовать ISA Server 2004 для определения маршрутизации между сетями, основываясь на типе доступа и соединения, необходимых между сетями. В некоторых случаях, если вам нужно более надежное и менее прозрачное соединение между сетями, вы можете определить отношения преобразования сетевых адресов (network address translation, NAT). В других случаях, если вы хотите просто направить трафик через ISA Server, вы можете определить отношение маршрутизации. В отличие от ISA Server 2000, в ISA Server 2004 все пакеты, проходящие между соединенными сетями, анализируются механизмами фильтрации и проверки с отслеживанием соединений
Маршрутизация и преобразование сетевых адресов	
Фильтрация с отслеживанием состояния соединения и проверка для VPN	Клиенты виртуальной частной сети (virtual private network, VPN) настраиваются как отдельная сетевая зона. Поэтому вы можете задать политики специально для клиентов VPN. Набор правил брандмауэра выборочно проверяет запросы от клиентов VPN, осуществляя фильтрацию с отслеживанием соединений и проверку этих запросов и динамически открывая соединения, основываясь на политике доступа

Табл. 1.2. (продолжение)

Новая функция	Ее возможности
Фильтрация с отслеживанием состояния соединения и проверка трафики, проходящего по туннелю VPN «узел-в-узел»	Сети, объединенные каналом «узел-в-узел>> в ISA Server 2000, считались надежными сетями, и к трафику, передававшемуся по каналу, не применялась политика брандмауэра. В ISA Server 2004 добавлена возможность фильтрации с отслеживанием состояния соединения и проверки всего трафика, проходящего по VPN-подключению «узел-в-узел». Это позволяет вам контролировать ресурсы, к которым могут получить доступ конкретные хосты или сети на противоположном конце канала. Пользовательские/групповые политики доступа применяются для получения тщательного контроля за использованием ресурсов по каналу связи
Поддержка безопасного клиента NAT для клиентов VPN, подключенных к VPN-серверу ISA Server 2004	В ISA Server 2000 только клиенты VPN, настроенные как клиенты брандмауэра, могли получить доступ к Интернету через свой VPN-сервер ISA Server 2000. В ISA Server 2004 расширена поддержка клиента VPN — теперь клиенты SecureNAT могут получить доступ в Интернет без установки программного обеспечения клиента брандмауэра на своем клиентском компьютере. Вы также можете усилить безопасность корпоративной сети, если введете клиентскую/групповую политику брандмауэра для клиентов VPN SecureNAT В ISA Server 2004
Изолирование VPN-no дключений	усилена функция изолирования VPN-подключений Windows Server 2003. Изолирование VPN-подключений позволяет вам изолировать клиенты VPN в отдельной сети до тех пор, пока они не выполнят заранее определенный набор требований к безопасности. Клиентам VPN, которые не проходят тестирование на безопасность, может быть предоставлен ограниченный доступ к серверам, который поможет им выполнить требования к безопасности в сети
Способность публиковать PPTP VPN серверы	С помощью ISA Server 2000 вы могли публиковать только L2TP/IPSec NAT-T VPN серверы. Правила публикации серверов ISA Server 2004 позволяют вам публиковать IP протоколы и PPTP серверы. PPTP фильтр уровня приложений в ISA Server 2004 осуществляет комплексный контроль соединения. Кроме того, вы можете легко опубликовать VPN сервер Windows Server 2003 NAT-T L2TP/IPSec с использованием публикации серверов в ISA Server 2004
Поддержка туннельного режима IPSec для VPN-подключений «узел-в-узел»	В ISA Server 2000 использовались протоколы PPTP и L2TP/IPSec VPN для соединения сетей через Интернет с применением VPN-подключения «узел-в-узел». В ISA Server 2004 улучшена поддержка соединения «узел-в-узел», теперь вы можете использовать туннельный режим IPSec в качестве VPN протокола
Расширенная поддержка протоколов	В ISA Server 2004 расширена функциональность ISA Server 2000. Теперь у вас есть возможность контролировать доступ и использование любого протокола, включая протоколы уровня IP. Это позволяет пользователям применять приложения типа ping и tracert и устанавливать VPN-подключения PPTP. Кроме того, через ISA Server может проходить трафик протокола IPSec

(см. след. стр.)

Табл. 1.2. (продолжение)

Новая функция	Ее возможности
Поддержка сложных протоколов с установкой нескольких начальных соединений	Для многих потоковых мультимедиа и аудио/видео приложений необходимо, чтобы брандмауэр мог работать со сложными протоколами. В ISA Server 2000 поддерживалось управление сложными протоколами, но администратор брандмауэра должен был создавать сложные скрипты для создания определений протоколов, для которых нужны многочисленные начальные исходящие соединения. ISA Server 2004 позволяет вам создавать определения протоколов с помощью простого в применении мастера новых протоколов New Protocol Wizard
Настраиваемые определения протоколов	ISA Server 2004 позволяет вам контролировать номера портов источника и назначения для любого протокола, для которого вы зададите правило брандмауэра (Firewall Rule). Это дает возможность администратору брандмауэра ISA Server 2004 осуществлять строгий контроль того, каким пакетам разрешено входить и выходить через брандмауэр
Пользовательские группы брандмауэра	Для контроля пользовательского и группового доступа в ISA Server 2000 применялись пользователи и группы, созданные в Active Directory или на локальном компьютере с брандмауэром. В ISA Server 2004 также используются эти источники, но у вас еще есть возможность создавать произвольные группы, которые состоят из групп, уже имеющихся в лок;шьной базе учетных записей или в домене Active Directory. Это увеличивает вашу свободу контроля доступа, основанную на членстве пользователей или групп, потому что администратор может создавать произвольные группы из уже существующих. Это отменяет требование, состоящее в том, что администратор брандмауэра также должен быть администратором домена для того, чтобы давать разрешение группам безопасности на осуществление контроля входящего или исходящего доступа
Передача верительных данных (credential) клиента брандмауэра службе Web прокси	Редиректор HTTP должен был передавать запросы службе Web прокси для того, чтобы клиенты брандмауэра могли извлечь пользу из Web-кэша в ISA Server 2000. В ходе этого процесса верительные данные пользователя (мандаты) удалялись, а запрос не выполнялся, если требовались мандаты пользователя. В ISA Server 2004 эта проблема была решена: теперь клиенты брандмауэра могут получить доступ к Web-кэшу через фильтр HTTP
Поддержка службы RADIUS при проведении проверки подлинности клиентов Web-прокси	Для того чтобы выполнить проверку подлинности клиентов Web-прокси в ISA Server 2000, компьютер должен был быть членом домена Active Directory или учетная запись пользова теля должна была содержаться в локальной базе данных пользователей на брандмауэре компьютера. ISA Server 2004 позволяет вам выполнять проверку подлинности пользователей в Active Directory и в других аутентификационных базах данных, используя службу RADIUS для отправки запросов к Active Directory. Правила Web-публикаций также могут использовать службу RADIUS для проверки подлинности удаленных соединений

Табл. 1.2. (продолжение)

Новая функция	Ее возможности
Делегирование базовой проверки подлинности	Опубликованные Web-сайты защищены от неавторизованного доступа, потому что они требуют от брандмауэра ISA Server 2004 проверки подлинности пользователя, прежде чем соединение будет перенаправлено на опубликованный Web-сайт. Это предотвращает проникновение неавторизованных пользователей на опубликованный Web-сервер
Сохранение IP-адреса источника в правилах Web-публикаций	Правила Web-публикаций в ISA Server 2000 заменяли IP-адрес источника удаленного клиента на IP-адрес из внутреннего интерфейса брандмауэра, прежде чем передавать запрос на опубликованный Web-сервер. В ISA Server 2004 эта проблема была устранена: теперь вы можете на основе правил выбирать, должен ли брандмауэр заменять исходный IP-адрес своим собственным или передавать исходный IP-адрес удаленного клиента на Web-сервер
Проверка подлинности БесгигШ для клиентов Web-прокси	В ISA Server 2004 проверка подлинности удаленных соединений производится с помощью двухфакторной проверки подлинности SecrurlD. Это обеспечивает очень высокий уровень безопасности проверки подлинности, потому что пользователь должен «знать что-то» и «иметь что-то», для того чтобы получить доступ к опубликованному Web-серверу
Проверка подлинности на основе форм	ISA Server 2004 может генерировать формы, используемые OWA-сайтами, для проверки подлинности ш основе форм. Это повышает безопасность удаленного доступа к OWA-сайтам, не разрешая неавтори зова нным пользователям устанавливать соединение с OWA-сервером
Удаленный доступ к службам терминалов с использованием VPN-подключения по протоколу SSL	Компьютеры, работающие под Windows Server 2003 Service Pack 1, поддерживают передачу данных протокола RDP по SSL для обеспечения безопасного SSL VPN-подключения к службам терминалов Windows Server 2003. ISA Server 2004 позволяет вам безопасно публиковать свой сервер терминала, применяя технологию безопасного SSL VPN-подключения Новый
Мастер безопасных Web-публикаций (Secure Web Publishing Wizard)	мастер безопасных Web-публикаций позволяет вам устанавливать безопасные SSL VPN туннели к Web-сайтам вашей внутренней сети. Функция моста SSL-SSL позволяет ISA Server 2004 расшифровывать зашифрованный трафик и проводить трафик через механизм проверки с отслеживанием соединений в рамках HTTP-политики. Опция SSL-туннелирования ретранслирует не модифицированный зашифрованный трафик на опубликованный Web-сервер
Принудительное шифрование для безопасных соединений Exchange RPC	На брандмауэре ISA Server 2004 можно установить политику RPC, которая предотвратит передачу незашифрованных сообщений от удаленных клиентов Outlook MAPI, выполняющих соединение через Интернет. Это укрепляет сеть и безопасность сервера Exchange, поскольку так запрещается обмен мандатами пользователя и данными в незашифрованном **формате**

(см. след. стр.)

Табл. 1.2. (продолжение)

Новая функция	Ее возможности
Фильтрация данных протокола HTTP на основе правил	HTTP-политика в ISA Server 2004 позволяет брандмауэру осуществлять глубинную проверку данных протокола HTTP с отслеживанием соединений (фильтрация уровня приложения). Степень проверки определяется правилами. Это позволяет вам по своему усмотрению настроить ограничения для входящего и исходящего HTTP-доступа
Возможность блокировать доступ ко всему исполняемому содержимому	Вы можете настроить HTTP-политику в ISA Server 2004 так, чтобы блокировались все попытки установления подключений к исполняемому содержимому Windows вне зависимости от расширения файла, который используется в ресурсе
Возможность контролировать загрузки HTTP-файлов по расширению файла	HTTP-политика в ISA Server 2004 позволяет вам разрешить все расширения файлов; все расширения, кроме конкретной группы расширений; или блокировать все расширения, кроме конкретной группы расширений
Применение HTTP-фильтрации ко всем клиентским соединениям в ISA Server 2004	В ISA Server 2000 была возможность блокировать содержимое клиентских HTTP- и FTP-соединений на Web-прокси по типу MIME (Multipurpose Internet Mail Extensions, многоцелевые расширения электронной почты в Интернете) (для протокола HTTP) или по расширению файла (для протокола FTP). HTTP-политика в ISA Server 2004 позволяет вам контролирова-ь HTTP-доступ для всех клиентских соединений ISA Server 2004
Возможность блокировать содержимое HTTP-соединений на основании ключевых слов или строк (подписей)	Глубинная проверка HTTP-соединений в ISA Server 2004 позволяет вам создавать "HTTP-подписи», которые сравниваются с URL запроса, заголовками запроса, телом запроса, заголовками ответа и телом ответа. Это дает вам точный контроль над тем, к какому содержимому могут получить доступ внутренние и внешние пользователи через брандмауэр ISA Server 2004
Возможность контролировать, какие из HTTP-методов разрешены	Вы можете контролировать, какие HTTP-методы (также известные как «HTTP-команды») разрешены на брандмауэре, путем установки контроля доступа на доступ пользователей к различным методам. Например, вы можете ограничить HTTP-метод POST, который запретит пользователям отправлять данные на Web-сайты с помощью HTTP-метода POST
Возможность блокировать незашифрованные Exchange RPC-соединения от полных клиентов Outlook MAPI	Правила безопасной публикации сервера Exchange в ISA Server 2004 позволяют удаленным пользователям устанавливать соединение с сервером Exchange с помощью полнофункционального клиента Outlook MAPI через Интернет. Однако клиент Outlook должен быть настроен на использование безопасного RPC для шифрования соединения. RPC-политика в ISA Server 2004 позволяет вам блокировать все нешифрованные соединения клиента Outlook MAPI
FTP-политика	FTP-политику в ISA Server 2004 можно настроить так, чтобы разрешить пользователям загружать и размещать информацию по протоколу FTP или же ограничить FTP-доступ пользователя только загрузкой

Табл 1.2. (продолжение)
.

Нова функция	Ее возможности
Преобразование ссылок	Некоторые опубликованные Web-сайты могут включать ссылки на внутренние адреса компьютеров. Поскольку для внешних клиентов доступны только брандмауэр ISA Server 2004 и внешнее пространство имен, а не внутреннее пространство сетевых имен, то эти ссылки могут оказаться испорченными. ISA Server 2004 включает в себя функцию преобразования ссылок, которая позволяет вам создавать словарь определений для внутренних имен компьютеров, которые преобразовываются в общеизвестные имена
Мониторинг записей из журнала в режиме реального времени	ISA Server 2004 позволяет вам просматривать журналы брандмауэра, Web-прокси и средства контроля SMTP-сообщений в режиме реального времени. Консоль управления отображает записи журнала по мере их внесения в системный журнал брандмауэра
Встроенная функция запросов журналов	Вы можете запрашивать системные журналы, используя встроенную функцию запросов журнала. Журналы можно запрашивать на предмет информации, содержащейся в любом поле, записанном в журналах. Вы можете ограничить область действия запроса определенными временными рамками. Результаты появятся на консоли ISA Server 2004, их можно будет скопировать в буфер обмена и вставить в другое приложение для более детального анализа
Верификаторы соединений	Вы можете проверить возможность соединения, производя постоянный мониторинг соединений к конкретному компьютеру или URL с компьютера с ISA Server 2004 с помощью верификаторов соединений. Вы можете указать, какой метод будет использоваться для определения возможности соединения: ping, TCP-соединение с портом или HTTP-метод GET. Вы можете выбрать соединение, которое вы будете отслеживать, указав IP-адрес, имя компьютера или URL
Публикация *отчетов*	Задачи ISA Server 2004 по созданию отчетов можно настроить так, чтобы копия отчета автоматически сохранялась в локальной папке или в совместно используемом сетевом файле. Совместно используемой папке или файлу, в котором сохраняется отчет, может быть установлено соответствие в виртуальном каталоге Web-сайта так, чтобы другие пользователи могли просмотреть этот отчет. Вы также можете вручную опубликовать отчеты, для которых не была настроена автоматическая публикация после создания отчета
Уведомление по электронной почте о создании отчета	Вы можете настроить функцию создания отчетов на то, чтобы вам было отправлено сообщение по электронной почте после того, как создание отчета было завершено В ISA Server 2000 было жестко задано время создания резюме отчетов — 12:30. Отчеты основываются на информации, содержащейся в резюме журналов. ISA Server 2004 позволяет вам просто настроить время создания резюме журналов. Это дает вам возможность задавать время создания дневных отчетов
Возможности по настройке времени для создания резюме журнала	

(см. след. стр.)

Табл. 1.2. (окончание)

Новая функция	Ее возможности
Возможность записывать информацию в базу данных MSDE (Microsoft Data Engine, двигатель данных Microsoft)	Журналы теперь могут сохраняться в формате MSDE. Ведение журнала в локальной базе данных увеличивает скорость обработки и гибкость запросов
Возможность импортировать и экспортировать конфигурационные данные	Вы можете использовать эту функцию для того, чтобы сохранить параметры конфигурации в файл XML, а затем импортировать эту информацию из файла на другой сервер
Мастер передачи полномочий (Delegated Permissions Wizard) для ролей администратора брандмауэра	Мастер передачи полномочий помогает вам назначить административные роли пользователям и группам пользователей. Эти заранее определенные роли передают уровень административного контроля, который разрешен пользователям В конкретных службах ISA Server 2004

Помимо этих новых функций, есть множество улучшений функций, которые входили в ISA Server 2000. В главе 2 мы также рассмотрим их более подробно.

ПРИМЕЧАНИЕ Некоторые из функций, перечисленных в табл. 1.2, можно было добавить в ISA Server 2000 с помощью установки Feature Pack 1, но они не входили в основную комплектацию, как в ISA Server 2004.

ISA: личное представление

Пока мы работали с данным программным продуктом, начиная с азов, мы многое прочитали о том, что вскоре выйдет ISA Server 2004. Многое из прочитанного было полезной информацией, а некоторые сообщения поддерживали заблуждения, о которых мы уже говорили:

- «Это хорошая улучшенная модернизированная версия, но не скажу, что она сколь-нибудь важна. Она не поможет им конкурировать с Checkpoint» (www.infoworld.com/a rticle/04/05/03/HNisase rver_l.html).
- «Некоторые настаивают на том, что ISA Server — это брандмауэр, но на самом деле это сервер. Гартнер (Gartner) абсолютно уверен в том, что брандмауэры являются шлюзами для обработки пакетов и устройствами обработки потока данных, а не серверами. С точки зрения рынка, большинство наиболее совре менных инсталляций являются устройствами» (www.infoworld.com/article /04/O5/O3/HNisaserver_l.html).
- «Я работал на крупных предприятиях: мы использовали брандмауэр Cisco в ка честве внешнего, а позади него ставили ISA Server, — сказал Крис Дэрроу (Chris Darrow), консультант TCP-IP Inc. — консалтинговой компании с главным офи сом в Сакраменто, Калифорния. — Этот брандмауэр является хорошим допол нением к брандмауэрам Checkpoint или Cisco, но один этот брандмауэр я бы не

стал использовать» (http://searchwin2000.techta rget.com/originalContent/0,289142, sidI_gci967964,00.html).

- «Франко в рамках темы "Strange Setup" ("Странная установка") спрашивал, поче му сервер ISA корпорации Microsoft имеет два интерфейса, что позволяет ему обойти брандмауэр. В последующих публикациях разъяснялось, что для ISA Server требуется именно такая установка и что эта программа является хорошим HTTP-прокси, кэшем и средством проверки подлинности для сети Windows. (Читай: лучше, чем брандмауэр.) А весь остальной трафик должен все равно проходить через брандмауэр»(http://sandbo$_x$.rulemaker.net/ngps/infosec/rwiz/fwiz-2004-02 -28).

Наиболее часто в таких комментариях и дискуссиях встречается следующее:

- Вера в миф об аппаратном брандмауэре. Мы развеяли этот миф в информаци онном бюллетене, который был опубликован на сайте ISAServer.org в марте 2004 года (www.isaserver.org/pages/newsletters/march2004.asp).
- Представление о том, что решения Cisco и Checkpoint (и другие традиционные брандмауэры) являются в сущности более безопасными при отсутствии пони мания брандмауэра ISA Server 2004 и ясной позиции относительно того, что именно вызвало появление их убеждения, что прочие брандмауэры предостав ляют лучшую степень защиты.
- Предположение, что программное обеспечение, работающее на базе операци онной системы Windows от Microsoft, не достойно доверия (вероятно, поэтому сторонники этого мифа не применяют серверы Microsoft Exchange и Microsoft SQL, поскольку они также работают на базе операционной системы Microsoft).
- Утверждение, что следует размещать наиболее слабый канал непосредственно перед самыми ценными данными (это похоже на размещение охранника с ав томатом перед зданием банка или пуделя перед открытой дверцей сейфа).

Совершенно ясно, что ряд комментирующих или промышленных аналитиков не понимает суть безопасности, обеспечиваемой брандмауэром в XXI веке, и по-прежнему придерживается маркетинговой информации 1997 г. от ведущих производителей брандмауэров. Но проблема состоит в том, что прославленный в прошлом году фильтр пакетов с отслеживанием состояния соединений просто не может сравниться с серьезными брандмауэрами с возможностью работы на уровне приложения типа ISA Server 2004.

Резюме

Важность безопасности стала очевидной для сетевых администраторов уже давно, но события нового тысячелетия, включая повышенный уровень виртуальных атак и физические атаки на США и их сторонников внутри страны и за рубежом, убедили нас в том, что современный мир опасен и что эти угрозы распространяются и на компьютерные сети, содержащие данные, от которых во многом зависят наши жизни. Защита цифровой информации стала высшим приоритетом для бизнеса и

частных лиц, а ключевым элементом обеспечения защиты любого компьютера, подключенного к сети (сегодня это относится почти к каждому компьютеру), является брандмауэр.

Своим происхождением ISA Server 2004 обязан Microsoft Proxy Server и ISA Server 2000, но корпорация Microsoft рассматривает этот брандмауэр как совершенно новый продукт. Полностью изменился пользовательский интерфейс, были добавлены ключевые функции (а некоторые функции были убраны), и ISA стал полнофункциональным брандмауэром, который разработан так, чтобы выдержать конкуренцию с «главными игроками» среди производителей брандмауэров: как программных брандмауэров промышленного уровня, так и аппаратных брандмауэров-устройств.

Репутация Microsoft по части обеспечения безопасности пострадала потому, что раньше они делали акцент на свойствах и функциональности в ущерб безопасности. Однако компания полностью пересмотрела свои приоритеты и сегодня ежегодно тратит миллионы долларов на безопасность. Ее инициатива «Trustworthy Computing initiative» и трехуровневая модель безопасности — безопасность при разработке, безопасность по умолчанию и безопасность в применении — подчеркивают безопасность, которая была включена при разработке ISA Server 2004 на каждом уровне.

В ISA Server 2004 используется подход к безопасности, основанный на политиках; это упрощает задачу администраторов по реализации политик безопасности, установленных руководством. Разработка соответствующих политик является ключевым шагом в планировании использования вашего брандмауэра, и оно включает оценку потребностей в безопасности, анализ факторов риска, оценку угроз и уровней угроз, анализ слабых мест в системе защиты организации и сети, анализ организационных факторов, которые оказывают влияние на безопасность, анализ юридических факторов и, наконец, анализ факторов стоимости.

Для того, чтобы быть эффективным, хороший план обеспечения безопасности должен придерживаться многоуровневого подхода. Нужно признавать, что в большинстве сетей более одного периметра, и применять различные меры по обеспечению безопасности (которые также могут включать использование нескольких брандмауэров) для обеспечения лучшей защиты важных ценностей (приложений для решения критически важных задач и данных) в центре сети.

Брандмауэры выполняют роль стражей у ворот (у входа в сеть или подсеть). Первыми брандмауэрами были простые устройства фильтрации пакетов, но современные сложные многоуровневые брандмауэры могут фильтровать пакеты на сетевом, транспортном уровнях и уровне приложения модели OSI для того, чтобы обеспечить максимальную безопасность. ISA Server 2004 является брандмауэром сетевого уровня с фильтрацией пакетов, с фильтрацией уровня канала и приложения, он также включает функции создания виртуальных частных сетей, обнаруже-

ния и предупреждения вторжений и Web-кэширования для улучшения производительности сети как для внутренних, так и для внешних пользователей.

ISA Server 2004 включает в себя много новых функций, а многие функции, которые он позаимствовал у ISA Server 2000, были улучшены и расширены. По мере чтения этой книги вы сначала ознакомитесь с понятиями, связанными с последней версией брандмауэра ISA, затем вы научитесь устанавливать, конфигурировать, управлять, использовать и устранять неисправности этого брандмауэра с помощью подробных пошаговых инструкций.

Приступим!

Глава

Изучение функциональных возможностей ISA Server 2004

Основные темы главы:

- **Новый GUI: больше, чем просто приятный интерфейс**
- **Старые функции обретают новые возможности**
- **Новые функции**
- **Отсутствующие функции: удалены, но не забыты**

В ISA Server 2004 сохранены многие функции, известные и ценимые администраторами еще по ISA 2000, во многих случаях они были сделаны еще более функциональными и простыми в использовании. Например, были улучшены администрирование виртуальных частных сетей, проверка подлинности, правила брандмауэра, OWA-публикации (Outlook Web Access publishing), поддержка FTP, безопасные Web-публикации, правила кэширования, средство контроля сообщений SMTP, настройка создания отчетов и т. д.

Также в ISA Server 2004 было добавлено множество новых функций, например: поддержка нескольких сетей, фильтрация и проверка с отслеживанием соединений для VPN-трафика (Virtual Private Network), изолирование VPN-подключений, пользовательские группы брандмауэра, создание форм на брандмауэре, которые используются службой OWA для проверки подлинности на основе форм, преобразование ссылок и т. д.

Интерфейс GUI (Graphical User Interface, графический пользовательский интерфейс) был полностью переработан и стал более удобным и интуитивно понятным для пользователей.

В этой главе представлен обзор нового интерфейса ISA 2004, обсуждаются старые функции, которые были улучшены, а также новые дополнения, которые облегчают работу администратора ISA Server. Здесь также будут рассмотрены несколько функций, которые входили в набор функций ISA Server 2000, но были удалены из ISA Server 2004, что сделало его более ясным и простым. Удаление устаревших функций отражает стремление корпорации Microsoft позиционировать ISA Server 2004 на рынке, прежде всего, как средство обеспечения безопасности и брандмауэр, который может конкурировать с ведущими производителями на рынке, и лишь в последнюю очередь — как сервер кэширования и ускорения. Это дает основание считать ISA 2004 более ценным продуктом и позволяет экономить средства организациям, которые не хотят покупать два отдельных продукта или дорогие дополнительные устройства к своим брандмауэрам.

Новый GUI: больше, чем просто приятный интерфейс

Прежде всего, рассмотрим первое, что бросается в глаза пользователю ISA Server — графический интерфейс. Без сомнения интерфейс ISA Server 2004 интуитивно более понятен, чем интерфейс ISA Server 2000. Основная цель группы разработчиков состояла в том, чтобы сделать интерфейс более понятным для пользователя, и они с этим справились. Любой, кто не знаком с ISA Server 2000, может обратиться к интерфейсу ISA Server 2004 и, нажимая различные клавиши, выполнить большую часть административных задач, не обращаясь к файлу Help (Помощь).

Изучение графического интерфейса

На рис. 2.1 показан интерфейс управления ISA Server 2000, а на рис. 2.2 — новый интерфейс ISA Server 2004. Очевидно, первый во многом похож на любую консоль MMC (Microsoft Management Console) с простой левой панелью в виде дерева и правой панелью с дополнительной информацией.

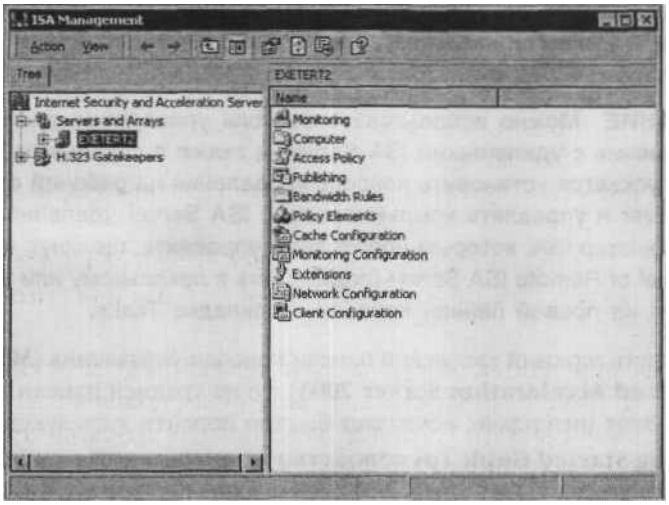


Рис. 2.1. Интерфейс ISA Server 2000 — обычная консоль MMC

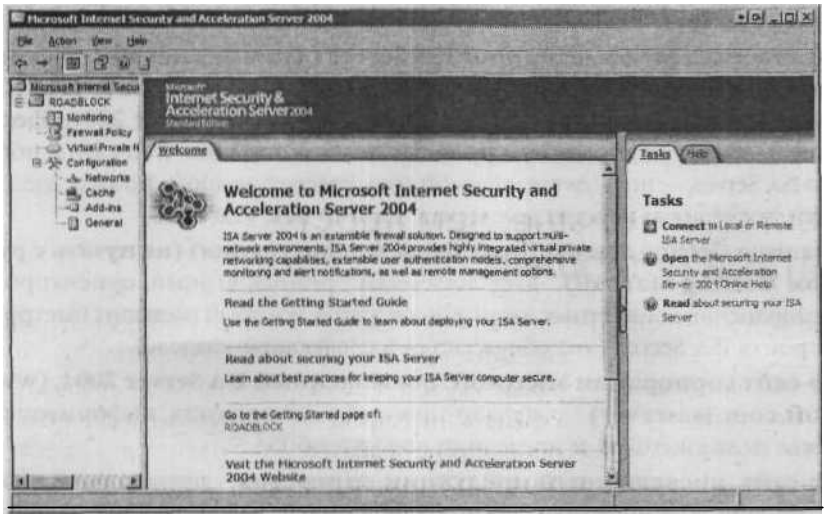


Рис. 2.2. Интерфейс управления ISA Server 2004 — удобный, состоящий из трех частей с закладками интерфейс

Консоль ISA Server 2004 более богата: в ней есть окно из трех панелей, которое не только включает уже знакомую древовидную структуру на левой панели, но также содержит страницы с закладками на центральной и правой панелях. Это позволяет легко выбрать тип задач, которые необходимо выполнить, и получить конкретную помощь в их осуществлении. Больше не требуется открывать множество других диалоговых окон, чтобы найти необходимую настройку. Теперь можно легко выполнять наиболее распространенные типы административных задач. Этому интерфейсу (когда нужно лишь выбрать пункт и щелкнуть его) можно легко и быстро научить любого ИТ-администратора.

ПРИМЕЧАНИЕ Можно использовать консоль управления для установления соединения с удаленными ISA Server, а также с локальным ISA Server. Также допускается установить консоль управления на рабочей станции или на ISA Server и управлять компьютерами с ISA Server удаленно. Вы выбираете компьютер ISA, которым необходимо управлять, щелкнув кнопку Connect to Local or Remote ISA Server (подключить к локальному или удаленному ISA Server) на правой панели консоли на вкладке Tasks.

Если щелкнуть верхний узел левой панели консоли управления **(Microsoft Internet Security and Acceleration Server 2004),** то на средней панели появится окно приветствия. Этот интерфейс позволяет быстро перейти к следующим опциям:

- **The Getting Started Guide (руководство по начальной конфигурации ISA Server), документ HTML (рис. 2.3)** Здесь даны подробные инструкции по ус тановке и конфигурированию ISA Server 2004 и представлен обзор функций («A Feature Walk-Through»), который покажет сценарии выполнения конкретных типовых задач.
- **Best Practices for Securing your ISA Server (лучшие способы обеспечения защиты ISA Server)** позволяет перейти в раздел Security and Administration (Бе зопасность и администрирование) файла Help для ISA Server 2004. Здесь также имеется ссылка на страницу с руководствами и статьями Web-сайта, посвящен ного ISA Server, — http://www.mic rosoft.com/isaserver/techinfo/howto/. Здесь можно найти последнюю версию документа Security Best Practices.
- **Страница Getting Started (начальная конфигурация) (не путать с руковод ством Getting Started!)** дает логически организованный, ориентированный на выполнение конкретных задач список шагов, который позволит быстро и легко настроить ISA Server (это обсуждается в следующем разделе).
- **Web-сайт корпорации Microsoft, посвященный ISA Server 2004, (www.microsoft.com/isaserver)** содержит новые версии продукта, информацию о под держке пользователей и последние новости об ISA Server.
- **Web-сайт, посвященный продукции партнеров,** представляет обширный список дополнений сторонних производителей, расширяющих функциональ ные возможности ISA Server. На сайте есть ссылки на сайты партнеров, разбор конкретных случаев, новости и обзоры от партнеров.

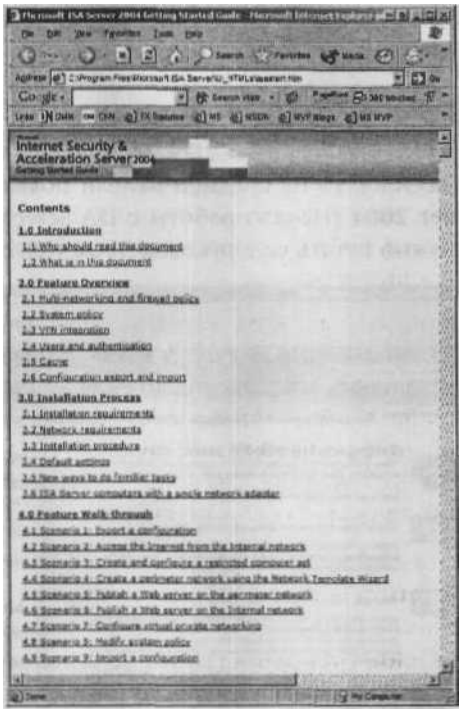


РИС. 2.3. Руководство Getting Started Guide для ISA Server 2004 — инструкции по установке и обзор функций

Изучение узлов управления

В зависимости от того, что выбрано на левой панели, на средней панели отображаются различные элементы конфигурирования, на которых можно щелкнуть кнопкой мыши. Узлы на левой панели включают в себя:

- ISA Server (Name) (Верхний узел ISA Server, Имя);
- Monitoring (Узел мониторинга);
- Firewall Policy (Узел политики брандмауэра);
- Virtual Private Network (VPN) (Узел виртуальной частной сети, VPN);
- Configuration (Узел конфигурирования).

Узел конфигурирования включает в себя четыре подузла:

- Networks (Сети);
- Cache (Кэш);
- Add-ins (Встраиваемые дополнительные устройства);
- General (Общие).

В следующих разделах будет рассмотрен каждый из этих узлов, их интерфейсы и выполняемые ими действия.

Узел ISA Server (Name)

Если выбирается узел, представляющий ISA Server (на рисунках в данной книге имя брандмауэра — ROADBLOCK), то на средней панели появится страница **Getting Started with ISA Server 2004** (Начало работы с ISA Server 2004), показанная на рис. 2.4. Опять же, не нужно путать ее с руководством Getting Started Guide.

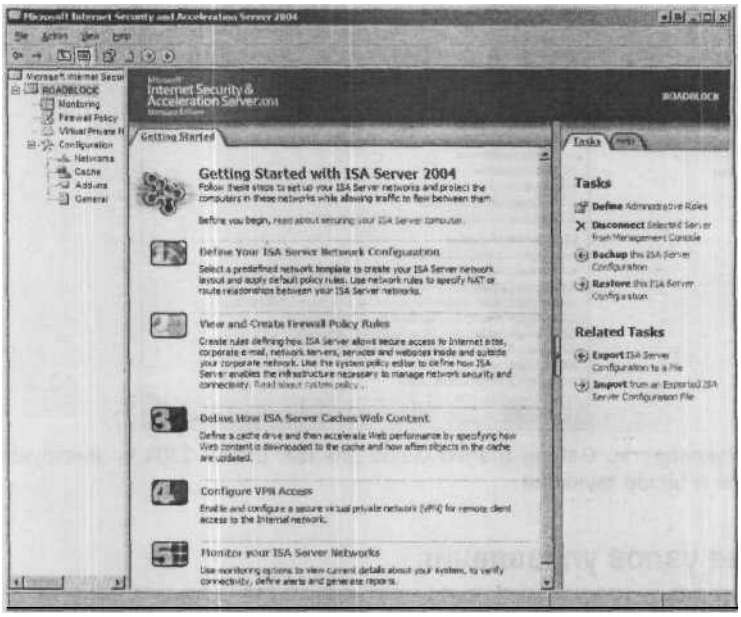


Рис. 2.4. Выбор имени ISA Server — на левой панели отображается страница Getting Started

Страница **Getting Started** (Начало работы) позволяет легко настроить ISA Server и/или сервер кэширования. Здесь представлены опции, предназначенные для выполнения следующих задач:

- **Defining Your ISA Server Network Configuration (Определение сетевой конфигурации ISA Server)** позволяет выбрать заранее определенный сетевой шаблон, который можно использовать для создания схемы сети с ISA Server и для применения правил и политик, установленных по умолчанию. Можно задать отношения NAT или отношения маршрутизации между несколькими сетями с ISA Server.
- **View and Create Firewall Policy Rules (Просмотр и создание правил политик брандмауэра)** позволяет настраивать правила, которые определяют спо-

соб предоставления ISA Server безопасного доступа к внутренним и внешним Web-сайтам, другим интернет-сайта м, серверам, e-mail **и** другим службам.

- **Define How ISA Server Caches Web (Определить способ кэширования ISA Server Web-контента)** настраивает кэширование, прежде всего определяя диск для кэширования, а затем правила **кэширования,** которые контролируют, какой Web-контент будет загружаться **в кэш, и** частоту обновления кэша.
- **Configure VPN Access (Настройка VPN-доступа)** позволяет создавать шлюз VPN для того, чтобы позволить удаленным пользователям устанавливать соеди нение с внутренней сетью посредством создания **виртуальной** частной сети.
- **Monitor your ISA Server Network (Наблюдение за сетью с ISA Server)** содержит варианты просмотра информации о системе и для проверки установ ления соединения (включая мониторинг пользователей *в* режиме реального времени: на каких Web-сайтах находятся **и** какие приложения используют). Можно также создавать уведомления, чтобы сообщить администраторам о кон кретных событиях по электронной почте, и настраивать создание однократных или регулярных отчетов.

ПРИМЕЧАНИЕ Каждый из вариантов на странице **Getting Started** в действительности переводит пользователя на один из узлов, показанных на левой панели. Таким образом, щелкнув кнопкой мыши вариант **Define Your ISA Server Network Configuration,** вы будете переведены в точно такой же интерфейс, как если бы вы щелкнули узел Networks в разделе Configuration на левой панели; если вы щелкнете на варианте **View and Create Firewall Policy Rules,** то окажетесь в том же самом интерфейсе, как если бы вы щелкнули вариант **Firewall Policy** на левой панели, и т. д. После ознакомления с консолью управления ISA Server 2004, наверное, будет проще щелкнуть соответствующий узел на левой панели, но на странице **Getting Started** все варианты настройки, которые потребуются при первоначальной настройке ISA Server на компьютере, организованы в упорядоченный список.

Если выбран верхний узел ISA Server на вкладке **Tasks** (Задачи) правой панели, то видны значки для выполнения нескольких задач, которые имеют отношение к ISA Server в целом. Они включают *в* себя:

- **Define Administrative Roles (Определить административные роли)** вы зывает мастера делегирования **административных** функций Administration Dele gation Wizard, с помощью которого можно назначить административные роли отдельным пользователям или группам пользователей. Эти роли определяют, какие полномочия имеют пользователи для администрирования ISA Server.
- **Disconnect Selected Server from Management Console (Отключить выбран ный сервер от консоли управления)** позволяет отключиться от локально го или удаленного ISA Server.

- **Backup this ISA Server Configuration (Создать резервную копию этой конфигурации ISA Server)** позволяет сохранить конфигурацию ISA Server в виде файла XML
- **Restore this ISA Server Configuration (Восстановить эту конфигурацию ISA Server)** позволяет воспользоваться файлом XML, созданным выбором создания резервной копии, для того чтобы восстановить конфигурацию.

Раздел Related Tasks (Родственные задачи) включает экспорт и импорт файлов конфигурации для ISA Server (в формате XML).

Секреты ISA Server

Чем отличается создание резервной копии/восстановление от экспорта/импорта?

Нам часто задают вопрос: «Чем отличаются функции Backup (Создание резервной копии) и Restore (Восстановление) от функций Export (Экспорт) и Import (Импорт)?». Это хороший вопрос, потому что на первый взгляд они кажутся одинаковыми. В обоих случаях мы сохраняем конфигурацию ISA Server в файл XML, а затем обращаемся к ней и применяем ее к ISA Server. Единственное отличие между этими двумя диалоговыми окнами сохранения файла, состоит в том, что *в* диалоговом окне **Export** (Экспорт) есть два флажка, которых нет в диалоговом окне **Backup** (Создание резервной копии):

- Export user permission settings (Настройки полномочий пользователя по экспорту);
- Export confidential information (Экспорт конфиденциальной информации — будет применяться шифрование).

Оба эти набора функций позволяют сохранить информацию о конфигурации, но функция экспорта/импорта позволяет осуществлять более тщательный контроль над сохраняемой информацией и способом ее сохранения.

С помощью функции Backup/Restore сохраняется общая информация о конфигурации сервера. Она состоит из правил политик брандмауэра, элементов правил, настроек уведомлений, настроек кэширования и настроек VPN. Невозможно сохранять эту информацию частично: в этом случае действует принцип «все или ничего».

Используя функцию экспорта/импорта, можно сохранить всю конфигурацию или ее конкретные фрагменты. Например, можно сохранить только информацию о сетях или об одной сети или только правила создания Web-цепочек или даже только одно конкретное правило создания цепочек, только выборочные политики брандмауэра, только настройку кэширования и т. д. Если выбран экспорт всей конфигурации, то будет сохранена следующая информация:

- правила доступа;
- правила публикации;
- элементы правил;
- настройка уведомлений;
- настройка кэширования;
- свойства ISA Server и вся общая информация о конфигурации.

Можно выбирать, экспортировать ли конфиденциальную информацию, например пароли пользователей, совместно используемые ключи для IPSec и совместно используемые настройки RADIUS. Также можно выбирать, экспортировать ли настройки полномочий пользователей. При использовании функции Backup выбор отсутствует: происходит автоматическое сохранение конфиденциальной информации и настроек полномочий пользователей. В любом случае при сохранении конфиденциальной информации она зашифровывается в целях защиты. В процессе операции экспорта указывается пароль, который нужно будет ввести при импорте конфигурации.

Зачем же экспортировать всю конфигурацию, вместо создания резервной копии? Экспорт всей конфигурации часто используется для клонирования сервера — создания второго ISA Server с идентичной конфигурацией. Если вам нужно, чтобы несколько ISA Server имели одинаковую конфигурацию, например для нескольких филиалов, этот способ является самым быстрым.

Важно отметить, что когда экспортируется вся конфигурация целиком, в нее включаются настройки сертификатов. Если импортируется конфигурация на другой ISA Server, на котором не установлены такие же сертификаты, то брандмауэр на этом сервере работать не будет.

Мы более подробно рассмотрим задачи начального конфигурирования ISA Server в главе 6.

Узел Monitoring

Узел мониторинга в ISA Server 2004 является гораздо более совершенным, чем интерфейс мониторинга и создания журналов в ISA Server 2000. Это достаточно нагруженный узел, т. к. на средней панели отображаются семь страниц с вкладками:

- Dashboard (Инструментальная панель);
- Alerts (Оповещения);
- Sessions (Сеансы);
- Services (Службы);
- Reports (Отчеты);
- Connectivity (Соединения);
- Logging (Ведение журналов).

Вкладка **Dashboard** (Инструментальная панель) (см. рис. 2.5) представляет собой обзор всех параметров, имеющихся **на** вкладке (за исключением вкладки Logging). Точно так же, когда вы смотрите на приборную панель автомобиля, то можете следить за всем, что происходит со всеми параметрами одного интерфейса.

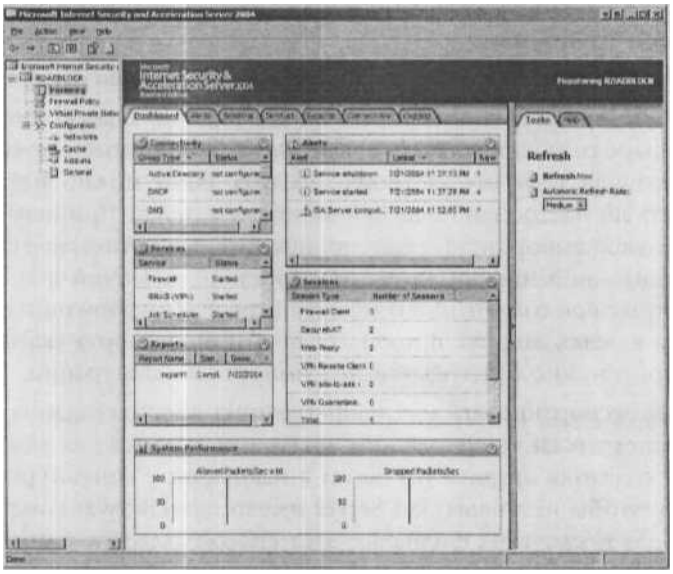


Рис. 2.5. Вкладка **Dashboard** (Инструментальная панель) — одновременный обзор всех параметров наблюдения

Инструментальная панель также предоставляет информацию о производительности системы; можно видеть в графическом представлении количество пакетов, проходящих за секунду (x 10), и количество пакетов, отбрасываемых за сеьунду.

Каждый раздел инструментальной панели имеет значок, который указывает на статус этого параметра:

- **галочка внутри зеленого кружка** означает, что все в порядке;
- **восклицательный знак внутри желтого треугольника** означает предупреж дение;
- **значок X внутри красного кружка** означает проблему или потенциальную проблему.

Более подробную информацию о каждом параметре можно получить, щелкнув соответствующую вкладку.

Вкладка **Alerts** (Оповещения) (см. рис. 2.6.) предоставляет информацию об имевших место важных событиях, например при запуске или остановке служб, при обнаружении вторжения, при превышении лимита соединений и т. д. Можно выбрать, при каких событиях будут создаваться оповещения.

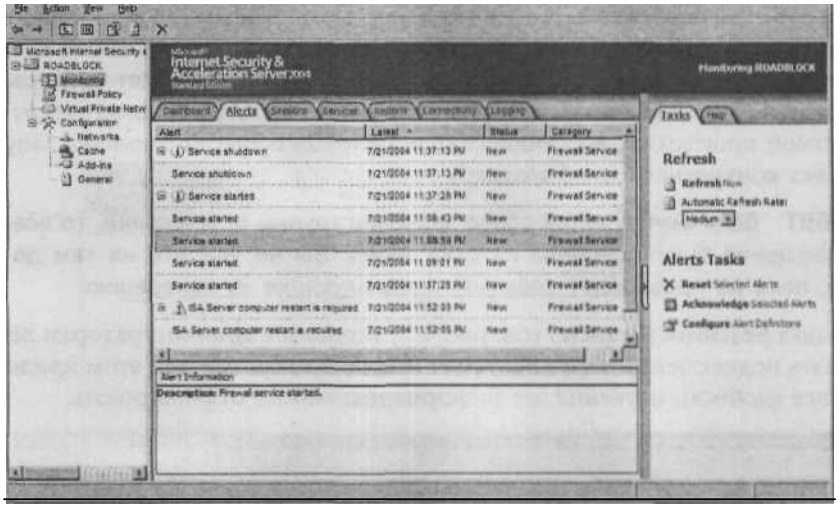


Рис. 2.6. Вкладка Alerts (Оповещения) извещает о важных событиях, которые происходят на ISA Server

Как видно на рис. 2.6, если щелчком выбрать оповещение, то внизу средней панели будет показана более подробная информация об этом событии. Оповещения отмечаются значками, которые показывают относительную важность каждого из них. Эти значки знакомы администраторам Windows, поскольку они в точности повторяют значки, используемые в оснастке Event Viewer (Просмотр событий) и в журналах приложений.

- **строчная буква «i» в белом кружке** означает, что это информационное опо вещение. Никаких действий предпринимать не нужно;
- **восклицательный знак в желтом треугольнике** означает предупреждение. Возможно, нужно что-то предпринять;
- **значок X в красном кружке** означает ошибку, проблему или потенциальную проблему, которая требует к себе немедленного внимания.

Правая панель задач позволяет вручную обновить окно Alerts или же установить частоту автоматического обновления (не обновлять, редко, средняя частота, часто). На вкладке **Alerts Tasks** можно сбросить значения выбранных оповещений, щелкнув те оповещения, значения которых нужно сбросить (можно выделить несколько оповещений, удерживая клавишу <Ctrl> при их выборе), а затем нажав кнопку **Reset.** Программа спросит, уверены ли вы, что хотите сбросить значение оповещения. Щелкните кнопку **Yes,** чтобы подтвердить сброс.

Также можно выбрать вариант **Acknowledge** (Уведомлять), подтверждая что вы работаете с этим оповещением. Благодаря этому данное оповещение не будет удалено из окна Alerts, однако его просмотр будет удален с инструментальной панели.

Наконец, можно настроить оповещения, выбирая их из списка заранее определенных событий оповещения, а также можно указать, сколько раз должно произойти событие или же сколько подобных событий должно произойти за секунду, чтобы было создано оповещение. Можно также указать, что произойдет при появлении оповещения (отправка оповещения по электронной почте администратору, запуск конкретной программы, внесение записи в журнал событий Windows, запуск или остановка конкретной службы/служб).

СОВЕТ Если выполняется сброс значений группы оповещений, то все эти оповещения будут удалены из окна Alerts. Вы не увидите их там до тех пор, пока не произойдут события, инициирующие их генерацию.

Вкладка **Sessions** (Сеансы) (см. рис. 2.7) позволяет администраторам легко отслеживать подключения через ISA Server и использованные при этом приложения. Для более удобного изучения эту информацию можно отфильтровать.

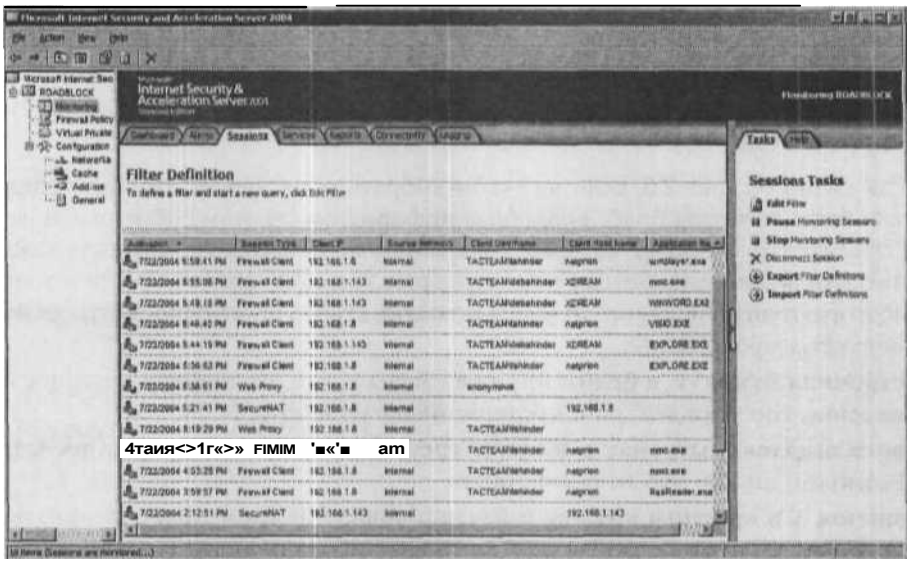


Рис. 2.7. Использование вкладки Sessions (Сеансы) — просмотр информации о том, кто устанавливал соединения через ISA Server

Вкладка **Services** (Службы) (см. рис. 2.8) показывает статус и период работоспособного состояния **служб** ISA Server и других связанных с ним служб, работающих на компьютере с операционной системой Windows 2000 или Windows Server 2003. Можно запускать и останавливать службы из этого окна или из раздела **Services Tasks** (Задачи служб) на правой **панели, или** же дважды щелкнув службу, которую вы хотите запустить или остановить.

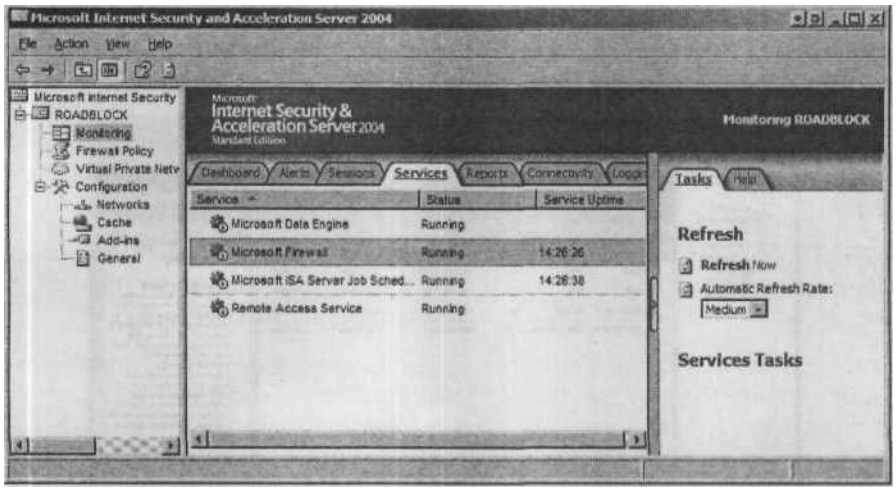


Рис. 2.8. Вкладка Services (Службы) — остановка и запуск служб ISA Server

Можно использовать вкладку **Reports** (Отчеты) (см. рис. 2.9, для того, чтобы создавать разовый отчет или настраивать создание регулярных отчетов. Мастер создания новых отчетов New Report Wizard позволяет создать разовый отчет. Вариант Report jobs (Задания на отчет) позволяет создавать регулярные отчеты ежедневно, еженедельно или ежемесячно. Можно указать, какую информацию следует включать в отчеты.

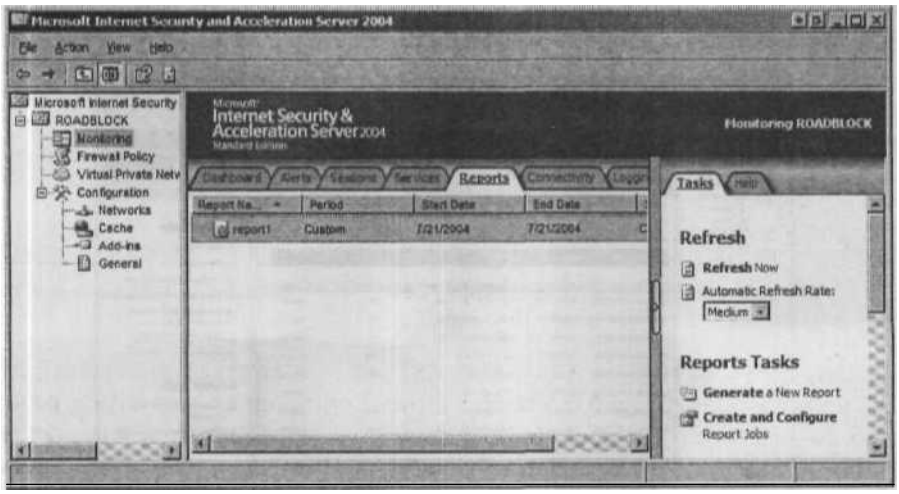


Рис. 2.9. Вкладка Reports (Отчеты) — создание отчетов по журналам

Вкладка Connectivity (Соединения) (см. рис. 2.10) позволяет создавать, экспортировать и импортировать верификаторы соединений. Верификаторы соедине-

ний — это объекты, которые осуществляют мониторинг статуса соединения между компьютером с ISA Server и отдельным компьютером или URL Соединения можно определять через сообщения PING, через порт TCP или HTTP-запрос.

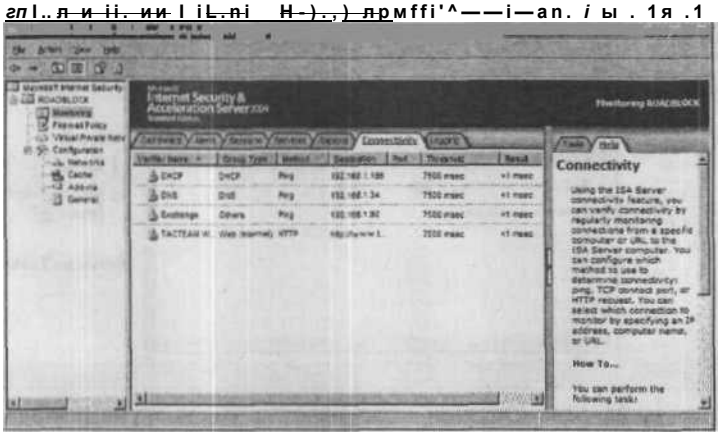


РИС. **2.10.** Вкладка **Connectivity** (Соединения) — мониторинг статуса соединений между ISA Server и конкретным компьютером или URL

Последняя вкладка в окне Monitoring — это вкладка **Logging** (Ведение журналов) (см. рис. 2.11), Ее можно использовать для того, чтобы настроить процесс создания журналов для брандмауэра, Web-прокси и журналов средств контроля сообщений SMTP. Кроме того, можно отредактировать фильтры так, чтобы ограничить выводимые данные, экспортировать или импортировать определения фильтров, а также создавать запросы к журналам.

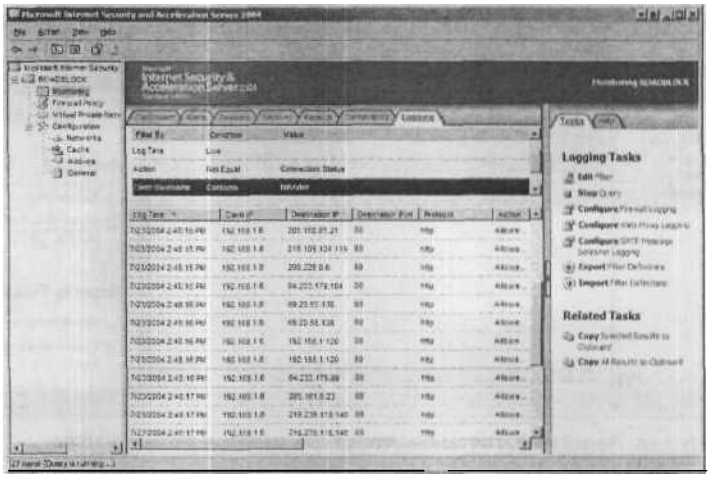


Рис. 2.11. Вкладка **Logging** (Ведение журналов) — фильтрация и создание запросов данных в файлах журналов ISA Server

Узел Firewall Policy

Если выбрать узел **Firewall Policy** (Политика брандмауэра), то на средней панели появится список правил политик брандмауэра, а на правой панели будут отображаться вкладки под названием Toolbox (Инструментарий), Tasks (Задачи) и Help (Помощь), как это показано на рис. 2.12.

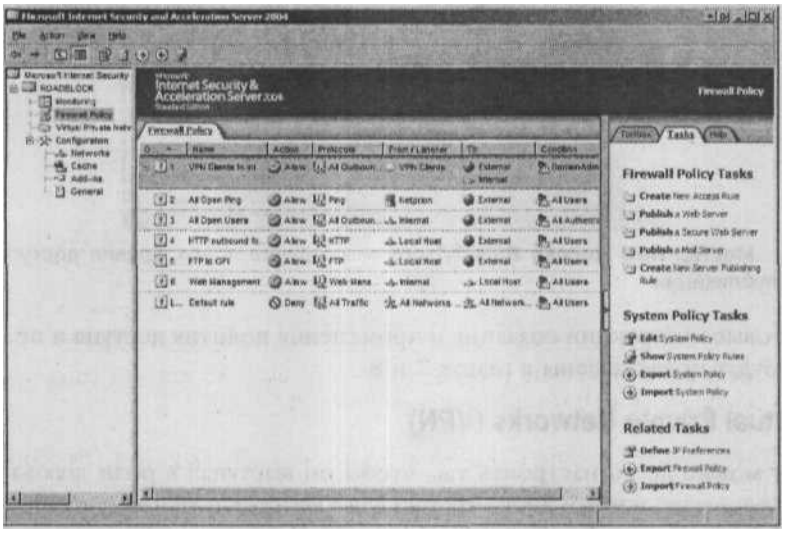


Рис. 2.12. Firewall Policy (Политика брандмауэра) — конфигурирование правил

Узел **Firewall Policy** (Политика брандмауэра) является «ядром» интерфейса ISA Server. Именно здесь создаются правила доступа, правила Web-публикации, правила публикации почтовых серверов и **другие** правила публикации серверов для контроля входящего и исходящего доступа к сети. Кроме того, здесь можно редактировать политику системы, определять приоритеты IP-адресов, а также экспортировать и импортировать как политики системы, так и политики брандмауэра. Новые правила доступа можно легко создавать с помощью мастера создания новых правил доступа New Access Rule Wizard, окно которого представлено на рис. 2.13-

Рис. 2.13. Мастер **New Access Rule Wizard** — создание новых правил доступа и правил публикации

Пошаговые инструкции создания и применения политик доступа и правил публикации будут представлены в главах 7 и 8.

Узел Virtual Private Networks (VPN)

ISA Server можно легко настроить так, чтобы он выступал в роли шлюза VPN для пользователей с удаленным доступом или для VPN-подключений «узел-в-узел». Узел **Virtual Private Networks** (Виртуальные частные сети), показанный на рис. 2.14, предоставляет удобный интерфейс для выполнения наиболее распространенных задач конфигурирования VPN и контроля клиентского доступа.

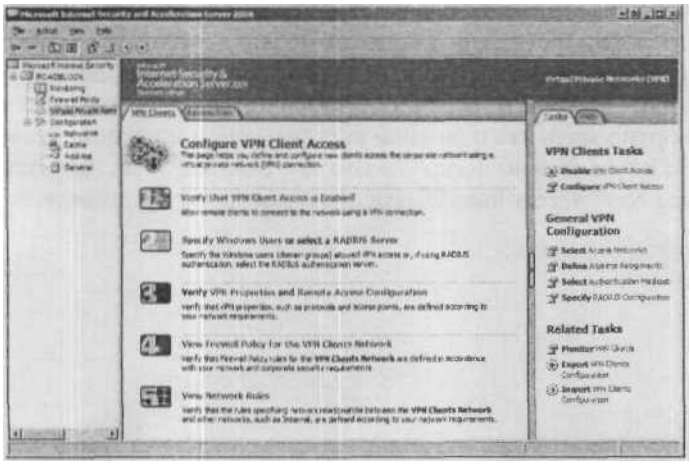


Рис. 2.14. Узел **Virtual Private Networks** (Виртуальные частные сети) для настройки виртуальных частных сетей

На средней панели представлен список задач конфигурирования, включая следующие:

- проверка разрешения доступа VPN-клиента;
- указание пользователей Windows, для которых разрешен VPN-доступ, или вы бор сервера RADIUS для проверки подлинности;
- проверка свойств VPN и конфигурации удаленного доступа;
- просмотр правил политики брандмауэра для сети VPN-клиентов;
- просмотр правил, которые определяют сетевые отношения между сетью VPN-клиентов и другими сетями.

На правой панели Tasks (Задачи) можно настроить клиентский доступ (указав число одновременных VPN-соединений, выбрав группы, для которых разрешен VPN доступ, указав разрешенные протоколы VPN и установление соответствий для пользователей из прочих пространств имен (не Windows)). Можно даже одним щелчком запретить любой доступ к VPN.

Подробнее процедуры создания и управления виртуальными частными сетями обсуждаются в главе 9.

Узел Configuration: подузел Networks

В узле **Configuration** (Конфигурирование) есть четыре подузла. Если выбрать подузел **Networks** (Сети), то на средней панели появится набор страниц-вкладок, который включает в себя **Networks** (Сети), **Network sets** (Подмножества сетей), **Network rules** (Сетевые правила) и **Web-chaining** (Создание Web-цепочек), как это показано на рис. 2.15.

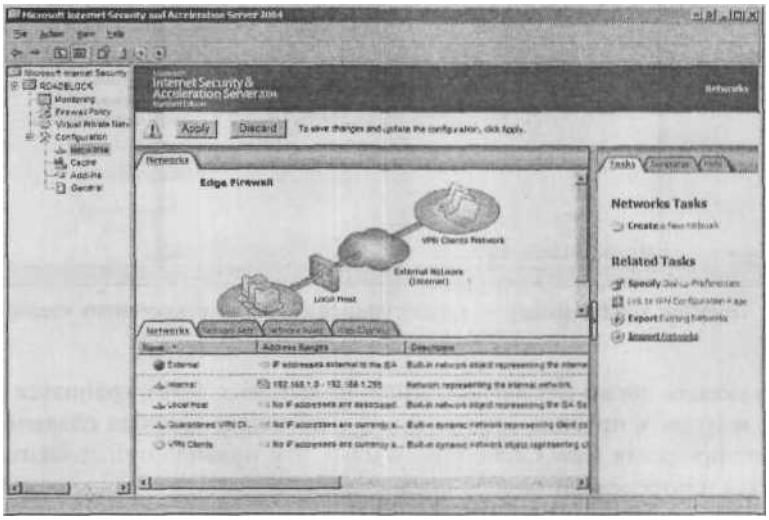


Рис. 2.15. Вкладка Networks (Сети) — настройка сетей, подмножеств сетей, сетевых правил и создания Web-цепочек

На правой панели находятся вкладки: **Tasks** (Задачи), **Templates** (Шаблоны) и **Help** (Помощь).

Вкладка **Networks** используется для создания и настройки сетей в конфигурациях с несколькими подсетями. Вкладка **Network Sets** позволяет группировать сети и применять правила к группе или подмножеству сетей. Вкладка **Network Rules** используется для создания, экспорта и импорта правил, определяющих, какой тип соединения разрешен между различными сетями с помощью преобразованных (NAT) или маршрутизируемых соединений (и разрешен ли он вообще). Вкладка **Web Chaining** используется для создания правил образования Web-цепочек, позволяющих маршрутизировать запросы от клиентов к вышестоящему ISA Server или в другое место сети.

Конфигурации с несколькими подсетями рассматриваются в главе 12.

Узел Configuration: подузел Cache

Подузел **Cache** (Кэш), изображенный на рис. 2.16, используется для настройки кэширования на ISA Server.

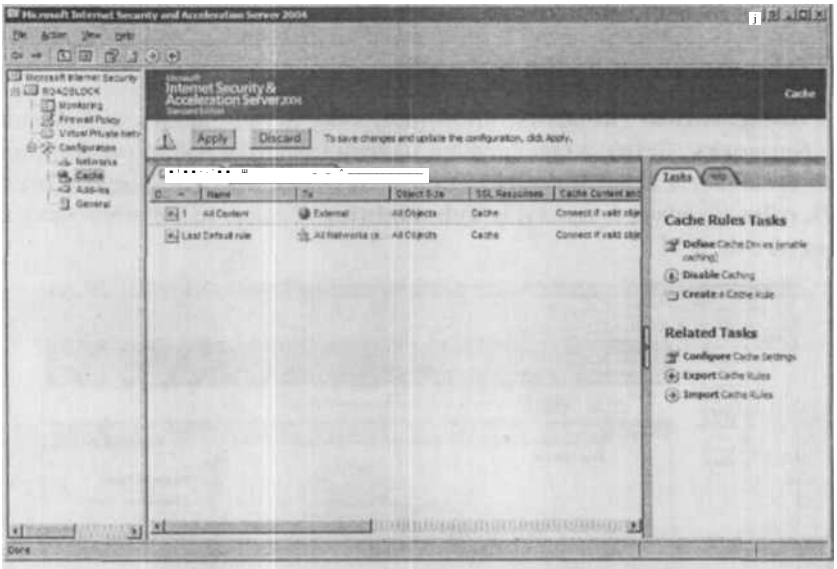


Рис. 2.16. Подузел Cache (Кэш) — конфигурирование или отключение кэширования на ISA Server

Можно указать лиски для кэширования, на которых будет храниться содержимое кэша, и создать правила кэширования с помощью мастера создания нового правила кэширования New Cache Rule Wizard. Эти правила применяются в конкретных сетях и определяют способ предоставления доступа к сохраняемым в кэше объектам при поступлении к ним запроса, а также время кэширования содержи-

мого и ограничение размеров кэшируемых объектов. Здесь можно задать общие настройки кэширования и правила кэширования для экспорта и импорта. Можно также полностью отключить кэширование, при этом ISA Server будет функционировать только как брандмауэр.

Пошаговые процедуры конфигурирования и использования ISA Server *в* качестве сервера кэширования будут описаны в главе 11.

Узел Configuration: подузел Add-ins

Подузел **Add-ins** (Расширения) используется для настройки фильтрации на уровне приложения (application layer filtering, ALF) на ISA Server. Именно здесь можно активировать, просматривать, изменять и отключать фильтры приложений и Web-фильтры. Некоторые фильтры устанавливаются и активируются по умолчанию, при установке ISA Server. Подузел Add-ins показан на рис. 2.17.

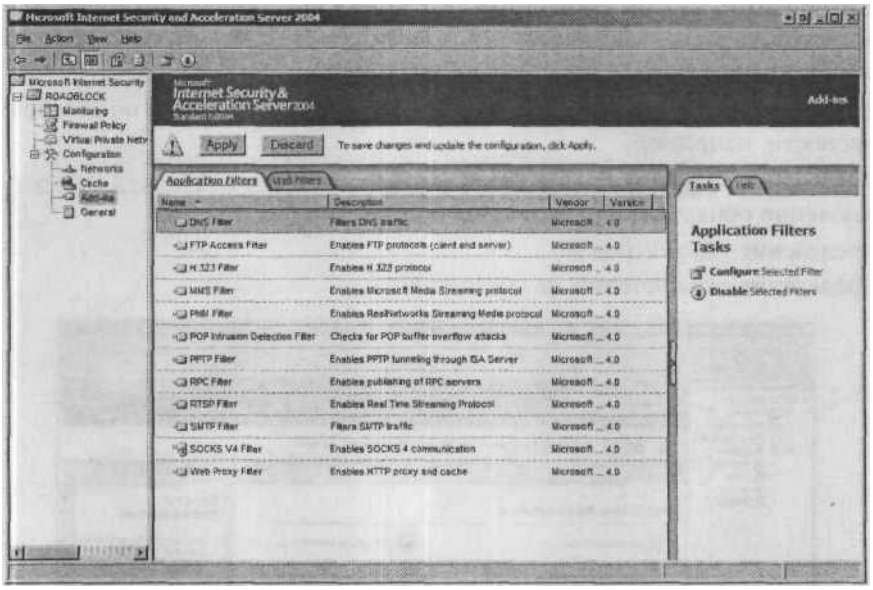


Рис. 2.17. Подузел **Add-ins** (Расширения) — настройка фильтров приложений и Web-фильтров

Узел Configuration: подузел General

Наконец, подузел **General** (Общее) (рис. 2.18) включает общие административные задачи, а именно:

- **Delegation of administration** (делегирование административных полномочий) дает право пользователям и группам выполнять определенные административные задачи;

- **Configuration of firewall chaining** (конфигурирование создания цепочек брандмауэров) для того, чтобы указать, как передаются запросы от клиентов брандмауэра и клиентов SecureNAT к вышестоящим серверам;
- **Specification of Dial-up preferences** (установка параметров dial-up соедине ния) применяется, если используется учетная запись dial-up;
- **Specification of certificate revocation** (указание аннулирования сертификатов) для того чтобы ISA Server мог проверить факт наличия поступающих сертифика тов в списке аннулированных сертификатов CRL (Certificate Revocation List);
- **Definition of Firewall client settings** (определение настроек клиента бранд мауэра) включая настройку приложений;
- **Viewing of ISA Server computer details** (просмотр информации о компьюте ре, на котором установлен ISA Server). Эта информация включает в себя версию ISA, название и ID продукта, дату создания и установочный каталог;
- **Configuration of link translation** (настройка преобразования ссылок) позво ляет выбрать типы содержимого (контента), определяющие страницы, к кото рым будет применяться преобразование ссылок.

Этот подузел также позволяет выполнять более сложные задачи по обеспечению безопасности, например:

- определение серверов RADIUS;
- включение обнаружения вторжений и DNS-атак;
- определение параметров IP;
- определение ограничений на соединения.

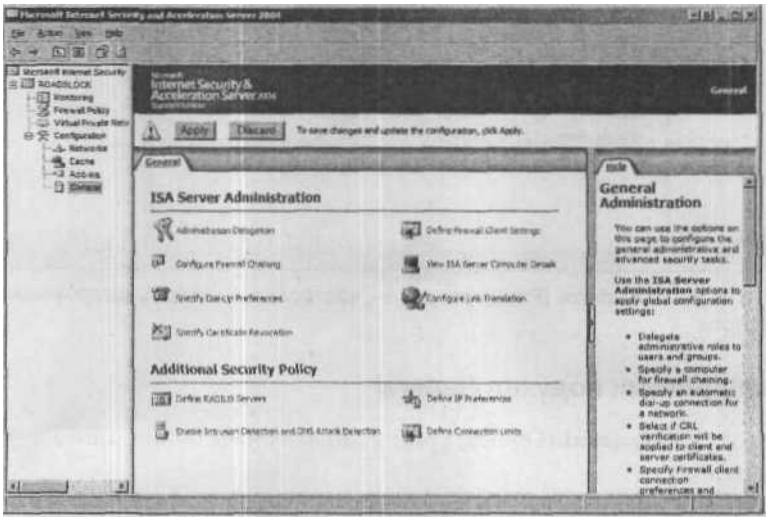


Рис. 2.18. Подузел General (Общие) используется для выполнения общих административных задач и более сложных задач по обеспечению безопасности

Старые функции обретают новые возможности

Интерфейс GUI является не единственной функцией, которая была усовершенствована в ISA Server 2004. По сути, в ISA Server 2004 были упрощены многие задачи, знакомые администраторам брандмауэров по ISA Server 2000. В следующих разделах мы обсудим некоторые наиболее важные улучшения, сгруппировав их по следующим категориям:

- удаленное управление;
- функции брандмауэра;
- создание виртуальных частных сетей и удаленный доступ;
- Web-кэш и Web-прокси;
- мониторинг и создание отчетов.

Усовершенствованные и улучшенные механизмы удаленного управления

Администраторы должны иметь возможность удаленного управления брандмауэрами ISA Server: со своих настольных компьютеров, со своих портативных компьютеров, когда они в пути или в другой местности, а иногда даже с компьютеров, которые они сами не контролируют, например с компьютеров общего пользования. Если в вашей компании есть множество ISA Server, установленных в различных местах, то вам не захочется физически контактировать с каждым компьютером, на котором установлен ISA Server для выполнения каких-либо административных задач.

> ПРИМЕЧАНИЕ При желании можно скопировать файл Help для ISA Server 2004 на рабочую станцию или на другой компьютер, на котором не установлен ISA Server, тогда к нему можно всегда получить доступ через консоль ISA Management или службы терминалов/удаленный настольный компьютер, даже если у вас нет соединения с компьютером, на котором установлен ISA Server. Для этого нужно перейти в папку Microsoft ISA Server на ISA Server (обычно установка выполняется в папку Program Files) и найти файл isa.chm. Скопируйте этот файл на вашу рабочую станцию или на жесткий диск, на котором нет ISA Server, и *вы* сможете получить доступ к файлам Help, не подключаясь к ISA Server.

ISA Server 2004 предоставляет несколько различных способов удаленного управления брандмауэрами. В следующих разделах будут обсуждаться три способа удаленного управления:

- консоль ISA Management;
- службы терминалов Windows 2000 или удаленный рабочий стол Windows Server 2003;
- Web-интерфейсы сторонних производителей.

Удаленное управление посредством консоли ISA Management

С помощью консоли управления можно установить соединение с удаленным ISA Server или с несколькими ISA **Server.** У каждого ISA Server будет свой верхний узел на левой панели, как показано на рис. 2.19.

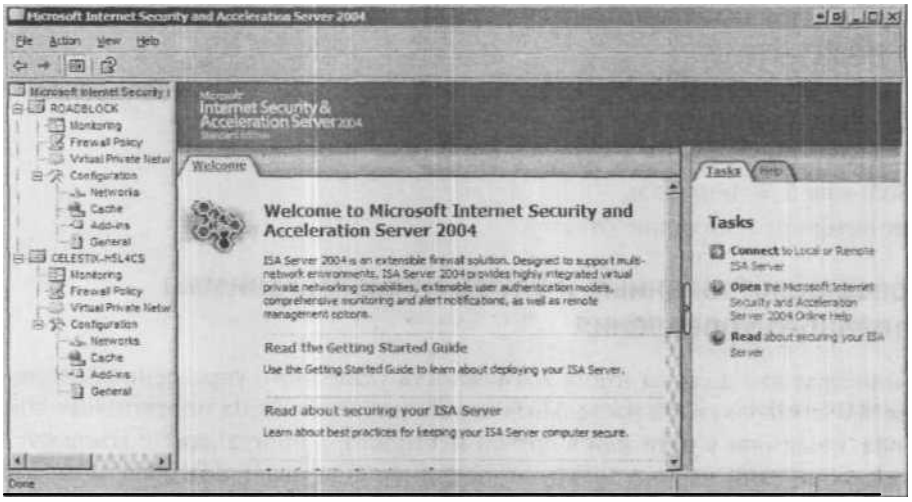


Рис. 2.19. С помощью консоли управления можно установить соединение с несколькими ISA Server одновременно

Для того чтобы установить соединение со вторым или следующим ISA Server, щелкните кнопку **Connect to Local or Remote ISA Server** (Установить соединение с локальным или удаленным ISA Server) на правой панели и введите имя или IP-адрес удаленного сервера и верификационные данные для получения к нему доступа, как показано на рис. 2.20.

> СОВЕТ Если соединение установить не удается, изучите предлагаемые далее инструкции и добавьте ваш компьютер в список Remote Management Computers (Компьютеры удаленного управления) в узле политики брандмауэра ISA Firewall Policy.

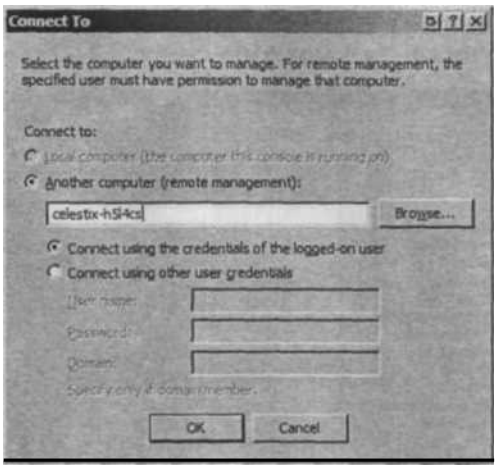


Рис. 2.20. Используйте диалоговое окно Connect To (Установка соединения) для добавления удаленного ISA Server в консоль управления

ПРИМЕЧАНИЕ С помощью консоли управления можно установить удаленное соединение только с брандмауэрами ISA Server 2004. При попытке установить соединение с брандмауэром ISA Server 2000 появится сообщение: «A failure occurred. The task was not activated» («Произошел сбой. Задача не активирована»).

Для осуществления удаленного управления ISA Server нужно настроить системную политику так, чтобы было активировано удаленное управление. Для того чтобы настроить системную политику:

1. На компьютере с установленным ISA Server щелкните узел **Firewall Policy** (Политика брандмауэра) на левой панели консоли управления.
2. Щелкните правило **System Policy** (Системная политика) под названием «Allow remote management from selected computers using MMC» («Разрешить удаленное управление с выбранных компьютеров посредством консоли MCC»), чтобы просмотреть это правило.
3. Для того чтобы добавить компьютер, на правой панели щелкните **Edit System Policy** (Редактировать системную политику) в разделе **System Policy Tasks** (Задачи системной политики), Откроется окно редактирования системных политик **System Policy Editor** (Редактор системной политики).
4. На правой панели окна **Editor** (Редактор) в разделе **Configuration Groups** (настройка групп) перейдите к пункту **Remote Management** (Удаленное управление) и щелкните **Microsoft Management Console** (MMC).
5. Откройте вкладку **From** (От), по умолчанию вы увидите надпись **Remote Management Computers** (Удаленно управляемые компьютеры) в поле под названи-

ем This rule applies to traffic from these sources (Это правило применяется к трафику от этих источников), как показано на рис. 2.21.

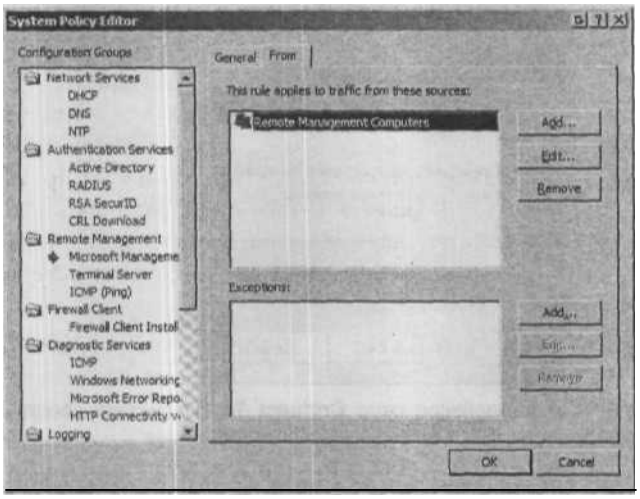


Рис. 2.21. Используйте редактор **System Policy Editor** (Редактор системной политики) для того, чтобы настроить компьютеры удаленного управления

6. Дважды щелкните **Remote Management Computers** (Удаленно управляемые компьютеры).
7. В окне свойств, как показано на рис. 2.22, щелкните кнопку **Add** (Добавить) и выберите **Computer** (Компьютер), **Address Range** (Диапазон адресов) или **Sub net** (Подсеть).

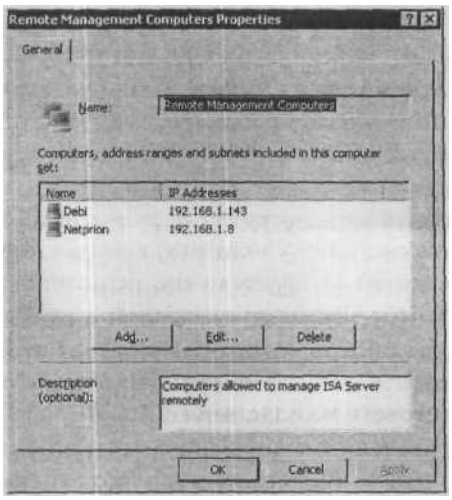


Рис. 2.22. Добавление компьютера, диапазона адресов или подсети в список компьютеров удаленного управления

Можете добавить IP-адрес отдельного компьютера, с которого необходимо удаленно управлять ISA Server, диапазон адресов или *всю* подсеть. Компьютеры, к которым применяется это правило, будут единственными, откуда вы сможете управлять ISA Server.

Можно также добавить сетевые объекты (сети целиком, подмножества сетей, компьютеры, диапазоны адресов, подсети и подмножества компьютеров) непосредственно к правилу вместо того, чтобы добавлять их в список **Remote Management Computers** (Удаленно управляемые компьютеры). Это может пригодиться, если, к примеру, нужно разрешить VPN-клиентам удаленно управлять ISA Server. В этом случае щелкните **Add** (Добавить) на вкладке **From** (От), затем в диалоговом окне **Add Network Entities** (Добавить сетевые объекты) откройте **Networks** (Сети) и выберите **VPN clients** (VPN-клиенты).

Лучше (и безопаснее) добавить в список **Remote Management Computers** (Удаленно управляемые компьютеры) отдельные компьютеры. Однако, если необходимо управлять ISA Server с различных рабочих станций в пределах организации и заранее неизвестно с какого компьютера будет осуществляться управление, можно добавить в этот список подсеть, диапазон адресов или даже всю внутреннюю сеть (что не рекомендуется).

Секреты ISA Server

Установка консоли управления

Прежде чем можно будет управлять ISA Server с компьютера, на котором не установлен ISA Server, нужно установить консоль управления. Можно установить консоль на компьютерах с ОС Windows Server 2003, Windows XP и Windows 2000.

Для этого вставьте установочный диск ISA Server или перейдите к установочным файлам ISA Server на файловом сервере. Дважды щелкните на файле isaautorun.exe для того, чтобы запустить программу установки ISA Server 2004. На первой странице установки щелкните **Install ISA Server 2004.**

Если консоль устанавливается на компьютере, работающем под управлением ОС, отличной от Windows 2000 Server или Windows Server 2003, то появится сообщение о том, что на этом компьютере невозможно установить ISA Server 2004. В любом случае нажмите **Continue** (Продолжить), на экране появится список компонентов, которые можно установить, включая консоль управления. Продолжайте работу с мастером установки для того, чтобы установить консоль управления на вашем компьютере. В списке программ она будет обозначаться как Microsoft ISA Server.

После того, как соединение с удаленным ISA Server с помощью консоли управления установлено, можно выполнять любые административные зада-

(см. след. стр.)

чи, как будто вы работаете за локальным ISA Server. Это **значительное** усовершенствование по сравнению с консолью удаленного управления в ISA Server 2000. Например, в ISA Server 2000 не было возможности настраивать виртуальные частные сети или управлять ими. В ISA Server 2004 можно управлять всеми элементами ISA Server удаленно.

Удаленное управление с помощью служб терминалов/удаленного рабочего стола

Еще один способ управления ISA Server с удаленного компьютера состоит *в* использовании служб терминалов (если используется ISA Server 2004 на базе сервера Windows 2000) или удаленного рабочего стола (если используется ISA Server 2004 на базе сервера Windows 2003). Преимущество этого метода заключается в том, что при этом не нужно устанавливать программное обеспечение консоли управления ISA Server на удаленном компьютере.

Если ISA Server управляется удаленно с компьютера с ОС Windows XP или Windows Server 2003, то нет необходимости устанавливать какое-либо программное обеспечение, поскольку клиентское программное обеспечение RDC (Remote Desktop Connection, установка соединения с удаленным рабочим столом) уже установлено (его можно найти в списке **Programs/Accessories/Communications).**

Если необходимо управлять ISA Server с компьютера с ОС Windows 2000 или Windows 9x, то сначала нужно установить программное обеспечение клиента служб терминалов или клиента RDC.

ПРИМЕЧАНИЕ Если ISA Server работает на базе ОС Windows 2000 Server, то на сервере должны быть установлены службы терминалов, которые дслжны работать в режиме удаленного администрирования или в режиме сервера приложений. Если ISA Server работает на базе ОС Windows Server 2003, то нужно убедиться в том, что на вкладке Remote в апплете свойств System панели управления установлен флажок Allow users **to connect remotely to this computer** (Разрешить пользователям удаленный доступ к этому компьютеру). Кроме того, в пользовательской учетной записи должно быть разрешение на установление соединения с сервером посредством служб терминалов или удаленного рабочего стола.

После того, как преодолены все вышеперечисленные препятствия, можно с: легкостью управлять ISA Server с помощью служб терм и налов/удале нного рабочего стола. Установите соединение с сервером так же, как устанавливается соединение с сервером терминалов/сервером удаленного рабочего стола, и рабочий стол сервера появится на экране компьютера, позволяя выполнять любые административные задачи, как если бы вы работали за дисплеем самого сервера (рис. 2.23).

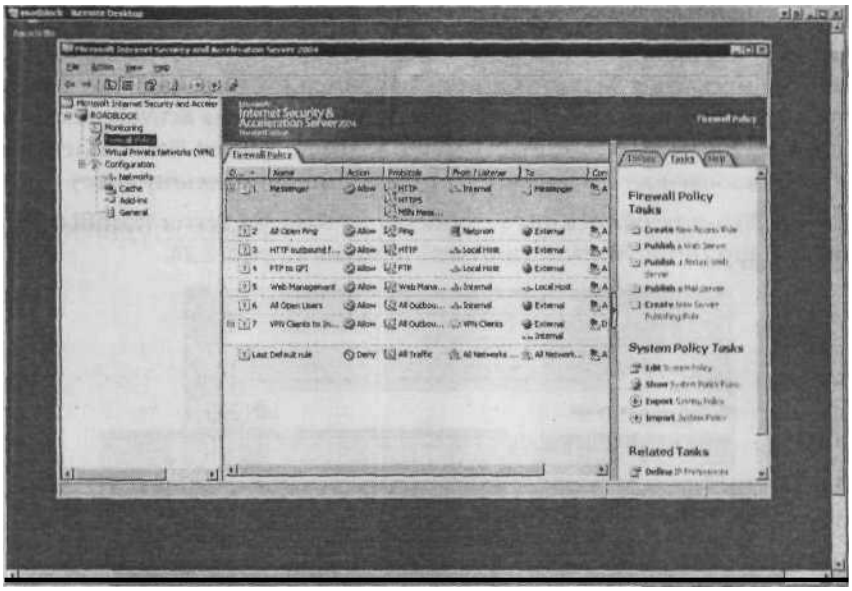


Рис. 2.23. С помощью служб терминалов или клиента RDC можно вывести рабочий стол ISA Server на экран компьютера

Так же как и при удаленном управлении с помощью консоли управления, возможно, потребуется изменить системную политику ISA Server, чтобы разрешить управление посредством служб терминалов, прежде чем можно будет воспользоваться этим методом удаленного управления. Процедура та же самая, только после того, как в правой панели консоли управления выбирается **Edit System Policy** (Редактировать системную политику) (на левой панели при этом выделен раздел **Firewall Policy** (Политика брандмауэра), нужно щелкнуть на **Terminal Server** (Сервер терминала) в разделе **Remote Management** (Удаленное управление). Затем на вкладке **From** (От) нажмите кнопку **Add** (Добавить) для того, чтобы добавить сети, подмножества сетей, компьютеры, подмножества компьютеров, диапазоны IP-адресов или подсети. Это те самые компьютеры, которым будет разрешено управление ISA Server посредством служб терминалов/удаленного рабочего стола.

Графические Web-интерфейсы удаленного управления от сторонних производителей

Сторонние производители, например партнеры корпорации Microsoft, которые создают устройства на базе ISA Server, предлагают пользователям Web-интерфейсы, которые можно использовать для управления ISA Server с любого компьютера из любой точки земного шара. При этом на клиентском компьютере не нужно устанавливать никакое программное обеспечение, а на ISA Server не нужна никакая

дополнительная настройка. Однако, возможно, придется воспользоваться браузером Internet Explorer и/или изменить настройки безопасности браузера, чтобы разрешить применение Web-интерфейса, например для того, чтобы Web-интерфейс работал корректно, придется включить средства управления ActiveX. Также, возможно, придется добавить Web-сайт ISA Server к группе Trusted Sites (Надежные узлы) или к зоне безопасности локальной сети (Local Intranet security zone).

Пример Web-интерфейса для устройства на базе ISA Server RoadBLOCK производства RimApp (http://www.rimapp.com) показан на рис. **2.24.**

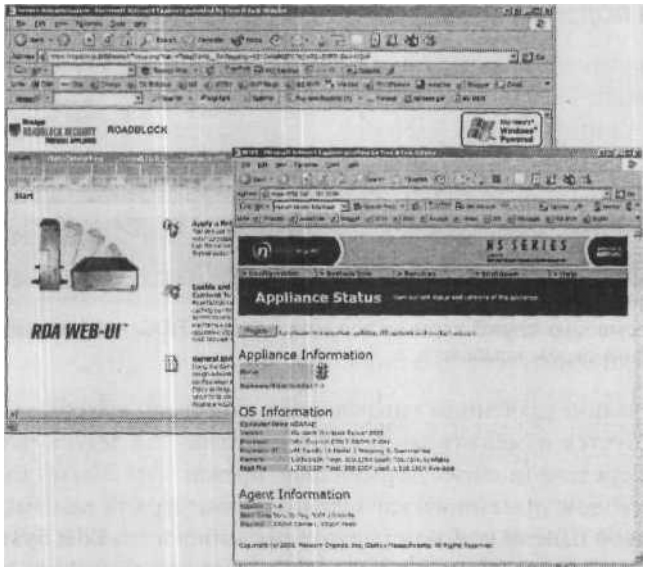


Рис. 2.24. Сторонние производители предлагают Web-интерфейсы для устройств-брандмауэров на базе ISA Server

Улучшенные функции брандмауэра

Улучшенная функциональность является главным приоритетом корпорации Microsoft н ISA Server 2004, наверное, **даже** еще большим, чем в ISA Server 2000. И хотя название его осталось тем же: «Internet Security *and* Acceleration Server», акцент при разработке и маркетинге был сделан в большей степени на функции обеспечения безопасности и в меньшей — на функции ускорения. ISA Server 2004 был разработан с расчетом на конкуренцию с популярными брандмауэрами типа Checkpoint и PIX, которые не включают в комплект поставки функции кэширования. Поэтому естественно, что многие усовершенствования коснулись функций безопасности и брандмауэра ISA. Они включают в себя:

- улучшенную поддержку протоколов;
- улучшенную проверку подлинности;
- упрощенный доступ к популярным службам, таким как OWA и FTP;
- расширенные возможности определения сетевых объектов;
- улучшенную функциональность правил брандмауэра;
- улучшения публикации серверов и Web-публикации.

В следующих разделах вкратце будет рассмотрен каждый из этих пунктов.

Улучшенная поддержка протоколов

ISA Server 2004 предоставляет возможность контроля доступа и использования любого протокола, включая протоколы уровня IP (уровня 3), например протокола ICMP (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет). Это позволяет использовать такие утилиты, как ping и tracert, а также устанавливать VPN-подключения с помощью протокола PPTP. Также можно разрешить прохождение через ISA Server IPSec-трафика, а в ISA Server 2000 такой трафик контролировать было невозможно.

На транспортном уровне (уровень 4) в ISA Server 2004 также добавлена новая поддержка перенаправления портов и улучшенная поддержка протокола FTP. В ISA Server 2004 соединение, установленное с одним портом, может быть перенаправлено на другой номер порта, а FTP-серверы могут быть опубликованы на различных номерах портов без необходимости каких-либо конкретных изменений конфигурации клиента — нужно просто создать правило публикации FTP-сервера.

Потоковые данные и голосовые/видео приложения часто требуют от брандмауэра возможности управления *«сложными протоколами»,* для работы которых необходима установка нескольких соединений. В ISA Server 2000 есть возможность работы со сложными протоколами, но для этого необходимо уметь разрабатывать сложные сценарии для создания определения протоколов, требующих нескольких исходящих начальных соединений. ISA Server 2004 предоставляет возможность легко создавать определения протоколов с помощью мастера New Protocol Wizard. Эти определения можно создавать «на лету» при создании правила доступа, или же можно создать новый протокол в узле **Firewall Policy** (Политика брандмауэра), выбрав **Protocols** (Протоколы) на вкладке **Toolbox** (Инструментарий) на правой панели и щелкнув **New** (Новый) (рис. 2.25).

Кроме того, с помощью ISA Server 2004 можно контролировать номера портов источника и адресата для любого протокола, для которого создается правило брандмауэра. Это позволяет администратору ISA Server 2004 жестко контролировать то, какие именно пакеты проходят через брандмауэр.

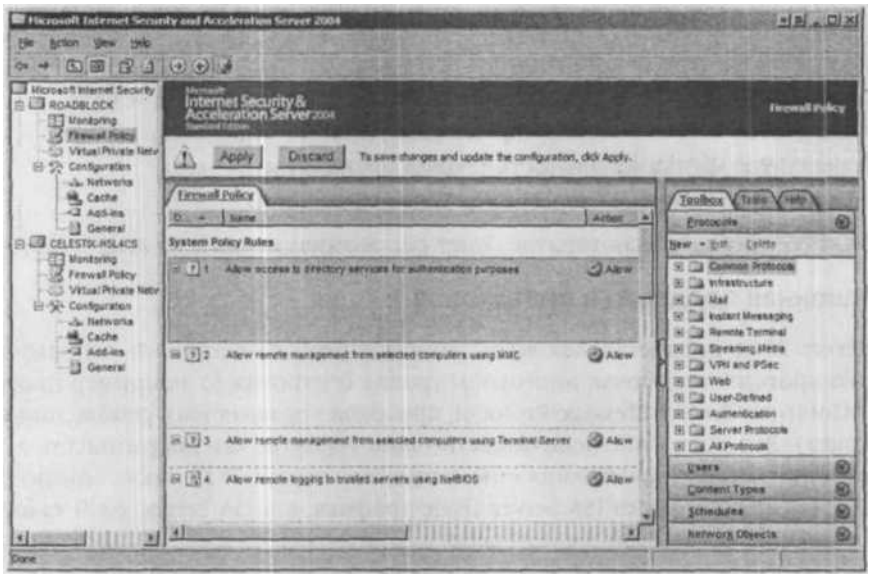


Рис. 2.25. ISA Server 2004 дает возможность легко создавать определения новых протоколов

Улучшенная проверка подлинности

Также в ISA Server 2004 были улучшены процедуры проверки подлинности. Проверка подлинности пользователей может проводиться с помощью **встроенной** службы проверки подлинности Windows или службы RADIUS или других пространств имен. Можете применить **правила** к пользователям **или** группам пользователей в любом пространстве имен. Используя SDK (Software Development Kit, набор инструментальных средств разработки программного обеспечения), сторонние разработчики могут **расширить** эти типы встроенной проверки подлинности, предоставляя дополнительные механизмы проверки подлинности.

Была решена наиболее распространенная проблема проверки подлинности в ISA Server 2000: для того чтобы клиенты брандмауэра могли воспользоваться Web-кэшированием в ISA Server 2000, редиректор должен был перенаправлять запросы к службе Web-прокси. В процессе **удалялись** верительные данные пользователей, а впоследствии, если эти данные вновь требовались, то запрос не выполнялся. В ISA Server 2004 эта проблема была решена: теперь клиентам брандмауэра разрешен доступ к Web-кэшу через HTTP-фил ьтр, при этом дополнительная проверка подлинности **службой** Web-прокси больше не требуется.

В ISA Server 2000 также **возникали** некоторые проблемы с проверкой подлинности на Web-сайте Hotmail. Для их устранения нужно было разрешить прямой доступ *к* сайту. Улучшенный HTTP-фильтр в ISA Server 2004 решил и эту проблему.

Теперь все пользователи могут получить доступ к Hotmail благодаря легко конфигурируемому правилу брандмауэра; дополнительные настройки клиента или брандмауэра не нужны.

Упрощенный доступ к популярным службам 0WA и FTP

Теперь гораздо проще настроить службу OWA на работу с ISA Server 2004 благодаря мастеру OWA-публикаций — OWA Publishing Wizard. Виртуальные частные сети с помощью протокола SSL (Secure Sockets Layer) предоставляют удаленный доступ посредством безопасных соединений (без привлечения клиентов).

Мастер OWA Publishing Wizard в ISA Server 2004 поможет настроить правило брандмауэра, создающее виртуальную частную сеть OWA SSL **с** сервером Exchange. Все объекты сети можно создавать «в процессе», и при этом не требуется выходить из мастера, для того чтобы создать политику. Кроме того, мастер OWA Publishing Wizard теперь поддерживает службы Outlook Mobile Access и ActiveSync, которые невозможно было настроить в мастере ISA Server 2000. Настройка Web-приемника не была встроена в мастер ISA Server 2000, но она имеется в ISA Server 2004. Появилось больше возможностей настройки Web-приемника; в ISA Server 2000 приходилось глобально задавать свойства Web-прием ника. То есть, если активировался HTTP-приемник, то он активировался для всех Web-приемников. В ISA Server 2004 можно индивидуально задать свойства для каждого Web-приемника.

В ISA Server 2000 было сложно настроить исходящий доступ к FTP-серверам, осуществляющим прослушивание на нестандартных портах, для этого был необходим клиент брандмауэра. В ISA Server 2004 есть возможность получать доступ к FTP-серверам в Интернете, которые прослушивают на переменных номерах портов, при этом не требуется никакая специальная конфигурация клиента или брандмауэра ISA Server 2004. Также в ISA Server 2000 существовала проблема с публикацией FTP-сервера на переменных номерах портов, но в ISA Server 2004 эта задача легко решается: нужно всего лишь создать правило публикации FTP-сервера. Как это сделать, будет рассказано в главе 8.

Инструменты и ловушки

Принцип работы защищенных сокетов

Компания Netscape изначально разработала протокол SSL как протокол системы защиты, предназначенный для использования при передаче информации посредством Web-браузера. Компания Netscape лицензировала шифрование по схеме открытого ключа RSA. В протоколе SSL используется шифрование по схеме открытого ключа (асимметричное шифрование), с помощью которого **выполняется** проверка подлинности и защита целостности данных в сообщениях, которыми обмениваются два компьютера. Вот упрощенная схема работы этого протокола:

(см. след. стр.)

1. Клиентский компьютер отправляет запрос на установление безопасного соединения с сервером.
2. Сервер отправляет свой аутентификационный сертификат и открытый ключ клиенту.
3. Клиент проверяет достоверность сертификата и, если она подтверждает ся, отправляет серверу случайным образом сгенерированный ключ шиф рования, зашифрованный с помощью открытого ключа, полученного от сервера.
4. Сервер расшифровывает ключ шифрования, используя открытый ключ, соответствующий открытому ключу, с помощью которого клиент его за шифровал.
5. Клиент и сервер теперь могут обмениваться данными в защищенном ре жиме, используя созданный в процессе сеанса связи симметричный ключ шифрования.

Расширенные возможности определения сетевых объектов

В ISA Server 2000 сетевые объекты определялись на основе IP-адресов (наборов адресов клиентов) или на основе полностью заданных имен доменов (подмножеств адресатов). В ISA Server 2004 имеется большая свобода в определении сетевых объектов. Можете определять их, основываясь на следующих категориях:

- **Networks** (Сети) в данном контексте сеть определяется как диапазон IP-адресов;
- **Network sets** (Подмножества сетей);
- **Computers** (Компьютеры) Компьютер в данном случае определяется как но ситель отдельного IP-адреса. Для того чтобы применить правило к компьюте рам с несколькими сетевыми адаптерами или с несколькими IP-адресами, при своенными одному сетевому адаптеру, нужно использовать подмножество ком пьютеров, диапазон адресов или даже подсеть;
- **Address ranges** (Диапазоны адресов) Имеются в виду IP-адреса;
- **Subnets** (Подсети) Подсеть также определяется как диапазон IP-адресов; в этом случае адреса составляют подсеть;
- **Computer sets** (Подмножества компьютеров) Подмножество сетей — это груп па сетей, точно так же подмножество компьютеров — это группа компьютеров (более точно сказать: группа непоследовательных IP-адресов);
- **URL set** (Подмножество URL) Это группа унифицированных указателей инфор мационных ресурсов (Web-адресов);
- **Domain name set** (Подмножество имен доменов);
- **Web-listener** (Web-приемник) Это программный структурный компонент, ко торый определяет, какие IP-адреса и порты будут использоваться для обработ ки Web-запросов.

Эти сетевые объекты определяют источник и адресат для правил брандмауэра. При создании правила всегда указываются объекты источника и адресата, к которым будет применяться это правило. Полный список категорий с подкатегориями представлен на рис. 2.26.

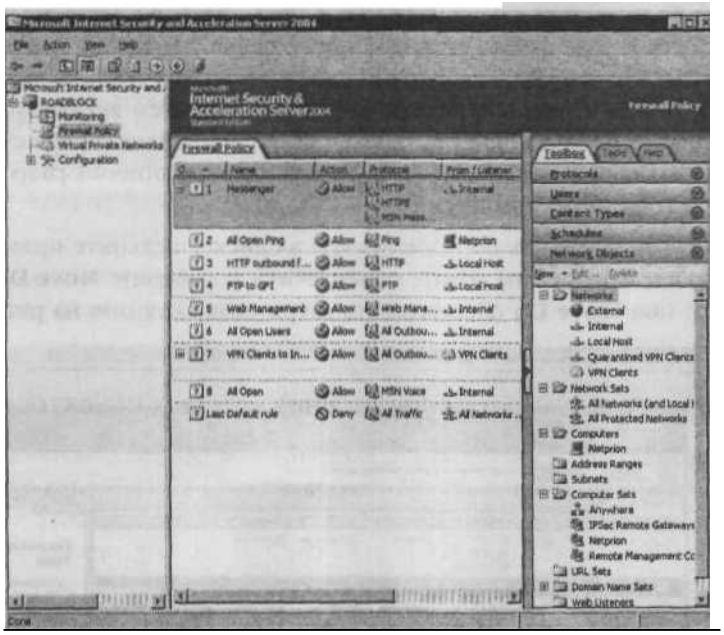


Рис. 2.26. ISA Server 2004 — обеспечение большей свободы в определении сетевых объектов

Методы работы с сетевыми объектами обсуждаются в главе 4.

Улучшенная функциональность правил брандмауэра

Ключевой компонент контроля доступа через брандмауэр ISA — политика брандмауэра, которая состоит из правил системной политики, правил публикации *и* правил доступа (все вместе они называются правилами политики брандмауэра). ISA Server 2004 включает в себя новый набор мастеров работы с правилами, которые как никогда облегчают создание политик доступа. В ISA Server 2000 политики исходящего доступа требовали наличия фильтров IP-пакетов, правил сайта, содержимого и правил протокола. В ISA Server 2004 политики доступа можно создавать с помощью усовершенствованного мастера правил брандмауэра Firewall Rule Wizard, который позволяет сходу конфигурировать любой элемент политики. Нет нужды выходить из мастера работы с правилом для того, чтобы создать новый сетевой объект, как это приходилось делать при работе с ISA Server 2000. Любой сетевой объект или отношение, необходимое для правила, можно создать непосредственно в новом мастере.

Контроль доступа в ISA Server 2000 основывался на правилах **Allow rule** (Разрешающее правило) и Deny **rule** (Запрещающее правило). Обычно сначала обрабатывались запрещающие правила, а затем разрешающие правила. Правила системной политики обрабатываются раньше, чем правила, заданные пользователем. Теперь правила брандмауэра представляют собой упорядоченный список, при этом параметры соединения сначала сравниваются с правилом, идущим первым в списке. ISA Server 2004 перемещается вниз по списку правил до тех пор, пока не найдет правило, соответствующее параметрам соединения, а затем активирует политику соответствующего правила. Такой подход к политике брандмауэра существенно упрощает локализацию неисправностей и определение причин разрешения или запрещения конкретного соединения.

Для того чтобы изменить порядок правил в списке, щелкните правой кнопкой мыши на правиле, которое вы хотите переместить, и выберите **Move Down** (Переместить вниз) или **Move Up** (Переместить вверх), как показано на рис. 2.27.

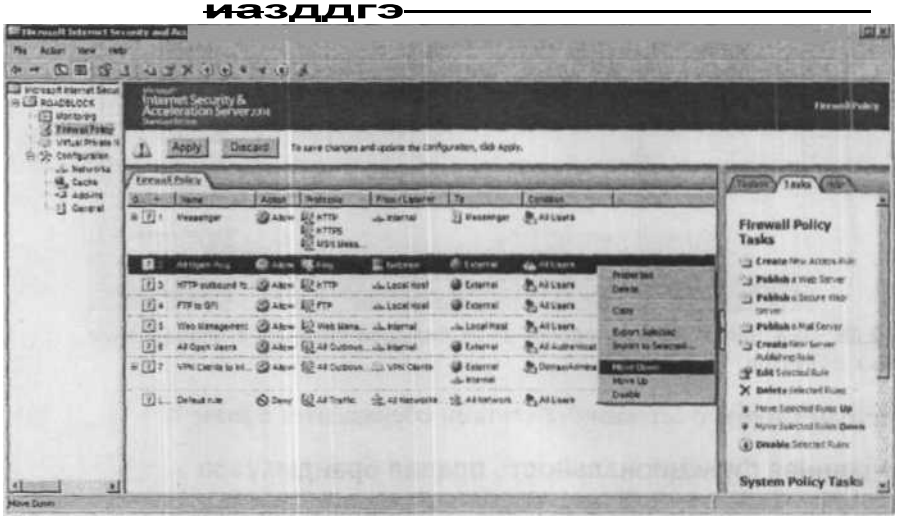


РИС. 2.27. Изменение порядка обработки правил доступа и правил публикации

ПРИМЕЧАНИЕ Можете изменить порядок определенных пользователем правил (правил публикации и доступа), но нельзя изменить порядок правил системной политики.

В ISA Server 2000 была возможность указывать, к каким сайтам и протоколам мог получить доступ пользователь, но нельзя было разрешить пользователю получить доступ к конкретному сайту с помощью определенного протокола или использовать конкретный протокол для получения доступа к определенному сайту. Расширенные правила брандмауэра в ISA Server 2004 позволяют определять источник *и* адресата для каждого отдельного протокола, к которым разрешен доступ пользо-

вателя или группы. Это повышает гибкость при осуществлении контроля входящего и исходящего доступа через брандмауэр ISA.

Правила системной политики подробно обсуждаются в главе 6. Как создавать и работать с заданными пользователем правилами брандмауэра рассказывается в главах 7 и 8.

Усовершенствованные функции публикации серверов и Web-публикации

В ISA **Server** 2004 были улучшены функции публикации серверов и Web-публикации. В ISA Server 2000 правила публикации серверов перенаправляли входящие соединения на **опубликованный** сервер на тот же самый порт, с которого был получен исходный запрос. В ISA Server 2004 появилась возможность принимать соединение на определенном номере порта, а затем перенаправлять запрос на другой номер порта на опубликованном сервере.

В ISA Server 2004 можно разместить серверы под защитой брандмауэра либо в корпоративной сети, либо в сети периметра и публиковать их службы в защищенном режиме. В отличие от ISA Server 2000, в ISA Server 2004 есть два отдельных мастера Web-публикации (Web Publishing Wizard). Первый предназначен для публикации защищенного Web-сервера, что позволяет удаленным пользователям получать доступ к Web-серверу по протоколу SSL (рис. 2.28).

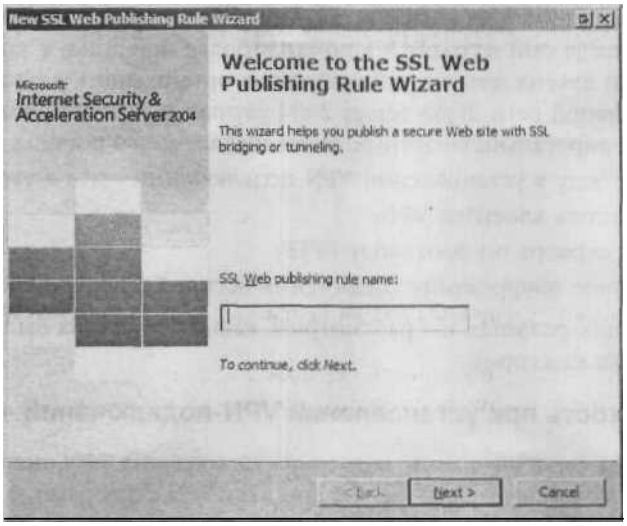


Рис. 2.28. Мастер ISA Server 2004 для публикации Web-сайтов по протоколу SSL

Также появился новый мастер публикации почтового сервера Mail Server Publishing Wizard, который позволяет вам публиковать любой почтовый сервер, работающий

с протоколами ШАР, POP3, SMTP или RPC, или сервер новостей на базе протокола NNTP (Network News Transfer Protocol, сетевой протокол передачи новостей), кроме того, можно публиковать службы Outlook Web Access, Outlook Mobile Access или Exchange ActiveSync.

Улучшенные мастера Web Publishing Wizard позволяют публиковать Web-сайты легко и быстро. Например, настройка Web-приемника не входила в мастера в ISA Server 2000, а в ISA Server 2004 она предусмотрена. Также появилось гораздо больше возможностей настройки Web-приемника; в ISA Server 2004 нужно было глобально задавать свойства для Web-приемника. То есть при активации HTTP-приемника, он активировался для всех Web-приемников. В ISA Server 2004 можно устанавливать свойства отдельно для каждого Web-приемника.

В ISA Server 2000, прежде чем создавать правило публикации сервера или правило Web-публикации, необходимо было создать ряд новых элементов политики, которые могли потребоваться в правиле. В ISA Server 2004 элементы политики можно создавать по ходу работы в мастере Rule Wizard (Мастер правил).

Улучшенные функции создания виртуальных частных сетей и удаленного доступа

Создание виртуальных частных сетей приобретает для компаний все большее значение вследствие стремительного роста числа сотрудников, осуществляющих дистанционный доступ, исполнителей и сотрудников отдела продаж, которым нужен доступ к сети, когда они находятся *в* командировке или дома, а также из-за наличия партнеров и других лиц, не работающих в организации, которым нужен доступ к корпоративной сети. В ISA Server 2004 улучшена и расширена функциональность создания виртуальных частных сетей и удаленного доступа, включая:

- большую свободу в установлении VPN-подключений «узел-в-узел»;
- лучший контроль клиентов VPN;
- публикацию сервера по протоколу PPTP;
- принудительное шифрование соединений Secure Exchange RPC.

В последующих разделах мы рассмотрим, какие улучшения были предприняты в каждой из этих категорий.

Большая гибкость при установлении VPN-подключений «узел-в-узел»

В ISA Server 2004 были улучшены возможности создания VPN, позволяющие устанавливать подключения «узел-в-узел» с другими VPN-серверами, с помощью протокола IPSec в туннельном режиме. Это повышает уровень способности к взаимодействию виртуальных частных сетей по сравнению с ISA Server 2000. Это означает, что можно установить ISA Server 2004 в филиале и установить соединение «узел-в-узел» в туннельном режиме IPSec между сетью филиала и сетью главного офиса, даже если в главном офисе используется граничный брандмауэр сторонних про-

изводителей типа Cisco PIX, Check Point или любой другой брандмауэр, который поддерживает создание виртуальных частных сетей по протоколу IPSec. В ISA Server 2000 для соединения сетей через Интернет посредством VPN-подключения «узел-в-узел» можно было использовать только VPN-протоколы PPTP и L2TP/IPSec.

В ISA Server 2000 сети, связь между которыми осуществлялась через подключение «узел-в-узел», считались надежными сетями; поэтому политика брандмауэра не применялась к сообщениям, проходившим через этот канал. В ISA Server 2004 ко всем сообщениям, проходящим через VPN-подключение «узел-в-узел», применяется фильтрация и проверка с отслеживанием соединений. Это обеспечивает возможность контроля, доступа к ресурсам конкретных хостов или сетей на другой стороне канала. Политики доступа для пользователей/групп можно использовать для того, чтобы контролировать использование ресурсов именно по этому подключению.

Улучшенный контроль VPN-клиентов

В отличие от ISA Server 2000 политика брандмауэра ISA Server 2004 применяется ко *всем* сетевым интерфейсам, включая интерфейсы VPN. Для обеспечения лучшей безопасности и более строгого контроля можно ограничить VPN-клиенты выбранной группой серверов и протоколов внутренней сети. Например, можно разрешить полный клиентский доступ по интерфейсу Outlook MAPI к серверу Exchange внутренней сети, но не предоставлять этим пользователям доступ ко всем прочим серверам или протоколам сети. В этом случае можно настроить правила брандмауэра ISA Server 2004 так, чтобы ограничить доступ пользователей VPN только клиентскими службами MAPI сервера Exchange.

VPN-клиенты настраиваются как отдельная сетевая зона. Это означает, что можно создавать отдельные политики для VPN-клиентов. Набор правил брандмауэра выборочно проверяет запросы от VPN-клиентов, осуществляя фильтрацию с отслеживанием соединений и проверку этих запросов и динамически открывая соединения, основываясь на политике доступа.

В ISA Server 2000 только VPN-клиенты, настроенные как клиенты брандмауэра, могли получать доступ к Интернету через свой подключенный VPN-сервер ISA Server 2000. В ISA Server 2004 улучшена поддержка VPN-клиентов: теперь клиентам SecureNAT разрешается получать доступ к Интернету, причем нет необходимости устанавливать программное обеспечение клиента брандмауэра на **клиентский** компьютер. Можно также усилить безопасность корпоративной сети, назначив политику брандмауэра для пользователей/групп на клиентах SecureNAT, которые соединены посредством VPN.

Публикация сервера с помощью протокола PPTP

Также были улучшены возможности публикации VPN-серверов. В ISA Server 2000 можно было публиковать только L2TP/IPSec NAT-T VPN-серверы. В ISA Server 2004 можно публиковать VPN-серверы, расположенные под защитой брандмауэра ISA Server 2004, с помощью протокола PPTP. PPTP-фильтр уровня приложений в ISA Server 2004 осуществляет комплексный контроль соединения. Кроме того, можно легко опубликовать VPN-сервер Windows Server 2003 NAT-T L2TP/IPSec с использованием публикации серверов в ISA Server 2004. ISA Server 2004 также поддерживает совместимые с NAT-T VPN-серверы на базе IPSec, находящиеся под защитой брандмауэра.

Принудительное шифрование соединений Secure Exchange RPC

Политика RPC может быть назначена на брандмауэре ISA Server 2004 для того, чтобы исключить обмен незашифрованными сообщениями между удаленными клиентами Outlook MAPI, соединенными через Интернет. Это усиливает безопасность сети и сервера Exchange благодаря тому, что не происходит обмена верительными данными пользователей и данными в незашифрованном формате.

Расширенная и улучшенная функциональность Web-кэша и Web-прокси

Важно помнить, что несмотря на акцент на безопасность, ISA Server 2004 является больше чем просто брандмауэром — это ко всему прочему полнофункциональный сервер кэширования. Функции Web-кэша и Web-прокси претерпели в ISA Server 2004 некоторые улучшения, включая:

- улучшенный мастер Cache Rule Wizard (Мастер правил кэширования);
- большая гибкость при кэшировании SSL-наполнения;
- установление соответствий маршрутов для правил Web-публикации;
- улучшенная функция загрузки содержимого по расписанию.

В следующих разделах подробно обсуждается каждый из этих пунктов

Улучшенный мастер Cache Rule Wizard

В ISA Server 2000 правила кэширования создавались с помощью удобного интерфейса мастера. Однако в ISA Server 2004 мастер Cache Rule Wizard претерпел некоторые изменения. С одной стороны, теперь его легко найти. В интерфейсе ISA Server 2000 правила кэширования задавались с помощью мастера New Routing Rule Wizard (Мастер нового правила маршрутизации) (рис. 2.29), который (что было неочевидно) располагался в узле Network Configuration (Настройки сети) на левой панели консоли (а не в узле Cache Configuration (Настройки кэша), где его естественнее было бы искать).

Рис. 2.29. Правила кэширования в ISA Server 2000

В ISA Server 2004 правила кэширования создаются в узле **Configuraiton/Cache** (именно здесь его и будет искать большинство пользователей) нажатием правой кнопкой мыши узла **Cache** *(Кэш)* и выбором New (Новый), а затем **Cache** Rule (Правило кэширования), как показано на рис. 2.30, или просто щелчком **Create a Cache Rule** (Создать правило кэширования) на правой панели Tasks, как показано на рис. 2.30.

Кроме того, теперь обеспечивается большая гибкость и ясность при выборе сетевых объектов, к которым будет применяться правило. В ISA Server 2000 можно было выбрать всех адресатов, всех внешних адресатов, всех внутренних адресатов, конкретное подмножество адресатов или всех адресатов, кроме указанной группы.

В ISA Server 2004 можно применить правило кэширования к любому объекту из списка сетевых объектов, который обсуждался ранее: сети целиком, подмножества сетей, отдельные компьютеры, диапазоны адресов, подсети, подмножества компьютеров, подмножества имен доменов или подмножества URL

В мастере ISA Server 2004 можно более точно задать условия, при которых содержимое, к которому обращаются пользователи, сохраняется в кэше. Кроме того, что можно установить сохранение содержимого в кэше в том случае, если заголовки источника или запроса указывают на необходимость кэширования, можно также кэшировать динамическое содержимое, кэшировать содержимое для последующего использования в режиме офф-лайн и кэшировать содержимое, которое требует проверки подлинности пользователя на основе правил.

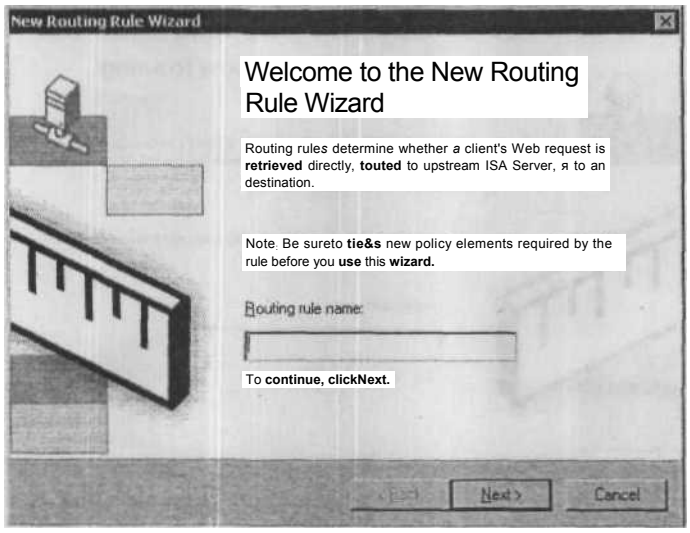


Рис. 2.30. Создание правила кэширования в ISA Server 2004

Подробнее мастер Cache Rule Wizard будет рассмотрен в главе 11.

Большая гибкость при кэшировании SSL-контента

В ISA Server 2000 у пользователя не было возможности *не* кэшировать SSL-контент. Это представляло определенную проблему, поскольку SSL является безопасным наполнением и из соображений безопасности нежелательно сохранять его в кэше.

В ISA Server 2004 эта проблема решена. Когда создается правило кэширования, SSL-контент кэшируется по умолчанию, но можно отключить его кэширование, установив флажок на странице **Cache Advanced Configuration** (Расширенные настройки кэширования). Или же после того, как было создано правило кэширования, можно настроить его так, чтобы SSL-контент не кэшировался, щелкнув правой кнопкой мыши на правиле, выбрав **Properties** (Свойства) и открыв вкладку **Advanced** (Дополнительно), а затем сняв флажок, как показано на рис. 2.31.

Возможность управления кэшированием SSL-ответов является приятным дополнением к возможностям ISA Server 2004.

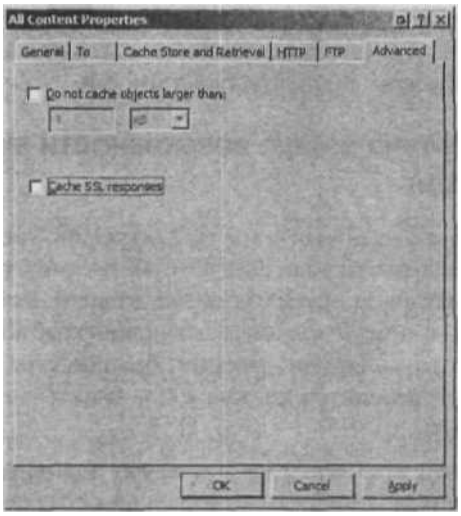


Рис. 2.31. ISA Server 2004 — можно выбрать **режим** *не* кэширования **SSL-контента**

Отображение маршрутов для правил Web-публикации

Правила Web-публикации в ISA Server 2000 требовали, чтобы маршрут, который пользователь включал в исходный запрос, был таким же, как на опубликованном Web-сервере. В ISA Server 2004 существенно улучшена гибкость Web-публикаций: теперь вы можете перенаправлять маршрут, отправленный пользователем на брандмауэр, на любой маршрут по вашему выбору на опубликованном Web-сервере.

При настройке отображения маршрута в ISA Server 2004, ISA заменяет маршрут, который содержится *в* запросе, на маршрут, на который установлено отображение.

Отображение маршрутов настраивается путем редактирования правила Web-публикации после того, как это правило было создано. В диалоговом окне Properties (Свойства) правила публикации выберите вкладку Paths (Маршрут) и добавьте маршрут, на который необходимо отображать запросы, в формате /path/*.

Подробнее об отображении маршрутов будет рассказано при обсуждении создания правил публикации в главе 8.

Улучшенная функция загрузки содержимого по расписанию

Функция загрузки содержимого по расписанию также была улучшена в ISA Server 2004. В ISA Server 2000 нельзя было задать расписание загрузки содержимого с сайтов, требующих проверки подлинности пользователя. Это ограничивало возможность автоматизации процесса загрузки содержимого.

В ISA Server 2004 можно указать учетную запись, которая будет использоваться для проверки подлинности, тем самым можно задать расписание загрузки содержимого с сайтов, требующих проверки подлинности.

Расширенные и улучшенные возможности мониторинга и создания отчетов

Функции мониторинга и создания отчетов в ISA Server 2000 не удовлетворяли многих пользователей (справедливости ради следует отметить, что сходные жалобы поступали также на брандмауэры и других производителей). Разумеется, создание «бумажной копии» (или в данном случае цифровой копии) работы брандмауэра не столь впечатляюще, как некоторые другие функции брандмауэра, но документирование является существенным элементом обеспечения защиты сети и ее клиентов к современном деловом мире.

Корпорация Microsoft прислушалась к мнению пользователей и внесла огромное количество улучшений и добавлений в функции создания журналов, отчетов и мониторинга в ISA Server 2004, включая следующие:

- мониторинг записей журнала в режиме реального времени;
- мониторинг и фильтрация сеансов брандмауэра в режиме реального времени;
- встроенный механизм создания запросов к журналам;
- верификаторы соединений;
- возможность настройки отчетов;
- возможность публикации отчетов;
- оповещение по электронной почте об отчетных заданиях;
- возможность настройки времени создания сводки журнала;
- улучшенные функции записи журналов в базу данных SQL;
- возможность записи журналов в базу данных MSDE.

Мы вкратце рассмотрим каждый из этих пунктов в следующих разделах.

Мониторинг записей журнала в режиме реального времени

В ISA Server 2004 можно просматривать журналы брандмауэра, Web-прокси и средства контроля сообщений SMTP в режиме реального времени. Консоль управления отображает записи журнала но мере их внесения в файл журнала брандмауэра (рис. 2.32). Это отличается от возможностей ISA Server 2000, где приходилось обращаться к самому файлу журнала (по умолчанию он создавался ежедневно) или создавать отчет для того, чтобы просмотреть информацию в журнале.

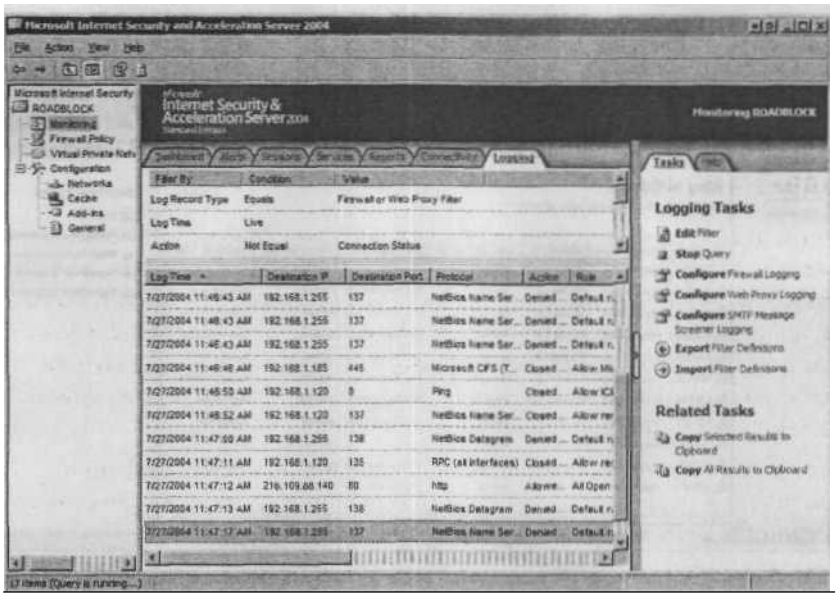


Рис. 2.32. Мониторинг журналов в режиме реального времени в ISA Server 2004

Мониторинг и фильтрация сеансов брандмауэра в режиме реального времени

В ISA Server 2004 есть возможность просматривать все активные соединения с брандмауэром. Используя вкладку Sessions (Сеансы) консоли Monitoring (Мониторинг), как показано на рис. 2.33, можно отсортировать или отключить отдельные сеансы или группы сеансов. С помощью встроенной функции фильтрации сеансов можно также отфильтровать записи в интерфейсе Sessions (Сеансы) с тем, чтобы сосредоточиться на конкретных интересующих вас сеансах.

Как показано на рис. 2.33, можно видеть тип сеанса (выполняет ли пользователь соединение через клиент брандмауэра, клиент SecureNAT или клиент Web-прокси), IP-адрес пользователя, имя пользователя и имя клиентского компьютера и даже используемое приложение.

Это полезно при выявлении неисправностей и определении того, применяются ли пользователями неавторизованные или проблемные приложения.

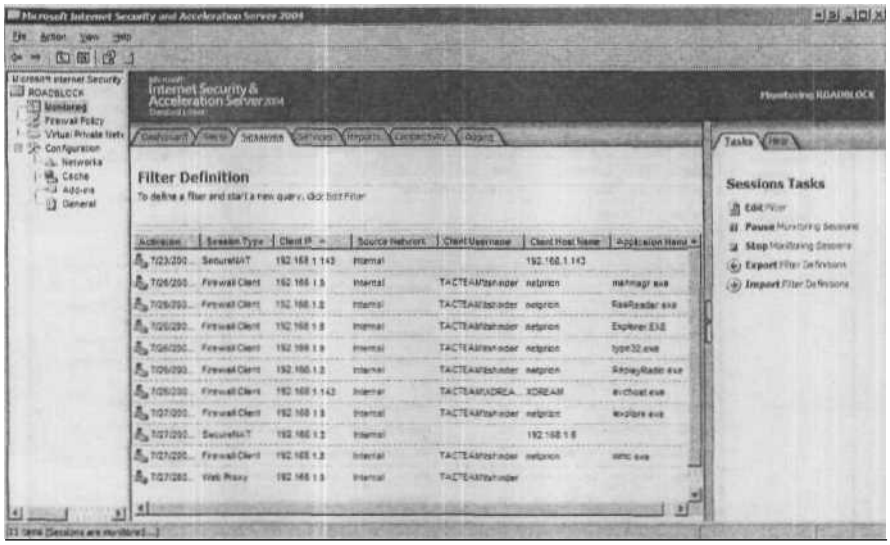


Рис. 2.33. Функция сеансов — просмотр всех активных соединений через брандмауэр

Встроенный механизм создания запросов к журналам

В ISA Server 2004 можно создавать запросы к файлам журналов с помощью встроенного механизма создания запросов к журналам. Можно запрашивать в журналах информацию, содержащуюся в любом поле, записанном в файлах журналов. Результаты запроса отображаются на консоли просмотра журнала ISA Server 2004 и их можно скопировать в буфер обмена и вставить в другое приложение для более внимательного анализа.

Можно настроить фильтры так, чтобы ограничить результаты запроса. Например, можно ограничить область запроса конкретным промежутком времени или указать, что в отчете должны использоваться данные в режиме реального времени. Эту настройку выполнить просто (рис. 2.34).

ПРИМЕЧАНИЕ Средство просмотра журнала можно использовать для просмотра информации о журналах брандмауэра и Web-прокси, но для просмотра журнала средства контроля сообщений SMTP оно не подходит.

Помимо времени создания журнала, можно выполнять фильтрацию по различным критериям, включая (но не ограничиваясь только этим) IP-адреса клиента и адресата, имя пользователя, протокол, имя сервера, службу или URL

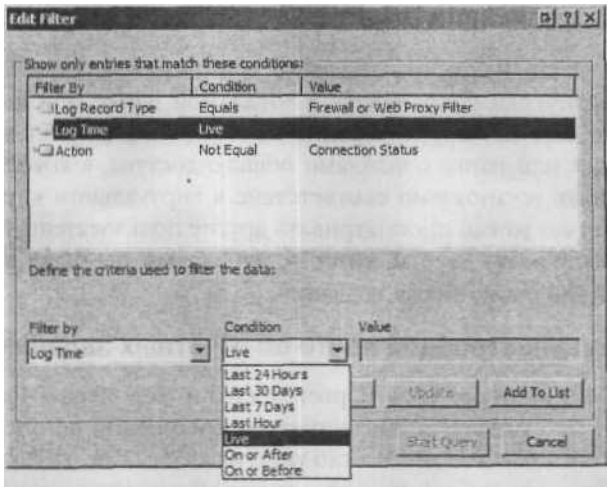


Рис. 2.34. Настройка фильтров для ограничения результатов запроса

Верификаторы соединений

В ISA Server 2004 есть возможность верификации соединений путем регулярного мониторинга соединений с конкретным компьютером или URL с компьютера ISA Server 2004 с помощью верификаторов соединений (Connection Verifiers) на вкладке **Connectivity** (Соединения) консоли **Monitoring** (Мониторинг). Можно настроить, какой метод будет использоваться для определения соединений: ping, TCP соединение с портом или метод HTTPGET. Можно также выбрать, какие соединения будут отслеживаться, указав IP-адрес, имя компьютера или URL

Мастер верификации соединений Connectivity Verifier Wizard позволяет создать новые верификаторы соединений.

Улучшенные возможности настройки отчетов

В ISA Server 2000 был лишь ограниченный набор возможностей настройки отчетов, генерируемых брандмауэром. Однако в ISA Server 2004 включается расширенный набор функций настройки отчетов, который позволяет включать в отчеты брандмауэра больше информации.

Мастер создания новых отчетов New Report Wizard помогает настроить разовые отчеты, а мастер задания новых отчетов New Report Job Wizard позволяет вам настроить регулярные отчеты. В любом случае вы можете выбрать, какая информация будет включена в отчет, период времени, за который создается отчет, а также необходимость публикации отчета.

Возможность публикации отчетов

В ISA Server 2004 можно настроить отдельные отчеты или задания отчетов так, чтобы их копия автоматически сохранялась в локальной папке или в сетевой папке с файлами общего доступа. Опубликованные отчеты сохраняются в формате HTML, а локальной папке или папке с файлами общего доступа, в которой сохраняются отчеты, может быть установлено соответствие в виртуальном каталоге Web-сайта так, чтобы этот отчет могли просматривать другие пользователи. Кроме того можно вручную опубликовать отчеты, которые изначально не были настроены на автоматическую публикацию после создания.

Оповещение по электронной почте об отчетных заданиях

В ISA Server 2004 в мастерах New Report Wizard и New Report Job Wizard можно настроить отчет на отправку администратору сообщения по электронной почте после того, как отчет был создан. Можно указать сообщение, которое будет отправляться, и, если настроить публикацию отчета, можно автоматически включить ссылку на отчет в сообщение по электронной почте.

Возможность настройки времени создания сводки журнала

В ISA Server 2000 было жестко запрограммировано ежедневное создание сводок журналов в 12:30. Отчеты основывались на информации, содержащейся в сводках журналов, поэтому такая настройка ограничивала время суток, когда мог быть создан точный отчет. В ISA Server 2004 есть возможность легко настроить время создания сводок отчетов. Это, в свою очередь, дает большую свободу в определении времени суток, когда будут создаваться ваши отчеты.

По умолчанию по-прежнему установлено время 12:30, но его легко изменить-, щелкните на стрелках вверх и вниз, как показано на рис. 2.35.

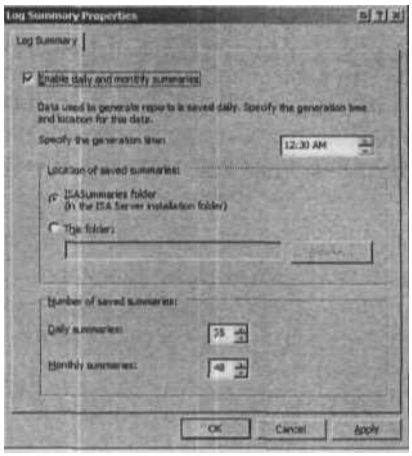


Рис. 2.35. В ISA Server 2004 можно изменить время создания сводок отчетов

Улучшенные функции записи журналов в базу данных SQL

В ISA Server 2004 можно записывать журналы в базу данных SQL, которая находится на другом компьютере внутренней сети. В ISA Server 2004 также были улучшены возможности записи журналов, что обеспечивает гораздо более высокую производительность по сравнению с записью журналов в базу данных SQL в ISA Server 2000.

Возможность записи журналов в базу данных MSDE

В ISA Server 2004 журналы можно сохранять в формате MSDE. Запись журнала в локальную базу данных увеличивает скорость и гибкость запросов. Данные, которые сохраняются в базе данных MSDE, можно просматривать с помощью средства просмотра журналов и сохранять в текстовом файле.

> СОВЕТ Если у вас имеется лицензия на SQL Server 2000, то можно использовать инструменты SQL (например, Enterprise Manager, инструменты запроса и т. п.) для просмотра базы данных и создания отчетов.

Новые функции

Помимо всех улучшенных функций, которые обсуждались в предыдущем разделе, корпорация Microsoft добавила в ISA Server 2004 ряд совершенно новых функций. В следующих разделах мы рассмотрим три наиболее важные новые функции:

- поддержка нескольких сетей;
- новые функции фильтрации на уровне приложения (Application Level Filtra tion, ALF);
- a контроль изолирования VPN-подключений.

Поддержка нескольких сетей

Большим ограничением ISA Server 2000 было то, что в нем не была предусмотрена поддержка нескольких сетей. Современные сложные сети требуют умения работать с несколькими сетями и определять отношения между ними. В ISA Server 2004 корпорация Microsoft представила многосетевую модель, которая подходит для соединенных между собой сетей, применяемых на многих предприятиях. Теперь можно создавать правила сетей и контролировать взаимодействие различных сетей друг с другом.

В ISA Server 2004 входит ряд встроенных определений сетей, включая следующие:

- внутренняя сеть (Internal network) — включает адреса первичной защищенной сети;
- внешняя сеть (External network) — включает адреса, которые не принадлежат никакой другой сети;
- сеть VPN-клиентов — включает адреса, присвоенные VPN-клиентам;
- сеть локального хоста (Local host network) — включает IP-адреса на ISA Server.

Можно сконфигурировать одну или несколько сетей, каждая из которых будет иметь определенные отношения с другими сетями. В ISA Server 2000 весь трафик проверялся в соответствии **с** таблицей LAT (Local Address Table, таблица локальных адресов), включавшей только диапазоны адресов внутренней сети, но в ISA Server 2004 были расширены функции брандмауэра и функции обеспечения безопасности: теперь проверяется и трафик между любыми сетями или сетевыми объектами.

Сетевые политики

Новые функции поддержки нескольких сетей в ISA Server 2004 облегчают задачу по обеспечению защиты сети от внутренних и внешних угроз безопасности путем ограничения взаимодействия между **клиентами** даже в пределах одной организации. Функции поддержки нескольких сетей могут работать со сложными схемами сети периметра (также называемой демилитаризованной зоной или экранированной подсетью), позволяя настраивать способы получения клиентами доступа к сети периметра в различных сетях. Политика доступа между сетями основывается на уникальной зоне безопасности, представленной каждой сетью.

Сетевые шаблоны

В ISA Server 2004 имеются сетевые шаблоны, которые можно использовать для того, чтобы **с** легкостью сконфигурировать политику брандмауэра по управлению трафиком между несколькими сетями. Эти шаблоны разработаны с учетом наиболее распространенных схем, включая:

- ISA Server в качестве граничного брандмауэра;
- сеть периметра (DMZ, демилитаризованная зона);
- ISA Server в качестве внешнего брандмауэра с использованием внутреннего бранд мауэра от сторонних производителей;
- ISA Server, применяемый между сетью периметра и внутренней сетью;
- сервер кэширования/Web-прокси с одним сетевым адаптером.

Способы конфигурирования нескольких сетей, создание правил сети и применение сетевых шаблонов рассматриваются в главе 4.

Новые функции фильтрации на уровне приложения (ALF)

Фильтрация на уровне приложения является одной из сильных сторон ISA Server 2004; *в* отличие от традиционных брандмауэров с фильтрацией пакетов ISA Server может выполнять глубинный анализ обмена сообщениями на уровне приложения, тем самым защищая сеть от многих современных типов угроз, которые происходят на этом уровне. **Функциональность** фильтрации на уровне приложения ISA Server 2000 была улучшена путем добавления следующих новых возможностей:

- возможность фильтрации передачи данных по протоколу HTTP на основе правил;
- м способность блокировать доступ ко всем исполняемым файлам;

- способность контролировать HTTP-загрузки по расширению файла;
- применение HTTP-фильтрации ко всем соединениям, устанавливаемым клиентами;
- контроль HTTP-доступа на базе подписей;
- контроль разрешенных HTTP-методов;
- способность форсировать использование безопасных Exchange RPC-соединений;
- контроль передачи данных по протоколу FTP на базе политик;
- преобразование ссылок.

В следующих разделах будут рассмотрены все эти пункты.

Фильтрация передачи данных по протоколу HTTP на основе правил

HTTP-политика в ISA Server 2004 позволяет брандмауэру выполнять глубинную проверку передачи данных по протоколу HTTP с отслеживанием соединений (фильтрацию потока данных приложения). Степень проверки можно настроить с помощью правил. Это означает, что можно настроить ограничения для входящего и исходящего HTTP-доступа. В ISA Server 2000 HTTP-фильтрация выполнялась глобально, с использованием устройства сканирования URL (URLscan), установленного с помощью Feature Pack 1 для ISA Server 2000.

Возможность блокировать доступ ко всем исполняемым файлам

Можно настроить HTTP-политику ISA Server 2004 так, чтобы блокировать все попытки установления соединения с исполняемыми файлами Windows независимо от расширения файла, используемого источником. Этим самым блокируются все ответы, в которых первое слово загруженного двоичного кода — MZ. Можно также блокировать доступ по расширению файла (см. следующий раздел).

ПРЕДУПРЕЖДЕНИЕ Блокировка всех исполняемых файлов Windows не подразумевает обязательную блокировку всех типов файлов, которые могут представлять возможную опасность. Например, файлы с расширениями pit и com не блокируются с помощью этого фильтра, потому что первые два байта их двоичных кодов — не MZ. Вы можете заблокировать эти и другие потенциально угрожающие безопасности типы файлов, настроив фильтры на блокировку по расширению файла.

ПРИМЕЧАНИЕ Первые два байта файла содержат его файловую подпись. Файловая подпись MZ, которая изначально использовалась для исполняемых файлов MS-DOS, является аббревиатурой имени программиста корпорации Microsoft Марка Збиковски (Mark Zbikowski).

Способность контролировать HTTP-загрузки по расширению файла

HTTP-политика в ISA Server 2004 позволяет с легкостью разрешить все расширения файлов, разрешить все расширения кроме конкретной группы расширений *и л и* блокировать все расширения за исключением указанной группы. Это дает большую свободу в осуществлении контроля над тем, какие типы файлов могут скачиьать пользователи, особенно если это делается на базе правил. Это означает, что можно применить блокировку определенных расширений к конкретным пользователям или группам.

Применение HTTP-фильтрации ко всем соединениям, устанавливаемым клиентами

В ISA Server 2000 была возможность блокировать содержимое (контент) для клиентов Web-прокси по HTTP- и FTP-соединениям в зависимости от MIME-типа (Multipurpose Internet Mail Extensions, многоцелевые расширения электронной поч"ы в Интернете) для НТГР или расширения файла для FTP. С помощью HTTP-политики в ISA Server 2004 можно контролировать HTTP-доступ для всех соединений, устанавливаемых клиентами ISA Server 2004, независимо от типа клиента. В коробочной версии ISA Server 2000 не было глубинной проверки исходящих соединений.

Контроль HTTP-доступа на базе подписей

Глубинная проверка передачи данных по протоколу HTTP в ISA Server 2004 также позволяет создавать HTTP-подписи, которые могут сравниваться с URL запроса, заголовками и телом запроса, а также с заголовками и телом ответа. Это дает возможность осуществлять очень жесткий контроль содержимого, к которому могут получить доступ внешние и внутренние пользователи через брандмауэр ISA Server 2004.

Подпись — это цепочка символов, в поисках которой ISA Server проверяет тело и заголовок запроса и тело и/или заголовок ответа. Если цепочка найдена, то данные будут заблокированы. Можно выполнять поиск текстовой или битовой цепочки. Блокировка, основанная на текстовых подписях, может выполняться, только гели HTTP-запросы и ответы имеют кодировку UTF-8.

Контроль разрешенных HTTP-методов

Можно контролировать то, какие HTTP-методы будут разрешены на брандмауэре, путем установки контроля доступа пользователей к различным методам. Например, можно ограничить HTTP-метод POST, запретив пользователям отправлять данные на Web-сайты с помощью этого метода. Допускается разрешить все методы, разрешить методы выборочно или заблокировать конкретные методы и разрешить все остальные.

ПРИМЕЧАНИЕ HTTP-методы представляют собой команды, которые указывают серверу, какие действия нужно предпринять в ответ на данный запрос. Они также иногда называются HTTP-глаголами (HTTP-verbs), потому что состоят из слов, обозначающих действие: GET (Получить данные, указанные в URI (Uniform Resource Identifier, универсальный идентификатор ресурса)), PUT (Сохранить данные URL), POST (Создать объект, связанный с конкретным объектом) и т. д.

Способность вмешательства в безопасные Exchange RPC-соединения

Правила публикации сервера Secure Exchange в ISA Server 2004 позволяют удаленным пользователям устанавливать соединение с сервером Exchange с помощью полнофункционального клиента Outlook MAPI через Интернет. Однако клиент Outlook должен быть настроен на использование безопасного RPC так, чтобы соединение было зашифровано. RPC-политика в ISA Server 2004 позволяет блокировать незашифрованные соединения, установленные клиентами Outlook MAPI.

В традиционных брандмауэрах необходимо было открывать ряд портов для того, чтобы разрешить удаленный доступ к службам Exchange RPC с помощью клиента Outlook MAPI, что ставило безопасность под угрозу. В ISA Server 2004 эта проблема решается с помощью RPC-фильтра.

Контроль передачи данных по протоколу FTP на базе политик

Можно настроить FTP-политику ISA Server 2004 так, чтобы разрешить пользователям загружать и размещать файлы по протоколу FTP или же можно ограничить FTP-доступ пользователя только загрузкой. Это дает возможность более тщательного контроля обмена данными по протоколу FTP и лучшего обеспечения безопасности. Если при настройке FTP-фильтрации выбран вариант Read Only (Только чтение) на вкладке Protocols (Протоколы), то размещение файлов по протоколу FTP будет заблокировано.

Фильтр FTP-доступа является более функциональным, чем определяемый пользователем протокол FTP, потому что он динамически открывает конкретные порты для дополнительного подключения и может выполнять преобразование адресов, необходимое для дополнительного подключения. Этот фильтр также может различать разрешения на чтение и запись, что дает возможность более точного контроля доступа.

Преобразование ссылок

Некоторые из опубликованных Web-сайтов могут включать ссылки на имена компьютеров (NetBIOS). Для внешних клиентов доступны только пространство имен брандмауэра ISA Server 2004 и внешнее пространство имен, а не внутреннее пространство имен. Это означает, что когда внешние клиенты пытаются получить доступ на сайты через эти ссылки, эти ссылки оказываются ошибочными.

ISA Server 2004 включает в себя функцию преобразования ссылок, позволяющую создать словарь определений для имен внутренних компьютеров, которым будут сопоставляться общеизвестные имена. Это особенно полезно, например, при публикации Web-сайтов SharePoint. Директория преобразования ссылок также может преобразовывать запросы, выполненные к нестандартным портам; тогда преобразователь ссылок добавит номер порта при возврате URL клиенту.

ПРИМЕЧАНИЕ Хотя преобразование ссылок не включалось в коробочную версию ISA Server 2000, его можно было добавить к ISA Server 2000 путем установки Feature Pack 1.

СОВЕТ По умолчанию преобразование ссылок применяется только к HTML-документам, но можно по желанию добавить и другие группы контента.

ПРЕДУПРЕЖДЕНИЕ Если в документе содержатся внутренние ссылки, которым не были сопоставлены их соответствующие внешние ссылки в словаре преобразования ссылок, то внутренние имена NetBIOS станут доступны для внешних пользователей. Это может представлять определенную угрозу безопасности, поскольку у внешних пользователей появляется возможность узнать внутренние имена компьютеров.

Контроль изолирования VPN-подключений

Это еще одна функция, которой не было в ISA Server 2000. ISA Server 2004 усиливает функцию изолирования сетевого доступа (Network Access Quarantine Control), встроенную в Windows Server 2003, что обеспечивает изолирование VPN-подключений, позволяющее изолировать VPN-клиенты отдельной сети до тех пор, пока они не будут удовлетворять предопределенному набору требований безопасности. Даже если ISA Server 2004 установлен на базе ОС Windows 2000, все равно можно использовать функцию изолирования с небольшими ограничениями. В любом случае можно указать условия, которые должны соблюсти VPN-клиенты для того, чтобы получить доступ во внутреннюю сеть. Вот эти условия:

- на компьютере должны быть установлены пакеты обновлений и служебные пакеты программ;
- на компьютере должно быть установлено и активировано антивирусное программное обеспечение;
- на компьютере должно быть установлено и активировано программное обеспечение персонального брандмауэра.

VPN-клиенты, которые пройдут предопределенные тесты безопасности, могут получить доступ к сети на базе политик брандмауэра для VPN-клиентов. VPN-клиенты, которые не прошли тесты безопасности, могут получить ограниченный доступ к серверам, которые помогут им соответствовать требованиям безопасности,

например серверы, на которых они могут загрузить необходимые им заплаты и пакеты обновлений.

Преимущества, которые дает изолирование VPN-подключений в ISA Server 2004

Контроль **изолирования** VPN-подключений является замечательной **функцией,** помогающей защитить сеть от удаленных пользователей, устанавливающих VPN-подключения с компьютеров, на которых не установлены современные пакеты обновлений и заплаты, нет **установленного** и активированного антивирусного программного обеспечения и/или нет персональных брандмауэров, защищающих от атак из Интернета. Ряд сторонних производителей брандмауэров предлагает сходный набор функций, хотя обычно он идет под другим именем. Но в большинстве случаев нужно использовать только их программное обеспечение для VPN-клиентов (за дополнительную плату), чтобы воспользоваться этой функцией. В ISA Server 2004 не требуется никакое специальное клиентское программное обеспечение; используются **клиенты** PPTP или L2TP, встроенные во все современные операционные системы Windows.

Возможности для применения контроля изолирования VPN-подключений

Для того чтобы можно было использовать изолирование VPN-подключений по маршрутизируемому и удаленному доступу (Routing and Remote Access), ISA Server 2004 должен быть установлен на компьютере с ОС Windows Server 2003. Тогда можно изолировать VPN-клиенты на базе политик сервера RADIUS. Если ISA Server 2004 установлен на сервере Windows 2000, то все равно имеется возможность активировать режим изолирования через ISA Server и настроить политику брандмауэра для сети с изолированными VPN-клиентами.

Контроль изолирования является превосходной функцией для обеспечения соответствия политике безопасности вашей компании, когда пользователи получают доступ к сети извне по VPN, а ее установка очень простая. Необходимо создать профили Connection Manager и коннектоиды (connectoids, стандартные соединения Windows) для своих VPN-клиентов с помощью Connection Manager Administration Kit (CMAK), входящего в комплект поставки сервера Windows 2000 и Windows Server 2004.

Затем можно активировать изолирование на сервере либо с помощью политики RADIUS, либо с помощью политики ISA Server. Если клиент не соответствует требованиям политики безопасности в данный период времени, которая позволяет ему перейти из сети с изолированными VPN-клиентами в сеть с VPN-клиентами, то он будет отключен. Если имеются такие клиенты, которые не будут изолированы, даже если они не пройдут тесты безопасности, например компьютер генерального директора, то можно создать список исключений, к которому не будет применяться изолирование.

Требования для активации контроля изолирования VPN-подключений

Для того чтобы использовать контроль изолирования, нужно установить компонент приемника на ISA Server. Это программный структурный компонент, который принимает сообщения от VPN-клиентов для ISA Server о том, что сценарий контроля изолирования был успешно выполнен. Приемник принимает сообщения от службы уведомления. Набор Resource Kit в ISA **Server** 2004 содержит приемник, службу Remote Access Quarantine Agent (Rqs.exe) и компонент службы уведомления (Rqc.exe), которые можно использовать или же можно создать свой собственный приемник. Когда **клиентский** компьютер соответствует политикам безопасности, служба уведомления посылает сообщение-уведомление приемнику, и клиент выходит из режима изолирования.

Но сложность состоит в том, что в этом случае необходим специалист по написанию сценариев изолирования, которые будут выполняться на клиентском компьютере с профилем Connection Manager.

> ПРЕДУПРЕЖДЕНИЕ Сообщение-уведомление не шифруется и не требует проверки подлинности. Это означает, что злоумышленники могут получить доступ к этому сообщению.

А как быть с клиентами, которые не соответствуют политике? Можно настроить Web-сервер, разрешающий анонимный **доступ** для таких клиентов: так они смогут загрузить инструкции и/или программное обеспечение, необходимые для того, чтобы соответствовать политике. Изолированные клиенты могут получить доступ к этому серверу, но не к другим ресурсам сети.

Способы настройки политики контроля изолирования ISA Server 2004 обсуждаются в главе 9.

Отсутствующие функции: удалены, но не забыты

В ISA Server 2004 старым функциям, которые были в ISA Server 2000 мало функциональны или не совсем удачны, присвоены некоторые новые возможности, а также они были улучшены и расширены. Однако было бы ошибкой не упомянуть несколько функций, которые использовались в ISA Server 2000, но отсутствуют в ISA Server 2004.

Эти функции либо редко использовались, либо плохо работали в ISA Server 2000. Однако учтите, что если все-таки потребуются именно эти функции, то необходимо подумать, прежде чем выполнять обновление до ISA Server 2004 или приобретать программы сторонних производителей, в которых есть такие функции. Перечислим наиболее важные из этих функций:

- разбиение потоковых данных;
- шлюз H.323;

- контроль пропускной способности;
- активное кэширование.

Давайте кратко рассмотрим, что означает каждая из этих функций и почему компания Microsoft не включила их в ISA Server 2004.

Разбиение потоковых данных

В ISA Server 2000 была возможность разбиения потоковых данных с использованием WMT-технологий (Windows Media Technologies[1]) для того, чтобы снизить необходимую пропускную способность, используемую для передачи аудио/видео данных, в зависимости от числа внутренних клиентов, которые просматривают одни и те же потоковые данные. Если большое число пользователей в вашей организации часто просматривали или прослушивали одинаковые потоковые данные, то эта функция могла оказаться полезной. Эту функцию можно было применять к потоковым данным, которые использовали WMT-сервер, расположенный во внутренней сети, или же можно было установить WMT-сервер на самом ISA Server.

По отзывам потребителей, большинство компаний, в которых применялся ISA Server, не пользовались функцией разбиения потоковых данных, поэтому корпорация Microsoft не включила эту функцию в ISA Server 2004.

Шлюз H.323

Шлюз H.323 использовался для обработки вызовов и маршрутизации вызовов VoIP (Voice over IP, передача голоса по IP-протоколу). VoIP позволяет совершать телефонные звонки через Интернет вместо использования телефонных линий компании. В результате можно сэкономить на междугородних звонках в организациях, где много таких звонков.

Но появились сообщения о проблемах с утечкой памяти (memory leak) в службе привратника ISA Server, когда на службу направлялись неправильно сформированные пакеты. Эти атаки были безуспешными, если на ISA Server не был сконфигурирован шлюз H.323. Хотя эта проблема была устранена в Service Pack 1 к ISA Server 2000, многие пользователи перестали использовать службу шлюза H.323 или не использовали ее вообще из-за этой проблемы и из-за сложности конфигурирования шлюза H.323 для многих пользователей ISA Server. Более того, во многих более современных продуктах по работе с VoIP использовался протокол инициации сеанса SIP (Session Initiation Protocol) вместо H.323. Протокол SIP является менее сложным, он был разработан как альтернатива H.323. Cisco и другие производители

[1] Новейший из доступных сегодня комплексов технологий обработки и передачи цифрового звука и видео. В состав Windows Media Technologies входят Windows Media Player, Windows Media Services, Windows Media Tools и Windows Media Audio SDK — *Примеч. пер.*

предлагают IP-телефонию, основанную на протоколе SIP (Cisco также имеет свой собственный протокол VoIP под названием Skinny). Для эффективного применения H.323 на обоих концах соединения должен быть шлюз протокола H.323.

Компания Microsoft отказалась от поддержки шлюза H.323 в ISA Server 2004 из-за его редкого использования по ранее указанным причинам.

Контроль пропускной способности

В ISA Server 2000 входила функция контроля пропускной способности. Можно было щелкнуть правой кнопкой мыши узел Bandwidth Rules (Правила пропускной способности) и установить флажок активации контроля пропускной способности, а затем установить эффективную пропускную способность в Кбайт/с. Под эффективной пропускной способностью подразумевается либо реальная пропускная способность, используемая устройством вроде модема, либо общая пропускная способность. Можно также использовать правила пропускной способности, чтобы указать, какие соединения имеют приоритет над остальными.

Хотя сама идея казалась удачной, пользователи жаловались на то, что контроль пропускной способности в ISA Server 2000 не работал или работал как-то не так. Пользователи ожидали, что контроль пропускной способности будет ограничивать пропускную способность каждого соединения. Но на деле оказывалось по-другому. Вместо этого правила пропускной способности использовались службой качества обслуживания по планированию пакетов (quality of service packet scheduling service) для определения приоритета соединений. Но еще больше сбивало пользователей с толку то, что когда они понимали принцип работы правил пропускной способности и настраивали их правильно, возникали многочисленные проблемы с тем, что постепенно эти правила переставали работать вообще. Единственным решением, казалось, было переформатирование диска и переустановка операционной системы и ISA Server — задачи, которые рядовой администратор брандмауэра не хотел бы выполнять регулярно.

Поэтому в ISA Server 2004 не была включена поддержка функции контроля пропускной способности.

Активное кэширование

В ISA Server 2000 поддерживались не только прямой /обратный и распределенный/иерархический типы кэширования, но также и активное кэширование. Эта функция автоматически генерировала запросы на обновление объектов, которые сохранялись в кэше, без какого-либо вмешательства со стороны пользователя. Эти обновления могли выполняться на основе продолжительности времени хранения объекта в кэше или последнего доступа на сервере источника. При включенном активном кэшировании ISA Server автоматически обновлял содержимое кэша, прежде чем истекал срок хранения объектов. ISA Server следил за тем, к каким объектам

в кэше было больше всего обращений, и повторно кэшировал их, даже если их никто не запрашивал.

Можно было настроить политику активного кэширования, определяя, как часто должны обновляться объекты в кэше, для того, чтобы уравновесить необходимость в наличии обновленных кэшированных объектов и необходимую производительность сети.

Хотя активное кэширование может обеспечить своевременное обновление наиболее часто запрашиваемых объектов, оно также может потреблять большую часть пропускной способности сети и влиять на общую производительность сети. Активное кэширование не было активированным по умолчанию в ISA Server 2000, а отзывы потребителей показали, что эта функция не имела большого значения для большинства пользователей ISA Server. В соответствии со своей направленностью на повышение функциональности брандмауэра в ISA Server 2004 компания Microsoft эту функцию не включила.

Выводы

В ISA Server 2004 появилось много новых функций. В этой главе мы обсудили радикально измененный графический пользовательский интерфейс, который является одним из наиболее явных изменений ISA Server 2000. С появлением ISA Server 2004 компания Microsoft сделала еще один большой шаг от прокси-сервера к рынку серьезных брандмауэров. Хотя новый продукт основан на ISA Server 2000, ISA Server 2004 во многих отношениях является совершенно новым продуктом, а не обновлением предыдущей версии. Основной акцент, более чем когда либо ранее, сделан на безопасности.

В ISA Server 2004 сохранились многие из функций, входящих в ISA Server 2000, но большинство из них были улучшены или расширены. В ISA Server появилось много нового: от функциональных мастеров и большей гибкости в конфигурировании до совершенно новых способов выполнения привычных задач по администрированию брандмауэра.

Компания Microsoft также добавила несколько совершенно новых функций в ISA Server 2004. Наиболее всесторонней и, пожалуй, наиболее долгожданной новой функцией является поддержка нескольких сетей, которая расширяет возможности ISA Server 2004 и делает его предпочтительным при работе в больших многосетевых средах. Новая функция фильтрации на уровне приложения (ALF) дает ISA Server 2004 еще больше преимуществ, когда речь заходит о таких функциях, как внешняя защита от спама, а контроль изолирования VPN-подключен и й дает администраторам возможность обеспечить соответствие удаленных VPN-клиентов тем же стандартам безопасности, которым соответствуют клиенты внутренней сети.

В этой главе мы не пытались рассмотреть каждую функцию, которая была улучшена или добавлена в ISA Server. Мы лишь постарались дать общее представление

о некоторых отличиях ISA Server 2004 от его предшественника. В этой главе мы не углублялись в подробности того, как применять все эти новые и улучшенные функции, мы лишь описали их. Пошаговые инструкции по их использованию будут изложены в следующих главах данной книги.

Мы обратили внимание и посетовали на исчезновение ранее присутствовавших функций, которые заслужили (или не заслужили) признание пользователей ISA Server 2000. В общем, мы считаем, что набор функций ISA Server 2004 является более цельным и его гораздо легче настраивать и администрировать. Степень доверия к ISA Server 2004 подтверждается тем фактом, что в настоящее время у нас есть несколько компьютеров с ISA Server 2004, которые защищают нашу сеть. Мы считаем, что ISA Server является одним из лучших решений в области защиты/кэширования, доступных на современном рынке. В следующей главе мы сравним его с несколькими конкурентами и покажем вам, почему мы считаем его лучшим.

Краткое резюме по разделам

Новый GUI: больше, чем просто приятный интерфейс

0 Основной задачей группы разработчиков ISA Server 2004 было сделать интерфейс более удобным для пользователя, и они справились с поставленной задачей.

0 Консоль ISA Server 2004 имеет гораздо больше возможностей, чем консоль ISA Server 2000: ее окно состоит из трех панелей, на левой панелях находится уже знакомая древовидная структура, а на средней и правой панелях расположены закладки, с помощью которых можно легко выбрать тип задач, которые вы хотите выполнить, и получить инструкции по их выполнению.

0 Узлы левой панели включают: верхний узел ISA Server (Name), узлы Monitoring, Firewall Policy, Virtual Private Networks (VPN) и Configuration.

0 Узел Configuration включает в себя четыре подузла: Networks, Cache, Add-ins и General.

0 Страница Getting Started позволяет легко подготовить к работе ISA Server в качестве брандмауэра и/или сервера кэширования.

0 Dashboard представляет собой общий обзор всех областей управления, представленных на закладках (за исключением Logging).

И Узел политики брандмауэра является ядром интерфейса ISA Server. Именно здесь вы создаете правила доступа, правила Web-публикации, правила публикации почтовых серверов и другие правила публикации серверов для того, чтобы контролировать доступ в и из вашей сети.

0 Узел Virtual Private Networks имеет удобный интерфейс для выполнения наиболее распространенных задач по конфигурированию VPN и контролю клиентского доступа.

0 Вкладка Networks узла Configuration используется для создания и настройки сетей в многосетевой среде.

0 Подузел Cache используется для определения диска, на который выполняется кэширование, для создания правил кэширования, установки общих настроек кэширования или для отключения кэширования, что позволяет использовать ISA Server в режиме брандмауэра.

0 Подузел Add-ins используется для настройки фильтрации на уровне приложения (ALF). Именно здесь вы можете активировать, просмотреть, изменить или отключить фильтры приложений и Web-фильтры.

0 Подузел General включает общие административные задачи.

Старые функции обретают новые возможности

0 Если в компании имеется несколько установленных ISA Server в различных местах, то вряд ли вам захочется физически проверять каждый компьютер с ISA Server для управления им.

0 Есть три способа удаленного управления брандмауэрами ISA Server 2004: консоль управления ISA Server, службы терминалов Windows или удаленный рабочий стол Windows Server 2003, а также Web-интерфейс от сторонних производителей.

И ISA Server 2004 позволяет контролировать доступ и применение любого протокола, включая протоколы IP-уровня.

0 В ISA Server 2004 был улучшен процесс проверки подлинности. Проверка подлинности пользователей выполняется с помощью встроенной службы проверки подлинности Windows или удаленной службы RADIUS или других пространств имен.

0 Теперь проще настроить службу OWA на работу с ISA Server 2004 благодаря наличию мастера OWA-публикаций OWA Publishing Wizard.

0 ISA Server 2004 предоставляет больше свободы в определении сетевых объектов, потому что можно указать их в соответствии со следующими категориями: Networks, Network sets, Computers, Computer sets, Address ranges, Subnets, URL sets. Domain name sets и Web listeners.

0 В ISA Server 2004 входит новый набор мастеров создания правил, которые делают задачу создания политик безопасности как никогда легкой.

0 В ISA Server 2000 правила Server Publishing Rules перенаправляли входящие соединения на опубликованный сервер на тот же порт, с которого был получен исходный запрос. В ISA Server 2004 имеется возможность устанавливать соединение через конкретный номер порта, а затем перенаправлять запрос на другой номер порта на опубликованном сервере.

0 В ISA Server 2004 была улучшена и расширена функция создания VPN и удаленного доступа, включая большую гибкость в установлении VPN-подключений «узел-

в-узел», лучший контроль за VPN-клиентами, публикация серверов по протоколу PPTP и принудительное шифрование для безопасных Exchange RPC соединений.

И В ISA Server 2004 также были улучшены функции Web-кэширования и Webпрокси, включая усовершенствованный мастер Cache Rule Wizard, большую гибкость в кэшировании SSL-контента, отображение маршрутов для правил Web-публикации и расширенные возможности по загрузке содержимого.

0 Корпорация Microsoft прислушалась к мнению потребителей и усовершенствовала и расширила функции создания журналов, мониторинга и создания отчетов в ISA Server 2004. Сюда относится мониторинг записей журналов в режиме реального времени, мониторинг и фильтрация сеансов брандмауэра в режиме реального времени, встроенный механизм создания запросов к журналам, верификаторы соединений, возможность настройки отчетов, возможность публикации отчетов, уведомление об отчетах по e-mail, возможность настраивать время создания сводки журнала, улучшенные функции записи журнала в базу данных SQL и возможность записи журнала в базу данных MSDE.

Новые функции

0 В ISA Server 2004 корпорация Microsoft представила многосетевую модель, которая подходит для взаимосвязанных сетей, применяемых во многих компаниях.

0 Теперь вы можете создавать сетевые правила и контролировать взаимодействие различных сетей друг с другом.

0 ISA Server 2004 включает в себя несколько встроенных определений сетей: внутренняя сеть (содержащая адреса первичной защищенной сети), внешняя сеть (включающая адреса, которые не принадлежат никакой другой сети), сеть VPN-клиентов (включающая адреса, присвоенные VPN-клиентам) и сеть локального хоста (включающая IP-адреса ISA Server).

В Новые функции поддержки нескольких сетей в ISA Server 2004 позволяют с легкостью защитить сеть от внутренних и внешних угроз безопасности путем ограничения соединений между клиентами даже в пределах одной организации.

0 Можно использовать ISA Server 2004 для того, чтобы определить отношения маршрутизации между сетями в зависимости от типа доступа и взаимодействия, необходимых между сетями.

0 В ISA Server 2004 имеются сетевые шаблоны, которые можно использовать для облегчения настройки политики брандмауэра, управляющей трафиком между несколькими сетями.

0 HTTP-политика ISA Server 2004 позволяет брандмауэру выполнять глубинную проверку с отслеживанием HTTP-соединений (фильтрацию на уровне приложения). Можно настроить степень проверки на базе правил.

S Можно настроить HTTP-политику ISA Server 2004 так, чтобы блокировать все попытки соединения с исполняемыми файлами Windows вне зависимости от расширения файла, используемого источником.

0 HTTP-политика ISA Server 2004 позволяет разрешить все расширения файлов, разрешить все расширения за исключением определенной группы расширений или блокировать *все* расширения за исключением определенной группы.

0 С помощью HTTP-политик и ISA Server 2004 можно контролировать HTTP-доступ для всех клиентских соединений ISA Server 2004 независимо от типа клиента.

0 Глубинная проверка HTTP-соединений в ISA Server 2004 также позволяет создавать «HTTP-подписи», которые могут сравниваться с URL запроса, заголовками запроса, телом запроса, заголовками ответа и телом ответа.

0 Можно контролировать, какие HTTP-методы разрешены на брандмауэре, путем установки контроля пользовательского доступа к различным методам.

0 Правила публикации сервера Secure Exchange в ISA Server 2004 позволяют удаленным пользователям устанавливать соединение через Интернет с сервером Exchange путем применения полнофункционального клиента Outlook MAPI.

0 Можно настроить FTP-политику ISA Server 2004 так, чтобы разрешить пользователям размещать и загружать данные по протоколу FTP, или же можно ограничить доступ пользователей *к* FTP только загрузкой данных.

0 В ISA Server 2004 входит функция преобразования ссылок, которая позволяет создать словарь определений для имен внутренних компьютеров, которым сопоставляются общеизвестные имена.

0 В ISA Server 2004 усилена функция контроля изолирования сетевого доступа, встроенная в Windows Server 2003, что позволяет изолировать VPN-подключения и изолировать VPN-клиенты в отдельной сети до тех пор, пока они не будут удовлетворять предопределенному набору требований безопасности.

0 В ISA Server 2004 добавлена поддержка перенаправления портов и возможность публикации FTP-серверов на дополнительных портах.

Отсутствующие функции: удалены, но не забыты

S3 В ISA Server 2000 была возможность разбиения потоковых данных с помощью технологий WMT, что позволяло снизить объем пропускной способности, необходимый для передачи аудио или видео, в зависимости от числа внутренних клиентов, которые просматривали одинаковые потоковые данные. В соответствии с отзывами потребителей большинство компаний, использовавших ISA Server, не пользовались функцией разбиения потоковых данных, поэтому корпорация Microsoft не включила эту функцию в ISA Server 2004.

0 Шлюз H.323 использовался для обработки вызовов и маршрутизации вызовов VoIP. Корпорация Microsoft отказалась от поддержки шлюза H.323 в ISA Server 2004 из-за его редкого использования.

И В ISA Server 2000 входила функция контроля пропускной способности, но пользователи жаловались, что контроль пропускной способности в ISA Server 2000 не

работал или работал не так, как ожидалось. В ISA Server 2004 функция контроля пропускной способности не поддерживается.

И В ISA Server 2000 поддерживались не только прямой/обратный и распределенный/иерархический типы кэширования, но и активное кэширование. Эта функция автоматически инициировала запросы на обновление объектов, которые хранились в кэше, без вмешательства со стороны пользователей. Следуя акценту на функциональности брандмауэра ISA Server 2004, корпорация Microsoft отказалась от функции активного кэширования.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: ISA Server 2004 — это брандмауэр или сервер кэширования?

О: ISA Server 2004 можно настроить на одновременную работу в режиме брандмауэра и сервера кэширования или же его можно использовать только в качестве брандмауэра. Функция кэширования является отключенной по умолчанию: она включается администратором. Организациям необходим сильный брандмауэр. Брандмауэр ISA Server 2004 обеспечивает безопасность сетей с помощью функций динамической фильтрации пакетов (фильтрации с отслеживанием соединений), обнаружения вторжений, укрепления системы и глубинной проверки на уровне приложения. При разработке и позиционировании на рынке ISA Server 2004 корпорация Microsoft делает акцент на функциональности брандмауэра.

В: Ухудшает ли использование функции кэширования работу ISA Server в качестве брандмауэра?

О: Нет. Кэширование — это сложный механизм, связанный с памятью и дисковым пространством, который позволяет улучшить производительность сетевого доступа путем сохранения объектов, к которым чаще **всего** обращаются пользователи. Web-кэширование встроено в службы брандмауэра, которые обеспечивают возможность установления связи по **протоколу** HTTP, возможность фильтрации и другие задачи, имеющие отношение к безопасности, типа контроля содержимого и блокировки URL.

В: Могу ли я использовать только функции брандмауэра?

О: Архитектура брандмауэра ISA Server 2004 сильно отличается от архитектуры ISA Server 2000. Поэтому брандмауэр ISA Server 2004 не различает функции брандмауэра и функции кэширования — все службы опосредуются службами бранд-

мауэра. Нельзя полностью отключить Web-кэширование, если в данной организации оно не требуется.

В: Должна ли у меня быть установлена служба Active Directory для того, чтобы я мог использовать брандмауэр ISA Server 2004?

О: Нет. Установка службы Active Directory не требуется. Хотя брандмауэр ISA Server 2004 может использовать пользователей и группы, содержащиеся в Active Directory, для того, чтобы обеспечить жесткий контроль входящего и исходящего доступа, что не может сделать ни один другой брандмауэр, представленный на рынке, вам не требуется служба Active Directory или домен NT для извлечения пользы из брандмауэра ISA Server 2004.

В: Как в ISA Server обрабатываются потоковые данные?

О: В ISA Server 2004 предусмотрены фильтры приложений, которые управляют обменом потоковыми данными. В особенности обеспечивается поддержка потоковых данных приложений Windows Media, RealAudio и Apple QuickTime. В ISA Server 2004 не поддерживается разбиение потоковых данных.

В: Чем отличаются политики доступа в ISA Server 2004 и ISA Server 2000?

О: Политика доступа в ISA Server 2000 основывалась на правилах протокола, сайта и содержимого, на фильтрах IP-пакетов, правилах публикации серверов и правилах Web-публикации, причем запрещающие правила обрабатывались до разрешающих правил. Напротив, в ISA Server 2004 политика доступа является единым, упорядоченным списком правил брандмауэра, которые обрабатываются сверху вниз: применяется то правило, соответствующее характеристикам соединения, которое находится выше остальных в списке.

В: Как в ISA Server 2004 поддерживается сервер Exchange?

О: В ISA Server 2004 обеспечивается уникальный уровень защиты для серверов Microsoft Exchange. Удаленный доступ к серверу Microsoft Exchange может устанавливаться в высоко защищенном режиме с помощью безопасной RPC-публикации, безопасной публикации службы 0WA и безопасной публикации протоколов POP3/IMAP4/SMTP. Брандмауэр создает мост SSL-SSL, который обеспечивает непревзойденный уровень проверки SSL-контента по сравнению с другими брандмауэрами класса ISA Server 2004. Кроме того, брандмауэр ISA Server 2004 может выполнять проверку подлинности на основе форм от имени OWA-сайта во внутренней сети путем генерации журнала на самой форме. Это предупреждает неавторизованные соединения с OWA-сайтом.

В: Могу ли я разместить VPN-сервер под защитой брандмауэра ISA Server 2004?

О: Да. В отличие от ISA Server 2000, вы можете публиковать другие протоколы (GRE) помимо TCP/UDP с помощью ISA Server 2004. Вы можете публиковать PPTP или NAT-T совместимые L2TP/IPSec VPN-серверы, расположенные под защитой бранд-

мауэра ISA Server 2004. В действительности вы можете настроить брандмауэр ISA Server 2004 как VPN-сервер и опубликовать VPN-сервер, расположенный под защитой брандмауэра ISA Server 2004.

В: Что представляет собой возможность работы ISA Server 2004 с несколькими сетями?

О: Функция работы с несколькими сетями в ISA Server 2004 сильно повышает гибкость при работе с брандмауэром и расширяет взгляд на сеть с позиции таблицы LAT, принятый в ISA Server 2000. Брандмауэры ISA Server 2004 применяют политику брандмауэра ко всем сетевым интерфейсам, а администратор брандмауэра может установить отношения маршрутизации между этими интерфейсами. Каждое правило брандмауэра включает ссылку на сеть источника и сеть адресата. В отличие от других брандмауэров, в ISA Server 2004 нет необходимости создавать правила для каждого интерфейса, потому что этот брандмауэр автоматически создает необходимые фильтры с отслеживанием соединений для того, чтобы пропустить или отвергнуть соединение на основе интерфейсов, используемых для сети источника и сети адресата.

В: Что такое системная политика брандмауэра?

О: Системная политика брандмауэра — это предустановленный набор правил брандмауэра, позволяющих брандмауэру ISA Server 2004 взаимодействовать со службами сетевой инфраструктуры во внутренней сети. Системная политика брандмауэра вступает в силу сразу же после установки программного обеспечения ISA Server 2004. Администратор брандмауэра может настроить системную политику брандмауэра после того, как брандмауэр был запущен в первый раз.

В: Какие VPN-протоколы поддерживаются в ISA Server 2004?

О: В ISA Server 2004 поддерживаются протоколы PPTP и L2TP/IPSec для клиент-серверных VPN-подключений. Когда ISA Server 2004 установлен на базе ОС Windows Server 2003, VPN-клиент может воспользоваться IPSec NAT-T. Это позволяет VPN-клиенту, VPN-серверу или им обоим находиться за устройствами NAT и использовать безопасные соединения по протоколу L2TP/IPSec. Брандмауэры ISA Server 2004 поддерживают протоколы PPTP, L2TP/IPSec и туннельный режим IPSec для VPN-подключений «узел-в-узел».

В: Что такое фильтрация на уровне приложения?

О: Фильтрация на уровне приложения позволяет брандмауэру ISA Server 2004 определять достоверность данных, проходящих через него, путем проверки команд и данных протокола уровня приложения. Брандмауэр ISA Server 2004 настроен на распознавание законных команд и данных для протокола уровня приложения и последующее пропускание законных соединений и отбрасывание незаконных. Традиционные брандмауэры не могли определить законность попытки соединения или сообщения, потому что им были известны только IP-адреса

источника и адресата и номера портов. Традиционные брандмауэры пропускали вредоносные коды, потому что они не понимали протоколы уровня приложения. Брандмауэры ISA Server 2004 могут интерпретировать наиболее распространенные протоколы уровня приложения, используемые в современном Интернете. Эта способность позволяет брандмауэрам ISA Server 2004 защищать сеть от известных и неизвестных угроз сейчас и в будущем.

В: Влияет ли функция фильтрации на уровне приложения в ISA Server 2004 на производительность?

О: Глубинная проверка команд и данных протокола уровня приложения требует некоторого объема памяти, дискового пространства и мощности процессора. Уровень нагрузки определяется числом правил и соединений в секунду, анализируемых брандмауэром. Более крупные наборы правил брандмауэра вызывают большую нагрузку, чем небольшие. В ISA Server 2004 имеется встроенная консоль Performance (Производительность), которую можно использовать для того, чтобы оценить влияние различных настроек набора правил. Поскольку ISA Server 2004 работает на базе аппаратной конфигурации компьютера, довольно просто обновить аппаратную часть, которая по результатам анализа производительности является узким местом. Традиционные аппаратные брандмауэры предполагают покупку новой лицензии или, что еще хуже, покупку нового устройства, когда требуется обновить аппаратное обеспечение.

В: Могу ли я настроить форму подачи информации в отчетах ISA Server 2004?

О: Функции создания отчетов в ISA Server 2004 позволяют настроить многие компоненты встроенных в ISA Server 2004 отчетов. Например, можно увеличить число имен пользователей, которые отображаются в отчете Web Usage (Отчет об использовании Интернета), число сайтов, которые отображаются в этом отчете и способ сортировки приложений, которые приводятся в отчете Application Usage (Отчет об использовании приложений). Это лишь небольшой пример настроек, которые можно выполнить в отчетах ISA Server 2004.

Глава 3

Рейтинг брандмауэров и место в нем ISA Server 2004

Основные темы главы:

Параметры сравнения брандмауэров

Сравнение ISA Server 2004 с другими брандмауэрами

Параметры сравнения брандмауэров

Нам было непросто представить ISA Server ИТ-сообществу, заинтересованному в обеспечении безопасности. После того, как мы ответили на основополагающий вопрос, упомянутый в главе 1, «ISA Server — это настоящий брандмауэр?», возник второй вопрос, на который всегда хотели получить ответ потенциальные пользователи: «Что представляет собой ISA Server по сравнению с другими брандмауэрами?».

Часто, задавая такой вопрос, ярые сторонники брандмауэров от Checkpoint или РГХ пытаются бросить нам вызов. Иногда такой вопрос поступает от новоиспеченных или же опытных сетевых администраторов. Судя по всему, перед ними была поставлена задача выбора брандмауэра для использования в организациях, но они пришли в замешательство от обилия рекламных материалов, информации от производителей и похвал или жалоб других пользователей брандмауэров.

Для того чтобы аргументировано ответить на этот вопрос, нам пришлось ознакомиться не только с ISA Server 2004, но и с функциями и схемами лицензирования, и принципами ценообразования конкурирующих брандмауэров. Эта глава преследует три основные цели:

- дать ответ на несколько наиболее распространенных вопросов тем читателям, которые являются ответственными за выбор брандмауэра и/или средства кэши рования для своих сетей;
- а предоставить рациональную базу для выбора ISA Server 2004, которая будет основываться на данных и фактах, а не на пристрастных утверждениях;
- снабдить подходящими аргументами тех читателей, которые уже знают, что они хотят использовать в своих сетях ISA Server 2004, но которым еще нужно убе дить в этом руководство своей компании.

Если взглянуть на ассортимент продукции большинства основных производителей устройств с функциями брандмауэра, то можно заметить, что существует несколько различных моделей этих устройств, не говоря уже о множестве различных схем лицензирования и обилии дополнений, которые расширяют их функциональность и предлагаются за отдельную плату.

Попытка сравнения продукции разных производителей является непростой задачей, и часто в таком сравнении нет явного победителя. Напротив, обнаруживается, что правильный выбор сильно зависит от инфраструктуры сети, от того, какая роль отводится брандмауэру, и от предпочтения одних функций другим.

Часто слышатся жалобы сетевых администраторов: «Я могу купить брандмауэр SonicWail за 500 долларов. ISA Server 2004 стоит в три раза больше, а он даже не включает в себя никакого аппаратного обеспечения». Вообще-то, это правда. Но нужно учесть следующее.

- Брандмауэр SonicWail (или NetScreen или WatchGuard) стоимостью менее 500 дол ларов не предназначен для применения в крупной или даже средней сети пред-

приятии. Эти брандмауэры низшей ценовой категории являются моделями класса SOHO (Small Office/Home Office, класс программного обеспечения, предназначенного для малого или домашнего офиса) или дистанционными моделями.

- Брандмауэры класса SOHO ограничены небольшим числом пользователей (обычно 10-25), а дистанционные брандмауэры разработаны для защиты отдельного компьютера пользователя, работающего из дома и устанавливающего соединение с сетью компании удаленно (дистанционные брандмауэры во многом похожи на персональные брандмауэры).
- Брандмауэры класса SOHO и дистанционные брандмауэры возможно не поддерживают удаленного доступа по виртуальной частной сети или поставляются лишь с одной лицензией на пользование VPN; дополнительные VPN-клиенты нужно приобретать за отдельную плату. Эти брандмауэры могут поддерживать ограниченное число VPN-туннелей (5-Ю) даже при наличии дополнительных лицензий.
- Брандмауэры низшей ценовой категории работают на базе маломощного аппаратного обеспечения. Например, брандмауэр SonicWall SOHO 3 требует наличия процессора с частотой 133 МГц и 16 Мбайт оперативной памяти. Напротив, можно выбирать, на какой аппаратной платформе устанавливать ISA Server и другие брандмауэры на базе аппаратного обеспечения (нужно лишь, чтобы она соответствовала минимальным требованиям для работы ОС и брандмауэра).
- Производительность брандмауэров низшей ценовой категории часто очень низкая (например, пропускная способность в 75 Мбит/с по сравнению с подтвержденной тестами пропускной способностью ISA-сервер, которая составляет до 1,5 Гбит/с).

По мере углубления в сравнительные характеристики становится понятно, что простое сравнение цен бессмысленно. В сравнительном анализе также должны учитываться расходы на администрирование, схема лицензирования и набор функций сравниваемых продуктов. Фраза «Я могу купить брандмауэр дешевле, чем за 500 долларов» равносильна фразе «Я могу купить часы за 5 долларов» или «Я могу купить новый автомобиль за 10 000 долларов». Все эти фразы истинны, но многие потребители предпочитают израсходовать 50 500 или даже 5 000 долларов на часы и 20 000, 30 000 долларов или большую сумму на покупку новой машины. Почему? Большинство покупателей скажут, что они ставят во главу угла вопросы надежности, функциональности и долгого срока эксплуатации. Конечно, свою роль в принятии решений для них может играть общественный статус, особенно если они платят за вещь очень много.

Разумеется, если бы для защиты сети было достаточно брандмауэров стоимостью менее 500 долларов, то те же самые производители не предлагали бы брандмауэры, которые стоят в три, пять, десять или иногда в двадцать раз больше, чем брандмауэры низшей ценовой категории.

Эта глава не является попыткой представить все так, как будто ISA Server является лучшим брандмауэром для любой сети в любой ситуации. В ней приводятся

факты, которые поддерживают нашу точку зрения: ISA Server — это серьезный конкурент на рынке промышленных брандмауэров, и он может отстоять свое место в конкуренции с корифеями рынка брандмауэров (Cisco и Check Point) и со многими брандмауэра ми/УРЫ-устройствами низшей ценовой категории, используемыми в настоящее время.

> ПРИМЕЧАНИЕ В промышленной среде часто нет необходимости и не рекомендуется использовать один и тот же брандмауэр для всех устройств. Хорошая стратегия всесторонней защиты подразумевает использование различных продуктов от разных производителей для обеспечения наиболее эффективной защиты от современных типов угроз. Например, в компании приняли решение использовать один или несколько быстрых брандмауэров с фильтрацией пакетов, типа PIX, на границе с Интернетом, и разместить брандмауэр с фильтрацией на уровне приложения, типа ISA Server, в демилитаризованной зоне или перед каждой подсетью отдела.

В следующих разделах будут рассмотрены некоторые факторы, которые необходимо учитывать при сравнении различных брандмауэров. Они подразделяются на три обширные категории.

- **Расходы и лицензирование** Сюда включаются не только начальные вложе ния в программное и аппаратное обеспечение или расходы на покупку специ ализированного устройства, но также учитываются и схемы лицензирования, на пример требование наличия отдельной лицензии для каждого VPN-клиента, до полнительные модули, контракты на поддержку, сравнительная стоимость об новления и другие факторы, влияющие на TCO (Total Cost of Ownership, полная стоимость владения), например расходы на администрирование, обучение пер сонала и т. д.
- **Спецификации и функции** Здесь речь идет об архитектуре и операцион ной системе, производительности и количестве одновременно поддерживаемых сеансов, функциях фильтрации и функциях защиты и предупреждения вторже ний, функциях VPN (поддержка протоколов, клиентов, определенного количе ства туннелей, изолирования VPN-подключений и обеспечения безопасности), функции Web-кэширования (при наличии) и интеграции и взаимодействия *с* серверами Windows и другими серверами.
- **Сертификация** Сертификация независимыми организациями типа ICSA Labs (International Computer Security Association, международная ассоциация компь ютерной безопасности) в США и Checkmark в Великобритании может подтвер дить, что брандмауэры соответствуют минимальным критериям, основанным на стандартных процедурах тестирования.

Сравнительный анализ, приведенный в данной главе, основан на информации, полученной из документации производителей, на опросах производителей и администраторов, использующих различные брандмауэры, и на непосредственной оценке практики использования некоторых продуктов.

ПРЕДУПРЕЖДЕНИЕ Информация, представленная в данной главе, была действительной на момент исследований и написания данной книги, но рынок программных средств обеспечения безопасности постоянно меняется. Постоянно появляются новые продукты, и выходят обновленные старые продукты. Часто происходит смена бизнес-структуры или владельцев компаний-производителей (например, одна из основных компаний, продукция которой рассматривается в нашем аналитическом сравнении, NetScreen, была куплена компанией Juniper Networks вскоре после написания данной книги); все это может привести к изменениям в самой продукции.

В данном анализе мы сравним стоимость, функции и функциональность ISA Server 2004 с несколькими его основными конкурентами на рынке брандмауэров. В этой главе мы рассмотрим следующих конкурентов ISA Server 2004:

- Checkpoint (включая устройства от Nokia);
- устройства обеспечения безопасности Cisco PIX;
- устройства обеспечения безопасности NetScreen (теперь в собственности Juniper Networks);
- устройства обеспечения безопасности SonicWall;
- устройства обеспечения безопасности Watchguard;
- программное обеспечение для промышленных брандмауэров Symantec Enterprise Firewall (включая устройства от Symantec);
- устройства Blue Coat Systems ProxySG;
- открытые брандмауэры (IPchains, Juniper FWTK, IPCop).

Разумеется, в этот список не включены все брандмауэры, доступные на современном рынке; однако сюда вошли устройства, занимающие самые крупные сегменты рынка.

Стоимость работы брандмауэра

Для сетевого администратора стоимость брандмауэра, возможно, будет не первой в списке приоритетов при выборе наиболее подходящего продукта. Ему требуется брандмауэр, который наиболее эффективно справится с поставленной задачей и который наиболее прост в **применении,** управлении и обновлении. Однако для тех, кто принимает окончательное решение (руководитель финансового отдела, отдела обеспечения или владелец малого бизнеса), стоимость — очень важный показатель.

Важно помнить, что стоимость включает в себя гораздо больше, чем просто начальную цену покупки устройства или пакета программного/аппаратного обеспечения. Принимающие решения должностные лица, которые учитывают интересы бюджета компании, интересуются полной стоимостью, т. е. всеми финансовыми расходами после покупки данного продукта на протяжении его использования. При сравнении различных продуктов нужно учесть следующие факторы:

- капиталовложения;
- дополнительные модули или расширения;
- схемы лицензирования;
- поддержку;
- обновление;
- полную стоимость владения.

Каждый из этих факторов подробно рассматривается в следующих разделах.

Капиталовложения

Под «капиталовложениями» понимается как начальная стоимость лицензии на программное обеспечение или аппаратное устройство, так и стоимость дополнительных модулей, лицензий для клиентов или других компонентов, необходимых для полнофункционального применения брандмауэра или средства кэширования в сети. Многие производители рекламируют «базовую цену», которая не обязательно включает в себя все, что потребуется для использования устройства в нужных целях (например, если необходимо использовать брандмауэр в качестве VPN-шлюза, возможно, придется купить лицензии, которые не включаются в цену брандмауэра для каждого VPN-клиента).

Дополнительные модули и расширения

Во многих брандмауэрах предусмотрено расширение их функциональных возможностей с помощью дополнительных модулей или дополнительных устройств или программного обеспечения, не входящего в основной комплект поставки. Например, большинство производителей брандмауэров не включают Web-кэширование в качестве стандартной функции брандмауэра, некоторые из них предоставляют возможность добавить эту функцию с помощью программного модуля, например Checkpoint, или предлагают дополнительное аппаратное устройство, которое выполняет эту функцию, например Cisco. В ISA Server 2004, так же как и в Blue Coat, функция Web-кэширования встроена в брандмауэр, так что можно сэкономить сотни или даже тысячи долларов, потому что не придется покупать дополнительное программное обеспечение или устройство, чтобы получить эту функцию.

Для точного сравнения стоимости ISA Server с другими устройствами необходимо также учесть стоимость дополнений, необходимых для обеспечения того же уровня функциональности, как и в коробочной версии ISA Server.

Некоторые функции и возможности, поставляемые производителями в виде дополнений, включают:

- Web-кэширование;
- 1DS/IDP (Intrusion-Detection System/Intrusion Detection&Prevention System);
- сканирование и обнаружение вирусов;

- централизованное управление несколькими брандмауэрами;
- генерацию отчетов;
- высокую доступность/выравнивание нагрузки;
- PKI (Public Key Identification, идентификация открытым ключом)/проверку подлинности по смарт-картам.

В коробочную версию ISA Server 2004 включается большая часть этих функций, поэтому они не требуют дополнительных расходов.

Кроме того важно отметить, что поскольку устройства ASIC (Applications Specific Integrated Circuit, специализированная интегральная схема) не включают жесткий диск, на который записываются файлы журналов, для них часто требуется специальное аппаратное обеспечение для записи журналов. Например, для записи журналов брандмауэра PIX нужен отдельный сервер. Часто при расчете стоимости об этом забывают. Люди часто жалуются, что ISA Server требует покупки аппаратного обеспечения компьютера и лицензии на операционную систему, но запись файлов журналов, созданных устройством ASIC, также требует подобных расходов.

Схемы лицензирования

Важно понимать схему лицензирования каждого продукта для того, чтобы провести их сравнение. Схема лицензирования может существенно повлиять на общую стоимость брандмауэра/устройства обеспечения безопасности. Некоторые производители предоставляют лицензии на базе подписки, требуя ежегодную плату за лицензию на программное обеспечение. Другие назначают начальную плату за лицензию, при этом дополнительная плата потребуется при обновлении продукта до более новой версии (при этом можно получить скидку на покупку лицензии по сравнению с теми, кто покупает **этот** продукт впервые).

Цены на лицензии также различаются в **зависимости** от того, как будет использоваться брандмауэр. Например, лицензия на второй брандмауэр в кластере для обеспечения отказоустойчивости и восстановления после сбоя, возможно, будет ниже, чем первая лицензия на активный брандмауэр. Производители могут использовать различные термины для определения уровней лицензирования. Например, Cisco предлагает лицензии на брандмауэр PIX в двух видах: Restricted (Ограниченная) или Unrestricted (Неограниченная) лицензия, помимо лицензии на использование брандмауэра в режиме восстановления после отказа (FO, Failover mode). Тип лицензии определяется ключом активации. Ограниченная лицензия ограничивает число поддерживаемых интерфейсов, а также объем оперативной памяти, доступной для программного обеспечения. Неограниченная лицензия позволяет использовать весь объем оперативной памяти, поддерживаемый аппаратным обеспечением, и максимальное количество интерфейсов, поддерживаемых аппаратным обеспечением. Ограниченная лицензия не поддерживает использование брандмауэра в конфигурации восстановления после отказа, а неограниченная поддерживает. Можно

также купить специальную лицензию, например «R to UR» для обновления ограниченной лицензии до неограниченной или «FO to R» или «FO to UR» для обновления лицензии на работу в режиме восстановления после отказа до ограниченной или неограниченной лицензии.

Лицензии на некоторые брандмауэры устанавливаются по числу пользователей. Это реализуется с помощью отправки сообщения ping и подсчета количества ответов от хостов (в таком случае сетевые принтеры и другие устройства, которым присвоены IP-адреса, могут рассматриваться как «пользователи») или путем отслеживания числа внутренних узлов, которые получают доступ к Интернету через внешний интерфейс. Например, брандмауэр от Check Point FireWall-1 (FW-1) прослушивает IP-трафик на всех внутренних интерфейсах и подсчитывает число различных IP-адресов. Когда число IP-адресов превышает лимит, установленный в лицензии, администраторам отправляется оповещение по электронной почте и производится запись в журнал событий.

Многие производители также предусматривают схемы лицензирования в зависимости от количества пользователей в компании; для покупателей большого количества брандмауэров предлагаются меньшие цены. Производители брандмауэров на базе аппаратного обеспечения также предлагают лицензии, ограниченные по сроку действия, который истекает после предустановленного количества дней.

ПРИМЕЧАНИЕ Одно заметное преимущество брандмауэров на базе программного обеспечения, например ISA Server 2004, Check Point и промышленного брандмауэра от Symantec, состоит в том, что их легко можно оценить перед покупкой путем установки оценочной версии продукта.

Возможно, вы захотите выяснить, нужны ли для полной функциональности брандмауэра дополнительные лицензии помимо лицензии на программное обеспечение брандмауэра. Некоторые производители за дополнительную плату предлагают лицензии для каждого VPN-подключения. Несмотря на то, что их цена относительно небольшая (15-35 долларов за одну лицензию), если имеется много пользователей VPN, то итоговая сумма будет внушительной. Возможно, потребуется получить дополнительную лицензию для использования определенных функций типа шифрования по стандарту 3DES. Наконец, могут потребоваться дополнительные лицензии на применение дополнительных модулей. Например, использование графического пользовательского интерфейса Motif для подключения к консоли управления брандмауэра FW-1 от Check Point версии FW-1 4.1 и выше предполагает дополнительные расходы на покупку лицензии Motif. Если необходимо использовать протокол LDAP (Lightweight Directory Access Protocol, облегченный протокол службы каталогов) с брандмауэром FW-1, то также придется приобрести дополнительную лицензию.

Расходы на поддержку

Еще один скрытый фактор, влияющий на стоимость, нужно принять во внимание при сравнении цен на различные брандмауэры, — стоимость поддержки, которая сильно зависит от производителя. Контракты на поддержку могут стоить от ста до нескольких тысяч долларов в год.

Некоторые производители включают бесплатную поддержку в течение определенного периода времени. Например, Cisco предоставляет бесплатную техническую поддержку в течение 90 дней, а для брандмауэра Check Point FW-1 нужно покупать контракт на поддержку/обновление для получения технической поддержки, причем стоимость такого контракта ежегодно составляет 50% от стоимости самого программного обеспечения.

Некоторые производители предлагают различные уровни контрактов на поддержку. Например, Symantec предлагает «Золотой», «Платиновый» и «Премиальный» базовые планы поддержки своих брандмауэров. «Золотой» план подразумевает поддержку по телефону в рабочее время с понедельника по пятницу, а « Плати новый» обеспечивает поддержку в нерабочее время. Имея « Премиальный» контракт, вы получаете технического специалиста и трех дополнительных технических консультантов («Золотой» и «Платиновый» контракты предоставляют вам двух технических консультантов).

Если планируется покупка контракта на поддержку, его стоимость нужно учитывать при сравнении различных брандмауэров.

> ПРИМЕЧАНИЕ Многие производители требуют заключения контракта на поддержку ежегодно. Это означает, что если вы пропустили один год и не заключили контракт на поддержку, производитель может потребовать купить контракт на поддержку на текущий год и на предыдущий год.

Расходы на обновление

Стоимость обновления брандмауэра является еще одним важным фактором, который нужно учесть при сравнении цен на брандмауэры. Брандмауэры на основе программного обеспечения, установленные на базе стандартного аппаратного обеспечения, могут сильно выиграть при установке более быстрого процессора или добавления еще одного процессора, при установке более быстрых сетевых адаптеров, большего объема оперативной памяти или при установке самого брандмауэра на новой, более мощной машине. С другой стороны, аппаратные устройства, возможно, придется заменить полностью или же их обновление потребует еще больших расходов. Например, было прекращено производство Cisco PIX Firewall Classic модели 10 000 и 510, и оно не может работать с программным обеспечением брандмауэров PIX версии 6.0 и старше. Это означает, что если потребуются функции, которые предоставляет новое программное обеспечение, придется купить новое устройство PIX.

ПРИМЕЧАНИЕ Еще важно принять во внимание то, что если/когда для брандмауэра на базе программного обеспечения нужно обновить аппаратное обеспечение на более мощное, то можно использовать обновляемое аппаратное обеспечение в качестве файлового сервера, рабочей станции или отвести ему другую роль в сети. Устройство обеспечения безопасности на базе аппаратного обеспечения, работающее на базе лицензионной ОС, имеет меньше возможностей для использования в другой роли.

Независимо от типа брандмауэра (на базе аппаратного или программного обеспечения) стоимость периодического обновления программного обеспечения также важна. Необходимо ответить на следующие вопросы.

- Обновления и пакеты исправлений предоставляются бесплатно или за них нужно платить?
- Существуют ли скидки на покупку обновленных версий программного обеспечения или вам нужно покупать полную версию?

Также нужно учесть расходы на администрирование, необходимые при выполнении обновления. Например, в процессе обновления текущей версии PIX 5.0 или более ранней версии невозможно использовать протокол FTP для передачи образа программного обеспечения непосредственно во флэш-память устройства, поэтому нужно использовать программу boothelper (помощник загрузки в PIX) или режим диспетчера. Современные версии PIX поддерживают команду, позволяющую копировать образ программного обеспечения напрямую с TFTP-сервера на устройство. В любом случае для того, чтобы ввести нужные команды для обновления программного обеспечения нужно использовать интерфейс командной строки.

Полная стоимость владения

После того, как учтены все факторы, влияющие на стоимость, можно определить полную стоимость владения (Total Cost of Ownership, TCO) для каждого продукта, для более точного сравнения цен. При вычислении TCO для каждого из конкурирующих продуктов нужно учесть не только непосредственные расходы, которые мы рассмотрели в предыдущих разделах, но также косвенные расходы, например:

- **кривая обучения:** стоимость материалов, учебных курсов и т. п., необходимых для того, чтобы администраторы научились конфигурировать и управлять брандмауэром;
- **расходы на администрирование:** время работы администратора, необходимое для конфигурирования и управления брандмауэром; необходимый уровень опытности администратора (что может повысить расходы на персонал);
- **расходы на производительность:** влияют на производительность пользователей сети;
- **убытки от простоя:** потери в производительности и в прибыли, например от упущенных сделок электронной коммерции, связанных с применением и надежностью брандмауэра.

Большинство моделей TCO подразделяют все факторы, определяющие стоимость, на две обширные категории: стоимость приобретения и текущие или рабочие расходы. В первую категорию входят стоимость покупки аппаратного обеспечения, начальная стоимость лицензии на программное обеспечение и единовременные расходы на установку, включающие оплату работы администратора, наемных консультантов (если таковые требуются), расходы на начальное обучение и т. д. Вторая категория включает в себя контракты на поддержку от производителей, внутренние расходы на администрирование, наемных независимых консультантов для поиска неисправностей и обслуживание, обслуживание и обновление аппаратного обеспечения, обновление и модернизацию программного обеспечения, текущее обучение и другие расходы. Конечно, набор этих расходов зависит от потребителя, от того, как будет использоваться брандмауэр, и от опыта и навыков персонала компании.

ПРИМЕЧАНИЕ Для брандмауэров на базе программного обеспечения существует больший разброс цен, и поэтому имеется больше возможностей определять полную стоимость владения, потому что можно воспользоваться ценовой конкуренцией различных производителей аппаратного обеспечения, а брандмауэры на базе аппаратного обеспечения предоставляют лишь небольшой выбор различных конфигураций аппаратного обеспечения с небольшим разбросом цен у разных торговых посредников.

Спецификации и функции

После того как все вопросы, связанные со стоимостью, решены и бюджет определен, вторая обширная категория параметров для сравнения брандмауэров включает функции и возможности каждого продукта. Можно разделить эту категорию на следующие подкатегории:

- общие технические требования (аппаратные и программные);
- функции брандмауэров (включая такие функции, как обнаружение вторжений);
- возможности VPN-шлюза;
- функции Web-кэширования (если имеется);
- сертификация брандмауэра.

Рассмотрим каждую из этих подкатегорий по отдельности.

Общие технические требования

Общие технические требования относятся к аппаратному обеспечению (для устройств) или минимальным требованиям к аппаратному обеспечению (для брандмауэров на базе программного обеспечения), а также к тому, насколько масштабируемым, наращиваемым и надежным является продукт в работе и как он поддерживает функции высокой работоспособности/отказоустойчивости типа объедине-

ния в кластеры/восстановления после сбоя и выравнивания нагрузки. К другим важным параметрам сравнения относятся совместимость и возможность взаимодействия с другими программами и аппаратными устройствами в сети и простота использования (которая непосредственно влияет на расходы на администрирова' ние). Приведенный далее список представляет собой отправную точку для сравнения этих технических требований.

- **Технические требования к аппаратному обеспечению** Сюда относится аппаратная архитектура (брандмауэр на базе программного обеспечения, уст ройство на базе жесткого диска, устройство ASIC). Для брандмауэров на базе программного обеспечения необходимо знать минимальные системные требо вания, а также максимальные аппаратные ресурсы, которые может использовать брандмауэр. Эта подкатегория также включает скорость процессора, объем па мяти, число портов (и тип порта: 10/100 Ethernet, гигабитный Ethernet и т. д.), размер диска (для устройств на базе жесткого диска) и другие физические фак торы. Этот параметр сравнения особенно важен для брандмауэров на базе ап паратного обеспечения, потому что аппаратное обеспечение обновить не так легко, как программное.
- **Масштабируемость** В эту подкатегорию входит способность программного брандмауэра или устройства к наращиванию по мере роста организации и сети. Следует учесть такие факторы: сколько соединений может поддерживать бранд мауэр и сколько он поддерживает одновременных VPN-туннелей, а также дру гие факторы в зависимости от конфигурации сети. Также необходимо иметь возможность конфигурирования нескольких устройств для совместной работы и их централизованного управления.
- **Надежность** Этот параметр имеет отношение к минимизации времени простоя и является результатом нескольких факторов, включая аппаратные и программ ные. Например, устройства на базе ASIC являются более надежными, потому что в них нет съемных частей, что исключает возможность механического выхода из строя. Надежность программного обеспечения зависит от точности программи рования и от сложности брандмауэра и операционной системы, на базе которой он работает, а также от возможности взаимодействия со всеми остальными при ложениями (дополнительные модули, устройства расширения от сторонних про изводителей и другие приложения), работающими на данной машине. Одним из элементов надежности является *отказоустойчивость* — способность системы работать после отказа одного или нескольких компонентов.
- **Высокая работоспособность** Этот параметр тесно связан с надежностью и обозначает резервы (типа резервных источников питания или кластеризации нескольких брандмауэров **с** автоматическим восстановлением после сбоя), ко торые обеспечивают функционирование брандмауэра после выхода из строя ап паратного или программного обеспечения.

- **Выравнивание нагрузки** Этот параметр означает способность распределять нагрузку по обработке данных между несколькими брандмауэрами для повышения производительности и распределения возрастающего объема трафика.
- **Совместимость/способность к взаимодействию** Этот параметр означает способность брандмауэра взаимодействовать с другими устройствами, серверами и клиентами сети; например, может ли брандмауэр интегрироваться с почтовым сервером для того, чтобы обеспечить защиту обмена сообщениями по протоколу RPC? Особенно при работе в сетевом окружении Windows, нужно знать, насколько хорошо брандмауэр интегрируется со службой Active Directory (может ли он использовать пользовательские и групповые учетные записи службы Active Directory для проверки подлинности), с серверами Exchange, SharePoint и другими серверами Microsoft, которые используются в сети.
- **Простота использования** Этот параметр означает простоту установки и конфигурирования (применительно к брандмауэрам на базе программного обеспечения), удобный для пользователей интерфейс управления (интерфейс GUI, Web-интерфейс или интерфейс CLI — Command Line Interface, интерфейс командной строки) и насколько легко удаленно управлять брандмауэром и централизованно управлять несколькими брандмауэрами.

  СОВЕТ Некоторые факторы, например простота использования, не поддаются оценке, а являются, скорее, результатом субъективного мнения. Интерфейс, который кажется удобным одному пользователю, может быть сложным для другого. В отличие от технических требований к аппаратному обеспечению или от функций программного обеспечения, например количества поддерживаемых VPN-туннелей, нельзя полагаться на документацию от производителя в определении того, насколько простым будет интерфейс. Рекомендуется при оценке этого фактора поговорить с администраторами брандмауэров, использующими этот продукт, или в идеале протестировать этот продукт в лабораторных условиях. Особенно просто протестировать брандмауэры на базе программного обеспечения, к которым прилагаются оценочные версии; не следует пропускать этот шаг, потому что придется ежедневно работать с этим интерфейсом.

Брандмауэр и дополнительные функции

При сравнении брандмауэров от различных производителей следует обратить внимание на несколько характерных для брандмауэра функций. Спецификации на продукцию с Web-сайтов производителей могут послужить отправной точкой, но по мере сужения выбора придется углубиться в эту тему и прочитать независимые обзоры о продукте или поговорить с ИТ-профессионалами, которые непосредственно работали с рассматриваемым продуктом.

Помните, что когда производитель утверждает, что в его продукте поддерживается конкретная функция, это еще не все. Нужно оценить, как реализована эта

функция. Например, фильтрация на уровне приложения (Application Layer Filtering, ALF) может означать, что в брандмауэре предусмотрены фильтры для обнаружения нескольких типов атак на уровне приложения, типа атак переполнения буфера DNS или POP3. При этом брандмауэр может не поддерживать глубинную фильтрацию на уровне приложения (анализ содержимого пакетов данных для конкретных, заданных администратором, текстовых строк, например).

> СОВЕТ В рекламных материалах часто приводятся необъективные данные для того, чтобы представить продукт в лучшем виде. Также помните, что различные производители часто используют различную терминологию для описания одних и тех же функций, что усложняет сравнение продуктов только на основе документации от производителя. Например, функцию, которую корпорация Microsoft называет «SSL bridging» (создание мостои SSL), другие производители называют «SSL termination and initiation» (завершение и инициация SSL).

К некоторым важным функциям брандмауэра, которые необходимо учитывать при сравнении, относятся следующие.

- Фильтрация **на уровне приложения** Большинство современных брандмауэров включают фильтрацию на уровне приложения в том или ином виде, но уровень фильтрации может сильно отличаться в разных продуктах. Наиболее распространенная реализация этой функции подразумевает наличие фильтров, которые осуществляют поиск атак на уровне приложения, например атак на DNS или POP3. Еще один тип фильтрации на уровне приложения — сканирование URL, позволяющее контролировать Web-запросы и отвергать те из них, которые не соответствуют предустановленным администратором правилам по содержимому, алфавиту, длине, HTTP-методам, заголовкам, расширениям и т. д. SMTP-фильтры и средства контроля сообщений SMTP могут проверять обмен сообщениями электронной почты **и** могут использоваться в качестве средства против **спама** для блокировки сообщений с конкретных доменов, адресов источника или с определенным содержимым.
- Поддержка протоколов При сравнении **поддержки** различных протоколов вам нужно не только определить, какие протоколы поддерживает тот или иной брандмауэр, но и какон их поддерживает. Например, могут ли политики доступа применяться к конкретному приложению, службе или протоколу? А VPN-политика? А качество обслуживания? В точности определите, какие фильтры приложения включены в каждый продукт; узнайте, какие дополнительные фильтры предусмотрены для данного продукта и насколько просто (или сложно) создавать свои собственные фильтры. В зависимости от нужд вашей организации нужно рассмотреть, поддерживаются ли брандмауэром следующие категории приложений: службы аутентификации/безопасности (HTTPS, IPSEC, ISAKMP — Internet Security Association and Key Management Protocol, протокол управления ключами и аутентификаторами защищенных соединений/IKE — Internet Key

Exchange, протокол обмена ключами), LDAP, RADIUS, SecurlD, TACACS — Terminal Access Controller Access Control System, система контроля доступа к контроллеру доступа к терминалу/TACACS-i-, CVP — Content Vectoring Protocol, протокол векторизации содержимого, почтовые службы — POP3, SMTP, ШАР, Интернет-службы (IM, совместное использование файлов, NNTP, PCAnywhere), промышленные службы (DCOM — Distributed Component Object Model, распределенная модель компонентных объектов, Citrix ICA — Interapplication Communications Architecture, архитектура межпрограммных связей, Sun NFS (Network File System, сетевая файловая система), Lotus Notes, SQL (Structured Query Language, язык структурированных запросов), протоколы маршрутизации (EGP — Exterior Gateway Protocol, протокол внешней маршрутизации), IGRP (Internet Gateway Routing Protocol, протокол Интернет-маршрутизации), GRP (Gateway Routing Protocol, протокол маршрутизации), OSPF (Open Shortest Path First, первоочередное открытие кратчайших маршрутов), RIP (Routing Information Protocol — протокол маршрутной информации), службы TCP/UDP (Bootp, Finger, Echo, FTP, NetBEUI, NetBIOS over IP, SMB — Server Message Block, блок серверных сообщений, RAS, PPTP), службы RPC, службы ICMP и службы потоковых мультимедиа.

Обнаружение вторжений Большинство современных брандмауэров включают некоторый уровень встроенного обнаружения и предупреждения вторжений (IDS/IDP). В некоторых продуктах IDS поставляется в виде отдельного модуля или предлагают функцию IDS, не входящую в коробочную версию. В других продуктах предлагается IDS в зачаточной форме и более сложная версия IDS/IDP за дополнительную плату. Сравните наиболее распространенные атаки, на обнаружение которых настроена функция IDS брандмауэра (например, WinNuke, Ping смерти, Teardrop и атаки переполнения буфера являются распространенными типами атак, но первые три атаки являются более старыми и большинство современных систем уже защищены от них с помощью обновлений). Также нужно учесть способ отправки оповещений об обнаружении вторжений, например по электронной почте, на пейджер; следует, кроме того, проверить доступность дополнительных продуктов с функцией IDS (как от производителя брандмауэра, так и от сторонних производителей), для того чтобы повысить эффективность функции IDS.

ПРИМЕЧАНИЕ Важным элементом оценки эффективности функции IDS является число ложных положительных ответов, возвращаемых IDS.

Производительность брандмауэра/количество подключений Необходимое количество одновременных сеансов, поддерживаемых брандмауэром, определяется вашими потребностями, которые зависят от размера организации. Это число может сильно отличаться в зависимости от производителя и в пределах линейки продуктов одного производителя. Нужно учесть производительность брандмауэра в мегабитах в секунду или гигабитах *в* секунду (Мбит/с или Гбит/с). Обратите внимание, что это значение будет другим (и более высоким)

по сравнению с производительностью VPN из-за нагрузок на VPN, особенно когда для VPN-подключений используются строгие стандарты шифрования типа 3DES или AES. Производительность и технические требования к подключениям являются часто основными факторами различия между различными моделями от одного производителя, но если приобретен брандмауэр на базе программного обеспечения, то эти значения также могут зависеть от аппаратного обеспечения, на базе которого он устанавливается.

- **Создание журналов и отчетов** Большинство современных брандмауэров включают функцию создания журналов, отличается лишь сложность и область охвата журналов. Необходимо учесть формат записи журнала и то, насколько просто импортировать журналы в таблицы или другие программы, а также при нять во внимание потребности организации в создании журналов. Достаточно ли журналов в текстовом формате или нужна возможность записывать журна лы в базу данных SQL? В некоторых брандмауэрах предусматривается возмож ность создания отчетов, при которой информация, содержащаяся в журналах, анализируется и накапливается в виде настраиваемых отчетов. В других бранд мауэрах эта функция предлагается в виде дополнительного модуля. Также нуж но учесть наличие программного обеспечения от сторонних производителей, предназначенного для анализа файлов журналов и создания отчетов.

Функции VPN

Большинство современных брандмауэров, кроме тех, которым отводится роль только персональных или дистанционных брандмауэров, включают в себя встроенные VPN-шлюзы. Создание виртуальных частных сетей является важным элементом обмена информацией с помощью удаленного доступа для многих организаций. Сотрудники организаций благодаря VPN могут работать из дома или находясь в дороге. При сравнении поддержки VPN различными устройствами обеспечения безопасности нужно учитывать несколько факторов.

- **Поддержка VPN-протоколов** Какие VPN-протоколы поддерживаются: IPSec, PPTP, L2TP, SSL VPN? Поддерживается ли протокол NAT-T (NAT-Traversal)? Какие протоколы аутентификации поддерживаются для VPN-подключений? Поддер живается ли двухфакторная проверка подлинности (ActivCard, Authenex, SecurlD)? Какие методы шифрования поддерживаются (DES, 3DES, AES)? Некоторые про изводители предлагают дополнительные лицензии за отдельную плату для ис пользования строгих схем шифрования.
- **Удаленный доступ/УР^подключение «узел-в-узел»** Потребности органи зации определяют, нужна ли вам поддержка VPN-подключений «узел-в-узел» (для соединения двух сетей), VPN-подключения удаленного доступа, также называе мые клиент-серверными VPN (которые позволяют отдельному компьютеру ус танавливать соединение с сетью), или и то и другое. В некоторых недорогих бран дмауэрах поддерживается только VPN-подключение «узел-в-узел».

VPN-клиенты VPN-подключения удаленного доступа предполагают установку на клиентском компьютере программного обеспечения VPN-клиента (VPN-подключение по протоколу SSL осуществляется через Web-браузер). Все современные версии ОС Windows включают клиенты корпорации Microsoft PPTP и L2TP, встроенные в ОС. Многие брандмауэры/устройства VPN требуют специализированного клиентского программного обеспечения, лицензию на которое возможно получить за дополнительную плату. В некоторых случаях можно воспользоваться клиентами корпорации Microsoft для брандмауэров сторонних производителей с целью реализации базовых функций VPN, но для использования расширенных возможностей потребуется специализированное программное обеспечение от производителей.

VPN-подключения/производительность Потребности организации определяют необходимое число одновременных VPN-подключений. В документации к брандмауэру этот параметр часто обозначается как число поддерживаемых VPN-туннелей. Если брандмауэр поддерживает несколько VPN-протоколов, необходимо проверить число допустимых подключений для каждого протокола, например число поддерживаемых PPTP-подключений может отличаться от числа L2TP-подключений. Производительность VPN обычно выражается в Мбит/с. Производительность зависит от используемого метода шифрования. Например, при использовании шифрования по схеме AES производительность будет ниже, чем при использовании 3DES.

Изолирование VPN-подключений Это способность блокировать или разрешать VPN-подключения на основе определенных администратором условий (например, активирована ли на клиентском компьютере антивирусная программа или брандмауэр и установлены ли на нем обновления средств обеспечения безопасности). Пользователи, компьютеры которых не удовлетворяют этим критериям, могут быть перенаправлены на Web-сайт, где они могут загрузить необходимые обновления. Некоторые производители называют это форсированием удаленной политики (remote policy enforcement), верификацией конфигурации клиента или другими терминами и предлагают эту функцию в виде пакетов программ от сторонних производителей или в виде программного обеспечения VPN-клиента за отдельную плату.

ПРИМЕЧАНИЕ NAT-T — технология, позволяющая использовать протокол IPSec совместно с NAT (Network Address Translation, преобразование сетевых адресов), что раньше было невозможно. Корпорация Microsoft определяет NAT-T как «набор возможностей, которые позволяют приложениям, предназначенным для работы в сети, обнаруживать то, что они находятся под защитой устройства NAT, узнавать внешний IP-адрес и устанавливать соответствия портов для перенаправления пакетов с внешнего порта NAT на внутренний порт, используемый приложением. Все эти действия производятся автоматически, и пользователю не нужно вручную устанавливать соответствия портов или регулировать работу других подобных механизмов».

Функции Web-кэширования

При сравнении возможностей по Web-кэшированию нужно учесть ряд функций. Какие функции необходимы, зависит от таких факторов, как размер и структура организации, как и насколько используется внешний доступ к Интернету в сети и есть ли у организации собственные Web-серверы.

- **Прямое кэширование** Все серверы Web-кэширования поддерживают прямое кэширование. Оно используется для ускорения ответов на внешние запросы, когда пользователи внутренней сети запрашивают Web-объект с сервера в Интерне те. Часто запрашиваемые объекты сохраняются на сервере кэширования, таким образом, к ним можно получить доступ по более быстрому соединению в ло кальной сети. Изучение ISA Server показывает, что в типичной промышленной сетевой среде 35-50% запросов могут быть обработаны с помощью прямого кэширования.
- **Обратное кэширование** Обратное кэширование используется, когда у орга низации есть внутренние Web-сайты, доступные для внешних пользователей Ин тернета. Сервер кэширования сохраняет объекты, которые наиболее часто запрашиваются с внутреннего Web-сервера, и передает их пользователям Ин тернета. Это ускоряет доступ внешних пользователей и разгружает внутренние Web-серверы, тем самым уменьшая трафик, проходящий через внутреннюю сеть.
- **Распределенное кэширование** Это средство распределения нагрузки меж ду несколькими равноправными серверами кэширования.
- **Иерархическое кэширование** Это средство размещения нескольких серве ров кэширования в сети в иерархическом порядке, для того чтобы запросы об служивались сначала локальным кэшем, а затем централизованным кэшем, прежде чем запрос перейдет на обработку на интернет-сервер. Распределенное и иерар хическое кэширование могут использоваться в комбинации.
- **Правила кэширования** Серверы кэширования могут использовать опреде ленные администратором правила для определения того, как обрабатывать за просы от внутренних и внешних Web-клиентов. Правила могут контролировать доступ к конкретным протоколам, пропускную способность или содержимое. Правила могут применяться на базе учетных записей пользователей или член ства в группе.

Сертификация брандмауэров

Еще один фактор, который может оказаться важным (но возможно и нет) для организации, состоит в том, прошел ли данный брандмауэр сертификацию. Сертификация означает, что некая организация определила, что выбранный брандмауэр удовлетворяет определенным минимальным стандартам. Для того чтобы сертификация имела смысл, она должна выполняться независимой организацией (не производителем) на основании стандартной процедуры практического тестирования в лабораторных условиях (а не просто сравнения функций на бумаге).

Лаборатория ICSA Labs (подразделение TruSecure Corporation) — самая общепризнанная организация, выполняющая тестирование и сертификацию брандмауэров и других продуктов обеспечения сетевой безопасности. В настоящее время ICSA производит тестирование на основе совокупности критериев Modular Firewall Product Certification Criteria version 4, приведенных на сайте http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria_4.0.shtml.

Тестирование ICSA базируется на практической оценке брандмауэров с использованием подхода под названием «черный ящик» (black box), основанного на функциональности.

В Великобритании компания NSS Network Testing Laboratories производит сертификацию Checkmark для продуктов обеспечения компьютерной безопасности (http://www.nss.co.uk/Certification/Certification.htm). Другие программы тестирования/сертификации, разработанные для оценки продуктов обеспечения компьютерной безопасности, используют критерии ITSEC (Information Technology Security Evaluation Criteria, критерии оценки безопасности информационных технологий), которые признаются во Франции, Германии, Нидерландах, Великобритании и в службе TCSEC Министерства обороны США. Эти правительственные программы оценки уступили место процессу Common Criteria Security Evaluation, который был утвержден в качестве стандарта Международной организацией по стандартизации (ISO).

ПРИМЕЧАНИЕ ISA Server 2000 был сертифицирован по версии 3a на базе Windows 2000 Server. С отчетом ICSA (от ноября 2001 г.) можно ознакомиться по адресу: http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/microsoftisas2000/labreport_cid303.shtml. В момент публикации данной книги ISA Server 2004 не был еще доступен широкой публике и поэтому не прошел сертификационное тестирование ICSA.

Сравнение ISA Server 2004 с другими брандмауэрами

В этом разделе мы сравним технические требования, функции и возможности ISA Server 2004 и некоторых конкурирующих продуктов. Поскольку многие производители представляют на рынке многочисленные модели брандмауэров, мы попытались выбрать по одному продукту каждого производителя, наиболее похожему на ISA Server 2004 по применению, целевой группе потребителей и цене. Бессмысленно сравнивать ISA Server, разработанный для применения в средних и крупных промышленных сетях, с персональными брандмауэрами и брандмауэрами класса SOHO. Также мы не пытались сравнивать ISA Server с промышленными брандмауэрами высшей ценовой категории, которые в десятки раз дороже.

Мы рассмотрим, насколько ISA Server 2004 выдерживает конкуренцию со следующими брандмауэрами:

- Checkpoint;
- Cisco PIX;
- NetScreen;
- SonicWall;
- WatchGuard;
- Symantec Enterprise Firewall;
- BlueCoat SG.

Параметры сравнения ISA Server 2004

Корпорация Microsoft определяет ISA Server 2004 как «усовершенствованный брандмауэр уровня приложения, решение в области VPN и Web-кэширования, которое позволяет потребителям с легкостью преумножить ИТ-инвестиции путем улучшения безопасности и производительности сети. ISA Server 2004 является членом системы Microsoft Windows Server System™, всесторонней и интегрированной серверной инфраструктуры, разработанной для удовлетворения потребностей разработчиков и ИТ-профессионалов». Давайте кратко рассмотрим некоторые из его ключевых функций и технических требований в контексте нашей модели сравнительного анализа.

Ключевые функции и общие технические требования

В ISA Server 2004 имеются следующие ключевые функции для усовершенствованной защиты от хакеров, взломщиков и сетевых атак.

- **Многоуровневая проверка** помогает защитить ИТ-имущество и корпоративную интеллектуальную собственность типа IIS, сервера Exchange, Sharepoint и другой сетевой инфраструктуры от хакеров, вирусов и неавторизованного использования с помощью всеобъемлющих и гибких политик, настраиваемых фильтров протоколов и отношений сетевой маршрутизации.
- **Усовершенствованная фильтрация на уровне приложения** позволяет передавать сложный трафик уровня приложения в Интернет, при этом обеспечивается высокий уровень безопасности, производительности и защиты от самых новых типов атак.
- **Безопасный входящий трафик и защита от** внутренних **атак по клиентскому VPN-подключению** достигаются за счет унифицированного управления политиками VPN и брандмауэра, глубинной проверки содержимого и встроенной функции изолирования VPN-подключений.
- **Встроенные возможности по работе с несколькими сетями, сетевые шаблоны, маршрутизация и проверка с отслеживанием соединений** позволяют легко использовать ISA Server в существующем сетевом окружении в качестве пограничного брандмауэра, брандмауэра отдела или филиала, не меняя сетевую инфраструктуру.

ISA Server 2004 имеет ряд расширенных, простых в применении функций, которые включают:

- **простые, легкие в овладении и использовании инструменты управления,** сокращающие время адаптации для новых администраторов, позволяя избежать появления брешей в системе безопасности из-за неправильной конфигурации брандмауэра;
- **предотвращение простоев в предоставлении сетевого доступа** обеспечивается тем, что администраторам предоставлена возможность безопасно и уданно управлять службами брандмауэра и Web-кэширования;
- **экономия расходов на пропускную способность** достигается за счет уменьшения исходящего интернет-трафика и сохранения содержимого на локальных компьютерах, а также за счет возможности эффективно и экономически выгодно распределять содержимое Web-серверов *и* приложений электронной коммерции ближе к потребителю;
- **интеграция со службой Windows Active Directory, VPN-решениями от сторонних** производителей **и другими элементами существующей инфраструктуры,** что облегчает задачу обеспечения безопасности корпоративных приложений, пользователей и данных в среде Windows или в смешанной среде;
- **объединение партнеров, пользователей и Web-ресурсов, посвященных [$A Server,** которое наряду с формальными программами поддержки пользователей от корпорации Microsoft, предоставляет массу возможностей для получения поддержки и интересующей информации.

Высокая производительность является очень важным приоритетом в современном деловом мире, и ISA Server 2004 предлагает такие функции, которые наиболее востребованы организациями, заинтересованными в производительности:

- **возможность предоставления быстрого и безопасного доступа в любом месте в любое время** для корпоративных приложений и данных, например сервер Exchange;
- **безопасная, надежная и высокопроизводительная инфраструктура** для предоставления как входящего, так и исходящего интернет-доступа и механизмы проверки подлинности на основе единой формы для различных интернет-стандартов;
- **интегрированное решение на основе одного сервера,** которое размещает на границе сети только необходимые службы, включая безопасность брандмауэра, VPN и Web-кэширование;
- **способ масштабирования инфраструктуры обеспечения безопасности** по мере роста потребностей сети путем создания гибкой многосетевой инфраструктуры;

- **повышенная производительность сети и уменьшенный расход пропускной способности** с помощью применения Web-кэширования в корпоративных центрах обработки данных и филиалах.

Далее рассматриваются некоторые общие технические требования, которые обсуждались в качестве параметров сравнения, и то, как этим техническим требованиям удовлетворяет ISA Server 2004.

Поддержка аппаратной платформы и системные требования

ISA Server 2004 является брандмауэром на базе программного обеспечения, который может быть установлен на ОС Windows 2000 Server (пакет обновлений SP4 и выше) или Windows Server 2003. На компьютере должен быть установлен браузер Internet Explorer 6 или более поздней версии. Далее перечислены минимальные требования к аппаратному обеспечению:

- процессор с частотой 300 МГц;
- 256 Мбайт оперативной памяти;
- диск, отформатированный под файловую систему NTFS (New Technology File System, файловая система новой технологии) и 150 Мбайт свободного пространства;
- по одному сетевому адаптеру для каждой сети, подключенной к ISA Server.

> **ПРИМЕЧАНИЕ** Минимальные поддерживаемые требования к аппаратному обеспечению, перечисляемые корпорацией Microsoft, должны рассматриваться как абсолютный минимум для установки ISA Server 2004, но они не являются оптимальными техническими требованиями к аппаратному обеспечению. Производительность ISA Server 2004 существенно возрастет при наличии обновленного аппаратного обеспечения. Рекомендуется в качестве реальных базовых требований к аппаратному обеспечению взять хотя бы процессор с частотой 800 МГц и оперативную память объемом 1 Гбайт. Следует учесть, что если в качестве сервера Web-кэширования используется ISA Server, то потребуется больше свободного дискового пространства для кэша.

Надежность

Надежность системы является очень важным фактором, который нужно учесть для устройства, предназначенного для решения критически важных задач, например сетевого брандмауэра. К факторам, обеспечивающим надежность ISA Server 2004, относятся следующие.

- Windows Update можно использовать для автоматического обновления операционной системы, на базе которой работает ISA Server 2004.
- Существуют планы по добавлению новых возможностей на сайт Windows Update, позволяющие брандмауэру ISA Server 2004 производить собственное обновление. Во время написания этой книги было неизвестно, когда эта функция станет доступной.

- Качество аппаратного обеспечения, на базе которого работает брандмауэр, яв ляется основным фактором, определяющим надежность системы. Резервные аппаратные компоненты типа источников питания, сетевых интерфейсов и программных или аппаратных массивов RAID (Redundant Array of Independent Disks, матрица независимых дисковых накопителей с избыточностью) могут существенно повысить общую надежность брандмауэра.
- Инструменты создания резервных копий конфигурации брандмауэра включе ны в пользовательский интерфейс брандмауэра ISA Server 2004. Они просты в использовании и позволяют администратору брандмауэра создавать резервную копию всей конфигурации брандмауэра и восстанавливать его на том же или на другом компьютере.

Масштабируемость

Масштабируемость можно разделить как минимум на две категории:

- **внешняя масштабируемость** означает способность адаптироваться к расши рению сети по мере того, как она разрастается от исходного размера и в нее добавляются новые удаленные офисы, дистанционные компьютеры и т. д.;
- **внутренняя масштабируемость** означает способность адаптироваться к рас тущему числу пользователей и к увеличению трафика по мере роста сети.

Версия ISA Server 2004 Standard Edition имеет возможность внешней масштаби-руемости путем использования встроенной службы выравнивания сетевой нагруз-ки, включенной в ОС Windows Server 2003, на базе которой работает брандмауэр. ISA Server 2004 Standard Edition также имеет возможность внутренней масштаби-руемости путем добавления оперативной памяти, свободного дискового простран-ства или более мощного процессора/процессоров. Количество процессоров, под-держиваемое в окончательной версии продукта, еще не было объявлено.

Расширяемость

Расширяемость означает способность добавлять к продукту функции и возможно-сти с помощью предлагаемого производителем или сторонними производителя-ми дополнительного программного обеспечения, сценариев и других компонен-тов. Поскольку ISA Server 2004 — это брандмауэр на базе программного обеспече-ния, то он поддерживает практически неограниченное расширение фильтрации на уровне приложения и других компонентов контроля доступа и работы с сетью. Многие конкуренты на рынке брандмауэров на базе аппаратного обеспечения для добавления новых свойств и функций заставляют потребителей в целях обновле-ния приобретать совершенно новое аппаратное обеспечение или отдельные аппа-ратные/программные устройства, не входящие в комплект поставки. В отличие от этого, потребитель может расширить брандмауэр ISA Server 2004 без дополнительных расходов с использованием свободно распространяемого комплекта ISA Server 2004 Software Development Kit (SDK).

Брандмауэр ISA Server 2004 также можно расширить с помощью покупки средств, предлагаемых потребителям сторонними производителями. Дополнения могут обеспечить выполнение таких расширенных функций как обнаружение и блокировка вирусов, высокая работоспособность и выравнивание нагрузки, контроль доступа, безопасность содержимого, функции обнаружения вторжений, проверка подлинности, например возможность использовать маркеры RSA SecurlD, дополнительные функции кэширования и более сложные функции мониторинга, создания журналов и отчетов.

ПРИМЕЧАНИЕ Чтобы ознакомиться с некоторыми дополнениями к ISA Server, смотрите статью авторов книги в журнале Windows&NET (май 2004) под названием Improving on ISA Server или в разделе Software Add-ons на сайте www.isaserver.org.

Высокая работоспособность

Высокая работоспособность означает способность продукта восстанавливаться для сети и ее пользователей после сбоя с минимальным временем простоя. Служба выравнивания сетевой нагрузки (Network Load Balancing, NLB) Windows Server 2003 поддерживает отказоустойчивые массивы NLB. Если один член NLB-массива в ISA Server 2004 становится недоступным, другие компьютеры в NLB-массиве могут обслуживать запросы для входящих и исходящих соединений. Это обеспечивает отказоустойчивость в случае проблем с аппаратным или программным обеспечением, которые выводят из строя один из серверов.

Сторонние производители могут предложить альтернативы службе Windows NLB. Также существует ряд производителей аппаратного обеспечения, которые предоставляют высокоскоростные и работоспособные устройства, работающие на уровне приложения. Эти устройства могут конкурировать с брандмауэрами ISA Server 2004.

Совместимость/способность к взаимодействию

К вопросам совместимости и способности к взаимодействию при сравнения относятся следующие параметры (но это не полный перечень): *ш* интеграция с Active Directory;

- интеграция с серверами Exchange;
- работа в смешанной сетевой среде.

Рассмотрим каждый из этих параметров подробнее.

Интеграция с Active Directory

Компьютеры с установленными брандмауэрами ISA Server 2004 могут соединяться с доменом Active Directory во внутренней сети и для проверки подлинности пользователей для входящего и исходящего доступа использовать базу данных пользователей, содержащуюся в этом домене или в других надежных доменах.

Клиентское приложение брандмауэра ISA Server 2004 позволяет брандмауэру ISA Server 2004 производить проверку подлинности всех пользователей домена Active Directory и других надежных доменов. Эта проверка подлинности является прозрачной для пользователя и позволяет брандмауэру получать информацию о пользователе и приложении для всех TCP и UDP-подключений. Эта информация хранится в журналах брандмауэра ISA Server 2004 и может использоваться для проверки работы пользователя в Интернете и для отслеживания приложений, с помощью которых пользователь получил доступ к Интернету.

Брандмауэры ISA Server 2004 поддерживают проверку подлинности службы RADIUS. Операционные системы Windows 2000 и Windows Server 2003 включают службу IAS (Internet Authentication Server, сервер проверки подлинности для Интернета), которая является реализацией службы RADIUS корпорацией Microsoft. Сервер IAS может перенаправлять входящие и исходящие запросы контроллеру домена Active Directory для проверки подлинности. Если IAS или другой сервер RADIUS используется для проверки подлинности пользователей, то брандмауэру ISA Server 2004 нет нужды соединяться с доменом Active Directory.

ПРИМЕЧАНИЕ Проверка подлинности с помощью службы RADIUS поддерживается для входящих и исходящих соединений через Web-прокси и только для входящих VPN-подключений. Обратите внимание, что клиент брандмауэра не может использовать службу RADIUS для проверки подлинности на домене Active Directory.

ПРИМЕЧАНИЕ Во время написания этой книги предполагалось, но еще не подтвердилось, что когда выйдет ISA Server 2004 Enterprise Edition, при сохранении конфигурации массивы Enterprise Arrays не будут зависеть от службы Active Directory. По сравнению с тем, что в ISA Server 2000 использовалась поддержка службы Active Directory для сохранения информации о конфигурации массива, это будет большим достижением.

Интеграция с серверами Exchange

Интеграция с Exchange является одним из основных преимуществ, повышающих продажи ISA Server 2004, а также основным конкурентным преимуществом по сравнению с другими брандмауэрами. Далее перечислено несколько ключевых факторов, объясняющих превосходную способность ISA Server 2004 интегрироваться с серверами Exchange.

- **Создание мостов SSL-SSL в ISA Server 2004** позволяет устанавливать удаленный доступ к OWA-сайту, расположенному под защитой ISA Server 2004. Большинство конкурирующих брандмауэров не способны фильтровать обмен сообщениями по протоколу HTTP, происходящему по туннелю SSL, и пропускают эти сообщения. Напротив, функция создания мостов SSL-SSL позволяет брандмауэру ISA Server 2004 « распаковывать» зашифрованные SSL-сообщения, пропуская

HTTP- сообщени я через сложные фильтры уровня приложения в ISA Server 2004, затем запаковывая HTTP-с о общения и передавая по SSL-туннелю зашифрованную SSL-информацию на OWA-сайт. В отличие от конкурирующих брандмауэров ISA Server 2004 не позволяет хакерам скрывать свои атаки в зашифрованном SSL-туннеле. Функция создания моста SSL-SSL в ISA Server 2004 может быть расширена до поддержки сервера Outlook 2003/Exchange Server 2003 RPC по HTTPS (SSL)-coeflHHeHHio. Конкурирующие брандмауэры, которые не поддерживают создание мостов SSL, не способны обеспечить защиту от этих атак, потому что они не могут распознать содержимое сообщений RPC no HTTPS (SSL)-соединению. Напротив, брандмауэр ISA Server 2004 может использовать функцию создания мостов SSL-SSL для того, чтобы проверять содержимое RPC по HTTPS (55Ь)-соединению и блокировать эти атаки.

Фильтр ISA Server 2004 Secure Exchange RPC позволяет организациям, имеющим сервер Exchange, предоставлять удаленный доступ к серверу Exchange компании с помощью клиента Outlook 2000/2002/2003. Независимо оттого, где расположен пользователь: во внутренней сети или на удаленном сайте на другом континенте, он может включить свой ноутбук, запустить Outlook, и все будет работать. Существенное улучшение производительности становится очевидным, когда используются брандмауэры ISA Server 2004 для публикации сервера Exchange с помощью средства безопасной публикации Secure Exchange RPC Publishing. На момент написания данной книги единственным конкурентом, который также предлагает эту функцию, был брандмауэр Firewall-1 от Checkpoint, который недавно получил лицензию от корпорации Microsoft на этот RPC-фильтр.

Брандмауэры ISA Server 2004 поддерживают проверку подлинности на основе форм для всех версий сервера Exchange. Проверка подлинности на основе форм использует форму входа в систему, которая обычно генерируется на компьютере с установленным сервером Exchange. Многие конкурирующие брандмауэры разрешают начальное соединение с сервером Exchange для того, чтобы сервер Exchange мог сгенерировать форму входа в систему, которая будет возвращена пользователю, желающему зайти на Web-сайт OWA. Напротив, брандмауэры ISA Server 2004 генерируют форму входа в систему на брандмауэре и отправляют ее пользователю в Интернете. Пользователь заполняет форму и отправляет на брандмауэр, где производится проверка подлинности пользователя. Только после того, как пользователь пройдет проверку подлинности на брандмауэре с помощью сгенерированной брандмауэром формы входа в систему, пользователю разрешается доступ к Web-сайту Exchange OWA. Кроме того, ISA Server 2004 является важным дополнением для владельцев серверов Exchange 2000 и Exchange 55, потому что эти версии сервера Exchange не поддерживают проверку подлинности на основе форм; в этом случае брандмауэр ISA Server 2004 может сгенерировать форму входа в систему для этих предыдущих версий сервера Exchange. Более того, можно использовать проверку подлинности на основе форм для того, чтобы запретить пользователям получать доступ к вложе-

ниям из сеансов 0WA и запретить оставлять файлы cookies и кэшированную информацию на клиентском компьютере, с которого удаленный пользователь получил доступ к OWA-сайту.

- **Средство контроля SMTP-сообщений в ISA Server 2004** позволяет органи зациям осуществлять программу многоуровневой защиты сообщений электрон ной почты от вложений, содержащих спам и вирусы; эта программа начинает действовать в сети периметра. Хотя многие организации требуют, чтобы более мощные приложения по проверке на спам и вирусы располагались на внутрен них границах, например на компьютере с установленным сервером Exchange или на вн утреннем SMTP-ретрансляторе, потребитель сможет использовать сред ство контроля SMTP-сообщений в качестве внешнего средства контроля спама/ вирусов для блокировки сообщений электронной почты, основываясь на клю чевых словах, содержащихся **в** теме или в теле сообщения, и блокировать вло жения с определенным размером, расширениями файлов и именами файлов. Обе эти функции могут использоваться для снижения нагрузки на первичные уст ройства фильтрации спама и вирусов. Во время написания данной книги ни один из брандмауэров сходной с ISA Server 2004 ценовой категории не предлагал такой набор функций даже за дополнительную плату.
- **HTTP-фильтр ISA Server 2004 сопоставляет** обмен сообщениями по прото колу HTTP с набором ограничений для файлов на основе правил. Этот фильтр может использоваться вместе с функцией создания мостов SSL-SSL в ISA Server 2004 для обеспечения защиты Web-публикации Exchange OWA, чтобы предо ставить администратору брандмауэра полный контроль над HTTP-трафиком, который перемещается на Web-сайт 0WA (или с него). Ни один из конкурентов в классе брандмауэра ISA Server 2004 не обеспечивает такой уровень глубинной проверки HTTP-сообщений для безопасных OWA-соединений по протоколу SSL

Работа в смешанной сетевой среде

Для работы ISA Server 2004 в смешанной среде нужно учесть два основных фактора:

- операционные системы различных клиентов;
- существующая смешанная сетевая инфраструктура.

ISA Server 2004 хорошо работает в среде с различными операционными системами клиентов. Конфигурации клиентов Web-прокси и SecureNAT поддерживаются **всеми** операционными системами. Клиент Web-прокси — это компьютер, интернет-браузер которого настроен на применение брандмауэра ISA Server 2004 в качестве своего сервера Web-прокси. Все современные браузеры поддерживают конфигурацию клиента Web-прокси. Сетевому администратору не нужно затрагивать операционные системы клиентов, чтобы сделать компьютеры клиентами Web-прокси. Существует множество методов автоматической настройки браузеров клиентов, например записи протокола WPAD (Web Proxy Autodiscovery Protocol, протокол автоматического обнаружения Web-прокси) на серверах DNS/DHCP, групповая

политика Windows (Windows Group Policy), IEAK и сценарии входа в систему (logon scripts).

На компьютерах, использующих конфигурацию клиента SecureNAT, клиентская операционная система имеет настроенный по умолчанию шлюз, который перенаправляет запросы Интернета на компьютер с брандмауэром ISA Server 2004. Опять же, сетевому администратору не нужно вручную настраивать эти системы, потому что настройки по умолчанию шлюза клиентских операционных систем могут быть легко выполнены с помощью протокола DHCP.

Простота использования

Важным элементом, определяющим простоту использования любого программного продукта, является пользовательский интерфейс. ISA Server 2004 предлагает администраторам удобный графический интерфейс, не только имеющий множество преимуществ по сравнению с большинством своих конкурентов, но также значительно улучшенный по сравнению с интерфейсом ISA Server 2000. Далее перечислены наиболее важные характерные черты графического интерфейса ISA Server 2004.

- **Интуитивно понятный интерфейс** Брандмауэр ISA Server 2004 имеет существенные преимущества по сравнению с брандмауэрами своего класса в данной области. Интерфейс ISA Server 2004 разработан так, чтобы предоставить администратору простую в использовании и интуитивно понятную систему конфигурирования и управления. Это важнейшее преимущество ISA Server 2004 — основной интерфейс конфигурирования брандмауэра вполне понятен, а безопасную конфигурацию брандмауэра можно задать в течение нескольких часов, при этом вам не нужен большой опыт и специальные обучающие курсы. Интерфейс ISA Server 2004 также был существенно улучшен по сравнению с интерфейсом ISA Server. 2000.
- **Сценарии управления** ISA Server 2004 позволяет администратору использовать сценарии для управления сервером. Практически каждую функцию, которую можно настроить с помощью пользовательского интерфейса, можно так же задать с помощью сценариев администрирования. Установочный компакт-диск ISA Server 2004 включает бесплатную полную версию ISA Server 2004 SDK. Организации, в штате которых состоят программисты, могут создавать сложные сценарии и пользовательские дополнения для своего брандмауэра ISA Server 2004. Это является конкурентным преимуществом для организаций, имеющих подобных специалистов, потому что большинство прочих коммерческих брандмауэров не дают в распоряжение пользователей такие инструменты разработки без дополнительной платы.
- **Простые в использовании мастера управления и конфигурирования** Конфигурирование брандмауэра — сложный процесс. Одна неверная настройка может привести к потенциально разрушительным последствиям. Для того чтобы снизить риск неправильной конфигурации, в ISA Server 2004 включают-

ся десятки мастеров конфигурирования, помогающие администраторам брандмауэра выполнять сложные задачи. В каждом мастере имеются соответствующие возможности выполнения данного задания, а практически каждый шаг содержит ссылку на обширную справочную систему (Help), входящую в брандмауэр ISA Server 2004. Это важное преимущество брандмауэра ISA Server 2004.

- **Обширная справочная система** Наверное, одним из наиболее сложных случаев при администрировании брандмауэра является ситуация, когда администратор пытается применить новую процедуру и хочет узнать, как она выполняется и каково значение терминов, используемых в интерфейсе управления брандмауэром. В брандмауэр ISA Server 2004 включена обширная справочная система, которая предоставляет подробное объяснение понятий, используемых при конфигурировании брандмауэра, и также дает пошаговое описание процедур. Файл справки также содержит ссылки на базу знаний в режиме он-лайн, где представлены более подробные материалы о конфигурировании.
- **База правил, которая позволяет легко выявлять неисправности** Администраторам брандмауэра ISA Server 2000 было сложно определить, какое правило применялось к конкретному подключению. Это осложняло выявление неисправностей в базе правил брандмауэра, когда соединения разрешались или запрещались, а причина разрешения или запрета была не ясна, Напротив, база правил брандмауэра ISA Server 2004 представляет собой упорядоченный список. Все подключения, выполняющиеся через брандмауэр, сравниваются с правилами в базе правил брандмауэра, и база правил обрабатывается сверху вниз. Это позволяет администратору брандмауэра ISA Server 2004 с легкостью определить, какое правило разрешило или запретило подключение.
- **Простота расширения** Штатные программисты и сторонние компании могут с легкостью разработать пакеты дополнений с помощью свободно распространяемого SDK, а администраторы могут добавить фильтры ISAPI (Internet Server API, интерфейс прикладного программирования интернет-сервера) для того, чтобы расширить функциональность ISA Server.

Удаленное управление

Возможность удаленного управления является важной, потому что многие подразделения организации могут быть географически разнесены. У администраторов должна быть возможность управлять брандмауэрами без необходимости физического контакта с ними. Далее перечислены некоторые решения в области удаленного управления брандмауэрами ISA Server 2004.

- **Консоль удаленного управления ISA Server 2004** Администраторы брандмауэра ISA Server 2004 могут установить ту же самую консоль управления ISA Server 2004, которая используется на самом компьютере с брандмауэром, на станцию управления в любой другой части сети. Консоль удаленного управления может также использоваться для управления несколькими брандмауэрами ISA Server 2004. Это сильно упрощает управление несколькими брандмауэрами. Администратор

брандмауэра может установить соединение с несколькими брандмауэрами, тогда имя каждого брандмауэра появится на левой панели консоли, по которой легко перемещаться. Напротив, интерфейсы управления на базе Интернета, предлагаемые другими производителями, часто требуют, чтобы администратор брандмауэра открывал несколько окон браузера, а затем пытался управлять каждым брандмауэром из отдельного окна.

- **Управление с помощью протокола удаленного рабочего стола** Еще один эффективный способ управления одним или несколькими брандмауэрами ISA Server 2004 состоит в использовании клиентских служб терминалов, установленных на базе ОС Windows 2000 и предыдущих операционных систем, или с помощью подключения клиента удаленного рабочего стола, встроенного в ОС Windows XP и Server 2003. Это позволяет администратору брандмауэра ISA Server 2004 устанавливать соединение с локальной консолью одного или нескольких брандмауэров по сети. Хотя клиент удаленного рабочего стола требует, чтобы открывалось несколько окон для установления соединения с несколькими брандмауэрами ISA Server 2004, можно использовать утилиты удаленного рабочего стола Windows Server 2003 для управления несколькими брандмауэрами из одного RDP-интерфейса и перемещаться между компьютерами, щелкая имя брандмауэра на левой панели консоли.

Создание журналов/отчетов

По сравнению с ISA Server 2000, в ISA Server 2004 были существенно улучшены и сделаны удобными для использования функции создания журналов и отчетов. Далее приводятся основные улучшения этих функций по сравнению с ISA Server 2000 и продуктами конкурентов.

- **Dashboard** Инструментальная панель (dashboard) ISA Server 2004 представляет собой отдельный интерфейс, из которого администратор брандмауэра может получать информацию о следующих параметрах: Connectivity (Подключения), Service status (Статус службы), Report status (Статус отчета), Alerts (Оповещения), active Sessions (Активные сеансы) и overall System Performance (Общая производительность системы). Инструментальная панель предоставляет большое количество информации в одном месте в привлекательном и удобном для анализа виде.
- **Alerts** Функция оповещений (Alerts) была расширена, и теперь она предоставляет всю информацию об оповещениях, связанную с работой брандмауэра, в одном месте консоли управления ISA Server 2004. Администраторам брандмауэра не нужно обращаться к оснастке Event Viewer (Просмотр событий) для того, чтобы увидеть подробности оповещения брандмауэра. Кроме того, значения оповещений могут быть сброшены (при этом оповещения будут удалены из интерфейса) или подтверждены (Acknowledged) (оповещения остаются в интерфейсе, но помечаются как подтвержденные). Брандмауэр ISA Server 2004 позволяет администратору брандмауэра использовать ряд заранее сконфигурирован-

ных оповещений, а также создавать свои собственные оповещения с предпринимаемыми действиями.

- **Sessions** Консоль Sessions (Сеансы) позволяет администраторам брандмауэра просматривать активные подключения, выполняемые через брандмауэр. Сеан сы могут быть отфильтрованы так, чтобы администратор брандмауэра мог со средоточиться на интересующих его соединениях. Кроме того, с помощью кон соли Sessions могут быть прерваны подключения к брандмауэру.
- **Connectivity Monitors** Мониторы соединений в ISA Server 2004 позволяют ад министратору брандмауэра создавать закладки (keep tabs) для ряда сетевых служб, играющих жизненно важную роль для сети и подключения к Интернету. Мони торы соединений сгруппированы в несколько классов: Active Directory, DHCP, DNS, Published Servers (Опубликованные серверы), Web (Internet) и Others (Другие). Каждая из этих групп представляет службы, имеющие критически важное зна чение для работы сети. Оповещение создается, когда монитор соединений об наруживает сбой в работе сетевой службы.
- **Reporting** Встроенная функция создания отчетов позволяет администратору создавать отчеты о работе брандмауэра. Можно создавать однократные отчеты или же отчеты по расписанию (регулярные). Мастер конфигурации отчетов позволяет с легкостью создавать отчеты. Информация, входящая в отчет, сосре доточена на применении протоколов, на наиболее популярных сайтах, произ водительности кэша и наиболее активных пользователях.
- **Logging** Функция создания журналов в ISA Server 2004 позволяет администра тору брандмауэра просматривать информацию о подключении в режиме реаль ного времени. Создание журналов в режиме реального времени может исполь зоваться для быстрого обнаружения неисправностей в конфигурации брандма уэра и для выполнения ответных действий при появлении атак. Кроме того, администратор брандмауэра может использовать запросы базы данных к жур налам брандмауэра и изучать конкретную интересующую его информацию. Запись журналов в ISA Server 2004 производится в базы данных, что делает ра боту с ними более удобной. ISA Server 2004 позволяет записывать журналы в базы данных MSDE, SQL или в виде файлов. Машина базы данных MSDE поставляется вместе с ISA Server, и, если у вас уже есть лицензия на SQL, то можно выполнять запросы к этой базе данных.

У большинства конкурентов ISA Server есть сходные функции создания журналов и отчетов. Однако конкурентным преимуществом ISA Server является то, что эти функции входят в основной комплект поставки и не требуют дорогих дополнений, как в некоторых конкурирующих продуктах. Одним недостатком функции создания журналов и отчетов в ISA Server является то, что встроенная функция создания отчетов не предполагает настройку, которая требуется некоторым пользователям. Поэтому для того, чтобы получить информацию о статистике использования для каждого пользователя и для отдельных сайтов, приходится покупать продукцию сторонних производителей.

Брандмауэр и его функции

Теперь подробнее рассмотрим брандмауэр ISA Server 2004 и его функции.

Возможности фильтрации на уровне приложения

Одна из самых сильных сторон ISA Server 2004 — выполнение фильтрации на уровне приложения (ALF). Функция фильтрации на уровне приложения позволяет брандмауэру ISA Server 2004 обеспечивать защиту от атак, которые основаны на слабых местах или дырах в конкретном протоколе или службе уровня приложения,

Наиболее впечатляющая особенность фильтрации на уровне приложения в ISA Server 2004 — улучшенный фильтр защиты HTTP-данных. Фильтр защиты HTTP-данных можно настроить на проверку и блокирование HTTP-соединений на основании практически любой характеристики HTTP-соединений. Далее приводятся примеры того, как может использоваться улучшенный фильтр защиты HTTP-данных:

- блокировка сценариев Java;
- блокировка управления ActiveX;
- блокировка приложений совместного использования файлов;
- блокировка загрузок на основании расширения файла или типа MIME;
- блокировка размещения файлов по протоколу HTTP;
- блокировка неправильно установленных HTTP-соединений;
- блокировка URL на основании любого компонента URL;
- блокировка Web-страниц, содержащих заданные ключевые слова или фразы.

Помимо фильтра защиты HTTP-данных в брандмауэре ISA Server 2004 имеются фильтры приложений для следующих протоколов:

- DNS;
- FTP;
- H.323;
- MMS (Microsoft Media Streaming);
- PNM (Real Networks Streaming);
- обнаружение вторжений по протоколу POP;
- PPTP;
- RPC;
- Exchange RPC;
- RTSP (Real Time Streaming Protocol, протокол передачи мультимедийной инфор мации);
- SMTP;
- SOCKS V4;
- Web-прокси (отвечающий за функциональность Web-прокси);
- SecurlD;

- RADIUS;
- преобразование ссылок;
- проверка подлинности на основе форм службы OWA.

Большинство конкурентов предлагают сходные функции фильтрации потока данных приложений. Однако есть несколько функций фильтрации и проверки данных уровня приложения, выделяющих брандмауэр ISA Server 2004 на фоне конкурентов.

- **Фильтр Secure Exchange RPC** За исключением Checkpoint NG брандмауэры ISA Server 2004 и ISA Server 2000 являются единственными, которые могут обеспечить безопасный входящий и исходящий доступ к серверу Exchange с помощью полнофункционального почтового клиента Outlook MAPI. Фильтр Secure Exchange RPC брандмауэра ISA Server 2004 позволяет внешним пользователям получать доступ к полному спектру служб сервера Exchange посредством полнофункциональных клиентов Outlook 2000, Outlook 2002 и Outlook 2003 MAPI. Кроме того, сеть можно сконфигурировать так, чтобы независимо от местонахождения пользователя (внутри или вне корпоративной сети) служба Outlook работала без необходимости изменения любой из настроек клиента Outlook.
- **Фильтр преобразования ссылок** Проведенные исследования показывают, что ISA Server 2004 является единственным брандмауэром, позволяющим перезаписывать URL в обратных сценариях прокси. Это огромный подарок для организаций, требовавших возможности установления удаленного доступа к Web-приложениям, которые не записывались с учетом соединений удаленного доступа из Интернета. Фильтр преобразования ссылок отменяет требование перезаписи Web-приложений локальных сетей для их применения в Интернете. Эта функция сама по себе помогает организации сэкономить тысячи долларов на каждом приложении.
- **Фильтр проверки подлинности на основе форм для** службы **OWA** Эта уникальная функция ISA Server 2004 позволяет брандмауэру генерировать форму входа в систему, которую видят пользователи, входящие на Web-сайт OWA. Это повышает безопасность сайта OWA, потому что пользователи должны пройти проверку подлинности, прежде чем им будет разрешено установить соединение с сайтом 0WA. Кроме того, верительные данные пользователя не кэшируются на компьютере, подключенном к сайту OWA. Эта функция полезна в случае, когда пользователи выполняют вход на сайт OWA с ненадежных компьютеров, например из сервис-центра аэропорта. Еще одна функция безопасности, предоставляемая проверкой подлинности на основе форм — блокировка проверки подлинности по времени: если пользователи не работают в течение определенного промежутка времени, то им нужно пройти повторную проверку подлинности. Наконец, функция проверки подлинности на основе форм распространяет эти функции на все версии Exchange OWA включая Exchange 5.5, Exchange 2000

и Exchange 2003. Без применения ISA Server 2004 только Exchange 2003 поддерживает преимущества проверки подлинности на основе форм.

Поддержка протоколов

Поддержка протоколов является очень важным вопросом для пользователей, находящихся под защитой брандмауэра. Брандмауэр должен поддерживать все протоколы, необходимые пользователям в сети. Если брандмауэр не может поддерживать протокол, необходимый пользователям, то этот брандмауэр очень быстро заменят на другой, который обеспечит поддержку данного протокола. Кроме того, организациям требуется возможность тщательного контроля доступа к протоколам; не у всех пользователей должен быть доступ к одним и тем же протоколам. Некоторым пользователям нужно предоставить ограниченный доступ к протоколам, а другим требуется доступ к широкому кругу протоколов.

Далее приведены ключевые функции поддержки протоколов в ISA Server 2004.

- **Фильтры уровня приложения** В ISA Server 2004 имеется несколько фильтров уровня приложения, обеспечивающих поддержку протоколов, например FTP-фильтр, H.323-фильтр, MMS-фильтр и PNM-фильтр. Эти фильтры управляют подключениями по этим «сложным» протоколам. Пользователи не смогут применять эти протоколы, если для них нет фильтров уровня приложения. Кроме того, фильтры уровня приложения необходимы для поддержки доступа клиента SecureNAT к «сложным» протоколам.
- **Клиент брандмауэра** Программное обеспечение клиента брандмауэра предоставляет уникальный уровень доступа для компьютеров, на которых оно установлено. Программное обеспечение клиента брандмауэра позволяет компьютеру использовать практически любой протокол для установления соединения с Интернетом, включая все «сложные» протоколы. Наиболее выигрышной с точки зрения конкуренции функцией программного обеспечения клиента брандмауэра является то, что фильтрам приложений не нужно записываться для того, чтобы поддерживать сложные протоколы. Программное обеспечение клиента брандмауэра работает совместно со службой брандмауэра (firewall service) на брандмауэре ISA Server 2004 для управления подключениями. Ни один из брандмауэров, представленных в настоящее время на рынке, на это не способен. Клиент брандмауэра может быть легко установлен, причем сетевому администратору не нужен физический контакт с компьютером. Программное обеспечение можно установить с помощью служб SMS, Active Directory Group Policy Software Distribution или сценариев входа в систему и сценариев управления.
- **ISA Server 2004 Software Development Kit (SDK)** Организации могут создавать свои собственные фильтры приложений с помощью информации и инструментов, входящих *в* набор инструментальных средств разработки программного обеспечения (SDK) для ISA Server 2004. Фильтры приложений могут быть созданы для выполнения различных задач, например блокировки загрузок для

клиентов SecureNAT и клиентов брандмауэра. Любая организация, в штате которой состоят программисты C++, может использовать ISA Server 2004 SDK безо всякой дополнительной платы.

- **Поддержка протоколов VPN** В отличие от многих брандмауэров в своем классе, брандмауэр ISA Server 2004 может применять фильтрацию и проверку с отслеживанием соединений к VPN-подключениям. Это позволяет брандмауэру ISA Server 2004 обеспечивать полную поддержку VPN-клиентов, когда эти клиенты устанавливают соединение с корпоративной сетью или с Интернетом посредством VPN-подключения. Это означает, что корпоративная политика брандмауэра может применяться к VPN-клиентам без утраты поддержки наиболее важных протоколов.

Обнаружение вторжений

ISA Server 2004 включает в себя набор фильтров обнаружения вторжений, лицензированных компанией IIS (Internet Security Systems). Эти фильтры обнаружения вторжений сосредоточены на обнаружении и блокировании атак на сетевом уровне. Кроме того, ISA Server 2004 включает в себя фильтры обнаружения вторжений, которые обнаруживают и блокируют атаки на уровне приложения.

ISA Server 2004 может обнаруживать следующие типы вторжений или атак:

- атаки передачи внешних данных в Windows (атаки Windows out-of-band);
- атаки с обратной адресацией (Land-атаки);
- атака Ping of Death;
- IP-атаки без создания подключения (IP half scan);
- UDP-бомбы;
- сканирование портов (port scan);
- переполнение буфера имен узлов в DNS (DNS host name overflow);
- переполнение буфера номеров узла в DNS (DNS length overflow);
- зонная передача в DNS (DNS zone transfer);
- переполнение буфера POP3;
- переполнение буфера SMTP.

Когда брандмауэр ISA Server 2004 обнаруживает одну из этих атак, он может предпринять следующие действия:

- направить оповещение в журнал событий ISA Server 2004;
- остановить или перезапустить службы ISA Server 2004;
- произвести запуск сценария или программы администрирования;
- направить сообщение на ящик электронной почты или на пейджер администратора.

Одним недостатком ISA Server на фоне конкурентов является то, что система обнаружения вторжений, входящая в ISA Server 2004, не является настраиваемой, и

нельзя создавать свои собственные правила для обнаружения вторжений. Однако для расширения функций обнаружения вторжений за дополнительную плат)' можно использовать приложения от сторонних производителей, например систему интернет-безопасности Real Secure IDS .

VPN-функции

ISA Server 2004 поддерживает следующие протоколы VPN:

- Point-to-Point Tunneling Protocol (PPTP);
- Layer 2 Tunneling Protocol/IPSec (L2TP/IPSec);
- туннельный режим IPSec.

Протоколы PPTP и L2TP/IPSec могут использоваться как для VPN-подключений удаленного доступа, так и для VPN-подключений «узел-в-узел». Туннельный режим IPSec «узел-в-узел» может использоваться *только* при VPN-подключениях «узел-в-узел».

Туннельный режим IPSec используется *только* для обеспечения совместимости с VPN-серверами сторонних производителей. Его не следует применять при установлении подключений «узел-в-узел» между брандмауэром ISA Server 2004 и другими продуктами от корпорации Microsoft, поддерживающими VPN (Windows 2000/ Windows 2003 RRAS или ISA Server 2000).

VPN-подключения удаленного доступаЛ/РЫ-подключения «узел-в-узел»

Функция поддержки VPN в ISA Server 2004 обеспечивает два типа VPN-подключений:

- VPN-подключения удаленного доступа;
- VPN-подключения «узел-в-узел».

VPN-подключения удаленного доступа позволяют отдельным компьютерам, настроенным в качестве VPN-клиентов, устанавливать соединение с брандмауэром ISA Server 2004 и получать доступ к ресурсам корпоративной сети. VPN-клиенты удаленного доступа могут использовать протокол PPTP или протокол L2TP/IPSec Улучшенные механизмы проверки подлинности, например SecurlD, RADIUS, сертификаты EAP/TLS, биометрические и другие средства, поддерживаются VPN-сервером удаленного доступа ISA Server 2004.

VPN-подключения «узел-в-узел» позволяют брандмауэру ISA Server 2004 устанавливать соединение с другим VPN-сервером и соединять между собой целые сети через Интернет. VPN-подключения «узел-в-узел» позволяют организациям отказаться от дорогих арендуемых выделенных линий, что приводит к существенному снижению расходов.

Основное преимущество ISA Server 2004 состоит в том, что политики доступа брандмауэра применяются к VPN-подключениям удаленного доступа и «узел-в-узел». В отличие от продуктов многих конкурентов, которые разрешают полный доступ VPN-клиентов к корпоративной сети, VPN- подключения через ISA Server 2004 подчиняются политикам доступа брандмауэра. Это позволяет администратору бранд-

мауэра ISA Server 2004 устанавливать параметры контроля доступа по VPN-подключениям для каждого пользователя. При установлении VPN-подключения с брандмауэром ISA Server 2004 пользователь может получить доступ только к тем ресурсам, которые ему необходимы для выполнения работы. Другие сетевые ресурсы будут для него недоступны.

ПРИМЕЧАНИЕ Общераспространенная проблема, связанная с некоторыми VPN-службами сторонних производителей, состоит в том, что для поддержки каждого пользователя может потребоваться дополнительная конфигурация. Это означает, что если в VPN-службе стороннего производителя не предусмотрена совместная работа с Active Directory, то пользователям приходится входить в систему дважды. Даже когда служба поддерживает совместную работу с Active Directory, часто все равно требуется дополнительная конфигурация. По сравнению с брандмауэрами/устройствами VPN сторонних производителей, интеграция с Active Directory является большим преимуществом ISA Server.

Поддержка VPN-клиента

Все операционные системы Windows включают программное обеспечение VPN-клиента Windows. Далее перечислены преимущества применения VPN-клиента Windows.

- **Не требуется программное обеспечение сторонних производителей** Это важное преимущество на фоне конкурентов. Пользователям не нужно уста навливать никакое дополнительное программное обеспечение, и они могут скон фигурировать VPN-подключения с помощью понятного и простого в примене нии мастера подключения VPN-клиента. Программное обеспечение VPN-клиента требует минимальную конфигурацию, и большинство пользователей могут ус тановить соединение с ISA Server 2004 за считанные минуты.
- **Не возникает проблем с совместимостью** VPN-клиент Windows был раз работан для работы с клиентской операционной системой, на базе которой он применяется. Напротив, программное обеспечение VPN-клиента от сторонних производителей в операционной системе Windows может как работать корректно, так и давать сбои, при этом могут возникать известные или неизвестные кон фликты **с** другими сетевыми компонентами операционной системы Windows. Кроме того, задачи поиска неисправностей сводятся к минимуму, потому что потребитель может позвонить в службу поддержки корпорации Microsoft и по лучить ответы на вопросы, связанные с применением VPN-клиента. Напротив, когда потребитель использует VPN-клиент от стороннего производителя, ему приходится обращаться то к производителю операционной системы, то к про изводителю VPN-клиента до тех пор, пока не будет найдено окончательное ре шение проблемы.

- **Упрощенная конфигурация и реализация VPN** Набор инструментальных средств CMAK (Connection Manager Administration Kit, набор средств для управления соединением) от корпорации Microsoft, входящий в Windows 2000 и Windows Server 2003, позволяет с легкостью создавать VPN-клиент, для которого предустановлены правильные настройки VPN-клиента. Набор CMAK позволяет выполнить конфигурацию программного обеспечения VPN-клиента и запаковывает ее в исполняемый файл. Этот файл можно отправить по электронной почте, сохранить на диске или загрузить, или его могут загрузить с сервера корпоративные пользователи VPN. Пользователю нужно только дважды щелкнуть на файле, и он будет автоматически установлен, пользователю при этом не нужно принимать никаких решений. В отличие от продуктов многих конкурентов, эта функция автоматизации VPN-клиента предоставляется потребителю бесплатно. Набор CMAK также используется для создания профилей клиентских соединений для работы с функцией изолирования VPN-подключений (обсуждается в следующем разделе).
- **Поддержка документов IETF RFC, определяющих процесс передачи IPSec-трафика** (NAT **Traversal)** NAT-Traversal (NAT-T) — это механизм, используемый для разрешения передачи IPSec-трафика по VPN-подключениям через брандмауэры и сетевые устройства, которые применяют преобразование сетевых адресов (NAT). Это наиболее распространенная конфигурация, и почти все организации используют NAT в той или иной форме, потому что это позволяет сократить число необходимых открытых IP-адресов. Конкуренты ISA Server разработали несколько различных механизмов NAT, многие из которых несовместимы друг с другом и повышают сложность конфигурирования брандмауэров. Напротив, VPN-клиент корпорации Microsoft использует промышленный стандарт NAT Traversal, который хорошо работает совместно с брандмауэром.

Изолирование VPN-подключений

Функция изолирования VPN-подключений в ISA Server 2004 повышает безопасность соединений VPN-клиентов благодаря тому, что, прежде чем клиентам разрешается установить соединение с корпоративной сетью, они должны пройти предварительную проверку. Они остаются в особой изолированной сети до тех пор, пока они не будут удовлетворять требованиям корпоративной безопасности. Политика изолирования требует, чтобы на компьютерах VPN-клиентов были установлены обновленные версии программ обеспечения безопасности, последние версии служебных пакетов программ, современные файлы для определения вирусов и т. д. Политики изолирования VPN-подключений управляются централизованно, и нет необходимости распределять файлы с изолированием VPN-под ключе ний по отдельным VPN-клиентам.

Функция изолирования VPN-подключений является важным конкурентным преимуществом ISA Server 2004. Для ее реализации не нужно покупать никакое дополнительное программное обеспечение и вносить дополнительную плату за лицен-

зию. Также нет ограничения на число VPN-клиентов, устанавливающих соединение с помощью функции изолирования VPN-подключений.

Конкуренты ISA Server предлагают управляемые решения для VPN-клиентов, схожие с функцией изолирования VPN-подключений, но их решения обходятся организациям значительно дороже. Для того чтобы воспользоваться этими преимуществами, зачастую нужно устанавливать патентованное программное обеспечение для VPN-клиента от сторонних производителей. Напротив, функция изолирования VPN-подключений в ISA Server 2004 входит непосредственно в комплект поставки и работает с любым VPN-клиентом Windows. Можно создавать управляемые клиенты с помощью набора инструментальных средств CMAK, а затем программное обеспечение для управляемых клиентов можно легко и быстро применять для всех нужных пользователей.

Пропускная способность VPN-подключений

Предполагается, что ISA Server 2004 Enterprise Edition поддерживает такое количество VPN-подключений, которое разрешено операционной системой, на базе которой он работает. ОС Windows 2000 и Windows Server 2003 Standard Edition поддерживают 1 000 одновременных VPN-подключений. Windows Server 2003 Enterprise Edition и Datacenter Editions поддерживают свыше 16 000 PPTP-подключений и 30 000 12TP-подключений.

Пропускная способность VPN-подключений зависит от аппаратной платформы, на базе которой установлены Windows и ISA Server 2004. Добавление процессоров и плат шифрования существенно повышает пропускную способность и производительность VPN-подключений.

Функции Web-кэширования

Помимо функций брандмауэра и создания VPN-подключений, брандмауэр ISA Server 2004 также может выступать в качестве сервера Web-прокси. Компьютер с установленным ISA Server 2004 может применяться в смешанном режиме брандмауэра и сервера Web-кэширования или в качестве выделенного сервера Web-кэширования.

> ПРИМЕЧАНИЕ Если брандмауэр ISA Server 2004 сконфигурирован для работы только в режиме сервера Web-кэширования, то он теряет большинство функций брандмауэра по обеспечению защиты сети.

Прямое кэширование

Прямое кэширование происходит, когда пользователь в сети, находящийся под защитой брандмауэра ISA Server 2004, выполняет запрос к статическому Web-контенту (Web-содержимому). Запрашиваемое содержимое размещается в Web-кэше после того, как первый пользователь выполнит запрос. Следующий пользователь, запрашивающий то же содержимое из Интернета, получает его из Web-кэша с ком-

пьютера ISA Server 2004, а не с Web-сервера в Интернете. Это уменьшает количество трафика по интернет-соединению и снижает общие расходы. Кроме того, Web-**контент** доставляется пользователю гораздо быстрее из кэша, чем с Web-сернера. Это повышает производительность, и пользователи остаются довольны.

Основное преимущество прямого кэширования в ISA Server 2004 состоит в том, что оно позволяет сэкономить расходы на снижении использования пропускной способности интернет-соединения.

Обратное кэширование

Обратное кэширование происходит, когда пользователь из Интернета выполняет запрос Web-контента, который расположен на Web-сервере, опубликованном с помощью правила Web-публикации ISA Server 2004. Брандмауэр ISA Server 2004 получает Web-контент с Web-сервера во внутренней сети или в другой сети, защищенной брандмауэром, и возвращает информацию пользователю Интернета, который запросил этот Web-контент. Компьютер с ISA Server 2004 кэширует содержимое, которое он получает с Web-сервера внутренней сети. Когда следующий пользователь запрашивает ту же информацию, Web-контент передается из кэша ISA Server 2004, а не с исходного Web-сайта.

Процесс обратного кэширования имеет два принципиальных преимущества.

- **Обратное кэширование снижает использование пропускной способности сети** Обратное кэширование снижает использование пропускной способности внутренней сети, потому что кэшируемое содержимое передается непосредственно с компьютера с ISA Server 2004. Не требуется расходовать пропускную способность внутренней сети, что позволяет другим пользователям внутренней сети использовать эту пропускную способность для выполнения своей работы. Корпоративные сети, для которых является актуальным вопрос разумного использования пропускной способности, выигрывают от применения такой настройки.
- **Обратное кэширование делает доступным Web-контент** Еще более важным преимуществом обратного кэширования является его способность делать содержимое Web-сайта доступным, когда Web-сервер находится в автономном режиме (offline). Web-серверы могут переходить в автономный режим, когда на них выполняются операции регулярного технического обслуживания или после того, как на этих серверах произошел программный или аппаратный сбой. Независимо от причины перехода в автономный режим, время ожидания, в течение которого сервер находится в автономном режиме, может быть неприятным для интернет-пользователей, когда они пытаются получить доступ к этому сайту. Функция обратного кэширования в ISA Server 2004 позволяет перевести Web-сервер в автономный режим, а содержимое Web-сайта будет по-прежнему доступно для интернет-пользователей, потому что оно передается из кэша ISA Server 2004.

Сравнение брандмауэров ISA Server 2004 и Check Point

Согласно информации с Web-сайта и маркетинговых материалов Check Point, эти брандмауэры используются на 97 из 100 предприятий списка «100 businesses» журнала Fortune. Помимо Cisco PIX, Check Point является основным конкурентном ISA Server на рынке брандмауэров для крупных и средних предприятий. Согласно информации от International Data Corp. от 17 декабря 2003 г., предоставленной TechTarget (h ttp://searchsecurity.tech target.com /originalContent/0,289142,sidl4_gci941717, 00.html), Checkpoint остается лидером на рынке брандмауэров/УРЫ-технологий: его доля на рынке составляет 48%.

> ПРИМЕЧАНИЕ При сравнении доли на рынке важно помнить, что многие крупные компании являются сторонниками многоуровневой защиты (defense-in-depth), и поэтому они применяют несколько брандмауэров от различных производителей. Поэтому тот факт, что 97% из 500 компаний, перечисленных в журнале Fortune, используют Check Point, не означает, что они также не используют другие брандмауэры наряду с Check Point.

Среди устройств обеспечения безопасности Nokia (которая использует программное обеспечение от Check Point FW-1/VPN-1 на своей операционной системе IPSO) занимает третье место после Cisco и NetScreen.

В этом разделе представлен обзор программного обеспечения брандмауэра Check Point и устройств Nokia. Рассматриваются общие технические требования Check Point, аппаратные и системные требования, возможности фильтрации на уровне приложения, поддержка VPN и возможностей Web-кэширования **и** изучается то, как с ними конкурирует ISA Server 2004.

Check Point: общие технические требования

Check Point NG (Next Generation, следующее поколение) является современной версией продуктов обеспечения безопасности Firewall-1 и VPN-1. Check Point предлагает набор программ для обеспечения безопасности NG, включающий FW-1 Pro, VPN-1 Pro, SmartCenter/SmartCenter Pro, Check Point Express, Smart View Monitor/ Reporter, SmartUpdate, ClusterXL и VPN-клиенты SecuRemote и SecureClient. Ограниченную по времени оценочную версию этого набора программ можно скачать с сайта https://www.checkpoint.com/GetSecure/MediaEngine?action=MP_OrderStart.

Программы FW-1/VPN-1 можно купить в качестве брандмауэра на базе программного обеспечения/устройства VPN, который можно установить на любую из нескольких операционных систем (см. **след.** разд.) или на устройстве от Nokia, работающем на базе специализированной операционной системы IPSO. Можно также **купить** устройство Nokia с установленным программным обеспечением от Check Point или закачать программное обеспечение с сайта Check Point (предъявив свой ID для входа в систему) и выполнить установку самостоятельно. Можно скачать об-

новление операционной системы IPSO для того, чтобы установить его перед установкой программного обеспечения NG.

Лицензия на Check Point Fire Wall-1 и Check Point VPN-1 выдается на определенное количество IP-адресов (25, 50, 100, 250, неограниченное количество). Специализированное программное обеспечение клиента VPN-1 (VPN-1 SecureClient) предлагается факультативно за дополнительную плату.

Цены зависят от торгового посредника, который предлагает множество различных продуктов от Check Point (а также устройства других производителей типа Nokia, работающие с программным обеспечением Check Point FW-1/VPN-1). Далее приводятся цены на некоторые наиболее распространенные программные продукты, предлагаемые популярными торговыми посредниками (основываясь на информации с портала Hardware Central), действительные во время написания данной книги.

Шлюз FW-1 с функцией SmartCenter для обеспечения безопасности одним компьютером, защищающим 100 IP-адресов, стоит от 5 150 до 5 516 долларов США.

По информации с Web-сайта Check Point цены на продукты начинаются с'

- 24 100 долларов США для промыш лен ных версий (более 500 пользователей);
- 4 995 долларов США для предприятий среднего размера (100-500 пользователей);
- 399 долларов США для филиалов[1].

Для FW-1 и VPN-1 предлагаются годовые лицензии, требующие, чтобы покупатель каждый год платил за пользование FW-1. Программное обеспечение клиента SecuRemote VPN-1 является бесплатным. Однако усовершенствованный клиент VPN-1 SecureClient для Windows и Macintosh (который включает в себя персональный брандмауэр и настройки безопасности для отдельных компьютеров) стоит от 2 300 долларов США за 25 IP-адресов до 40 000 долларов США за 1 000 IP-адресов.

Добавление сервера с фильтрацией содержимого UFP (URL Filtering Protocol, протокол URL-фильтрации) или CVP повышает цену на сумму, размер которой зависит от используемого аппаратного или программного обеспечения.

> ПРИМЕЧАНИЕ UFP-серверы располагают списками URL, которые обозначены как разрешенные или запрещенные. CVP-серверы анализируют поток данных и разрешают или запрещают соединения на основании правил политики.

Check Point: поддержка платформы и системные требования

Программное обеспечение брандмауэра Check Point FireWall-1 работает на базе следующих операционных систем:

Продукт VPN-1 Edge для филиалов включает в себя только функции VPN и брандмауэра с проверкой с отслеживанием состояния соединений (ине поддерживает фильтрацию уровня п ри ложе ни я /се рверы без опасн ости).

- Windows NT/2000;
- Sun Solaris;
- Linux (RedHat);
- Check Point SecurePlatform;
- Nokia IPSO (специализированная ОС на базе UNIX);
- IBM AIX.

При установке на компьютере с ОС Windows Check Point FW-1 NG требует 40 Мб свободного дискового пространства, процессор с частотой от 300 МГц и как минимум 128 Мб оперативной памяти. Эти ресурсы необходимы для модуля первичного управления брандмауэром. Для GUI-клиентов потребуется дополнительно 40 Мб дискового пространства и 32 Мб оперативной памяти.

Продукты Check Point FW-1/VPN-1 позиционируются на рынке как программные продукты и как продукты, предустановленные на аппаратных устройствах.

За исключением устройств, базовая операционная система должна быть правильно настроена для правильной работы FW-1. Проблемы могут вызвать пакеты исправлений и **обновлений** для операционной системы. Лишь спустя два года после появления ОС Solaris 2.7 эта операционная система стала поддерживаться FW-1; уже прошло 9 месяцев после выхода FW-1, но он все еще не поддерживает ОС Windows Server 2003.

Как на фоне продуктов от Check Point выглядит ISA Server 2004? Как и Check Point, ISA Server 2004 — это брандмауэр на базе программного обеспечения и его можно установить на множестве различных аппаратных конфигураций. В отличие от Check Point, ISA Server 2004 не может быть установлен на базе ОС UNIX. Минимальные системные требования этих брандмауэров совпадают.

ISA Server 2004 был разработан специально для интеграции с ОС Windows и применения ее функций, в том числе:

- выравнивание сетевой нагрузки (Network Load Balancing, NLB);
- изолирование VPN-подключений;
- Active Directory;
- службы Windows DHCP, DNS и WINS;
- проверка подлинности с помощью службы RADIUS.

Все эти службы Windows входят в коробочную версию базовой ОС Windows 2000 Server или Server 2003 без дополнительной платы.

Check Point: возможности фильтрации на уровне приложения

В своих новейших продуктах «NG with Application Intelligence» (NG с возможностью работы на уровне приложения) компания Check Point предлагает возможности фильтрации на уровне приложения. В продуктах компании Check Point прикладные прокси называются «серверами безопасности», а для обозначения технологий

предупреждения атак на уровне приложения, встроенных в FireWall-1 и SmartDefense используется термин «Application Intelligence». Компания Check Point сравнительно недавно стала использовать фильтрацию на уровне приложения (эта функция не включалась в версии до 4.0).

Фильтрация содержимого может выполняться посредством плагина URL Filtering Protocol Server for FW-1 (SurfControl). Этот плагин предоставляет список категорий секретных Web-сайтов, и его можно установить на компьютере с FW-1 или на отдельном сервере. Фильтрация содержимого также может выполняться посредством CPV-сервера (Content Vectoring Protocol, протокол векторизации содержимого). Устройства и службы фильтрации содержимого типа Websense могут работать совместно с FW-1.

Брандмауэр ISA Server 2004 выполняет интеллектуальную проверку с отслеживанием соединений с использованием интеллектуальных прикладных фильтров. В нем можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запроса и ответа, но и осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или отфильтровывать определенные типы файлов. Как и FW-1, ISA Server 2004 работает с Websense, SurfControl и другими продуктами от сторонних производителей, предназначенными для фильтрации.

Брандмауэр ISA Server 2004 проверяет все аспекты HTTP-соединений. SMTP-фильтр защищает от неверных SMTP-команд, которые вызывают переполнение буфера, а средство контроля SMTP-сообщений блокирует спам и почту, содержащую опасные вложения. RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC, и пропускает через сервер Exchange только законные соединения. DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак. ISA Server SDK позволяет легко создавать Web-фильтры и прикладные фильтры.

Check Point: поддержка VPN

Компания Check Point предоставляет ряд различных решений в области создания виртуальных частных сетей:

- VPN-1 Edge: для удаленных узлов/филиалов;
- VPN-1 Express: для предприятий среднего размера с большим количеством уз лов и поддержкой до 500 пользователей;
- VPN-1 Pro: сложные сети уровня предприятия (включает в себя FW-1);
- VSX: для виртуальных локальных сетей, центров обработки данных, крупных сегментированных сетей.

Все они поддерживают проверку с отслеживанием состояния соединений, URL-фильтрацию, VPN-подключения «узел-в-узел» и сертификаты X.509. Функции обнаружения вторжений SmartDefense, фильтрация содержимого и прикладные прокси (сервер безопасности), восстановление после отказа с отслеживанием состояния

соединений и выравнивание нагрузки поддерживаются только в VPN-1 Express, VPN-1 Pro и VSX. К другим функциям VPN относятся:

- возможность создавать VPN-подключения с помощью одношаговой операции (one-click VPNs);
- шифрование и проверка подлинности для IPSec-трафика;
- в качестве стандарта шифрования в SecuRemote используется 128—256-битное AES-шифрование, а для шифрования данных 56— 168-битное 3OE3-шифрование;
- поддержка VPN QoS с помощью дополнительного модуля (FoodGate-1);
- поддержка VPN-подключений на базе протокола SSL посредством Web-браузера;
- поддержка VPN-клиента Microsoft L2TP.

Программное обеспечение Check Point SecureClient (программное обеспечение VPN-клиента, доступное за дополнительную плату) обеспечивает функциональность, сходную с функцией изолирования VPN-подключений ISA Server (в Check Point эта функция называется «client configuration verification» проверка конфигурации клиента), и также предоставляет для клиентской машины персональный брандмауэр.

Брандмауэр ISA Server 2004 обеспечивает поддержку контроля пользовательского и группового доступа и VPN-подключения удаленного доступа и «узел-в-узел», причем проверка и фильтрация с отслеживанием состояния соединений позволяют вам контролировать то, что проходит через VPN-подключение. VPN-подключения подчиняются политикам брандмауэра точно так же, как и любое другое подключение; это обеспечивает тщательный контроль используемых протоколов, серверов, с которыми можно устанавливать соединение, время суток/продолжительность соединения и IP-адрес, с которого разрешено соединение. Кроме того:

- ISA Server поддерживает сертификаты X.509 для шифрования IPSec-трафика и общие ключи для организаций, которые не хотят использовать PKI.
- VPN мастера ISA Server позволяют с легкостью устанавливать VPN-подключения. ISA Server поддерживает использование CMAK для создания VPN-коннектоидов, позволяющих пользователям устанавливать соединение с VPN одним щелчком мыши, и поддерживает автоматически загружаемую телефонную **книгу.** CMAK также позволяет вам настраивать маршруты для VPN-клиентов. Мастера CMAK позволяют с легкостью справиться со всеми задачами не только администрато ру, но и пользователю.
- ISA Server использует интернет-стандарт IETF RFC L2TP IPSec Nat Traversal (NAT-T) для установки соединений с VPN Server 2003.
- ISA Server 2004 поддерживает стандарт шифрования 3DES.
- ISA Server 2004 не поддерживает VPN QoS, однако QoS имеет ограниченную функциональность за пределами корпоративной сети, потому что каждый про межуточный маршрутизатор также должен поддерживать QoS, а вероятность этого низкая.
- ISA Server поддерживает SSL-туннелирование.

- ISA Server 2004 поддерживает клиенты Microsoft PPTP и L2TP.
- ISA Server поддерживает изолирование VPN-подключений посредством функции изолирования в Windows Server 2003 с использованием клиентов Windows PPTP и L2TP без дополнительной платы.

Check Point: Web-кэширование

Функции Web-кэширования не включаются в основное программное обеспечение Check Point; их можно добавить, купив дополнительный модуль или программу не входящую в коробочную версию.

В ISA Server 2004 входят функции Web-кэширования без дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются **внутренние** пользователи, с удаленных Web-серверов. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи, с серверов, опубликованных брандмауэром ISA Server 2004. Web-объекты, запрашиваемые удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2:004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 держать в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, потому что данные берутся из памяти, а не с диска. ISA Server 2004 дает вам возможность оптимальным образом сохранять данные в кэше на диске, что минимизирует доступ к диску как для операций чтения, так и для операций записи. ISA Server 2004 также поддерживает создание цепочек Web-прокси, что позволяет брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси (сервер восходящего потока).

Сравнение брандмауэров ISA Server 2004 и Cisco PIX

Компания Cisco предлагает **устройства** обеспечения безопасности PIX в виде нескольких моделей и конфигураций. Диапазон моделей включает как небольшие, относительно недорогие модели, предназначенные для небольших офисов и удаленных пользователей, например PIX 501, так и высокопроизводительные дорогие модели, позиционируемые на рынке для предприятий и поставщиков сетевых услуг, например PIX 535, а также ряд промежуточных моделей, предназначенных для предприятий различного размера.

Многие источники признают компанию Check Point лидером на рынке (учитывая, что ее продукция продается как в виде брандмауэров на базе программного обеспечения, так и уже установленной на устройствах от Nokia). Однако когда речь заходит о брандмауэрах, то, по данным International Data Corp., представленным агентством новостей CNET News (http://news.com.com/2 100-7355-5079045.html), в

2003 г. возглавила рынок устройств компания Cisco. Ее доля продаж на рынке составила 34,3%-

Брандмауэры PIX обычно применяются в качестве граничных брандмауэров и для создания сетей периметра (DMZ). Их аппаратное обеспечение оптимизировано для хорошей производительности **(как** и все брандмауэры на базе аппаратного обеспечения), а простота их функций по фильтрации пакетов делает эти брандмауэры наиболее уместными на границе с Интернетом.

В этом разделе представлен обзор устройств PIX. Рассматриваются их общие технические требования, поддержка платформы и системные требования, возможности фильтрации на уровне приложения, поддержка VPN и возможностей Web-кэширования, а также проводится сравнение с ISA Server 2004.

Cisco PIX: общие технические требования

Лицензии на брандмауэры PIX как правило не ограничивают число пользователей. Программное обеспечение VPN-клиента Cisco (которое не является необходимым, но добавляет дополнительные функции) обычно стоит от 30 до 50 долларов США для одного клиента. Потребители, у которых есть контракты на техническую поддержку и разрешения на применение шифрования, могут закачать программное обеспечение клиента без дополнительной платы. Брандмауэры PIX прошли сертификацию Common Criteria EAL4.

Брандмауэры PIX серии 500 включают в себя множество моделей. На момент написания данной книги предлагались следующие модели PIX:

- **PIX 501** Разработан для применения в небольших офисах и для удаленных пользователей. Обеспечивает пропускную способность брандмауэра до 10 Мбит/с и пропускную способность VPN-подключения 3 Мбит/с (с применением стан дарта шифрования 3DES). Включает в себя один интерфейс lOBaseT и четырех-портовый интегрированный коммутатор 10/100.
- **PIX 5О6Е** Разработан для применения в филиалах/удаленных офисах. Обеспе чивает пропускную способность брандмауэра до 20Мбит/с и пропускную спо собность VPN-подключения 3 Мбит/с *(с* применением стандарта шифрования 3DES). Имеет два интерфейса autosense lOBaseT.
- **PIX 515E** Разработан для применения на небольших/средних предприятиях. Обеспечивает пропускную способность брандмауэра до 188 Мбит/с, встроен ную поддержку до 2 000 IPSec-туннелей. Поддерживает до шести интерфейсов 10/100.
- PIX **525** Разработан для предприятий и поставщиков услуг. Обеспечивает про пускную способность брандмауэра до ЗбО Мбит/с, пропускную способность подключений до 70 Мбит/с (с применением стандарта шифрования 3DES), под держку 2 000 IPSec-туннелей. Может обрабатывать 280 000 одновременных се ансов брандмауэра. Поддерживает до восьми интерфейсов 10/100 или три ин терфейса Gigabit Ethernet.

- **PIX 535** Разработан для крупных предприятий и поставщиков услуг. Обеспечивает пропускную способность брандмауэра до 1 Гбит/с и пропускную способность VPN-подключения до 95 Мбит/с (с использованием схемы шифрования 3DES), поддержку до 2 000 IPSec-туннелей. Может обрабатывать 500 000 одновременных сеансов брандмауэра. Поддерживает до десяти интерфейсов 10/100 или девять интерфейсов Gigabit Ethernet.

Цены начинаются от 500 долларов США за PIX 501 с лицензией на 10 пользователей (795 долларов США за неограниченное число пользователей) до более 20 000 долларов США за PIX 535. Далее приводятся цены на модели PIX, действительные во время написания данной книги:

- PIX 501п 495-795 долларов США;
- PIX 506Еп 959 долларов США;
- РГХ 515ЕП 2 495-2 695 долларов США;
- PIX 525п 10 920-14 759 долларов США;
- PIX 535п 20 000-24 000 долларов США.

На всех моделях устройств применяется одинаковое программное обеспечение PIX. Отличается аппаратная платформа, особенно скорость процессора, объем оперативной памяти, пропускная способность, число допустимых соединений, максимальное количество интерфейсов и наличие поддержки восстановления после отказа. В табл. 31 приводятся различные аппаратные конфигурации для различных моделей.

Табл. 3.1. Сравнение аппаратного обеспечения для различных моделей PIX

Модель	**501**	**506E**	**51**SE	**525**	**535**
Процессор	133 МГц	300 МГц	433 МГц	600 МГц	1 ГГц
RAM	16 Мб	32 Мб	**32** Мб, 64 Мб	256 Мб	1 Гб
Флэш-память	8 Мб	8 Мб	16 Мб	16 Мб	16 Мб
Пропускная способность	10 Мбит/с	20 Мбит/с	188 Мбит/с	360 Мбит/с	1 Гбит/с
Соединения	7 500	25 000	**130** 000	280 000	**500** 000
Максимальное количество интерфейсов	1	+ 1 четырехпортовый коммутатор	2	6	8
Восстановление после отказа	Нет	Нет	Да	Да	Да

Брандмауэр ISA Server основан на программном обеспечении и поэтому не ограничен аппаратным обеспечением определенного производителя. Это дает большую свободу, и пропускная способность определяется аппаратной конфигурацией, на базе которой он будет установлен. Тестирование ISA Server показало, что его производительность составляет до 1,59 Гбит/с. Программное обеспечение бранд-

мауэра не ограничивает количество интерфейсов; ISA Server поддерживает столько интерфейсов, сколько позволяет аппаратное обеспечение.

Cisco PIX: поддержка платформы и системные требования

Устройства Cisco работают на базе патентованной **встроенной** операционной системы PIX OS. Эта операционная система была создана специально для служб системы защиты, и поэтому она является операционной системой повышенного уровня безопасности. Она основана на операционной системе Cisco IOS, которая используется маршрутизаторами Cisco, только в ней меньше команд и есть некоторые дополнительные команды или команды под другим названием.

Администраторы, не знакомые с операционной системой OS, должны ознакомиться с новой операционной системой.

Аппаратная конфигурация зависит от модели PIX, как показано в табл. 3.1.

Что касается брандмауэра ISA Server 2004, он работает на стандартных платформах Intel, которые легко обновляются, и его можно установить на базе ОС Windows 2000 Server или Windows Server 2003 при наличии стандартного, привычного интерфейса управления и возможности использовать аппаратное обеспечение на ваш выбор. Это делает ISA Server более масштабируемым, чем устройства, привязанные к аппаратному обеспечению.

Безопасность ОС Windows Server 2003 может быть усилена путем применения ряда специальных профилей (profile), входящих в пакет Server 2003 SP2 для мастера Security Configuration Wizard. Корпорация Microsoft также предоставляет руководство по укреплению защиты системы, включающее конкретные рекомендации по конфигурированию и стратегии применения ISA Server 2004. Этот документ можно скачать по адресу: http://www.microsoft.com/technet/prodtechnol/isa/2004/pl a n/secu ri ty ha rden i nggu ide. mspx.

Cisco PIX: Возможности фильтрации на уровне приложения

Брандмауэры PIX предлагают проверку на уровне **приложения с** отслеживанием соединений с помощью алгоритма ASA (Adaptive Security Algorithm, адаптивный алгоритм защиты) для того, чтобы различать информацию об IP-адресации, встроенную в пакеты данных пользователей или открытые дополнительные (вторичные) каналы на динамически назначенных портах, например FTP, H.323. Это позволяет службе NAT преобразовывать встроенные адреса. Брандмауэры PIX включают такую поддержку, как URL-фильтрация, созданная для работы со службами фильтрации содержимого сторонних производителей — WebSense и N2H2. С помощью этой функции можно разрешать или запрещать доступ к Web-сайтам на основании созданного администратором списка разрешенных и запрещенных сайтов. Это требует подписки и доступа к серверу WebSense от NetPartner или к серверу N2H2 через Интернет. PIX захватывает URL-запросы и отправляет запрос к базе данных на сер-

вере WebSense или N2H2, а затем запрещает или разрешает запрос на основании политики допустимого использования, установленной администратором. Фильтрация содержимого блокирует ActiveX или Java-апплеты.

В устройствах Cisco принято называть прикладные прокси «fixup protocols» (протоколы адресной привязки). Они обрабатываются посредством команды адресной привязки. Эти прокси включают в себя FTP, HTTP, H.323, ils, rsh, rtsp, SMTP, SIP, Skinny и SQL. Протоколы уровня приложения, поддерживаемые функцией обнаружения вторжений в «родных» службах PIX, не нуждаются в дополнительном конфигурировании.

Что касается ISA Server 2004, то он выполняет интеллектуальную проверку с отслеживанием состояния соединений с применением интеллектуальных прикладных фильтров. Можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запросов и ответов, но и осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или по определенным типам файлов. ISA Server 2004 также может работать вместе с WebSense и другими фильтрами сторонних производителей.

ISA Server 2004 проверяет все аспекты обмена HTTP-сообщениями. SMTP-фильтр ISA Server защищает от неверных SMTP-команд, которые приводят к переполнению буфера, а средство контроля сообщений SMTP блокирует спам и почту, содержащую опасные вложения.

RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC, и пропускает к серверу Exchange только проверенные соединения.

DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак.

SDK ISA Server позволяет легко создавать Web-фильтры и фильтры приложения.

Cisco PIX: поддержка VPN

Все брандмауэры Cisco PIX включают в себя поддержку VPN. Они поддержи ва ют программное обеспечение VPN-клиентов Cisco (для Windows, Linux, Solaris и Mac OS X), аппаратную платформу Cisco для VPN-клиентов (PIX 501 и 5O6E, маршрутизаторы Cisco серий 800 и 1700) и клиентов PPTP и L2TP Microsoft. Данные шифруются с использованием стандартов шифрования: 56-битный DES, 1б8-битный 3DES или 256-битный AES.

> ПРИМЕЧАНИЕ Пользователи PIX могут скачать лицензию на шифрование с помощью стандартов 3DES/AES или 56-битного DES бесплатно с Web-сайта Cisco.

Применение VPN-политики (которое схоже с функцией ISA Server 2004 по изолированию VPN-подключений) обеспечивается VPN-клиентом Cisco Secure v.3.x. и

старше. Политики VPN-доступа и требования к конфигурации загружаются с центрального шлюза и передаются клиенту после установления VPN-подключения. Потребители, купившие договоры на техническое обслуживание и разрешения на применение шифрования, могут загрузить программное обеспечение клиента без дополнительной платы.

Что касается ISA Server 2004, то в нем можно применять политику брандмауэра к интерфейсам VPN. Что, наверное, является еще более важным, ISA Server не требует добавления к VPN-клиентам никакого программного обеспечения. ISA Server поддерживает VPN-клиенты PPTP и L2TP/IPSec, встроенные в ОС Windows 9x./ME, Windows XP, Windows NT, 2000 и Server 2003. Изолирование VPN-подключений ISA Server позволяет администраторам устанавливать определенные условия, которым должны удовлетворять VPN-клиенты, прежде чем им будет разрешено устанавливать соединение (например, должны быть установлены самые последние пакеты служебных программ/обновлений), и направлять клиенты на сервер, чтобы загрузить и установить необходимые обновления.

Мастера VPN ISA Server позволяют администраторам легко создавать VPN, а набор инструментальных средств CMAK может использоваться для обеспечения клиентам соединений, устанавливаемых одним щелчком мыши.

Cisco PIX: Web-кэширование

Что касается Check Point, функции Web-кэширования не включаются в брандмауэры/VPN устройства Cisco. Их можно приобрести за дополнительную плату вместе с Cisco Content Engine (набор средств для работы с содержимым).

Программное обеспечение Cisco ACNS (Application and Content Networking Software), предназначенное для работы с приложениями и содержимым в сетевой среде, реализуется на базе модул ей/устройств кэширования Cisco Content Engine, цена на которые колеблется в пределах от 2 500 до 18 000 долларов США. Оно обеспечивает интегрированное кэширование и доставку содержимого. Устройства Content Engines являются устройствами кэширования, работающими на базе ОС Cisco IOS. Программное обеспечение Cisco для кэширования работает на основе Content Engine и обеспечивает разбиение потоковых данных и кэширование, кэширование с помощью прокси (HTTP, FTP, SSL-туннелирование) и прозрачное кэширование.

Для реализации прозрачного кэширования программное обеспечение для кэширования и ACNS поддерживают протокол WCCP (Web Cache Communication Protocol, протокол Web-кэширования), разработанный Cisco для перенаправления конкретных типов трафика в Web-кэш. Протокол WCCP также используется компаниями CacheFlow (теперь BlueCoat), NetApp и Squid.

Брандмауэр ISA Server 2004 включает в себя функции Web-кэширования без какой-либо дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на

внешние Web-серверы. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи на серверы, которые были опубликованы с помощью брандмауэра ISA Server 2004. Web-объекты, запрошенные удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 сохранять в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, т. к. объекты берутся из памяти, а не с диска. ISA Server 2004 позволяет сохранять данные в кэше на диске, что сводит к минимуму доступ к диску как для операций записи, так и для операций чтения. ISA Server 2004 также поддерживает **создание** цепочек Web-прокси, позволяющих брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси.

Сравнение брандмауэров ISA Server 2004 и NetScreen

Компания NetScreen занимала второе место среди производителей устройств обеспечения безопасности в 2003 г. Согласно информации, предоставленной International Data Corp. (IDC) и опубликованной службой новостей CNET News на сайте hup-.// news.com.com/2100-7355-5079045html, ее доля на рынке составила *16%.*

Компания Juniper Networks подписала договор на приобретение NetScreen Technologies в феврале 2004 г. Juniper Networks представляет на рынке маршрутизаторы и коммутаторы для поставщиков услуг и крупных предприятий.

В этом разделе представлен обзор устройств брандмауэров от NetScreen. Рассматриваются общие технические требования, поддержка платформы и системные требования, возможности фильтрации на уровне приложения, поддержка VPN и Web-кэширования и производится сравнение с ISA Server 2004.

> ПРИМЕЧАНИЕ Juniper Networks не имеет отношения к набору инструментальных средств Juniper Firewall Tool Kit (FWTK), открытой утилите брандмауэра для ОС Linux/UNIX, которая обсуждается далее в этой главе *в* разделе «Сравнение ISA Server 2004 с открытыми брандмауэрами».

NetScreen: общие технические требования

Устройства NetScreen включают в себя возможности брандмауэра и VPN-подключений по протоколу IPSec. В них также входят функции защиты от вирусов на базе технологии Trend Micro AV. Компонент брандмауэра реализует проверку с отслеживанием соединений и ограниченную проверку на уровне приложения.

Устройства NetScreen созданы на базе архитектуры ASIC, которая включает RISC-процессоры (Reduced Instruction Set Computer, процессор с сокращенным набором

команд) и обеспечивает ускоренную обработку данных. Устройства работают на базе патентованных программно-аппаратных средств ScreenOS, встроенных во флэш-память, а не в жесткий диск. Это обеспечивает устройству некоторые преимущества перед традиционными устройствами, программно-аппаратное обеспечение которых встроено в жесткий диск, потому что при этом меньше вероятность механического повреждения и выхода устройства из строя.

Компания NetScreen производит ряд различных устройств от низшей ценовой категории серии 5 (5XP, 5XP Elite, 5GT, 5GN Plus, 5XT, 5XT Elite) до высшей ценовой категории серий 200, 500 и 5 000. Модели средней ценовой категории включают NetScreen 25 и 50. Диапазон цен — от 500 до почти 100 000 долларов США. Далее приведены цены на модели NetScreen, действительные на время написания данной книги:

- NetScreen 5XP (10 пользователей) 495 долларов США;
- NetScreen 5GT 495 долларов США;
- NetScreen 5XT 695 долларов США;
- NetScreen 5XP Elite (неограниченное число пользователей) 995 долларов США;
- NetScreen 5GT Plus 995 долларов США;
- NetScreen 5XT Elite 1195 долларов США;
- NetScreen 25 3 495 долларов США;
- NetScreen 50 5 695 долларов США;
- NetScreen 204 9 995 долларов США;
- NetScreen 208 14 245 долларов США;
- NetScreen 500 22 500 долларов США;
- NetScreen 5200 99 000 долларов США.

Стоимость дополнений для расширения функциональности устройств может существенно повысить необходимые капиталовложения. Например, во время написания данной книги устройства NetScreen IDP (Intrusion Detection and Prevention, обнаружение и предупреждение вторжений) стоили от 7 995 долларов США за ГОР 10 до 34 995 долларов США за ГОР 500. Лицензия для удаленного VPN-клиента NetScreen (v. 8) стоила от 95 долларов США за Ю пользователей, 195 долларов США за 100 пользователей и до 995 долларов США за 1 000 пользователей. VPN-клиент удаленной защиты NetScreen (который также включает в себя персональные брандмауэры для удаленных пользователей) стоил 345 долларов США за 10 пользователей, 2 495 долларов США за 100 пользователей и 19 995 долларов США за 1 000 пользователей.

В табл. 3.2 сравниваются наиболее интересные с точки зрения конкуренции с ISA Server 2004 функции, входящие в популярные модели NetScreen.

Табл. 3.2. Сравнение функций р1азличных моделей NetScreen

Функция	**NetScreen** 200 Series	**NetScreen** 50	**NetScreen 25**	**NetScreen 5XP**
Количество одновременных сеансов	128 000	**а 000**	4 000	2 000
Пропускная способность брандмауэра	400-550 М бит/с	ПО Мбит/с	100 Мбит/с	10 Мбит/с
Пропускная способность VPN с шифрованием 3DES	200 Мбит/с	50 Мlэит/с	20 Мбит/с	10 Мбит/с
Политики	4 000	1 000	500	100
Прозрачный режим (все интерфейсы)	Да	Да	Да	Да
Режим маршрутизации (все	Да	Да	Да	Да
NAT	Да	Да	Да	Да
PAT	Да	Да	Да	Да
Виртуальные IP	4	2	2	1
Отображаемые IP	4 000	1 000	1 000	32
Статические IP-маршруты	256	60	60	16
Выделенные VPN туннели	1 000	100	25	10
Высокая работоспособность	Да	ОС Future-Screen OS	**Нет**	Нет

Все модели устройств NetScreen поддерживают следующие функции:

- Manual key, IKE, проверка подлинности PKI (X.5O9), запросы сертификатов PKCS 7 и 10;
- стандарты шифрования DES, 3DES и AES;
- автоматическая регистрация сертификатов (SCEP);
- источники сертификатов: VeriSign, Microsoft, Entrust, RSA Keon, iPlanet (Netscape), Baltimore, DOD PKI;
- внешние базы данных RADIUS, RSA SecurelD, LDAP.

Брандмауэр ISA Server основан на программном обеспечении и поэтому не привязан к конкретному производителю аппаратного обеспечения. Это дает большую свободу и обеспечивает пропускную способность в зависимости от аппаратной конфигурации, на которой он будет установлен. По результатам тестирования, пропускная способность брандмауэра ISA Server составила до 1,59 Гбит/с. Программное обеспечение не ограничивает число интерфейсов; ISA Server поддерживает столько интерфейсов, сколько допускает существующее аппаратное обеспечение.

Безопасность ОС Windows Server 2003 может быть усилена применением ряда профилей, входящих в служебный пакет Server 2003 SP2 для мастера настройки защиты Security Configuration Wizard. Корпорация Microsoft также предлагает руководство по укреплению системы, которое включает в себя конкретные рекомендации по настройке и **стратегии** применения ISA Server 2004. Этот документ можно скачать с сайта www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx.

NetScreen: поддержка платформы и системные требования

Устройства NetScreen работают на базе патентованной операционной системы ScreenOS, которая, в свою очередь, работает на патентованном аппаратном обеспечении на базе ASIC. Программное обеспечение брандмауэра NetScreen не может быть установлено на базе универсальных компьютерных операционных систем. ОС ScreenOS усилена и оптимизирована для работы с программным обеспечением брандмауэра.

Аппаратные конфигурации моделей NetScreen могут быть различными, как показано в табл. 3.2.

Что касается ISA Server 2004, то этот брандмауэр работает на базе стандартных платформ Intel, которые можно легко модернизировать, и устанавливается на ОС Windows 2000 Server или Windows Server 2003, что обеспечивает стандартный, знакомый интерфейс управления и свободу в выборе аппаратного обеспечения. Это делает ISA Server более масштабируемым, чем устройства, привязанные к аппаратному обеспечению.

NetScreen: возможности фильтрации на уровне приложения

Брандмауэры компании NetScreen обеспечивают технологию «глубинной проверки» для защиты уровня приложения, при которой происходит интеграция обнаружения и предуп реждения вторжений по основным типам атак из Интернета, которые направлены на следующие протоколы:

- HTTP;
- POP3;
- IMAP;
- SMTP;
- FTP;
- DNS.

Компания NetScreen внедрила технологию обнаружения вторжений после покупки OneSecure. Для более сложного обнаружения вторжений NetScreen представляет на рынке отдельный продукт NetScreen IDP, который может использоваться за брандмауэром и перед серверами, предназначенными для решения критически важных задач.

Все модели устройств NetScreen поддерживают Websense (внешнюю службу URL-фильтрации).

В свою очередь ISA Server 2004 выполняет проверку с отслеживанием состояния соединений с помощью интеллектуальных фильтров уровня приложения. Можно не только определить достоверность данных, проходящих через брандмауэр, в заголовках запросов и ответов, но и осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или фильтровать по определенному типу файла. Брандмауэр ISA Server 2004 поддерживает Websense и другие продукты и службы от; сторонних производителей, предназначенные для фильтрации.

ISA Server 2004 проверяет в с е аспекты обмена данными по протоколу HTTP. SMTP-фильтр защищает от неверных SMTP-команд, которые приводят к переполнениям буфера, а средство контроля сообщений SMTP блокирует спам и почту, содержащую опасные вложения. RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC и пропускает к серверу Exchange только достоверные соединения. DNS-фильтрация предотвращает **атаки** на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атаки. SDK ISA Server позволяет с легкостью создавать Web-фильтры и фильтры приложений.

NetScreen: поддержка VPN

Все брандмауэры NetScreen включают поддержку VPN. Они поддерживают патентованное программное обеспечение VPN-клиента NetScreen как в форме удаленного клиента, так и в форме удаленного клиента защиты (последний включает в себя персональные брандмауэры для удаленных пользователей). За лицензию на программное обеспечение VPN-клиента взимается дополнительная плата.

Данные шифруются с помощью стандартов шифрования: 5б-битный DES. 168-битный 3DES или 256-битный AES. NetScreen поддерживает проверку подлинности PKI по сертификату X.509. Сертификаты должны быть получены от сертификационной службы (отдельной системы, работающей на базе специализированной ОС либо во внутренней сети, или общедоступной сертификационной службы типа Verisign).

- NetScreen поддерживает создание VPN-подключений по протоколам IPSec *я* SSL;
- NetScreen поддерживает VPN-подключения удаленного доступа и «узел-в-узел»;
- пропускная способность VPN-подключения зависит от модели устройства (ап паратного обеспечения).

Реализация защиты клиентских компьютеров с помощью брандмауэра выполняется путем применения удаленного клиента защиты NetScreen Remote Security Client (за дополнительную плату), который устанавливает программное обеспечение персонального брандмауэра на клиентском компьютере и выполняет обновления через Интернет. Это обеспечивает выполнение некоторых функций изоли-

рования VPN-подключений. Политики VPN привязаны к учетным записям пользователей, а не к компьютерам. Политики не вступят в силу до тех пор, пока не будет установлено и запущено программное обеспечение брандмауэра.

Что касается ISA Server 2004, он поддерживает пользовательский и групповой контроль доступа, VPN-подключения «узел-в-узел» и удаленного доступа с проверкой и фильтрацией с отслеживанием состояния соединений, что позволяет контролировать трафик, проходящий через VPN-подключения. VPN-подключения подчиняются политикам брандмауэра, как и любое другое подключение; это обеспечивает жесткий контроль используемых протоколов, серверов, с которыми может быть установлено соединение, время суток/продолжительность соединения и IP-адрес, с которого разрешается соединение. Кроме того:

- ISA Server поддерживает сертификаты X.509 для шифрования IPSec-трафика и за ранее определенные ключи для организаций, которые не хотят пользоваться PKI.
- Мастера VPN-подключений ISA Server позволяют легко создавать VPN. ISA Server поддерживает использование набора CMAK для создания VPN-коннектоидов, позволяющих пользователям устанавливать соединение с VPN одним щелчком мыши, а также автоматически загружаемую телефонную книгу. CMAK также позволяет настраивать маршруты для VPN-клиентов. Мастера CMAK облегчают работу администратора и рядового пользователя.
- ISA Server использует технологию Nat Traversal (NAT-T) стандарта IETF RFC про токола L2TP IPSec для установки соединения с VPN на базе Server 2003.
- ISA Server 2004 поддерживает стандарт шифрования 3DES.
- ISA Server 2004 не поддерживает службу VPN QoS, однако QoS имеет ограниченную функциональность за пределами корпоративной сети, потому что каждый про межуточный маршрутизатор должен также ее поддерживать, а вероятность этого низкая.
- ISA Server поддерживает SSL-туннелирование.
- ISA Server 2004 поддерживает клиенты Microsoft PPTP и L2TP.
- ISA Server поддерживает изолирование VPN-подключений посредством функции изолирования в Windows Server 2003 с использованием стандартных клиентов Windows PPTP и L2TP без дополнительной платы.

NetScreen: Web-кэширование

Брандмауэр/устройства VPN от NetScreen не обладают функциями Web-кэши рования. При использовании продуктов NetScreen Web-кэширование/ускорение могут быть добавлены к сети с помощью применения средств кэширования типа ISA Server.

Брандмауэр Server 2004 включает в себя функции Web-кэширования без дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на внешних Web-серверах. Обратное кэширование позволяет брандмауэру ISA Server 2004

кэшировать объекты, к которым обращаются удаленные пользователи на серверах, опубликованных с помощью брандмауэра ISA Server 2004. Web-объекты, запрашиваемые удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, и последующие запросы тех же объектов обрабатываются из Web-кэша брандмауэра без перенаправления запросов на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 держать в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, потому что данные берутся из памяти, а не с диска. ISA Server 2004 предоставляет возможность оптимальным образом сохранять данные в кэше на диске, что минимизирует доступ к диску как для операций чтения, так и для операций записи. ISA Server 2004 также поддерживает создание цепочек Web-прокси, что позволяет брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси (сервер восходящего потока).

Сравнение брандмауэров ISA Server 2004 и SonicWall

По информации International Data Corp., опубликованной агентством новостей CNET News на сайте http://news.com.com/2100-7355-5079045.html, в 2003 г. компания SonicWall занимала четвертое место среди производителей устройств защиты (после Cisco, Netscreen и Nokia). Ее доля на рынке составила 5,4%.

В этом разделе представлен обзор устройств SonicWall. Рассматриваются общие технические требования SonicWall, поддержка платформы и системные требования, возможности фильтрации на уровне приложения, поддержка VPN и Web-кэширования *и* проводится сравнение с ISA Server 2004.

SonicWall: общие технические требования

Брандмауэры/УР1Ч -устройства от SonicWall используют архитектуру ASIC и основаны на технологии проверки с отслеживанием состояния соединений, которая была сертифицирована ICSA. Во время написания данной книги на рынке были представлены следующие устройства от SonicWall:

- SOHO3: для малого бизнеса или филиалов;
- SOHO TZW имеет встроенный беспроводной шлюз;
- TELE3: для удаленных пользователей;
- TELE TZ: для удаленных пользователей; включает в себя архитектуру WorkPort (рабочий порт), которая физически отделяет корпоративную и домашнюю сеть;
- TELE TZX: как и предыдущая модель, включает встроенный четырехпортовый коммутатор MDIX для соединения устройств в нескольких сетях;
- TELE3 SP/TELE3 SPi: для предприятий POS (Point of Sale, с оплатой продаж на месте), с восстановлением после сбоя, рассчитанный на широкополосные и

аналоговые модемные соединения; поддерживает полосу по требованию и управление использованием ISDN-соединения;

- PRO 100: для небольших и крупных предприятий; неограниченное число сете вых узлов; интегрированная сеть периметра (DMZ);
- TZ 170: для небольших предприятий и ИТ-администраторов с ограниченным количеством ресурсов; **включает** встроенный пятипортовый коммутатор MDIX и защищенный процессор (security processor) (system on a chip, система в мик росхеме); основанная на политике технология NAT; дополнительные обновле ния для восстановления после сбоя и выравнивания нагрузки;
- PRO 230: для монтажа в стойке; поддерживает несколько защищенных зон, про верку подлинности на уровне пользователя, управление пропускной способно стью, DHCP-передач и через туннели VPN, автоматические обновления;
- PRO 330: для промышленных сетей; включает высокую работоспособность, га рантированное автоматическое восстановление после сбоя при сочетании с устройством зеркалирования, резервное питание;
- PRO ЗОбО: для сложных сетей; использует операционную систему следующего поколения SonicOS 2.0; дополнительные обновления позволяют добавить функ ции восстановления после аппаратного сбоя, восстановление после сбоя ISP, автоматизированный дополнительный (вторичный) VPN-шлюз; поддерживает аппаратную спецификацию AES; процессор включает в себя выделенный крип тографический акселератор (dedicated cryptographic accelerator); несколько интерфейсов на одной зоне безопасности, основанную на политике техноло гию NAT.
- RPO 4060: брандмауэр промышленного класса с теми же функциями, как и у PRO 3060; включает годовую техническую поддержку 8 часов в день/5 дней в неде лю и текущие обновления программного обеспечения.

В табл. 33 сравниваются технические требования и функции различных моделей SonicWall.

Табл. .3. Сравнение функций различных моделей SonicWall
3

Модел	Процес-сор	RAM	Интер-фейсы	Одновре-менные соедине-ния	Количест-во пользова-телей бранд-мауэра	Пропуск-ная способ-ность бранд-мауэра	Пропуск-ная спо-собность C3DES	VPN-туннели/ политики
SOHO	133 МГц	**16 Мб**	**2 10/100** baseT	**6 000**	10/25/50/ Не ограни-чено	75Мбит/с **(в двух нап-**равлениях)	**20 Мбит/с**	10
SOHO TZW	**1**33 МГц	**16 Мб**	*2* 10/100 baseT	**6** 000	**10/25**	75 Мбит/с **(в** двух **нап-равлениях)**	20 Мбит/с	10
TELE3	133 МГц	**16 Мб**	2 10/100 baseT	**б** 000	**5**	75 Мбит/с (в двух нап-равлениях)	20 Мбит/с	**5**

(см. след. **стр.)**

Табл. 3. (окончание)
3.

Модель	Процессор	НАМ	Интерфейсы	Одновременные соединения	Количество телей мауэра	Пропускная способность брандмауэра	Пропускная способность C3DES	VPN-туннели/политики
TELET	133 МГц	16 Мб	3 10/100 baseT	6 000	5	75 Мбит/с (в двух направлениях)	20 Мбит/с	5
TELE-TZX	133МГц	16 Мб	3 10/100 baseT, четырехпортовый коммутатор	6000	5	75 Мбит/с (в двух направлениях)	20 Мбит/с	5
ШВЗ SP/SPi	133 МГц	16 Мб	2 10/100 baseT, lv.90 1 ISDN	6 000	**10**	75 Мбит/с (в двух направлениях)	20 Мбит/с	10
PRO	1J3 МГц	16 Мб	3 10/100 baseT	6 000	Не ограничено	75 Мбит/с (в двух направлениях)	20 Мбит/с	***50***
TZ **170**	SonicWall Security Processor	64 Мб	7 10/100 baseT	б 000	10/25/Не ограничено	90 Мбит/с (в двух направлениях)	свыше 30 Мбит/с	5-50/2-10 политик для подключений •узел-в-узел»
PRO	233 МГц	64 Мб	3 10/100 baseT	30 000	Не ограничено	190Мбит/с (в двух направлениях)	45 Мбит/с	1 000
PRO	233 МГц Strongar RISC	64 Мб	3 10/100 baseT	128 000	Не ограничено	190 Мбит/с (в двух направлениях)	45 Мбит/с	1000
PRO 3060	2 ГГц Intel	256 Мб	6 10/100 baseT	**128 000**	Не ограничено	более 300 Мбит/с (в двух направлениях)	75 Мбит/с (то же для AES)	500-1 000
PRO 4060	2 ГГц **Intel**	256 Мб	6 10/100 baseT	500 **000**	Не ограничено	более 300 Мбит/с (в двух направлениях)	5 90 Мбит/с (то же для AES)	1000/3 000

Устройства SonicWall имеют различную цену в зависимости от модели и торгового посредника. Во время написания данной книги цены на типичные модели были такими:

- SonicWall SOHO3n 445 долларов США (10 пользователей), 645 долларов США (25 пользователей), 795 долларов США (50 пользователей);

SonicWall TZWn 449 долларов США (10 пользователей), 599 долларов США (25 пользователей);

SonicWall TZ170n 410 долларов США (10 пользователей), 576 долларов США (25 пользователей), 825 долларов США (неограниченное число пользователей);

SonicWall Tele3 TZXn 493 долларов США;

SonicWall ТекЗ SPn 534 доллара США;

SonicWall Pro 230n 1 655 долларов США (неограниченное число пользователей);

SonicWall Pro ЗОбОп 2 319 долларов США (неограниченное число пользователей);

SonicWall Pro 4060m 4 995 долларов США (неограниченное число пользователей).

Цены на дополнения, обновления и услуги для продуктов SonicWall в момент написания книги были следующими:

- VPN для продуктов SonicWall SOHO 410 долларов США;
- SonicWall VPN для PRO 100n 576 долларов США;
- VPN-клиент SonicWall 451 долларов США (10 пользователей), 659 долларов США (50 пользователей), 825 долларов США (100 пользователей);
- дополнение для фильтрации содержимого 75 долларов США (5 узлов), 495 долларов США (50 узлов), 695 долларов США (не ограничено);
- обновление VPN для SOHOn 495 долларов США.

(Источник: http://www.tribecaexpress.com/sonicwall_firewalls_price.htm).

Служба фильтрации содержимого SonicWall (Content Filtering Service, CFS) предполагает оплату за год использования; цена на нее определяется на основании количества узлов. Продукты для неограниченного числа узлов на момент написания данной книги стоили от 695 долларов США за год для стандартной службы до 95 5 долларов в год для устройств PRO 3060 и PRO 4060. (Источник :http://www.somcguard.com/ContentFilteringService.asp).

К другим дополнениям относятся:

- подписка на антивирусное программное обеспечение стоимостью от 136 дол ларов США *в* год для 5 пользователей до 19 195 долларов США в год для 1 000 пользователей;
- система управления Global Management System стоимостью 1 655 долларов США за программное обеспечение и лицензию на 10 узлов; 12 446 за 100 последова тельных лицензий;

- договоры на обслуживание стоимостью от 95 долларов США (SOHO 10 узлов) до 20 749 (GMS с неограниченным количеством узлов).

(Источник: www.tribecaexpress.com/sonicwall_firewalls_price.htm).

SonicWall: поддержка платформы и системные требования

Устройства SonicWall работают на базе специализированных аппаратных устройств на базе ASIC, технические требования к которым показаны в табл. 33. Устройства работают на базе одноцелевой операционной системы SonicOS. В настоящее время есть две версии этой операционной системы;

- SonicOS v.2.0s работает с продуктами низшей ценовой категории и является упрощенной версией операционной системы, в которой используются масте ра для помощи пользователям в задании настроек;
- SonicOS v.2.0e работает с более мощными продуктами (PRO ЗОбО и 4060) и поз воляет определять зоны защиты, для которых можно по отдельности задавать политики безопасности и определять группы пользователей, к которым эти политики будут применяться.

Что касается брандмауэра ISA Server 2004, то он работает на стандартных платформах Intel, которые легко обновляются, и его можно установить на базе ОС Windows 2000 Server или Windows Server 2003 при наличии стандартного, привычного интерфейса управления и возможности использовать аппаратное обеспечение на ваш выбор. Это делает ISA Server более масштабируемым, чем устройства, которые привязаны к аппаратному обеспечению.

ОС Windows Server 2003 может быть укреплена путем применения ряда специальных профилей, входящих в пакет Server 2003 SP2 для мастера Security Configuration Wizard. Корпорация Microsoft также предоставляет руководство по укреплению защиты системы, включающее конкретные рекомендации по конфигурированию *и* стратегии применения ISA Server 2004. Этот документ можно скачать по адресу: http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx.

SonicWall: возможности фильтрации на уровне приложения

Фильтрация содержимого осуществляется с помощью службы фильтрации содержимого SonicWall (Content Filtering Service, CFS), распространяемой на основе подписки. Это означает, что необходимо оплатить стоимость подписки, чтобы воспользоваться функциями глубинной фильтрации Web-контента. URL-рейтинги Web-сайтов и список разрешенных сайтов (согласно определенным администраторюм политикам) кэшируются на локальном устройстве как часть этой службы.

Эта служба поставляется в двух версиях: standard (стандартная) и premium (премиум). Стандартная версия фильтрует только те сайты, которые есть в базе данных. Премиум-версия также анализирует страницы, которых нет в базе данных, и добавляет их в базу. Есть также специальные версии этой службы, предназначенные для правительственных и учебных учреждений.

Стандартная версия CFS фильтрует Web-контент на основании 14 предопределенных категорий:

- Violence (жестокость);
- Hate/racism (ненависть/расизм);
- Intimate apparel (интимная одежда)
- Nudism (нудизм);
- Pornography (порнография);
- Weapons (оружие);
- Adult/mature content (только для взрослых);
- Cult/occult (культ/оккультизм);
- Illegal drugs (запрещенные законом лекарства);
- Drugs (наркотики);
- Criminal skills (преступные навыки);
- Sex education (половое воспитание);
- Gambling (азартные игры);
- Alcohol/tobacco (алкоголь/курение).

В премиум-версии добавлены дополнительные категории типа Abortion (аборты), Arts/Entertainment (искусство/развлечения), Auctions (аукционы); Brokerage/Trading (маклерство/коммерция), Humor/Jokes (юмор/шутки), News/Media (новости/средства массовой информации); Personal/Dating (общение/знакомства); Religion (религия); Streaming Media/MP3 (потоковые данные/MP3), Software Downloads (загрузка программного обеспечения) и многие другие (всего 52 категории).

Премиум-версия работает только на базе продуктов SonicWall четвертого поколения и требует улучшенной ОС SonicOS. CFS не работает с более старыми продуктами SonicWall первого поколения, но ее предшественник SonicWall Content Filter List (CFL) может использоваться для более старых моделей.

Что касается ISA Server 2004, то он включает в себя глубинную фильтрацию на уровне приложения без дополнительной платы. Однако ISA Server 2004 также может использовать Websense или другие продукты и службы сторонних производителей по желанию пользователя.

> ПРИМЕЧАНИЕ При настройке фильтров для различного типа содержимого и Web-сайтов нужно учесть расходы на администрирование и обеспечение качества функционирования фильтров. В случае, если наилучшим выбором является служба по подписке, ISA Server 2004 также может обеспечить фильтрацию содержимого с помощью службы по подписке типа Websense.

ISA Server 2004 выполняет проверку с отслеживанием состояния соединений с использованием интеллектуальных прикладных фильтров. Можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запро-

са и ответа, но и осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или отфильтровывать определенные типы файлов.

ISA Server 2004 проверяет все аспекты HTTP-соединений. SMTP-фильтр защищает от неверных SMTP-команд, которые вызывают переполнение буфера, а средство контроля SMTP-сообщений блокирует спам и почту, содержащую опасные вложения.

RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC, и пропускает через сервер Exchange только законные соединения. DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак.

Для выполнения фильтрации на уровне приложения ISA Server не требуется служба по подписке за дополнительную плату.

SonicWall: поддержка VPN

Устройства SonicWall включают поддержку VPN. Модели PRO поддерживают от 500 до 3 000 одновременных VPN-туннелей. Устройства SonicWall поддерживают VPN-подключения по протоколам IPSec и PPTP.

SonicWall использует патентованный VPN-клиент VPN Client 8.0 (за дополнительную плату), который необходим для автоматической поддержки сертификатов, L2TP и для доступа к VPN-шлюзу с применением сервисов разрешения имен DNS, WINS и LMHOST вместо IP-адресов.

Средство поддержки клиентов SonicWall Client Policy Provisioning позволяет клиентам автоматически загружать конфигурационные данные VPN-клиента с VPN-шлюза с патентованным клиентом Global VPN Client.

В момент написания этой книги устройства SonicWall предлагались вместе с лицензиями на ограниченное количество VPN-клиентов в зависимости от модели, как показано в приведенном далее списке:

- SOHO TZW — 1 пользователь;
- T2 1 7 0 — 1 пользователь;
- PRO 2040 — 10 пользователей;
- PRO 306 — 25 пользователей;
- PRO 406 — 1 000 пользователей.

Если количество пользователей VPN превышает это число, то можно купить дополнительные лицензии.

В некоторые модели не входят лицензии для VPN-клиентов, а именно: я

TELE3;

- TELE3TZ;
- TELE3TZX;

- TELE3SP;
- SOHO3 Ю узлов;
- SOHO3 25 узлов;
- SOHO3 50 узлов;
- TZ 170 10 узлов.

В ISA Server 2004 число одновременных VPN-подключений зависит от операционной системы и составляет от 1 000 (Standard Edition) до более 1б 000 PPTP-подключений и 30 000Ь2TP-подключений (Enterprise edition, Datacenter edition) в зависимости от операционной системы, на которой он установлен. Кроме того, ISA Server поддерживает VPN-подключен ия по протоколу IPSec для подключений «узел-в-узел», а также протоколы PPTP и более безопасный L2TP для подключений удаленного доступа. ISA Server может применять политику брандмауэра к VPN-интерфейсам.

Брандмауэр ISA Server не требует для своих VPN-клиентов никакого дополнительного программного обеспечения. ISA Server поддерживает VPN-клиенты PPTP и L2TP/IPSec, встроенные в ОС Windows 9x/ME, Windows XP, Windows NT, 2000 и Server 2003- За VPN-клиенты не нужно дополнительно платить.

Изолирование VPN-подключений ISA Server позволяет администраторам устанавливать определенные условия, которым должны удовлетворять VPN-клиенты, прежде чем им будет разрешено устанавливать соединение (например, должны быть установлены самые последние пакеты служебных программ/обновлений), и направлять клиенты на сервер, чтобы загрузить и установить необходимые обновления. Функция изолирования VPN-подключений является функцией Windows Server 2003, и она позволяет вам блокировать VPN-доступ, если клиент не удовлетворяет предопределенным критериям конфигурации, включая установку текущих служебных пакетов и обновлений, антивирусных программ и брандмауэра. Для использования этой функции не нужно никакое патентованное клиентское программное обеспечение, и ее можно применять к любому количеству клиентов, определяемому возможностями операционной системы.

SonicWall: Web-кэширование

Продукты компании SonicWall не включают в коробочную версию Web-кэширование. Однако если подписаться на службу фильтрации содержимого Согнет Filtering Service (CFS), то разрешенные Web-сайты — которые были определены политиками и проверены по базе данных CFS — кэшируются на локальном устройстве для более быстрого отклика.

Что касается ISA Server 2004, в него включена функция Web-кэширования без отдельной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на внешние Web-серверы. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи на серверы,

которые были опубликованы с помощью брандмауэра ISA Server 2004. Web-объекты, запрошенные удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 сохранять в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, т. *к.* объекты берутся из памяти, а не с диска. ISA Server 2004 позволяет сохранять данные в кэше на диске, что сводит к минимуму доступ к диску как для операций записи, так и для операций чтения. ISA Server 2004 также поддерживает создание цепочек Web-прокси, позволяющих брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси.

Сравнение брандмауэров ISA Server 2004 и WatchGuard

Согласно информации, предоставленной International Data Corp. и опубликованной агентством новостей CNET News на сайте http://news.com.com/2100-7355-5079045.html, компания WatchGuard занимала пятое место (после Cisco, NetScreen, Nokia и SonicWall) среди производителей устройств защиты в 2003 г. Ее доля на рынке составляла 4%.

Watchguard: общие технические требования

Во время написания данной книги компания Watchguard предлагала следующие модели устройств:

- SOHO 6: разработана для малых предприятий и удаленных офисов; обеспечи вает фильтрацию пакетов с отслеживанием соединений и возможности VPN;
- Firebox X: разработана для небольших и средних предприятий; имеет возмож ности масштабирования;
- Firebox Vclass: разработана для средних предприятий; поддерживает высокоско ростные соединения по сети и улучшенные сетевые функции.

Сравнение функций различных моделей устройств WatchGuard показано в табл. **34.**

Табл. 3.4. Сравнение различных моделей WatchGuard

Функция	Firebox X	SOHO 6	Firebox Vc las s
Пропускная способ- ность брандмауэра	до 275 Мбит/с	До 75 Мбит/с	До 2 Гбит/с
Пропускная способ- ность VPN	до 100 Мбит/с	До 20 Мбит/с	До 1,1 Гбит/с
Одновременные сеансы	500 000	7 000	500 000

Табл. 3.4. (окончание)

Фун1ция	Firebox X	SOHO6	Firebox Vclass
Интс:рфейсы	6 10/100 (3 активных)	6 10/100	V200, VI00: 2 lOOOBaseSX Fiber Gegabit Ethernet, 2 Dedicated HA V80, V60, V60L4 10/100 2 Dedicated HA VI0: 2 10/100
VPN-•туннели	До 1 000	До 10	До 40 000
ALF	HTTP, SMTP, FTP, DNS, H.323, DCE-RPC, RTSP, http	HTTP	SMTP, HTTP
Фил]^грация спама	Дополнительная функция	Нет	Нет
URL-фильтрация	Дополнительно	Дополнительно	Нет
Выажая работоспо-собиюсть	Активная/ пассивная	Нет	Акт вн:1я /11 ;тссii иная
QoS	Нет	Нет	Да
Лиц(;нзии для мобильных VP N •по л ьзо вател е й	До 1 000	До 10 (дополни тел ь н о)	До 20
Сре;1ства диагнос-тики сети	Нет	Нет	Да
Инт(:рфейс команд-ной строки	Нет	Нет	Да
Мониторинг в режиме реального времени	Да	Нет	Да
Регистрация предыстории	Да	Нет	Нет
Возможность обновления	С марта 2004 г.	Обновление с 10 до 25 или 50 пользователей	V60L обновляется floV60

Далее приводятся цены на различные модели WatchGuard Firebox, действительные в момент написания данной книги:

- SOHO 6 / 1 0 пользователей — 549 долларов США;
- SOHO 6 / 5 0 пользователей — 899 долларов США;
- Firebox III 700/ 250 пользователей — 2 490 долларов США;
- Firebox III 2500/ 5 000 пользователей — 5 790 долларов США;
- Firebox VI0 / неограниченное число пользователей (20/75 Мбит/с) — 799 дол ларов США;

- Firebox V60 / неограниченное число пользователей (100/200 Мбит/с) — 599 долларов США;
- Firebox V80 / неограниченное число пользователей (150/200 Мбит/с) — 8 490 долларов США;
- Firebox VI00 / неограниченное число пользователей (300/600 Мбит/с) — 14 490 долларов США.

Дополнительные пользовательские лицензии можно получить для SOHO и Firebox V10 (коробочная версия поддерживает 10 пользователей). Программное обеспечение VPN Manager необходимо для более чем одного VPN-узла в следующих моделях SOHO:

- 4 узла Fireboxesn — 796 долларов США;
- 20 узлов Fireboxesn — 2 796 долларов США;
- неограниченное число Fireboxesn — 6 396 долларов США.

Стоимость программного обеспечения для VPN-клиента составляет:

- 5 пользователей — 220 долларов США;
- 50 пользователей — 1 800 долларов США.

Стоимость программного обеспечения VPN-клиента Vclass MU составляет:

- 100 пользователей — 780 долларов США;
- 1 000 пользователей — 1 440 долларов США.

Менеджер централизованной политики Centralized Policy Manager (CPM) используется для нескольких устройств Vclass. Стоимость CPM для Windows NT/2000 составляет:

- 10 устройств — 2 840 долларов США;
- 100 устройств — 12 680 долларов США.

(Информация о ценах на продукцию WatchGuard взята с сайта http://www.securehq.com/group.wml&storeid=l&deptid=76&groupid=222&sessionid= 200437249417233).

WatchGuard: поддержка платформы и системные требования

Устройства компании WatchGuard работают на базе патентованной операционной системы и программного обеспечения брандмауэра (Security Management System), которую можно сконфигурировать тремя способами:

- InternetGuard: обеспечивается защита корпоративных сетей и хост-бастионов и определяется безопасность уровня предприятия;

м GroupGuard: обеспечивается защита систем отделов, ограничивается поток информации и пакетов, определяются уровни привилегированности при работе с Интернетом на групповом уровне;

- HostGuard: обеспечивается защита конкретных серверов.

Брандмауэр ISA Server 2004 работает на стандартных платформах Intel, которые легко обновляются, и его можно установить на базе ОС Windows 2000 Server или Windows Server 2003 при наличии стандартного, привычного интерфейса управ-

ления и возможности использовать аппаратное обеспечение на любой выбор. Это делает ISA Server более масштабируемым, чем устройства, привязанные к аппаратному обеспечению.

ОС Windows Server 2003 может быть укреплена путем применения ряда специальных профилей, входящих в пакет Server 2003 SP2 для мастера Security Configuration Wizard. Корпорация Microsoft также предоставляет руководство по укреплению защиты системы, которое включает конкретные рекомендации по конфигурированию и стратегии применения ISA Server 2004. Этот документ можно скачать по адресу: http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx.

WatchGuard: возможности фильтрации на уровне приложения

Модели WatchGuard Firebox (за исключением более дешевых моделей — SOHO и VI0) поддерживают прокси уровня приложения, которые блокируют основные типы атак уровня приложения. Можно задать правила протоколов для протоколов HTTP, FTP и SMTP. Firebox III модели 500, 700, 1000, 2500 и 4500 и Firebox Vclass модели V60L, V60, V80, V100 и V200 поддерживают следующие типы прокси:

- SMTP. Проверяет содержимое входящих и исходящих сообщений электронной почты, запрещает исполняемые вложения, выполняет фильтрацию по адресу, фильтрует неправильные заголовки, поддельные (spoofed) имена доменов и ID сообщений, определяет максимальное число получателей сообщения и макси мальный размер сообщения, разрешает определенные символы в адресах элек тронной ПОЧТЫ;
- HTTP. Блокирует Web-трафик на всех портах, кроме 80, фильтрует содержимое типа MIME, Java, ActiveX, удаляет незнакомые заголовки, удаляет cookies, фильт рует содержимое в соответствии с политиками;
- FTP. Фильтрует FTP-команды сервера, использует правила только для чтения, чтобы контролировать изменения в файлах, устанавливает ограничение по вре мени для бездействующих соединений;
- DNS. Проверяет неправильные заголовки и пакеты, фильтрует содержимое за головков по несоответствию классу, типу и длине;
- H.323. Ограничивает открытые порты.

Брандмауэры Vclass обеспечивают встроенное обнаружение вторжений, настраиваемое создание журналов и оповещений для следующих типов атак: ш блокирование сценариев Java (Java script blocking);

- IP source route (попытка вторжения с использованием IP-опции «маршрут от правителя»;
- отказ от обслуживания (DoS);
- распределенная атака DoS (DDOS, Distributed Denial of Service);
- Ping of Death (попытка послать пакет, длина которого больше теоретического предела 65536 байтов);

- затопление системы ICMP (ICMP flood);
- синхронная атака на TCP (TCP SYN flood);
- затопление UDP (UDP flood).

Автоматические журналы встроены в ASIC для обнаружения следующих атак:

- атака с обратной адресацией (LAND);
- Teardrop;
- NewTear;
- OpenTear;
- Overdrop;
- Jolt2;
- SSPING;
- Bonk/Boink;
- Smurf;
- Twinge.

В свою очередь механизм обнаружения вторжений ISA Server 2004 может обнаруживать следующие типы атак:

- атака передачи внешних данных в Windows (Windows out-of-band, WinNuke);
- атака с обратной адресацией (LAND);
- Ping of death;
- IP-атака без создания подключения (IP half scan);
- UDP-бомбы;
- сканирование портов (port scan);
- переполнение буфера имен узлов в DNS (DNS host name overflow);
- переполнение буфера номер узла в DNS (DNS length overflow);
- зонная передача в DNS (DNS zone transfer);
- переполнение буфера POP3 (POP3 buffer overflow);
- переполнение буфера SMTP (SMTP buffer overflow).

ISA Server включает в себя глубинную фильтрацию на уровне приложения без дополнительной платы. ISA Server 2004 выполняет проверку с отслеживанием состояния соединений с применением интеллектуальных фильтров приложения. Можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запросов и ответов, но также осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или по определенным типам файлов. ISA Server 2004 также может работать вместе с WebSense и другими фильтрами сторонних производителей.

ISA Server 2004 проверяет все аспекты обмена HTTP-сообщениями. SMTP-фильтр ISA Server защищает от неверных SMTP-команд, которые приводят к переполнению буфера, а средство контроля сообщений SMTP блокирует спам и почту, содержащую опасные вложения.

RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC, и пропускает к серверу Exchange только проверенные соединения.

DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак.

WatchGuard: поддержка VPN

Количество VPN-туннелей и пропускная способность VPN для моделей WatchGuard Firebox сильно зависят от модели. Устройства низшей ценовой категории (SOHO, Firebox III 700, Firebox V10) поддерживают небольшое количество VPN-клиентов или не поддерживают их вообще. Поддержка VPN для различных моделей показана в табл. 3-5.

Табл. 3.5. Сравнение поддержки VPN с различными моделями WatchGuard

Модель	Пропускная способность **VPN**	Максимальное количество VPN-клиентов	Количество VPN-клиентов, подключенных бесплатно	Количество VPN-узлов
SOHO6	20 Мбит/с	5	0	1/5
Firebox III 700	5 Мбит/с	150	0	1000
Firebox III 2500	75 Мбит/с	1 000	50	1 000
Firebox VI0	20 Мбит/с	0	0	10
Firebox V60	100 Мбит/с	400[1]	20	400[1]
Firebox V80	150 Мбит/с	8 000[1]	20	8 000[1]
Firebox VI00	300 Мбит/с	20 000'	20	20 000'

Общее количество соединений типа клиент плюс узел

Firebox V80, промышленный брандмауэр WatchGuard, поддерживает следующие VPN-протоколы:

- IPSec with IKE;
- L2TP over IPSec для внешних Ь2ТР-серверов;
- PPTP over IPSec для внешних PPTP-серверов;
- IPSec Security Services;
- туннельный и транспортный режим (Tlinnel and Transport Mode);
- ESP (Encapsulated Security Payload, протокол инкапсулирующей защиты содер жимого);
- AH (Au thentication Header, заголовок аутентификации);
- AH + ESP;
- шифрование и проверка подлинности для IPSec;
- DES и 3DES;

- MD5 и SHA-1;
- RSA;
- DSS (Digital Signature Standard, стандарт цифровой подписи);
- Certificate Management;
- автоматический список аннулированных сертификатов (CRL) через LDAP-сервер;
- цифровые сертификаты X.509 v2 and v3, PKCS #10, and PKCS *7.

Для моделей WatchGuard Firebox требуется патентованный VPN-клиент Mobile User, который должен быть установлен, наряду с политикой настройки безопасности (security configuration policy), на каждом клиентском компьютере. VPN-клиент включает в себя программное обеспечение персонального брандмауэра для клиентского компьютера.

В брандмауэре ISA Server 2004 мастера VPN-подключений ISA Server позволяют легко создавать VPN. ISA Server поддерживает использование набора CMAK для создания VPN-коннектоидов, которые позволяют пользователям устанавливать соединение с VPN одним щелчком мыши, а также автоматически загружаемую телефонную книгу. CMAK также позволяет настраивать маршруты для VPN-клиентов. Мастера CMAK облегчают работу администратора и рядового пользователя.

ISA Server использует технологию Nat Traversal (NAT-T) стандарта IETF RFC протокола L2TP IPSec для установки соединения с VPN на базе Server 2003.

ISA Server 2004 поддерживает VPN-подключения удаленного доступа и «узел-в-узел». ISA Server может применять политику брандмауэра к VPN-интерфейсам.

ISA Server 2004 поддерживает клиенты Microsoft PPTP и L2TP. ISA Server не требует добавления к VPN-клиентам никакого программного обеспечения. ISA Server поддерживает VPN-клиенты PPTP и L2TP/IPSec, встроенные в ОС Windows 9x/ME, Windows XP, Windows NT, 2000 и Server 2003.

Изолирование VPN-подключений ISA Server позволяет администраторам устанавливать определенные условия, которым должны удовлетворять VPN-клиенты, прежде чем им будет разрешено устанавливать соединение (например, должны быть установлены самые последние пакеты служебных программ/обновлений, должны быть установлены и активированы антивирусные программы и персональные брандмауэры), и направлять клиенты на сервер, чтобы загрузить и установить необходимые обновления. Это превышает возможности VPN-клиента Mobile User от WatchGuard, который обеспечивает применение и обновление программного обеспечения брандмауэра.

WatchGuard: Web-кэширование

Устройства WatchGuard не включают функции Web-кэширования. Web-кэширование/ускорение можно добавить к сети с помощью продуктов WatchGuard и с применением такого устройства кэширования, как ISA Server.

Брандмауэр ISA Server 2004 включает в себя функции Web-кэширования без какой-либо дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на внешние Web-серверы. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи на серверы, которые были опубликованы с помощью брандмауэра ISA Server 2004. Web-объекты, запрошенные удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 сохранять в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, т. к. объекты берутся из памяти, а не с диска. ISA Server 2004 позволяет сохранять данные в кэше на диске, что сводит к минимуму доступ к диску как для операций записи, так и для операций чтения. ISA Server 2004 также поддерживает создание цепочек Web-прокси, позволяющих брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси.

Сравнение брандмауэров ISA Server 2004 и промышленного брандмауэра Symantec

Компания Symantec широко известна благодаря распространенному антивирусному программному обеспечению Norton и обширной базе данных вирусов, предлагаемой в Интернете. Компания объявила о 31% росте доходов за третий квартал с датой окончания 02 января 2004 г. В общей доле доходов 51% составили средства обеспечения безопасности предприятий, администрирование и службы. (Щеточник: http://www.symantec.com/press/2004/n040121.html.)

Компания Symantec представляет на рынке брандмауэры/устройства VPN низшей ценовой категории класса SOHO, решения для малого бизнеса и удаленных пользователей, а также средства безопасности (шлюзы) для предприятий, которые выполняют фильтрацию на уровне приложения, обеспечивают централизованное управление и высокую работоспособность. Компания Symantec также предлагает брандмауэр на базе программного обеспечения, который работает на базе ОС Windows и Solaris.

В этом разделе представлен обзор программного обеспечения брандмауэра Symantec. Рассматриваются общие технические требования Symantec, поддержка платформы и системные требования, возможности фильтрации на уровне приложения, поддержка VPN и возможности Web-кэширования в сравнении с ISA Server 2004.

Symantec: общие технические требования

Брандмауэры/устройств а VPN от Symantec, которые были представлены на рынке во время написания данной книги, можно разбить на три основные категории, как показано в табл. 3.6.

Табл. 3.6. Категории брандмауэров/устройств **VPN от** Symantec

Брандмауэр/устройство VPN (небольшой /удаленный офис)	Устройства защиты (шлюзы) промышленного уровня	Брандмауэр/устройство VPN (промышленный уровень)
Symantec Firewall/VPN 100	SGS 5420	Symantec Enterprise Firewall
Symantec Firewall/VPN 200	SGS 5440	
Symantec Firewall/VPN 200R	SGS 5460	

В табл. 3-7 показаны ключевые функции брандмауэра/устройств а VPN от Symantec для небольших/удаленных офисов, представленные во время написания данной книги.

Табл. 3.7. Сравнение моделей брандмауэров/устройств VPN от Symantec для небольших/удаленных офисов

Функция	Firewall/VPN **100**	Firewall/VPN **200**	**Firewall/ VPN** 200R
Функции брандмауэра по проверке с отслеживанием соединений	**Да**	**Да**	
Обнаружение вторжений	**Да**	Да	Да
VPN-подключения удаленного доступа	**Нет**	**Нет**	Да
VPN-подключен и я «шлюз-шлюз»	Да	Да	Да
Встроенный VPN-клиент	**Нет**	Нет	Да
VPN-подключения по протоколу IPSec	Да	Да	Да
Интерфейс DSL/кабельный интерфейс	Да	Да	Да
Интерфейс T-1/ISDN	Да	Да	Да
Поддержка PPPoE	**Да**	Да	Да
LAN 10/100 порты	4	8	8
WAN порты	1	2	2
Выравнивание нагрузки	**Нет**	Да	Да
Количество пользователей (р е коме н дуется)	**15-25**	30-40	30-40
Восстановление после сбоя	Подключение по телефонной линии через внешний модем	Подключение по телефонной линии через внешний модем	Подключение по телефонной линии через внешний модем
Конфи гури рован и е	Web-интерфейс	Web-интерфейс	Web-интерфейс

Табл. 3.7. (окончание)

Функция	Firewall/VPN100	Firewall/VPN 200	Firewall/ VPN 200Й
Процессор	ARM7	ARM7	ARM7
Производительность WAN (в обоих направлениях)	8 Мбит/с	8 Мбит/с	8 Мбит/с
Web-кэширование	Нет	Нет	Нет
Фильтрация содержимого на уровне приложения	Нет	Нет	Нет
Встроенный DHCP-сервер	Да	Да	Да
NAT	Да	Да	Да

Современные устройства безопасности (шлюзы) Symantec для предприятий во время написания данной книги выходили в серии 5400 (SGS 5430, SGS 5440, SGS 5460). В табл. 3-8 представлено сравнение функций трех устройств защиты (шлюзов) для предприятий.

Табл. 3.8. Сравнение различных моделей устройств защиты (шлюзов) промышленного уровня от Symantec

Функция	SGS 5420	SGS 5440	SGS 5460
Функции брандмауэра по проверке с отслеживанием соединений	Да	Да	Да
WAN порты	6	б	8
Порты 10/100	6	0	0
Порты Gigabit	0	б	8
Максимальное количество узлов (рекомендуетс я)	500	2 500	4 500
Одновременные соединения	64 000	190 000	200 000
Пропускная способность с отслеживанием соединений	200 Мбит/с	1,4 Гбит/с	1,8 Гбит/с
Скорость проверки (Full inspection)	95 Мбит/с	680 Мбит/с	730 Мбит/с
VPN W/3DES	90 Мбит/с	400 Мбит/с	600 Мбит/с
VPN w/AES	30 Мбит/с	80 Мбит/с	90 Мбит/с
Память	520 Мб	1 Гб	2 Гб
Емкость жесткого диска	40 Гб	80 Гб	80 Гб
Обнаружение вторжений на базе подписей (signature-based)	Да	Да	Да
Совместимость VPN с IPSec	Да	Да	Да
Проверка на уровне приложения	Да	Да	Да
Фильтрация HTTP-с одержим ого	Да	Да	Да
We b-кэширование	Нет	Нет	Нет
Защита от спама	Да	Да	Да

Symantec представляет на рынке два пакета программного обеспечения, которые разработаны под ОС Windows NT/2000 или Solaris: Symantec Enterprise Firewall и Symantec Enterprise VPN. Во время написания данной книги текущей версией была версия 7.0. Symantec Enterprise Firewall прошел сертификацию ICSA.

Это программное обеспечение является основой для устройств защиты промышленного уровня (шлюзов). Пакет Symantec Enterprise Firewall 7.0 включает в себя:

- брандмауэр гибридного типа;
- *ш* глубинную проверку пакетов;
- прокси уровня приложения;
- автоматическое укрепление системы;
- широкий набор методов проверки подлинности (RADIUS, LDAP, цифровые сертификаты, S/Key, Defender, SecurelD, доменная проверка подлинности Windows);
- интегрированную фильтрацию Web-контента;
- интегрированное выравнивание нагрузки;
- сертификацию EAL-4;
- поддержку AES;
- NAT для входящего и для исходящего трафика как по VPN-подключениям, так и без них;
- URL-фильтрацию WebNOT.

Пакет Symantec Enterprise VPN включает в себя следующие возможности:

- поддержку VPN-подключений по протоколу IPSec; способность работать с другими VPN-клиентами и серверами, совместимыми с IPSec;
- работает независимо от брандмауэра и интегрируется в сетях с брандмауэрами сторонних производителей;
- одношаговое конфигурирование и подключение;
- удаленное централизованное управление большими группами устройств.

Стоимость брандмауэров/устройств VPN от Symantec для небольших или удаленных офисов во время написания этой книги составляла:

- Symantec Firewall/VPN 100 — 499 долларов США;
- Symantec Firewall/VPN 200 — 899 долларов США;
- Symantec Firewall/VPN 200R — 1 199 долларов США.

Стоимость устройств защиты (шлюзов) промышленного уровня от Symantec во время написания данной книги показана в приведенном далее списке. Эти цены включают базовую лицензию (брандмауэр на 50 узлов, одна VPN-сессия от ктиента к шлюзу).

- Symantec SGS 5420 — 2 999,99 долларов США;
- Symantec SGS 5440 - 6 899,98 долларов США;
- Symantec SGS 546О - 11 534,98 долларов США.

Базовая лицензия рассчитана на брандмауэр с 50 узлами, неограниченное количество VPN-подключений шлюз-шлюз и одну VPN-сессию от клиента к шлюзу. Базовая лицензия также включает в себя техническую поддержку в течение года по схеме Gold Maintenance, обновления определений вирусов, типов атак и URL-фильтрации с помощью LiveUpdate.

Само устройство содержит все поддерживаемые функции защиты, но на некоторые из функций защиты, включая следующие, должна быть получена отдельная лицензия:

- дополнительный модуль Event Manager, предназначенный для централизованного создания журналов, оповещений и отчетов;
- дополнительный модуль Advanced Manager (включающий в себя Event Manager), предназначенный для централизованного управления наборами правил и политиками безопасности;
- дополнительные функции высокой работоспособности и выравнивания нагрузки;
- дополнительный расширенный набор антивирусных средств;
- дополнительные гибридные наборы средств для предупреждения и обнаружения вторжений (мониторинг в режиме реального времени, обнаружение и предупреждение с помощью обнаружения отклонений в работе протоколов и атак);
- дополнительные одновременные VPN-сессии.

Symantec: поддержка платформы и системные требования

Модель SGS основана на брандмауэре Raptor, на системе обнаружения вторжений Recourse IDS (Intrusion Detection System) и на антивирусном программном обеспечении Symantec. Версия программного обеспечения Symantec Enterprise Firewall работает с ОС Windows NT/2000 или Solaris. Компьютеры с ОС Windows требуют наличия процессора PIII с частотой 400 МГц, 256 Мб RAM и 8 Гб свободного пространства на диске. Для компьютеров с ОС Solaris требуется Solaris 7 или 8, шина Sun UltraSPARC I или II sbus или шина PCI, 256 Мб RAM и 8 Гб свободного пространства на диске.

Брандмауэр ISA Server 2004 работает на стандартных платформах Intel, которые легко обновляются, и его можно установить на базе ОС Windows 2000 Server или Windows Server 2003 при наличии стандартного, привычного интерфейса управления и возможности использовать аппаратное обеспечение на ваш выбор.

Безопасность ОС Windows Server 2003 может быть усилена путем применения ряда специальных профилей, входящих в пакет Server 2003 SP2 для мастера Security Configuration Wizard. Корпорация Microsoft также предоставляет руководство по укреплению защиты системы, которое включает конкретные рекомендации по конфигурированию и стратегии применения ISA Server 2004. Этот документ можно скачать по адресу: http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx.

Symantec: возможности фильтрации на уровне приложения

Symantec обеспечивает фильтрацию уровня приложения для обнаружения втсржений, защиты HTTP и SMTP/POP3 и для FTP-фильтрации (защиты от вирусов и этак). В брандмауэре используется продукт ManHunt (который Symantec купила у Recourse Technologies) для IDS. Утилита ManHunt пассивно выполняет обнаружение вторжений или активно блокирует конкретные типы атак. Symantec использует фильтрацию содержимого WebNot для контроля URL-трафика. Фильтрация для защиты от спама также продается в виде отдельной дополнительной функции.

В брандмауэре ISA Server 2004 встроенная функция обнаружения вторжений проверяет протоколы HTTP, POP3, ШАР, SMTP, FTP и DNS. ISA Server 2004 выполняет проверку с отслеживанием состояния соединений с применением интеллектуальных прикладных фильтров. Можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запросов и ответов, но также осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или по определенным типам файлов.

ISA Server 2004 проверяет все аспекты обмена HTTP-сообщениями. SMTP-фильтр ISA Server защищает от неверных SMTP-команд, которые приводят к переполнению буфера, а средство контроля сообщений SMTP блокирует спам и почту, содержащую опасные вложения. DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак.

С самого начала ISA Server был создан для выполнения фильтрации на уровне приложения, а SDK ISA Server позволяет легко создавать Web-фильтры и фильтры приложения.

Symantec: поддержка VPN

Symantec Enterprise VPN 7.0 работает на базе ОС Windows NT/2000 и Solaris *7/8* и включается в устройства Enterprise Gateway (шлюзы предприятия). VPN-клиент Symantec Enterprise работает на базе ОС Windows 9x, ME, 2000, NT 4.0 и XP. Программное обеспечение Enterprise VPN интегрировано с программным обеспечением Enterprise Firewall в устройствах защиты от Symantec.

Symantec Enterprise VPN включает в себя:

- поддержку VPN-подключений по протоколу IPSec, способность работать с дру гими VPN-клиентами и серверами, совместимыми с IPSec;
- работу независимо от брандмауэра и интеграцию в сети с брандмауэрами сторонних производителей;
- конфигурирование и подключение за один шаг;
- удаленное централизованное управление большими группами устройств.

VPN-клиент промышленного уровня включает программное обеспечение персонального брандмауэра; удаленные политики создают файл самонастройки для клиентов, а VPN-сервер выполняет сканирование VPN-подключений.

8 ISA Server 2004 число одновременных VPN-подключений зависит от операционной системы и составляет от 1 000 (Standard Edition) до более 16 000 PPTP-подключений и 30 000 Ь2ТР-подключений (Enterprise edition, Datacenter edition). ISA Server поддерживает VPN-подключения по протоколу IPSec для подключений «узел-в-узел», а также протокол PPTP и более безопасный протокол L2TP для подключений удаленного доступа. ISA Server может применять политику брандмауэра к VPN-интерфейсам.

ISA Server не требует для своих VPN-клиентов никакого дополнительного программного обеспечения. ISA Server поддерживает VPN-клиенты PPTP и L2TP/IPSec, встроенные в ОС Windows 9x/ME, Windows XP, Windows NT, 2000 и Server 2003.

Изолирование VPN-подключений ISA Server позволяет администраторам устанавливать определенные условия, которым должны удовлетворять VPN-клиенты, прежде чем им будет разрешено устанавливать соединение (например, должны быть установлены самые последние пакеты служебных программ/обновлений), и направлять клиенты на сервер, чтобы загрузить и установить необходимые обновления.

Функция изолирования VPN-подключений является функцией Windows Server 2003 и позволяет блокировать VPN-доступ, если клиент не удовлетворяет предопределенным критериям конфигурации, включая установку текущих служебных пакетов и обновлений, антивирусных программ и брандмауэра. Для использования этой функции не нужно никакое патентованное клиентское программное обеспечение, и ее можно применять к любому количеству клиентов, определяемому возможностями операционной системы.

Symantec: Web-кэширование

Брандмауэры Symantec не выполняют Web-кэширования. Для реализации этих функций в сети нужно использовать отдельное устройство или средства Web-кэширования от сторонних производителей.

В ISA Server 2004 включена функция Web-кэширования без дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на внешние Web-серверы. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи на серверы, которые были опубликованы с помощью брандмауэра ISA Server 2004. Web-объекты, запрошенные удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 сохранять в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, т. к. объекты берутся из памяти, а не с ДИСКГ.. ISA Server 2004 позволяет сохранять данные в кэше на диске, что сводит к минимуму доступ к диску как для операций записи, так и для операций чтения. ISA Server 2004 также поддерживает создание цепочек Web-прокси, позволяющих брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси.

Сравнение брандмауэров ISA Server 2004 и Blue Coat SG

Компания Blue Coat Systems является одним из немногих конкурентов ISA Server, представляющих на рынке брандмауэр с интегрированным Web-кэшированием. Первоначально она была известна под названием CacheFlow, а в 2002 г. компания сменила свое название и заинтересовалась рынком средств защиты. По данным с Web-сайта компании, она насчитывает более 3 000 клиентов и более 14 000 реализованных по всему миру устройств, причем в числе ее клиентов состоят более 70% компаний из списка промышленных компаний Dow-Jones Industrial companies. Согласно данным IDC, компания Blue Coat занимает 33% рынка средств рабсты с содержимым, что позволяет ей быть первой в этой области. Устройства Blue Coat прошли сертификацию ICSA.

В данном разделе представлен обзор устройств Blue Coat SG.

Blue Coat: общие технические требования

Blue Coat разработала три серии устройств защиты и кэширования:

- SG 400 для небольших и средних предприятий с количеством пользователей до 250;
- SG 800 для промышленных сетей с количеством пользователей до 2 000;
- SG 8000 для промышленных сетей с количеством пользователей от 1 000 до 10 000 и более, обеспечивает расширяемую модульную платформу, которая позво ляет настраивать размер диска, объем памяти и интерфейсы.

Конфигурации этих моделей представлены в табл. 39.

Табл. 3.9. Сравнение различных моделей Blue Coat SG

Модель	**Диск**	Память	**Интерфейсы**
SG400-0	Один IDE 40 Гб	256 Мб	2 10/100
SG400-1	Два IDE 40 Гб	512 Мб	2 10/100
SG800-0	Один 18 Гб или один 36 Гб Ultra SCSI	512 Мб	2 10/100
SG800-0B	Два 18 Гб или два 36 Гб Ultra SCSI	768 Мб	2 10/100

Табл. 3.9. (окончание)

Модель	Диск	Память	Интерфейсы
SG800-1	Один 73 Гб Ultra SCSI	1 Гб	2 10/100, один слот расширения для 10/100, 10/100/1000 илиSX 2
SG800-2	Два 73 Гб Ultra SCSI	1,5 Гб	10/100, один слот расширения для 10/100, 10/100/1000 или SX
SG8OO-3	Четыре 73 Гб Ultra SCSI	2 Гб	2 10/100, один слот расширения для 10/100, 10/100/1000 или SX
SG8000-1[1]	Два 15 000 RPM 73 Гб	1 Гб	4 10/100/1000
SG8000-2[1]	Четыре 15 000 RPM 73 Гб	2 Гб	4 10/100/1000
SG8OOO-3'	Шесть 15 000RPM 73 Гб	3 Гб	4 10/100/1000
SG8000-4[1]	Восемь 15 000 RPM 73 Гб	4 Гб	4 10/100/1000

[1] Все модели серии SG8000 работают на базе двух процессоров Хеоп с частотой 3,2 ГГц.

Стоимость устройств Blue Coat SG во время написания данной книги составляла:

- SG400 — от 3 495 долларов США;
- SG800 — от 5 995 долларов США;
- SG8000 — от 40 000 долларов США.

Стоимость лицензии на фильтрацию содержимого оплачивается дополнительно; для 500 пользователей двухгодичная лицензия стоила *9* 140 долларов США во время написания данной книги.

Blue Coat: поддержка платформы и системные требования

Устройства Blue Coat работают на базе патентованной укрепленной операционной системы SGOS. ОС SGOS и программное обеспечение брандмауэра с интегрированным кэшированием устанавливаются на патентованном аппаратном обеспечении на базе диска (не ASIC).

Брандмауэр ISA Server 2004 работает на стандартных платформах Intel, которые легко обновляются, и его можно установить на базе ОС Windows 2000 Server или Windows Server 2003 при наличии стандартного, привычного интерфейса управления и возможности использовать аппаратное обеспечение на любой вкус. Это делает ISA Server более масштабируемым, чем устройства, привязанные к аппаратному обеспечению, более удобным для пользователей, чем Blue Coat.

Безопасность ОС Windows Server 2003 может быть усилена путем применения ряда специальных профилей (profile), входящих в пакет Server 2003 SP2 для мастера Security Configuration Wizard. Корпорация Microsoft также предоставляет руководство по укреплению защиты системы, включающее конкретные рекомендации

по конфигурированию и стратегии применения ISA Server 2004. Этот документ можно скачать по адресу: http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx.

Blue Coat: возможности фильтрации на уровне приложения

Устройства Blue Coat имеют правила фильтрации пакетов, которые определяются с помощью языка политик содержимого Content Policy Language (CPL) и списков контроля доступа (Access Control Lists, ACL). Устройства SG поддерживают проверку подлинности по протоколам NTLM (NT LAN Manager), LDAP (Lightweght Directory Access Protocol, облегченный протокол службы каталогов) и службы RADIUS.

Устройства Blue Coat SG поддерживают фильтрацию содержимого от основных производителей средств фильтрации (WebSense, SurfControl, SmartFilter). Политики можно определить так, чтобы они поддерживали фильтрацию MIME-типа. Поддерживается фильтрация заголовков содержимого. Для фильтрации вредоносных кодов, скачиваемых из Интернета, требуется антивирусное программное обеспечение сторонних производителей. Устройства SG интегрируются с Symantec и TrendMicro по протоколу ЮАР для AV-сканирования Web-контента.

Активное содержимое может быть заблокировано, Web-контент может быть удален и заменен, а информация в заголовках содержимого может быть ограничена, удалена или заменена. Можно блокировать или регистрировать трафик IM или одноранговых приложений и контролировать действия клиентов, например запрещать им загружать файлы. Также включается блокировка всплывающих рекламных объявлений.

В устройствах Blue Coat используется система обработки политик, которая применяет триггеры защиты, основанные на различных факторах, включая пользователей/группы, протоколы, время суток, местоположение или тип содержимого.

Устройства Blue Coat поддерживают управление пропускной способностью.

Что касается ISA Server, он обеспечивает фильтрацию пакетов, фильтрацию уровня канала и фильтрацию уровня приложения, наряду с проверкой/фильтрацией с отслеживанием состояния соединений. ISA Server включает глубинную фильтрацию на уровне приложения без какой-либо дополнительной платы.

ISA Server 2004 выполняет проверку с отслеживанием состояния соединений с использованием интеллектуальных прикладных фильтров. Можно не только определить достоверность данных, проходящих через брандмауэр в заголовках запроса и ответа, но и осуществлять фильтрацию по текстовым цепочкам для фильтрации по ключевым словам или отфильтровывать определенные типы файлов.

ISA Server 2004 проверяет все аспекты HTTP-соединений. SMTP-фильтр защищает от неверных SMTP-команд, которые вызывают переполнение буфера, а средство контроля SMTP-сообщений блокирует спам и почту, содержащую опасные вложения.

RPC-фильтрация ISA Server защищает от атак и вредоносных кодов, направленных на службы RPC, и пропускает через сервер Exchange только законные соединения.

DNS-фильтрация предотвращает атаки на уровне приложения, нацеленные на опубликованные DNS-серверы, а фильтры POP3 защищают опубликованные почтовые серверы POP3 от атак.

Blue Coat: поддержка VPN

Поддержка VPN не включается в базовый пакет для брандмауэра Blue Coat и устройств Web-кэширования.

Брандмауэр ISA Server 2004 поддерживает следующие протоколы VPN:

- сквозной туннельный протокол PPTP;
- протокол L2TP/IPSec
- туннельный режим IPSec;
- VPN удаленного доступа;
- VPN «узел-в-узел».

Политики удаленного доступа брандмауэра применяются к VPN-подключениям удаленного доступа и «узел-в-узел». ISA Server использует VPN-клиенты PPTP и L2TP, которые бесплатно включаются во все операционные системы Windows.

Blue Coat: Web-кэширование

Устройства SG поддерживают следующие типы кэширования:

- прямое кэширование;
- обратное кэширование;
- активное кэширование;
- распределенное кэширование;
- иерархическое кэширование;
- кэширование потоковых данных.

Браузеры клиентов можно автоматически настроить с помощью файла PAC (Proxy Autoconfiguration, автоматическая конфигурация прокси).

Обратное кэширование выполняется с использованием коммутатора уровня 4/7 или маршрутизатора, поддерживающего WCCP (Web Cache Communication Protocol, протокол управления кэшированными данными). Он перенаправляет Web-запросы так, что они отсылаются к кэшу, а не к серверу, к которому они были направлены.

Статистика (размер, применение и изменения) по всем Web-объектам, к которым были обращения, сохраняется операционной системой, а затем используется для создания «схем обновления» для каждого объекта. Эти схемы применяются функцией активного кэширования. Невозможно задать обновление объектов на определенное время.

В ISA Server 2004 включена функция Web-кэширования без дополнительной платы. Прямое кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются внутренние пользователи на внешние Web-серверы. Обратное кэширование позволяет брандмауэру ISA Server 2004 кэшировать объекты, к которым обращаются удаленные пользователи на серверы, опубликованные с помощью брандмауэра ISA Server 2004. Web-объекты, запрошенные удаленными пользователями, кэшируются на брандмауэре ISA Server 2004, причем последующие запросы тех же объектов обслуживаются из Web-кэша брандмауэра, а не перенаправляются на опубликованный Web-сервер, расположенный под защитой брандмауэра ISA Server 2004.

Быстрое кэширование в оперативной памяти позволяет брандмауэру ISA Server 2004 сохранять в памяти объекты, к которым чаще всего обращаются пользователи. Это оптимизирует время отклика, т. к. объекты берутся из памяти, а не с диска. ISA Server 2004 позволяет сохранять данные в кэше на диске, что сводит к минимуму доступ к диску как для операций записи, так и для операций чтения. ISA Server 2004 также поддерживает создание цепочек Web-прокси, позволяющих брандмауэру ISA Server 2004 перенаправлять Web-запросы на вышестоящий сервер Web-прокси.

Сравнение брандмауэров ISA Server 2004 с открытыми брандмауэрами

Открытые (бесплатные) брандмауэры разрабатываются и распространяются по общедоступной лицензии GNU (General Public License) и другим открытым лицензиям; как и в случае других бесплатных программ, их исходный код предлагается бесплатно для всех желающих. В результате многие пользователи могут его перепроверять, что теоретически облегчает задачу поиска и устранения ошибок в программном обеспечении.

Бесплатные брандмауэры популярны среди технически образованных пользователей (например, хакеров как в положительном, так и в отрицательном смысле этого слова), а также сторонников и знатоков открытых операционных систем. Очевидное преимущество (стоимость) часто компенсируется следующими недостатками:

- **Сложность в применении** Часто для настройки открытого программного обеспечения необходимы глубокие технические знания. Многие бесплатные брандмауэры (хотя не все) работают на базе интерфейса командной строки и малопонятных команд, которые нужно запомнить; для этого требуется некото рое время, особенно если администраторы мало знакомы с базовой операци онной системой.
- **Нехватка документации** Поскольку это программное обеспечение разраба тывается для последующего бесплатного распространения, возможно, у програм мистов нет ни времени, ни желания подготавливать коммерческую документацию **и** файлы справки для этого продукта. Вкупе с менее понятным интерфейсом это осложняет и замедляет процесс обучения новых пользователей, повышая скры-

тую стоимость продукта с учетом административного времени, необходимого для выхода на хороший уровень работы с продуктом.

- **Слабая или отсутствующая система создания журналов и оповещений, отсутствие мониторинга в режиме реального времени** Это «дополнительные» функции, которые часто не входят в открытые брандмауэры. Они могут быть менее важными при домашнем применении или в лабораторных условиях, но они имеют существенное значение для промышленной среды, когда администраторы должны отслеживать события, предоставлять информацию для судебных разбирательств и подкреплять принимаемые решения хорошо документированной информацией.

Несмотря на эти недостатки, ряд открытых брандмауэров завоевал популярность в некоторых бизнес-кругах. Среди наиболее распространенных брандмауэров можно назвать IPchains, Juniper Firewall Tool Kit (FWTK) и IPCop.

IPChains/IP Tables

Брандмауэр IPChains является частью операционной системы Linux, которая обеспечивает фильтрацию пакетов и преобразование сетевых адресов (часто называемое «маскированием IP-адресов» (IP Masquerade) среди пользователей Linux). Администраторы могут создавать «цепочки» или таблицы правил, которые могут применяться к каждому входящему или исходящему пакету. Эти правила применяются в том порядке, в котором вы их создаете. Эти правила могут быть объединены в «цепочки» для конкретных типов трафика.

Утилита IPchains выполняет функции брандмауэра в традиционном смысле этого слова: фильтрация пакетов на сетевом уровне модели OSI. Она может перенаправлять потоковые протоколы более высокого уровня, например SMTP, POP, NNTP и DNS, но не может проверять содержимое и обеспечивать соответствие данных внутри пакетов данному протоколу.

Утилита IPTables похожа на IPchains, но она выполняет проверку с отслеживанием состояния соединений, в то время как IPchains не отслеживает соединения. Обе поддерживают перенаправление и часто используются вместе с другими продуктами типа Squid или FWTK для прокси уровня приложения.

Функции VPN могут быть добавлены с помощью открытого программного обеспечения, которое можно загрузить из Интернета.

В свою очередь, брандмауэр ISA Server 2004 — полнофункциональный брандмауэр, работающий на нескольких уровнях. Он имеет функции Web-кэширования; обеспечивает простоту управления с помощью графического интерфейса, производительность промышленного уровня и централизованное управление.

ISA Server обеспечивает сложную фильтрацию на уровне приложения и встроенные функции обнаружения вторжения. ISA Server включает все функции VPN-шлюза и поддерживает VPN-подключения по протоколам PPTP, L2TP и IPSec.

FWTK/ipfirewall

Juniper Firewall ToolKit был разработан компанией Obtuse Systems для работы на базе ОС Linux и BSD (Berkeley Software Distribution')/FreeBSD. Он основывался на ipfirewall и предлагал набор инструментов для создания брандмауэров прокси.

Ipfirewall является пакетным фильтром ядра, который поставляется вместе с FreeBSD. Он позволяет настраивать компьютер в качестве маршрутизатора с фильтрацией пакетов, или же можно использовать его на компьютерах (не настроенных в качестве маршрутизаторов) в качестве персонального брандмауэра для фильтрации входящих и исходящих пакетов.

Однако применение фильтра ipfirewall совершенно неудобно для пользователей. Необходимо добавлять опции в конфигурационный файл ядра системы и перекомпилировать ядро. Когда устанавливается фильтр ipfirewall, то по умолчанию стоит настройка «запрещать все ip ото всех ко всем» («deny ip from any to any»). Это означает, что все оказывается заблокированным и невозможно обратно перезагрузиться на сервер после того, как установлен этот брандмауэр.

Конфигурирование выполняется посредством утилиты ipfw. Это утилита командной строки, которая может использоваться для включения и отключения брандмауэра, добавления и удаления правил, перемещения их в другие наборы и т. д. Может существовать до 65 535 правил. Брандмауэр сравнивает каждый пакет с каждым правилом и выполняет заложенные в правиле(-ах) действия. Правило по умолчанию (разрешить или запретить) определяет, блокируются или разрешаются все пакеты по умолчанию.

Динамические правила с ограниченным сроком службы могут создаваться для того, чтобы открывать брандмауэр «по требованию» для легального трафика.

Брандмауэр ISA Server 2004 — полнофункциональный брандмауэр, работающий на нескольких уровнях. Он имеет функции Web-кэширования, обеспечивает простоту управления с помощью графического интерфейса и производительность промышленного уровня, а также централизованное управление.

ISA Server обеспечивает сложную фильтрацию на уровне приложения и встроенные функции обнаружения вторжения. ISA Server включает все функции VPN-шлюза и поддерживает VPN-подключения по протоколам PPTP, L2TP и IPSec.

IPCop

Брандмауэр IPCop удобен для пользователей. Он работает на базе Linux и управляется с помощью интерфейса Web UI, что также обеспечивает возможность удаленного управления. В брандмауэр включены функции NAT для обеспечения защиты небольших ЛВС. IPCop основан на коде Smoothwall и получил общедоступную ли-

[1] Программное изделие Калифорнийского университета (адаптированная для Интернета реализация операционной системы UNIX с комплектом утилит, разрабатываемых и распространяемых университетом). — *Примеч. пер.*

цензию GNU GPL. Этот брандмауэр основан на цепочках IP, а графический интерфейс делает его гораздо более простым в управлении.

IPCop имеет больше функций, чем другие открытые брандмауэры на базе командной строки. Он включает функции VPN (только для IPSec) и функции обнаружения вторжений Snort IDS. Он реализуется в виде сочетания операционной системы/брандмауэра, которые устанавливаются как единый пакет. Операционная система является усеченной версией Linux, в которой отсутствуют дополнительные функции.

IPCop поддерживает до трех сетевых интерфейсов и позволяет устанавливать демилитаризованную зону (DMZ). Для простоты установки эти интерфейсы обозначены зеленым, красным и оранжевым цветом (для внутренней, внешней сети и DMZ). Доступ из демилитаризованной зоны во внутреннюю сеть предоставляется через «микроканалы DMZ» (DMZ pinholes).

Служба Web-прокси также входит в IPCop, но по умолчанию она отключена.

Опять-таки ISA Server 2004 является полнофункциональным брандмауэром, работающим на нескольких уровнях, и имеет функции Web-кэширования; он обеспечивает простоту управления с помощью графического интерфейса и производительность промышленного уровня, а также централизованное управление.

ISA Server обеспечивает сложную фильтрацию на уровне приложения и встроенные функции обнаружения вторжения. ISA Server включает все функции VPN-шлюза и поддерживает VPN-подключения по протоколам PPTP, L2TP и IPSec.

Выводы

В табл. ЗЛО представлено обобщенное сравнение ISA Server 2004 с его основными конкурирующими коммерческими брандмауэрами во время написания данной книги.

Табл. 3.10. Сравнение ISA Server 2004 с основными конкурирующими брандмауэрами

Функция	ISA Server	Checkpoint NG/Nokia 350	Cisco PIX 51SE	Netscreen SO	SonicWall Pro 230	WatchGuard V80	Symantec 5420
Архитектура	ПО	Устройство	Устройство с ПО	Устройство (на базе ASIC)	Устройство	Устройство	Устройство[1]
Операционная система	Windows 2000, Windows Server 2003	IPSO; также работает на базе Windows NT/2000, Solaris, Linux, AIX	PIX OS (на бис IOS)	ScreenOS (2 версии,	SonicOS simple (простая) и enhanced (расширен.)	Патентованная ОС	Патентованная ОС
Пропускная способность	По результатам теста до 1,59 Гбит/с	350 Мбит/с	188 Мбит/с	170 Мбит/с	190 Мбит/с	200 Мбит/с	200 Мбит/с

(см. след. стр.)

Интерфейсы VPN-туннели

Табл. 10. (продолжение)

Функция	ISA Server NG/Nokia350	Checkpoint	Cisco PIX	Nets c re en 50	SonicWall Pro 230	WatchGuard V80	Symantec o230
	Нет ограничений на ПО	4 10/100	6	4 10/100 2 порта НА	3 10/100	3 10/100	*4* 10/100,
	1000 (Standard) 16 000 +PPTP, 30 000L2TP (Enterprise)[2]	12 500	2 000	100	500	8 000	
Поддержка VPN	PPTP, L2TP, IPSec, SSL	IPSec, SSL, L2TP	Патентованный, MS L2TP, PPTP	IPSEC, SSL	IPSec, PPTP	IPSec, L2TP (другие модели поддерживают PPTP)	IPSec
VPN-клиент	Бесплатно, все клиенты ОС Windows	Патентованный или клиент MS L2TP		Патентованный, за дополнительную плату	Патентованный, поставляется в комплекте (10)	Патентованный, за дополнительную плату	Патентованный, с лицензией на каадый туннель
Изолирование VPN-подключений	Включается как часть ОС Windows Server ver 2003, позволяет форси-ровать конфигурирование клиента: установка SP, анти вирусное ПО, брандмауэр; работаете бесплатным VPN-клиентом, входящим в ОС Windows	Называется • верификация конфигурации клиента» (client configuration verification) Требуется VPN-клиент Secure Client (за дополнительную плату)	Конфигурации загружаются и передаются клиентам с центрального шлюза; необходим VPN-клиент Cisco Secure VPN client v.3x	Офаничение, реализация персонально-го брандмауэра и обновлений. Необходим клиент NetScreen Remote Security Client (за дополнительную плату)	Конфигурационные загружаются с VPN-шлюза клиентами, на который применяется патентованное клиентское ПО Global VPN client	Ограничен-ное, реализация персонального брандмауэра Необходим патентованный клиент Mobile User VPN client	Промышленный VPN-клиент включает ПО персонального брандмауэра По литики удаленного доступа сездают файл самонастройки для клиент;!; сервер выполняет сканирование VPN-под ключений Secured
Обнаружение втор-	Основано на технологии по лицензии **OTIIS**	ISS Real Secure IDS, встроенная/ пассивная проверка TCP-потока	Защищает от 55 атак; есть отдельное устройство IDS	**IDS основывается на** OneSecure; IDS предлагается дополнительно	Об наружение и предупреждение DoS-атак	В наличии IDS и IDP,функщ-. обнаружение аномалий протоколов	функщ-:я IDS/I DP по выявлению аномалий (Recourse)

Табл. 3. 10. (продолжение)

Функция	**ISA Server** NG/Nokia350	Checkpoint 515E	Cisco **PIX**	Netscreen 50	SonicWall Pro 230	Watch Guard V80	Symantec 5420
	Глубинная фильтрация на уровне приложения, включающая фильтрацию	Фильтрация на уровне приложения NG, включает прикладные прокси, фильтрацию содержимого по протоколу UFP	Fixups; ASA; фильтрация URL, Web-sense или N2H2;фильтрация содержимого блокирует Java/ActiveX	HTTP, POP3, ШАР, SMTP, FTP, DNS, поддерживает WebSense			Атаки; HTTP, FTP и SMTP сканируются на вирусы, фильтрация содержимого
Фильтрация на уровне приложения	символов в цецочке-, FTP, POP3, IMAP		HTTP, SMTP, DNS,	Web (HTTP, HTTPS), *CLI,* Telnet, SSH, Global Pro	Web-интерфейс, CLI, SNMP, Global Mgmt System (централизованное управление)	Java-based GUI; CLI; Multi-box mgmt (CPM) дополнительно	Интерфейс на базе Web (SSL), консоль управления Symantec
Интерфейс управления	Привычная консоль Windows MMC для локального и удаленного управления, CLI (интерфейс команд-	CLI, FTP, SSH, Voyager (локальное управление) Horizon Mgr (удаленное	SNMP, Telnet, Web: PIX (PDM), CLI, Telnet, SSH, console port	Менеджер устройств (дополнительно)	По CFS подписке	Не входит	Не входит
Web-кэширование	Используется выравнивание нагрузки, восстановление после отказа входит в Windows 2000/2003 без дополнительной плати	В этой модели не поддерживается кластеризация	плату предлагается Cisco Content Engine Восстановление после отказа при покупке второго устройства	Поддерживает только активный/пассивный режим (в других сериях A/A)	Восстановление после аппаратного сбоя пре-ный режим доставляется (в других сериях A/A) отдельную плату	Поддерживает активный/пассивный режим	A/A, A/P, LB (макс, размер кластера 8)
Высокая работоспособность	ной строки), удаленный рабочий стол/ службы терминалов Включено без дополнительно прямое/обратное кэширование	управление) Не входит, предлагается за дополнительную	Не входит; дополнительной платы;	Не входит			

(см. след. стр.)

Табл. 3.10. (окончание)

Функция	ISA Server NG/Nokia 350	Checkpoint	Cisco PIX 515E	Netscreen 50	SonlcWall Pro 230	WatchGuard V80	Symantec 5420
Дополнения (за отдельную плату)	Большое количество дополнений от сторонних производителей для расширения функциональных возможностей	Управление, IDS, кластеризация, фильтрация содержимого, отчеты, кэширование	Кэширование (Content engine), IDS, анти-вирус-фильтрация	ГОР, фильтрация спама (SurfControl), AV ное ПО, содержимого	AV, фильтрация содержимого, GSM для управления несколькими объектами	A/A НА, сканирование на вирусы, служба обновления	AV, фильтрация содерж1-мого, дополнительные VPN-клиенты, лицензии НА/LB
Лицензирование	На основе версии (Standard Edition или Enterprise Edition), нет дополнительной платы за VPN-клиент	Ежегодная подписке, дополнительная плата за VPN-клиенты		Основная, расширенная лицензия, дополнительная плата за VPN-клиенты	Неограниченная лицензия для пользователя брандмауэра; дополнительная плата за VPN-клиенты	Неограниченные лицензии для пользователей; дополнительная полнительная плата за VPN-клиенты	Базовия лицензия на 50 узлов, на 1 VPN-сессию
Цена	1 499 долларов США (Standard Edition)	3 695 долларов США	В зависимости от функциональности; R, UR, F, VPN-клиент за дополнительную плату	5 695 долларов США	I 699 долларов США	12 995 долларов США	2 999 долларов США
			4 989 долларов США				

[1] Программное обеспечение промышленного брандмауэра Symantec, работающее на базе устройств серии 5400, также можно приобрести как брандмауэр на базе программного обеспечения, который будет работать на базе ОС Windows или Solaris.

[/] Windows Server 2003 Standard Edition поддерживает 1000 PPTP и 1000 L2TP подключений. Windows Server 2003 Enterprise и DataCenter Edition теоретически поддерживают неограниченное число VPN-подключений, но системный реестр ограничивает количество PPTP-подключений до 16 384, а L2TP-подключений до 30 000 для этих версий.

Сравнение архитектуры

Все конкуренты ISA Server 2004, за исключением Checkpoint, Symantec и открытых продуктов (IPchains, FWTK и IPCop), позиционируются на рынке как устройства, в которых аппаратное и программное обеспечение продаются вместе. Большинство из них работает на базе патентованных операционных систем. Многие используют архитектуру ASIC.

Хотя форм-фактор этих устройств имеет ряд достоинств — установка «под ключ» без необходимости установки операционной системы или программного обеспечения, операционная система оптимизирована для данного программного обеспе-

чения, высокая производительность аппаратного обеспечения на базе ASIC, — они также имеют свои недостатки: большая сложность в обновлении, меньшая свобода в выборе конфигурации аппаратного обеспечения, невозможность соответствия аппаратного обеспечения росту производительности системы. В некотором смысле сравнение устройства с брандмауэром на базе программного обеспечения или со средством кэширования подобно сравнению яблок с апельсинами, особенно в отношении цены. Например, важными факторами при выборе устройства являются процессор, память и количество сетевых интерфейсов. Что касается программного обеспечения, эти факторы определяются аппаратным обеспечением, на базе которого вы будете устанавливать программу, при этом вы не ограничены тем выбором, который предлагает производитель.

Будучи брандмауэром на базе программного обеспечения, ISA Server дает большую свободу в выборе и модернизации аппаратного обеспечения, чем брандмауэры на базе аппаратного обеспечения. Предполагается, что некоторые производители будут предлагать ISA Server 2004 с установкой на устройствах защиты, что позволит ему непосредственно конкурировать с другими устройствами.

Сравнение функциональности

Все конкуренты ISA Server за исключением одного (Blue Coat) конкурируют с ним только в части одной из его функций: брандмауэр/VPN или Web-кэш и рование. Поэтому, хотя устройства PIX или NetScreen на первый взгляд предлагают те же функции брандмауэра/VPN по той же или меньшей цене, у них нет функций кэширования. Добавление функций кэширования существенно повышает стоимость подобных продуктов, иногда даже удваивая ее. Если учитывается стоимость добавления кэширования к конкурирующему брандмауэру, то цена ISA Server обычно кажется более привлекательной.

Blue Coat, предлагающий функции брандмауэра и кэширования, имеет один, но существенный недостаток, — в нем нет поддержки VPN.

Сравнение цен

При объективном сравнении (используя сопоставимое аппаратное обеспечение и учитывая необходимость в функциях брандмауэра и кэширования) цена на ISA Server является предпочтительной по сравнению со всеми его ко н ку рентам и за исключением, естественно, открытых брандмауэров. Конкурировать с бесплатными продуктами можно по другим критериям, но не по цене.

Однако открытые программы имеют свои недостатки.

- IPchains/FWTK и сходные продукты, основанные на Linux или ядре UNIX, обеспечивают ограниченный набор функций брандмауэра. Они являются брандмауэрами с фильтрацией пакетов, но они не выполняют сложную фильтрацию на

уровне приложения или не поддерживают встроенный VPN-шлюз, что является само собой разумеющимся для коммерческих продуктов.

- IPchains/FWTK и сходные продукты используют интерфейс командной строки и текстовые файлы для конфигурации и управления. Для их использования не обходим большой опыт и знание операционной системы UNIX. Поскольку они распространяются бесплатно, обычно разработчики не обеспечивают их под держку. К ним мало сопроводительной документации, и, возможно, придется положиться на поддержку других пользователей (списки рассылки, доски объяв лений) или немало заплатить, чтобы получить поддержку сторонних специали стов в случае возникновения проблем.
- Некоторые бесплатные продукты, типа IPCop, более удобны для пользователей, являются простыми в установке и имеют графический интерфейс управления. IPCop даже включает в себя средство Web-прокси/кэширования: Squid. Он так же включает систему обнаружения вторжений Snort. Однако он разработан для домашнего применения и для класса SOHO, а не для крупных промышленных предприятий. В нем не предусмотрена глубинная фильтрация на уровне при ложения, и ему так же не хватает технической поддержки, как и другим откры тым продуктам.

Каждый брандмауэр имеет свои достоинства и недостатки, и выбор подходящего именно для вашей сети часто бывает непростым. Если мы и восхищаемся ISA Server 2004, то только потому, что это соответствует истине. Мы работали с этим брандмауэром и сравнивали его с другими популярными продуктами на протяжении долгого времени, и полагаем, что ISA Server 2004 обошел своих главных конкурентов с точки зрения стоимости, функций и функциональности и простоты в применении. Именно поэтому мы и написали эту книгу.

Б этой главе представлены параметры сравнения различных брандмауэров, с помощью которых можно выбрать брандмауэр для вашей организации. Если вы выбираете ISA Server 2004, то в остальной части данной книги показывается, как с ним работать.

Краткое резюме по разделам

Параметры сравнения брандмауэров

И Если посмотреть на линейки продукции большинства крупных производителей устройств защиты, можно увидеть от трех до десяти и более различных моделей, не говоря уже о многообразии различных схем лицензирования и большом количестве дополнений, расширяющих функциональность и предлагающихся за дополнительную плату.

И Не так просто провести сравнение продуктов различных производителей, и часто в таком сравнении не будет явного «победителя». Напротив, оказывается, что

правильный выбор во многом зависит от сетевой инфраструктуры, той роли, которая отводится брандмауэру, и от предпочтения одних функций другим.

0 По мере углубления в параметры сравнения приходит понимание, что простое сравнение цен является бессмысленным. Сравнительный анализ также должен учитывать административные расходы, схемы лицензирования и набор функций сравниваемых продуктов.

И Для тех, кто сам принимает решение (начальник финансового отдела, менеджер отдела закупок или владелец малого бизнеса), стоимость может быть очень важным фактором. Однако важно помнить о том, что стоимость включает в себя гораздо больше, чем просто начальную цену покупки брандмауэра или аппаратного/программного устройства.

0 При сравнении различных продуктов вам нужно учесть следующее: капиталовложения, дополнительные модули, схемы лицензирования, техническую поддержку, обновления и полную стоимость владения (TCO).

0 При вычислении TCO для каждого продукта нужно учесть не только непосредственные расходы, которые обсуждались в предыдущих разделах, но также и косвенные расходы, например расходы на обучение, администрирование, поддержание производительности и простои.

0 Разобравшись с вопросами цены и определив бюджет, которым мы ограничены, обратимся ко второй обширной категории сравнения, включающей функции и функциональность каждого продукта.

0 Общие технические требования определяют аппаратное обеспечение (для устройств) или минимальные аппаратные требования (для брандмауэров на базе программного обеспечения), а также насколько масштабируемым, расширяемым и надежным является продукт в применении и как он поддерживает функции высокой работоспособности /отказоустойчивости типа кластеризации/восстановления после сбоя и выравнивания нагрузки.

0 Спецификации на продукты с Web-сайтов производителя могут послужить в качестве отправной точки, но по мере сужения выбора возможно захочется углубиться и прочитать независимые обзоры продукта и/или поговорить с ИТ-профессионалами, которые лично работали с конкретными продуктами.

0 Некоторые важные функции брандмауэра, которые нужно учесть в сравнении, включают в себя фильтрацию на уровне приложения, поддержку протоколов, обнаружение вторжений, пропускную способность брандмауэра и количество поддерживаемых одновременных подключений, возможности по созданию журналов и отчетов.

0 Большинство современных брандмауэров, кроме выступающих только в функции персональных/удаленных брандмауэров, включают встроенные VPN-шлюзы. При сравнении поддержки VPN различными устройствами защиты нужно учесть несколько факторов.

0 При сравнении функций VPN нужно учесть поддержку VPN-протоколов, типы поддерживаемых VPN-подключений (удаленного доступа или «узел-в-узел»), стоимость и функциональность VPN-клиентов, количество поддерживаемых одновременных VPN-подключений, пропускную способность VPN, возможности изолирования VPN-подключений.

И При сравнении возможностей Web-кэширования нужно учесть ряд функций. Какие из них вам потребуются, зависит от таких факторов, как размер и структура вашей организации, как и насколько используется внешний доступ к Интернету пользователями вашей сети и есть ли у вашей организации свои Web-серверы.

0 При сравнении, возможностей Web-кэширования нужно учесть такие факторы, как возможность прямого кэширования, возможность обратного кэширования, поддержка распределенного и иерархического кэшировании и использование правил кэширования.

И Еще один фактор, который может оказаться важным для вашей организации, состоит в том, является ли брандмауэр сертифицированным. Для того чтобы сертификация имела смысл, она должна быть выполнена независимой организацией (а не производителем) на основании стандартного практического тестирования в лабораторных условиях (а не просто сравнение функций на бумаге).

0 ICSA Labs является наиболее признанной организацией, выполняющей сертификацию брандмауэров и других продуктов для защиты сети.

Сравнение ISA Server 2004 с другими брандмауэрами

0 Корпорация Microsoft определяет ISA Server 2004 как «улучшенный брандмауэр уровня приложения, решение в области VPN и Web-кэширования, которое позволяет потребителям легко снизить существующие инвестиции в ИТ путем улучшения защиты и производительности сети».

0 ISA Server 2004 включает следующие ключевые функции: проверка на нескольких уровнях, улучшенная фильтрация на уровне приложения, безопасный входящий трафик и защита от внутренних атак по подключениям через VPN-клиенты, интегрированные возможности работы с несколькими сетями, сетевые шаблоны и маршрутизация и проверка с отслеживанием состояния соединений.

0 Простота в применении ISA Server 2004 включает в себя следующие функции: простые в овладении и применении инструменты управления, предотвращение простоя доступа к сети, экономия стоимости пропускной способности, интеграция с Windows Active Directory, VPN-решениями от сторонних производителей и другой существующей инфраструктурой, обширное сообщество партнеров, пользователей и большое количество Web-ресурсов.

0 Функции, обеспечивающие высокую производительность ISA Server 2004, включают в себя: способность обеспечить быстрый безопасный доступ в любое место/в любое время; безопасная, надежная и высокопроизводительная инфраструк-

тура, интегрированное решение в виде одного сервера; возможность масштабирования инфраструктуры защиты; расширенная производительность сети и сниженные расходы на использование пропускной способности.

0 ISA Server 2004 является брандмауэром на базе программного обеспечения, который можно установить на базе ОС Windows 2000 Server (со служебным пакетом Service Pack 4 или выше) или на базе ОС Windows Server 2003- Также на компьютере должен быть установлен Internet Explorer б или более поздняя версия.

0 ISA Server является надежным, масштабируемым и расширяемым и поддерживает высокую работоспособность благодаря службе выравнивания сетевой нагрузки Windows Server 2003.

0 ISA Server обеспечивает совместимость и возможность совместной работы с Active Directory, с сервером Exchange и другими продуктами Microsoft Server System и в смешанном сетевом окружении.

И ISA Server 2004 предоставляет в распоряжение администраторов удобный графический интерфейс, который не только имеет много преимуществ по сравнению с большинством своих конкурентов, но также был значительно улучшен по сравнению с интерфейсом ISA Server 2000.

Й ISA Server 2004 обеспечивает возможность удаленного управления с помощью консоли управления ISA Server и протокола удаленного рабочего стола RDP.

0 ISA Server 2004 обеспечивает улучшенные возможности по созданию журналов и отчетов с помощью инструментальной панели, панели оповещений, сеансов, мониторинга соединений, мастера настройки отчетов и способности просматривать информацию о соединениях в режиме реального времени.

0 Одна из сильных сторон ISA Server 2004 состоит в его способности выполнять фильтрацию на уровне приложения. Функция фильтрации на уровне приложения позволяет брандмауэру ISA Server 2004 обеспечивать защиту от атак, основанных на слабых местах или дырах в конкретном протоколе уровня приложения или в службе.

И ISA Server 2004 включает следующие функции, выделяющие его среди конкурентов: фильтр Secure Exchange RPC, фильтр преобразования ссылок и фильтр OWA на основе форм.

0 ISA Server 2004 включает набор фильтров обнаружения вторжений, получивших лицензию от IIS. Эти фильтры обнаруживают и блокируют атаки на уровне приложения.

Я ISA Server 2004 поддерживает следующие VPN-протоколы: PPTP, L2TP/IPSec и туннельный режим IPSec.

0 Функция VPN ISA Server 2004 поддерживает два типа VPN-подключений: VPN-подключения удаленного доступа и VPN-подключения «узел-в-узел».

0 Функция изолирования VPN-подключений ISA Server 2004 повышает безопасность клиентских VPN-подключений благодаря предварительной проверке VPN-клиентов, прежде чем им будет разрешено подключиться к корпоративной сети.

0 Помимо функций брандмауэра и VPN ISA Server 2004, брандмауэр ISA Server 2004 также может выступать в качестве сервера Web-прокси. Компьютер с ISA Server 2004 может использоваться в качестве сочетания брандмауэра и сервера Web-кэширования или как выделенный сервер Web-кэширования.

0 ISA Server 2004 поддерживает прямое и обратное кэширование, и несколько ISA Server можно настроить для использования распределенного или иерархического кэширования.

0 Дополнительные модули Check Point нужно приобретать за отдельную плату, во многих случаях эти же функции включаются в ISA Server без дополнительной платы.

Й В Check Point нет функций Web-кэширования; их можно добавить в качестве дополнительного решения или дополнительных модулей.

0 Клиентское обеспечение SecureClient от Check Point предлагается за отдельную плату, оно необходимо для реализации верификации конфигурации VPN-клиента, аналогичной функции изолирования VPN-подключений ISA Server, входящей в комплект поставки.

0 Для брандмауэров Cisco PIX требуются дополнительные продукты от сторонних производителей для обеспечения таких возможностей, как глубинная проверка содержимого, которая включается в ISA Server бесплатно.

0 В брандмауэры Cisco PIX не входят функции Web-кэширования, их можно добавить при покупке Cisco Content Engine или средства кэширования от сторонних производителей.

0 Реализация политики конфигурирования VPN для PIX требует наличия патентованного VPN-клиента Cisco Secure v.3.x и старше.

13 Для реализации функций, входящих в ISA Server (более сложные функции обнаружения вторжений/глубинная проверка содержимого, кэширование), в устройствах NetScreen необходимо купить дополнительные устройства или продукты от сторонних производителей.

И В NetScreen используется патентованный VPN-клиент или клиент безопасности (включающий персональный брандмауэр); он приобретается за отдельную плату.

0 Реализация VPN конфигурации в NetScreen обеспечивает только выполнение политик клиента брандмауэра.

0 Для реализации функций, входящих в ISA Server (более сложные функции обнаружения вторжений/глубинная проверка содержимого, кэширование), в устройствах SonicWall необходимо купить дополнительные устройства или продукты от сторонних производителей.

В В NetScreen используется патентованный VPN-клиент, который приобретается за дополнительную плату.

И Для загрузки данных о конфигурации клиента с VPN-шлюза требуется клиент защиты.

0 В недорогих моделях WatchGuard нет прокси уровня приложения. Фильтрация на уровне приложения включает только протоколы HTTP, FTP, DNS.

0 В WatchGuard не входят функции Web-кэширования. Стоимость добавления средства кэширования должна учитываться при сравнении его цены с ISA Server.

0 В WatchGuard используется патентованное программное обеспечение удаленного VPN-клиента, приобретаемое за отдельную плату.

И Для реализации функций, входящих в ISA Server (более сложные функции обнаружения вторжений/глубинная проверка содержимого, кэширование), в устройствах Symantec необходимо купить дополнительные устройства или продукты сторонних производителей.

И В продукты от Symantec не входят функции Web-кэширования. Стоимость добавления средства кэширования должна учитываться при сравнении его цены с ISA Server.

В В WatchGuard используется патентованное программное обеспечение удаленного VPN-клиента, приобретаемое за отдельную плату.

0 Blue Coat является единственным из основных конкурентов ISA Server 2004, в который входят функциональные возможности Web-кэширования.

0 В Blue Coat не входят функциональные возможности создания VPN-подключений удаленного доступа и «узел-в-узел».

В Для брандмауэров Blue Coat фильтрация содержимого может выполняться только с помощью служб сторонних производителей.

0 Открытые брандмауэры пользуются большей популярностью у технически образованных пользователей (например, у хакеров), а также у тех, кто является сторонником и знаком с открытыми операционными системами.

0 Преимущество в цене на открытые брандмауэры часто противостоит сложности в применении, недостатку документации, технической поддержки и слабым или отсутствующим функциям создания журналов и оповещений.

0 IPChains обладает ограниченными функциональными возможностями брандмауэра и не включает службы, наличие которых считается обычно очевидным для коммерческих брандмауэров: фильтрация на уровне приложения, VPN-шлюз, IDS и др.

0 Juniper Firewall ToolKit был разработан компанией Obtuse Systems. Этот продукт работает на базе ОС Linux и BSD/FreeBSD. Он основывается на ipfirewall и предлагается в виде набора инструментов для создания брандмауэров-прокси.

0 IPflrewall является пакетным фильтром ядра ОС, который поставляется вместе с FreeBSD. Он выполняет только фильтрацию пакетов на сетевом уровне, а фильтрация на уровне приложения должна выполняться другой программой/службой.

0 IPCop — это удобный в применении брандмауэр, который работает на базе ОС Linux и управляется посредством Web-интерфейса, что обеспечивает возможность удаленного управления. Он включает функциональные возможности NAT для обеспечения защиты небольшой ЛВС. Он основан на коде Smoothwall и имеет лицензию GNU GPL. Этот брандмауэр основан на цепочках IP (ipchains).

0 IPCop разработан *для* домашнего применения и для пользователей класса SOHO, а не для промышленных сетей.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Почему корпорация Microsoft не предлагает ISA Server в качестве устройства защиты «под ключ»?

О: В сотрудничестве со своими партнерами корпорация Microsoft предлагает устройства защиты с установленным ISA Server, которые могут оказаться более привлекательными по сравнению с другими брандмауэрами на базе аппаратного обеспечения и устройствами кэширования для тех, кто предпочитает преимущества форм-фактора устройства гибкости и возможности обновления брандмауэров на базе программного обеспечения. Среди компаний, предлагающих устройства на базе ISA Server, можно назвать Hewlett-Packard, Network Engines, RimApp и других производителей аппаратного обеспечения. Эти устройства на базе ISA Server 2004 работают на базе укрепленной версии ОС Windows Server и обеспечивают готовность устройства «под ключ» и такую интеграцию с сетями на базе Windows, которую может обеспечить только ISA Server 2004.

В: Является ли базовая операционная система ISA Server (Windows 2000 Server или Windows Server 2003) небезопасной, и не является ли брандмауэр сам небезопасным по этой причине?

О: Нет и еще раз нет. Инициатива корпорации Microsoft по обеспечению безопасности началась с выхода Windows 2000 Server, операционной системы, обеспечивающей защиту на несколько порядков выше, чем предыдущие операционные системы корпорации Microsoft. В Windows 2000 появилось множество новых функций обеспечения безопасности, таких как службы проверки подлинности Kerberos, шифрования файлов, службы Active Directory, менеджера настройки защиты Security Configuration Manager, TLS (Transport Layer Security, защита транспортного уровня), IPSec, поддержки проверки подлинности PKI, на основе смарт-карт, L2TP VPN и др. Эта тенденция получила продолжение и усилилась с выходом ОС Windows Server 2003, которая основывается на концепциях «secure by design» (безопасность, обеспечиваемая при разработке) и «secure by default» (безопасность при применении настроек по умолчанию), при которой службы типа IIS являются отключенными в коробочной версии.

U ISA Server 2004 используется мастер настройки защиты Windows Server 2003 Security Configuration Wizard (входящий в SP2), который включает в себя специальный профиль ISA Server для укрепления операционной системы для работы с брандмауэром ISA.

Bi Как ISA Server может конкурировать с дешевыми устройствами NetScreen и SonicWall, цены на которые не превышают 500 долларов США?

O: Если вы изучите техническую документацию к устройствам низшей ценовой категории, то увидите, что они предназначены для использования в классе SOHO или в дистанционном режиме. Их цена ниже, но у них также меньше функциональных возможностей. Например, они поддерживают намного меньше одновременных VPN-туннелей, меньше одновременных сеансов брандмауэра и/или у них гораздо меньше пропускная способность. ISA Server не предназначен для применения в классе SOHO или для дистанционного режима (хотя он хорошо справится с этими задачами). Он разработан для средних и больших сетей, и в его технической документации это находит свое отражение. Кроме того, упомянутые брандмауэры низшей ценовой категории не имеют функций Web-кэширования. Если в сеть будет добавлено средство кэширования, то это существенно повысит общие расходы на безопасность.

B: Большинство популярных брандмауэров, например PIX, SonicWall и NetScreen, предлагаются в виде нескольких моделей. Почему ISA Server выходит только в двух версиях (Standard и Enterprise)? Как, имея только две версии, можно масштабировать ISA Server для удовлетворения нужд небольших и очень крупных организаций?

O: В этом состоит отличие устройств и брандмауэров на базе программного обеспечения. Если вы вникните в суть дела, вы поймете, что программное обеспечение брандмауэра является одинаковым для различных моделей (хотя некоторые его функции могут быть отключены в некоторых моделях; чтобы их включить, нужно приобрести дополнительные лицензии). Различия между моделями в основном касаются аппаратного обеспечения: процессоров, объема памяти, количества и типа сетевых интерфейсов и т. д. Что касается ISA Server, вы можете установить его программное обеспечение на любом компьютере, который удовлетворяет минимальным требованиям. Поэтому вы можете сами определять аппаратную платформу, а не ограничиваться выбором из предопределенного набора моделей.

Различие ISA Server Standard Edition и Enterprise Edition заключается в наборе их функций: функции Standard Edition являются лишь частью всех функций Enterprise Edition. В Enterprise Edition поддерживаются промышленные политики, массивы кэширования и мастера для создания массивов NLB. Enterprise Edition также поддерживает гораздо большее количество VPN-туннелей (более *1б* 000 по протоколу PPTP и более 30 000 по протоколу L2TP).

В: Почему ISA Server использует только протокол CARP для взаимодействия между серверами кэширования, в то время как другие прокси кэширования поддерживают различные протоколы типа ICP, HTCP, Cache Digests и WCCP?

О: Протокол CARP был выбран для обеспечения взаимодействия между распределенными кэшами ISA Server, потому что он является оптимальным для этой цели. Протокол CARP поддерживает запросы на маршрутизацию, как со стороны сервера, так и со стороны клиента. Маршрутизация со стороны сервера подобна маршрутизации, поддерживаемой протоколами WCCP и ICP. Маршрутизация со стороны клиента является более эффективной, потому что клиент способен заранее определить, какой член массива отвечает за данный URL, и отправить свой запрос напрямую этому члену массива. Протокол CARP использует более эффективный метод для кэширования содержимого между несколькими серверами, потому что CARP, в отличие от ICP, следит за тем, чтобы кэшируемый Web-контент не дублировался на различных серверах, а алгоритм CARP обеспечивает метод определения, на каком сервере хранится кэшированное содержимое.

В: Сравните функцию изолирования VPN-подключений ISA Server со сходными функциями, представленными у других производителей брандмауэров/устройств VPN.

О: Изолирование VPN-подключений обеспечивается с помощью функции изолирования сетевого доступа Network Access Quarantine в ОС Windows Server 2003. эта функция позволяет вам блокировать подключения от VPN-клиентов, которые не удовлетворяют набору критериев, определенных администратором, например на компьютере клиента должны быть установлены текущие служебные пакеты и обновления, должно быть установлено и активировано антивирусное программное обеспечение, а также должно быть установлено и активировано программное обеспечение персонального брандмауэра. Другие производители, предлагающие сходные функциональные возможности, обычно реализуют их на базе собственного патентованного программного обеспечения VPN-клиента. Это программное обеспечение предлагается отдельно, а его стоимость превышает стоимость их стандартного патентованного VPN-клиента. Если же их стандартный клиент поддерживает эти функциональные возможности, то брандмауэр обычно предлагается с ограниченным количеством лицензий для VPN-клиентов и вам приходится покупать дополнительные лицензии, если пользователей VPN у вас больше. Конфигурация клиента у некоторых производителей предполагает только наличие установленного программного обеспечения персонального брандмауэра и не требует установки служебных пакетов и обновлений. Функция изолирования VPN-подключений ISA Server работает на базе программного обеспечения VPN-клиента Windows, которое встроено во все современные операционные системы Windows, и за эти функции не нужно дополнительно платить.

В: Зачем мне платить за ISA Server, если я могу использовать открытый брандмауэр и программы кэширования типа IPChains и Squid, которые работают на базе Linux, открытой операционной системы?

О: Как сказал знаменитый писатель-фантаст Роберт Хайнлен (Robert A. Heinlein), TANSTAAFL ("There ain't no such thing as a free lunch» — за все в этом мире нужно платить). Цена, которую вы платите за «бесплатное» программное обеспечение бывает разной:

- разочарование и потраченное время администратора, когда он заучивает малопонятные команды, или ошибки в конфигурации, вызванные одной опечаткой в текстовом конфигурационном файле;
- D стоимость книг или контрактов на обслуживание от сторонних производителей, когда вы обнаружите, что документации к открытому коду мало и что она малопонятна, а поддержки от разработчиков нет;
- необходимость позже перейти на коммерческий продукт в дополнение или вместо открытого продукта, потому что бесплатный продукт не дает всех необходимых функций или настолько неудобен в применении, что вы не знаете, как его использовать.

Если говорить конкретно, IPchains/iptables и FWTK — это очень ограниченные брандмауэры, которые не включают фильтрацию на уровне приложения, VPN-шлюз и другие функции, обычные для коммерческих продуктов. Брандмауэр IPCop более удобен в применении, но он разработан для класса SOHO и для домашнего применения, а не для предприятия. Ни один из открытых продуктов не рассчитан на интеграцию с сетями Microsoft и бесперебойную поддержку почтовых серверов Exchange, серверов совместной работы SharePoint и других продуктов от корпорации Microsoft, которые поддерживаются ISA Server.

Глава

Конфигурирование сетей в среде ISA Server 2004 и подготовка сетевой инфраструктуры

Основные темы главы;

- **Сети с брандмауэром ISA и тактика защиты**
- **План конфигурирования сети с ISA Server 2004 в концепции Тома и Деб Шиндеров**
- **Определение сетей и отношений между ними с точки зрения брандмауэров ISA**
- **Создание цепочек Web-прокси как форма сетевой маршрутизации**
- **Создание цепочек брандмауэров как форма сетевой маршрутизации**
- **Настройка брандмауэра ISA в качестве DHCP-сервера**

В этой главе обсуждаются возможности брандмауэра ISA по работе в сети. Глава начинается с обсуждения представления о брандмауэре ISA и его месте в корпоративных сетях. Затем рассматривается схема сети, которая используется во всех сетевых сценариях, обсуждаемых в данной книге. При этом приводится подробное описание настройки средства VMware для создания копий конфигураций.

Затем представлен углубленный обзор того, как брандмауэр ISA «видит» сети и как настраивать брандмауэр для обеспечения вз а и мо действия в локальных и нелокальных сетях. Также обсуждается несколько тем, которые с трудом можно отнести к какой-либо категории, но которые лучше всего вписываются в эту главу, посвященную общим представлениям о сети. Глава завершается обсуждением вспомогательных сетевых служб, которые нужно учесть при установке брандмауэра ISA. Это очень важно, поскольку эти службы и поддержка большого количества сетевых служб благоприятно сказываются на работе брандмауэра ISA.

В некоторых разделах этой главы рассматриваются понятия и процедуры, которые более подробно раскрываются в других главах. Возможно, некоторые термины или понятия данной главы, которые еще не были определены, будут не совсем ясны. Наберитесь терпения и найдите описание этих терминов или понятий в других главах книги. Также можно задать вопрос на доске объявлений www.isaserver.org. Для этого нужно написать BOOK в заголовке сообщения и указать номер страницы в книге, на которой что-то непонятно, а затем отправить сообщение автору по электронной почте на адрес tshinder@isaserver.org.

Сети с брандмауэром ISA и тактика защиты

В каждой книге представлен уникальный подход к теме, то же можно сказать и о подходе к брандмауэрам ISA, представленном в данной книге. По мере чтения этой книги можно заметить, что продукт ISA 2004 называется «брандмауэр ISA». Термины «ISA» и «брандмауэр» не случайно употребляются вместе. Это сделано для того, чтобы донести до читателя мысль о том, что брандмауэр ISA является готовым промышленным брандмауэром, который в настоящее время способен предоставить более высокий уровень защиты, чем любой другой брандмауэр на рынке.

Именно с точки зрения преимуществ ISA Server излагаются все темы, касающиеся брандмауэра ISA, в данной книге. Брандмауэр ISA можно установить в любом месте сети: в качестве внешнего брандмауэра сети периметра на границе с Интернетом, в качестве внутреннего брандмауэра отдела или сегмента сети и даже в качестве брандмауэра, предназначенного для защиты группы жизненно важных сетевых служб. Свобода в размещении брандмауэра ISA по отношению к другим сетевым службам и брандмауэрам свидетельствует о способности брандмауэра ISA обеспечивать защиту ресурсов сети независимо от того, где эти ресурсы расположены.

Если вы читаете эту главу книги, то можно предположить, что у вас уже установлен брандмауэр ISA или вы собираетесь его установить. В обоих случаях, перо-

ятно, придется столкнуться со специалистами по проектированию сетей или с администраторами DMZ (demilitarized zone, демилитаризованная зона) или маршрутизаторов, которые поверили в маркетинговые ходы производителей брандмауэров на базе аппаратного обеспечения, убедивших их в том, что брандмауэры на базе аппаратного обеспечения являются единственным средством обеспечения защиты с помощью брандмауэра.

Для того чтобы облегчить задачу обсуждения брандмауэров с так называемыми специалистами по брандмауэрам на базе аппаратного обеспечения, в этой главе приведен иной подход и представление о брандмауэре ISA и о том, как это соотносится с маркетинговой политикой производителей брандмауэров на базе аппаратного обеспечения. Будут рассматриваться следующие темы, которые помогут прояснить ситуацию и «положить на лопатки» всех клеветников на брандмауэр ISA:

- многоуровневая защита;
- заблуждения, связанные с брандмауэром ISA;
- почему брандмауэр ISA нужно размещать перед важными ресурсами;
- улучшенная топология сети и брандмауэра.

После изучения этого раздела вы сможете правильно разместить брандмауэр ISA для защиты сети.

> ПРИМЕЧАНИЕ Цель данного раздела состоит в том, чтобы показать, что брандмауэр ISA представляет собой настоящий сетевой брандмауэр для промышленного применения. Здесь не ставится цель показать, что этот брандмауэр может удовлетворить любые нужды потребителей в любых возможных ситуациях. В другие брандмауэры могут входить функции, необходимые для организации, но не поддерживаемые брандмауэром ISA. В то же время брандмауэр ISA включает важные для обеспечения защиты функции, которые не входят в другие брандмауэры.

Многоуровневая защита

Наверное, любой администратор брандмауэра слышал старую шутку. Начальник спрашивает администратора брандмауэра: «Наша сеть в безопасности?» и слышит в ответ: «Конечно, ведь у нас есть брандмауэр». К сожалению, такова точка зрения многих сетевых администраторов и администраторов брандмауэров. Они рассматривают брандмауэр на границе сети в качестве основной защиты от всех видов сетевых атак.

С грустью приходится констатировать, что брандмауэр на границе сети представляет собой лишь небольшую часть общего плана обеспечения безопасности. Хотя брандмауэр на границе с Интернетом является ключевым компонентом схемы обеспечения защиты сети, он *всеголишь часть,* а эта часть практически не может обеспечить *многоуровневую защиту.*

Многоуровневая защита имеет отношение к философии безопасности, состоящей в том, что существует множество секций или зон безопасности в пределах одной организации, и каждая из них должна быть под защитой. Интерфейс между зонами безопасности представляет собой особую *границу,* и каждая граница требует особого подхода к защите и контролю доступа.

Количество зон безопасности может быть различным в зависимости от организации и от того, какова схема ее сети. В небольших организациях может быть сеть, состоящая из одного сегмента, который находится под защитой брандмауэра на границе с Интернетом. В более крупных организациях могут быть очень сложные сети с несколькими зонами безопасности, а в пределах одних зон безопасности могут находиться другие зоны безопасности. Для каждой зоны безопасности определяется свой уровень контроля входящего и исходящего доступа, а политика брандмауэра должна быть настроена так, чтобы она удовлетворяла уникальным требованиям контроля доступа для каждой зоны безопасности.

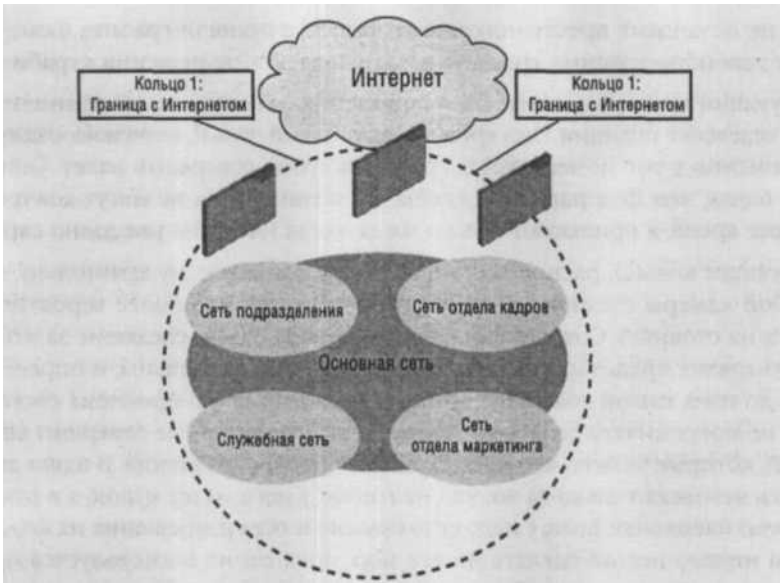
Вне зависимости от сложности сети при размещении и конфигурировании брандмауэра нужно руководствоваться *принципом наименьшего уровня приви>егий.* Принцип наименьшего уровня привилегий состоит в том, что доступ разрешается только тем пользователям, которым необходим этот ресурс, и только к тем ресурсам, к которым пользователям разрешено иметь доступ. Например, если имеется группа пользователей, которым необходим доступ только к Web-сайту Microsoft, единственный протокол, который им нужен в работе, — HTTP, и им нужно предоставить доступ к Web-сайту Microsoft по протоколу HTTP в период с 9:00 до 17.00, то в брандмауэре должна быть создана такая политика доступа. Предоставление пользователям доступа к ресурсам, которые им не нужны для выполнения работы, повышает общую площадь атаки на сеть.

Для того чтобы продемонстрировать, как зоны безопасности определяют контроль доступа, конфигурирование и размещение брандмауэра, обратимся к типичной промышленной сети и покажем, как ее можно разделить на зоны безопасности. Эти зоны будут называться «кольцами*, каждое из которых можно сравнить с капустным листом, а кочерыжку — с наиболее важными ресурсами в сети, требующими наивысшего уровня защиты и контроля доступа.

Вот эти кольца:

- кольцо 1: граница с Интернетом;
- кольцо 2: граница с основной сетью;
- кольцо 3: граница сети с корпоративным имуществом;
- кольцо 4: защита локального хоста.

На рис. 4.1 показано самое внешнее кольцо — граница с Интернетом.



Кольцо 1: граница с Интернетом. Защита на этом уровне сосредоточена
нI предупреждении неавторизованного доступа
> службам сети предприятия, которые не разрешены явно
для удаленного доступа. Высокоскоростная фильтрация
пакетов требуется для обеспечения дополнительного контроля доступа
и высокоскоростной маршрутизации к сегментам сети предприятия.

Рис. 4.1. Кольцо 1: граница с Интернетом

Граница с Интернетом является первой точкой атаки на внешние хосты. Поскольку большинство людей испытывает больший страх перед неизвестным, чем перед известным, сетевые администраторы и администраторы брандмауэров полагают, что они должны размещать наиболее интеллектуальные и мощные брандмауэры в этом месте. Если особенно не задумываться над этим вопросом, то такая точка зрения имеет смысл.

Проблема состоит в том, что подавляющее большинство сетевых атак приходит изнутри сети, поэтому наиболее мощные средства защиты нужно размещать ближе к самым ценным данным. Если рассмотреть, как вообще в мире обеспечивается защита ценностей, то станет ясно, что брандмауэр на границе с Интернетом не должен быть самым мощным или сложным брандмауэром — он должен быть самым быстрым.

Сначала рассмотрим основания размещения наиболее сильных средств защиты ближе всего к самым ценным ресурсам, а затем обсудим причину размещения на внешней границе сети самого быстрого брандмауэра.

Подумайте, как банк обеспечивает защиту денег в своих хранилищах. Прежде всего, существуют федеральные службы безопасности. Этот внешний уровень

защиты не остановит преступников, которые уже пришли грабить банк, но он заставляет законопослушных граждан воздерживаться от решения ограбить банк.

Следующий уровень защиты по направлению к банковскому хранилищу — это местное отделение полиции. Они кружат вокруг целый день и, возможно, окажутся перед банком именно в тот момент, когда грабитель готов совершить налет. Они немного ближе к банку, чем федеральные службы, но полицейские не могут дежурить перед банком все время, а приезжают только тогда, когда налетчик уже давно скрылся.

Следующее кольцо, расположенное ближе к банковскому хранилищу, представляет собой камеры слежения у главного входа (или, что более вероятно, камеры слежения на стоянке). Сотрудники службы охраны банка, следящие за этими камерами, возможно, предотвратят ограбление, если они бдительны, и определят преступника до того, как он совершит попытку ограбления. Но проблема состоит в том, что они не могут ничего делать до тех пор, пока грабитель не совершит каких-либо действий, которые укажут, что происходит попытка ограбления. В наши дни нельзя задержать человека только за то, что на голове у него надет чулок, а в руке он держит пустую наволочку. Если у него есть оружие и есть разрешение на его ношение, то с ним ничего нельзя сделать до тех пор, пока он не воспользуется оружием в незаконных целях или хотя бы не возьмет его с собой в банк (в зависимости от местных или федеральных законов). Однако этот метод защиты более сложный, и вероятность того, что предотвратить ограбление поможет он, а не кольцо федеральных служб или кольцо местных полицейских, выше.

Следующее кольцо — между внешней территорией банка и зоной, где сидят банковские служащие. Если грабитель не будет замечен федеральными службами, прибудет к месту, когда поблизости не будет полицейской машины, если он выглядит, как обычный посетитель, его не заметили на камерах слежения и он застрелит вооруженного охранника, прежде чем охранник застрелит его (предположим, что в стране или в штате, где совершается ограбление, гражданам не разрешается иметь при себе оружие; если же это не так, то грабителю придется столкнуться еще и с вооруженными гражданами), то последней преградой на его пути будет дверь в банковское хранилище. Если он не является взрывотехником или взломщиком сейфов, то дверь в банковское хранилище всякий раз будет его останавливать.

Дверь в банковское хранилище обеспечивает наивысший уровень безопасности, она является наиболее укрепленной и « непроницаемой» из всех уровней защиты в банке. Поэтому она находится непосредственно перед хранилищем, чтобы защитить деньги *в* случае, если взломщик преодолеет все остальные кольца безопасности, предназначенные для защиты банковских ценностей.

Однако ни одно кольцо, насколько бы защищенным оно ни было, не является непреодолимым. (Стоит напомнить об этом так называемым специалистам по брандмауэрам на базе аппаратного обеспечения в следующий раз, когда они скажут о невозможности обойти брандмауэр на базе аппаратного обеспечения.)

Предположим, что грабитель не взрывотехник и не взломщик сейфов. Поэтому он скорее всего воспользуется средствами так называемой социотехники (сходными методами пользуются хакеры). В данном случае применение социотехники состоит в том, что грабитель будет угрожать жизни клиентов и служащих банка до тех пор, пока управляющий банка не откроет дверь в хранилище.

Поскольку деньги можно потом еще заработать, а человеческую жизнь не вернуть, то управляющий откроет дверь хранилища.

Можно подумать, что игра проиграна, а грабитель добился своего. Он проник сквозь последнее кольцо защиты и забрал себе деньги (давайте не будем рассматривать тот факт, что для успешного завершения ограбления грабителю нужно выйти из банка с наличными).

Однако есть еще один уровень защиты — это защита в самих деньгах. В сумках с деньгами могут быть разрывные пакеты с чернилами, которые сработают, если кто-то перемещает сумки в непредусмотренное время или неправильно, или же деньги помечены, и их легко будет найти, когда грабитель начнет их тратить. Если банк надеется возместить свои убытки, он должен убедиться, что средства защиты используются и для денег, поскольку это является последним кольцом защиты банком своего имущества.

Суть в том, что банк, как и любое другое предприятие, защищая свое имущество, размещает наиболее сложные и непреодолимые барьеры ближе всего к наиболее ценному имуществу. Обычно злоумышленник прилагает все свои силы, чтобы преодолеть самое внешнее кольцо защиты. К тому времени, когда он доберется до внутреннего кольца, он либо полностью истощит свои ресурсы, либо готов сдаться. В любом случае злоумышленнику приходится сталкиваться со все более мощными средствами защиты по мере того, как сам он слабеет. Это помогает ускорить его провал. В табл. 4.1 представлено несколько колец защиты, защищающих имущество банка.

Табл. 4.1. Кольца защиты имущества банка

Уровень защиты банка	**Реализация**
Федеральные службы	Внешний уровень защиты. Помогает честным людям оставаться честными
Местный департамент полиции	Обеспечивает защиту в том редком случае, когда полицейские оказываются рядом с банком во время ограбления; обычно срабатывает после того, как ограбление совершено
Камеры слежения банка	Позволяют бдительным охранникам остановить ограбление, если они могут выявить момент его начала
Охранник в банке	Охранник в банке может застрелить грабителя, если грабитель не застрелит его первым. Способен среагировать, когда ограбление уже началось, и обеспечивает гораздо большую защиту, чем предыдущие уровни

(см. след. стр.)

Табл. 4.1. (окончание)

Уровень защиты банка	Реализация
Дверь в хранилище	Самый сильный уровень защиты, расположенный непосредственно перед наиболее ценным имуществом банка
Взрывающиеся чернила, анестезирующий газ и другие средства защиты	Представляет собой «защиту на уровне хоста» и повышает возможность возместить имущество, которое было украдено

Зная такую схему защиты банковского хранилища, как объяснить точку зрения многих сетевых администраторов и администраторов брандмауэров, которые говорят: «Да, я думаю, что брандмауэр ISA очень хороший, но я не успокоюсь, пока не установлю брандмауэр ISA под защиту брандмауэра на базе аппаратного обеспечения».

Такое утверждение означает, что брандмауэр ISA не столь «силен», как традиционный брандмауэр на базе аппаратного обеспечения, выполняющий фильтрацию пакетов. Но есть ли смысл в том, чтобы размещать самое слабое средство защиты непосредственно перед наиболее ценными сетевыми ресурсами?

Парадокс состоит в том, что эти администраторы сетей и брандмауэров все делают правильно, но сама причина их действий является неверной. «Специалисты по брандмауэрам» и продавцы аппаратных брандмауэров годами убеждали их в том, что только брандмауэр ASIC (т. е. аппаратный) может быть безопасным и что так называемые программные брандмауэры в сущности своей небезопасны по причинам X, Y и Z.

Причина X обычно связана с операционной системой, на базе которой работает брандмауэр, и после того, как они в течение нескольких минут с энтузиазмом повторяют: "Windows не безопасна», создается впечатление, что к причинам Y и Z они так и не перейдут. В табл. 4.2 представлена информация о причинах Y и Z, приведенная производителями аппаратных брандмауэров для объяснения того, почему программные брандмауэры небезопасны.

Табл. 4.2. Причины небезопасности программных брандмауэров

Причина	Объяснение
X	Невозможно обеспечить безопасность для ОС Windows
У	Большие прибыли производителей аппаратных брандмауэров от продаж аппаратных брандмауэров
Z	Еще большие прибыли производителей аппаратных брандмауэров от продаж заменяемых частей и дополнений

Таким образом традиционные аппаратные брандмауэры на базе аппаратного обеспечения с фильтрацией пакетов с отслеживанием соединений должны располагаться на границе сети с Интернетом, потому что, хотя они не могут обеспечить высокий уровень защиты, необходимый современным сетям, имеющим соедине-

ние с Интернетом, они могут пропускать пакеты очень быстро и выполнять фильтрацию пакетов с отслеживанием соединений. Скорость очень важна для организаций, загружающих из Интернета большой объем информации. Брандмауэры на уровне приложения, выполняющие большой объем работы и обеспечивающие высокую степень защиты, не могут обработать такой объем трафика и обеспечить проверку на уровне приложения с отслеживанием соединений, которая требуется от современного сетевого брандмауэра.

Брандмауэры на базе аппаратного обеспечения, выполняющие фильтрацию с отслеживание соединений, могут обрабатывать большой объем трафика, выполнять базовую фильтрацию пакетов и разрешать входящий трафик только к тем службам, доступ к которым необходимо предоставить удаленным пользователям (контроль внешнего доступа не является очень эффективным для высокоскоростных брандмауэров с фильтрацией пакетов на границе с Интернетом).

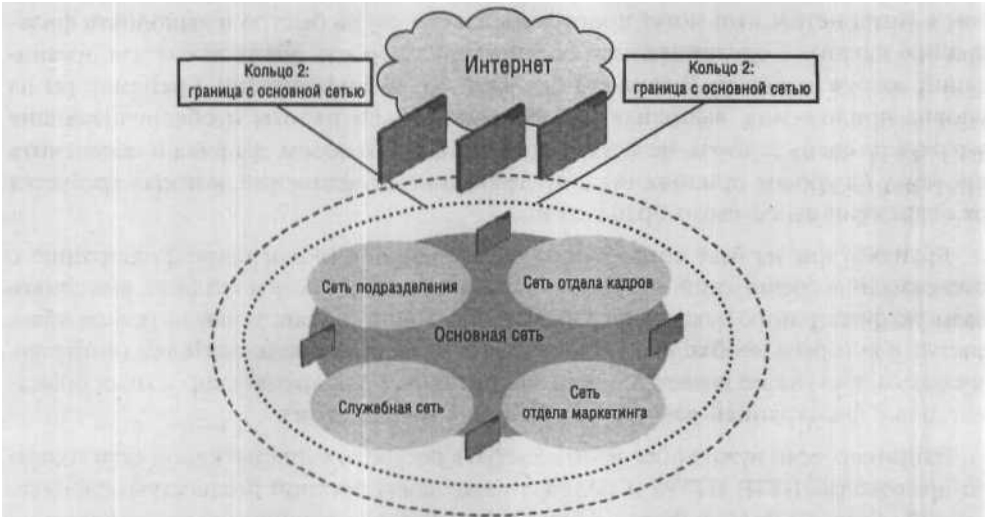
Например, если нужно обеспечить доступ к ресурсам корпоративной сети только по протоколам HTTP, HTTPS и IMAP4, то высокоскоростной брандмауэр с фильтрацией пакетов с отслеживанием соединений будет только принимать запросы на новые входящие соединения для TCP-портов 80, 143 и 443. Высокоскоростной брандмауэр с фильтрацией пакетов может быстро определить порт назначения и достоверность информации на уровне 4 и ниже и принять или отклонить трафик на основе элементарного анализа. Такой подход обеспечивает лишь минимальный уровень защиты, и он далек от того, что требуется для защиты современных сетей, имеющих хосты с выходом в Интернет.

Поэтому в следующий раз услышав фразу: «Я не успокоюсь, пока не установлю брандмауэр на базе аппаратного обеспечения перед брандмауэром ISA», вы поймете, что этот человек не понимает, что по мере продвижения в глубь сети уровень защиты повышается, а не понижается.

Кольцо 2 — это граница с основной сетью, которая отделяет внутренние интерфейсы брандмауэров на границе с Интернетом *и* внешние интерфейсы брандмауэров в сегментах основной сети. На рис. 4.2 показано размещение четырех брандмауэров на границе с основной сетью по краям корпоративной основной сети.

Корпоративная основная сеть представляет собой сеть, к которой подключаются все остальные сегменты корпоративной сети. Объем трафика на один брандмауэр на границе с основной сетью меньше, чем на один брандмауэр на границе с Интернетом, поскольку брандмауэров на границе с основной сетью больше.

Например, имеются два высокоскоростных брандмауэра с фильтрацией пакетов на границе с Интернетом, каждый из которых обрабатывает трафик со скоростью 5 Гбит/с, что в сумме составляет 10 Гбит/с. Имеются четыре брандмауэра на границе с основной сетью, предполагается, что нагрузка между ними распределяется поровну; получим, что каждый из брандмауэров на границе сосновной сетью обрабатывает трафик со скоростью 2,5 Гбит/с.



Кольцо 2: граница с основной сетью. Основ ная сеть предприятия представляет собой сеть, к которой подключаются все прочие сегменты корпоративной сети. Входящий и исходящий из сети трафик распределяется между большим числом брандмауэров. Это обеспечивает прохождение меньшего объема трафика на брандмауэре в точках доступа в основную сеть *и* повышенный уровень защиты брандмаузра путем выполнения проверки на уровне приложения. Эти брандмауэры НЕ различают пользовательс кий/г руп по вой режим и не обеспечивают строгий контроль входящего/исходящего доступа для пользователей/групп.

Рис. 4.2. Кольцо 2: граница с основной сетью

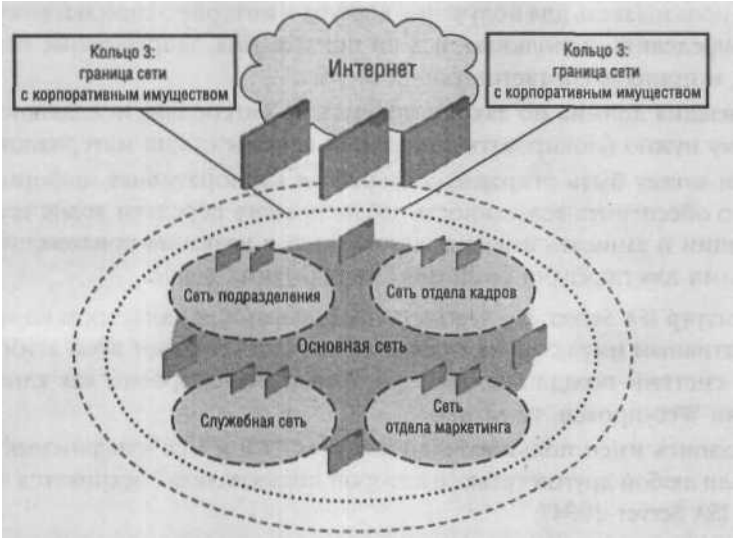
Брандмауэры на границе с основной сетью могут выполнять работу брандмауэра по защите корпоративных ресурсов, проверяя данные уровня приложения с отслеживанием состояния соединений как для входящего, так и для исходящего трафика. Поскольку современные атаки нацелены на уровень приложения (здесь и хранятся «деньги»), то брандмауэры уровня приложения на границе с основной сетью выполняют проверку законности соединений на уровне приложения, перемещаясь по ним.

Например, если разрешить входящий HTTP-трафик, то брандмауэры с проверкой на уровне приложения с отслеживанием состояния соединений, расположенные на границе с основной сетью, могут обеспечить настоящую защиту сети, проверяя параметры связей по протоколу HTTP и блокируя подозрительные соединения на брандмауэре.

Это хорошее место для размещения брандмауэра ISA Server 2004. Поскольку брандмауэр ISA Server 2004 является моделью брандмауэра с проверкой на уровне приложения с отслеживанием соединений, то он может выполнить сложную задачу по защите корпоративной основной сети и сети внутри нее, а также сделать так, чтобы ненадлежащий трафик (например, порожденный вирусами) не перешел через кольцо границы с основной сетью. Брандмауэры ISA Server 2004 прошли тестирование и получили подтверждение как брандмауэры, способные работать с многогигабитным трафиком, основываясь на аппаратной настройке и правилах брандмауэра.

Следующий периметр защиты — кольцо *3,* расположенное на границе основной сети и сети с корпоративным имуществом. Корпоративное имущество включает в себя пользовательские рабочие станции, серверы, ЛВС отделов, сети руководящего звена и все остальное, что необходимо защитить от неавторизованного доступа. Граница между основной сетью и сетью с корпоративным **имуществом** — это *граница сети с корпоративным имуществом.* Именно на этом кольце нужно обеспечить максимальный уровень **защиты, потому** что, если атакующий нарушит целостность этого кольца, он сможет получить доступ к корпоративному имуществу и осуществить успешную атаку.

На рис. 43 показано расположение границ сети с корпоративным имуществом в кольце 3.



Кольцо 3: граница сети с корпоративным имуществом. Корпоративное имущество включает в себя важные ресурсы, которые должны быть защищены от атак извне и должны останавливать исходящие из сети с корпоративным имуществом атаки. Объем входящего и исходящего через брандмауэр сети с корпоративным имуществом трафика меньше для каждого брандмауэра, чем на брандмауэре на границе основной сети, потому что он распределяется между несколькими брандмауэрами. Это позволяет осуществлять более глубинную проверку на уровне приложения и жесткий контроль доступа для пользователей/групп для входящего и исходящего доступа через брандмауэр на границе сети с корпоративным имуществом. В качестве сетей с корпоративным имуществом можно рассматривать ЛВС отделов, пользовательские ЛВС, сегменты/сети сетевых служб, сети управления и т. д. Наиболее безопасные и мощные брандмауэры нужно размещать на этом уровне, потому что это последняя линия защиты сети обороны.

Рис. 4.3. Кольцо 3: граница сети с корпоративным имуществом

Именно на этом уровне становится критически важным применение брандмауэра ISA Server 2004. В отличие от аппаратного устройства фильтрации пакетов здесь нужна настоящая защита с помощью брандмауэра. Простой фильтрации пакетов недостаточно, когда дело доходит до защиты ресурсов на кольце сети с корпоративным имуществом. Необходимо не только позаботиться о том, чтобы все входящие соединения под вер гал ис ь тщательно й проверке на уровне приложения, но также

нужно контролировать, что выходит из сети с корпоративным имуществом, используя жесткий пользовательский/групповой контроль доступа.

Жесткий контроль исходящего пользовательского/группового доступа является абсолютным требованием. В отличие от типичного аппаратного брандмауэра с фильтрацией пакетов, который выпускает весь трафик, брандмауэры на границе сети с корпоративным имуществом должны контролировать исходящие соединения на основе пользовательского/группового членства, потому что:

- необходимо обеспечить возможность вести журнал имен пользователей для всех исходящих соединений так, чтобы можно было призвать пользователей к ответственности за то, что они делают в Интернете;
- необходимо обеспечить возможность вести журнал приложений, которые применял пользователь для получения доступа к интернет-сервисам, это позволяет определить, использовались ли приложения, запрещенные сетевой политикой, и принять соответствующие меры;
- организация должна по закону отвечать за материалы, исходящие из ее сети; поэтому нужно блокировать выход всех ненадлежащих материалов из сети;
- из сети может быть отправлена секретная корпоративная информация. Необходимо обеспечить возможность заблокировать передачи вовне секретной информации и записать имена пользователей и названия приложений, применяемых ими для передачи секретной информации вовне.

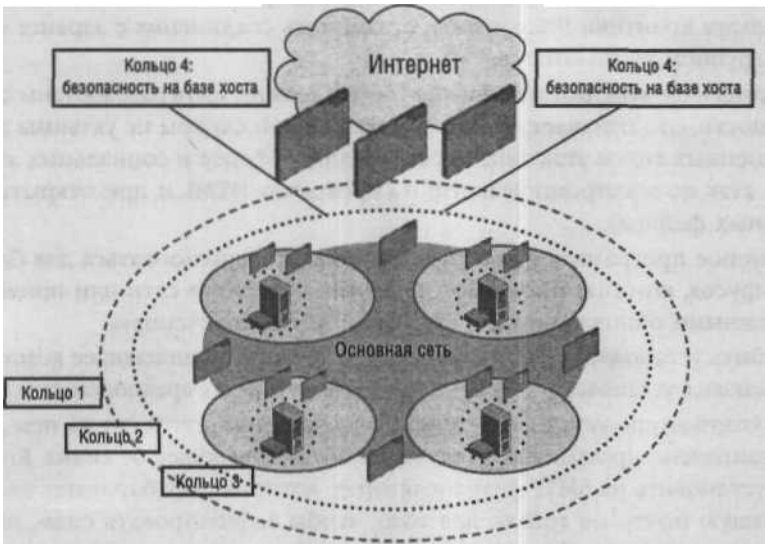
Брандмауэр ISA Server 2004 является идеальным брандмауэром на границе сети с корпоративным имуществом, поскольку он удовлетворяет всем этим требованиям. Когда системы позади брандмауэра правильно настроены как клиенты брандмауэра или Web-прокси, то можно:

- вести запись имен пользователей для всех TCP и UDP-соединений с Интернетом (или любой другой сетью, с которой пользователь соединяется через брандмауэр ISA Server 2004);
- вести запись приложений, которые применяются пользователями для установления этих TCP и UDP-соединений через брандмауэр ISA Server 2004;
- блокировать соединения к любому имени домена или IP-адресу, основываясь на имени пользователя или членстве в группе;
- блокировать доступ к любому содержимому вне сети, основываясь на имени пользователя или членстве в группе;
- блокировать передачу информации из сети с корпоративным имуществом в любую другую сеть, основываясь на имени пользователя или членстве в группе.

Глубинная проверка на уровне приложения с отслеживанием соединений и контроль доступа требуют определенной производительности обработки данных. Необходимо правильно соразмерить свои серверы, чтобы они удовлетворяли требованиям производительности по обработке данных уровня приложения с отслеживанием состояния соединений. К счастью, даже имея сложные наборы правил,

брандмауэр ISA Server 2004 способен обрабатывать трафик со скоростью 1,5 Гбит/с и больше на каждом сервере при подходящей аппаратной конфигурации.

Кольцо 4 представляет собой самый внутренний периметр защиты в этой модели. Кольцо 4 — это кольцо защиты локального хоста. Кольцо защиты локального хоста является соединением между хост-системами и сетью, с которой они непосредственно соединены. На рис. 4.4 представлено положение кольца 4.



Кольцо 4: защита локального хоста. Это наиболее важное кольцо безопасности, которым чаще всего пренебрегают. Когда враги уже у ворот, лучше, чтобы под рукой оказалось наиболее мощное оружие, потому что это последняя возможность защитить самое ценное имущество. Безопасность на базе хоста, реализованная в брандмауэре на базе хоста, отключает неиспользуемые службы, которые увеличивают 'площадь атаки', используя доступные IPSec фильтры, которые разрешают только запрошенный трафик и обеспечивают то, что программное обеспечение ОС, приложения и службы на хосте настроены на автоматическое пропускание только разрешенного трафика и на отбрасывание атак. Также требуется, чтобы программное обеспечение хоста создавалось с учетом обеспечения безопасности и не было подвержено таким известным типам атак, как переполнение буферов.

Рис. 4.4. Кольцо 4: защита локального хоста

Подходы к безопасности локального хоста несколько отличаются от той защиты, которую предоставляют брандмауэры сетевого уровня, но принципы в обоих случаях одни и те же. Безопасность на базе хоста требует обеспечить контроль того, какой входящий и исходящий трафик разрешается на хост-компьютере, и чтобы приложения, применяемые на хосте, были разработаны с учетом безопасности. Вот некоторые моменты, которые необходимо учитывать при создании кольца защиты локального хоста:

- использование брандмауэра, основанного на хосте, для осуществления контроля за тем, какие исходящие и входящие соединения разрешены и какие приложения могут отправлять и получать данные. Это типичный подход «персонально-

го брандмауэра», но его также можно расширить для обеспечения поддержки серверных приложений помимо поддержки персонального брандмауэр;! для пользовательских рабочих станций;

в политика IPSec (в системах, которые ее поддерживают) может использоваться для того, чтобы контролировать, какой входящий и исходящий трафик разрешен для конкретных хостов. Если какая-то рабочая станция или сервер не должна быть подключена ко всем возможным компьютерам, то можно заблокировать ее, используя политики IPSec, чтобы ограничить соединения с заранее определенной группой компьютеров;

- приложения и службы, работающие на хостах, должны быть разработаны с учетом безопасности. Это означает, что эти приложения и службы не уязвимы для рас пространенных типов атак типа переполнения буферов и социальных атак (на пример, атак по электронной почте по протоколу HTML и при открытии при крепленных файлов);
- антивирусное программное обеспечение должно использоваться для блокиро вания вирусов, которые поступают из других сегментов сети или привносятся с ненадежными обновлениями и программным обеспечением;
- должно быть установлено программное обеспечение, защищающее компьютеры и запрещающее установку рекламных программ и прочих вредоносных программ;
- если на компьютере установлен клиент электронной почты, то на нем должно быть установлено программное обеспечение, защищающее от спама. Его также следует установить на SMTP-ретрансляторах, которые обрабатывают входящую и исходящую почту, не только для того, чтобы заблокировать спам, несущий потенциально опасную нагрузку, но также чтобы снизить потери в производи тельности труда, вызванные спамом;
- пользователи и установленные службы должны работать по принципу наимень шего уровня привилегий для того, чтобы ограничить влияние вредоносного программного обеспечения в случае, если оно будет запущено. Например, мно жество программ рекламного характера, программ-шпионов, вирусов, мусорное ПО (scumware), паразитное ПО (rootkit) не могут быть установлены, если у учет ной записи устанавливающего их пользователя нет полномочий администра тора или привилегированного пользователя.

Защита локального хоста является последней линией обороны. Ни один брандмауэр не может полностью компенсировать слабые места на уровне хоста. Защита, обеспечиваемая сетевым брандмауэром, может помочь в том, чтобы контролировать доступ из корпоративной сети в корпоративную сеть и предотвращать атаки из нелокальных сетей, которые будут проходить через брандмауэр ISA, но только защита на уровне локального хоста может предотвратить атаки, исходящие из локальной сети, когда соединение не проходит через сетевой брандмауэр.

Теперь, хорошо разобравшись в разнообразных уровнях защиты, мы видим, что слова: «Я не успокоюсь, пока не установлю брандмауэр ISA под защиту фильтра

пакетов на базе аппаратного обеспечения» означают то же самое, что и фраза: «Я не успокоюсь, пока не защищу свою межконтинентальную баллистическую ракету с помощью пуделя».

Обратите внимание на то, что для небольших сетей, в которых имеется лишь одно кольцо, а именно кольцо на границе с Интернетом, все рассуждения, приведенные ранее, являются спорными. Вместо размещения традиционного брандмауэра с фильтрацией пакетов перед брандмауэром ISA в сети с одним периметром, лучше приобрести два брандмауэра ISA или два сложных брандмауэра уровня приложения и поместить брандмауэр ISA позади другого брандмауэра уровня приложения. Так брандмауэр ISA сможет реализовать необходимый высокий уровень пользовательской/групповой безопасности.

Заблуждения, связанные с брандмауэром ISA

Администраторам брандмауэра ISA приходится сталкиваться с неверными представлениями и заблуждениями, связанными с брандмауэром ISA, и проводить обучение коллег и менеджеров. Далее перечислены основные заблуждения, связанные с брандмауэром ISA.

- Брандмауэры на базе программного обеспечения в сущности своей слабые. Обеспечение безопасности сети можно доверить только брандмауэрам на базе аппаратного обеспечения.
- Невозможно доверять безопасности любой службы, работающей на базе опе рационной системы Windows. Невозможно обеспечить безопасность брандма уэра, работающего на базе операционной системы Windows.
- Компьютеры с установленным ISA Server могут стать хорошими прокси-серве рами, но для защиты сети нужен настоящий брандмауэр.
- Брандмауэры ISA работают на аппаратной платформе Intel, и только те бранд мауэры, все компоненты которых «неподвижны», могут быть надежными бранд мауэрами. У брандмауэра не должно быть съемных частей.
- «У меня есть брандмауэр и есть ISA Server».
- Настоящий брандмауэр невероятно трудно конфигурировать, в идеале в нем должен использоваться интерфейс командной строки, что делает брандмауэр доступным только для специально обученного персонала.

Рассмотрим все эти заблуждения.

Брандмауэры на базе программного обеспечения в сущности своей слабые

Администраторам брандмауэра ISA приходится встречаться с теми, кто:

- не знает, что представляет из себя брандмауэр ISA;

- думает, что это какой-то сервер кэширования, похожий на сервер кэширования производства бывшей компании CacheFlow (которая была куплена компанией Bluecoat) или Squid;
- полагает, что неуязвимы только брандмауэры на базе аппаратного обеспечения, а так называемые программные брандмауэры не подходят для использования по периметру.

Обучение тех, кто никогда не слышал о брандмауэре ISA, может стать очень приятным занятием. Им нужно рассказать о том, что брандмауэр ISA обеспечивает жесткий контроль входящего и исходящего доступа так, как это в настоящее время не делает ни один другой брандмауэр на рынке, как он блокирует программы совместного использования файлов, как он предотвращает нарушение политик сетевой безопасности со стороны злоумышленников (например, скачивание материалов, охраняемых авторским правом), как брандмауэр ISA обеспечивает наилучшую защиту для служб Microsoft Exchange, включая OWA и MAPI/RPC, и что этот брандмауэр настолько просто настраивать, что остальные брандмауэры промышленного класса на рынке просто не выдерживают конкуренции.

Встречаются администраторы сетей и брандмауэров, которые слышали о брандмауэре ISA, но имеют неправильное представление, состоящее в том, что «ISA представляет собой нечто вроде Web-прокси или сервера кэширования» (со слов специалиста по брандмауэрам, которого я как-то встретил на конференции, посвященной безопасности).

Брандмауэры ISA являются настоящими брандмауэрами промышленного уровня, которые обеспечивают жесткий контроль входящего и исходящего доступа и фильтрацию на уровне приложения, которая необходима для защиты современных сетей, а не сетей в 1990-х гг., когда вполне хватало традиционных брандмауэров с фильтрацией пакетов.

Сложнее всего переубедить тех, кто считает, что только брандмауэры на базе аппаратного обеспечения могут обеспечить надлежащий уровень защиты. Годами им говорили о том, что брандмауэры на базе аппаратного обеспечения (на базе ASIC) представляют собой пик развития брандмауэров и что любой брандмауэр на базе программного обеспечения (не на базе ASIC) правильнее назвать «прокси». Удивительно, как они согласуют свои убеждения с тем фактом, что первое место по продажам занимает брандмауэр Checkpoint на базе программного обеспечения.

Такое представление о брандмауэрах на базе аппаратного обеспечения имеет историческое обоснование. В 1990-х гг. брандмауэры на базе аппаратного обеспечения могли обеспечить достаточный уровень защиты и производительности, используя простые механизмы фильтрации пакетов, которые изучают адрес источника и назначения, порты и протоколы и быстро принимают решения. Поскольку логика фильтрации встроена в ASIC, взломать такую базовую систему не просто. Однако взломщики двадцать первого века поняли, что совсем не обязательно взла-

мывать набор инструкций брандмауэра с фильтрацией пакетов для того, чтобы обойти сравнительно слабую защиту, которую обеспечивают системы на базе аппаратного обеспечения с фильтрацией с отслеживанием состояния соединений.

Прекрасную статью, развенчивающую миф о превосходстве ASIC, вы можете прочитать по адресу: http://www.issadvisor.com/viewtopic.php?t=368. Автор приводит доводы в пользу отказа от применения брандмауэров на базе аппаратного обеспечения, потому что они никогда не смогут соответствовать современному уровню угрозы и потому что брандмауэры на базе программного обеспечения являются будущим сетевых брандмауэров и защиты периметра. Большое преимущество брандмауэра ISA состоит в том, что его можно быстро обновить и расширить так, чтобы он мог справиться не только с современными угрозами, но и с атаками, защита от которых обязательно потребуется в будущем.

Невозможно доверять безопасности любой службы, которая работает на базе операционной системы Windows

Это распространенная тема для дискуссий среди сторонников брандмауэров на базе аппаратного обеспечения. Часто возникает вопрос о том, как можно быть уверенным в безопасности сети, используя брандмауэры ISA на базе операционной системы Windows, хотя необходимо устранение дыр в защите и ошибок в самой операционной системе. Это хороший и разумный вопрос. Приведем несколько фактов, которые нужно учесть, если вы хотите использовать брандмауэр ISA на базе операционной системы Windows:

- не все обновления применимы к брандмауэру ISA в качестве сетевого брандма уэра. Многие из этих обновлений рассчитаны на службы. Поскольку клиент ские или серверные службы не запускаются на компьютере с брандмауэром ISA, то большинство из обновлений будет бесполезно;
- некоторые из обновлений предназначены для решения проблем, имеющих от ношение к центральным компонентам операционной системы, например RPC (которая подверглась атаке со стороны червя Blaster). Поскольку брандмауэр ISA применяет политику безопасности ко *всем* интерфейсам, придется задать не кое правило доступа, которое разрешит атакам доступ к брандмауэру. В кон кретном случае с RPC фильтр безопасности RPC блокирует Blaster и связанные с ним атаки. IIS к этому не имеет отношения, потому что службы IIS (за исклю чением, может быть, службы IIS SMTP) не запускаются на брандмауэре. Другие службы становятся доступными, только если открыть все порты на брандмауэр и открыть вход для атак. Правильно сконфигурированный брандмауэр ISA го раздо безопаснее, чем операционная система, на базе которой он работает, потому что сетевой доступ к брандмауэру сильно усечен;
- прочие обновления имеют отношение к стабильности. Все производители бранд мауэров регулярно выпускают обновления, а если нет, то их программы уязви мы, даже если они об этом не знают и не признали их уязвимость публично;

- некоторые обновления требуют перезапуска системы. Перезапуск можно за планировать на удобное время. Обратите внимание на то, что не нужно уста навливать все обновления, потому что не все (или даже большая часть) имеют отношение к брандмауэру ISA. Число необходимых перезапусков должно быть незначительным;
- если не доверять службам, работающим на базе операционной системы Windows, то как можно доверять базовой операционной системе при установке Exchange, SQL, SharePoint и других серверов от Microsoft?
- можно усилить защиту операционной системы, на базе которой работает бранд мауэр ISA. В Windows Server 2003 SP1 имеется профиль в мастере SCW (Security Configuration Wizard, мастер настройки безопасности), который позволяет легко автоматически укрепить защиту базовой операционной системы с помощью SCW;
- можно усилить защиту базовой операционной системы вручную вместо исполь зования мастера настройки безопасности. Вслед за ISA Server 2004 будет выпу щено руководство по усилению защиты операционной системы. В нем будет по казан процесс усиления защиты базовой операционной системы, который не окажет влияния на службы брандмауэра ISA. Этот вопрос был очень важен при работе с ISA Server 2000, поскольку многие пытались усилить защиту операци онной системы, а это приводило к побочным эффектам, о которых не знали или не планировали.

Хотя вопрос базовой операционной системы является важным фактором, можно отметить, что базовая операционная система Windows Server 2003 определенно не является важным фактором. Что касается Windows 2000, усиление безопасности этой базовой операционной системы может иметь большее значение, но все равно невозможно усилить защиту операционной системы до такой степени, что она сможет сравниться с уровнем безопасности, обеспечиваемым любым аппаратным брандмауэром.

Из брандмауэров ISA получаются хорошие прокси-серверы, но для защиты сети нужен «настоящий брандмауэр»

Брандмауэр ISA фактически является брандмауэром с фильтрацией с отслеживанием соединений и прокси-брандмауэром. Подобные брандмауэры смешанного типа являются наиболее сложными и безопасными брандмауэрами в настоящее время.

Типичный брандмауэр с фильтрацией пакетов использует очень простой механизм контроля входящего и исходящего доступа: порт источника и адресата, IP-адрес источника и назначения, а для ICMP — IP-адрес источника и назначения, а также тип и код ICMP. Фильтры пакетов могут быть созданы для каждого входящего и исходящего соединения. Более сложные фильтры пакетов могут динамически открывать отвечающие порты. Брандмауэры ISA способны динамически открывать порты с помощью функции динамической фильтрации пакетов.

Брандмауэр уровня канала передачи данных (уровень 2 модели OSI) схож с так называемыми «брандмауэрами с отслеживанием соединений». Следует отметить, что термин «с отслеживанием соединений» может означать все, что угодно. Впервые он был использован в маркетинговых целях, а большинство подобных терминов было предназначено для того, чтобы продавать продукцию, а не для того, чтобы оценить или определить конкретную функцию или способ действия продукта.

Однако большинство считает, что фильтрация (в отличие от проверки) с отслеживанием соединений является механизмом, при котором фильтр с отслеживанием соединений отслеживает состояние соединения на транспортном уровне (уровень 4 модели OSI). Протокол TCP может определять состояние соединения, а протокол UDP не может. Поэтому соединения по протоколу UDP должны иметь «псевдосостояния», которые необходимы для фильтрующего устройства с отслеживанием соединений. Фильтрация с отслеживанием соединений также полезна при защите от ряда атак уровня, находящегося под уровнем приложения, например атак на сеансовом уровне.

Большинство брандмауэров на базе аппаратного обеспечения на этом и останавливается. Они могут выполнять простую фильтрацию пакетов, динамическую фильтрацию пакетов и фильтрацию пакетов с отслеживанием соединений (фильтрацию с отслеживанием состояния соединений). Эти брандмауэры также часто обладают современными функциями маршрутизации, из-за наличия которых они скорее относятся к категории сетевых маршрутизаторов, а не современных брандмауэров. Функции маршрутизации брандмауэров ISA, напротив, не столь впечатляющи, как в традиционных брандмауэрах, основанных на фильтрации пакетов.

Как уже говорилось ранее, брандмауэр с фильтрацией пакетов является полезным на кольце 1 границы с Интернетом из-за его скорости обработки. Основная проблема этих брандмауэров состоит в том, что в действительности они не могут обеспечить уровень безопасности, необходимый для остановки проникновения на кольца 2 и 3, где должен выполняться тщательный контроль на уровне приложения.

Именно здесь в игру вступают прокси-брандмауэры. Прокси-брандмауэр способен проверить все содержимое соединения на уровне приложения, деконструировав и реконструировав все сообщение на уровне приложения. Например, прокси-брандмауэр реконструирует все HTTP-сообщение, изучает команды и данные, содержащиеся в нем, проверяет содержимое и сравнивает его с правилами для уровня приложения. Затем прокси-брандмауэр пропускает или блокирует соединение, основываясь на правилах для уровня приложения, заданных для протокола HTTP.

Одна из наиболее распространенных HTTP-атак — это атака на каталог (directory traversal). Многие широко распространенные черви используют возможность перемещения по каталогу, чтобы получить доступ к исполняемым файлам на Web-сервере. Например, взгляните на такую ссылку: www.iusepixfirewalls.com/scripts/ ,.%5c../winnt/systm32/cmd.exe?/c+ dir+c\. Она запускает на выполнение файл cmd.exe и запускает команду «dir c:\», которая выдает список всех файлов в каталоге *C:*\.

Обратите внимание на строку «%5c». Это код смены алфавита Web-сервера, представляющий обычные символы в виде %пп, где пп — элемент из двух символов. Код смены алфавита «%5c» представляет символ *«\»*. Ускоритель корневого каталога IIS, возможно, не будет производить проверку на наличие кодов смены алфавита и выполнит запрос. Операционная система Web-сервера понимает коды смены алфавита и выполнит команду.

Коды смены алфавита также помогают обходить слабые фильтры входящего трафика. Если фильтр осуществляет поиск строки символов «../•> (точка, точка, слэш), то злоумышленник мог просто изменить ввод на *«%2e%2e/»*. Эта строка символов имеет то же значение, что и «../», но фильтр ее не обнаружит. Код смены алфавита %2e представляет символ «.» (точка). Брандмауэр ISA, будучи сложным брандмауэром с отслеживанием соединений, работающим на уровне приложения, легко блокирует такие атаки.

Прокси-брандмауэры могут блокировать атаки любого протокола уровня приложения: SMTP, NNTP, протоколы обмена сообщениями IMP, POP3, IMAP4 и др. Сложные брандмауэры ISA Server 2004, сочетающие в себе фильтрацию и проверку с отслеживанием соединений на уровне приложения, можно легко модернизировать с помощью программных средств так, чтобы они могли блокировать самые новые типы атак на уровне приложения. Брандмауэры, основанные на фильтрации пакетов, напротив, совершенно не распознают атаки на уровне приложения, и даже аппаратные брандмауэры с начатками контроля уровня приложения невозможно быстро модернизировать, чтобы они могли отражать современные атаки на уровне приложения, что объясняется ограниченностью развития и возможностей по обработки данных ASIC (аппаратного обеспечения).

Брандмауэры ISA работают на аппаратной платформе Intel, а в брандмауэрах не должно быть «съемных частей»

Почему у брандмауэра не должно быть съемных частей, в то время как наши серверы Exchange, SQL, FTP, Web-сервер и любой сервис для решения критически важных задач прекрасно работают, имея съемные части? Приведем несколько преимуществ использования платформы Intel для брандмауэров:

- когда из строя выходит модуль памяти, процессор или сетевая карта, ее можно заменить на аналогичный продукт по цене комплектующих. Для этого не нуж но возвращаться к производителю исходного аппаратного обеспечения и пла тить ему огромные суммы за то, чтобы получить оригинальное устройство;
- чтобы модернизировать память, процессор, устройство хранения, сетевую кар ту или любой другой компонент, можно взять подходящие комплектующие и установить на компьютер. Не нужно идти к производителю исходного аппарат ного обеспечения, чтобы получить модернизированные версии комплектующих по завышенным ценам;

- поскольку программное обеспечение ISA Server 2004 устанавливается на жест ком диске, то нет ограничений объема памяти и запоминающего устройства, которые есть для монолитных аппаратных устройств. Можно установить стан дартные фильтры для уровня приложения, увеличить размер кэша, отрегулиро вать производительность и настройки безопасности и выполнить настройку, необходимую для конкретной сетевой среды;
- вопрос о «съемных частях» относится главным образом к жестким дискам. По казатели MTBF (Mean Time Beetween Failures, среднее время наработки на от каз) для жесткого диска теперь ушли в прошлое. Даже диски IDE (Integrated Device Electronics, встроенный интерфейс устройств) обеспечивают бесперебойную работу до трех с лишним лет при условии нормальной эксплуатации. А когда диск выходит из строя, конфигурацию брандмауэра ISA Server 2004 легко вос становить, потому что вся конфигурация хранится в простом файле XML. Мож но создать резервную копию этого файла, и через 15 минут брандмауэр будет работать и восстанавливать утерянные настройки. Сравните это с вышедшей из строя памятью аппаратного устройства, которое потребует возврата всего уст ройства производителю.

Вопрос восстановления после отказа, наверное, является наиболее веской причиной в пользу применения программных брандмауэров. Отдельный брандмауэр ISA или целый массив из десяти брандмауэров ISA можно восстановить за несколько минут, при этом не нужно заменять весь блок или обращаться к производителю за недостающим аппаратным обеспечением. А если используются съемные диски, то весь массив можно восстановить меньше чем за 30 минут!

У меня есть брандмауэр и есть ISA Server

«У меня есть брандмауэр, и я хочу установить под его защиту ISA Server. Как мне это сделать?» Такое высказывание принадлежит пользователям ISA Server, поэтому ясно, что в нем нет намерения очернить брандмауэр ISA. Напротив, это означает, что даже сами администраторы брандмауэра ISA не понимают, что брандмауэры ISA являются *брандмауэрами* для их сети, и что устройства фильтрации пакетов с отслеживанием соединений, которые они ставят перед брандмауэрами ISA, обычно выполняют базовую фильтрацию пакетов, которая помогает разгрузить процессор.

Справедливости ради мы должны признать, что не все используют ISA Server 2004 в качестве брандмауэра. Да, имеется возможность установить брандмауэр ISA в режиме одной сетевой карты, что можно сравнить с режимом «только кэширования», который был предусмотрен для ISA Server 2000. Однако в режиме с одной сетевой картой функциональные возможности брандмауэра ISA будут сильно ограничены. Большая часть функциональности брандмауэра не будет использована, и компьютер будет выполнять лишь функции Web-прокси.

Это не означает, что брандмауэр ISA в режиме с одной сетевой картой не может обеспечить защиту. Задействованными остаются достаточно функций брандмауэра, чтобы брандмауэр ISA мог обеспечить собственную защиту и защиту соединений через Web-прокси, осуществляемых через брандмауэр ISA в режиме с одной сетевой картой. Брандмауэр ISA в режиме с одной сетевой картой разрешает только те соединения с самим собой, которые заданы в системной политике брандмауэра. Он разрешает только те соединения с корпоративной сетью, которые разрешены в правилах Web-публикаций, а единственные разрешенные исходящие соединения, которые могут быть выполнены через брандмауэр ISA в режиме с одной сетевой картой, — это те соединения, которые разрешены через список правил доступа для соединений по протоколам HTTP/HTTPS.

Хотелось бы, чтобы все организации использовали брандмауэр ISA Server 2004 по назначению, а именно как полнофункциональный брандмауэр с фильтрацией пакетов и проверкой данных уровня приложения с отслеживанием соединений, но понятно, что крупные организации, возможно, потратили миллионы долларов на покупку других брандмауэров. Эти организации все же хотят воспользоваться преимуществами прокси-компонентов, предоставляемых брандмауэром ISA для обеспечения лучшей защиты служб OWA, OMA, ActiveSync и IIS. Поэтому важно обратить внимание на то, что брандмауэр ISA Server 2004, даже в урезанном режиме работы с одной сетевой картой, обеспечивает высокий уровень защиты для прямых и обратных прокси-соединений.

Почему брандмауэр ISA нужно размещать перед ценными ресурсами

Причины размещения брандмауэра ISA перед самыми ценными сетевыми ресурсами.

- Брандмауэры ISA работают на базе стандартного аппаратного обеспечения, что позволяет контролировать расходы и дает возможность обновлять аппаратное обеспечение с помощью стандартных комплектующих, когда это необходимо.
- Для брандмауэров на базе программного обеспечения можно быстро обновить конфигурацию с помощью специального программного обеспечения для работы на уровне приложения от Microsoft и сторонних производителей.
- Для брандмауэров на базе программного обеспечения можно быстро заменить вышедшие из строя компоненты, при этом не требуется возвращать весь бранд мауэр производителю и не придется держать наготове резервы.
- Брандмауэры ISA должны размещаться позади высокоскоростных брандмауэров с фильтрацией пакетов. Это важно для сетей, где существует многогигабитный Интернет-трафик. Брандмауэры с фильтрацией пакетов снижают общий объем трафика, который приходится обрабатывать каждому внутреннему брандмауэ ру ISA. Это уменьшает общую величину рабочей нагрузки на брандмауэры ISA и позволяет им выполнять настоящую проверку на уровне приложения с отсле живанием состояния соединений, необходимую для защиты ресурсов вашей сети.

- Хотя брандмауэр ISA не может соответствовать возможностям традиционных аппаратных брандмауэров на базе ASIC по фильтрации пакетов, он обеспечивает гораздо более высокий уровень функциональных возможностей брандмауэра с помощью своих функций фильтрации пакетов с отслеживанием соединений и проверки на уровне приложения с отслеживанием соединений.
- Брандмауэр ISA способен выполнять проверку подлинности всех соединений, проходящих через брандмауэр. Это является аргументом в пользу того, чтобы размещать брандмауэр непосредственно перед сетью с корпоративным имуществом. В идеале один брандмауэр ISA, не выполняющий проверку подлинности, размещается перед другим брандмауэром ISA, выполняющим проверку подлинности, так, чтобы сложная проверка и фильтрация пакетов с отслеживанием соединений на уровне приложения выполнялась до того, как эти соединения попадут на брандмауэры ISA, выполняющие проверку подлинности.

Улучшенная топология сети и брандмауэра

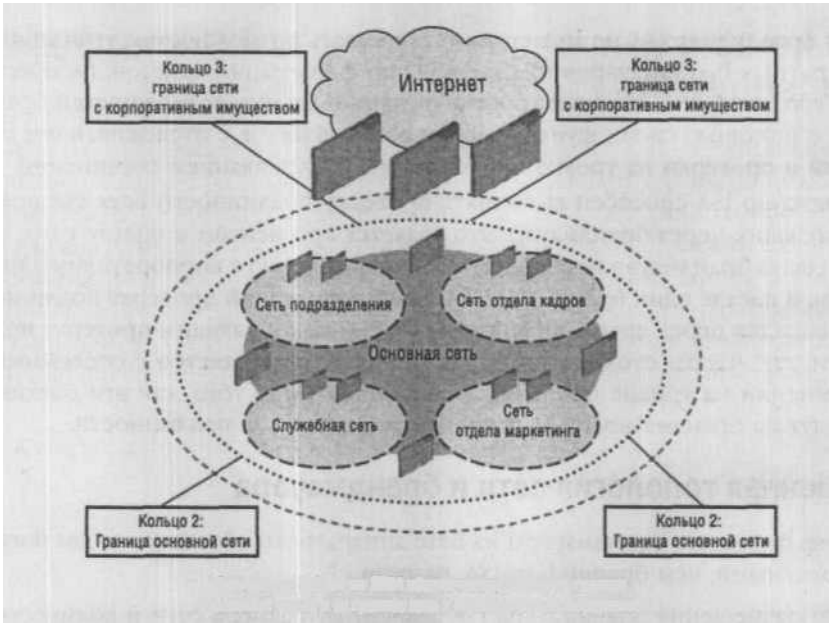
Итак, миф о том, что брандмауэры на базе аппаратного обеспечения являются более безопасными, чем брандмауэр ISA, развеян.

Место размещения брандмауэра ISA зависит от размера сети и количества колец или зон безопасности, которые нужно защитить. Если сеть большая, то лучше всего подходит обсуждавшаяся ранее схема, основанная на четырех кольцах, причем основная сеть и сеть с корпоративным имуществом будут под защитой брандмауэров ISA. Брандмауэр ISA на границе с основной сетью настраивается на выполнение полной фильтрации и проверки на уровне приложения с отслеживанием соединений, при этом он не контролирует исходящий доступ, а брандмауэры ISA на границе сети с корпоративным имуществом обеспечивают фильтрацию и проверку на уровне приложения с отслеживанием соединений, а также контроль входящего и исходящего пользовательского/группового доступа.

На рис. 4.5 представлена конфигурация основной сети и сети с корпоративным имуществом.

В более простых сетевых конфигурациях, не имеющих нескольких колец или много гигабитных сетевых подключений, нет необходимости в размещении быстрого брандмауэра с фильтрацией пакетов на границе с Интернетом.

Однако необходимо разместить доступные извне службы или сегмент DMZ (демилитаризованная зона, фрагмент сети, расположенный между LAN и Интернетом) между границей с Интернетом и сетью с корпоративным имуществом. Это и будет сегмент DMZ (см. рис. 4.6). Можно разместить брандмауэр ISA на границе с Интернетом и быть уверенными в более высоком уровне защиты и контроля доступа по сравнению с обеспечиваемым обычным брандмауэром с фильтрацией пакетов. Кроме того, можно настроить внутренний брандмауэр ISA для осуществления жесткого контроля входящего и исходящего пользовательского/группового доступа.



Брандмауэр ISA Server 2004 обеспечивает защиту НА границе с
основной сетью и на грткш (яти с корпоративным имуществом

Рис. 4.5. Основная сеть и сеть с корпоративным имуществом

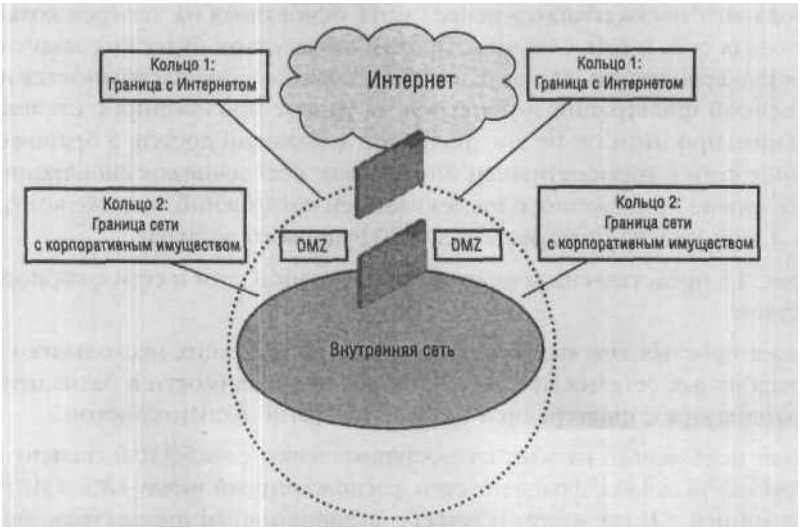


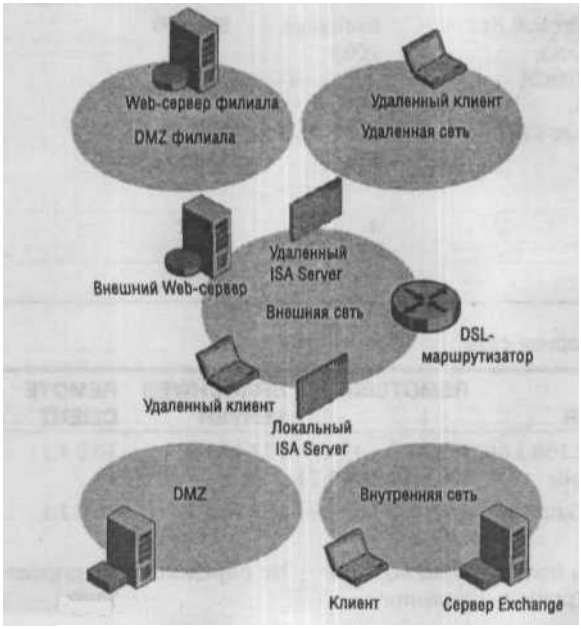
Рис. 4.6. Сегмент DMZ

Для самой простой конфигурации требуется только один брандмауэр, расположенный на границе с Интернетом. Брандмауэр ISA в этом случае обеспечит сети гораздо более высокий уровень защиты и безопасности, чем простой высокоскоростной брандмауэр с фильтрацией пакетов.

План конфигурирования сети с ISA S в концепции Тома и Деб Шиндеров

Каждый из приведенных примеров конфигурации брандмау^ модель сети, созданную специально для этой книги. Эту конфш создать в лабораторных условиях: лабораторная сеть может со теров или же можно использовать программное обеспечение ви. рационной системы. Два наиболее популярных приложения визуал* ционной системы — это Microsoft Virtual PC и VMware Workstation. В да. чае использовалось приложение VMware, потому что оно имеет улучшенные *. вые функции. Однако Microsoft Virtual PC или Virtual Server также вполне подходят для большинства сценариев тестирования брандмауэра ISA.

На рис. 4.7 изображены компьютеры и некоторые части компьютеров в лабораторной сети, используемой в качестве модели в данной книге.



Сервер Exchange

Рис. 4.7. Лабораторная сеть

В табл. 43 и 4.4 представлены наиболее важные характеристики компьютеров, входящих в лабораторную сеть.

		сеть			
		CLIENT	**EXCHANGE 2003FE**	**ISALOCAL**	**EXTCLIENT**
		10.0.0.3	172.16.0.2	Int: 10.0.0.1 Ext: 192.1 68.1.70 Dmz: 172.16.0.1	192.168.1.90
	■.Л	10.0.0.1	172.16.0.1	192.168.1.60	Не определено
	Ю.0.0.2	10.0.0.2	10.0.0.2	Int: 10.0.0.2 Ext: не определено Dmz: не определено	Не определено
WINS	10.0.1.2	10.0.0.2	10.0.0.2	Int: *1*0.0.0.2 Ext: не определено Dmz; не определено	Не определено
ОС	Windows Server 2003	Windows XP	Windows Server 2003	Windows Server 2003	Windows XP
Службы	DS (msfirewall org)[5], DNS, WINS, DHCP, RADIUS, Enterprise CA	**Her**	Exchange 2003	**ISA 200**	Нет
Распреде-ление ОЗУ[1]	128 Мб	128 Мб	128 Мб	**128** Мб	64 Мб
VMNet[2]	2	2	4	Int: 2 Ext:0 Dmz: 4	Не определено

Табл. 4.4. Лабораторная сеть

Настройка	**OSL ROUTER**	**REMOTEISA**	**SERVER**	**CLIENT**	**EXTERNAL WEB[2]**
IP-адрес	Int: 192.168.1.60 Ext: Public	Int: 10.0.1.1 Ext: 192.168.1.71	172.16.1.2	10.0.1.2	192.168.1.24*
Шлюз по умолчанию	Public Gateway	192.168.1.60	172.16.1.1	10.0.1.1	Не определено
DNS	Общего пользо-вания (public)	Общего поль-зования[4]	Не определено	Не лено	Не определено
WINS	Не определено	Не определено	Не определено	Не лено	Не определено
ОС	Не определено	Windows Server 2003	Windows Server 2003	Windows XP	Windows 2000
Службы	Не определено	ISA 2004	SMTP, WWW, NNTP,FTP	Не лено	SMTP, WWW, NNTP, FTP
Распреде-ление ОЗУ	Не определено	128 Мб	64 Мб	128 Мб	64 Мб

Табл. 4.4. (окончание)

Настройка	DSL ROUTER	REMOTEISA	BRANCHWEB SERVER	REMOTE CLIENT	EXTERNAL WEB[2]
VMNet	**Не определено**	**Int:6** **Ext: 0** *Dmz:* 5	**5**	6	**Не определено**

[1] Распределение оперативной памяти — это объем памяти хоста, выделенный для виртуальной машины. Если виртуальные машины не используются, то можно использовать объем памяти, предлагаемый каждой операционной системой.

[2] VMNet — это VMware-сегмент виртуальной Ethernet, к которому подключен интерфейс виртуальной машины. Если у виртуальной машины имеется более одного интерфейса, то приводится VMNet для каждого интерфейса.

[3] Сервер EXTERNALWEB — это Web-сервер в лабораторной сети.

[4] Брандмауэр ISA REMOTEISA использует DNS-сервер общего пользования, так что брандмауэр ISA может разрешать общедоступные имена хостов.

[5] Имя домена Active Directory, используемое во внутренней сети, — msfirewall.org. Расщепленная DNS-конфигурация моделируется так, что хосты внутренней и внешней сети могут устанавливать соединение с ресурсами с помощью одного и того же имени домена Active Directory.

Эта конфигурация лабораторной сети является основой для упражнений и примеров, приведенных в данной книге. При создании такой же сети на всех физических компьютерах можно не обращать внимания на распределение памяти, приведенное в табл. 4.3 и 4.4. Эти распределения памяти использовались в сети VMware в лабораторных условиях для того, чтобы можно было одновременно поддерживать работу до семи виртуальных машин на базе операционной системы хоста. Хотя производительность виртуальных машин была ниже, когда на базе компьютера с процессором Pentium IV (1,5 ГГц и 1 Гб памяти) работали более четырех виртуальных машин, но ее было вполне достаточно для проведения тестирования.

Лабораторные хосты были размещены в различных виртуальных сетях VMnet так, чтобы сети были полностью сегментированы. Каждая сеть VMnet представляет собой отдельный широковещательный домен Ethernet. Это позволяет моделировать реальный сетевой обмен сообщениями, как будто он происходит в кабельной сети, и упрощает анализ системных журналов и службы мониторинга сети. Для тестирования сценариев конфигурации брандмауэра ISA рекомендуется размещать каждый сетевой идентификатор (ID) в отдельной VMnet.

Обратите внимание, что не для всех сценариев нужны все машины. Для любого конкретного сценария, представленного в данной книге, требуется только подмножество машин, описанных в табл. 4.3 и 4.4 и представленных на рис. 4.7. Также не нужно создавать виртуальную машину для каждого хоста, представленного в таблицах. Например, машина с Windows XP может выступать в роли CLIENT, EXTERNALCLIENT и REMOTECLIENT. Единственное, что нужно сделать, — это сменить имя машины, IP-адрес и VMnet на виртуальной машине.

Одно большое преимущество использования виртуальных машин перед физическими устройствами состоит в том, что можно создавать копии базовой конфигурации для каждого хоста в виртуальной лаборатории брандмауэра ISA. Можно сохранить копию каждой виртуальной машины сразу после задания базовой конфигурации и вернуться к ней после завершения тестирования определенного сценария.

Подробные инструкции настройки отдельных машин в лабораторной сети в данной книге не представлены, однако подробно **рассмотрена** процедура создания виртуальной машины для компьютера ISALOCAL с помощью VMware Workstation 4.0. После рассмотрения этого примера станет ясно, как использовать VMware для создания остальных виртуальных машин для данной модели виртуальной сети с брандмауэром ISA

ПРИМЕЧАНИЕ Решение использовать VMware основано на богатом опыте работы с этим продуктом с тех пор, как он был представлен широкой публике. В данной книге не ставится цели произвести на читателя впечатление, как будто VMware в чем-то превосходит Virtual PC в качестве средства создания виртуальной среды операционной системы. Корпорация Microsoft широко использует Virtual PC при тестировании продуктов и проведении тренингов. При тестировании брандмауэра ISA на платформе Virtual PC было отмечено, что производительность виртуальной машины была немного лучше. Однако VMware обеспечивает лучшую поддержку сетевых сценариев, которые обычно воспроизводятся в лабораторных условиях, поэтому для тестирования сценариев брандмауэров она подходит немного лучше. Более подробную информацию о Virtual PC можно получить на сайте: www. microsoft. com/windows/virtualpc/cfefault.mspx.

Создание виртуальной машины ISALOCAL

Сначала необходимо приобрести программное обеспечение VMware Workstation, предварительно загрузив и протестировав его оценочную версию. На сайте http://www.vmware.com/download/ дана ссылка для загрузки этой программы, на сайте http://www.vmware.com/support/ws45/doc/ можно ознакомиться с системными требованиями, которым должен удовлетворять компьютер.

После загрузки файла, запустите установочный файл VMware Workstation. После завершения установки нужно перезагрузить компьютер,

Виртуальная машина ISALOCAL работает с программным обеспечением брандмауэра ISA на базе ОС Windows Server 2003, которое можно установить с дисковода для компакт-дисков, подключенного к операционной системе **хоста** или использовать образ файла CD («образ iso». Эти образы iso широко используются на сайте загрузок MSDN (Microsoft Developer Network, собрание документов компании Microsoft, содержащее сведения обо всех ее разработках). Если имеется только копия Windows Server 2003 на компакт-диске, то можно создать файл с расширением «.iso» с компакт-диска, Это существенно упростит создание виртуальных машин с помо-

щью VMware Workstation, поскольку файл с расширением «iso» можно установить в качестве дисковода для компакт-дисков, и загрузиться с дисковода для компакт-дисков iso, чтобы установить Windows Server 2003.

Можно также создать собственные файлы с расширением «iso». Это помогает при работе с виртуальными машинами, потому что iso-файлы можно использовать *в* качестве виртуальных дисководов для компакт дисков. Например, нужно создать iso-файл для компакт-диска ISA 2004. Существует несколько типов программных приложений, которые позволяют это сделать. Например, можно использовать программу WinlSO, которую можно загрузить на сайте www.winiso.com/.

> СОВЕТ Оценочную версию программного обеспечения Windows Server 2004 Enterprise Edition можно загрузить на сайте https://microsoft.order-5.com/windowsserver2003evaldl/. Эта оценочная версия представлена в виде файла iso, который можно использовать в качестве виртуального дисковода для компакт-дисков.

В данном примере используется iso-файл. После того как iso-файл будет записан на локальный жесткий диск операционной системы хоста, для создания виртуальной машины ISALOCAL нужно выполнить следующие действия. 1. Откройте приложение VMware. В окне **VMware Workstation** (Рабочая станция VMware) (рис. 4.8) щелкните значок **New Virtual Machine** (Новая виртуальная машина).

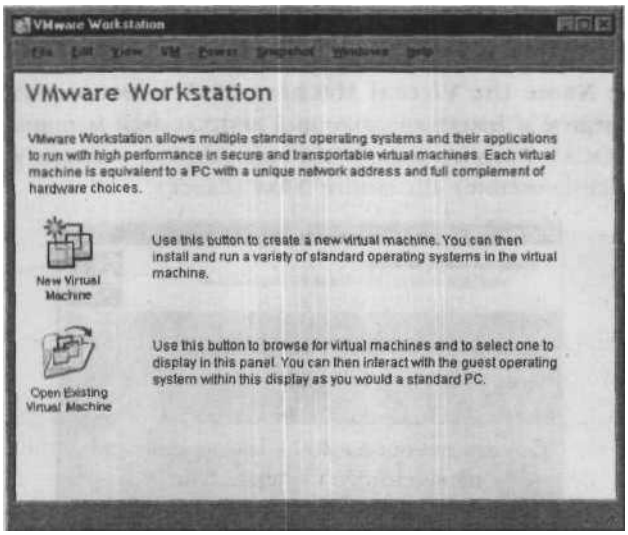


Рис. 4.8. Окно VMware Workstation (Рабочая станция VMware)

2. Щелкните **Next** (Следующий) на странице **Welcome to the New Virtual Machine Wizard** (Вас приветствует мастер создания новой виртуальной машины).

3. На странице **Select the Appropriate Configuration** (Выберите подходящую конфигурацию) выберите вариант **Custom** (Пользовательская). Щелкните **Next** (Далее).
4. На странице **Select a Guest Operating System** (Выберите гостевую операционную систему) (рис. 4.9) выберите вариант Microsoft Windows. Из списка **Version** (Версия) выберите Windows Server 2003 Enterprise Edition. Щелкните **Next (Далее).**

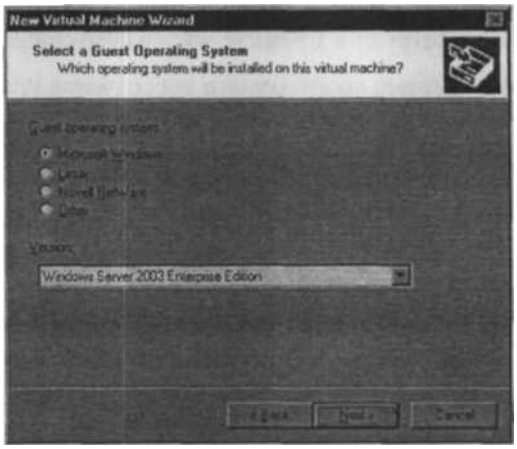


Рис. 4.9. Страница **Select a Guest Operating System** (Выберите гостевую операционную систему)

5. На странице **Name the Virtual Machine** (Дайте имя виртуальной машине) (рис. 410) введите в текстовое поле имя виртуальной машины, в данном примере — ISALOCAL Введите маршрут к виртуальной машине в текстовое поле **Location** (Расположение). Щелкните **Next** (Далее).

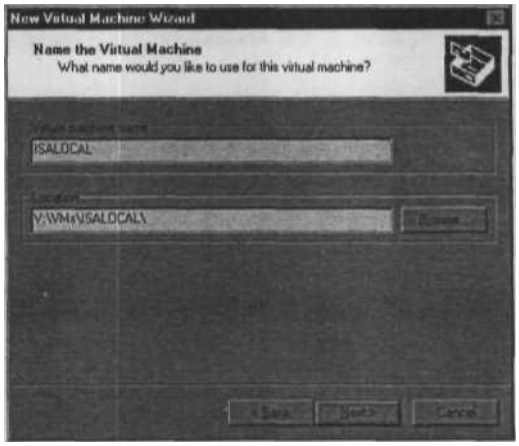


Рис. 4.10. Страница **Name the Virtual Machine** (Дайте **имя** виртуальной машине)

б. На странице **Memory for the Virtual Machine** (Память для виртуальной машины) (рис. 4.11) укажите объем памяти системы хоста, который будет выделен данной виртуальной машине. В данной виртуальной сети **с** брандмауэром ISA машине ISALOCAL выделено 128 Мб памяти. Введите 128 в соответствующее текстовое поле. Щелкните **Next** (Далее).

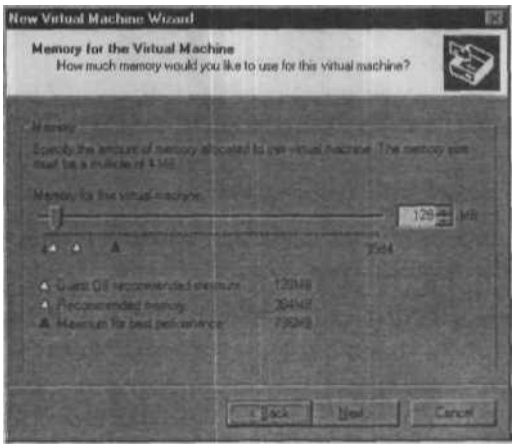


Рис. 4.11. Страница **Memory for the** Virtual Machine (Память для виртуальной машины)

7 На странице **Network** Type (Тип сети) (рис. 4.1 2) выберите вариант Use **bridged networking** (Использовать мостовое соединение сетей). Этот вариант позволяет соединять первую сетевую интерфейсную карту виртуальной машины с реальной сетью, к которой подключена операционная система хоста. На этом интерфейсе виртуальной машине может быть присвоен реальный IP-адрес, при этом может выполняться соединение со всеми компьютерами в реальной сети и с Интернетом через реальный сетевой шлюз. Этот интерфейс будет играть роль внешнего интерфейса виртуальной машины брандмауэра ISA ISALOCAL. Виртуальная машина ISALOCAL будет использовать этот интерфейс для установки соединения с реальным сетевым интернет-шлюзом (в данной сети это DSL-маршрутизатор). Позже к этой виртуальной машине будут добавлены еще две сетевые интерфейсные карты, которые будут использоваться для соединения виртуальной **машины ISALOCAL** с **VMnet2** (Внутренняя сеть) и **VMNet4** (сеть DMZ). Щелкните **Next** (Далее).

8. На странице **Select I/O Adapter Types** (Выберите типы адаптеров ввода-выво да) **используйте** установку по умолчанию и щелкните **Next** (Далее).

9. На странице **Select a Disk** (Выберите диск) выберите вариант **Create a New Virtual Disk** (Создать новый **виртуальный** диск). Этот вариант позволяет создать файл виртуального жесткого диска **на диске операционной** системы хоста. Вир туальная машина будет рассматривать этот файл как жесткий диск. Щелкните **Next** (Далее).

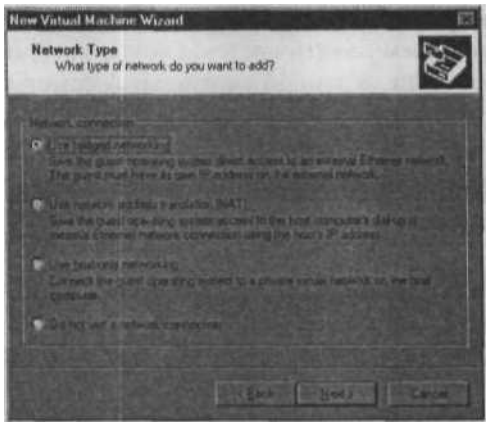


Рис. 4.12. Страница **Network Type** (Тип сети)

10. На странице **Select a Disk Type** (Выберите тип диска) выберите вариант **IDE** (Recommended) (IDE, рекомендуется) и щелкните **Next** (Далее).
11. На странице **Specify Disk Capacity** (Укажите емкость диска) (рис. 4.13) используйте значение по умолчанию 4.0 для записи **Disk size (GB)** (Размер диска, Гб). Хотя Windows Server 2003 и программное обеспечение брандмауэра ISA не требуют такого объема дискового пространства, не нужно беспокоиться о том, что файл виртуального диска займет так много места на физическом диске системы хоста. Введенное значение представляет собой максимальный размер, которого может достигать диск виртуальной машины. Хотя виртуальная машина всегда считает размер своего жесткого диска как значение, указанное на этой странице, реальный размер файла виртуального жесткого диска на операционной системе хоста растет постепенно по мере размещения новых данных на жестком диске виртуальной машины. Щелкните **Next** (Далее).

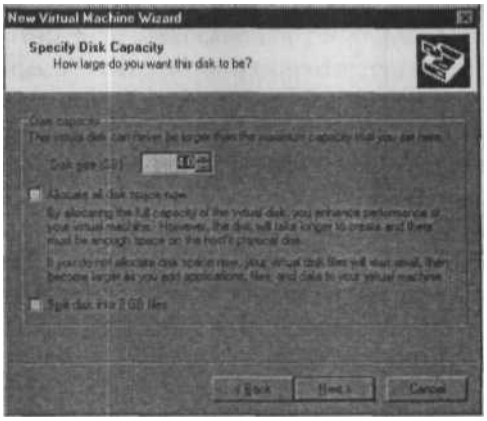


Рис. 4.13. Страница **Specify Disk Capacity** (Укажите емкость диска)

12. На странице **Specify Disk File** (Укажите файл диска) используйте имя файла диска по умолчанию и щелкните **Finish** (Завершение). 13. В окне ISALOCAL

щелкните меню VM, а затем щелкните **Settings** (Настройки).

14. В диалоговом окне **Virtual Machine Control Panel** (Панель управления вирту альной машины) щелкните вкладку **Hardware** (Аппаратное обеспечение). На вкладке Hardware щелкните **Add** (Добавить).
15. Щелкните Next на странице **Welcome to the Add Hardware Wizard** (Вас при ветствует мастер установки нового аппаратного обеспечения).
16. На странице **Hardware Type** (Тип аппаратного обеспечения) (рис. 4.14) выбе рите вариант **Ethernet Adapter** (Адаптер Ethernet) и щелкните **Next (Далее).**

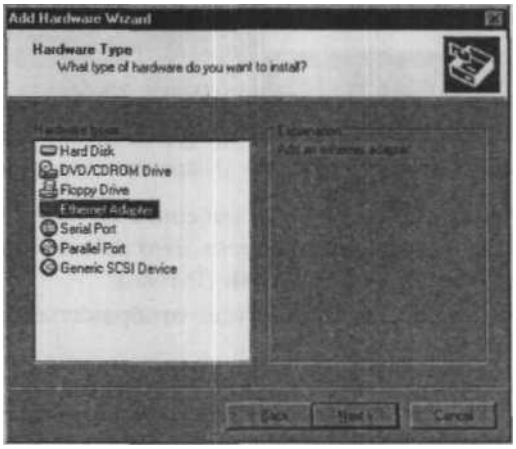


Рис. 4.14. Страница Hardware Type (Тип аппаратного обеспечения)

17. На странице **Network Type** (Тип сети) выберите вариант **Custom** (По выбору). Выберите VMNet2 из выпадающего списка. Этот сетевой интерфейс будет со единен с внутренней сетью. Щелкните **Finish** (Готово).
18. Вторая сетевая интерфейсная карта появится в списке **Device** (Устройство) под именем NIC 2.
19. В диалоговом окне **Virtual Machine Control Panel** (Панель управления вирту-альной машины) щелкните вкладку **Hardware** (Аппаратное обеспечение). На вкладке **Hardware** (Аппаратное обеспечение) щелкните **Add** (Добавить).
20. Щелкните **Next** (Далее) на странице **Welcome to the Add Hardware Wizard** (Вас приветствует мастер установки нового аппаратного обеспечения).
21. На странице **Hardware Type** (Тип аппаратного обеспечения) (рис. 4.15) выбе рите вариант **Ethernet Adapter** (Адаптер Ethernet) и щелкните **Next** (Далее).

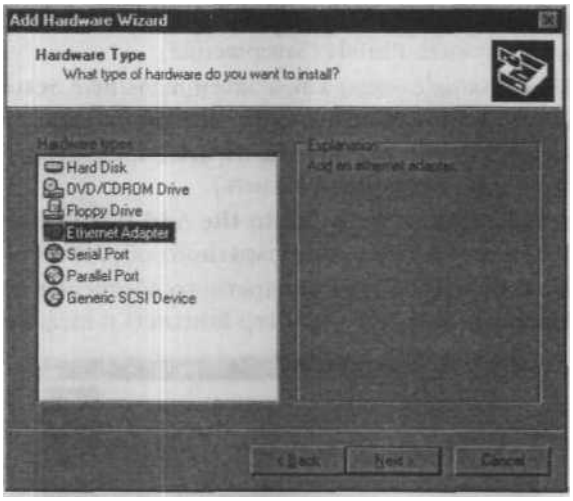


Рис. 4.15. Страница **Hardware Type** (Тип аппаратного обеспечения)

22. На странице **Network Type** (Тип сети) выберите вариант **Custom** (По выбору). Выберите VMNet4 из выпадающего списка. Этот сетевой интерфейс будет под ключаться к сети DMZ. Щелкните **Finish** (Готово).
23. Вторая сетевая интерфейсная карта будет отображаться в списке Device под именем NIC3.
24. Щелкните запись CD-ROM I (IDE 1:0) в списке **Device** (Устройство).
25. В правой части диалогового окна (рис. 4.16) выберите вариант **Use ISO image** (Использовать образ iso) и с помощью кнопки **Browse** (Обзор) укажите место расположения iso-файла для Windows Server 2003.

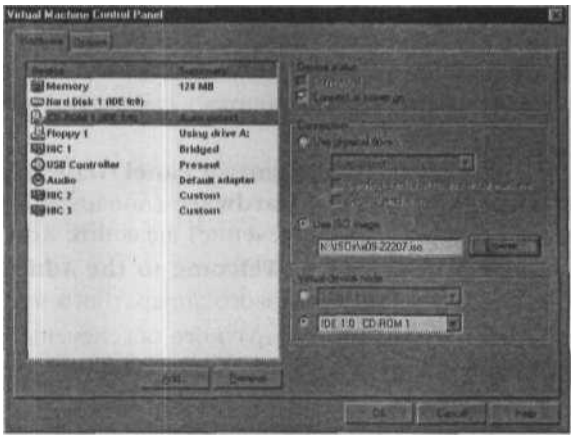


Рис. 4.16. Выбор образа iso

26. В списке Device выберите запись **USB Controller** (Контроллер USB). Щелкните Remove (Удалить).
27. Щелкните OK в диалоговом окне **Virtual Machine Control Panel** (Панель управления виртуальной машины).

Настройка аппаратного обеспечения виртуальной машины выполнена, теперь можно перейти к установке Windows Server 2003. Для завершения установки Windows Server 2003 выполните следующие действия.

1. В левой части окна ISALOCAL — VMware Workstation (рис. 4.1 7) щелкните ссылку **Start this virtual machine** (Запустить эту виртуальную машину) (рис. 4.17). Машина загрузит компакт-диск, представленный iso-файлом.

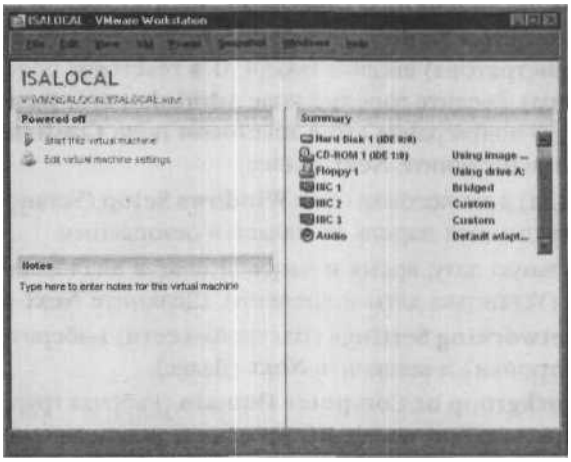


Рис. 4.17. Запуск виртуальной машины

2. Когда откроется страница **Setup Notification** (Уведомление об установке), нажмите клавишу <Enter>.
3. Нажмите клавишу <Enter> на странице **Welcome to Setup** (Вас приветствует программа установки).
4. Нажмите клавишу <F8> на странице **Windows Licensing Agreement** (Лицензионное соглашение Windows).
5. Нажмите клавишу <Enter> на странице **Partition Setup** (Разбивка диска).
6. Выберите вариант по умолчанию **Format the partition using the NTFS file system** (Отформатировать с помощью файловой системы NTFS) на странице форматирования и нажмите клавишу <Enter>. Диск будет отформатирован.
7. Процесс установки перейдет к копированию файлов Windows Server 2003 из образа iso на виртуальный диск. Виртуальная машина автоматически перезагрузится после завершения копирования файлов.

8. После перезагрузки программа установки перейдет в режим графического ин терфейса.
9. Щелкните **Next** (Далее) на странице **Regional and Language Options** (Регио ны и языки).
10. Введите ваше имя и название организации на странице **Personalize Your Soft ware** (Личные данные). Щелкните **Next** (Далее).
11. Введите ключ программного продукта в диалоговом окне **Your Product Key** (Ваш ключ программного продукта). Щелкните **Next** (Далее).
12. На странице **Licensing Modes** (Схемы лицензирования) введите значение 500 в текстовое поле Per server. **Number of concurrent connections** (Количество одновременных соединений на сервер). Щелкните **Next** (Далее).
13- На странице **Computer Name and Administrator Password** (Имя компьютера и пароль администратора) введите ISALOCAL в текстовое поле **Computer name** (Имя компьютера). Введите пароль в поле **Administrator password** (Пароль администратора) и подтвердите его в текстовом поле **Confirm password** (Подтвердить пароль). Щелкните **Next** (Далее).
14. Щелкните **Yes** (Да) в диалоговом окне **Windows Setup** (Установка Windows), что означает, что введенный пароль не является безопасным.
15. Введите правильную дату, время и часовой пояс в диалоговом окне **Date and Time Settings** (Установка даты и времени). Щелкните **Next** (Далее).
16. На странице **Networking Settings** (Настройки сети) выберите **Typical settings** (Типичные настройки) и щелкните **Next** (Далее).
17. На странице **Workgroup or Computer Domain** (Рабочая группа или домен ком пьютера) примите вариант по умолчанию. После установки машины EXCHANGE-2OO3BE в локальной сети (VMNet2) нужно присоединить машину ISALOCAL к домену msfirewall.org. Щелкните **Next** (Далее).
18. Процесс установки продолжается, а затем виртуальная машина перезагрузится.
19. Зайдите на машину **ISALOCAL** с помощью созданной учетной записи и пароля администратора.

Установка программного обеспечения Windows Server 2003 выполнена, теперь можно присвоить сетевым интерфейсным картам виртуальной машины соответствующие IP-адреса. Для выполнения настройки сетевых интерфейсных карт виртуальной машины ISALOCAL и для настройки других вариантов операционной системы выполните следующие действия.

1. После входа на виртуальную машину ISALOCAL щелкните меню VM и в нем ко манду **Install VMware Tools** (Установить инструменты VMware).
2. В диалоговом окне ISALOCAL щелкните **Install** (Установить).
3. Щелкните **Next** (Далее) на странице **Welcome to the installation wizard for VMware Tools** (Вас приветствует мастер установки инструментов VMware).

4. На странице **Setup Type** (Тип установки) выберите **Complete** (Полная) и щелкните **Next** (Далее).
5. Щелкните **Install** (Установить) на странице **Ready to Install the Program** (Установка программы).
6. В каждом диалоговом окне **Hardware Installation** (Установка аппаратного обеспечения) щелкните кнопку **Continue Anyway** (Продолжить в любом случае).
7. Щелкните **Yes** (Да) в диалоговом окне **VMware Tools Installation** (Установка инструментов VMware), что означает, что на виртуальной машине не включено ускорение аппаратного обеспечения.
8. Если появится страница установки Windows Server 2003, закройте ее.
9- Сверните окно **NotePad** (Блокнот), в котором открылся файл HWAccel.txt.
10. Щелкните **Advanced** (Дополнительные) на вкладке **Settings** (Настройки) диалогового окна **Display Properties** (Свойства экрана).
11. В диалоговом окне **Default Monitor and Standard VGA Graphics Adapter Properties** (Свойства по умолчанию: монитор и стандартный графический адаптер VGA) щелкните вкладку **Troubleshoot** (Диагностика).
12. На вкладке **Troubleshoot** (Диагностика) переместите движок полностью до настройки **Full** (Полное). Щелкните **Apply** (Применить), а затем ОК.
13. В диалоговом окне **Display Properties** (Свойства экрана) щелкните ОК.
14. На странице **Installation Wizard Completed** (Завершение работы мастера установки) щелкните **Finish** (Готово).
15. В диалоговом окне **VMware Tools** (Инструментарий VMware) щелкните **Yes** (Да). Виртуальная машина ISALOCAL с Windows Server 2003 будет перезагружена.
16. Выполните вход в систему как администратор.

Следующий шаг — настройка сетевых интерфейсных карт виртуальной машины.

1. Правой кнопкой мыши щелкните на свободном месте рабочего стола и выберите **Properties** (Свойства).
2. В диалоговом окне **Display Properties** (Свойства экрана) щелкните вкладку **Desktop** (Рабочий стол).
3. На вкладке **Desktop** (Рабочий стол) щелкните **Customize Desktop** (Настройка рабочего стола).
4. В диалоговом окне **Desktop Items** (Элементы рабочего стола) щелкните вкладку **General** (Общие). На вкладке **General** (Общие) установите флажки в полях My **Documents** (Мои документы), **My Computer** (Мой компьютер), **My Network Places** (Сетевое окружение) и **Internet Explorer.** Щелкните ОК.
5. Щелкните **Apply** (Применить), а затем ОК в диалоговом окне **Display Properties** (Свойства экрана).
6. Правой кнопкой мыши щелкните значок **My Network Places** (Сетевое окружение) и выберите **Properties** (Свойства).

7. Правой кнопкой мыши щелкните значок **Local Area Connection** (Подключение по локальной сети) *в* окне **Network Connections** (Сетевые подключения) и щелкните **Rename** (Переименовать). Назовите это подключение **WAN.**
8. Правой кнопкой мыши щелкните **Local Area Connection 2** (Подключение по локальной сети 2) и выберите **Rename.** Назовите это подключение **LAN.**
9. Правой кнопкой мыши щелкните **Local Area Connection 3** (Подключение по локальной сети 3) и выберите **Rename** (Переименовать). Назовите это подключение DMZ.

Теперь каждому интерфейсу можно присвоить IP-адрес. Начнем с внешнего интерфейса виртуальной машины брандмауэра ISA.

1. Правой кнопкой мыши щелкните интерфейс **WAN** и выберите **Properties** (Свойства).

   В диалоговом окне **WAN Properties** (Свойства глобальной сети) щелкните **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) и выберите **Properties** (Свойства).

   На вкладке **General** (Общие) диалогового окна **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета, TCP/IP) введите информацию об IP-адресе, как показано на рис. 4.18.

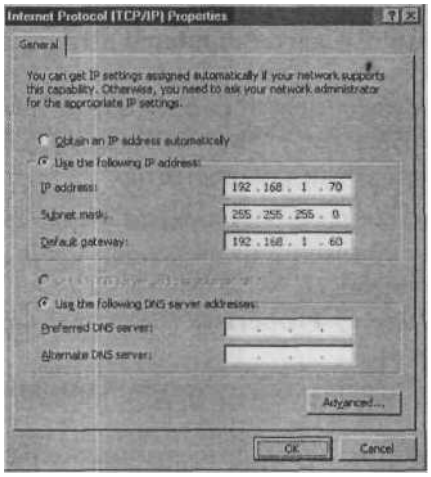


Рис. 4.18. Ввод информации об IP-адресе

4. Щелкните кнопку **Advanced...** (Дополнительно...).
5. В диалоговом окне **Advanced TCP/IP Settings** (Дополнительные параметры TCP/IP) щелкните вкладку DNS. На вкладке DNS снимите флажок в поле **Register this connection's addresses in DNS** (Зарегистрировать адрес этого подключения в DNS). Щелкните OK.

6. Щелкните OK в диалоговом окне Internet Protocol (TCP/IP) Properties (Свой ства протокола Интернета, TCP/IP).
7. Щелкните Close (Закрыть) в диалоговом окне WAN Properties (Свойства гло бальной сети).

Для настройки информации об IP-адресации интерфейса LAN выполните следующие действия.

1. Щелкните правой кнопкой мыши интерфейс LAN и выберите Properties (Свойства).
2. В диалоговом окне LAN Properties (Свойства локальной сети) щелкните запись Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и выберите Proper ties (Свойства).
3. На вкладке General (Общие) диалогового окна Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета, TCP/IP) (рис. 4.19) введите инфор мацию об IP-адресе, как показано на рис. 4.19.

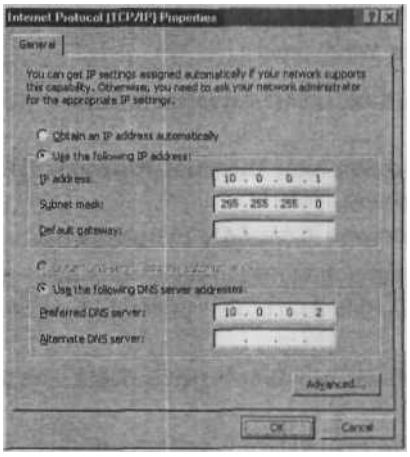


Рис. 4.19. Ввод информации об IP-адресе

4. Щелкните кнопку Advanced... (Дополнительно...).
5. В диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) щелкните вкладку DNS. На вкладке DNS снимите флажок в поле Register this connection's addresses in DNS (Зарегистрировать адрес этого подклю чения в DNS).
6. Щелкните вкладку WINS (рис. 420). На вкладке WINS щелкните Add (Добавить). В диалоговом окне TCPДР WINS Server (WINS-сервер TCP/IP) введите IP-адрес WINS-сервера. В данной виртуальной сети брандмауэра ISA контроллер домена также будет выступать в роли WINS-сервера. Введите 10.0.0.2 в этом диалого вом окне. Щелкните Add (Добавить).

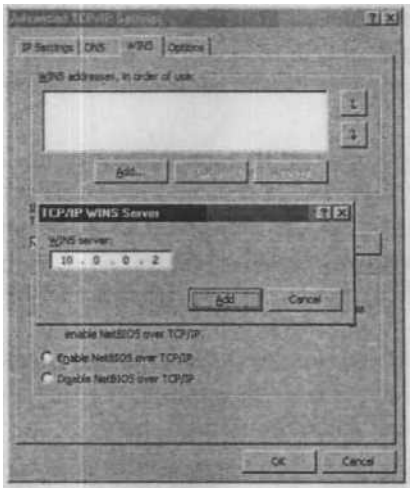


Рис. 4.20. Ввод адреса WINS-сервера

7. Щелкните ОК в диалоговом окне **Advanced TCP/IP Settings** (Дополнительные параметры TCP/IP).
8. Щелкните ОК в диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета, TCP/IP). 9. Щелкните ОК в диалоговом окне **LAN Properties** (Свойства локальной сети).

Наконец нужно настроить информацию об **IP-адресе** для интерфейса DMZ машины с брандмауэром ISA. Для настройки интерфейса DMZ выполните следующие действия.

1. Щелкните правой кнопкой мыши интерфейс **DMZ** и выберите **Properties** (Свойства).
2. В диалоговом окне **DMZ Properties** (Свойства демилитаризованной зоны) щелкните **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) **и** выберите **Properties** (Свойства).
3. На вкладке **General** (Общие) диалогового окна **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета, TCP/IP) введите информацию об IP-адресе, как показано на рисунке 4.21.
4. Щелкните кнопку Advanced... (Дополнительно...).
5. В диалоговом окне **Advanced TCP/IP Settings** (Дополнительные параметры TCP/IP) щелкните вкладку DNS. На вкладке **DNS снимите** флажок в поле **Register this connection's addresses in DNS** (Зарегистрировать адрес этого подключения в DNS).
6. Щелкните ОК в диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета TCP/IP).
7. Щелкните ОК в диалоговом окне **DMZ Properties** (Свойства демилитаризованной зоны).

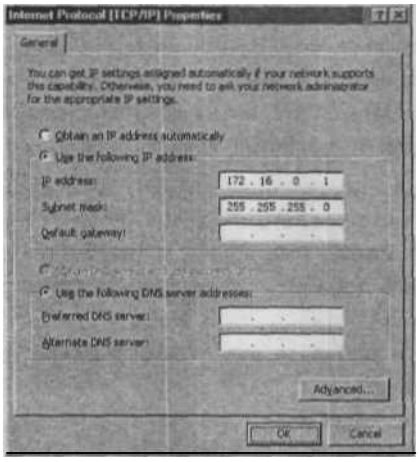


Рис. 4.21. Ввод информации об IP-адресе

Теперь операционная система Windows Server 2003 готова к работе с программным обеспечением брандмауэра ISA. В данный момент нужно создать копию конфигурации. Щелкните меню **Snapshot** (Копия) в окне **ISALOCAL-VMware Workstation** и щелкните **Save Snapshot** (Сохранить копию). Это позволит вернуться к базовой конфигурации операционной системы в случае, если нужно начать с чистого листа. При описании установки программного обеспечения брандмауэра ISA в главе 6 будет описано, как создать еще одну копию конфигурации *после* установки программного обеспечения брандмауэра ISA.

Методики, использованные при установке и настройке виртуальной машины ISALOCAL, могут применяться для установки других виртуальных машин в виртуальной сети брандмауэра ISA. Следует уделить особое внимание информации об IP-адресе для каждой виртуальной машины и присвоить каждой виртуальной машине верную виртуальную сеть. Проверить, правильно ли подключены машины к сетям, можно, послав команды ping с машин ISALOCAL или REMOTEISA на хосты в их сетях. Например, после создания машины EXCHANGE2OO3BE отправьте ping **10.0.0.2** с машины ISALOCAL. Если ответ не поступит, то, вероятнее всего, это объясняется тем, что либо была неправильно указана информация об IP-адресе на одной из машин, либо машины находятся в разных сетях VMnet.

Для того чтобы протестировать большинство сценариев, представленных в данной книге, нужно использовать следующие виртуальные **машины:**

- ISALOCAL;
- ISAREMOTE;
- CLIENT;
- EXCHANGE2003BE;
- REMOTECLIENT.

Обратите внимание, что не нужно заново выполнять всю настройку для машины REMOTECLIENT. Можно скопировать каталог для машины CLIENT в другое место, а затем изменить имя, информацию об IP-адресе и VMnet в копии. Это позволит создать машину REMOTECLIENT, которую можно использовать в упражнениях на создание VPN-подключений «узел-в-узел» в главе 9.

СОВЕТ Программное обеспечение VMware Workstation 4.0 поддерживает только три сетевые интерфейсные карты. Однако благодаря Александру Перилли (Alessandro Perilli) (http://www.virtualization.info) на виртуальную машину VMware можно добавить четвертую сетевую интерфейсную карту. Вот что нужно сделать. Откройте файл .vmz и добавьте эти строки в конец файла:

```
Ethernet3.present = "TRUE" ethernet3.addressType  =
"generated" ethernet3.generatedAddress  =  "00:0o: 29:
cb:7d:8f" ethernet3.generatedAddressOffset  =  "30"
ethernet3.connectionType  =  "custom" ethernet3.vnet =
"VMnet3"
```

Нельзя менять номер Ethernet и значение AddressOffset. Можно изменить значение address.Type, generatedAddress, connectionType и vnet.

Определение сетей и отношений между ними с точки зрения брандмауэров ISA

Одно из основных ограничений брандмауэра ISA Server 2000 заключалось в упрощенном понятии сети, они признавали только два типа сетей: надежные (trusted) и ненадежные (untrusted). Надежные сети включались в таблицу LAT (Local Address Table, локальная таблица адресов) брандмауэра ISA Server 2000. Любая сеть, которая не входила в таблицу LAT, считалась ненадежной. Политика брандмауэра ISA применялась ко всем взаимодействиям между хостами: входящим и не входяш,им в таблицу LAT. Взаимодействие между хостами LAT осуществлялось через брандмауэр ISA Server 2000, не подвергаясь механизмам фильтрации с отслеживанием соединений и проверки на уровне приложения брандмауэра ISA Server 2000.

Это создавало проблемы для администраторов брандмауэра ISA Server 2000, которые хотели создать сегменты DMZ (демилитаризованной зоны), имеющие прямое соединение с брандмауэром ISA Server 2000. Например, можно было выполнить **настройку** брандмауэра ISA Server 2000 **с** тремя сетевыми интерфейсами: внутренний интерфейс подключения ко внутренней сети, интерфейс DMZ подключения к сегменту DMZ общего доступа и внешний интерфейс подключения брандмауэра *к* Интернету.

В ISA Server 2000 такая конфигурация DMZ с тремя сетевыми интерфейсами обнаруживает большинство ограничений сетевой модели ISA Server 2000.

- Все взаимодействия между хостами LAT и другими хостами должны были вы полняться через службу NAT (служба трансляции сетевых адресов). Это означа ет, что все соединения между **внутренней** сетью и Интернетом, а также между внутренней сетью и сегментом DMZ выполнялись через службу NAT.
- Брандмауэр ISA Server 2000 не применял проверку с отслеживанием соедине ний на уровне приложения к соединениям между хостами Интернета и компь ютерами в сегменте DMZ. Эти соединения направлялись брандмауэром ISA Server 2000 из Интернета в сегмент DM2, и к ним применялась только фильтрация с отслеживанием соединений; то же самое можно наблюдать в случае с типичным брандмауэром на базе аппаратного обеспечения.
- Взаимодействие между хостами DMZ и хостами внутренней сети должно было выполняться по правилам публикации серверов и Web-публикации, потому что внутренняя сеть рассматривала сегмент DMZ как еще одну ненадежную сеть.
- Исходящие подключения из внутренней сети к сегменту DMZ подчинялись той же политике доступа, что и соединения между внутренней сетью и Интернетом. Например, если разрешался исходящий FTP-доступ из внутренней сети, то FTP-доступ разрешался ко *всем* сетям, не входящим в LAT. Если разрешался исходя щий доступ к конкретному протоколу, то у пользователей внутренней сети по являлся доступ к этому протоколу на *всех* узлах.
- Появилась возможность с помощью брандмауэра ISA Server 2000 заменять частные адреса на общедоступный адрес в сегменте DMZ. Однако брандмауэр ISA Server 2000 не распознавал этот сегмент как DMZ, а сегмент DMZ должен был разме щаться в LAT. Поскольку брандмауэр ISA Server 2004 применял политику бранд мауэра только к взаимодействию между хостами, входящими и не входящими в LAT, между внутренней сетью и сегментом DMZ с частным адресом брандмауэр не выполнял никакой фильтрации. Можно было использовать пакетные фильт ры RRAS (Routing and Remote Access Service, служба маршрутизации и удален ного доступа) для создания хоть какого-нибудь сегмента DMZ, но при этом па кетные фильтры RRAS обеспечивали еще меньшую гибкость и защиту, чем ме ханизмы фильтрации пакетов с отслеживанием соединений в брандмауэрах на базе аппаратного обеспечения.

Корпорация Microsoft признала эти недостатки брандмауэра ISA Server 2000 и исправила их. В брандмауэре ISA больше не используются таблицы LAT. Они и не требуются, потому что брандмауэр ISA не считает ни одну сеть надежной. В ISA Server 2000 надежность сети определялась с помощью таблицы LAT, которая теперь не является частью конфигурации брандмауэра ISA. Все подключения через брандма-уэр ISA подвергаются фильтрации с отслеживанием соединений и проверке с от-слеживанием соединений на уровне приложения брандмауэра ISA.

Другим важным улучшением сетевой модели брандмауэра ISA стала возможность контролировать отношения маршрутизации между любыми двумя сетями. Напри-мер, если нужно скопировать установку DMZ с тремя сетевыми подключениями:

внешний интерфейс, внутренний интерфейс и интерфейс DMZ, то можно использовать общие или частные адреса в сегменте DMZ и создать отношение типа «маршрут» или отношения NAT между внутренней сетью и сегментом DMZ. Можно даже выбирать между отношением типа «маршрут» и отношениями NAT между внутренней сетью и Интернетом. Это может стать особенно полезным, если во внутренней сети имеются общие адреса и нужно продолжать использовать их, не применяя службу NAT к исходящим соединениям с Интернетом.

В табл. 4.5 показаны новые и улучшенные функции сетевой модели брандмауэра ISA по сравнению с ISA Server 2000.

Табл. 4.5. Новые и улучшенные функции сетевой модели брандмауэра ISA

Функция	Описание
Все правила доступа включают элемент сети источника и адресата	Правила доступа контролируют, какие соединения проходят через брандмауэр. Два ключевых компонента правила доступа — это источник запроса на соединение и запрошенный адресат. Это позволяет установить жесткий контроль доступа по протоколу через брандмауэр. Можно разрешить пользователям IRC-доступ, но только в том случае, если запрос исходит из конкретной внутренней сети, а адресатом является другая сеть в пределах корпоративной ЛВС. IRC-запросы к любой другой сети, включая Интернет, запрещаются
Все соединения, проходящие через брандмауэр ISA, подвергаются фильтрации с отслеживанием соединений и проверке с отслеживанием соединений на уровне приложения	Все соединения, выполняемые через брандмауэр ISA, подчиняются политикам доступа брандмауэра ISA. В схеме сети брандмауэра ISA нет надежных сетей. Хотя можно выбрать маршрутизацию всех подключений от одной сети к другой по некоему правилу доступа, это не является обязательным требованием
Подключения между любыми двумя сетями можно маршрутизировать или проводить через службу NAT	Можно выбирать, как осуществлять соединения между любыми двумя сетями — с помощью маршрутизации или службы NAT. Можно выбрать службу NAT, если нужно скрыть адреса одной сети от другой сети, или же можно марш рути зировать пакеты из одной сети в другую сеть, если нужно использовать протоколы, которые не функционируют по NAT-подключениям. Возможность выбирать отношения **маршрутизации** *между* любыми двумя сетями обеспечивает гораздо большую свободу, чем используемый в ISA Server 2000 метод применения службы NAT для соединений между сетями, входящими и не входящими в LAT, и маршрутизации соединений между сетями LAT
Конфигурации клиентов брандмауэра и Web-прокси можно создавать для каждой сети	Можно создать несколько внутренних сетей и контролировать доступ между этими внутренними сетями с помощью правил доступа. Возможно, необходимо, чтобы в одной сети предоставлялся доступ клиенту Web-прокси, а не клиенту брандмауэра, в то же время **нужно,** чтобы в другой внутренней сети был доступ для клиента брандмауэра, но не для клиента Web-прокси. В брандмауэре ISA Server 2000 этого нельзя было сделать

Табл. 4.5. (окончание)

Функция	Описание
Брандмауэр ISA определяется как уникальная сеть	Одна из наиболее важных задач брандмауэра — самозащита. Существенным недостатком брандмауэра ISA Server 2000 является то, что механизм фильтрации пакетов применялся только к интерфейсам, не входящим в LAT. Поэтому интерфейсы, входящие в LAT, были полностью открытыми для подключений от любого хоста из LAT. Брандмауэр ISA определяет все свои интерфейсы как часть сети *локального хоста* и для разрешения подключений к *любому* интерфейсу брандмауэра ISA должны быть созданы правила доступа
VPN-клиенты относятся к отдельной сети	Брандмауэр ISA Server 2000 рассматривал VPN-клиентов как хосты LAT и не применял политику брандмауэра к соединениям VPN-клиентов. Брандмауэр ISA применяет как фильтрацию с отслеживанием соединений, так и проверку с отслеживанием соединений на уровне приложения ко всем соединениям между VPN-клиентами и любой другой сетью. Доступ VPN-клиентов к протоколам и компьютерам может быть ограничен по желанию
Изолированные VPN-клиенты представляют собой отдельную сеть	Брандмауэр ISA поддерживает изолирование VPN-подключений. Можно настроить брандмауэр ISA так, чтобы он запрашивал проверку VPN-клиентов, прежде чем они будут переведены в сеть VPN-клиентов. Это позволяет создавать собственные правила доступа, применяемые к изолированным VPN-клиентам, которые позволяют им обновить свои системы, чтобы удовлетворить требования безопасности сети Можно
Для упрощения конфигурирования правила доступа сети могут объединяться в группы	группировать сети, чтобы упростить контроль доступа. Например, нужно разрешить пользователям доступ из внутренних сетей A и B к ресурсам сети DMZ. Можно создать сети A и B и затем создать группу сетей, включающую обе эти сети, а затем разрешить доступ сетевой группе (Network Group). Сетевая группа затем упрощает создание правил доступа в последующих случаях, когда нужно создать правила доступа для этих двух сетей
Тщательный контроль сетевых объектов	Имеется контроль доступа на основании не только сети источника и адресата. Можно указать компьютеры, диапазоны адресов, подсети, подмножества компьютеров, подмножества URL и подмножества имен доменов. Каждый из этих сетевых объектов может использоваться для контроля доступа применительно к источнику и адресату в правилах доступа
Поддержка клиента SecureNAT	В брандмауэре ISA Server 2000 VPN-сервер требовал, чтобы VPN-клиенты были настроены как клиенты Web-прокси или как клиенты брандмауэра для доступа к Интернету через брандмауэр ISA, с которым у них было соединение. Брандмауэр ISA позволяет VPN-клиентам выступать в роли клиентов SecureNAT и позволяет им получать доступ в Интернет через тот же брандмауэр ISA, с которым они установили VPN-подключение. Конфигурация клиента SecureNAT расширена, потому что верительные данные VPN-клиента для входа в систему могут использоваться для разрешения контроля пользовательского/группового доступа между VPN-клиентом и любой другой сетью

Все эти моменты более подробно рассматриваются на протяжении этой книги.

ISA Server 2004: возможности при работе с несколькими сетями

Маркетинговая группа брандмауэра ISA 2004 использовала термин *multinetworking* (работа с несколькими сетями) применительно к новому и улучшенному набору сетевых функций брандмауэра ISA. Как и в большинстве случаев, сложно определить, что в точности означает этот маркетинговый термин. Возможно, под этим понимается способность брандмауэра ISA контролировать доступ между любыми двумя сетями с помощью фильтрации с отслеживанием соединений и проверки с отслеживанием соединений на уровне приложения. Этот термин также может означать способность брандмауэра ISA создавать несколько типов сетевых объектов и использовать эти сетевые объекты в правилах доступа. Он может также означать способность создавать несколько внутренних сетей, несколько сетей DMZ и несколько внешних сетей. Или он, возможно, означает все вышеперечисленное. Как и у термина *stateful* (с отслеживанием состояния соединений), у него нет конкретного значения, и его можно использовать в любом значении по желанию.

ПРЕДУПРЕЖДЕНИЕ Термин multinetworking, однако, не означает способность поддерживать несколько шлюзов по умолчанию на брандмауэре ISA. Это значит, что не может существовать один внешний интерфейс, подключенный к линии DSL, второй внешний интерфейс, подключенный к кабельной линии, и третий внешний интерфейс, подключенный к линии T1, и при этом невозможно использовать все эти три интерфейса для подключения к Интернету. Хотя все эти интерфейсы можно использовать для установки соединения с компьютерами через Интернет, только один из этих интерфейсов может использоваться для подключения к Интернету в целом, потому что для двух других интерфейсов необходимы определенные записи из таблицы маршрутизации для установки соединения с конкретными хостами или сетями в Интернете. Если нужно использовать несколько интернет-подключений для подключения к Интернету в целом, воспользуйтесь программным продуктом RainConnect от компании Rainfinity. Продукт RainConnect позволяет создавать несколько интерфейсов на брандмауэре ISA, а также дает возможность агрегации и присваивания приоритетов пропускной способности. Эта программа также позволяет публиковать ресурсы в защищенной сети за брандмауэром ISA и разрешать доступ к этим опубликованным ресурсам по всем интернет-подключениям и выравнивать нагрузку между ними на этих подключениях.

Для того чтобы получить представление о модели работы с несколькими сетями брандмауэра ISA 2004, рассмотрим схему сети. На рис. 4.22 показана типичная многосетевая конфигурация брандмауэра ISA.

Рис. 4.22. Работа с несколькими сетями в брандмауэре ISA

В этом примере есть четыре защищенные сети, непосредственно подключенные к брандмауэру ISA. Защищенная сеть включает в себя все сети, определенные на брандмауэре ISA, за исключением внешней сети по умолчанию. Внешняя сеть по умолчанию — это Интернет. Четыре защищенные сети в этой схеме: беспроводная сеть, DMZ, внутренняя сеть и сеть служб.

С помощью новой сетевой модели брандмауэра ISA можно создавать следующие правила доступа,-

- клиенты беспроводной сети могут получать доступ к Интернету, но им не раз решен доступ ко всем защищенным сетям. Пользователи беспроводной сети могут устанавливать VPN-подключение с брандмауэром ISA и получать доступ к сег менту внутренней сети, если им требуется этот доступ;
- серверы в сегменте DMZ могут получать доступ к серверам сегмента сети служб. Например, общий Web-сервер может получить доступ к серверу Exchange, но не может получить доступ к серверу SQL. В таком случае общий Web-сервер может выступать в роли RPC через HTTP-прокси для пользователей Outlook 2003. Хо сты в сегменте DM2 не могут получить **доступ** к Интернету, и им не разрешен доступ ко всем сегментам защищенной сети;
- пользователи и компьютеры внутренней сети могут получить доступ к ресур сам в Интернете и в сети служб. Это позволяет им использовать выборочные ресурсы, доступ к которым разрешен в Интернете, а также получать доступ к серверу Exchange. Пользователи внутренней сети не будут иметь доступа к ре сурсам в беспроводной сети или в сегменте DMZ;
- компьютеры в сети служб могут получать доступ к выборочным сайтам в Ин тернете (например, к сайту с обновлениями Windows Update). Они также могут

получать ограниченный доступ к внутренней сети. Например, сервер Exchange может быть членом домена сети Интернет и ему нужно взаимодействовать с контроллерами доменов во внутренней сети;

- VPN-клиентам может быть разрешен доступ к ресурсам в сети DMZ, в Интерне те, во внутренней сети и сети служб. Можно контролировать доступ различных VPN-клиентов к различным сетям с помощью контроля пользовательского/ группового доступа. Например, имеется группа пользователей под названием *ExchangeUsers* и нужно, чтобы они использовали клиента Outlook MAPI для ус тановки соединения с сервером Exchange, но не с другими ресурсами. Можно создать правило доступа, чтобы разрешить членам этой группы доступ к серве ру Exchange только с помощью безопасных Exchange RPC-вызовов к серверу Exchange. Если члены этой группы попытались бы использовать любой другой протокол, типа HTTP или CIFS (Common Internet File System, общий протокол доступа к файлам Интернет), то их попытки соединения были бы запрещены.

Функции работы с несколькими сетями позволяют осуществлять очень тщательный контроль доступа: можно контролировать, к каким адресатам может получить доступ хост любой сети. Даже VPN-клиенты, которые традиционно имеют доступ ко всем ресурсам корпоративной сети, как только они установят с ней соединение, могут теперь быть сильно ограничены после установления VPN-подключения.

Брандмауэр ISA: сети по умолчанию

Рассмотрим функции брандмауэра ISA по работе с несколькими сетями и то, как брандмауэр ISA рассматривает сети и как они используются, на примере сетей по умолчанию на брандмауэре ISA. Сразу же после завершения установки на брандмауэре ISA создаются сети по умолчанию:

- сеть локального хоста (Local Host Network);
- внутренняя сеть (Internal Network);
- внешняя сеть по умолчанию (External Network, default);
- сеть VPN-клиентов (VPN Clients Network);
- сеть изолированных VPN-клиентов (Quarantined VPN Clients Network).

Сети ISA 2004 должны соответствовать следующим критериям:

- на брандмауэре ISA должен быть один или несколько адаптеров. Если адаптер один, то все адреса рассматриваются как часть внутренней сети;
- сетевая интерфейсная карта должна иметь один или несколько IP-адресов. IP-адрес конкретного интерфейса должен принадлежать к сети локального хоста и к сети, с которой этот интерфейс имеет прямое соединение;
- за исключением сетей локального хоста, VPN-клиентов и изолированных VPN-клиентов IP-адрес может принадлежать только одной сети;
- все адреса, принадлежащие одной сетевой интерфейсной карте, должны при надлежать и той же сети.

В следующих разделах каждая из сетей по умолчанию рассматривается более подробно.

Сеть локального хоста

Сеть локального хоста — это встроенный сетевой объект, который определяет все IP-адреса на всех интерфейсах брандмауэра ISA. Например, если у брандмауэра ISA есть три сетевых интерфейса и десять IP-адресов, выделенных для внешнего интерфейса, два IP-адреса, выделенных для интерфейса DMZ, и один IP-адрес, выделенный внутреннему интерфейсу, то все 13 адресов будут составлять сеть локального хоста. Не нужно явно задавать никакие адреса сети локального хоста; адреса автоматически добавляются в сеть локального хоста при добавлении к интерфейсам.

Вкладка **Properties** (Свойства) сети локального хоста находится в узле Server-Name\Configuration\Networks. Щелкните вкладку **Networks** (Сети) на панели **Details** (Подробности), щелкните правой кнопкой мыши **Local Host** (Локальный хост) и выберите **Properties** (Свойства). Появится диалоговое окно **Properties** (Свойства), содержащее свойства сети локального хоста (рис. 4.23).

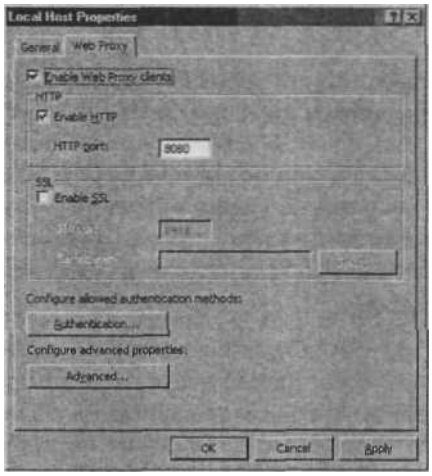


Рис. 4.23. Настройка приемника Web-прокси в сети локального хоста

В диалоговом окне **Local Host Network Properties** (Свойства сети локального хоста) есть две вкладки. Вкладка **General** (Общие) дает описание сети локального хоста. Вкладка **Web Proxy** (Web-прокси) позволяет включить приемник Web-прокси для сети локального хоста. Приемник Web-прокси является отключенным по умолчанию. Установите флажок в поле **Enable Web Proxy clients** (Разрешить клиентов Web-прокси), если нужно, чтобы приложения, работающие на брандмауэре ISA, выступали в роли клиентов Web-прокси.

ПРЕДУПРЕЖДЕНИЕ Для брандмауэра ISA *не включайте* Web-приемник сети локального хоста, чтобы разрешить хостам защищенной сети получать доступ к Интернету. Web-приемник сети локального хоста используется только компьютером с брандмауэром ISA. Ни один другой компьютер из защищенной или незащищенной сети не должен использовать Web-приемник локального хоста.

Например, если нужно использовать Web-браузер на самом брандмауэре ISA, то нужно включить приемник Web-прокси, а затем настроить браузер на использование IP-адреса одного из интерфейсов брандмауэра ISA в качестве своего сервера Web-прокси. Если IP-адрес на внутреннем интерфейсе брандмауэра ISA — 192.168.1.1, то этот IP-адрес следует использовать при настройке браузера в качестве клиента Web-прокси. Также нужно включить приемник Web-прокси в сети локального хоста, если требуется использовать задачи загрузки содержимого по расписанию.

Важный вопрос относительно сети локального хоста состоит в том, что как и в случае с сетями VPN-клиентов и изолированных VPN-клиентов, адреса, присвоенные этой сети, могут совпадать с адресами, присвоенными другим сетям. Во всех остальных случаях адреса, присвоенные другим сетям, не могут быть присвоены любой другой сети.

Например, если внутреннему интерфейсу брандмауэра ISA присвоен адрес 192.168.1.1, то этот адрес должен включаться в список адресов внутренней сети. Если у брандмауэра ISA есть адрес 172.16.0.1, присвоенный интерфейсу DMZ, то этот адрес должен включаться в список адресов, определяющих сеть DMZ. Распространенная ошибка состоит в том, что администраторы брандмауэра ISA не используют адреса, присвоенные сети локального хоста, потому что они придержи ваются общего принципа, состоящего в том, что одинаковые адреса не могут быть присвоены двум различным сетям.

СОВЕТ В брандмауэре ISA можно использовать адреса сети локального хоста для публикации служб, работающих на базе брандмауэра ISA. Например, можно настроить SMTP-ретранслятор на брандмауэре ISA и связать виртуальный SMTP-сервер с внутренним интерфейсом брандмауэра ISA. Затем этот IP-адрес публикуется при создании правила публикации SMTP-сервера. Также можно опубликовать сервер удаленного рабочего стола, работающий на базе брандмауэре ISA, связав сервер удаленного рабочего стола с одним из интерфейсов брандмауэра ISA, а затем опубликовать адрес этого интерфейса с помощью правила публикации сервера.

Внутренняя сеть

Внутренняя сеть ISA Server 2004 значительно отличается от внутренней сети ISA Server 2000. В ISA Server 2000 любая сеть, входящая в таблицу локальных адресов (Local Address Table, LAT), считалась внутренней сетью. Все взаимодействия между

хостами LAT (внутренней сети) не подвергались фильтрации и проверке *со* стороны брандмауэра ISA Server 2000. Причина этого состоит в том, что только взаимодействия между клиентами, входящими и не входящими в LAT, подвергались проверке со стороны брандмауэра ISA Server 2000.

В отличие от подхода к внутренним и внешним сетям, реализованном в брандмауэре ISA Server 2000, представление о внутренней сети для брандмауэра ISA связано с правилами системной политики, которые автоматически настраиваются на брандмауэре ISA.

Для того чтобы понять роль внутренней сети, нужно иметь общее представление о системной политике ISA 2004. Системная политика ISA 2004 является набором из 30 правил доступа, которые контролируют входящий и исходящий доступ к/от брандмауэра ISA. Эти правила создаются по умолчанию, но их можно изменить или даже отключить по желанию. Далее приведены примеры правил системной политики ISA 2004:

- разрешить доступ к службам каталогов в целях проверки подлинности;
- разрешить проверку подлинности Kerberos с ISA Server на надежные серверы;
- разрешить установку соединений по протоколу Microsoft CIFS (Common Internet File System, общий протокол доступа к файлам Интернета) с ISA Server на надежные серверы;
- разрешить установку соединений по интерфейсу NetBIOS с ISA Server на надежные серверы.

Для каждого из правил доступа системной политики соединения по умолчанию считаются от сети локального хоста к внугренней сети. Внутренняя сеть для брандмауэра ISA — это сеть, в которой расположены основные серверы сетевой инфраструктуры. Таким образом, правила системной политики по умолчанию разрешают соединения с серверами Active Directory, DNS-, DHCP-, WINS-серверами и файловыми серверами организации. Однако это представление о внутренней сети применяется для того, чтобы упростить установку брандмауэра ISA, потому что внутренняя сеть определяется в процессе установки программного обеспечения брандмауэра ISA. Но это определение внутренней сети не накладывает на пользователей никаких ограничений.

Важно отметить то, что можно создавать несколько *внутренних* сетей. Внутренней сетью может быть любая сеть, которая находится под защитой брандмауэра ISA. Фактически можно создавать сети DM2 и называть их внутренними сетями. Только внутренние сети по умолчанию имеют особое значение для брандмауэра ISA, и это значение связано с системной политикой.

> СОВЕТ Рекомендуется воспользоваться преимуществами внутренней сети по умолчанию и разместить все серверы на одной сетевой интерфейсной карте. Это сильно упрощает установку и настройку брандмауэра ISA, потому что позволяет усилить правила системной политики по умолчанию.

Свойства внутренней сети по умолчанию представлены в узле **ServerName\ Configuration\Networks.** Возможности конфигурирования внутренней сети по умолчанию точно такие же, как и для любой другой сети, создаваемой на брандмауэре ISA. Возможности конфигурирования внутренней сети могут использоваться как модель, на базе которой создаются или настраиваются другие внутренние сети или сети периметра на брандмауэре ISA.

Щелкните вкладку **Networks** (Сети) на панели **Details** (Подробности), а затем дважды щелкните **Internal network** (Внутренняя сеть). Щелкните вкладку **Addresses** (Адреса) и вы увидите диалоговое окно, похожее на изображенное на рис. 4.24.

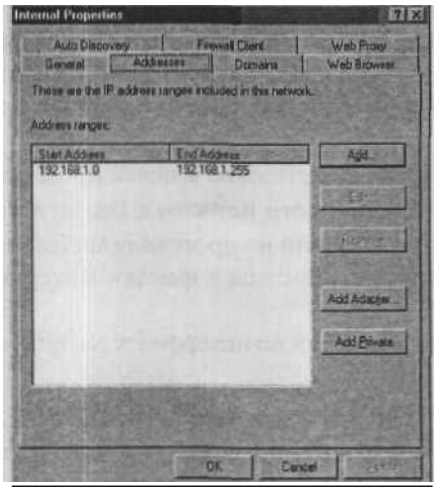


Рис. 4.24. Определение адресов внутренней сети

На вкладке **Addresses** (Адреса) введите адреса *всех* сетей, относящихся к адаптеру внутренней сети. В примере, показанном на рис. 4.25, внутренняя сеть]заключает в себя все адреса в диапазоне 192.168.1.0/24, определенные при установке программного обеспечения брандмауэра ISA.

Также легко добавить адреса в диапазон частных адресов. Щелкните кнопку **Add Private** (Добавить частный адрес) для добавления адресов в любой диапазон Ю адресов частной сети. На рис. 4.25 показано меню, появляющееся при нажатии на кнопку **Add Private** (Добавить частный адрес).

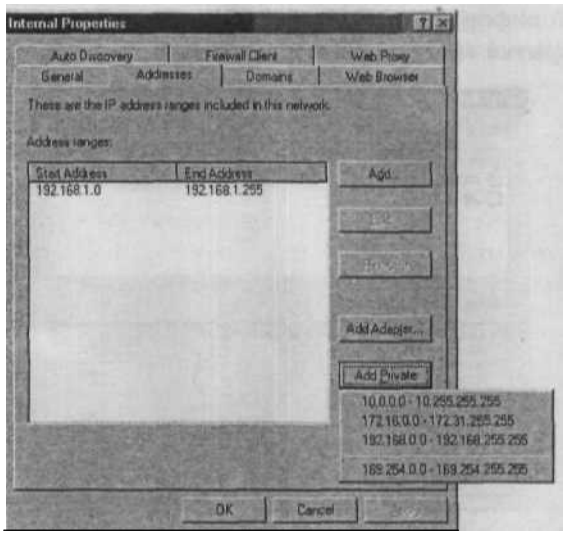


Рис. 4.25. Добавление адресов частной сети

ПРЕДУПРЕЖДЕНИЕ Не используйте диапазоны частных адресов, которые не входят во внутреннюю сеть, и не адресуйте весь диапазон частных адресов во внутреннюю сеть, если весь диапазон частных адресов не используется во внутренней сети. Это может привести к конфликтам, если имеются другие сети, которые используют подсети адресного диапазона частной сети. Например, две внутренние сети используют IP-адреса 192.168.1.0—192.168.1.255 и 192.168.2.0—192.168.2.255 соответственно. Присвоение внутренней сети адресного диапазона 192.168.0.0—192.168.255.255 станет причиной конфликта, который помешает использовать сетевые адреса 192.168.2.0/24 для второй внутренней сети. Поэтому рекомендуется никогда не пользоваться кнопкой Add Private при настройке адресов для сетей.

Лучшим способом добавления адресов к внутренней сети (и к другим создаваемым сетям) является использование кнопки **Add Adapter** (Добавить адаптер). На рис. 4.26 показан результат нажатия кнопки **Add Adapter** (Добавить адаптер).

В диалоговом окне **Select Network Adapters** (Выбрать сетевые адаптеры) можно выбрать сетевую интерфейсную карту, подключенную к внутренней сети, и использовать адреса из таблицы маршрутизации Windows для определения сети. Это более надежный метод определения конкретной сети, поскольку таблица маршрутизации Windows должна всегда содержать сведения обо всех сетях, к которым есть доступ с брандмауэра ISA. Это знание всех достижимых сетей возможно при использовании либо ручной настройки таблицы маршрутизации Windows, либо протокола динамической маршрутизации типа RIP (Routing Information Protocol, про-

токол маршрутной информации) или OSPF (Open Shortest Path First, протокол первоочередного открытия кратчайших маршрутов).

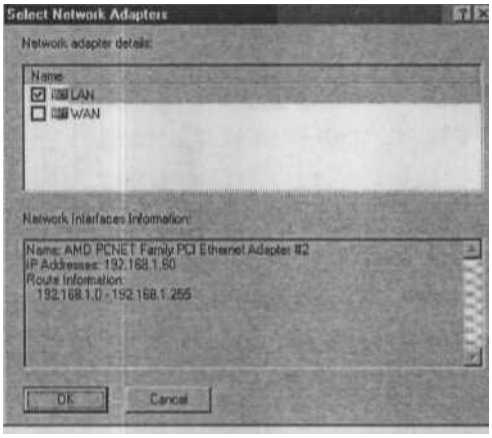


Рис. 4.26. Добавление адресов с помощью таблицы маршрутизации

Еще один способ добавления адресов в сеть состоит в использовании кнопки Add (Добавить). На рис. 4.27 показан результат нажатия кнопки Add (Добавить).

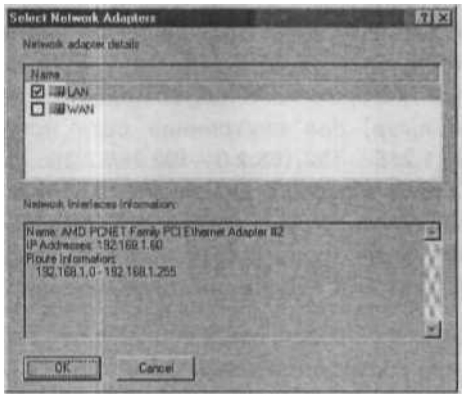


Рис. 4.27. Введение адресного диапазона

Щелкните вкладку Domains (Домены) (рис. 4.28). Здесь представлен список доменов внутренней сети. Когда клиент брандмауэра устанавливает соединение с хостом, расположенным в одном из этих доменов, запрос на соединение блокирует приложение клиента брандмауэра. Основная причина этого заключается в том, что если все компьютеры, расположенные в одном домене, находятся на одной сетевой интерфейсной карте, то компьютер клиента брандмауэра может выполнять соединение напрямую, не делая петлю через брандмауэр ISA. Это понижает общую

нагрузку на брандмауэр ISA и улучшает производительность клиента, потому что соединение не вызывает никакой нагрузки на брандмауэр. Кроме того, вкладка Domains (Домены) может использоваться для того, чтобы контролировать поведение клиентов Web-прокси, когда они получают доступ к внешним узлам. Отношения между вкладкой **Domains** (Домены) и клиентами Web-прокси обсуждаются далее в этой главе.

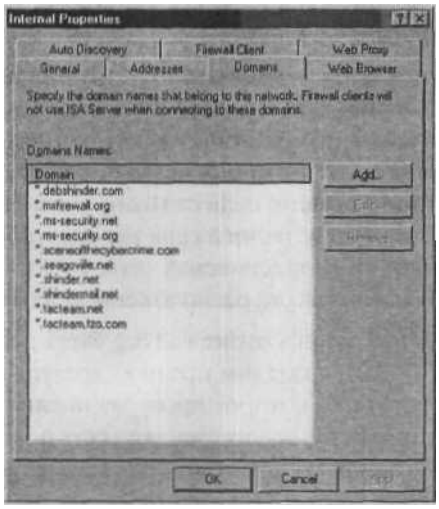


Рис. 4.28. Введение локальных доменов

Следует быть внимательными с записями на вкладке Domains (Домены), если домен внутренней сети охватывает несколько сетевых интерфейсных карт. На рис. 4.29 показан пример сценария, когда домен охватывает несколько сетевых интерфейсов.

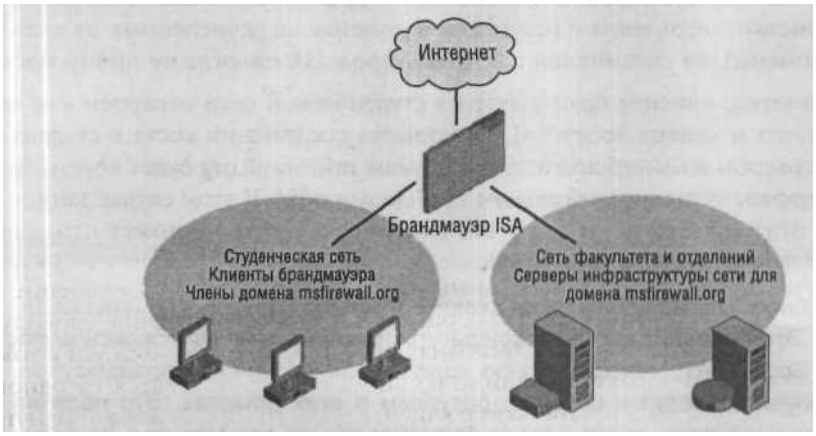


Рис. 4.29. Домен распространяется на внутренние сети

Это пример простой конфигурации университетской сети. На брандмауэре ISA есть три сетевых интерфейса: первый соединяет брандмауэр ISA с Интернетом, второй соединяет брандмауэр ISA с внутренней сетью, а третий соединяет брандмауэр ISA со второй внутренней сетью. Внутренняя сеть (сеть факультета и отделений) содержит серверы Active Directory и другие серверы инфраструктуры. Другая внутренняя сеть (студенческая сеть) содержит компьютеры студентов, которые вошли в университетский домен Active Directory, на этих компьютерах также установлен клиент брандмауэра.

Имя домена внутренней сети — *msfirewall.org*. Это имя домена следует добавить на вкладке Domains (Домены). Когда любой хост внутренней сети устанавливает соединение с любым хостом в домене msfirewall.org, компьютеры клиента брандмауэра во внутренней сети обходят брандмауэр ISA и устанавливают непосредственное соединение с хостами в домене msfirewall.org, расположенном за адаптером внутренней сети. Поскольку во внутренней сети нет хостов, которым нужно инициировать соединения с хостами в студенческой сети, то все в порядке. Это объясняется тем, что все серверы msfirewall.org расположены за адаптером внутренней сети.

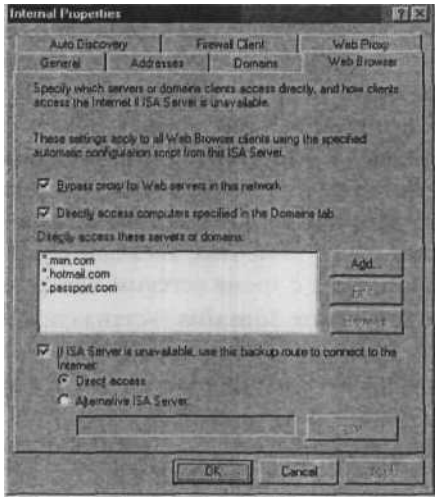
Теперь предположим, что запись msfirewall.org была добавлена на вкладку **Domains** (Домены) в сети DMZ, и создадим правило доступа (подробно правила доступа рассматриваются в главе 7), которое проверят подлинность клиентов студенческой сети и разрешает им доступ во внутреннюю сеть по протоколам HTTP, HTTPS (HyperText Transmission Protocol Secure, протокол защищенной передачи гипертекстов), FTP, SMTP и POP3. Если компьютеры, настроенные *только* как клиенты брандмауэра в студенческой сети, попытаются установить соединение с сервером POP3 во внутренней сети, запрос на соединение будет запрещен. Это объясняется тем, что интерфейс студенческой сети на брандмауэре ISA был настроен с помощью домена msfirewall.org на вкладке **Domains** (Домены). Поскольку компьютер, настроенный как клиент брандмауэра, будет обходить конфигурацию клиента брандмауэра при установке соединения с ресурсами в доменах, перечисленных на вкладке **Domains** (Домены), то соединения с брандмауэром ISA никогда не произойдет.

Если компьютер клиента брандмауэра в студенческой сети настроен как клиент брандмауэра и клиент SecureNAT, то попытка соединения хоста в студенческой сети с сервером во внутренней сети в домене msfirewall.org будет перенаправлена на интерфейс студенческой сети на брандмауэре ISA. В этом случае запрос на соединение будет отвергнут, потому что клиент SecureNAT не может отправить верительные данные на брандмауэр ISA.

> СОВЕТ Также можно добавить на вкладке Domains (Домены) домены внешней сети. Это позволит хостам, сконфигурированным как Web-прокси и/или клиенты SecureNAT, обходить свою конфигурацию клиента брандмауэра, чтобы получить доступ к интернет-ресурсам в этих доменах. Это полезно в тех редких случаях, когда клиент брандмауэра не совместим с конкретным программным обеспечением на компьютере клиента брандмауэра.

Рис. 4.30. Настройка доменов для прямого доступа к Web-прокси

В диалоговом окне **Internal Properties** (Внутренние свойства) щелкните на вкладке **Web Browser** (Web-браузер) (рис. 4.30).



Настройки на этой вкладке контролируют Web-браузеры во внутренней сети, которые настроены на использование сценария автоконфигурации (сценарий автоконфигурации более подробно рассматривается в главе 5). Имеется несколько вариантов на выбор.

я Bypass proxy for Web servers in this network (Обходить прокси для Web-серверов в этой сети). Это интересная настройка. В файле справки приводится такой комментарий: *"**Bypass proxy for web servers in this network.** Select this option ifthe Web browser on the Firewall client computer should bypass the ISA Server computer when accessing local Web servers»* (Обходить прокси для Web-серверов в этой сети. Выбирайте этот вариант, если Web-браузер на компьютере клиента брандмауэра должен обходить компьютер ISA Server при получении доступа к локальным Web-серверам). Вопрос в том, что такое локальный Web-сервер. Локальный по отношению к чему? В данном случае *локальный* означает любой Web-сервер, расположенный по адресу, входящему в адресный диапазон сети. Поэтому в случае внутренней сети, когда клиент Web-прокси со сценарием автоконфигурации пытается установить соединение с Web-сервером, адрес которого также находится во внутренней сети, клиент Web-прокси будет обходить Web-прокси на брандмауэре ISA и устанавливать соединение напрямую с Web-сервером во внутренней сети. Это дает определенные преимущества: хосты, расположенные за одним сетевым адаптером, не образуют петель через брандмауэр ISA для получения доступа к ресурсам, находящимся за одним сетевым интерфейсом.

- **Directly access computers specified on the Domains tab** (Напрямую устанав ливать доступ к компьютерам, указанным на вкладке Домены). Это позволяет кли енту Web-прокси, настроенному с помощью сценария автоконфигурации, исполь зовать домены, перечисленные на вкладке **Domains** (Домены) для *прямого дос туна.* Прямой доступ для клиентов Web-прокси позволяет компьютеру клиента Web-прокси обходить Web-прокси на брандмауэре ISA и устанавливать соедине ние напрямую с адресатом либо через компьютеры с конфигурацией клиента SecureNAT, либо с помощью компьютеров с конфигурацией клиента брандмауэ ра. Такой вариант оказывается полезным, если нужно использовать домены, уже добавленные на вкладку **Domains** (Домены), для прямого доступа. Однако не за бывайте об упомянутых ранее моментах, касающихся студенческой и внутрен ней сети в конфигурации DMZ с тремя сетевым интерфейсами.
- **Directly access these servers or domains** (Устанавливать прямой доступ к этим серверам или доменам). Можно при желании добавить список доменов или IP-адресов, которые должны быть настроены клиентами Web-прокси с помощью сценария автоконфигурации для обхода Web-прокси на брандмауэре ISA. В при мере, показанном на данном рисунке, был добавлен список доменов, которые следует обходить при использовании Outlook Express для доступа к учетной записи Hotmail. Когда компьютер клиента Web-прокси устанавливает соедине ние с этими доменами, конфигурация клиента Web-прокси игнорируется, а кли ент использует альтернативную конфигурацию клиента для доступа к этим сайтам, например конфигурации клиента SecureNAT или клиента брандмауэра.
- **If ISA Server is unavailable, use this backup route to connect to the Internet: Direct access or Alternative ISA Server** (Если ISA Server недоступен, используй те этот запасной маршрут для установки соединения с Интернетом: прямой до ступ или альтернативный ISA Server). Этот вариант немного вводит пользователя в заблуждение, потому что в нем подразумевается, что весь брандмауэр ISA дол жен быть недоступен, прежде чем пользователь выберет один из вариантов. Фак тически брандмауэр ISA может работать как обычно, но если возникает пробле ма с Web-прокси брандмауэра ISA, то используется одна из предлагаемых возмож ностей. Вариант **Direct Access** (Прямой доступ) позволяет компьютеру, настро енному как клиент Web-прокси, использовать альтернативную конфигурацию кли ента для получения доступа к Интернету или к другой сети-адресату. Это может быть либо конфигурация **клиента** SecureNAT, либо конфигурация клиента бранд мауэра. Вариант **Alternative ISA Server** (Альтернативный ISA Server) позволяет войти в FQDN (Fully Qualified Domain Name, полностью определенное имя доме на) или IP-адрес альтернативного брандмауэра ISA, с которым может выполнить соединение клиент Web-прокси для получения доступа в Интернет. Не **следует** использовать кнопку **Browse** (Просмотр) для поиска альтернативного сервера. Если в текстовом поле **Alternative ISA Server** (Альтернативный ISA Server) использу ется FQDN, то следует убедиться, что брандмауэр ISA может разрешить этот FQDN

для правильного IP-адреса с тем, чтобы брандмауэр ISA мог установить местоположение альтернативного Web-прокси.

СОВЕТ Малоизвестен тот факт, что один из наиболее мощных методов, который можно использовать для контроля доступа клиентов Web-прокси, — это сценарий автоконфигурации. По возможности клиентов Web-прокси следует всегда настраивать на применение *только* сценария автоконфигурации. Единственным исключением является случай, когда используется WPAD (Web Proxy Autodiscovery Protocol, протокол автообнаружения Web-прокси) и автообнаружение для конфигурирования клиентов Web-прокси. Когда используется автообнаружение, информация сценария автоконфигурации автоматически копируется на клиента Web-прокси. Сценарии автоконфигурации позволяют легко создавать список пропускаемых адресов (bypass list) для клиентов Web-прокси, так что они могут использовать альтернативные конфигурации клиентов для получения доступа к тем узлам, которые не работают с серверами Web-прокси, совместимыми с CERN (например, ISA 2004).

Щелкните на вкладке **Web Proxy** (Web-прокси), определяющей исходящий Web-приемник для сети. Клиенты Web-прокси в этой сети используют этот Web-приемник для установки соединения с Web-прокси на брандмауэре ISA. Исходящий приемник Web-прокси для сети можно активировать, установив флажок в поле **Enable Web Proxy clients** (Включить клиентов Web-прокси). Флажок также должен быть установлен в поле **Enable HTTP** (Разрешить HTTP) для Web-браузеров, настроенных как клиенты Web-прокси, для установки соединения с Web-прокси в этой сети. Данные действия показаны на рис. 4.31.

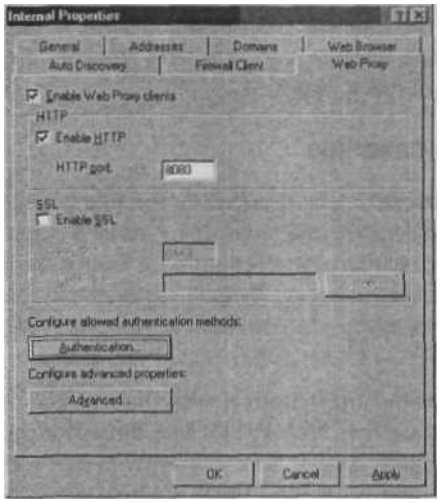


Рис. 4.31. Вкладка Web Proxy (Web-прокси)

Настройка **Enable SSL** (Разрешить SSL) на странице **Web Proxy** (Web-прокси) в ISA Server 2000 представляла собой любопытный случай, потому что если включался этот вариант, а затем Web-браузер настраивался на установку соединения с SSL-портом по умолчанию на исходящем SSL-приемнике Web-прокси, то попытка соединения не была успешной. Причина этого состоит в том, что Web-браузер, который настроен как клиент Web-прокси, не может установить SSL-подключение с приемником Web-прокси. Начальное соединение между клиентом Web-прокси и исходящим приемником Web-прокси должно всегда выполняться по протоколу HTTP.

Если соединение между клиентом Web-прокси и исходящим приемником Web-прокси должн о всегда выполняться по протоколу HTTP, то зачем на вкладке **Web Proxy** (Web-прокси) имеется вариант **Enable SSL** (Разрешить SSL)? Это объясняется тем, что в случае создания цепочки Web-прокси нижестоящий сервер Web-прокси можно настроить на перенаправление Web-запросов вышестоящему серверу Web-прокси с помощью SSL-подключения. Такая установка позволяет создавать исходящий мост HTTP-SSL между нижестоящим Web-прокси и вышестоящим Web-прокси.

> СОВЕТ Всегда оставалось загадкой, почему Web-браузер не был разработан для поддержки SSL-подключений к Web-прокси на брандмауэре ISA. Это позволило бы создавать безопасные SSL-подключения между клиентом и Web-прокси, при том что URL может относиться к HTTP-содержимому в Интернете. Может создаться впечатление, что эта функция не очень полезна, но фактически вероятнее то, что кто-то установил анализатор пакетов в вашей сети, чем то, что анализатор пакетов имеется на любой сети между вашей сетью и сетью-адресатом. Также с большой степенью вероятности можно утверждать, что хозяин анализатора пакетов ищет в вашей сети конкретные данные, например имена и пароли пользователей. Возможно следующие версии Web-клиента Internet Explorer будут поддерживать такой тип конфигурации.

Внешняя сеть по умолчанию

Внешняя сеть по умолчанию, созданная во время настройки брандмауэра ISA включает в себя все адреса, которые еще не определены в другой сети на брандмауэре ISA. Внешняя сеть по умолчанию не содержит каких-либо диалоговых окон для выполнения настроек пользователя. Любой адрес, который не задан в некоторой другой сети брандмауэра ISA автоматически включается во внешнюю сеть по умолчанию.

Это особенно интересно при упрощенной настройке брандмауэра ISA с одной интерфейсной сетевой картой. При установке программного обеспечения брандмауэра ISA на компьютере с одной сетевой картой или в случае применения шаблона настройки сети с одной сетевой картой к имеющейся конфигурации, все адреса в диапазоне адресов IPv4 добавляются к внутренней сети по умолчанию. По-

скольку все возможные адреса включены во внутреннюю сеть по умолчанию, то не существует адресов, которые были бы доступны для внешней сети по умолчанию.

> СОВЕТ В конфигурации брандмауэра с единственным сетевым адаптером все адреса рассматриваются как внутренние. Поскольку в таком случае нет внешних адресов, то невозможно использовать внешнюю сеть в правилах доступа в конфигурации с одним сетевым адаптером. Эта проблема будет обсуждаться подробнее при изучении шаблона настройки сети с одним сетевым адаптером.

Сеть VPN-клиентов

Сеть VPN-клиентов является одной из виртуальных сетей. Когда VPN-клиент или VPN-шлюз устанавливает соединение с брандмауэром ISA, этот адрес динамически добавляется к сети VPN-клиентов.

Например, предположим, что для присваивания адресов VPN-клиентам и шлюзам используется DHCP. Когда VPN-клиент устанавливает соединение с брандмауэром ISA, адрес, присвоенный VPN-клиенту, перемещается в список адресов, входящих в сеть VPN-клиентов. Правила доступа, в которых используется сеть VPN-клиентов для адреса источника или назначения, затем применяются к адресу, присвоенному VPN-клиенту или шлюзу. Когда VPN-клиент или шлюз разрывают соединение с брандмауэром ISA, этот адрес динамически удаляется из сети VPN-клиентов.

> СОВЕТ Имеется возможность присваивать IP-адреса VPN-клиентам и шлюзам, используя либо DHCP, либо статический пул адресов. Рекомендуется использовать DHCP, поэтому что это немного упрощает задачу. Если же используется статический пул адресов, то придется удалить эти адреса из определения внутренней сети, если адреса подсети будут использоваться для статического пула адресов VPN-клиентов. Этот вопрос подробнее рассматривается в главе 9, посвященной конфигурированию брандмауэра ISA в качестве VPN-сервера и шлюза.

Сеть изолированных VPN-клиентов

Сеть изолированных VPN-клиентов представляет собой виртуальную сеть, в которой адреса динамически присваиваются этой сети, когда изолированные VPN-клиенты устанавливают соединение с брандмауэром ISA. Сеть изолированных VPN-клиентов используется только при включенном режиме изолирования VPN-подключений на брандмауэре ISA.

В настоящее время изолирование VPN-подключений представляет собой скорее базовую платформу, а не то, чем может воспользоваться на практике рядовой администратор брандмауэра ISA. Но есть и хорошая новость: Federic Esnouf, MVP брандмауэра ISA, скомпилировал очень неплохой пакет изолирования VPN-подклю-

чений, который прост в установке и конфигурировании. Ознакомиться с решением Federic в области изолирования VPN-подключений можно по адресу: http:// fesnouf.online.fr/programs/QSS/qssinaction/QssI nAction.htm.

> СОВЕТ Если все сложные требования изолирования VPN-подключений не были выполнены, а изолирование VPN-подключений на брандмауэре ISA было включено, то все VPN-клиенты и шлюзы будут изолированы и никогда не смогут покинуть сеть изолированных VPN-подключений. Поэтому рекомендуется не включать режим изолирования VPN-подключений на брандмауэре ISA, если нет знаний на уровне разработчика и глубокого понимания базовой платформы, которая лежит в основе изолирования VPN-подключений.

Создание новых сетей

Обычно добавление новой сети, появившейся в сетевом окружении, происходит при установке дополнительных сетевых интерфейсных карт на брандмауэр ISA. Поскольку все адреса, расположенные на одной сетевой интерфейсной карте, рассматриваются брандмауэром ISA как сеть, необходимо создать новую сеть при добавлении дополнительных сетевых интерфейсных карт к брандмауэру.

Один из любопытных аспектов сети связан с тем, как его можно применить к сетям, расположенным *перед* внешним сетевым интерфейсом брандмауэра ISA. Внешний интерфейс брандмауэра ISA не всегда должен быть напрямую соединен с Интернетом. Во многих организациях брандмауэр ISA используется в качестве внутреннего брандмауэра, потому что требуется обеспечить наилучшую защиту корпоративного имущества. Организация контролирует соединение между внешним интерфейсом внутреннего брандмауэра и сетью, поэтому внешний интерфейс можно определить и настроить как сетевой объект в интерфейсе конфигурирования брандмауэра ISA.

Например, предположим, что у внешнего брандмауэра ISA есть две сетевых интерфейсных карты: одна из них соединена с сегментом DMZ, а другая — с: сетью корпорации. Поскольку адреса, используемые в сети DMZ, известны, можно создать сетевой объект, который определяет адресный диапазон, используемый в DMZ, а затем использовать этот сетевой объект для контроля трафика, входящего и исходящего из DMZ, когда он проходит через внутренний брандмауэр ISA.

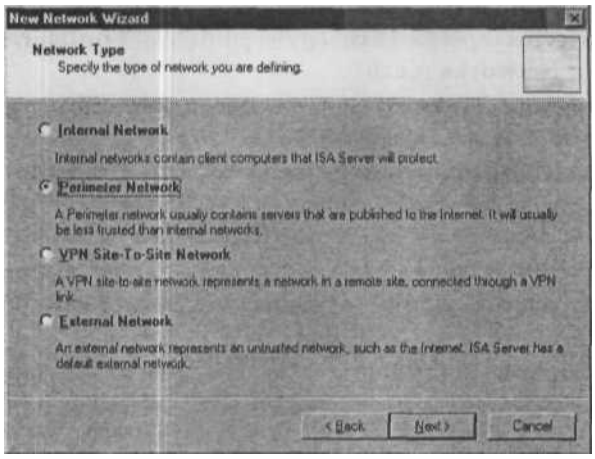
В следующем упражнении сетевой объект будет добавлен на брандмауэр ISA, когда будет установлена дополнительная сетевая интерфейсная карта для поддержки сегмента DMZ. Брандмауэр ISA уже имеет один внешний интерфейс с сетевым адресом 192.168.1.0/24 и один внутренний интерфейс 10.0.0.0/24. Новой сетевой интерфейсной карте присваивается IP-адрес 172.16.0.1/16, и для этого интерфейса DMZ будет создана новая сеть.

Для создания новой сети нужно выполнить следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел Configuration (Настройка). Щелкните узел **Networks** (Сети).
2. Щелкните на вкладке **Tasks** (Задачи) на панели задач. Щелкните ссылку **Create a New Network** (Создать новую сеть).
3. На странице **Welcome to the New Network Wizard** (Вас приветствует мастер соз дания новой сети) введите имя новой сети в текстовое поле **Network name** (Имя сети). В данном примере она будет называться **DMZ.** Щелкните **Next** (Далее).
4. На странице **Network Type** (Тип сети) выберите вариант **Perimeter Network** (Сеть периметра) (рис. 4.32). В открывшемся диалоговом окне должно быть четыре варианта:
   - o **Internal Network** (Внутренняя сеть) — создание НОВОЙ **внутренней** сети, расположенной «внутри* брандмауэра ISA. Этот критерий не является жестким, поскольку брандмауэр ISA не рассматривает окружающее в противопоставлении "внешнее - внутреннее», он применяет фильтрацию с отслеживанием соединений и проверку с отслеживанием соединений ш **уровне** приложения *ко всем* соединениям, устанавливаемым через него. Обозначение «внутренний» в данном случае применяется скорее для учета используемых ресурсов. При выборе этого варианта можно настроить сеть с помощью диалогового окна **Properties** (Свойства) и установить настройки, схожие с теми, которые можно установить для внутренней сети по умолчанию;
   - D **Perimeter Network** (Сеть периметра) — создание новых сегментов DMZ. Настройки сети периметра и внутренней сети, заданные мастером при их создании, практически не различаются. В диалоговом окне **Properties** (Свойства) представлены те же варианты, что и при создании внутренней сети. Основным преимуществом является то, что в пользовательском интерфейсе можно легко определить, **какие** сети являются внутренними, а какие — DMZ;
   - **D VPN Site-to-Site Network** (сеть VPN «узел-в-узел») — создание VPN-подключения "узел-в-узел» с другим офисом. Этот мастер позволяет задать адресный диапазон *и* конфигурацию VPN для VPN-подкяючения «узел-в-узел»;
   - **D External Network** (Внешняя сеть) — создание сети, находящейся «вне» брандмауэра ISA. Хотя брандмауэр ISA не делит все сети на внутренние и внешние, можно придерживаться следующего практического правила: любую сеть, доступную с интерфейса брандмауэра ISA, в которой есть шлюз по умолчанию, связанный с брандмауэром ISA, можно рассматривать как внешнюю сеть. Стоит обратить внимание на то, что при создании новой внешней сети, так же как и при создании новой внутренней сети или сети периметра, в диалоговом окне **Properties** (Свойства) приводятся одинаковые варианты конфигурации.
5. Щелкните **Next** (Далее).

Рис. 4.32. Определение типа сети

На рис. 4.32 показано определение типа сети и использование сети периметра.



6. На странице **Network Addressees** (Сетевые адреса) (рис. 4.33) определяется адресный диапазон для новой сети. Имеются три варианта:
   - **Add** (Добавить) — адресный диапазон можно добавить вручную. Это может пригодиться, когда не нужно определять весь адресный диапазон сети или нужно добавить к сети несколько непоследовательных диапазонов IP-адресов;
   - **Add Adapter** (Добавить адаптер) — в диалоговом окне можно выбрать адап тер для определения новой сети. Добавляемые адреса основываются на за писях в таблице маршрутизации Windows, относящихся к этому адаптеру Если перед созданием новой сети таблица маршрутизации ОС Windows была на строена верно, то будут добавлены все правильные адреса. Это самый про стой способ определения новой сети, если таблица маршрутизации содер жит верную информацию;
   - **Add Private** (Добавить частные). При нажатии этой кнопки появляется всплы вающее меню, в котором показаны три диапазона частных сетевых адресов. Настоятельно не рекомендуем использовать этот вариант, потому что во многих организациях повсеместно используются подмножества частных сетевых адресов.

Нажмите кнопку **Add Adapter** (Добавить адаптер) — появится диалоговое окно **Select Network Adapters** (Выберите сетевые адаптеры) (см. рис. 4.33). Установите флажок в поле **DMZ** (в данном примере адаптерам были присвоены осмысленные имена в окне **Network and Dial-up Connections** — сетевые и dial-up подключения). Будут выведены адреса, которые присвоятся сети на основании маршрутной информации, приведенной в разделе **Network Interfaces Information** (Информация о сетевых подключениях). Щелкните OK.

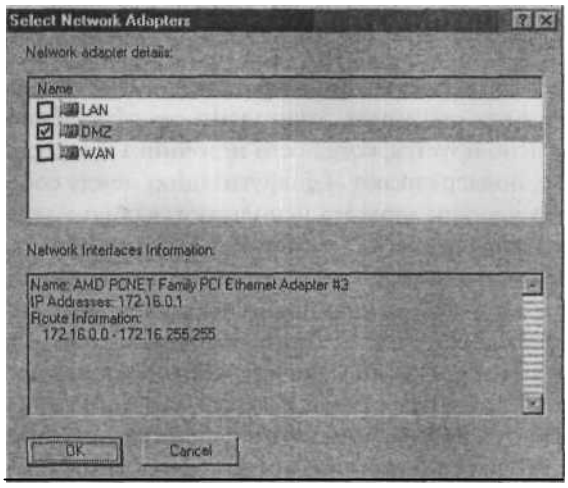


Рис. 4.33. Выбор сетевого адаптера

7. Щелкните **Next** (Далее) на странице **Network Addresses** (Сетевые адреса).
8. Щелкните **Finish** (Готово) на странице **Completing the New Network Wizard** (Завершение работы мастера создания новой сети).
9. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
10. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
11. Новая сеть появится в списке на вкладке **Networks** (рис. 4.34).

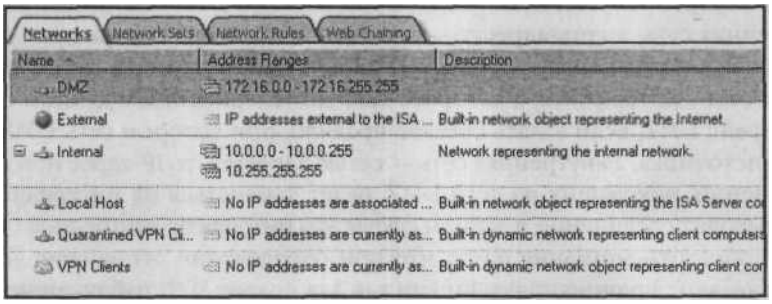


Рис. 4.34. Новая сеть появилась в списке сетей

Контроль маршрутизации с помощью сетевых правил

Новую сеть нельзя использовать до тех пор, пока не будут определены отношения маршрутизации между этой сетью и другими сетями, с которыми она взаимодействует. Эти отношения маршрутизации регулируются с помощью ***сетевых правил*** (Network Rules).

При создании сетевого правила используются три типа отношений маршрутизации:

- **Route** (Маршрут). В документации к брандмауэру ISA отношение типа «маршрут» определяется как «взаимное, эквивалентное» отношение. На практике этот тип отношения используется, когда сети источника и адресата, определенные в сетевом правиле, поддерживают маршрутизацию между собой. Например, если в сети источника и в сети адресата используются общие адреса, то между ними можно задать отношение типа «маршрут». Если и в сети источника, и в сети адресата используются частные адреса, то также можно выбрать отношение типа «маршрут». Если же в сети источника используются частные адреса, а в сети адресата — общие адреса, то этот тип отношения использовать нельзя (в большинстве случае, однако, есть исключения, когда брандмауэр ISA имеет запись в таблице маршрутизации, разрешающую маршрутизацию из частных сетей в сети общего пользования). Другой важной особенностью отношения типа «маршрут» является то, что IP-адрес источника всегда сохраняется (за исключением правил публикации, в которых можно контролировать, сохранять или нет IP-адрес источника, а IP-адрес сервера всегда заменяется на адрес приемника). Отношение типа «маршрут» следует использовать, если сеть источника и адресата поддерживают этот тип отношения и нужно обеспечить поддержку протоколов, несовместимых с NAT.
- **NAT.** Документация к брандмауэру ISA определяет отношение NAT как направленное. Направленность отношения NAT означает, что при настройке сетевого правила нужно учитывать сеть источника и сеть адресата. При использовании отношения NAT IP-адрес источника заменяется на адрес интерфейса, с которого выходит соединение. Например, предположим, что задано отношение NAT между внутренней сетью по умолчанию и сетью DMZ. Сеть-источник — это внутренняя сеть, а сеть-адресат — это сеть DMZ. Когда соединения устанавливаются из внутренней сети с сетью DMZ, IP-адрес источника заменяется на адрес сетевого интерфейса, с которого выходит соединение; в данном случае это интерфейс DMZ. Если задать сетевое правило, при котором сеть DMZ является сетью источника, а внутренняя сеть — сетью адресата, то I P-адрес источника для соединений, исходящих из сети DMZ, будет заменяться на интерфейс, с которого выходит соединение; в данном случае это интерфейс внутренней сети. Также нужно обратить внимание на то, что при определении отношения NAT соединения являются однонаправленными как для правил Web-публикации, так и для правил доступа.

Для любого соединения между конкретной сетью источника и сетью назначения нужно задать сетевое правило. Если на брандмауэре ISA все настройки выполнены правильно, но какая-то политика доступа отказывается работать, возможно, не задано сетевое правило, определяющее отношение маршрутизации между источником и адресатом или отношение маршрутизации задано неверно. Более под-

робно отношения маршрутизации рассматриваются далее в этой главе при обсуждении сетевых шаблонов брандмауэра ISA.

В следующем примере нужно создать сетевое правило, которое контролирует отношение маршрутизации между внутренней сетью и сетью DMZ. Поскольку *в* обеих сетях используются частные адреса, между сетями нужно задать отношение типа «маршрут». В данном случае предпочтительнее использовать этот тип отношений, потому что он дает большую свободу в выборе протоколов передачи между внутренней сетью и DMZ. Однако если нужно скрыть IP-адреса хостов внутренней сети, когда они устанавливают соединение с хостами в сети DMZ, то следует выбрать отношение NAT, не забывая, что при этом не будет поддержки протоколов, не работающих с NAT.

Для создания сетевого правила выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Настройка). Щелкните узел **Networks** (Сети).
2. В узле **Networks** (Сети) щелкните на вкладке **Network Rules** (Сетевые правила) на панели **Details** (Подробности) консоли.
3. На панели **Task** (Задача) щелкните на вкладке **Tasks** (Задачи). Щелкните **ссылку Create a New Network Rule** (Создать новое сетевое правило).
4. **На** странице **Welcome to the New Network Rule Wizard** (Вас приветствует мастер создания нового сетевого правила) введите имя правила в текстовое поле **Network rule name** (Имя сетевого правила). В данном примере имя правила: **Internal Я aDMZ.** Щелкните **Next** (Далее).
5. На странице **Network Traffic Sources** (Источники сетевого трафика) щелкните **Add** (Добавить).
6. В диалоговом ок не **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Networks** (Сети). Дважды щелкните **Internal** (Внутренняя). Щелкните **Close** (Закрыть).
7. Щелкните **Next** (Далее) на странице **Network Traffic Sources** (Источники сетевого трафика).
8. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелкните **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Networks** (Сети). Дважды щелкните сеть DMZ. Щелкните **Close** (Закрыть).
10. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелкните **Next** (Далее).
11. На странице **Network Relationship** (Сетевые отношения) выберите вариант **Route** (Маршрут) (рис. 4.35). Щелкните **Next** (Далее).

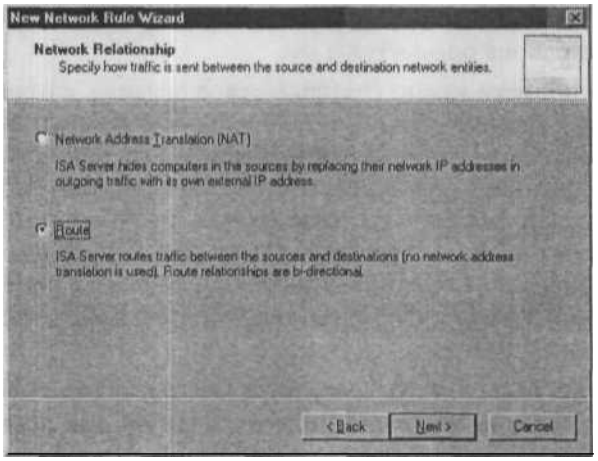


Рис. 4.35. Определение отношений маршрутизации

12. Щелкните **Finish** (Готово) на странице **Completing the New Network Rule Wizard** (Завершение работы мастера создания нового сетевого правила).
13. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
14. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
15. Новое сетевое правило появится на вкладке **Network Rules** (Сетевые правила) на панели **Details** (Подробности) консоли управления **Microsoft Internet Secu rity and Acceleration Server 2004.**

Сетевые объекты брандмауэра ISA 2004

При создании политик доступа на брандмауэре ISA всегда нужно указывать источник и адресат, для определения которых используются *сетевые объекты.* Сетевые объекты брандмауэра ISA обеспечивают большую свободу при создании политики доступа, потому что с их помощью можно устанавливать жесткий контроль взаимодействия между различными хостами.

Сетевые объекты брандмауэра ISA включают в себя:

- Networks (Сети);
- Network Sets (Подмножества сетей);
- Computers (Компьютеры);
- Address Ranges (Диапазоны адресов);
- Subnets (Подсети);
- Computer Sets (Подмножества компьютеров);
- URL Sets (Подмножества URL);

- Domain Name Sets (Подмножество имен доменов);
- Web Listeners (Web-приемники).

Сети

Обсуждению сетевого объекта *сеть* уже было уделено немало времени. Сети являются наборами адресов, достижимых с конкретного адаптера брандмауэра ISA. Например, если на брандмауэре ISA есть два адаптера, один из которых подключен к Интернету, а другой к корпоративной сети, то внутренняя сеть определяется как все адреса, расположенные за внутренним интерфейсом брандмауэра ISA.

Новый сетевой объект *сеть* можно создать в консоли управления **Microsoft Internet Security and Acceleration Server 2004** в узле **Networks** (Сети). При обсуждении создания новой сети подробно рассказывалось о том, как создать и настроить сетевой объект *сеть*.

Подмножества сетей

Подмножества сетей представляют собой наборы сетей. Существуют два подмножества сетей по умолчанию:

• All Networks (and local host) (Все сети и локальный хост); *ш*

All Protected Networks (Все защищенные сети).

Подмножество сетей **All Networks (and local host)** (Все сети, а также локальный хост) включает в себя все возможные адреса. Этот сетевой объект используется очень редко. Его можно использовать при выполнении тестирования или при использовании брандмауэра ISA в функции маршрутизатора с фильтрацией с отслеживанием соединений, а не в роли брандмауэра.

Сетевой объект **All Protected Networks** (Все защищенные сети) включает в себя все сети, определенные на брандмауэре ISA, за исключением внешней сети по умолчанию. Сетевой объект **All Protected Networks** (Все защищенные сети) обычно используется, когда необходимо применить правило доступа, контролирующее исходящий доступ ко всем сетям позади брандмауэра ISA.

Свойства сетевого объекта **Network Sets** (Подмножества сетей) по умолчанию можно посмотреть, выполнив следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Полити ка брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструменты). Щелкните *ссылку* **Network Objects** (Сетевые объекты). Появится список папок, представ ляющих сетевые объекты брандмауэра ISA.
3. Щелкните папку **Network Sets** (Подмножества сетей). Появятся два подмноже ства сетей по умолчанию.

4. Дважды щелкните **Network Sets** (Подмножества сетей) и вы увидите свойства подмножества сетей (рис. 4.36).

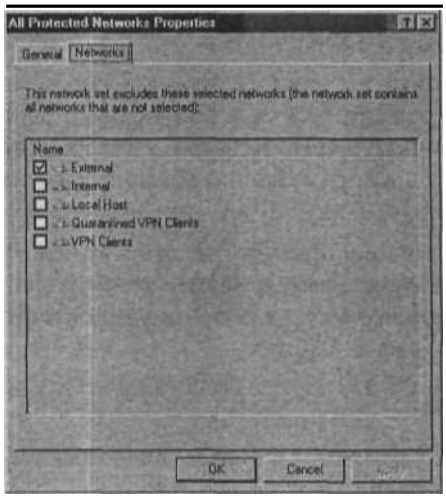


Рис. 4.36. Определение подмножеств сетей

Также можно создать новые подмножества сетей, если необходимо задать политику доступа, которая применяется к определенному набору сетей. Предположим, нужно создать подмножество сетей, которое включает сеть VPN-клиентов и внутреннюю сеть. Это подмножество можно использовать при создании правила доступа, которое контролирует взаимодействие между этими сетями. Для создания такого подмножества сетей нужно выполнить следующие действия (см. рис. 4.37):

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Политика брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструменты). Щелкните ссылку **Network Objects** (Сетевые объекты). Появится список папок, представляющих сетевые объекты брандмауэра ISA.
3. Щелкните папку **Network Sets** (Сетевые объекты). Щелкните меню **New** (Новый), а затем щелкните **Network Set** (Сетевой объект).

   На странице **Welcome to the New Network Set Wizard** (Вас приветствует мастер создания нового подмножества сетей) введите имя подмножества сетей в текстовое поле **Network set name** (Имя подмножества сетей). В данном примере — **VPN and Internal.** Щелкните **Next** (Далее).

   На странице **Network Selection** (Выбор сети) выберите вариант **Includes all selected networks** (Включает все выбранные сети). Также имеется вариант **Includes all networks except the selected network** (Включает все сети, кроме выбранной сети), который следует использовать при создании крупного под-

множества сетей, когда нужно исключить небольшое число сетей. В списке Name (Имя) установите флажок в полях **VPN Clients** (VPN-клиенты) и **Internal** (Внутренняя). Щелкните **Next** (Далее).

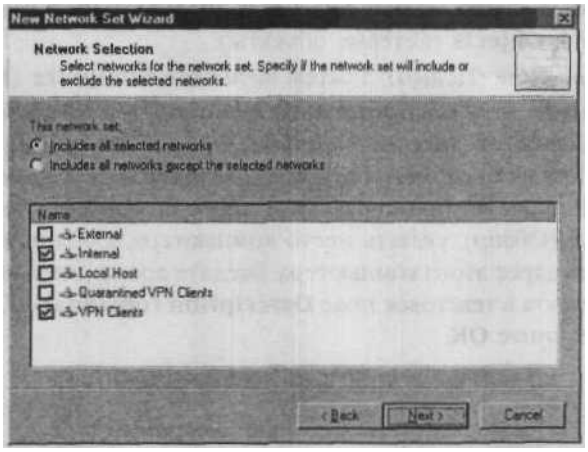


Рис. 4.37. Создание нового подмножества сетей

6. Щелкните **Finish** (Готово) на странице **Completing the New Network Set Wizard** (Завершение работы мастера создания нового подмножества сетей).
7. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
8. Щелкните OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
9. В списке **Network Sets** (Сетевые объекты) появится новое подмножество сетей.

Компьютеры

Сетевой объект *компьютеры* создается для тщательного контроля хостов источника и адресата, которым разрешено взаимодействовать между собой. Например, предположим, имеется DNS-сервер в корпоративной сети, который настроен на использование механизма продвижения данных DNS интернет-провайдера. Пользователям необходимо запретить использовать внешний DNS-сервер, и необходимо запретить рекурсию на DNS-сервере корпоративной сети. Можно ограничить DNS-сервер и сделать так, чтобы он использовал DNS-протокол только при взаимодействии с механизмом продвижения данных DNS на ISP. Брандмауэр ISA будет отвергать все соединения, которые пытается установить DNS-сервер с другими DNS-серверами в корпоративной сети.

Сетевых объектов *компьютеры* по умолчанию не существует. Для создания нового сетевого объекта *компьютеры* выполните следующие действия (см. рис. 4.38):

В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Политика брандмауэра).

На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструменты). Щелкните ссылку **Network Objects** (Сетевые объекты).

Щелкните меню **New** (Новый), а затем щелкните **Computer** (Компьютер). В диалоговом окне **New Computer Rule Element** (Новый элемент правила для объекта *компьютер)* введите имя компьютера, в данном примере — **DNS Server.** Если известен IP-адрес компьютера, можно ввести его в текстовое поле **Computer IP Address** (IP-адрес компьютера). Если адрес не известен, можно, используя кнопку **Browse** (Обзор), указать место компьютера, а брандмауэр ISA попытается определить адрес этого компьютера. Введите дополнительное описание этого сетевого объекта в текстовое поле **Description (optional)** (Описание, дополнительно). Щелкните ОК.

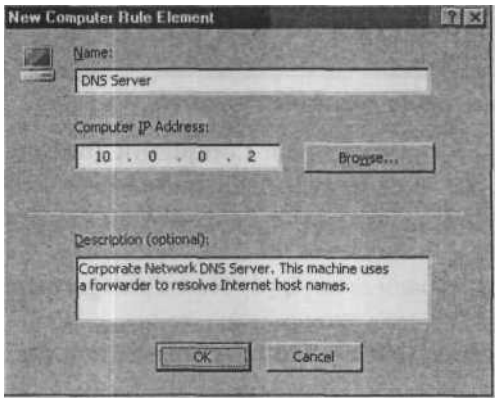


Рис. 4.38. Создание нового сетевого объекта *компьютеры*

5. Новый сетевой объект появится в списке **Computer Objects.**
6. Нажмите **Apply** (Применить), чтобы сохранить изменения и обновить полити ку брандмауэра.
7. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Диапазоны адресов

Сетевой объект *диапазоны адресов* позволяет создавать наборы соседних IP-адресов, например для применения одного правила доступа ко всем компьютерам в сегменте сети служб, находящемся под защитой брандмауэра ISA, или для контроля пользователем, работающим в конфигурации «сеть в сети», доступа пользователей одной сети к ресурсам другой сети. Можно создавать диапазоны адресов, представляющие каждую из сетей в объемлющей сети, и контролировать доступ с

помощью сетевых объектов *диапазоны адресов,* каждый из которых представляет отдельную сеть.

Не существует диапазонов адресов по умолчанию. Выполните следующие действия по созданию нового сетевого объекта *диапазон адресов* (см. рис. 4.39):

1. В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера, а затем щелкните узел Firewall Policy (Полити ка брандмауэра).
2. На панели Task (Задача) щелкните вкладку Toolbox (Инструменты). Щелкните ссылку Network Objects (Сетевые объекты).
3. Щелкните меню New (Новый), а затем щелкните Address Range (Диапазон ад ресов).
4. В диалоговом окне New Address Range Rule Element (Элемент правила для но вого диапазона адресов) введите имя диапазона адресов в текстовое поле Name (Имя). Введите первый адрес диапазона в текстовое поле Start Address (Началь ный адрес), а последний адрес диапазона в текстовое поле End Address (Ко нечный адрес). Введите описание диапазона адресов в текстовое поле Descrip tion (optional) (Описание, дополнительно). Щелкните OK.

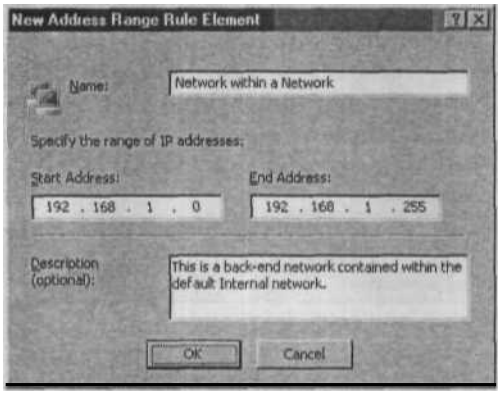


Рис. 4.39. Создание нового сетевого объекта *диапазон адресов*

5. Новый диапазон адресов появится в списке Address Ranges (Диапазон адресов).
6. Щелкните Apply (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
7. Щелкните OK *в* диалоговом окне Apply New Configuration (Применить новую конфигурацию).

Подсети

Сетевой объект *подсети* позволяет определить группу хостов, расположенных в одной подсети. В предыдущем примере было создано подмножество адресов, вклю-

чающее в себя всю подсеть. Но если в центре внимания вся подсеть, то лучше создать сетевой объект *подсети.* Не существует подсетей по умолчанию. Для создания нового сетевого объекта *подсеть* выполните следующие действия (см. рис. 440).

1. В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните имя сервера, а затем щелкните узел Firewall Policy (Полити ка брандмауэра).
2. На панели Task (Задача) щелкните вкладку Toolbox (Инструмент). Щелкните ссылку Network Objects (Сетевые объекты).
3. Щелкните меню New (Новый), а затем щелкните Subnet (Подсеть).
4. В диалоговом окне New Subnet Rule Element (Элемент правила для новой подсети) введите в текстовое поле Name (Имя) имя подсети. Введите идентификатор подсети в текстовое поле Network address (Сетевой адрес), а затем введите используемое для маски подсети количество бит в текстовое поле через слэш. Поле Network mask (Маска сети) будет заполнено автоматически. Введите описание этой подсети в текстовое поле Description (optional) (Описание, дополнительно). Щелкните OK.

Рис. 4.40, Создание нового сетевого объекта подсеть

5. Новая подсеть появится в списке Subnets (Подсети).
6. Щелкните Apply (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
7. Щелкните OK в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

Подмножества компьютеров

Сетевой объект *подмножество компьютеров* представляет собой набор IP-адресов компьютеров, объединенных общей функцией или целью. Например, можно создать

подмножество компьютеров для всех серверов сети, на которых никогда не регистрируются пользователи, или подмножество компьютеров, на которых не установлена ОС Windows и не поддерживается клиент брандмауэра, но тем не менее для которых нужно как-то контролировать доступ.

Существует три подмножества компьютеров по умолчанию:

- **Anywhere** (Любые);
- **IPSec Remote Gateways** (Удаленные шлюзы IPSec);
- **Remote Management Computers** (Компьютеры удаленного управления).

Подмножество компьютеров **Anywhere** (Любые) включает все адреса в адресном диапазоне IPv4. Это подмножество компьютеров можно использовать, если нужно разрешить взаимодействие для широковещательных протоколов. Например, если нужно сделать внешний интерфейс брандмауэра ISA DHCP-клиентом, можно использовать подмножество компьютеров **Anywhere** (Любые), чтобы разрешить клиентам пересылать всем станциям сети DHCP-запрос.

Подмножество компьютеров **IPSec Remote Gateways** (Удаленные шлюзы IPSec) автоматически создается при установлении VPN-подключения «узел-в-узел» с помощью туннельного режима IPSec. В это подмножество компьютеров не нужно добавлять записи вручную, потому что эту работу выполняют мастера VPN-подключений.

Подмножество компьютеров **Remote Management Computers** (Компьютеры удаленного управления) используется системной политикой брандмауэра ISA для разрешения соединения между компьютерами, работающими с консолью удаленного управления ISA. Компьютеры удаленного управления можно внести вручную, выполнив следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Полити ка брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструмент), затем ссыл ку **Network Objects** (Сетевые объекты).
3. Щелкните папку **Computer Sets** (Подмножества компьютеров).
4. Щелкните значок **Remote Management Computers** (Компьютеры удаленного управления), а затем меню **Edit** (Редактировать).
5. Щелкните **Add** (Добавить) в диалоговом окне **Remote Management Computers Properties** (Свойства компьютеров удаленного управления). Щелкните запись **Computer** (Компьютер), **Address Range** (Диапазон адресов) или **Subnet** (Под сеть) в выпадающем меню.
6. Введите данные в диалоговом окне **New Rule** Element (Новый элемент прави ла) и щелкните **ОК.**
7. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.

8. Щелкните OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Можно создавать собственные подмножества компьютеров, например для серверов, на которых никогда не регистрируются пользователи. Если организации нужна высокая степень защиты сети и требуется обеспечить проверку подлинности для всего входящего и исходящего доступа, то на всех операционных системах клиентов нужно установить клиента брандмауэра.

Но проблема в том, что на некоторых из серверов не регистрируются пользователи, например на исходящем SMTP-ретрансляторе или сервере Exchange. Для того чтобы эти компьютеры могли получить доступ к Интернету, в то же время обеспечивая некоторый уровень контроля доступа, можно использовать подмножество компьютеров и добавить компьютеры, на которых не регистрируются пользователи, в подмножество компьютеров.

Для создания нового подмножества компьютеров выполните следующие действия (см. рис. 4.41).

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Полити ка брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструменты). Щелкните ссылку **Network Objects** (Сетевые объекты).
3. Щелкните папку **Computer Sets** (Подмножества компьютеров).
4. Щелкните **New Menu** (Новое меню).
5. В диалоговом окне **New Computer Set Rule Element** (Элемент правила для но вого подмножества компьютеров) введите имя подмножества в текстовое поле **Name** (Имя), в данном примере — **Mail Relays** (Почтовые трансляторы).
6. Щелкните **Add** (Добавить). Выберите **Computer** (Компьютер), **Address Range** (Диапазон адресов) или **Subnet** (Подсеть). В данном примере выбрана запись **Computer** (Компьютер).
7. В диалоговом окне **New Computer Rule Element** (Элемент правила для ново го компьютера) введите имя подмножества компьютеров в текстовое поле Name (Имя), в данном примере — **BORAX.** В текстовое поле **Computer IP Address** (IP-адрес компьютера) введите IP-адрес сервера, входящего в эту группу. Если вы не помните IP-адрес (но при этом адрес должен быть разрешимым в DNS), вос пользуйтесь кнопкой Browse (Просмотр). Введите описание компьютера В тек стовое поле **Computer** (Компьютер). Щелкните OK.
8. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
9. Щелкните OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

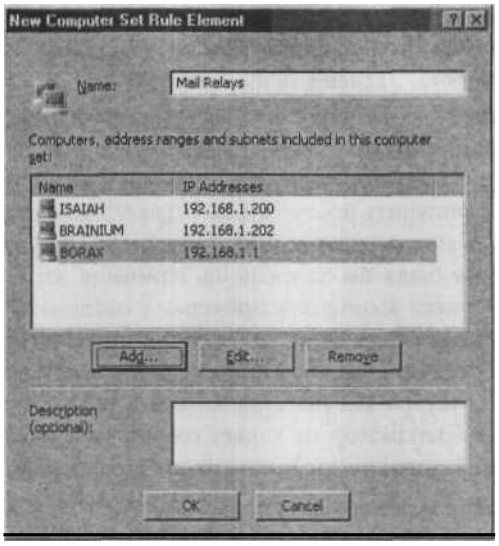


Рис. 4.41. Создание нового сетевого объекта *подмножество сетей*

Подмножество URL

Сетевой объект *подмножество URL* представляет собой набор из одного или нескольких URL Подмножества URL можно использовать для обеспечения тщательного контроля Web-сайтов, к которым могут получить доступ пользователи через брандмауэр ISA. Если попытаться использовать подмножество URL в правиле, применяемом не к протоколам HTTP или FTP, то подмножество URL применяться не будет, даже если создать такое правило.

Предположим, что создано подмножество URL, содержащее URL mail.isaserver-org.com. Нужно разрешить пользователям доступ к почте путем установки соединения с почтовым сервером с помощью SMTP-протокола, для этого создается правило доступа, разрешающее всем пользователям получать доступ к подмножеству URL, содержащему домен mail.isaserverorg.com. Если пользователи попытаются установить соединение, попытка соединения будет безуспешной, потому что подмножество URL не применяется к протоколам, отличным от HTTP/FTP.

Подмножеств URL по умолчанию не существует. При создании правила доступа с использованием подмножества URL нужно помнить их важные особенности.

- Для URL, входящего в подмножество URL, можно указать протокол и порт. Одна ко учитываться будут только FQDN и путь, протокол и порт будут проигнориро ваны. Протокол и порт контролируются другими аспектами правила доступа.
- При создании записи в подмножестве URL можно использовать групповые сим волы. Например, h *ttp:///'.* is a server.org, http://www.isaserver.org/' или даже http://

'.isaserver.org/*. Однако символы группирования должны размещаться в начале или в конце записи. В других местах записи их ставить нельзя. Например, запись http: //*.isaserver.org/'/articles неправильная.

- При создании записей подмножества URL для сайтов, предполагающих обязательное использование протокола SSL, убедитесь в том, что вы не включаете в URL указание пути. Например, при регистрации на сайте Hotmail через Web-браузер вы должны получить доступ к URL https://loginnet.passport.com. Если бы вы создали запись в подмножестве URL типа https: //lo gin net. pass port .com/*, то попытка соединения была бы запрещена. Причина этого состоит в том, что брандмауэр ISA не может выполнять проверку с отслеживанием соединений на уровне приложения для исходящих SSL-соединений. Поэтому брандмауэр ISA не может получить доступ ни к каким **маршрутам** после установки SSL-соединения. Поскольку на брандмауэре ISA имеется запись в подмножестве URL, включающая в себя путь, но брандмауэр не может определить путь в пределах SSL-туннеля, то он в целях безопасности запретит это соединение.

В следующем примере будет создано подмножество URL для разрешения пользователям Outlook Express и Microsoft Outlook 2003 получения доступа к своим учетным записям Hotmail через брандмауэр ISA. Это подмножество URL можно использовать в качестве источника в правиле доступа, применяемом ко всем пользователям или к пользователям, которые являются частью подмножества компьютеров, подсети или другого сетевого объекта.

Для создания сетевого объекта подмножество URL выполните следующие действия (см. 4.42).

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Полити ка брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструмент). Щелкните ссылку **Network Objects** (Сетевые объекты).
3. Щелкните папку **URLSets** (Наборы URL).
4. Щелкните **New Menu** (Новое меню), а затем щелкните **URL Set** (Наборы URL).
5. В диалоговом окне **New URL Set Rule Element** (Элемент правила нового под множества URL) введите имя подмножества URL в текстовое поле **Name** (Имя), н этом примере — **Hotmail Access.** Щелкните **New** (Новый). В текстовом поле над кнопкой **New** (Новый) введите первый URL, в данном примере — hup:// '.passport.com, и нажмите клавишу <ENTER>. Повторите процедуру, добавляя следующие URL: http://*.passport.net, http://'.msn.com, http://*.hotmail.com. Щелк ните ОК.
6. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
7. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

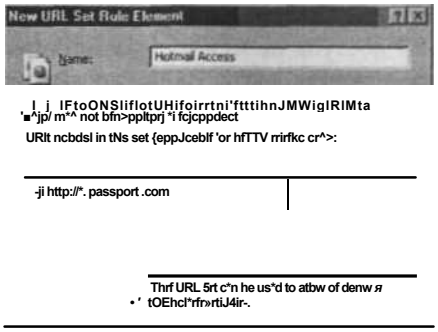


Рис. 4.42. Создание нового сетевого объекта *подмножество URL*

Подмножество имен доменов

Сетевой объект *подмножество имен доменов* очень похож на объект *подмножество URL* за исключением того, что он применяется ко всем протоколам и не включает указание пути, а только FQDN. Подмножество URL поддерживает групповые символы в начале FQDN, например '.isaserver.org. Оно не поддерживает групповые символы в конце FQDN, потому что это будет указанием на путь в URL, а указание пути поддерживается только подмножеством URL.

Существуют два подмножества имен доменов по умолчанию:

- **Microsoft Error Reporting Sites** (Сайты Microsoft, сообщающие об ошибке);
- **System Policy Allowed Sites** (Сайты, разрешенные системной политикой).

Подмножество имен доменов **Microsoft Error Reporting Sites** (Сайты Microsoft, сообщающие об ошибке) включает домены '.**watson.microsoft.com** и **watson. microsoft.com.** Это подмножество имен доменов используется правилом системной политики, что позволяет брандмауэру ISA отправлять информацию об ошибке корпорации Microsoft для дальнейшего анализа.

Подмножество имен доменов **System Policy Allowed Sites** (Сайты, разрешенные системной политикой) включает домены *.**microsoft.com,** *.**windows.com** и **•.windowsupdate.com.** Существуют правила системной политики, которые используют это подмножество имен доменов, чтобы разрешить брандмауэру ISA устанавливать соединение со службой обновлений Windows Update и получать другую информацию с Web-сайта Microsoft.

Подмножества имен доменов по своим функциям очень похожи на подмножества URL, и если в правиле доступа не нужно указывать путь, то можно использовать любое из них для обеспечения контроля доступа по протоколам HTTP/HTTPS или туннельного режима Web-прокси по протоколу FTP. Однако если необходимо контролировать любые другие протоколы, то следует использовать подмножества имен доменов, поскольку подмножества URL используются только для HTTP/H1TPS/FTP-соединений.

Для создания сетевого объекта *подмножество имен доменов* выполните следующие действия (см. рис. 4.43).

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Политика брандмауэра).
2. На панели **Task** (Задача) щелкните вкладку **Toolbox** (Инструмент). Щелкните ссылку **Network Objects** (Новые объекты).
3. Щелкните папку **Domain Name Sets** (Подмножество имен доменов).
4. Щелкните **New Menu** (Новое меню), а затем щелкните **Domain Name Set** (Подмножество имен доменов).
5. В диалоговом окне **New Domain Name Set Policy Element** (Элемент политики нового подмножества имен доменов) введите имя подмножества имен доменов в текстовое поле **Name** (Имя). Щелкните **New** (Новый). Введите имя домена или полное имя домена в текстовом поле и нажмите клавишу **<ENTER>.** Введите описание подмножества имен доменов в текстовое поле **Description (optional)** (Описание, дополнительно). Щелкните ОК.

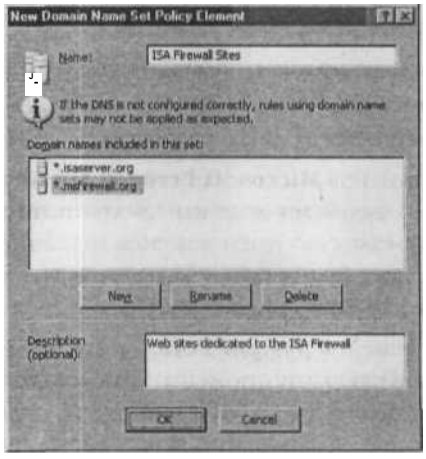


Рис. 4.43. Создание нового сетевого объекта *подмножество имен доменов*

6. В списке **Domain Name Sets появится** новое подмножество имен доменов (рис. 4.44).

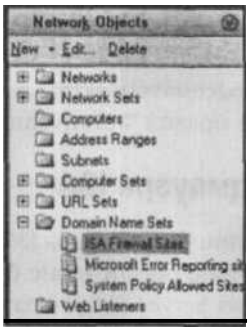


Рис. 4.44. Просмотр нового подмножества имен доменов

7. Щелкните Apply (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
8. Щелкните OK в диалоговом окне **Apply** New Configuration (Применить новую конфигурацию).

СОВЕТ Подмножества URL и подмножества имен доменов являются мощными средствами блокирования опасных и оскорбительных Web-сайтов. Однако довольно утомительно вводить 10 000 URL или доменов в подмножество URL или подмножество имен доменов. Для решения этой проблемы используйте сценарий для импортирования тысяч записей в подмножество имен доменов или подмножество URL из текстового файла. Для начала посетите сайт http://www.mvps.org/winhelp2002/hosts.htm, чтобы получить текстовый файл с URL или доменами оскорбительных сайтов. Затем обратитесь к статье автора «Strong Outbound Access Control using the ISA Firewall (2004): Using Scripts to Populate URL Sets and Domain Name Sets» («Жесткий контроль исходящего доступа с помощью брандмауэра ISA: использование сценариев для заполнения подмножеств URL и подмножеств имен доменов») на сайте http://isaserver.org/articles/2004domainseturlset.html. С помощью файла HOSTS и сценариев можно легко создать подмножества URL или подмножества имен доменов, чтобы заблокировать оскорбительные сайты.

Web-приемники

Web-приемники существенно отличаются от остальных сетевых объектов, рассматриваемых в этом разделе. Web-приемник не имеет жестко заданного места в представлении о сети, потому что он может использоваться в качестве источника или адресата в любом правиле доступа или правиле публикации.

Web-приемник используется для приема входящих соединений к Web-сайтам, которые являются неотъемлемой частью правил Web-публикации. Каждое правило Web-публикации предполагает, что Web-приемник принимает входящее соеди-

нение к опубликованному Web-сайту. Можно создать отдельные Web-приемники для HTTP и SSL-соединений и для IP-адресов на каждом интерфейсе брандмауэра ISA.

Подробнее Web-приемники рассматриваются в главе 8, в которой представлено описание Web-публикации и правил Web-публикации.

Сетевые шаблоны брандмауэра ISA

При установке и конфигурировании брандмауэра ISA можно использовать стандартные подходы. Обычно программное обеспечение брандмауэра ISA устанавливается на усиленной версии Windows Server 2003, а затем вручную производится настройка всех сетей, подключенных к брандмауэру ISA. Создаются сети, устанавливаются отношения маршрутизации между сетями с помощью сетевых правил, а затем создаются подробные политики внутреннего и внешнего доступа. Как только принцип работы брандмауэра ISA становится ясен, можно сконфигурировать брандмауэр ISA с 10 сетевыми интерфейсными картами и с мощной политикой входящего и исходящего доступа менее чем за час. Сравните это время с временем для настройки брандмауэра PIX сходной конфигурации, и вы сможете по достоинству оценить безопасность и простоту в применении брандмауэра ISA.

Если необходимо быстро приступить к работе и не тратить много времени на изучение принципов работы брандмауэра ISA, можно воспользоваться сетевыми шаблонами брандмауэра ISA. Существует несколько сетевых шаблонов, с помощью которых можно придать брандмауэру ISA следующие роли:

- граничный брандмауэр;
- внешний брандмауэр;
- внутренний брандмауэр;
- брандмауэр DMZ с тремя сетевыми интерфейсами;
- брандмауэр с одним сетевым интерфейсом с функцией Web-кэширования (шаблон с одной сетевой интерфейсной картой).

В этом разделе рассматриваются характеристики каждого сетевого шаблона, их функции и принципы работы.

Шаблон граничного брандмауэра

Шаблон граничного брандмауэра применяется, если брандмауэр ISA находится на границе корпоративной сети с Интернетом. Именно на границе с Интернетом у брандмауэра ISA имеется сетевой интерфейс, напрямую соединенный с Интернетом, и как минимум еще один сетевой интерфейс, соединенный с сетью, который находится под контролем администратора. Шаблон граничного брандмауэра предполагает наличие хотя бы одного внешнего интерфейса и хотя бы одного внутреннего интерфейса.

После запуска шаблона граничного брандмауэра в конфигурации брандмауэра ISA произойдут следующие важные изменения:

- создается сетевое правило, устанавливающее отношения маршрутизации между внутренней сетью и сетью VPN-клиентов по типу «маршрут»;
- внутренняя сеть по умолчанию остается; шаблон не удаляет внутреннюю сеть по умолчанию, созданную во время установки брандмауэра ISA.

Шаблон граничного брандмауэра максимально сохраняет все сетевые настройки по умолчанию.

Политики брандмауэра, поставляемые вместе с шаблоном граничного брандмауэра (табл. 4.6), становятся доступными при запуске шаблона. *Прежде чем* запускать шаблон, нужно убедиться в том, что значение каждой из этих политик понятно. После запуска шаблона следует проверить все политики брандмауэра и просмотреть все изменения. Рекомендуется начинать с политики Block all (Заблокировать все). Эта политика гарантирует наиболее безопасную конфигурацию и предотвращает непреднамеренное создание дыр в системе безопасности брандмауэра. Позднее можно создать правила доступа и правила публикации на брандмауэре ISA, чтобы контролировать исходящий и входящий доступ.

Табл. 4.6. Политики брандмауэра, поставляемые вместе с шаблоном граничного брандмауэра

Название политики	Описание	Создаваемые правила
Block all (Заблокировать все)	Эта политика блокирует весь доступ к сети через ISA Server. Этот вариант не создает никаких правил доступа, кроме правила по умолчанию, которое блокирует весь доступ. Используйте этот вариант, если вы сами хотите определить политику брандмауэра	Нет
Block Internet access, allow **access to ISP network services** (Заблокировать доступ к Интернету, разрешить доступ к сетевым службам интернет-провайдера)	Эта политика блокирует весь доступ к сети через ISA Server, за исключением доступа к службам внешней сети, например DNS. Этот вариант полезен, если службы предоставляются интернет-провайдером. Этот вариант следует использовать, если нужно определить политику брандмауэра самостоятельно	Разрешить DNS из внутренней сети и сети VPN-клиентов к внешней сети (Интернет)
Allow limited Web-access (Разрешить **ограниченный** Web-доступ)	Эта политика разрешает ограниченный Web-доступ только по протоколам HTTP, HTTPS и FTP. Весь остальной доступ к сети блокируется	Разрешить HTTP, HTTPS и FTP-соединения из внутренней сети во внешнюю (Интернет). Разрешить соединения по всем протоколам из сети VPN-клиентов во внутреннюю сеть

(см. след. стр.)

Табл. 4.6. (окончание)

Название политики	Описание	Создаваемые правили
Allow access for **all protocols** (Разрешить доступ по всем протоколам)	Эта политика разрешает неограниченный доступ к Интернету через ISA Server. ISA Server запрещает доступ из Интернета к защищенным сетям	Разрешить доступ по нсем протоколам из внутренней сети и сети VPN-клиентов во внешнюю сеть (Интернет). Разрешить сети VPN-клиентов доступ во внутреннюю сеть

Для применения шаблона граничного брандмауэра выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Н астройка). Щелкните узел **Networks** (Сети).
2. В узле **Networks** (Сети) на панели **Tasks** (Задачи) щелкните вкладку **Templates** (Шаблоны). Первым в списке сетевых шаблонов стоит **Edge Firewall Template** (Шаблон граничного брандмауэра), щелкните его.
3. Щелкните **Next** (Далее) на странице **Welcome to the Network Template Wizard** (Вас приветствует мастер сетевого шаблона).
4. На странице **Export the ISA Server Configuration** (Экспорт конфигурации ISA Server) имеется вариант создания копии текущей конфигурации брандмауэра ISA. Это полезная функция, потому что сетевой шаблон перепишет текущую конфи гурацию сети и политику брандмауэра. Если создать копию текущей конфигу рации, то можно с легкостью ее восстановить в случае, если результат работы мастера сетевого шаблона вам не понравится. Щелкните **Export** (Экспорт).
5. В диалоговом окне **Export Configuration** (Экспортировать конфигурацию) вве дите имя текущей конфигурации брандмауэра ISA в текстовое поле **File name** (Имя файла), в данном примере конфигурационный файл назван **Pre-Edge Fire wall Template.** Обратите внимание, что конфигурация сохраняется в формате XML Не нужно выбирать варианты **Export user permission settings** (Экспор тировать настройки полномочий пользователя) или **Export confidential infor mation (encryption will be used)** (Экспортировать конфиденциальную инфор мацию, будет использовано шифрование), потому что вы не связываете полно мочия пользователя с этим шаблоном и вряд ли будете использовать этот ре зервный файл для копирования конфигурации брандмауэра ISA на другой компьютер. Нужно лишь создать копию текущей сети и политики брандмауэра. Щелкните **Export** (Экспорт).
6. Появится диалоговое окно **Exporting** (Экспортирование). Щелкните ОК, когда мастер сообщит об успешном экспорте конфигурации.
7. Щелкните **Next** (Далее) на странице **Export the ISA Server Configuration** (Эк спортировать конфигурацию ISA Server).

8. На странице **Internal Network IP Addresses** (IP-адреса внутренней сети) установите адреса, представляющие внутреннюю сеть. Мастер сетевого шаблона воспользуется теми же адресами, которые применялись при создании внутренней сети при установке брандмауэра ISA. Существует возможность добавить во внутреннюю сеть по умолчанию дополнительные адреса с помощью кнопок **Add** (Добавить), **Add Adapter** (Добавить адаптер) и **Add Private** (Добавить частные). Кнопка **Add** (Добавить) позволяет вручную ввести диапазон или диапазоны адресов. Кнопка **Add Adapter** (Добавить адаптер) позволяет воспользоваться таблицей маршрутизации Windows, чтобы автоматически добавить адреса к внутренней сети, а кнопка **Add Private** (Добавить частный) автоматически добавляет все сетевые адреса к адресам, принадлежащим внутренней сети по умолчанию. В данном примере и чаще всего не следует менять адреса на этой странице. Щелкните **Next** (Далее). Страница **Internal Network IP Addresses** (IP-адреса внутренней сети) показана на рис. 445.

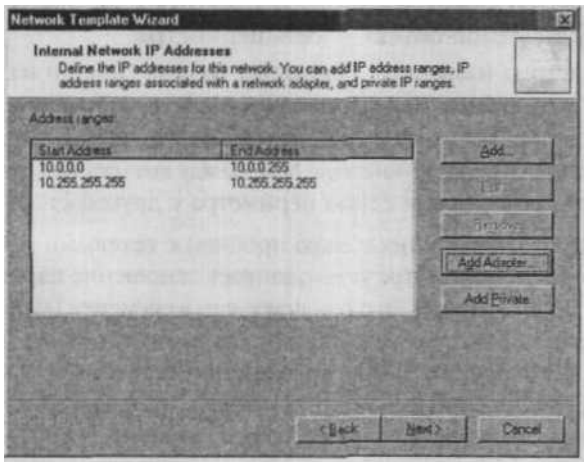


Рис. 4.45. Определение IP-адресов

9. На странице **Select a Firewall Policy** (Выбрать политику брандмауэра) выбе рите подходящую для организации политику брандмауэра. Описание политик брандмауэра приведено в табл. 4.6. Настоятельно рекомендуется выбрать поли тику брандмауэра **Block All** (Блокировать все), а затем, когда станет ясен прин цип работы политик брандмауэра ISA, настроить ее вручную. Это снизит веро ятность создания конфигурации, не обеспечивающей достаточной безопасно сти. В данном примере выбрана политика брандмауэра **Block All** (Блокировать все). Щелкните **Next** (Далее).
10. Щелкните **Finish** (Завершить) на странице **Completing the Network Template Wizard** (Завершение работы мастера сетевого шаблона).
11. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.

12. Щелкните OK в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

На данном этапе весь исходящий и входящий трафик на брандмауэре ISA запрещен, потому что была выбрана наиболее безопасная политика брандмауэра в сетевом шаблоне. Теперь можно настроить политики брандмауэра ISA в соответствии с потребностями конкретной организации.

Шаблон с тремя сетевыми интерфейсами или DMZ

Шаблон DMZ с тремя сетевыми интерфейсами позволяет настроить брандмауэр ISA с тремя и более сетевыми адаптерами на использование дополнительных сетевых адаптеров. При применении этого шаблона создается несколько сетевых правил, на первый взгляд парадоксальных.

После запуска сетевого шаблона DMZ с тремя сетевыми интерфейсами происходят следующие изменения:

- создается новый сетевой объект — сеть периметра;
- сетевое правило под названием Perimeter Access (Доступ из сети периметра) устанавливает отношение маршрутизации из сети периметра в Интернет;
- сетевое правило под названием Perimeter Configuration (Конфигурация сети периметра) устанавливает отношение NAT между внутренней сетью и сетью VPN-клиентов с одной стороны и сетью периметра с другой стороны.

В данном случае возникает несколько проблем с сетевыми правилами. Сетевое правило доступа из сети периметра устанавливает отношение маршрутизации между сетью периметра и Интернетом. Это означает, что в сегменте DMZ нужно использовать адреса общего назначения. Это обнаружится, если попытаться использовать частные адреса в сегменте DMZ. При применении сетевого шаблона DMZ с тремя сетевыми интерфейсами нужно изменить сетевое правило доступа из сети периметра на NAT, если используются частные адреса в сегменте DMZ. Еще больше проблем возникает с тем, что этот шаблон устанавливает отношение маршрутизации между сегментом DMZ и внутренней сетью по типу NAT. Эта настройка вполне понятна, если в сегменте DMZ используются общие адреса, но если в сегменте DMZ используются частные адреса, то эта конфигурация не подходит.

Сетевое правило конфигурации сети периметра устанавливает отношение маршрутизации между внутренней сетью и сетью VPN-клиентов по типу NAT. Хотя такой тип маршрутизации в данном случае будет работать, но он не работает со всеми протоколами, и это может привести к таким ситуациям, которых можно было бы избежать при использовании отношения маршрутизации по типу «маршрут» между внутренней сеть и сетью VPN-клиентов с одной стороны и сегментом DMZ с другой. Если в сегменте DMZ используются общие адреса, то нужно оставить отношение маршрутизации NAT. Но если в сегменте DMZ с тремя сетевыми интер-

фейсами используются частные адреса, то нужно поменять отношение маршрутизации на «маршрут».

При запуске сетевого шаблона DMZ стремя сетевыми интерфейсами можно выбрать одну из политик брандмауэра, приведенных в табл. 4.7. Рекомендуется выбрать политику брандмауэра Block all (Блокировать все), а затем настроить ее с конкретными правилами доступа и правилами публикации для конкретной организации.

Табл. 4.7. Политики брандмауэра для сетевого шаблона с тремя сетевыми интерфейсами

Название политики	Описание	Создаваемые правила
Block all (Заблокировать все)	Эта политика блокирует весь доступ к сети через ISA Server. Этот вариант не создает никаких правил доступа, кроме правила по умолчанию, которое блокирует весь доступ. Используйте этот вариант, когда нужно определить политику брандмауэра самостоятельно	Нет
Block Internet access, allow access to network services on the perimeter network (Заблокировать доступ в Интернет, разрешить доступ к сетевым службам на сети периметра)	Эта политика блокирует весь доступ к сети через брандмауэр ISA, **кроме** доступа к сетевым службам (DNS) в сети периметра. Этот вариант используется, когда нужно самостоятельно определить политику брандмауэра	Разрешить DNS-трафик из внутренней сети и сети VPN-клиентов в сеть периметра
Block Internet access, allow access to ISP network services (Заблокировать доступ к Интернету, разрешить доступ к сетевым службам интернет-провайдера)	Эта политика блокирует весь доступ к сети через ISA Server, за исключением доступа к службам внешней сети типа DNS. Этот вариант полезен, когда службы предоставляются интернет-провайдером. Этот вариант следует использовать, когда нужно определить политику брандмауэра самостоятельно	Разрешить DNS из внутренней сети, сети VPN-клиентов и сети периметра к внешней сети (Интернет) вайдером.
Allow limited Web-access (Разрешить ограниченный Web-доступ)	Эта политика разрешает ограниченный Web-доступ только по протоколам HTTP, HTTPS и FIT *я* блокирует весь остальной доступ к сети	Разрешить HTTP, HTTPS и FTP-соединения из внутренней сети и сети VPN-клиентов в сеть периметра и во внешнюю сеть (Интернет). Разрешить соединения по всем протоколам из сети VPN-клиентов во внутреннюю сеть интернет-провайдером

(см. след. стр.)

Табл. 4.7. (окончание)

Название политики	Описание	Создаваемые правила
Allow limited Web access, allow access to network services on perimeter network (Разрешить ограниченный Web-доступ, разрешить доступ к сетевым службам сети периметра)	Эта политика разрешает ограниченный Web-доступ только по протоколам HTTP, HTTPS и FTP и разрешает доступ к сетевым службам в сети периметра. Весь остальной доступ к сети блокируется. Этот вариант используется, когда службы сетевой инфраструктуры доступны в сети периметра	Разрешить HTTP, HTTPS и FTP-доступ из внутренней сети и сети VPN-клиентов в сеть периметра и во внешнюю сеть (Интернет). Разрешить DNS-трафик из внутренней сети и сети VPN-клиентов в сеть периметра. Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть
Allow limited **Web access, allow ISP network** services (Разрешить ограниченный Web-доступ, разрешить сетевые службы интернет-провайдера)	Эта политика разрешает ограниченный интернет-доступ и доступ к сетевым службам, например DNS, предоставляемым интернет-провайдером. Весь остальной доступ к сети блокируется	Разрешить HTTP-, HTTPS-, FTP-доступ из внутренней сети и сети VPN-клиентов во внешнюю сеть (Интернет). Разрешить DNS из внутренней сети, сети VPN-клиентов и сети периметра во внешнюю сеть (Интернет). Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть
Allow all protocols (Разрешить все протоколы)	Эта политика разрешает неограниченный доступ к Интернету через ISA Server. ISA Server блокирует доступ из Интернета к защищенным сетям. Позже можно изменить правила доступа, чтобы заблокировать конкретные типы сетевого доступа	Разрешить все протоколы из внутренней сети и сети VPN-клиентов в сеть периметра и внешнюю сеть (Интернет). Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть

Для того чтобы применить сетевой шаблон DMZ с тремя сетевыми интерфейсами, выполните следующие действия:] В консоли управления **Microsoft Internet Security and Acceleration Server**

2004 разверните имя сервера, а затем разверните узел **Configuration** (Настройка).

Щелкните узел **Networks** (Сети). 2. В узле **Networks** (Сети) на панели **Task** (Задача) щелкните вкладку **Templates**

(Шаблоны). Выберите сетевой шаблон **3-Leg Perimeter,** дважды щелкнув на этой записи.

3. Щелкните **Next** (Далее) на странице **Welcome to the Network Template Wizard.**
4. На странице **Export the ISA Server Configuration** (Экспорт конфигурации ISA Server) можно создать копию текущей конфигурации брандмауэра ISA. Это полезная функция, потому что сетевой шаблон перепишет текущую конфигурацию сети и политику брандмауэра. Копию текущей конфигурации можно использовать для ее восстановления, если результат работы мастера сетевого шаблона вам не понравится. Щелкните **Export** (Экспорт).
5. В диалоговом окне **Export Configuration** (Экспортировать конфигурацию) введите имя текущей конфигурации брандмауэра ISA в текстовое поле **File name** (Имя файла), в данном примере конфигурационный файл назван **Pre-3-Leg Perimeter Template.** Обратите внимание, что конфигурация сохраняется в формате XML Не нужно выбирать вариант **Export user permission settings** (Экспортировать настройки полномочий пользователя) или **Export confidential information (encryption will be used)** (Экспортировать конфиденциальную информацию, будет использовано шифрование), потому что вы не связываете полномочия пользователя с этим шаблоном и вряд ли будете использовать этот резервный файл для копирования конфигурации брандмауэра ISA на другой компьютер. Нужно лишь создать копию текущей сети и политики брандмауэра. Щелкните **Export** (Экспортировать).
6. Появится диалоговое окно **Exporting** (Экспортирование). Щелкните ОК, когда мастер сообщит, что он успешно экспортировал конфигурацию.
7. Щелкните **Next** (Далее) на странице **Export the ISA Server Configuration** (Экспортировать конфигурацию ISA Server).
8. На странице **Internal Network IP Addresses** (IP-адреса внутренней сети) установите адреса, определяющие внутреннюю сеть. Адреса, отображаемые по умолчанию, — это адреса, которые уже применялись при создании внутренней сети при установке брандмауэра ISA. Существует возможность добавить во внутреннюю сеть по умолчанию дополнительные адреса с помощью кнопок **Add** (Добавить), **Add Adapter** (Добавить адаптер) и **Add Private** (Добавить частные). Рекомендуется в данном случае использовать кнопку **Add Adapter** (Добавить адаптер) и избегать использования кнопки **Add Private** (Добавить частные). Щелкните **Next** (Далее).
9. На странице **Perimeter Network IP Addresses** (IP-адреса сети периметра) настройте адреса, которые являются частью нового сегмента DMZ. Для этого можно воспользоваться кнопками **Add** (Добавить), **Add Adapter** (Добавить адаптер) или **Add Private** (Добавить частные). В данном случае использована кнопка **Add Adapter** (Добавить адаптер). Щелкните ее.
10. Выберите адаптер, представляющий интерфейс DMZ, и установите флажок в поле рядом с этим адаптером. Важно сначала выбрать адаптер. Если адаптер не выбран, то в поле **Network Interfaces Information** (Информация о сетевых интерфейсах) (рис. 4.46) не будет отображаться корректная информация. В этом

поле показан список адресов, которые будут использоваться для определения сети DMZ. Щелкните ОК.

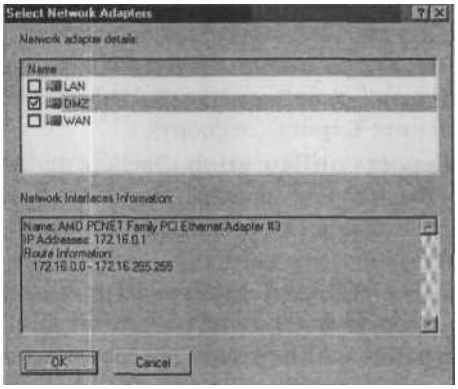


Рис. 4.46. Выбор сетевого адаптера

11. Щелкните **Next** (Далее) на странице **Perimeter Network IP Addresses** (IP-адреса сети параметра).
12. На странице **Select a Firewall Policy** (Выбрать политику брандмауэра) выберите политику брандмауэра, соответствующую требованиям конкретной организации. Настоятельно рекомендуется выбрать политику **Block all** (Блокировать все) и настроить политику в соответствии с требованиями организации позже. Выберите политику **Block all** (Блокировать все) и щелкните **Next** (Далее).
13. Щелкните **Finish** (Завершить) на странице **Completing the Network Template Wizard** (Завершение работы мастера сетевого шаблона).
14. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
15. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Шаблон внешнего брандмауэра

Сетевой шаблон внешнего брандмауэра используется, когда брандмауэр ISA находится перед другим брандмауэром. Так, брандмауэр ISA считается внешним, а брандмауэр, расположенный позади **него,** — внутренним. Внутренним брандмауэром может быть брандмауэр ISA или брандмауэр стороннего производителя; это не влияет на внешний брандмауэр ISA.

Шаблон внешнего брандмауэра предусматривает несколько предположений относительно конкретной сетевой инфраструктуры и характеристик сети, расположенной позади внешнего брандмауэра ISA: ■ шаблон внешнего брандмауэра предполагает, что сеть позади брандмауэра ISA —

это сеть периметра. После запуска шаблона внешнего брандмауэра внешний бранд-

мауэр не определяет «внутрен нюю» сеть. Новая сеть периметра, определенная этим шаблоном, будет играть роль бывшей внутренней сети по умолчанию;

- создается новое сетевое правило под названием Perimeter Access (Доступ к сети периметра). Это сетевое правило устанавливает отношение маршрутизации между сетью периметра и сетью VPN-клиентов с одной стороны и внешней сетью с другой. Предполагается, что будут использоваться общие адреса в сети позади внешнего брандмауэра ISA. Если в сети позади брандмауэра ISA не используют ся общие адреса, то сетевое правило по умолчанию станет причиной сбоев. Если в сети позади внешнего брандмауэра ISA используются частные адреса, следует изменить отношение маршрутизации типа «маршрут» в данном сетевом прави ле на NAT;
- в определенных обстоятельствах при наличии внешнего брандмауэра ISA поль зователю приходится столкнуться с таким явлением, как «сеть в Сети». Если между сетью периметра и сетью позади внутреннего брандмауэра ISA установлено отношение типа «маршрут», то нужно в определение сети периметра на внеш нем брандмауэре ISA включить все адреса сети, находящейся позади внутрен него брандмауэра ISA.

Последний пункт заслуживает особого внимания, потому что его последствия могут не сказаться сразу же. На рис. 4.47 показан пример **конфигурации** внешнего/внутреннего брандмауэра, в которой каждый из брандмауэров является брандмауэром ISA.

Рис. 4.47. Отношения маршрутизации в сети позади сети

В этом примере внутренний брандмауэр ISA определяет свою внутреннюю сеть как 10.0.0.0/24, а сеть периметра как часть своей внешней сети по умолчанию. Заметьте, что не нужно определять сеть периметра как часть внешней сети по умолчанию на внутреннем брандмауэре ISA. Можно просто создать новый сетевой объект под названием *сеть периметра* и присвоить сетевой адрес сети периметра этому сетевому объекту. Однако в данном случае просто предполагается, что сеть периметра является частью внешней сети по умолчанию на внутреннем брандмауэре ISA. На внутреннем брандмауэре ISA также имеется сетевое правило, которое устанавливает отношение типа «маршрут» между внутренней сетью внутреннего брандмауэра ISA и его внешней сетью.

К внешнему брандмауэру ISA был применен шаблон внешнего брандмауэра, поэтому у него нет внутренней сети. Напротив, внутренняя сеть была заменена на сеть периметра, как уже говорилось ранее. Адреса, входящие в сеть периметра внешнего брандмауэра ISA, включают все адреса сети периметра, а именно 192.168.1.0/24. На внешнем брандмауэре ISA заданы отношения NAT между сетью периметра и Интернетом.

Представим, что хост во внутренней сети позади внутреннего брандмауэра ISA пытается установить соединение с ресурсами в Интернете. Что произойдет? Поскольку между внутренней сетью внутреннего брандмауэра ISA и сетью периметра заданы отношения типа «маршрут», исходный IP-адрес этого хоста во внутренней сети будет сохранен. Когда внешний брандмауэр ISA получит запрос на соединение, он увидит исходный IP-адрес хоста внутренней сети, предположит, что в соединении используется ложный адрес, и запретит попытку соединения.

Почему? Потому что, когда на одном интерфейсе брандмауэр ISA получает пакет с IP-адреса, не достижимого с данного интерфейса, он рассматривает это как попытку проникновения. Поскольку у внешнего брандмауэра ISA нет определения сетевого адреса 10.0.0.0/16, он считает его частью внешней сети по умолчанию. Поскольку хосты внешней сети не могут напрямую устанавливать соединение с внутренним интерфейсом брандмауэра ISA, внешний брандмауэр ISA отбрасывает соединение, потому что он считает его ложным. Обнаружение подложного доступа является важным компонентом системы обнаружения и предупреждения вторжений брандмауэра ISA.

В этой ситуации можно добавить адреса внутренней сети внутреннего брандмауэра ISA к списку адресов для сети периметра внешнего брандмауэра ISA и добавить маршрут для внутренней сети внутреннего брандмауэра ISA в таблицу маршрутизации внешнего брандмауэра ISA. В таком **случае** внешний брандмауэр ISA будет знать, что внутренняя сеть внутреннего брандмауэра ISA достижима с интерфейса сети периметра внешнего брандмауэра ISA, и не будет запрещать такие соединения, как попытку подложного доступа.

Важно отметить, что такая конфигурация также является безопасной. Брандмауэр ISA по-прежнему может определять ложные пакеты на всех интерфейсах, включая внешний интерфейс.

В табл. 4.8 представлены политики брандмауэра для сетевого шаблона внешнего брандмауэра. Настоятельно рекомендуется использовать шаблон **Block all** (Блокировать все), а затем создавать собственные политики брандмауэра, соответствующие требованиям конкретной организации.

Табл. 4.8. Политики брандмауэра для сетевого шаблона внешнего брандмауэра

Название политики	Описание	Создаваемые правила
Block all (Заблокировать **все)**	Эта политика блокирует весь доступ к сети через ISA Server. Этот вариант не создает никаких правил доступа, кроме правила по умолчанию, которое блокирует весь доступ. Используйте этот вариант, если нужно определить политику брандмауэра самостоятельно	Нет
Block Internet access, allow access **to ISP network services** (Заблокировать доступ к Интернету, разрешить доступ к сетевым службам интернет-провайдера)	Эта политика блокирует весь доступ к сети через ISA Server, за исключением доступа к службам внешней сети типа DNS. Этот вариант полезен, если службы предоставляются интернет-провайдером. Этот вариант следует использовать, если нужно определить политику брандмауэра самостоятельно	Разрешить DNS из сети VPN-клиентов и сети периметра к внешней сети (Интернет)
Block Internet access (network services are on the perimeter network) (Блокировать доступ к Интернету (сетевые службы находятся *в* сети периметра))	Эта политика блокирует весь доступ к сети через брандмауэр ISA, кроме доступа к сетевым службам типа DNS в сети периметра. Этот вариант используется, если нужно определить политику брандмауэра самостоятельно	Разрешить DNS из внутренней сети и сети VPN-клиентов в сеть периметра
Allow limited Web-access (network services are on the perimeter network) (Разрешить ограниченный Web-доступ (сетевые службы находятся в сети периметра))	Эта политика разрешает ограниченный Web-доступ. Весь остальной доступ к сети блокируется	Разрешить HTTP, HTTPS и FTP-соединения из сети VPN-клиентов и сети периметра во внешнюю сеть (Интернет). Разрешить соединения по всем протоколам из сети VPN-клиентов в сеть периметра
Allow limited Web access, **allow ISP network services** (Разрешить ограниченный Web-доступ, разрешить сетевые службы, предоставленные интернет-провайдером)	Эта политика разрешает ограниченный Web-доступ и разрешает доступ к сетевым службам типа DNS, предоста в л енны м интерн ет - п ро ва й дером. Весь остальной доступ к сети блокируется	Разрешить HTTP, HTTPS и FTP-доступ из сети периметра и сети VPN-клиентов во внешнюю сеть (Интернет). Разрешить DNS-трафик из внутренней сети, сети VPN-клиентов и сети периметра во внешнюю сеть (Интернет). Разрешить все протоколы из сети VPN-клиентов в сеть периметра

(см. след. стр.)

Табл. 4.8. (окончание)

Название политики	Описание	Создаваемые правил;з
Allow unrestricted access (Разрешить не- ограниченный доступ)	Эта политика разрешает неограничен- ный доступ к Интернету через ISA Ser- ver. ISA Server блокирует доступ из сети периметра Интернета к защищенным сетям. Позже можно изменить правила доступа, чтобы заблокировать конкретные типы сетевого доступа	Разрешить в с е протоколы из сети VPN-клиентов в сеть

Для применения шаблона внешнего брандмауэра выполните следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем узел **Configuration** (Настройка). Щелк ните узел **Networks** (Сети).
2. В узле **Networks** (Сети) на панели **Task** (Задача) щелкните вкладку **Templates** (Шаблоны). Выберите сетевой шаблон **Front Firewall** (Внешний брандмауэр), дважды щелкнув на этой записи,
3. Щелкните **Next** (Далее) на **странице Welcome to the Network Template Wizard.**
4. На странице **Export the ISA Server Configuration** (Экспортировать конфигу рацию ISA Server) имеется вариант создания копии текущей конфигурации бранд мауэра ISA. Это полезная функция, потому что сетевой шаблон перепишет те кущую конфигурацию сети и политику брандмауэра. Если создать копию теку щей конфигурации, то можно с легкостью ее восстановить в случае, если ре зультат работы мастера сетевого шаблона вам не понравится. Щелкните **Export** (Экспортировать).
5. В диалоговом окне **Export Configuration** (Экспортировать конфигурацию) введите имя текущей конфигурации брандмауэра ISA в текстовое поле **File name** (Имя файла), в данном примере конфигурационный файл назван **Pre-Front Firewall Template.** Обратите внимание, что конфигурация сохраняется в фор мате XML Не нужно выбирать варианты **Export user permission settings** (Эк спортировать настройки полномочий пользователя) или **Export confidential information (encryption will be used)** (Экспортировать конфиденциальную информацию, будет использовано шифрование), потому что вы не связываете полномочия пользователя с этим шаблоном и вряд ли будете использовать этот резервный файл для копирования конфигурации брандмауэра ISA на другой компьютер. Нужно лишь создать копию текущей сети и политики брандмауэра. Щелкните **Export** (Экспортировать).
6. Появится диалоговое окно **Exporting** (Экспортирование). Щелкните ОК когда мастер сообщит об успешном экспорте конфигурации.
7. Щелкните **Next** (Далее) на странице **Export the ISA *Server* Configuration** (Эк спортировать конфигурацию ISA Server).

8. На странице **Perimeter Network IP Addresses** (IP-адреса сети периметра) ус тановите адреса, определяющие внутреннюю сеть. Адреса, отображаемые по умолчанию, — это адреса, которые уже применялись при создании внутренней сети при установке брандмауэра ISA. Существует возможность добавить допол нительные адреса с помощью кнопок **Add** (Добавить), **Add Adapter** (Добавить адаптер) **и Add Private** (Добавить частные). Рекомендуется в данном случае ис пользовать кнопку **Add Adapter** (Добавить адаптер) и избегать использования кнопки **Add Private** (Добавить частные). Щелкните **Next** (Далее).
9. На странице **Select a Firewall Policy** (Выберите политику брандмауэра) выбе рите политику брандмауэра, соответствующую требованиям конкретной органи зации. Настоятельно рекомендуется выбрать политику **Block all** (Заблокировать все) и настроить политику в соответствии с конкретными требованиями позднее. Выберите политику **Block all** (Блокировать все) и щелкните Next (Далее).
10. Щелкните **Finish** (Завершить) на странице **Completing the Network Template Wizard** (Завершение работы мастера сетевого шаблона).
11. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
12. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Шаблон внутреннего брандмауэра

Шаблон внутреннего брандмауэра очень похож на шаблон граничного брандмауэра, за исключением их сетевых графиков на консоли управления **Microsoft Internet Security and Acceleration Server 2004.** На рис. 4.48 показан сетевой график для шаблона внутреннего брандмауэра, а на рис. 4.49 показан сетевой график для шаблона граничного брандмауэра.

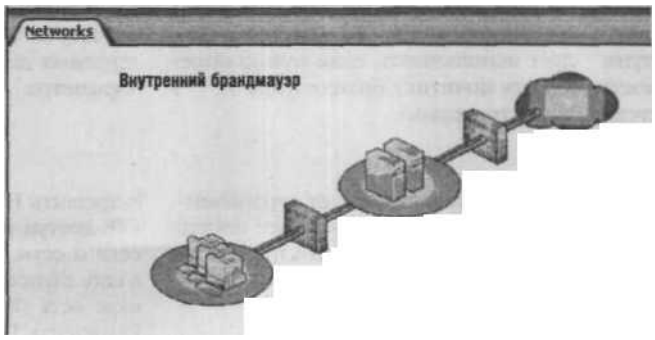
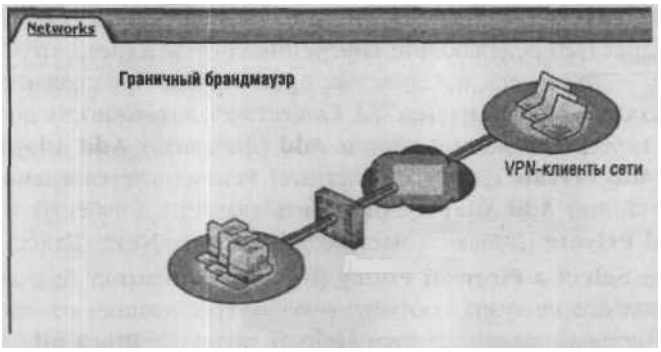


Рис. 4.48. Сетевой график для шаблона внутреннего брандмауэра



Внешняя сеть (Интернет)

Локальный хост

Внутренняя **сеть** Рис. 4.49. Сетевой

график для шаблона граничного брандмауэра

В табл. 4.9 представлены политики брандмауэра для шаблона внутреннего брандмауэра. Рекомендуется выбрать шаблон Block all (Блокировать все), *а* затем создать политики в соответствии с требованиями к безопасности конкретной организации.

Табл. 4.9. Политики брандмауэра для внутреннего брандмауэра

Название политики	Описание	Создаваемые правила
Block all (Заблокировать **все)**	Эта политика блокирует весь доступ к сети через ISA Server. Этот вариант не создает никаких правил доступа, кроме правила по умолчанию, которое блокирует весь доступ. Используйте этот вариант, если нужно определить политику брандмауэра самостоятельно	Нет
No access: Block Internet access **(network services are in the perimeter network)** (Нет доступа: заблокировать доступ к Интернету (сетевые службы находятся в сети периметра))	Эта политика блокирует весь доступ к сети через ISA Server, за исключением доступа к сетевым службам (DNS) в сети периметра. Этот вариант следует использовать, если нужно определить политику брандмауэра самостоятельно	Разрешить DNS из внугренней сети, сети VPN-клиентов к внешней сети (Интернет) за исключением адресных диапазонов сети периметра
Restricted access: Allow limited Web access (network services are on perimeter network) (Ограниченный доступ: разрешить ограниченный Web-*доступ* (сетевые службы находятся в сети периметра))	Эта политика разрешает ограниченный Web-доступ и разрешает доступ к сетевым службам в сети периметра. Весь остальной доступ к сети блокируется	Разрешить HTTP, HTTPS и FTP-доступ из внутренней сети и сети VPN-клиентов в сеть периметра и во внешнюю сеть (Интернет). Разрешить DNS-трафик из внутренней сети и сети VPN-клиентов в сеть периметра. Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть

Табл. 4.9. (окончание)

Название политики	Описание	Создаваемые правила
Restricted access: Allow limited Web-access, allow ISP network services (Ограниченный доступ: разрешить ограниченный доступ к Интернету, разрешить сетевые службы, предоставляемые интер нет-провайдером)	Эта политика разрешает ограниченный доступ к Интернету и доступ к сетевым службам типа DNS, предоставляемым интернет-провайдером. Весь остальной доступ к сети блокируется	Разрешить HTTP, HTTPS и FTP-соединения из внутренней сети и сети VPN-клиентов во внешнюю сеть (Интернет), Разрешить DNS из внутренней сети и сети VPN-клиентов во внешнюю сеть (Интернет) за исключением адресного диапазона сети периметра. Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть
Unrestricted Internet access: Allow all protocols (Неограниченный доступ к Интернету: разрешить все протоколы)	Эта политика разрешает неограниченный доступ к Интернету через ISA Server. ISA Server запрещает доступ из Интернета в защищенные сети. Позже можно изменить правила доступа, чтобы заблокировать конкретные типы сетевого доступа	Разрешить все протоколы из внутренней сети и сети VPN-клиентов во внешнюю сеть (Интернет) и диапазон адресов сети периметра, Разрешить все протоколы из сети VPN-клиентов во внутреннюю сеть

Для того чтобы применить шаблон внутреннего брандмауэра выполните следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Настройка). Щелкните узел **Networks** (Сети).
2. В узле **Networks** (Сети) на панели **Task** (Задача) щелкните вкладку **Templates** (Шаблоны). Дважды щелкните запись **Back Firewall Template** (Шаблон внут реннего брандмауэра).
3. Щелкните **Next** (Далее) на странице **Welcome to the Network Template Wizard.**
4. На странице **Export the ISA Server Configuration** (Экспортировать конфигу рацию ISA Server) имеется вариант создания копии текущей конфигурации бранд мауэра ISA. Это полезная функция, потому что сетевой шаблон перепишет текущую конфигурацию сети и политику брандмауэра. Если создать копию те кущей конфигурации, то можно с легкостью ее восстановить в случае, если ре зультат работы мастера сетевого шаблона вам не понравится. Щелкните **Export** (Экспортировать).
5. В диалоговом окне **Export Configuration** (Экспортировать конфигурацию) вве дите имя текущей конфигурации брандмауэра ISA в текстовом поле **File name** (Имя файла), в данном примере конфигурационный файл назван **Pre-Edge**

Firewall Template. Обратите внимание, что конфигурация сохраняется в формате XML. Не нужно выбирать варианты **Export user permission settings** (Экспортировать настройки полномочий пользователя) или **Export confidential information (encryption will be used)** (Экспортировать конфиденциальную информацию, будет использовано шифрование), потому что вы не связываете полномочия пользователя с этим шаблоном и вряд ли будете использовать этот резервный файл для копирования конфигурации брандмауэра ISA на другой компьютер. Нужно лишь создать копию текущей сети и политики брандмауэра. Щелкните **Export** (Экспортировать).

6. Появится диалоговое окно **Exporting** (Экспортирование). Щелкните ОК, когда мастер сообщит, что он успешно экспортировал конфигурацию.
7. Щелкните **Next** (Далее) на странице **Export the ISA Server Configuration** (Экспортировать конфигурацию ISA Server).
8. На странице Internal **Network IP Addresses** (IP-адреса внутренней сети) установите адреса, определяющие внутреннюю сеть. Мастер сетевого шаблона воспользуется теми же адресами, которые применялись для внутренней сети при установке брандмауэра ISA. Существует возможность добавить дополнительные адреса к внутренней сети по умолчанию с помощью кнопок **Add** (Добавить), **Add Adapter** (Добавить адаптер) и **Add Private** (Добавить частные). Кнопка **Add** (Добавить) позволяет вручную ввести диапазон или диапазоны адресов. Кнопка **Add Adapter** (Добавить адаптер) позволяет воспользоваться таблицей маршрутизации Windows, чтобы автоматически добавить адреса к внутренней сети, а кнопка **Add Private** (Добавить частные) автоматически добавляет все сетевые адреса к адресам, принадлежащим **внутренней** сети по умолчанию. В данном примере и чаще всего не следует менять адреса на этой странице. Щелкните **Next** (Далее).
9. На странице **Select *a* Firewall Policy** (Выберите политику брандмауэра) выберите политику брандмауэра (см. рис. 4.50), соответствующую требованиям конкретной организации (табл. 4.9). Настоятельно рекомендуется выбрать политику **Block all** (Блокировать все) и настроить политику брандмауэра в соответствии с конкретными требованиями позднее, когда станет ясен принцип работы политик брандмауэра ISA. Это снизит вероятность создания небезопасной конфигурации. В данном примере выберите политику **Block all** (Блокировать все) и щелкните **Next** (Далее).
10. Щелкните **Finish** (Завершить) на странице **Completing the Network Template Wizard** (Завершение работы мастера сетевого шаблона).
11. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
12. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

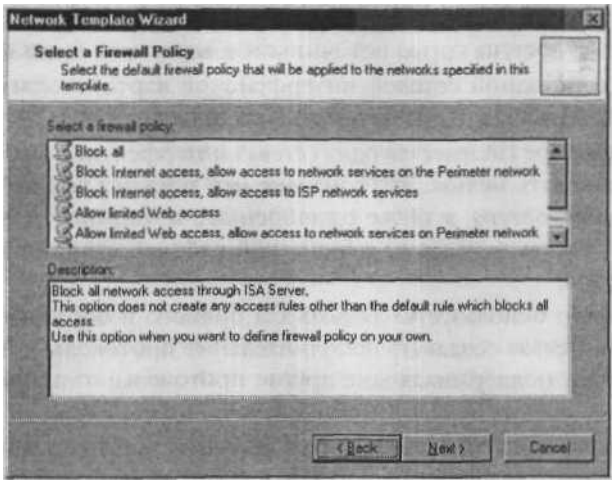


Рис. 4.50. Выбор политики брандмауэра

Шаблон с одним сетевым адаптером или шаблон сети с одним сетевым интерфейсом

Сетевой шаблон с одним сетевым адаптером используется, если нужно запустить брандмауэр ISA с одной сетевой интерфейсной картой. Если брандмауэр ISA установлен на компьютере с одним сетевым адаптером, то не нужно запускать шаблон с одним сетевым адаптером, а надо создать собственную политику доступа, в данном случае это предпочтительный метод настройки брандмауэра ISA. Шаблон сети с одним сетевым адаптером не создает политику доступа.

> **СОВЕТ** Если используется конфигурация с одной сетевой интерфейсной картой на компьютере с несколькими сетевыми картами, то можно соединить несколько сетевых сегментов с компьютером с установленным брандмауэром ISA. Однако брандмауэр ISA сможет только перенаправлять соединения с помощью протоколов HTTP, HTTPS и FTP-туннелей Web-прокси.

Шаблон с одним сетевым адаптером можно запускать на компьютерах с несколькими сетевыми интерфейсными картами, если отключить все сетевые интерфейсные карты, кроме одн ой. Однако, если используются несколько сетевых интерфейсов, следует помнить, что *все* эти интерфейсы рассматриваются как внутренние и что по отношению к компьютеру, к которому был применен шаблон сети с одним сетевым адаптером, никакие адреса не будут считаться внешними.

Нужно учитывать следующие особенности шаблона с одним сетевым адаптером: ■

после применения данного шаблона к брандмауэру ISA все адреса рассматриваются как внутренние. Брандмауэр ISA с одной сетевой интерфейсной картой

не различает внутреннее и внешнее, т. к. на нем есть только один интерфейс. Для всех правил доступа сетью источником и адресатом будет внутренняя сеть;

- брандмауэр ISA с одной сетевой интерфейсной картой поддерживает только протоколы HTTP, HTTPS и FTP-туннели Web-прокси;
- если на брандмауэре ISA имеется одна сетевая интерфейсная карта, клиент бранд мауэра использовать нельзя. Это означает, что теряется важный компонент за щиты, контроль доступа, а также расширенные возможности создания журна лов, которые имеются, когда на клиентской рабочей станции установлен кли ент брандмауэра;
- такой компьютер используется только для прямого и обратного кэширования и Web-прокси. Нельзя создавать дополнительные протоколы и нельзя создавать правила доступа, поддерживающие другие протоколы, отличные от интернет-протоколов;
- все мощные возможности брандмауэра в брандмауэре ISA в такой ситуации сво дятся к способности брандмауэра защитить самого себя. До тех пор, пока не будут созданы правила доступа, которые подвергают риску сам брандмауэр ISA, ника кие соединения с брандмауэром ISA установить невозможно;
- брандмауэр ISA нельзя сделать VPN-сервером;
- нельзя создать правила публикации серверов, можно создать лишь правила Web-публикации.

Рекомендуется использовать конфигурацию брандмауэра ISA с одним сетевым интерфейсом (с одной сетевой интерфейсной картой), только если в сети имеется еще один работающий брандмауэр ISA. Этот брандмауэр ISA обеспечивает мощную фильтрацию с отслеживанием соединений и мощную проверку с отслеживанием соединений на уровне приложения, а брандмауэр ISA с одной сетевой интерфейсной картой берет на себя нагрузку по обработке передачи данных через мост SSL-SSL (более подробно это обсуждается в главе 8 при рассмотрении публикации серверов в Интернете).

Для применения шаблона с одним сетевым адаптером нужно выполнить следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем узел **Configuration** (Настройка). Щелк ните узел Networks (Сети).
2. В узле **Networks** (Сети) на панели **Task** (Задача) щелкните вкладку **Templates** (Шаблоны). Дважды щелкните запись **Single Network Adapter Template.**
3. Щелкните **Next** (Далее) на странице **Welcome to the Network Template Wizard.**
4. На странице **Export the ISA Server Configuration** (Экспортировать конфигу рацию ISA Server) имеется вариант создания копии текущей конфигурации бранд мауэра ISA. Это полезная функция, потому что сетевой шаблон перепишет те кущую конфигурацию сети и политику брандмауэра. Если создать копию теку-

щей конфигурации, то можно с легкостью ее восстановить в случае, если результат работы мастера сетевого шаблона вам не понравится. Щелкните **Export** (Экспортировать).

5. В диалоговом окне **Export Configuration** (Экспортировать конфигурацию) введите имя текущей конфигурации брандмауэра ISA в текстовое поле **File name** (Имя файла), в данном примере конфигурационный файл назван **Pre-Edge Firewall Template.** Обратите внимание, что конфигурация сохраняется в формате XML. Не нужно выбирать варианты **Export user permission settings** (Экспортировать настройки полномочий пользователя) или **Export confidential information (encryption will be used)** (Экспортировать конфиденциальную информацию, будет использовано шифрование), потому что вы не связываете полномочия пользователя с этим шаблоном и вряд ли будете использовать этот резервный файл для копирования конфигурации брандмауэра ISA на другой компьютер. Нужно лишь создать копию текущей сети и политики брандмауэра. Щелкните **Export** (Экспортировать).

6. Появится диалоговое окно **Exporting** (Экспортирование). Щелкните ОК, когда мастер сообщит, что он успешно экспортировал конфигурацию. Щелкните

7. **Next** (Далее) на странице **Export the ISA Server Configuration** (Экспортировать конфигурацию ISA Server).

Ha На странице **Internal Network IP Addresses** (IP-адреса внутренней сети) (рис. 4.51) отображается список всех адресов в диапазоне IPv4 за исключением адресов в сети замыкания на себя. Щелкните **Next** (Далее).

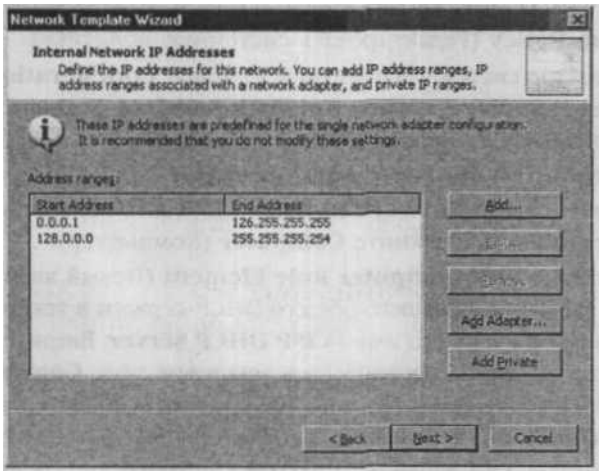


Рис. 4.51. Определение IP-адресов

9. На странице **Select a Firewall Policy** (Выберите политику брандмауэра) есть вариант **Single Default NIC** (Одна сетевая интерфейсная карта по умолчанию). Выберите этот вариант и щелкните **Next** (Далее).

10. Щелкните **Finish** (Готово) на странице **Completing the Network Template Wizard** (Завершение работы мастера сетевого шаблона).

Динамическое присваивание адреса на внешнем интерфейсе брандмауэра ISA

У многих небольших организаций нет статических IP-адресов, которые они могли бы присвоить внешнему интерфейсу брандмауэра ISA. Однако брандмауэр ISA поддерживает динамическое присваивание адресов на любом из своих интерфейсов. Настоятельно рекомендуется никогда не использовать динамическое присваивание адресов ни на каких интерфейсах, кроме внешнего интерфейса брандмауэра ISA.

Для того чтобы получить динамический адрес на внешнем интерфейсе, нужно изменить системную политику брандмауэра ISA, выполнив следующие действия.

1. Откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004,** разверните имя сервера и щелкните узел **Firewall Policy** (Поли тика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) на панели задач щелкните вкладку Tasks (Задачи). В группе **System Policy Tasks** (Задачи системной политики) щелк ните ссылку **Show System Policy Rules** (Показать правила системной политики).
3. Список **System Policy Rules** (Задачи системной политики) появится прежде правил **Firewall Policy** (Политика брандмауэра). Правой кнопкой мыши щелк ните правило системной политики № 8 **Allow DHCP replies from DHCP server to ISA Server** (Разрешить DHCP-ответы от DHCP-сервера ISA Server) и щелкни те **Edit System Policy** (Редактировать системную политику).
4. Откроется редактор системной политики, в разделе **Configuration Groups** (Груп пы конфигурирования) в группе **Network Services** (Сетевые службы) будет выделена запись **DHCP.** Щелкните вкладку **From** (От).
5. На вкладке **From** (От) щелкните **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые записи) щелкни те меню **New** (Новый). Щелкните **Computer** (Компьютер).
7. В диалоговом окне **New Computer Rule Element** (Новый элемент правила для компьютера) введите имя вашего общего DHCP-сервера в текстовое поле **Name** (Имя). В данном примере его имя — **ISP DHCP Server.** Введите IP-адрес DHCP-сервера вашего интернет-провайдера в текстовое поле **Computer IP Address** (IP-адрес компьютера). Введите описание объекта компьютер в текстовое поле **Description (optional)** (Описание, необязательно). Щелкните ОК.
8. В диалоговом окне **Add Network Entities** (Добавить новые сетевые объекты) щелкните папку **Computers** (Компьютеры), а затем дважды щелкните на запи си вашего сервера **ISP DHCP server.** Если IP-адрес DHCP-сервера вашего интер нет-провайдера неизвестен, щелкните папку **Networks** (Сети) и дважды щелк ните внешнюю сеть **External** (Внешняя). Щелкните **Close** (Закрыть).

9. Щелкните ОК в окне **System Policy Editor** (Редактор системной политики).
10. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
11. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
12. Теперь можно настроить внешний интерфейс на использование динамического присвоения адреса. Если на внешнем интерфейсе брандмауэра ISA запустить монитор сети, то на экране появится окно, изображенное на рис. 4.52.

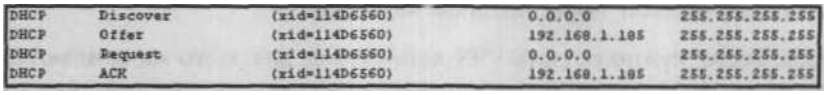


Рис. 4.52. Отслеживание DHCP-диалога с помощью монитора сети

Если IP-адрес DHCP-сервера неизвестен, его можно узнать с помощью команды ipconfig/all. В результате будет выведен IP-адрес DHCP-сервера интернет-провайдера.

Поддержка коммутируемых соединений для брандмауэров ISA, в том числе VPN-подключений к интернет-провайдеру

Чтобы установить соединение с интернет-провайдером в области с ограниченной поддержкой, организациям приходится использовать модемные коммутируемые соединения или VPN-подключения. Брандмауэр ISA поддерживает коммутируемые соединения с Интернетом: аналоговое модемное соединение или VPN-подключение. Оба типа соединений можно настроить в окне **Network Connections** (Сетевые подключения) брандмауэра ISA. Создаваемое соединение называется *коннектоидом* (connectoid) и отображается в окне **Network Connections** (Сетевые подключения) в виде значка. Затем брандмауэр ISA нужно настроить на применение этого коннектоида.

Начинающие администраторы брандмауэра ISA часто создают коннектоид и ожидают, что брандмауэр ISA будет его использовать, или же они настраивают коммутируемое соединение в консоли управления **Microsoft Internet Security and Acceleration Server 2004,** но не создают его в окне **Network Connections.**

Для выполнения коммутируемого соединения с брандмауэром ISA нужно выполнить три действия:

- Создать коммутируемый коннектоид.
- Настроить брандмауэр ISA так, чтобы он использовал этот коннектоид.
- Создать правило доступа, разрешающее брандмауэру ISA использовать VPN-протокол (только при использовании VPN-подключения для коммутируемой линии).

Рассмотрим пример того, как создать VPN-коннектоид и использовать его при настройке коммутируемых соединений брандмауэра ISA. Такая конфигурация распространена среди пользователей DSL в Европе. Также обсудим все доступные воз-

можности, с тем чтобы пользователи модемов коммутируемой линии передачи также могли извлечь пользу из данных инструкций.

> ПРЕДУПРЕЖДЕНИЕ При использовании коммутируемых VPN-подключений иногда наблюдаются проблемы с брандмауэром ISA и автоматическим набором. В ряде случаев оказывается, что коммутируемое соединение не выполняет автоматического набора. В такой ситуации нужно вручную установить VPN-подключение и настроить его так, чтобы при разрыве соединения происходил автоматический повторный набор. С аналоговыми модемными соединениями таких проблем не бывает.

Прежде всего, нужно создать VPN-коннектоид, для этого на компьютере с ОС Windows Server 2003 выполните следующие действия. Сходные действия выполняются и на компьютере с ОС Windows 2000.

1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и щелкните **Properties** (Свойства).
2. В окне **Network Connections** (Сетевые подключения) щелкните ссылку **New Connection Wizard** (Создание нового подключения).
3. Щелкните **Next** (Далее) на странице **Welcome to the New Connection Wizard** (Мастер новых подключений).
4. На странице **Network Connection Type** (Тип сетевого подключения) выбери те **Connection to the network at my workplace** (Подключить к сети на рабо чем месте) и щелкните **Next** (Далее).
5. На странице **Network Connection** (Сетевое подключение) выберите вариант **Virtual Private Network connection** (Подключение к виртуальной частной сети) и щелкните **Next** (Далее).
6. На странице **Connection Name** (Имя подключения) введите имя VPN-коннектоида в текстовое поле **Company Name** (Организация), в данном примере — **VPN to ISP.** Щелкните **Next** (Далее).
7. На странице **VPN Server Selection** (Выбор VPN-сервера) введите IP-адрес VPN-сервера интернет-провайдера в текстовое поле **Host name or IP address** (Имя компьютера или IP-адрес). Щелкните **Next** (Далее).
8. На странице **Connection Availability** (Доступность соединения) выберите ва риант **Anyone's use** (Все пользователи) и щелкните **Next** (Далее).
9. На странице **Completing the New Connection Wizard** (Завершение работы мастера новых подключений) щелкните **Finish** (Готово).
10. В диалоговом окне **Connect VPN to ISP** (Установить соединение VPN к ISP) щелкните **Properties** (Свойства).
11. В диалоговом окне **Connect VPN to ISP** щелкните вкладку **Options** (Парамет ры). **В** разделе **Redialing** (Параметры повторного звонка) установите флажок в поле **Redial if line is dropped** (Перезвонить при разрыве связи). В текстовое поле **Redial attempts** (Число повторений набора номера) введите 99- В выпа-

дающем списке **Time between redial attempts** (Интервал между повторениями) выберите **5 seconds** (5 секунд). В выпадающем списке **Idle time before hanging up** (Время простоя до разъединения) выберите **Never** (Никогда).

12. В диалоговом окне **Connect VPN to ISP** (Установить соединение VPN к ISP) вве дите имя пользователя и пароль, полученный от интернет-провайдера при по купке учетной записи. Установите флажок в поле **Save this user name and pass word for the following users** (Сохранять имя пользователя и пароль). Выбери те вариант **Anyone who uses this computer** (Для любого пользователя).
13. Щелкните **Connect** (Вызов), чтобы проверить коннектоид и убедиться, что с его помощью можно установить соединение с интернет-провайдером.

Теперь нужно настроить брандмауэр ISA на использование этого коннектоида.

1. В панели управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Настройка). Щелкните узел **General** (Общие).
2. В узле **General** (Общие) щелкните ссылку **Specify Dial-Up Preferences** (Ука зать параметры коммутируемого соединения).
3. В диалоговом окне **Dialing Configuration** (Настройка набора номера) имеет ся несколько вариантов:

a I will dial the connection myself (Я произвожу набор номера самостоятельно). Этот вариант используется, если нужно установить коммутируемое соединение, прежде чем пользователи в защищенной сети смогут получить доступ к Интернету через это подключение. Это требует вмешательства оператора для выполнения соединения, но после установки соединения оно может быть настроено на автоматический повторный набор в случае разрыва связи. Этот вариант следует использовать для VPN-подключений и для любого подключения, при котором автоматический набор номера не является эффективным;

a Allow automatic dialing to this network (Разрешить автоматический набор номера для установки соединения с этой сетью). Этот вариант позволяет брандмауэру ISA автоматически устанавливать соединение в ответ на запрос клиентов Web-прокси, SecureNAT и клиентов брандмауэра в защищенной сети за брандмауэром ISA. Следует быть внимательным при выборе этого варианта при использовании VPN-подключения. Если при включении этого варианта набор номера для установки соединения производится неправильно, то нужно отключить его и выбрать вариант **I will dial the connection myself** (Я произвожу набор номера самостоятельно);

□ **Configure this dial-up connection as the default gateway** (Настроить это коммутируемое подключение в качестве шлюза по умолчанию). Этот вариант позволяет брандмауэру ISA заменить свои текущие настройки шлюза и использовать VPN-сервер, к которому он подключается, в качестве нового шлюза по умолчанию. Этот вариант используется в большинстве случаев при

установке соединения с интернет-провайдером с помощью коммутируемого подключения;

- **a Use the following dial-up connection** (Использовать следующее коммутируемое соединение). Этот вариант позволяет выбрать созданный коммутируемый коннектоид;

□ **Use this account** (Использовать эту учетную запись). Следует ввести то же имя пользователя, что и при создании коммутируемого коннектоида. Не следует вводить верительные данные локального домена. Нужно ввести реальные верительные данные, которые были получены от интернет-провайдера в качестве учетной записи для входа в Интернет. 4. Щелкните **Apply** (Применить), затем ОК.

Если для коммутируемой связи используется VPN-подключение, то нужно создать правило доступа на брандмауэре ISA, которое позволит сети локального хоста использовать VPN-протоколы PPTP и L2TP/IPSec. Если интернет-провайдер использует другой VPN-протокол (например, патентованный протокол IPSec NAT-T), то нужно создать правило доступа, которое разрешает использование этого протокола. Большинство интернет-провайдеров используют либо протокол PPTP, либо L2TP/IPSec для простоты или повышения безопасности.

Для создания правила доступа, разрешающего VPN-подключение, выполните следующие действия.

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Полити ка брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните вкладку **Tasks** (Зада чи) на панели задач. Щелкните ссылку **Create a New Access Rule** (Создать но вое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила доступа) введите имя правила в текстовое поле **Access Rule name** (Имя правила доступа), в данном примере — **PPTP to ISP.** Щелкните **Next** (Далее).
4. Выберите **Allow** (Разрешающее) на странице **Rule Action** (Действие правила). Щелкните **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите **Selected protocols** (Выбранные протоколы) из выпадающего списка **This rule applies to** (Это правило приме няется к). Щелкните **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) (рис. 453) щелкните папку **VPN and IPSec** и дважды щелкните **PPTP.** Щелкните **Close** (Закрыть). Если используется другой протокол, выберите соответствующий VPN-протокол.
7. Щелкните **Next** (Далее) на странице **Protocols** (Протоколы).

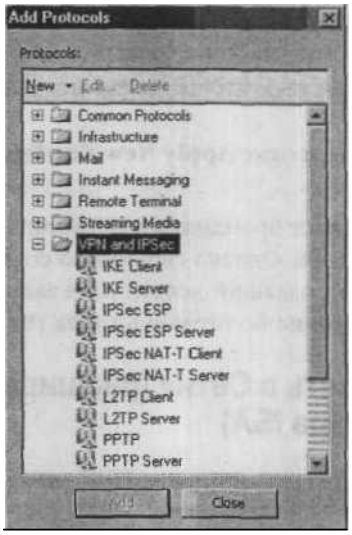


Рис. 4.53. Выбор VPN-протокола

8. На странице **Access Rule Sources** (Источники правила доступа) щелкните **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые записи) щелкните папку **Networks** (Сети), а затем дважды щелкните **Local Host** (Локальный хост). Щелкните **Close** (Закрыть).
10. Щелкните **Next** (Далее) на странице **Access Rule Sources** (Источники правила доступа).
11. На странице **Access Rule Destinations** (Адресаты правила доступа) щелкните **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните меню **New** (Новый) и щелкните **Computer** (Компьютер).
13. В диалоговом окне **New Computer Rule Element** (Новый элемент правила для компьютера) введите имя VPN-сервера интернет-провайдера в текстовое поле **Name** (Имя), в данном примере — **ISP VPN Server.** Введите IP-адрес VPN-сервера интернет-провайдера в текстовое поле **Computer IP address** (IP-адрес компьютера). Щелкните ОК.
14. Щелкните папку **Computers** (Компьютеры) в диалоговом окне **Add Network Entities** (Добавить сетевые объекты) и дважды щелкните запись **ISP VPN Server.** Щелкните **Close** (Закрыть).
15. Щелкните **Next** (Далее) на странице **Access Rule Destination** (Адресаты правила доступа).
16. Щелкните **Next** (Далее) на странице **User Sets** (Подмножества пользователей).

17. Щелкните **Finish** (Завершить) на странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила доступа).
18. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
19. Щелкните OK в диалоговом окне **Apply** New **Configuration** (Применить новую конфигурацию).

Эта конфигурация позволяет брандмауэру ISA устанавливать соединение с VPN-сервером интернет-провайдера. Однако еще нужно создать правила доступа, которые разрешат входящий и исходящий доступ к/из защищенных сетей брандмауэра ISA. Более подробно создание политики доступа рассматривается в главе 7.

Сетевой сценарий «сеть в Сети» (расширенная настройка брандмауэра ISA)

Для того чтобы полностью рассмотреть сценарий «сеть в Сети», нужно обратиться к базовой информации, приведенной ранее в этой главе. Вспомнив ключевые особенности сетевой модели брандмауэра ISA, можно подробно исследовать вопросы, связанные со сценарием «сеть в Сети». Этот сценарий часто вводит в заблуждение многих администраторов брандмауэра ISA, поэтому ему нужно уделить пристальное внимание.

Новая функция брандмауэра ISA по работе с несколькими сетями является его основным отличием от брандмауэра ISA Server 2000 с точки зрения подхода к сети. Брандмауэр ISA Server 2000 рассматривает сети как надежные и ненадежные. Для брандмауэра ISA Server 2000 является обязательным отношение между надежными сетями и таблицей LAT. Одно без другого невозможно. Надежные сети — это сети, входящие в таблицу LAT. Сети, не входящие в таблицу LAT, являются ненадежными. Взаимодействия между хостами LAT (хостами, IP-адреса которых содержатся в LAT) не подвергаются фильтрации с отслеживанием соединений и проверке с отслеживанием соединений на уровне приложения на брандмауэре ISA Server 2000.

В брандмауэре ISA Server 2004 таблиц LAT нет. Базовый принцип работы с несколькими сетями в брандмауэре ISA — ни одна сеть не является надежной по умолчанию и все соединения, выполняемые через брандмауэр ISA, подвергаются фильтрации с отслеживанием соединений и проверке с отслеживанием соединений на уровне приложения. Это позволяет обеспечить гораздо более высокий уровень защиты и контроля доступа, чем в брандмауэре ISA Server 2000. Не связывая между собой таблицу LAT и надежные сети, новый брандмауэр ISA позволяет администраторам осуществлять гораздо более жесткий контроль сетевых соединений.

Одним из ключевых понятий, которые необходимо знать для того, чтобы извлечь максимальную пользу из брандмауэра ISA, является понятие сетевого объекта. Далее перечислены наиболее важные моменты, касающиеся представления о сети брандмауэра ISA.

- Любой интерфейс может принадлежать только одной сети.
- Любой интерфейс не может принадлежать двум или нескольким сетям.
- На брандмауэр ISA можно установить столько сетевых интерфейсных карт, сколь ко поддерживается аппаратным обеспечением.
- Все IP-адреса, расположенные на одном сетевом интерфейсе, являются частью той же Сети.
- Все IP-адреса, определенные на брандмауэре ISA, считается защищенными се тями.
- Любой IP-адрес, который не определен на брандмауэре ISA, считается частью внешней сети по умолчанию.
- Сеть VPN-клиентов и сеть изолированных VPN-клиентов являются виртуальными или динамически создаваемыми сетями, что проявляется в том, что адреса до бавляются и удаляются из этих сетей, когда VPN-клиенты устанавливают и раз рывают соединение.
- Сеть, имеющая прямое подключение к конкретному интерфейсу, может считаться *корнем* конкретной сети. Например, если при создании сети на брандмауэре ISA используется адрес 10.0.0.0/16, то другие сети, находящиеся позади нее, долж ны иметь адреса 10.1.0.0/16, 10.2.0,0/16 и т. д. Затем можно суммировать всю сеть, связанную с этим адаптером, как 10.0.0.0/8; сюда войдут все сети, распо ложенные на этом интерфейсе.

Можно также добавить сети, находящиеся на одном интерфейсе, которые не суммируются. Например, адрес одной подсети на брандмауэре ISA — 10.0.0.0/16, а другая сеть, расположенная позади первой сети, имеет адрес 172.16.0.0/16. Такая конфигурация является допустимой для брандмауэра ISA. При определении сети, которую представляет этот сетевой интерфейс, нужно лишь включить все адреса в оба идентификатора сети.

Если на одном сетевом интерфейсе определено несколько сетей, то сети, не являющиеся частью подсети сети, считаются сетями в Сети (рис. 4.54). Брандмауэр ISA должен быть настроен с записью в таблице маршрутизации, которая предоставляет адрес шлюза сетям из подсети сети.

На рис. 4.54 показана базовая схема экспериментальной сети. Она будет использоваться для демонстрации ситуаций, с которыми может столкнуться пользователь при работе с конфигурацией «сеть в Сети». Идентификатор сети подсети — 10.0.0.0/24, а *сеть,* расположенная позади сервера Checkpoint имеет сетевой идентификатор 10.10.10.0/24. Вданном примере используется сервер Checkpoint, на его месте может быть любой брандмауэр или маршрутизатор с фильтрацией пакетов. Также сервер Checkpoint можно заменить на аппаратный маршрутизатор, коммутатор уровня 3 или даже на VPN-шлюз, который соединяет некую сеть с защищенными сетями брандмауэра ISA. На рис. 4.54 представлена внутренняя «сеть в Сети».

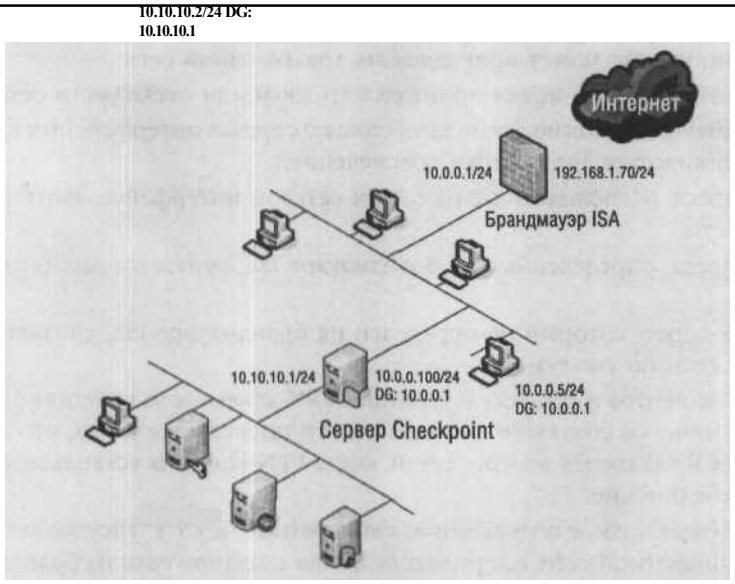


Рис. 4.54. Внутренняя «сеть в Сети»

Вкратце, клиент SecureNAT — это любой компьютер, настроенный с адресом шлюза по умолчанию, который маршрутизирует соединения в Интернет через брандмауэр ISA. Если клиент SecureNAT расположен в сети, непосредственно соединенной с брандмауэром ISA, то шлюз по умолчанию клиента SecureNAT является IP-адресом интерфейса брандмауэра ISA, к которому подключен клиент SecureNAT. Если клиент SecureNAT расположен на сетевом идентификаторе, отличном от интерфейса брандмауэра ISA, то клиент SecureNAT настраивается с адресом по умолчанию шлюза маршрутизатора, который будет перенаправлять интернет-запросы на интерфейс брандмауэра ISA.

На рис. 4.54 хост с IP-адресом 10.0.0.5/24 использует шлюз по умолчанию 10.0.0.1, потому что он находится на том же сетевом идентификаторе, что и локальный интерфейс брандмауэра ISA. Хост с IP-адресом 10.10.10.224 имеет шлюз по умолчанию 10.10.10.1, который перенаправляет интернет-запросы на локальный интерфейс сервера Checkpoint. Сервер Checkpoint настраивается с адресом по умолчанию шлюза 10.0.0.1, который является интерфейсом на брандмауэре ISA в той же сети, что и сервер Checkpoint. Сервер Checkpoint перенаправляет интернет-соединения на брандмауэр ISA, а брандмауэр ISA отправляет их на хост в Интернете.

Клиенты брандмауэра работают немного по-другому. Клиент брандмауэра настраивается с именем или IP-адресом брандмауэра ISA. Программное обеспечение клиента брандмауэра перехватывает все TCP- и UDP-соединения, выполняемые приложениями Winsock, с компьютером клиента брандмауэра и отправляет их напрямую на IP-адрес приемника клиента брандмауэра на интерфейсе брандмауэра ISA, т. е. в той же сети, в которой находится компьютер клиента брандмауэра.

Например, на рис. 4.54 клиент с IP-адресом 10.0.0.5/24 настраивается как клиент брандмауэра, а клиентское программное обеспечение настраивается на использование адреса 10.0.0.1 в качестве шлюза по умолчанию. Для клиента брандмауэра во внутренней сети с адресом 10.10.10.1/24 его приложение клиента брандмауэра также настроено на использование IP-адреса 10.0.0.1. Компьютер клиента брандмауэра отправляет соединения посредством программного обеспечения клиента брандмауэра прямо на брандмауэр ISA. Это означает, что клиент брандмауэра не зависит от текущей инфраструктуры маршрутизации в организации. Единственное требование состоит в том, чтобы в этой инфраструктуре был известен маршрут к сетям, в которых расположен интерфейс брандмауэра ISA.

Хотя эти различия могут показаться явными при работе с интернет-соединениями, если эти различия будут непонятны, то невозможно гарантировать успешную работу с конфигурацией «сеть в Сети».

На рис. 4.55 показан запрос и пути запроса между клиентом SecureNAT в подсети сети и сервером во внутренней сети (сети в Сети). Когда клиент SecureNAT в подсети сети отправляет запрос на соединение хосту во внутренней сети, клиент SecureNAT отправляет запрос на интерфейс брандмауэра ISA в той же сети, в которой находится клиент SecureNAT. Брандмауэр ISA перенаправляет запрос на интерфейс сервера Checkpoint, который может перенаправить его во внутреннюю сеть, а затем сервер Checkpoint перенаправляет соединение хосту адресата. Путь ответа проходит через сервер Checkpoint непосредственно на клиент SecureNAT, потому что сервер Checkpoint может перенаправить запрос напрямую клиенту и для этого ему не нужно использовать его адрес шлюза. На рис. 4.55 показан клиент SecureNAT, выполняющий соединение с сетью в Сети.

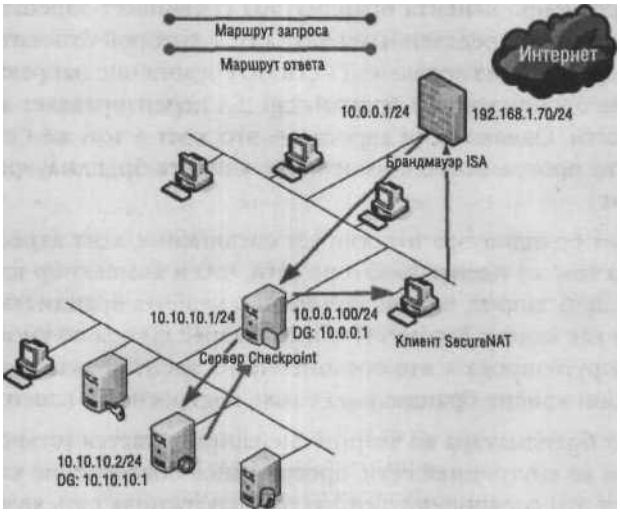


Рис. 4.55. Клиент SecureNAT выполняет соединение с сетью в Сети

Рассмотрим, как работает **клиент** брандмауэра. На рис. 4.56 показаны два сценария: первый сценарий: клиент брандмауэра выполняет соединение с внешней (нелокальной) сетью. Нелокальная сеть — это любая сеть, которая не находится в той же сети, в которой расположен клиент брандмауэра. Нелокальная сеть может быть расположена в Интернете или позади другого интерфейса, подключенного к брандмауэру ISA. Второй сценарий демонстрирует соединение клиента брандмауэра и локальной сети, которая является сетью, определенной как находящаяся в той же Сети, что и клиент брандмауэра, выполняющий запрос.

Первый сценарий показан на примере клиента брандмауэра, расположенного справа. Этот компьютер клиента брандмауэра пытается установить соединение с терминальным сервером по адресу 131.107.1.1. Правило доступа на брандмауэре ISA требует проверки подлинности до разрешения запроса на соединение к RDP-серверу (Reliable Datagram Protocol, надежный протокол доставки дейтаграмм) в Интернете. Клиент брандмауэра автоматически пересылает верительные данные клиента на брандмауэр, и, если правило доступа, разрешающее исходящие RDP-соединения, применимо к этому пользователю, соединение перенаправляется на удаленный RDP-сервер в Интернете.

Второй сценарий также показывает компьютер клиента брандмауэра, расположенный в той же подсети, что и локальный интерфейс брандмауэра ISA, но на этот раз RDP-соединение устанавливается с хостом во внутренней сети в Сети.

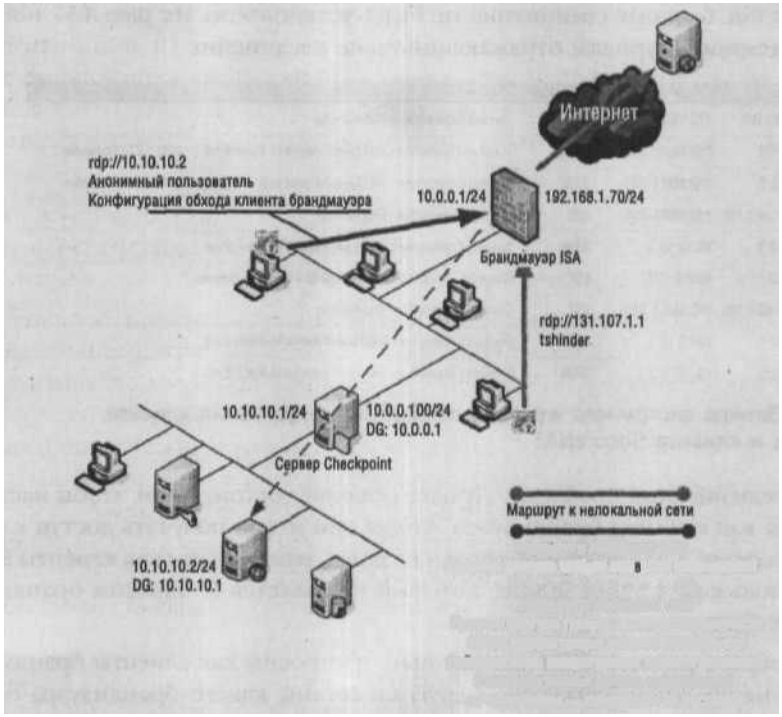
Именно здесь возникает проблема. Программное обеспечение клиента брандмауэра автоматически загружает *список* всех IP-адресов, определенных для Сети, к которой принадлежит клиент брандмауэра. В данном примере Сеть клиента брандмауэра включает все IP-адреса в диапазоне между 10.0.0.0/24 и 10.10.10.0/24. Программное обеспечение клиента брандмауэра сравнивает адресата запроса на соединение с адресами, определенными для Сети, к которой относится клиент брандмауэра. Если адресат не из локальной Сети, то соединение направляется на локальный интерфейс брандмауэра, а брандмауэр ISA перенаправляет это соединение к нелокальной сети. Однако если адресат — это хост в той же Сети, что и клиент брандмауэра, то программное обеспечение клиента брандмауэра проигнорирует это соединение.

Когда клиент брандмауэра игнорирует соединение, хост адресата должен быть расположен на том же идентификаторе сети, что и компьютер клиента брандмауэра, выполняющий запрос, или же компьютер клиента брандмауэра также должен быть настроен как клиент SecureNAT и иметь адрес шлюза по умолчанию, который способен маршрутизировать это соединение на идентификатор сети адресата. Во втором сценарии клиент брандмауэра также настроен как клиент SecureNAT.

Если клиент брандмауэра во втором сценарии пытается установить RDP-соединение с хостом во внутренней сети, программное обеспечение клиента брандмауэра игнорирует это соединение, потому что внутренняя сеть является частью той

же Сети, что и подсеть сети. Если клиент SecureNAT не может отправить верительные данные на брандмауэр ISA и если правило доступа, разрешающее RDP-соединения, требует проверки подлинности, то запрос на соединение будет отклонен. Вот что происходит по второму сценарию.

Если правило доступа не требует проверки подлинности, то второй сценарий будет работоспособным, потому что клиент брандмауэра сможет передать инициативу конфигурации клиента SecureNAT и установить соединение с хостом внутренней сети. Конечно, вся суть применения клиента брандмауэра состоит в том, чтобы обеспечить строгую пользовательскую /групповую проверку подлинности. На рис. 4.56 показаны маршруты клиента брандмауэра через локальные и нелокальные сети.



Маршрут к локальной сети Правило доступа требует п рове рки подлинности

• ..... •

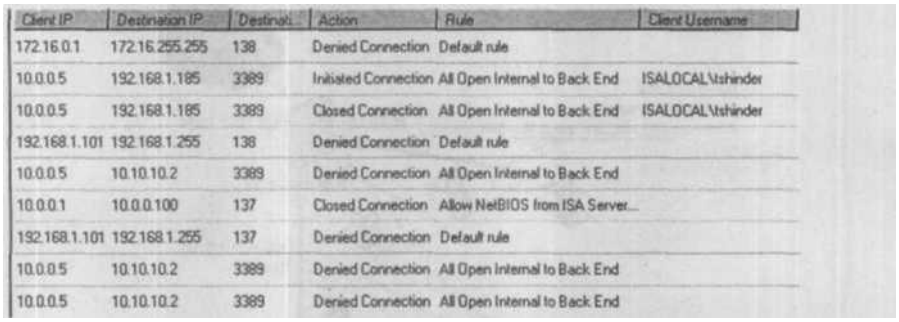
Маршрут к локальной сети
Прав ил о доступа требует проверки подлинности
Обход конфигурации клиента брандмауэра
Нейтрализация конфигурации клиента SecureNAT Если
ве рительные данные пользователя на ппрнмнм
— Eotjnmwm *м* состоится

Рис. 4.56. Маршруты клиента брандмауэра через локальные и нелокальные сети

Записи системного журнала показывают соединения с удаленным RDP-сервером и RDP-сервером в той же сети. Вторая и третья строки журнала показывают RDP-соединения с хостом в другой Сети. Клиент брандмауэра определяет, что адресатом соединения является хост в другой сети, перехватывает это соединение и перенаправляет его вместе с верительными данными пользователя на брандмауэр ISA. Информация о пользователе отражается в столбце Client Username (Имя

пользователя клиента), который подтвержд а ет, что соединение было обработано клиентом брандмауэра.

В пятой, восьмой и девятой строках системного журнала показаны попытки RDP-соединений с компьютером во внутренней сети, которая является частью той же Сети, что и компьютер клиента брандмауэра. Поскольку адресат находится в той же сети, что и компьютер клиента брандмауэра, клиент брандмауэра игнорирует запрос и инициативу перехватывает конфигурация клиента SecureNAT. Видно, что правило, разрешающее соединения с внутренней сетью в Сети, запрещает это соединение. Это соединение запрещено, потому что данное правило настроено так, чтобы запрашивать у пользователей проверку подлинности до выполнения соединения. Клиент SecureNAT никогда не сможет отправить верительные данные на брандмауэр ISA, поэтому соединение не будет установлено. На рис. 4.57 показаны записи системного журнала, отражающие такие соединения.



Client IP	Destination IP	Destinat...	Action	Rule	Client Username
172.16.0.1	172.16.255.255	138	Denied Connection	Default rule	
10.0.0.5	192.168.1.185	3389	Initiated Connection	All Open Internal to Back End	ISALOCAL\tshinder
10.0.0.5	192.168.1.185	3389	Closed Connection	All Open Internal to Back End	ISALOCAL\tshinder
192.168.1.101	192.168.1.255	138	Denied Connection	Default rule	
10.0.0.5	10.10.10.2	3389	Denied Connection	All Open Internal to Back End	
10.0.0.1	10.0.0.100	137	Closed Connection	Allow NetBIOS from ISA Server...	
192.168.1.101	192.168.1.255	137	Denied Connection	Default rule	
10.0.0.5	10.10.10.2	3389	Denied Connection	All Open Internal to Back End	
10.0.0.5	10.10.10.2	3389	Denied Connection	All Open Internal to Back End	

Рис. 4.57. Записи системного журнала показывают соединения клиента брандмауэра и клиента SecureNAT

Каково решение этой проблемы? Лучшее решение состоит в том, чтобы настроит компьютеры как клиенты брандмауэра, чтобы они могли получать доступ к ресур сам *в* других сетях, а для хостов подсети настроить компьютеры как клиенты Secure NAT, но использовать адрес шлюза, который не является IP-адресом брандмауэра ISA в той же Сети.

Компьютеры в подсети сети должны быть настроены как клиенты брандмауэра. Когда соединения устанавливаются с другими сетями, клиент брандмауэра обраба тывает эти соединения. Когда соединения устанавливаются с хостами в той же сети, клиент SecureNAT перехватывает инициативу и адрес шлюза по умолчанию буде установлен как интерфейс внутреннего маршрутизатора к внутренней *сети* в Сет Поскольку шлюз по умолчанию внутреннего маршрутизатора настроен как интер фейс брандмауэра ISA в той же сети, любой запрос клиента SecureNAT, который дол жен быть перенаправлен в Интернет, может выполняться внутренним маршрутиза тором. Это необходимо, если хост в подсети сети требует другой протокол (не Winsock, не TCP и не UDP), например протокол ICMP (для команд ping и tracert).

При такой конфигурации не нужно вносить никаких изменений во внутреннюю сеть в Сети. Клиенты брандмауэра в этой сети по-прежнему пересылают свои Winsock-запросы, направленные в другие Сети, на интерфейс брандмауэра ISA в той же сети. Конфигурация клиента SecureNAT также настроена на внутренний маршрутизатор, а этот маршрутизатор уже знает маршруты ко всем внутренним подсетям, поэтому брандмауэр ISA никогда не сможет запретить запрос, поскольку он его никогда не увидит. Конфигурация клиента SecureNAT для клиента внутренней сети позволяет установить прямое соединение с другими хостами в той же Сети. На рис. 4.58 показана рекомендуемая конфигурация.

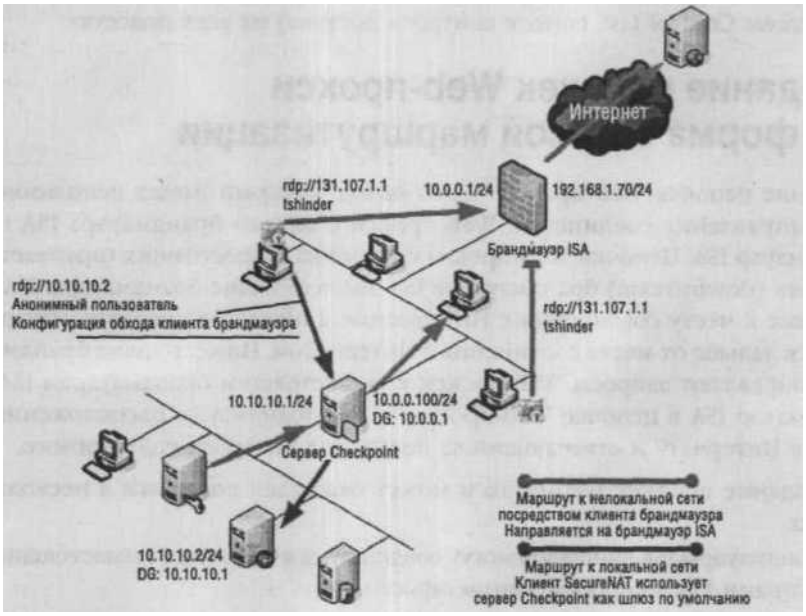


Рис. 4.58. Использование альтернативного адреса шлюза по умолчанию для хостов подсети

Сценарий сети в Сети является вполне работоспособным, все, что для него требуется, — включить все адреса на конкретном интерфейсе в эту Сеть. Основным ограничением в этом сценарии является то, что нельзя пользоваться клиентом брандмауэра для выполнения пользовательского/группового контроля трафика, проходящего между идентификаторами сети, расположенными в одной и той же Сети, определенной брандмауэром ISA.

Хотя на первый взгляд такое ограничение может вызвать разочарование пользователей, фактически брандмауэр ISA может контролировать трафик, проходящий через брандмауэр. Существуют приемы, позволяющие контролировать трафик из одной группы IP-адресов в другую с помощью правил доступа, но для того чтобы

брандмауэр ISA и любой брандмауэр вообще мог выполнять работу брандмауэра, соединения должны проходить через этот брандмауэр и перенаправляться из одной сети в другую сеть, находящуюся за тем же интерфейсом.

Примером такого приема может быть использование сетевого объекта *подсеть* или *диапазон адресов* для контроля доступа к другим компьютерам, расположенным в той же Сети. Фактически, можно осуществлять еще более жесткий контроль и использовать объекты типа компьютер. Заметьте, что этот прием применим только в ситуации, когда компьютеры расположены в одной подсети сети. Чтобы обеспечить сходный уровень контроля на всех внутренних подсетях, нужно создать списки ASL (Access Control List, список контроля доступа) на всех подсетях.

Создание цепочек Web-прокси как форма сетевой маршрутизации

Создание цепочек Web-прокси — это метод, который может использоваться для перенаправления соединений Web-прокси с одного брандмауэра ISA на другой брандмауэр ISA. Цепочки Web-прокси состоят из вышестоящих (upstream) и нижестоящих (downstream) брандмауэров ISA. Вышестоящие брандмауэры ISA находятся ближе к месту соединения с Интернетом, а нижестоящие брандмауэры ISA находятся дальше от места соединения с Интернетом. Нижестоящие брандмауэры ISA перенаправляют запросы Web-прокси к вышестоящим брандмауэрам ISA. Первый брандмауэр ISA в цепочке Web-прокси — это брандмауэр, расположенный ближе всего к Интернету и отвечающий за получение интернет-содержимого.

Создание цепочек Web-прокси может оказаться полезным в нескольких сценариях.

- Брандмауэры ISA филиалов могут соединяться в цепочки с вышестоящими бранд мауэрами ISA в корпоративном офисе.
- Брандмауэры ISA отделов, защищающие сети отделов организации, могут соеди няться в цепочки с вышестоящими брандмауэрами ISA, расположенными в сег менте сетевых служб, или с вышестоящими брандмауэрами ISA, которые имеют прямое соединение с Интернетом.
- Крупные корпоративные клиенты или интернет-провайдеры могут создавать цепочки из нижестоящих массивов Web-кэширования брандмауэра ISA и выше стоящего брандмауэра ISA или массива Web-кэширования брандмауэра ISA.

Используя цепочки Web-прокси, можно снизить общее использование пропускной способности как на канале связи с Интернетом, так и на всех каналах связи между нижестоящими и вышестоящими брандмауэрами ISA в цепочке Web-прокси. На рис. 4.59 показан пример цепочки Web-проски и прохождения потока информации через эту цепочку.

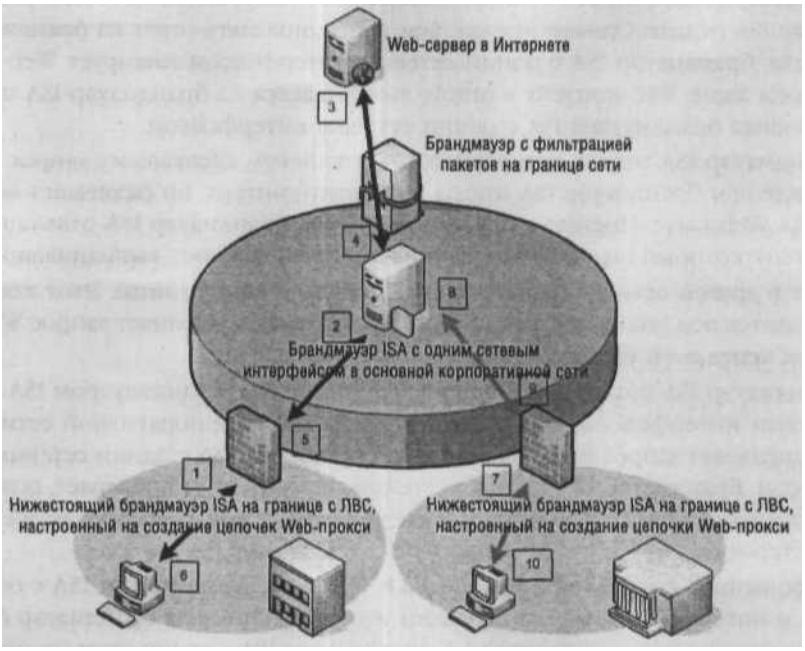


Рис. 4.59. WebProxyChaining.vsd

1. Клиент в защищенной Сети позади брандмауэра ISA выполняет запрос Web-стра ницы, расположенной на Web-сервере в Интернете. Запрос на соединение от правляется через брандмауэр ISA, защищающий ЛВС отдела.
2. Брандмауэр ISA перенаправляет этот запрос на соединение брандмауэру с од ним сетевым интерфейсом, расположенному в основной корпоративной сети. Брандмауэр ISA отдела настроен на использование цепочки Web-прокси для ус тановки соединения с брандмауэром ISA с одним сетевым интерфейсом. Посколь ку брандмауэр ISA с одним сетевым интерфейсом способен защититься от атак, атаки с хостов из основной сети или с хостов, расположенных на простом бран дмауэре на базе аппаратного обеспечения с фильтрацией пакетов перед бранд мауэром ISA с одним сетевым интерфейсом, не представляют для него серьез ной угрозы.
3. Брандмауэр с одним сетевым интерфейсом, работающий в режиме только Web-кэширования, перенаправляет запрос через простой аппаратный маршрутиза тор с фильтрацией пакетов.
4. Web-с ер в ер в Интернете возвращает ответ на брандмауэр ISA с одним сетевым интерфейсом через простой аппаратный брандмауэр с фильтрацией пакетов.

5. Брандмауэр ISA с одним сетевым интерфейсом перенаправляет ответ на бранд мауэр ISA отдела. Однако прежде чем перенаправлять ответ на брандмауэр ISA отдела, брандмауэр ISA с одним сетевым интерфейсом кэширует Web-контент в своем кэше. Web-контент в ответе возвращается на брандмауэр ISA отдела из Web-кэша брандмауэра ISA с одним сетевым интерфейсом.
6. Брандмауэр ISA отдела возвращает ответ клиенту, сделавшему запрос. Однако прежде чем брандмауэр ISA отдела возвратит контент, он размещает контент в своем Web-кэше. Именно из своего Web-кэша брандмауэр ISA отдела получает контент, который он затем передает на защищенный хост, выполнивший запрос.
7. Хост в другой сети выполняет запрос той же Web-страницы. Этот хост также находится под защитой брандмауэра ISA. Этот хост выполняет запрос Web-стра ницы через свой брандмауэр ISA.
8. Брандмауэр ISA объединен в цепочку Web-прокси с брандмауэром ISA с одним сетевым интерфейсом, находящимся в основной корпоративной сети. Он пе ренаправляет запрос на соединение на брандмауэр ISA с одним сетевым интер фейсом. Брандмауэр ISA с одним сетевым **интерфейсом** проверяет, содержится ли этот контент в его Web-кэше, прежде чем перенаправлять запрос на Web-сервер в Интернете.
9. Запрошенное содержимое находится в Web-кэше брандмауэра ISA с одним се тевым интерфейсом, и он возвращает это содержимое на брандмауэр ISA отде ла, который передал этот запрос. У брандмауэра ISA с одним сетевым интерфей сом нет необходимости в том, чтобы отправлять запрос на Web-сервер в Ин тернете, потому что эта информация уже содержится в его Web-кэше.
10. Брандмауэр ISA отдела перенаправляет Web-контент хосту, инициировавшему запрос.

В данном примере видна экономия не только пропускной способности на канале связи с Интернетом, но и на канале связи основной сети. То же самое наблюдается, когда другой хост из сети, защищенной брандмауэром, выполняет запрос того же Web-контента. В данном случае в Web-кэше брандмауэров ISA отделов уже содержится необходимая информация, и им не нужно перенаправлять этот запрос на брандмауэр ISA с одним сетевым интерфейсом в основной корпоративной сети. Это снижает общее использование пропускной способности основной корпоративной сети.

Создание Web-цепочек также может использоваться, когда производится настройка нижестоящих брандмауэров ISA на соединение с массивом Web-кэширования. Массивы Web-кэширования имеются в промышленной версии брандмауэра ISA. На рис. 4.60 показано, как можно настроить массив Web-кэширования для организации.

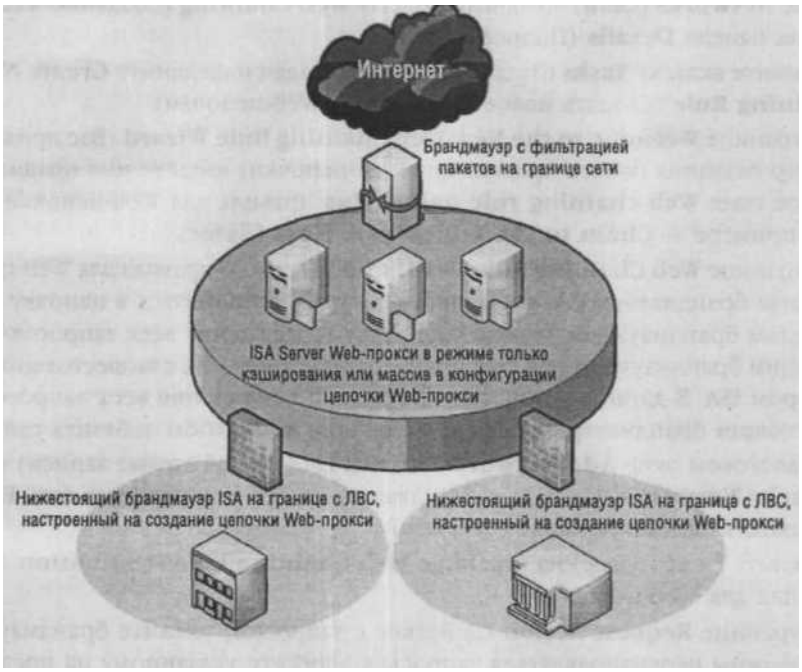


Рис. 4.60. Настройка массива Web-кэширования для организации

В этом примере нижестоящие брандмауэры ISA настроены в конфигурации создания Web-цепочек с массивом. Массив Web-кэширования предоставляет конфигурационную информацию для нижестоящих брандмауэров ISA, включая имена компьютеров, входящих в этот массив. Если один из членов массива по какой-либо причине перейдет в автономный режим, нижестоящие брандмауэры ISA попытаются обратиться к другому члену массива, который находится в оперативном режиме. Кроме того, когда член массива переходит в автономный режим, в массиве появляется информация о том, что этот член массива недоступен, и автономный компьютер исключается из массива. Остальные члены массива информируют нижестоящие брандмауэры ISA отделов о том, какие компьютеры в массиве находятся в оперативном режиме. Благодаря этому нижестоящие брандмауэры ISA не пытаются установить соединение с членом массива, находящимся в автономном режиме.

Настройка создания цепочек Web-прокси производится на вкладке **Web Chaining** (Создание Web-цепочки) в узле **Network** (Сеть). 1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Настройка).

Щелкните узел **Networks** (Сети).

2. В узле **Networks** (Сети) щелкните вкладку **Web Chaining** (Создание Web-цепочки) на панели **Details** (Подробности).
3. Щелкните вкладку **Tasks** (Задачи) на панели задач и щелкните **Create New Web Chaining Rule** (Создать новое правило для Web-цепочки).
4. На странице **Welcome to the New Web Chaining Rule Wizard** (Вас приветствует мастер создания нового правила для Web-цепочки) введите имя правила в текстовое поле **Web chaining rule name** (Имя правила для Web-цепочки), в данном примере — **Chain to ISA-1.** Щелкните **Next** (Далее).
5. На странице **Web Chaining Rule Destination** (Адресат правила для Web-цепочки) укажите брандмауэру ISA, что запросы должны соединяться в цепочку с выше стоящим брандмауэром. Можно установить соединение всех запросов с выше стоящим брандмауэром или соединение конкретных URL с вышестоящим брандмауэром ISA. В данном примере установлено соединение всех запросов с вышестоящим брандмауэром. Щелкните кнопку **Add,** чтобы добавить сайты.
6. В диалоговом окне **Add Network Entities** (Добавить сетевые записи) щелкните папку **Networks** (Сети), а затем дважды щелкните внешнюю сеть **External** (Внешняя). Щелкните **Close** (Закрыть).
7. Щелкните **Next** (Далее) на странице **Web Chaining Rule Destination** (Адресат правила для Web-цепочки).
8. На странице **Request Action** (Действие с запросом) укажите брандмауэру ISA, как должны перенаправляться запросы к адресату, указанному на предыдущей странице. Имеется несколько вариантов.
   - **Retrieve requests directly from the specified location** (Принимать запросы непосредственно с указанного адреса). Этот вариант настраивает брандмауэр ISA на отправку запросов к адресату, указанному на последней странице, напрямую на указанный сервер, а не на вышестоящий брандмауэр ISA. Это означает, что если брандмауэр ISA настроен на установку соединения с Интернетом способом, отличным от цепочки Web-прокси, то брандмауэр ISA будет перенаправлять это соединение по этому каналу. Если у брандмауэра ISA нет другого доступа к Интернету, кроме цепочки Web-прокси, то соединение не будет выполнено. Этот вариант представляет собой действия брандмауэра ISA по умолчанию, заключающиеся в том, чтобы не использовать цепочку Web-прокси, а вместо этого отправлять соединение на Интернет-сайт, к которому был сделан запрос.
   - **Redirect requests to a specified upstream server** (Перенаправлять запросы на указанный вышестоящий сервер). Этот вариант перенаправляет запросы на вышестоящий сервер Web-прокси. Этот вариант позволяет создать цепочку Web-прокси между этим сервером и вышестоящим брандмауэром ISA. Вариант **Allow delegation of basic authentication credentials** (Разрешить передачу верительных данных базовой проверки подлинности) выглядит загадочной. Какие верительные данные? Для каких адресатов? От кого защи-

щает проверка подлинности? Проверка подлинности производится для Web-сайта? Для вышестоящего Web-прокси? Для всех вышеперечисленных? Ни для кого из них? В данный момент невозможно с определенностью сказать, зачем нужен этот вариант. Возможно, он используется, когда цепочка Web-прокси создается при получении доступа к внутренним Web-сайтам, но нет уверенности, что этот ответ верный. Когда появится информация о том, что же означает этот вариант, мы сообщим вам об этом.

- **Redirect requests to** (Перенаправлять запросы к). Этот вариант позволяет перенаправлять запросы сайта, указанного на предыдущей странице, к другому Web-сайту. Например, предположим, нужно перенаправить запрос к списку запрещенных Web-сайтов на конкретный сайт корпоративной сети. В таком случае можно выбрать этот вариант, а затем ввести IP-адрес или FQDN внутреннего сайта. Также следует указать порт HTTP и порт SSL
- Use automatic **dialup** (Использовать автоматический набор номера). Этот вариант позволяет использовать коммутируемое соединение для этого правила. Если внешний интерфейс является коммутируемым соединением, то выбор этого варианта позволяет применить коммутируемое соединение для установки соединения с адресатом, указанным на предыдущей странице. Также этот вариант используется, если на одном брандмауэре ISA имеется сетевая интерфейсная карта и коммутируемое соединение. Сетевая интерфейсная карта может применяться для обычного соединения с Интернетом, а коммутируемое соединение может использоваться для установки соединения с помощью цепочек.

На рис. 4.61 показана настройка действия *по* запросу.

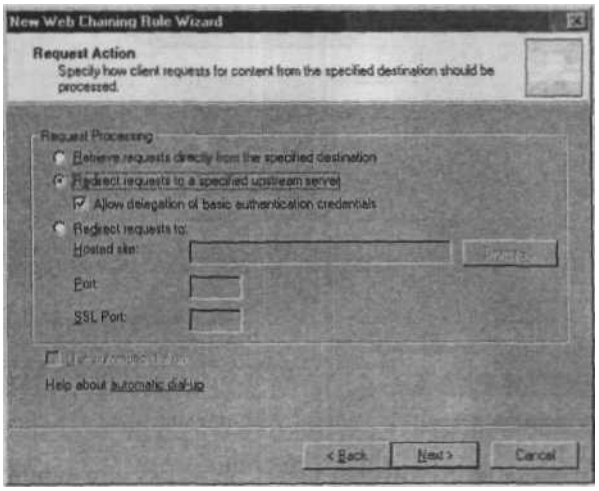


Рис. 4.61. Настройка действия с запросом

9. В данном примере использованы варианты **Redirect requests to a specified upstream server** (Перенаправлять запросы на указанный вышестоящий сервер) и **Disable the Allow delegation of basic authentication credentials** (Отклю чить разрешение передачи верительных данных базовой проверки подлиннос ти). Щелкните **Next** (Далее).
10. На странице **Primary Routing** (Первичная маршрутизация) введите IP-адрес или FQDN вышестоящего брандмауэра ISA Если введен FQDN, следует проверить, что нижестоящий брандмауэр ISA может разрешить это имя в правильный IP-адрес на вышестоящем брандмауэре ISA. Текстовые поля **Port** (Порт) и **SSL Port** (Порт SSL) содержат значения по умолчанию, которые работают со всеми остальны ми брандмауэрами ISA. Следует обратить внимание на то, что **SSL port** не ис пользуется для SSL-соединений с клиентов позади нижестоящего брандмауэра ISA в цепочке Web-прокси. SSL-соединения с клиентов позади нижестоящего бран дмауэра ISA туннелируются в соединение Web-прокси к порту TCP 8080 выше-стоящего брандмауэра ISA. Порт SSL используется, когда нужно обеспечить за щиту связи по цепочке Web-прокси между вышестоящим и нижестоящим бран дмауэром ISA с помощью протокола SSL. В этой книге недостаточно места, что бы подробно описывать этот тип конфигурации, но он будет описан в статье, которая вскоре появится на сайте www.isaserver.org.

На рис. 4.62 показана маршрутизация к вышестоящему Web-прокси.

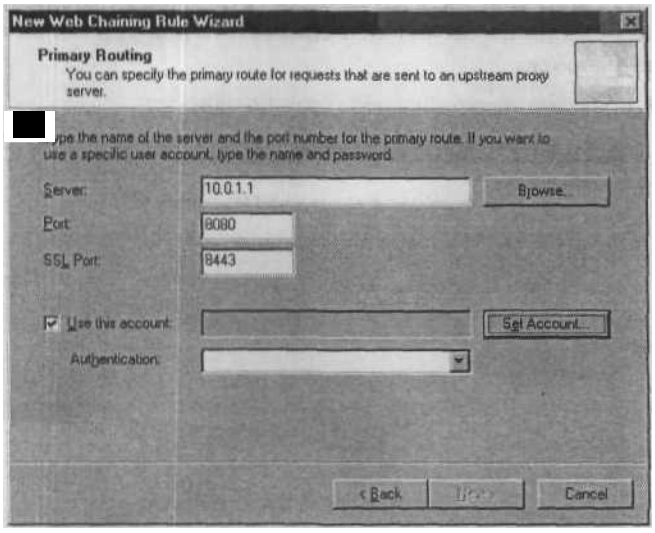


Рис. 4.62. Маршрутизация к вышестоящему Web-прокси

Настоятельно рекомендуется использовать проверку подлинности для вышесто-ящего Web-прокси. Когда на вышестоящем Web-прокси должна производиться проверка подлинности, нижестоящий Web-прокси должен отправлять верительные

данные на вышестоящий Web-прокси для получения доступа к Интернету. Можно настроить верительные данные для нижестоящего Web-прокси в цепочке Web-прокси, установив флажок в поле **Use this account** (Использовать эту учетную запись). Щелкните кнопку **Set Account** (Настроить учетную запись). В диалоговом окне **Set Account** (Настроить учетную запись) (рис. 4.63) введите имя пользователя в текстовое поле **User** (Пользователь) в формате COMPUTERNAME/Username (Имя компьютера/имя пользователя). Учетная запись пользователя настраивается в локальной базе данных пользователей вышестоящего брандмауэра ISA. Если вышестоящий брандмауэр ISA является членом домена, то можно использовать формат **DOMAINNAME/Username** (Имя домена/имя пользователя). Введите пароль и подтвердите пароль в текстовых полях **Password** (Пароль) и **Confirm password** (Подтвердить пароль). Щелкните ОК в диалоговом окне **Set Account** (Настроить учетную запись). В выпадающем списке **Authentication** (Проверка подлинности) выберите вариант **Integrated Windows.** Если создание цепочки Web-прокси настраивается для сервера Web-прокси брандмауэра стороннего производителя, то нужно использовать базовую проверку **подлинности.** Если используется базовая проверка подлинности, связь по цепочке Web-прокси должна устанавливаться с помощью протокола SSL, потому что базовые верительные данные пересылаются в виде открытого текста. Щелкните **Next** (Далее) на странице **Primary Routing** (Первичная маршрутизация). На рис. 4.63 показана настройка верительных данных.

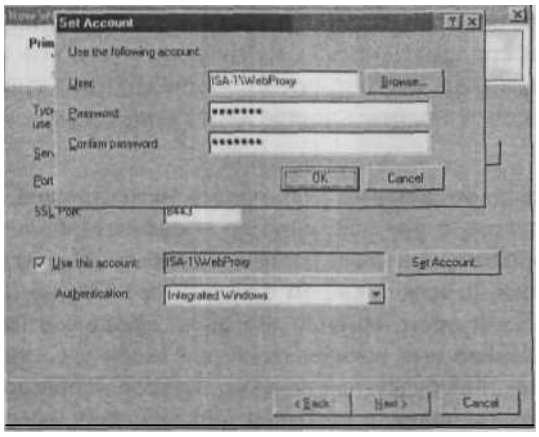


Рис. **4.63.** Настройка верительных данных

11. На странице **Backup Action** (Резервирование) имеется несколько вариантов.

- **D Ignore requests** (Игнорировать запросы). Если вышестоящий Web-прокси в цепочке Web-прокси недоступен, этот вариант удалит запрос, а клиент получит сообщение об ошибке, указывающее на то, что узел не доступен.
- □ **Retrieve requests directly from the specified location** (Получать запросы прямо с указанного адреса). Этот вариант позволяет нижестоящему бранд-

мауэру ISA в цепочке Web-прокси использовать другой метод, помимо цепочки Web-прокси, для установки соединения с Web-сайтом. Например, когда внешний интерфейс брандмауэра ISA может установить соединение с узлом адресата, не проходя через цепочку Web-прокси.

- **Route requests to an upstream server** (Направлять запросы на вышестоящий сервер). Этот вариант позволяет нижестоящему брандмауэру ISA в цепочке Web-прокси использовать другой брандмауэр ISA во второй цепочке Web-прокси. Этот вариант позволяет установить конфигурацию второй цепочки Web-прокси на нижестоящем брандмауэре ISA, которая используется, только когда первый вышестоящий брандмауэр ISA становится недоступным.
- **Use automatic dial-up** (Использовать автоматический набор номера). Этот вариант необходимо включить, если для установки соединения нижестоящего брандмауэра ISA с Интернетом используется коммутируемое соединение или необходимо, чтобы запросы к адресатам, заданным для этого правила, выполнялись по коммутируемому соединению, а не по первичному соединению брандмауэра ISA (т. е. через выделенную сетевую интерфейсную карту).

12. Выберите вариант **Ignore requests** (Игнорировать запросы) и щелкните **Next** (Далее) на странице **Backup Action** (Резервирование).
13. Щелкните **Finish** (Готово) на странице **Completing the New Web Chaining Rule Wizard** (Завершение работы мастера создания нового правила для Web-цепочки).

Теперь нижестоящий брандмауэр ISA настроен на создание цепочки Web-прокси с вышестоящим брандмауэром ISA. Не забудьте настроить правило доступа на вышестоящем брандмауэре ISA, которое позволит учетной записи, настроенной в правиле для Web-цепочки, получить доступ в Интернет с помощью протоколов HTTP, HTTPS и FTP.

СОВЕТ При создании цепочки Web-прокси нижестоящий брандмауэр ISA может быть настроен с учетной записью пользователя, которую он может использовать, если верительные данные, используемые клиентом для проверки подлинности на нижестоящем брандмауэре ISA, не принимаются вышестоящим брандмауэром. Именно это было сделано в предыдущем примере. В этом примере имя пользователя при входе в систему на вышестоящем брандмауэре ISA будет тем именем, которое использовалось для проверки подлинности в правиле создания цепочки Web-прокси. Однако если вышестоящий брандмауэр ISA может проверить подлинность пользователя, который инициировал начальное соединение, потому **что** вышестоящий брандмауэр принадлежит к тому же домену, что и клиент, и нижестоящий брандмауэр, или если у вышестоящего брандмауэра ISA это имя пользователя хранится в локальной памяти SAM **(Serial** Access Memory, память с последовательным доступом), то пользователь, создавший запрос, появится в журналах нижестоящего и вышестоящего брандмауэра ISA.

Создание цепочек брандмауэров как форма сетевой маршрутизации

Создание цепочек брандмауэров похоже на создание цепочек Web-прокси. При создании цепочек брандмауэров нижестоящий брандмауэр ISA настраивается как клиент брандмауэра для вышестоящего брандмауэра ISA. Преимущество конфигурации цепочки брандмауэров над конфигурацией цепочки Web-прокси состоит в том, что цепочка брандмауэров поддерживает все Winsock-протоколы TCP и UDP, а не только Web-протоколы (HTTP/HTTPS/FTP). Кроме того, цепочки Web-прокси поддерживают сложные протоколы, требующие вторичных соединений.

У нас не получилось настроить работу цепочки брандмауэров с брандмауэром ISA, поэтому данная конфигурация не рассматривается в этой книге подробно. Если эта функция будет исправлена в следующем служебном пакете или дополнении, то эта информация будет опубликована в виде подробного обучающего курса на сайте www.isaserver.org.

Настройка брандмауэра ISA в качестве DHCP-сервера

В некоторых организациях предпочитают использовать брандмауэр ISA в функции традиционного маршрутизатора класса SOHO, если брандмауэр ISA играет роль DHCP-сервера в корпоративной сети. Можно установить службу DHCP на брандмауэре ISA и создать правила доступа, позволяющие брандмауэру ISA предоставлять информацию об IP-адресации хостам в корпоративной сети.

Предположим, что DHCP-сервер уже установлен. Следующий шаг состоит в том, чтобы настроить брандмауэр ISA так, чтобы он разрешил передачу DHCP-запросов и DHCP-ответов с сообщениями, необходимыми для присваивания IP-адресов клиентам корпоративной сети.

Для того чтобы создать правило доступа для DHCP-запроса, выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем щелкните узел **Firewall Policy** (Политика брандмауэра). На панели задач щелкните вкладку **Tasks** (Задачи). Щелкните ссылку **Create a New Access Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите имя правила в текстовое поле **Access Rule** (Правило доступа), в данном случае — **DHCP Request.** Щелкните **Next** (Далее).
3. Выберите вариант **Allow** (Разрешающее) на странице **Rule Action** (Действие правила). Щелкните **Next** (Далее).

4. **На** странице **Protocols** (Протоколы) выберите вариант **Selected protocols** (К выбранным протоколам) из списка **This rule applies to** (Это правило при меняется). Щелкните **Add** (Добавить).
5. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Infrastructure** (Инфраструктура), а затем дважды щелкните запись **DHCP Request.** Щелкните **Close** (Закрыть).
6. Щелкните **Next** (Далее) на странице **Protocols** (Протоколы).
7. На странице **Access Rule Sources** (Источники правила доступа) щелкните **Add.**
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку Networks (Сети) и дважды щелкните запись **Internal** (Внутренние). Щелк ните **Close** (Закрыть).
9. Щелкните **Next** (Далее) на странице **Access Rule Sources** (Источники правила доступа).
10. На странице **Access Rule Destination** (Адресат правила доступа) щелкните **Add** (Добавить).
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Networks** (Сети) и дважды щелкните запись **Local Host** (Локальный хост). Щелкните **Close** (Закрыть).
12. На странице **Access Rule Destination** (Адресат правила доступа) щелкните Next (Далее).
13. На странице User **Sets** (Множества пользователей) щелкните **Next** (Далее).
14. На странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила) щелкните **Finish** (Завершить).
15. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
16. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

    Следующий шаг — создание нового правила доступа для DHCP-ответа.

17. Щелкните правой кнопкой мыши правило **DHCP Request** (DHCP-запрос) и щелкните Copy (Копировать). 18. Щелкните правой кнопкой мыши правило **DHCP Request** (DHCP-запрос) и

    щелкните **Paste** (Вставить). 19-Дважды щелкните правило **DHCP Request (1)** (DHCP-запрос, 1) и щелкните

    Properties (Свойства).

20. На вкладке **General** (Общие) правила **DHCP Request (1)** (DHCP-запрос, 1) пе реименуйте правило в **DHCP Reply** (DHCP-ответ) в текстовом поле **Name** (Имя).
21. Щелкните вкладку **Protocols** (Протоколы). Щелкните запись **DHCP (request)** (DHCP, запрос) и щелкните **Remove** (Удалить). Щелкните **Add** (Добавить). В диалоговом окне **Protocols** (Протоколы) щелкните папку **Infrastructure** (Ин фраструктура) и дважды щелкните запись **DHCP (reply)** (DHCP, ответ). Щелк ните **Close** (Закрыть).

22. Щелкните вкладку **From** (От). Щелкните запись **Internal** (Внутренний) и щелкните кнопку **Remove** (Удалить). Щелкните кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Networks** (Сети) и дважды щелкните запись **Local Host** (Локальный хост). Щелкните **Close** (Закрыть).
23. Щелкните вкладку To (К). Щелкните запись **Local Host** (Локальный хост) и щелкните **Remove** (Удалить). Щелкните **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните папку **Networks** (Сети) и дважды щелкните запись **Internal** (Внутренние). Щелкните **Close** (Закрыть).
24. Щелкните **Apply** (Применить), а затем щелкните ОК.
25. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
26. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

В такой конфигурации DHCP-сервер на брандмауэре ISA может предоставлять информацию об IP-адресации хостам во внутренней сети.

ПРЕДУПРЕЖДЕНИЕ DHCP-сервер также может предоставлять IP-адреса VPN-клиентам. Однако на брандмауэре ISA нельзя установить агента DHCP-ретранслятора и позволить VPN-клиентам пользоваться возможностями DHCP.

Резюме

В этой главе рассматривались возможности брандмауэра ISA по работе с сетями. Сначала обсуждалось место брандмауэра ISA в существующей в организации инфраструктуре брандмауэров. Затем рассматривались особенности смоделированной лабораторной сети, которая использовалась для демонстрации сценариев, представленных в этой книге. При этом были приведены подробные инструкции по настройке виртуальных машин VMware для поддержки брандмауэров ISA и других компьютеров в экспериментальной сети.

Затем рассматривалась концепция сети с точки зрения брандмауэра ISA. Подход нового брандмауэра ISA существенно отличается от подхода к внешним и внутренним сетям брандмауэра ISA Server 2000, при котором все внутренние сети считались надежными, а внешние ненадежными. Новый брандмауэр ISA не считает ни одну сеть надежной, а внутренняя сеть по умолчанию полностью отличается от понятия «внутренней» сети в предыдущей версии этого продукта. Также рассматривались все типы сетевых объектов брандмауэра ISA и типы сетевых шаблонов, которые можно использовать для упрощения задания сетевых настроек брандмауэра ISA.

Также рассматривались различные темы, связанные с наборами функциональных возможностей брандмауэра ISA по работе с сетями, включая создание цепочек Web-прокси, цепочек брандмауэров и использование брандмауэра ISA в качестве DHCP-сервера.

Краткое резюме по разделам

Сети с брандмауэром ISA и тактика защиты

И Традиционные брандмауэры являются простыми устройствам фильтрации с отслеживанием состояния соединений, иногда называемой «проверкой с отслеживанием соединений». Все современные брандмауэры выполняют фильтрацию с отслеживанием соединений.

0 В настоящее время атаки на сеть производятся на уровне приложения, и только брандмауэры, выполняющие проверку с отслеживанием соединений на уровне приложения, такие как брандмауэры ISA, способны обеспечить **защиту** от таких современных атак уровня приложения.

0 Простые брандмауэры с фильтрацией пакетов с отслеживанием соединений следует размещать на границе сети с Интернетом, если эффективная пропускная способность связи с Интернетом превышает скорость, с которой брандмауэр ISA с фильтрацией пакетов с отслеживанием соединений на уровне приложения может эффективно обрабатывать трафик (примерно 400 Мбит/с). Если Интернет-канал превышает ограничения пропускной способности брандмауэра ISA, то брандмауэры с фильтрацией пакетов с отслеживанием соединений следует размещать перед брандмауэром ISA с проверкой с отслеживанием соединений на уровне приложения, чтобы немного разгрузить первый брандмауэр.

й В любой сети существует несколько периметров защиты. Фильтрация с отслеживанием соединений и проверка с отслеживанием соединений на уровне приложения должны в идеале выполняться на каждом периметре.

0 Операционная система Windows может быть усилена в той степени, что она становится не более проницаемой, чем любой другой брандмауэр, включая аппаратные брандмауэры.

Э Поскольку брандмауэры ISA обеспечивают более высокий уровень защиты, чем аппаратные брандмауэры с фильтрацией пакетов с отслеживанием соединений, брандмауэры ISA следует размещать ближе к основным ресурсам сети.

План конфигурирования сети с ISA Server 2004 в концепции Тома и Деб Шиндеров

И Схема экспериментальной сети в этой главе предоставляет информацию, необходимую читателям для воспроизведения сетевой топологии, используемой в рассуждениях и примерах в этой книге.

0 В качестве тестовой среды использовалось программное обеспечение VMWare Workstation 4.51. Каждый сетевой идентификатор был присвоен отдельному виртуальному коммутатору VMNet, что позволило выделить широковещательный домен Ethernet для каждой сети так же, как это выполняется сетевым маршрутизатором.

0 Коробочная версия VMware 4.51 поддерживает только три сетевых адаптера для одной виртуальной машины. Благодаря методу, предложенному Александром Перилли (Alessandro Perilli), на виртуальной машине VMware можно установить четыре сетевых интерфейсных карты.

Определение сетей и отношений между ними с точки зрения брандмауэров ISA

0 В брандмауэре ISA не используются применявшиеся ранее таблицы LAT, когда внутренние сети считались надежными, а внешние — ненадежными. Новый брандмауэр ISA выполняет фильтрацию с отслеживанием соединений и проверку с отслеживанием соединений на уровне приложения на всех интерфейсах, включая VPN-интерфейсы.

И Термин «multi network ing» (работа с несколькими сетями) определяет подход брандмауэра ISA к сетям. Сети определяются на основании их расположения за конкретной сетевой интерфейсной картой, установленной на брандмауэре ISA, и между этими сетями заданы отношения маршрутизации.

И Взаимодействие между любыми двумя хостами в сети никогда не должно замыкаться через брандмауэр ISA. Хосты, расположенные в одной сети, должны всегда напрямую взаимодействовать друг с другом.

И Брандмауэр ISA содержит пять сетей по умолчанию: сеть локального хоста, внутреннюю сеть, внешнюю сеть, сеть VPN-клиентов и сеть изолированных VPN-клиентов.

0 Сеть локального хоста включает все адреса, связанные с брандмауэром ISA.

0 Внутренняя сеть включает все адреса, расположенные за сетевой интерфейсной картой, которая определяется как внутренняя сеть по умолчанию при установке программного обеспечения брандмауэра ISA.

El Внешняя сеть по умолчанию включает все адреса, которые не определены как часть сети на брандмауэре ISA.

0 Сеть VPN-клиентов включает все адреса, которые используются VPN-клиентами и шлюзами в любой момент времени.

0 Сеть изолированных VPN-клиентов включает все адреса VPN-клиентов и шлюзов, которые в текущий момент изолированы.

0 Можно создавать собственные внутренние сети, сети периметра, VPN-сети «узел-в-узел» и внешние сети.

0 Все взаимодействия между сетями определяются сетевыми правилами, задающими отношение маршрутизации между сетью источника и адресата. Между любыми двумя сетями могут быть отношения типа «маршрут» или отношения NAT.

0 Отношение типа «маршрут» является двунаправленным, исходный IP-адрес взаимодействующих хостов всегда сохраняется.

0 Отношение NAT является однонаправленным, исходный IP-адрес хоста всегда заменяется на первичный IP-адрес интерфейса, который покидают соединения в сети.

S3 Брандмауэр ISA поддерживает девять типов сетевых объектов: сети, подмножества сетей, компьютеры, диапазоны адресов, подсети, подмножества компьютеров, подмножества URL, подмножества имен доменов и Web-приемники. Каждый из сетевых объектов может контролировать источник и адресат любого соединения, устанавливаемого через брандмауэр ISA.

0 Коробочная версия брандмауэра ISA включает пять сетевых шаблонов: граничный брандмауэр, внешний брандмауэр, внутренний брандмауэр, брандмауэр с тремя сетевыми интерфейсами и брандмауэр с одним сетевым интерфейсом в режиме только Web-кэши ров а ни я (шаблон с одной сетевой интерфейсной картой).

0 Шаблон брандмауэра с одним сетевым интерфейсом в режиме только Web-кэширования необычен, поскольку все адреса включаются как часть его внутренней сети по умолчанию. Это означает, что внешних адресов не существует, а все адреса источника и адресата в правилах доступа должны быть из внутренней сети.

0 Брандмауэр ISA поддерживает коммутируемые соединения с Интернетом. Автоматический набор номера не всегда возможен для VPN-подключений, используемых для установления связи с Интернетом.

0 Брандмауэр ISA поддерживает динамическое присваивание адреса на своем внешнем интерфейсе. Однако для поддержки динамического присваивания адресов нужно настроить системную политику брандмауэра ISA.

0 Сценарий «сеть в Сети» представляет собой случай, когда несколько идентификаторов сети расположены за одной сетевой интерфейсной картой брандмауэра ISA. Все адреса, расположенные за конкретной сетевой интерфейсной картой брандмауэра ISA, являются частью одной сети, а брандмауэр ISA должен быть настроен с помощью записей в таблице маршрутизации, которые указывают правильный шлюз для каждого идентификатора сети, расположенного за этим интерфейсом.

Создание цепочек Web-прокси как форма сетевой маршрутизации

0 Создание цепочек Web-прокси позволяет соединять между собой серверы Web-прокси брандмауэра ISA для передачи запросов в Интернет. .

0 Вышестоящие серверы Web-прокси находятся ближе *к* интернет-каналу, а нижестоящие серверы Web-прокси находятся дальше от интернет-канала.

И Иногда цепочки Web-прокси называют Web-маршрутизацией, потому что создание цепочек Web-прокси можно настроить для одних запросов, а для других нельзя.

0 Создание цепочек Web-прокси позволяет сэкономить пропускную способность на канале связи с Интернетом и на любых каналах связи между вышестоящими и нижестоящими Web-прокси в цепочке Web-прокси.

Создание цепочек брандмауэров как форма сетевой маршрутизации

И Создание цепочек брандмауэров позволяет объединять брандмауэры ISA так, чтобы нижестоящий брандмауэр ISA выполнял функцию клиента Web-прокси для вышестоящего брандмауэра ISA. К сожалению, в данный момент эта функция, по-видимому, не работает.

Настройка брандмауэра ISA в качестве DHCP-сервера

И Брандмауэр ISA можно настроить как DHCP-сервер корпоративной сети.

0 DHCP-сервер на брандмауэре ISA может предоставлять возможности DHCP для DHCP-клиентов корпоративной сети.

0 DHCP-сервер брандмауэра ISA может предоставлять IP-адреса VPN-клиентам и шлюзам, но он не может предоставить возможности DHCP VPN-клиентам и шлюзам. Однако если разместить в корпоративной сети DHCP-сервер и настроить агент DHCP-ретранслятора на брандмауэре ISA, то VPN-клиентам можно предоставить DHCP-возможности.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом **www.syngress.com/solutions** (форма **«Ask the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Клиенты корпоративной сети могут установить соединение со всеми Web-сайтами, кроме Web-сайтов, управление которыми выполняется во внутренней сети. Почему?

О: Наиболее вероятной причиной является то, что клиенты корпоративной сети пытаются получить доступ к этим Web-сайтам через брандмауэр ISA. Это можно исправить: для этого нужно настроить клиенты Web-прокси и клиенты брандмауэра на использование прямого доступа к внутренним IP-адресам и доменам и настроить расщепленную структуру DNS так, чтобы хосты внутренней сети разрешали имена внутренних ресурсов в их внутренние IP-адреса.

В: На брандмауэре ISA имеются два интерфейса: один интерфейс соединяется с Интернетом, а другой интерфейс соединяется с корпоративной сетью. Также имеются пять идентификаторов сети под управлением маршрутизатора корпоративной сети. Для тех идентификаторов сети, которые не были покрыты внутренней сетью по умолчанию, было создано пять внутренних сетей. Теперь бранд-

мауэр ISA выдает сообщения об ошибках, в которых говорится, что эти внутренние сети недоступны с внутреннего сетевого интерфейса. Почему? О: Все IP-адреса за отдельной сетевой интерфейсной картой на брандмауэре ISA считаются частью той же сети. С точки зрения брандмауэра ISA взаимодействие между различными сетями должно осуществляться через брандмауэр ISA. Любое взаимодействие, осуществляемое между двумя хостами напрямую, происходит в пределах одной сети. Поэтому несмотря на то, что имеется несколько идентификаторов сети, расположенных на одном сетевом интерфейсе брандмауэра ISA, брандмауэр ISA рассматривает их как одну сеть, потому что брандмауэр ISA не обрабатывает соединения между двумя хостами, расположенными за одной сетевой интерфейсной картой брандмауэра ISA. Этим объясняется то, что не следует замыкать соединения между двумя хостами в одной сети через брандмауэр ISA.

В: Имеется брандмауэр ISA с одной сетевой интерфейсной картой и на нем был запущен сетевой шаблон для одной сетевой интерфейсной карты. Были созданы правила доступа, которые разрешают взаимодействие из внутренней сети с внешней, но эти правила доступа не работают. В чем здесь проблема?

О: Проблема в том, что когда вы запускаете сетевой шаблон для одной сетевой интерфейсной карты на брандмауэре ISA, внутренняя сеть изменяется и все адреса в диапазоне IPv4 включаются в определение внутренней сети (за исключением сетевого идентификатора обратной связи). Все правила доступа, созданные на брандмауэре ISA с одним сетевым интерфейсом, на котором был запущен сетевой шаблон для одной сетевой интерфейсной карты, должны включать в качестве адресов источника и назначения адреса внутренней сети или же можно использовать другие сетевые объекты для представления источника и адресата.

В: На брандмауэре ISA был установлен DHCP-сер вер, а также агент DHCP-ретранслятора. Попытки использовать агент DHCP-ретранслятора для того, чтобы предоставить возможности DHCP VPN-клиентам, ни к чему не приводят. Почему?

О: Когда DHCP-сервер установлен на брандмауэре ISA, невозможно предоставить возможности DHCP VPN-клиентам даже после установки агента DHCP-ретранслятора. Однако если установить DHCP-сервер в корпоративной сети и настроить агент DHCP-ретранслятора на брандмауэре ISA, то можно будет предоставить VPN-клиентам возможности DHCP.

В: На внешнем интерфейсе брандмауэра ISA использовался адрес, присвоенный DHCP. Этот адрес был получен до установки программного обеспечения брандмауэра ISA. Теперь этот адрес не работает. Что нужно сделать, чтобы опять получить адрес, присвоенный DHCP?

О: Нужно изменить системную политику на брандмауэре ISA так, чтобы она принимала DHCP-ответы или от внешней сети по умолчанию, или, что лучше, с конкретного IP-адреса DHCP-сервера интернет-провайдера.

Глава

Типы клиентов ISA Server 2004 и автоматизация настройки клиентов

Основные темы главы:

Типы клиентов ISA Server 2004

Автоматизация инициализации клиента ISA Server 2004

Автоматизация установки клиента брандмауэра

Один из наиболее важных и сложных для понимания вопросов, связанных с установкой и управлением брандмауэрами ISA Server 2004, — типы клиентов ISA Server 2004. Некоторые из этих типов клиентов имеют классические клиент-серверные отношения с ISA Server: клиент выполняет запрос данных с сервера, сервер затем выполняет работу по извлечению этих данных и возвращает их клиенту. Клиент-серверные отношения зависят от программного обеспечения клиента, установленного на клиентском компьютере и позволяющего осуществлять взаимодействие с конкретными службами на сервере.

В случае с ISA Server клиент может запросить данные в форме Web-страницы из Интернета, ISA Server выполнит работу по извлечению этой Web-страницы и доставке ее клиенту. Однако не все клиенты ISA Server 2004 имеют классические клиент-серверные отношения с брандмауэром, каждый тип клиента получает доступ к внешним сетям по-разному. Очень важно определить тип клиента ISA Server 2004 до *того,* как будет установлен и настроен ISA Server 2004. Неправильно выбранный тип клиента ISA Server 2004 может привести к впечатлению о некорректной работе брандмауэра.

Все компьютеры, устанавливающие соединение с ресурсами через брандмауэр ISA Server 2004, рассматриваются в качестве клиентов компьютера брандмауэра ISA Server 2004. Это не означает, что на всех компьютерах должно быть установлено программное обеспечение клиента или что их приложения должны быть настроены на установку прямого соединения с компьютером брандмауэра ISA Server 2004. Что касается ISA Server 2004, «клиент» не всегда участвует в классических «клиент-серверных» отношениях с брандмауэром ISA Server 2004.

Типы клиентов ISA Server 2004

Компьютеры, имеющие доступ к внешним сетям через ISA Server, относятся к одной или нескольким категориям в зависимости от типа клиента ISA Server 2004:

- ШКЯТ SecureNAT;
- клиент брандмауэра;
- клиент Web-прокси.

Отдельный компьютер может быть настроен так, чтобы играть роль различных типов клиента ISA Server 2004. Например, компьютер на базе Windows XP можно настроить в качестве клиента SecureNAT, клиента брандмауэра и клиента Web-прокси. Другой компьютер можно настроить как клиент SecureNAT и клиент Web-прокси.

В табл. 5.1 приводится обзор типов клиента ISA Server 2004 и указывается, как производится установка или конфигурирование каждого из них, какие операционные системы и протоколы они поддерживают, типы проверки подлинности пользователей и особые указания по применению для каждого типа.

Табл. 5.1. Обзор типов клиента ISA Server 2004

Параметр	**Клиент SecureNAT**	**Клиент брандмауэра**	**Клиент Web-прокси**
Нужно ли устанавливать программное обеспечение клиента?	Нет. Для клиентов SecureNAT требуется только указать адрес основного шлюза, который может перенаправлять запросы в Интернет через брандмауэр ISA Server 2004. Основной шлюз устанавливается в свойствах TCP/IP сетевого адаптера компьютера	Да. Программное обеспечение клиента брандмауэра должно быть установлено с совместно используемого инсталляционного ресурса для установки в сети. Этот инсталляционный ресурс может находиться на самом брандмауэре ISA Server 2004 или (что предпочтител ь но) на файловом сервере в другом месте сети	Нет. Однако Web-браузеры на клиентских компьютерах должны быть настроены на использование брандмауэра ISA Server 2004 в качестве своего Web-про кс и. Прокси устанавливается в настройках соединения Web-браузера
Поддержка операционной системы	Клиент SecureNAT поддержи вает все операционные системы. Этот тип клиента может использоваться с ОС Windows, MacOS, Unix, Linux и любыми другими операционными системами, которые поддерживают использование в сети протокола TCP/IP	Клиент брандмауэра поддерживает все платформы Windows, начиная *с* Windows 98 и заканчивая Windows Server 2003	Клиент Web-прокси поддерживает все платформы, но делает это с помощью Web-приложений. Все Web-браузеры, которые можно настроить на использование прокси-сервера, могут выступать в роли клиентов Web-прокси
Поддержка протоколов	Клиент SecureNAT поддерживает все простые протоколы. Сложные протоколы (требующие нескольких подключений) требуют установки фильтра приложения на компьютере брандмауэра ISA Server 2004	Клиент брандмауэра поддерживает все приложения на базе Wins oc k, которые используют протоколы TCP и UDP. Другие протоколы, отличные от TCP и UDP, клиент брандмауэра не поддерживает	Клиент Web-прокси поддерживает протоколы HTTP, HTTPS (SSL/TLS) и FTP по HTTP-туннелю (FTP с прокси)

(см. след. стр.)

Табл. 5.1. (окончание)

Параметр	Клиент SecureNAT	Клиент брандмауэра	Клиент Web-прокси
Поддержка проверки подлинности на уровне пользователя	Нет. Клиенты SecureNAT могут проверять подлинность на брандмауэре ISA Server 2004 только в случае, если приложения клиента поддерживают SOCKS 5, а фильтр приложения SOCKS 5 установлен на брандмауэре	Да. Клиент брандмауэра позволяет осуществлять жесткий контроль пользовательского/группового доступа, открыто передавая верительные данные клиента на брандмауэр ISA Server 2004	Да. Клиенты Web-прокси выполняют проверку подлинности на брандмауэре ISA Server 2004, если брандмауэр запрашивает верительные данные. Если у клиента Web-прокси имеется анонимное правило доступа, разрешающее соединение, то верительные данные не отправляются
Реализация	Все операционные системы, кроме Windows, можно настроить в качестве клиента Secure NAT, если им требуется доступ по протоколам помимо HTTP/HTTPS и FTP. Все операционные системы Windows, начиная с Windows 95, должны быть по возможности настроены как клиенты брандмауэра. Все серверы, опубликованные с помощью правил публикации серверов, должны быть настроены как клиенты SecureNAT. Клиент SecureNAT следует использовать на базе ОС Windows, только когда требуется исходящий доступ по протоколам ICMP или PPTP	На все операционные системы Windows, которые поддерживают установку клиента брандмауэра (версии после Windows 95), следует устанавливать клиент брандмауэра за исключением тех случаев, когда имеются технические или другие препятствия к этому. Клиент брандмауэра повышает общий уровень безопасности и доступности всех компьютеров, на которых он установлен	Все браузеры следует настраивать как клиенты Web-прокси с обязательной проверкой подлинности для Web-доступа по протоколам HTTP, HTTPS, FTP. Если проверка подлинности пользователя не требуется, то конфигурация Web-прокси также не нужна, потому что брандмауэр ISA Server 2004 обеспечит прозрачную функциональность Web-прокси для клиентов брандмауэра и Secure NAT

Клиент SecureNAT ISA Server 2004

В качестве клиента SecureNAT может рассматриваться любое устройство, настроенное с адресом основного шлюза, который может перенаправлять все адресованные в Интернет запросы через брандмауэр ISA Server 2004. То есть роль ISA Server тесно связана с ролью маршрутизатора для исходящего доступа. Клиент SecureNAT

не имеет традиционного клиент-серверного отношения с ISA Server. Чаще всего клиент SecureNAT встречается в трех типах сетей:

- в простой сети;
- в сложной сети;
- в сети VPN-клиентов.

Простая сеть означает, что за компьютером с брандмауэром ISA Server 2004 расположена только одна подсеть. Например, брандмауэр ISA Server 2004 расположен на границе сети: один его интерфейс напрямую соединен с Интернетом, а второй — с внутренней сетью. Все компьютеры позади брандмауэра ISA Server 2004 расположены в одной подсети (например, 10.0.0.0/8). Во внутренней сети маршрутизаторов нет. На рис. 5.1 представлена типичная простая сеть.

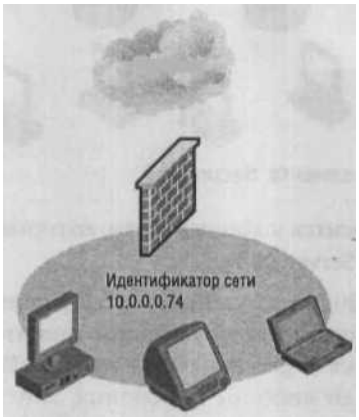


Рис. 5.1. Простая сеть для клиента SecureNAT

В такой простой сети основной шлюз клиентов SecureNAT настроен как IP-адрес внутреннего интерфейса брандмауэра ISA. Адрес основного шлюза можно настроить вручную или воспользоваться DHCP, чтобы автоматически присвоить адреса клиентам SecureNAT. DHCP-сервер может быть расположен на самом брандмауэре ISA Server 2004 или на отдельном компьютере во внутренней сети.

Сложная сеть предполагает, что внутренняя сеть состоит из нескольких идентификаторов сети, которыми управляет маршрутизатор или серия маршрутизаторов или коммутаторов уровня 3. В сложных сетях адрес основного шлюза, присвоенный каждому клиенту SecureNAT, зависит от расположения компьютера клиента SecureNAT. Адрес шлюза для клиента SecureNAT представляет собой адрес маршрутизатора, который позволяет клиенту SecureNAT получать доступ к другим сетям организации, а также к Интернету. Инфраструктура маршрутизации должна быть настроена так, чтобы обеспечивать поддержку клиента SecureNAT для того, чтобы запросы, направленные в Интернет, передавались на внутренний интерфейс брандмауэра ISA Server 2004. На рис. 5.2 показана сложная сеть для клиента SecureNAT.

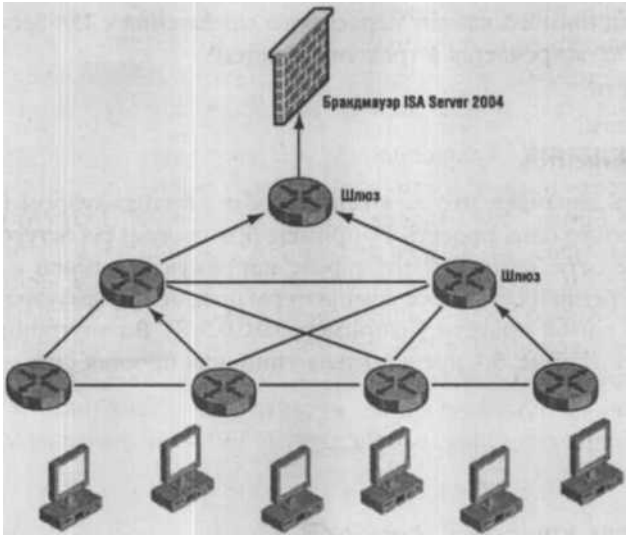


Рис. 5.2. Сложная сеть для клиента SecureNAT

Сеть VPN-клиентов относится к компьютерам, которые установили VPN-подключение с брандмауэром ISA Server 2004.

В случае с ISA Server 2000, когда компьютер VPN-клиента устанавливает соединение с VPN-сервером, таблица маршрутизации клиента меняется так, что адрес основного шлюза становится адресом на VPN-сервере. Если в конфигурацию клиента по умолчанию не были внесены изменения, клиент не сможет установить соединение с ресурсами в Интернете, хотя у него установлено соединение с VPN-сервером ISA Server 2000. Можно было настроить VPN-клиент ISA Server 2000 как клиент брандмауэра или клиент Web-прокси и разрешить VPN-клиенту доступ в Интернет через брандмауэр ISA Server 2000. Или же VPN-клиент ISA Server 2000 можно было настроить так, чтобы разрешить расщепленное туннелирование (split tunneling). Любой из этих методов позволяет клиенту одновременно устанавливать соединение с Интернетом и внутренними ресурсами через VPN-сервер.

В отличие от ISA Server 2000, VPN-клиент ISA Server 2004 не предполагает обязательную настройку VPN-клиентов в качестве клиентов брандмауэра или Web-прокси для того, чтобы получить доступ в Интернет через тот VPN-сервер ISA Server 2004, с которым они соединены. Поскольку VPN-клиенты не настроены как клиенты Web-прокси или брандмауэра, они фактически являются клиентами SecureNAT. Это позволяет пользователям VPN получать доступ к корпоративной сети через VPN-подключения и доступ в Интернет через соединение с брандмауэром ISA, а также исключает риск, скрытый в расщепленном туннели ровании.

Обратите внимание, что не обязательно разбираться в настройке таблицы маршрутизации VPN-клиента или в том, как различные версии VPN-клиента Windows

определяют маршрут по умолчанию. Нужно лишь помнить, что, когда VPN-клиент создает VPN-подключение с брандмауэром ISA Server 2004/VPN-сервером, этот клиент может установить соединение с Интернетом через брандмауэр ISA Server 2004, основываясь на правилах доступа, настроенных администратором.

> ПРЕДУПРЕЖДЕНИЕ Расщепленное туннелирование представляет собой серьезную угрозу безопасности, и его никогда не следует включать на VPN-клиентах. ISA Server 2004 поддерживает соединения VPN-клиента SecureNAT с Интернетом через тот же брандмауэр ISA Server 2004, с которым они соединены, и таким образом исключает необходимость в расщепленном туннелировании. Кроме того, брандмауэр ISA Server 2004 расширяет поддержку клиентом SecureNAT VPN-клиентов и позволяет осуществлять пользовательский/групповой контроль доступа для VPN-клиентов. Более подробно расщепленное туннелирование и связанный с ним риск, а также расширенная поддержка клиентами SecureNAT VPN-клиентов рассматриваются в главе 8.

Ограниченность клиента SecureNAT

Хотя настройка клиентов SecureNAT является самой простой по сравнению с другими типами клиента ISA Server 2004, этот тип клиента наименее безопасный и наименее мощный из трех основных типов клиента ISA Server 2004. Ограниченность клиента SecureNAT проявляется в следующем:

- неспособность проверять подлинность на брандмауэре для осуществления же сткого пользовательского/группового доступа;
- неспособность применять сложные протоколы без помощи фильтров приложения;
- зависимость от маршрутной инфраструктуры при получении доступа в Интер нет;
- обязательная настройка определения протокола на брандмауэре ISA Server 2004 для поддержки соединения.

Клиенты SecureNAT не отправляют верительные данные на брандмауэр ISA Server 2004, так как для этого должен существовать программный компонент клиента, который выполнит отправку. Базовый комплект протоколов TCP/IP не обеспечивает проверку подлинности пользователя и требует компонент приложения для отправки верительных данных пользователя. Поэтому клиенты брандмауэра и Web-прокси могут отправлять верительные данные клиентов, а клиент SecureNAT не может. Клиент брандмауэра использует программное обеспечение клиента брандмауэра для отправки верительных данных пользователя, а Web-браузер, настроенный на использование брандмауэра ISA Server 2004 в качестве Web-прокси, имеет встроенную способность отправлять верительные данные пользователя. Это означает, что на компьютерах, настроенных только как клиенты SecureNAT, невозможно осуществить жесткий контроль пользовательского/группового исходящего доступа.

Клиенты SecureNAT не могут устанавливать соединение с Интернетом (или любым другим объектом через брандмауэр ISA Server 2004) с помощью сложных протоколов без помощи фильтров приложения, установленных на ISA Server. Сложный протокол — это протокол, требующий несколько первичных или вторичных соединений. Классическим примером сложного протокола являются соединения по протоколу FTP в стандартном режиме.

Когда клиент FTP в стандартном режиме устанавливает соединение с FTP-сервером, начальное соединение («контрольный канал», control channel) устанавливается на порт TCP 20. Клиент FTP и FTP-сервер затем согласуют номер порта, на котором клиент FTP может получить данные (файл для скачивания) и FTP-сервер возвращает данные со своего порта TCP 21 на согласованный порт. Это входящее соединение является запросом на новое первичное соединение, а не ответом на первичное исходящее соединение, выполненное клиентом FTP.

Брандмауэр должен быть осведомлен обо всех соединениях между клиентом FTP в стандартном режиме и FTP-сервером так, чтобы для нового запроса на входящее соединение к брандмауэру ISA Server 2004 имелись подходящие порты. На брандмауэре ISA Server 2004 это выполняется с помощью интеллектуального фильтра приложения FTP-доступа (FTP Access Application Filter). На рис. 5.3 показано взаимодействие клиента FTP в стандартном режиме и FTP-сервера.

Рис. 5.3. Взаимодействие клиента FTP в стандартном режиме и FTP-сервера

Это ограничение применения сложных протоколов особенно важно, когда речь заходит об интернет-играх и аудио-, видеоприложениях, требующих нескольких входящих/исходящих соединений. Клиент SecureNAT не способен использовать эти приложения. Это становится возможным, только если на брандмауэре имеются специальные фильтры приложений, которые их поддерживают. Напротив, клиент брандмауэра с легкостью работает с приложениями, которые требуют нескольких входящих и исходящих первичных подключений, при этом на брандмауэре не требуется ничего устанавливать дополнительно.

Конечно, из каждого правила есть исключения, то же можно сказать о приведенном ранее утверждении. Клиенты SecureNAT могут поддерживать сложные протоколы, *если* установленное на клиенте SecureNAT приложение рассчитано на работу с прокси SOCKS 4. В данном случае это приложение рассчитано на работу со

службой SOCKS 4 брандмауэра ISA Server 2004. Служба SOCKS 4 может управлять соединениями от имени приложения компьютера клиента SecureNAT.

> ПРЕДУПРЕЖДЕНИЕ Хотя клиенты SecureNAT, работающие с приложениями SOCKS 4, способны поддерживать сложные протоколы для приложения, настроенного на применение SOCKS-прокси, SOCKS-прокси не позволяет клиенту воспользоваться возможностями пользовательской/групповой проверки подлинности. Фильтр приложения прокси SOCKS 4 на брандмауэре ISA Server 2004 не принимает верительные данные пользователя, что позволило бы выполнять пользовательский/групповой контроль доступа.

Клиент SecureNAT зависит от маршрутной инфраструктуры организации. В отличие от клиента брандмауэра и клиента Web-прокси, которые отправляют свои запросы на соединение с Интернетом напрямую на брандмауэр ISA Server 2004 (таким образом, им нужно знать лишь маршрут к внутреннему интерфейсу компьютера брандмауэра ISA Server 2004), клиент SecureNAT зависит от маршрутной инфраструктуры для передачи запросов в Интернет на внутренний интерфейс брандмауэра ISA Server 2004. Если на пути соединения встретится маршрутизатор, который не направляет соединения с Интернетом через брандмауэр ISA Server 2004, то попытка соединения не будет успешной.

> СОВЕТ Для каждого протокола, к которому нужно обеспечить доступ клиента SecureNAT, должно быть создано определение протокола на брандмауэре ISA Server 2004. Это необходимо сделать, даже если настроено правило доступа, разрешающее клиенту SecureNAT доступ ко всем протоколам. Для клиента SecureNAT «все протоколы» означает все протоколы, для которых имеются определения протоколов. Этим он отличается от клиента брандмауэра, для которого правило доступа, относящееся ко всем протоколам, означает все протоколы TCP и UDP независимо от того, имеется ли определение протокола для конкретного протокола (включая другие протоколы типа ICMP и протоколы уровня IP).

Из-за ограниченности клиентов SecureNAT компьютер должен быть настроен только как клиент SecureNAT, если существует хотя бы одно из приведенных далее условий:

- Компьютер не поддерживает программное обеспечение клиента брандмауэра и требует поддержки протоколов, которые не поддержи ваются клиентом Web-прокси (протоколы, отличные от HTTP/HTTPS и FTP).
- Компьютеру необходим исходящий доступ к ICMP и PPTP.
- По причинам, связанным с администрированием и политиками, нельзя устано вить клиента брандмауэра на компьютерах, на которых необходим доступ к протоколам, не поддерживаемый конфигурацией клиента Web-прокси.

Недостатки конфигурации SecureNAT представлены в табл. 5.2.

Табл. 5.2. Недостатки конфигурации клиента SecureNAT

Недостаток	Следствие
Неспособность выполнять проверку подлинности на брандмауэре ISA Server 2004	Клиент SecureNAT не способен отправлять верительные данные пользователя (имя пользователя и пароль) на брандмауэр ISA Server 2004. Это не позволяет осуществлять жесткий контроль пользовательского /группового исходящего доступа к Интернету. Единственный тип контроля исходящего доступа, имеющийся для клиентов SecureNAT, основан на исходном IP-адресе клиента
Неспособность использовать сложные протоколы	Сложные протоколы требуют несколько первичных и/или вторичных соединений. Интернет-игры, аудио-, видеоприложения и приложения обмена сообщениями часто требуют поддержки сложных протоколов. Клиент SecureNAT не может получить доступ к интернет-приложениям с помощью сложных протоколов без помощи фильтра приложения, установленного на компьютере брандмауэра ISA Server 2004. Единственное исключение — приложение, установленное на клиенте SecureNAT, настроено на поддержку SOCKS 4
Зависимость от маршрутной инфраструктуры существующей сети	Клиент SecureNAT не перенаправляет соединения напрямую на брандмауэр ISA Server 2004. Напротив, он зависим от маршрутной инфраструктуры организации. Каждый маршрутизатор на пути от клиента SecureNAT к брандмауэру ISA Server 2004 должен знать, что путь к Интернету проходит через брандмауэр ISA Server 2004. Это может потребовать настройки сетевых маршрутизаторов с новыми шлюзами (основными шлюзами)
Информация о пользователе не включается в журналы брандмауэра и Web-прокс и	Имя пользователя включается в журналы брандмауэра и Web-прокси, только когда клиент отправляет эту информацию на брандмауэр ISA. Клиент всегда должен отправлять информацию о пользователе на брандмауэр, потому что в заголовках уровней 1-6 нет пунктов, содержащих эту информацию. Только конфигурации **клиента** брандмауэра и Web-прокси могут отправлять информацию о пользователе на брандмауэр ISA и включать эту информацию в системные журналы. Соединения клиента SecureNAT позволяют записывать в журнал исходный IP-адрес, но информация о пользователе никогда не записывается

Преимущества клиента SecureNAT

Некоторые из слабых сторон клиента SecureNAT являются его сильными сторонами:

- поддержка клиентских операционных систем, отличных от Windows;
- поддержка протоколов, отличных от протоколов TCP/UDP (PPTP и ICMP);
- не требуется установка или настройка клиентского программного обеспечения.

Основная цель конфигурации клиента SecureNAT состоит в том, чтобы разрешить операционным системам сторонних производителей получать доступ к бо-

лее широкому кругу протоколов помимо тех, которые поддерживаются конфигурацией клиента Web-прокси. Клиент брандмауэра работает только с операционными системами Windows. Таким образом, если бы не существовало конфигурации клиента SecureNAT, то для операционных систем сторонних производителей были бы доступны только те протоколы, которые поддерживаются конфигурацией клиента Web-прокси (HTTP/HTTPS и FTP).

Клиент SecureNAT также имеет достоинства и при использовании с операционными системами Microsoft. Программное обеспечение клиента брандмауэра перехватывает исходящие TCP- и UDP-соединения, установленные приложениями Winsock, и перенаправляет их на брандмауэр ISA Server 2004. Сетевые протоколы типа ICMP (Internet Control Message Protocol, протокол управляющих сообщений) и GRE (Generic Routing Encapsulation, протокол инкапсуляции маршрута) (применяемые для VPN-протоколов PPTP) не используют UDP или TCP в качестве транспортного протокола, и поэтому они не оцениваются клиентом брандмауэра. Для поддержки исходящего доступа через брандмауэр ISA Server 2004 с помощью этих протоколов нужно настроить компьютеры клиентов как клиенты SecureNAT.

В данной ситуации есть одно существенное ограничение: невозможно осуществлять пользовательский/групповой контроль доступа по отношению к хостам, выполняющим исходящие соединения по прочим протоколам (не TCP/UDP). Например, нужно разрешить исходящие VPN-подключения по протоколу PPTP для определенной группы пользователей. Это невозможно, потому что протокол PPTP требует использование протокола GRE, а это приводит к обходу программного обеспечения клиента брандмауэра и, таким образом, на брандмауэр ISA Server 2004 не передается никакая информация о пользователе. Если создать правило доступа для исходящих PPTP-соединений, предполагающее проверку подлинности пользователя, то попытка соединения будет безуспешной. Единственный способ контроля исходящих PPTP-соеди нений заключается в обращении к исходным IP-адресам. Более подробно эта тема рассматривается в главе 8.

ПРИМЕЧАНИЕ Протокол ЮМР чаще всего используется утилитой ping, хотя другие утилиты, например tracert, также используют этот протокол. Протокол GRE требуется в том случае, если нужно разрешить клиентам исходящий доступ к внешним VPN-серверам по VPN-протоколу PPTP. Напротив, исходящие VPN-клиенты, использующие протокол NAT-T L2TP/IPSec, не должны быть настроены как клиенты SecureNAT. Протокол NAT-T L2TP/IPSec использует только порты UDP 500 и 4500 для исходящего доступа к VPN-серверам по протоколам NAT-T L2TP/IPSec.

Наверное наиболее распространенной причиной использования конфигурации клиента SecureNAT является возможность избежать установки или настройки клиентского программного обеспечения. Администраторы сетей и брандмауэров с неохотой устанавливают программное обеспечение на клиентских компьютерах. Кроме того, существует точка зрения, что установка клиента брандмауэра ISA Server

2004 и настройка клиента Web-прокси предполагают существенные административные трудозатраты, но на самом деле это не так.

Фактически, вероятность того, что программное обеспечение клиента брандмауэра помешает работе сетевых компонентов любого клиентского программного обеспечения, ничтожно мала, а когда установка и настройка клиента брандмауэра и клиента Web-прокси автоматизированы, административные трудозатраты также очень малы.

Далее в этой главе рассматривается, как автоматизировать установку и настройку клиента. В табл. 5.3 представлены преимущества конфигурации клиента SecureNAT.

Табл. 5.3. Преимущества конфигурации клиента SecureNAT

Преимущество	Следствие
Обеспечивает дополнительную поддержку протоколов для операционных систем сторонних производителей	Операционные системы сторонних производителей не поддерживают программное обеспечение клиента брандмауэра, Если нужно обеспечить поддержку протоколов, которые не разрешены конфигурацией клиента Web-прокси (т. е. *HTTP/* HTTPS/FTP), то конфигурация SecureNAT является единственной возможностью для операционных систем сторонних производителей, например Linux, UNIX и Macintosh
Поддержка протоколов, отличных от протоколов TCP/UDP	Клиент SecureNAT — единственная конфигурация клиента ISA Server 2004, поддерживающая протоколы, отличные от TCP/ШР. Ping, tracert и PPTP — вот лишь некоторые протоколы, требующие конфигурации клиента SecureNAT. Обратите внимание, что невозможно осуществить жесткий контроль пользовательского/группового доступа для протоколов, отличных от TCP/UDP, потому что конфигурация клиента SecureNAT не поддерживает проверку подлинности пользователя
Не требуется установка или настройка программного обеспечения клиента	Клиент SecureNAT не требует установки и настройки никакого программного обеспечения на компьютере клиента. Единственное требование состоит в том, что адрес основного шлюза на клиентском компьютере должен быть настроен так, чтобы запросы *в* Интернет перенаправлялись через брандмауэр ISA Server 2004
Лучшая общая конфигурация для опубликованных серверов	При публикации сервера в Интернете сервер часто должен не только принимать соединения с хостов в Интернете, но и инициировать новые соединения. Лучший пример — это SMTP-ретранслятор, настроенный для входящей и исходящей передачи. SMTP-ретранслятор не должен быть настроен как клиент SecureNAT для того, чтобы принимать входящие соединения с удаленного SMTP-сервера (потому что имеется возможность замены исходного IP-адреса интернет-хоста IP-адресом брандмауэра ISA). Однако SMTP-ретранслятор должен быть настроен как клиент SecureNAT для отправки исходящей почты на SMTP-серверы в Интернете. Этот вопрос рассматривается более подробно в главе 10

Разрешение имен для клиентов SecureNAT

Как указывалось ранее при обсуждении поддержки сетевых служб, разрешение имен является критически важным вопросом не только при установке программного обеспечения брандмауэра ISA Server 2004, но и для всех типов клиентов ISA Server 2004. Каждый клиент ISA Server 2004 по-своему разрешает имена. Клиент SecureNAT разрешает имена для хостов во внутренней и внешней сетях с помощью адреса DNS-сервера, настроенного на сетевом интерфейсе клиента SecureNAT.

То, что клиент SecureNAT должен разрешать имена на базе своей собственной конфигурации TCP/IP, может представлять определенную проблему для организаций, имеющих соединение с Интернетом, которым требуется доступ к ресурсам как при подключении к корпоративной сети, так и когда эти же хосты должны покидать внутреннюю сеть и устанавливать соединение с корпоративными ресурсами с удаленных мест. Кроме того, серьезные затруднения возникают, когда клиенты SecureNAT пытаются выполнить замыкание через брандмауэр ISA Server 2004, чтобы получить доступ ко внутренней сети или к другим защищенным сетям.

Клиенты SecureNAT должны быть настроены на использование DNS-сервера, который может разрешать как имена во внутренней сети, так и имена хостов в Интернете. Большинство организаций имеют свои собственные DNS-серверы в пределах корпоративной сети. В данном случае клиент SecureNAT должен быть настроен на использование внутреннего DNS-сервера, который может разрешать внутренние сетевые имена, а затем либо выполнять рекурсию для разрешения имен хостов в Интернете, либо использовать механизм продвижения данных DNS для разрешения имен хостов в Интернете.

Разрешение имен и «обратное замыкание» через брандмауэр ISA Server 2004

Рассмотрим пример организации, в которой используется имя домена internal.net для ресурсов, расположенных во внутренней сети позади брандмауэра ISA Server 2004. В этой организации используется одно и то же имя домена для предоставления ресурсов удаленным пользователям и для публикации этих ресурсов во внутренней сети. Например, компания имеет собственный Web-сервер во внутренней сети, а IP-адрес этого Web-сервера во внутренней сети 192.168.1.10.

Организация также имеет собственные DNS-ресурсы и в базе данных DNS присвоила имени хоста www.internal.net IP-адрес 222.222.222.1. Внешние пользователи используют имя www.internal.net для получения доступа к Web-серверу компании. Этот Web-сервер опубликован с использованием правил Web-публикации ISA Server 2004, и внешние пользователи могут без проблем получить к нему доступ.

Если клиенты SecureNAT во внутренней сети пытаются установить соединение с этим Web-сервером, то попытки установить соединения оказываются неудачными. Это объясняется тем, что клиенты SecureNAT настроены на использование того

же DNS-сервера, который используется внешними клиентами для разрешения имени www.internal.net. Это имя разрешается в общий адрес на внешнем интерфейсе брандмауэра ISA Server 2004, используемый в правиле Web-публикации. Клиент SecureNAT разрешает имя www.internal.net в этот адрес и перенаправляет соединение на внешний интерфейс брандмауэра ISA Server 2004, который затем перенаправляет запрос на Web-сервер во внутренней сети.

Web-сервер отвечает *напрямую компьютеру клиента SecureNAT,* потому что исходный IP-адрес в запросе, перенаправленном брандмауэром ISA Server 2004 на Web-сервер во внутренней сети, является IP-адресом клиента SecureNAT. Web-сервер во внутренней сети считает, что этот IP-адрес расположен в его локальной сети, и отвечает напрямую клиенту SecureNAT. Компьютер клиента SecureNAT отбрасывает ответ от Web-сервера, потому что он отправлял запрос на общий IP-адрес брандмауэра ISA Server 2004, а не на IP-адрес Web-сервера во внутренней сети. На рис. 5.4 показано, как клиент SecureNAT создает «обратное замыкание» через брандмауэр ISA Server 2004.

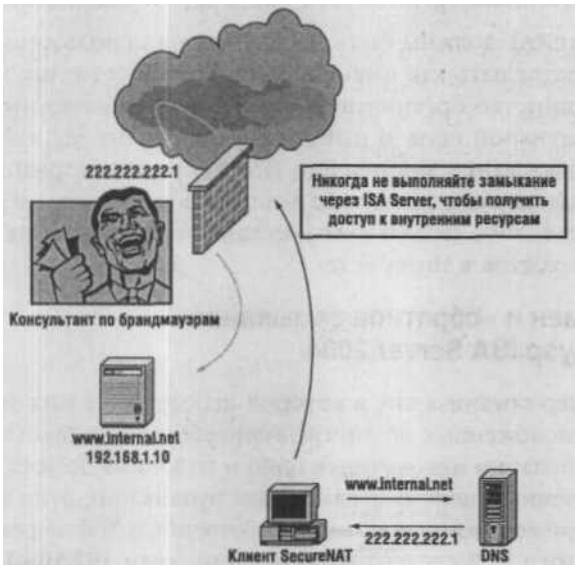


Рис. 5.4. «Обратное замыкание» клиента SecureNAT

Решение этой проблемы состоит в применении расщепленной инфраструктуры DNS. Практически во всех случаях, когда организации требуется удаленный доступ к ресурсам, расположенным во внутренней сети, расщепленная структура DNS является решением проблем с разрешением имен для клиентов SecureNAT и «блуждающих клиентов» (roaming clients) (хостов, которые располагаются то во внутренней сети, то за пределами корпоративной сети).

В расщепленной инфраструктуре DNS клиент SecureNAT настраивается на использование внутреннего DNS-сервера, который разрешает имена для ресурсов, основываясь на адресе ресурса во внутренней сети. Удаленные хосты также могут разрешать эти имена, но внешние хосты разрешают эти имена в IP-адреса на внешнем интерфейсе брандмауэра ISA Server 2004, который опубликовал эти ресурсы. Это позволяет клиенту SecureNAT избежать обратного замыкания через брандмауэр **ISA Server** 2004 и успешно выполнить соединения с опубликованными серверами. На рис. 5.5 показано, как расщепленная инфраструктура DNS разрешает проблему обратного замыкания дли клиентов SecureNAT. В табл. 54 представлены важные вопросы относительно применения DNS к клиентам SecureNAT.

ПРИМЕЧАНИЕ По этой же причине Web-разработчикам никогда не следует встраивать IP-адреса или имена в ссылки, возвращаемые Web-пользователям. Например, Web-разработчик может вставить ссылку, которая ведет на **http://192.168.1-1/info,** в Web-страницу ответа для пользователя. Клиенты внутренней сети могут получить доступ к этой ссылке, потому что этот IP-адрес является адресом Web-сервера во внутренней сети, а пользователи удаленного доступа не могут установить соединение с этим ресурсом, потому что к этому адресу невозможно получить доступ из Интернета. Многие Java-приложения и даже некоторые приложения Microsoft, например SharePoint Portal Server, страдают от такого типа неверного кодирования (хотя часть этих проблем можно решить с помощью функции преобразования ссылок брандмауэра ISA Server 2004).

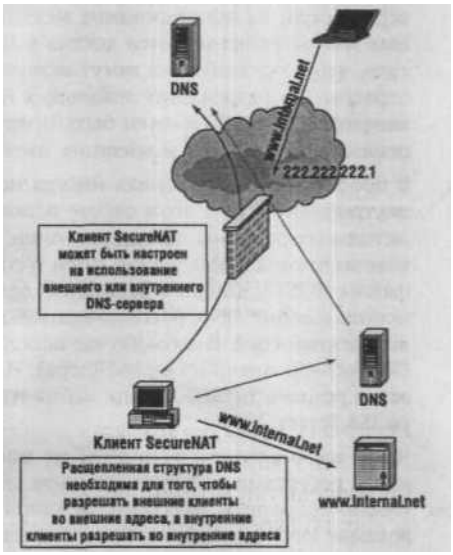


Рис. 5.5. Расщепленная инфраструктура DNS решает проблему разрешения адресов для клиента SecureNAT

Табл. 5.4. Применение DNS к клиентам SecureNAT

Применение DNS к клиентам SecureNAT	Следствие
Разрешение имен внутренних и внешних хостов	Клиент SecureNAT должен быть способен разрешать имена всех хостов с помощью адреса локально настроенного DNS-сервера. DNS-сервер должен быть способен разрешать имена внутренней сети, а также имена внешних хостов в Интернете. Если DNS-сервер, на использование которого настроен клиент SecureNAT, не способен разрешать локальные имена или имена из Интернета, запрос на разрешение имени не будет выполнен и попытка соединения будет разорвана Клиенты
Обратное замыкание через брандмауэр ISA Server 2004	SecureNAT не должны образовывать обратного замыкания через брандмауэр ISA Server 2004 для того, чтобы получить доступ к ресурсам внутренней сети. Чаще всего это происходит, когда сервер внутренней сети был опубликован в Интернете. Клиент SecureNAT настроен с DNS-сервером, который разрешает имя сервера в IP-адрес на внешнем интерфейсе брандмауэра ISA Server 2004. Клиент SecureNAT отправляет **запрос** на соединение на **этот** IP-адрес, и запрос на соединение не выполняется. Чтобы решить эту проблему, нужно настроить расщепленную инфраструктуру DNS Организации с
Организации с внутренними DNS-серверами	внутренними DNS-серверами должны настроить эти серверы на разрешение имен внутренних и внешних хостов. Внутренние DNS-серверы отвечают за имена доменов внутренней сети. DNS-серверы должны быть настроены на выполнение рекурсии по отношению к DNS-серверам в Интернете или на использование механизма продвижения данных для разрешения имен хостов в Интернете. Следует отметить, что в организации могут использоваться различные серверы для разрешения локальных и внешних имен, но для клиента SecureNAT должен быть предусмотрен механизм разрешения внутренних и внешних имен с помощью DNS
Организации, в которых нет внутренних DNS-серверов	В небольших организациях иногда не бывает DNS-сервера во внутренней сети. В этом случае используются альтернативные методы разрешения локальных имен, например WINS, широковещательное разрешение имен NetBIOS или локальные файлы HOSTS. Клиенты SecureNAT должны быть настроены на использование DNS, **расположенной** в Интернете (например, внутренней сети. В этом случае используются альтернативный DNS-сервер интернет-провайдера). Или настраивать DNS-сервер в режиме только кэширования на компьютере брандмауэра ISA Server 2004
Клиент SecureNAT не может установить соединение с Интернетом	Чаще всего клиенты SecureNAT не могут установить соединение с ресурсами в Интернете из-за сбоя в разрешении имен. Нужно проверить, настроен ли клиент SecureNAT на использование DNS-сервера, который разрешает имена хостов в Интернете. Можно воспользоваться утилитой nslookup, чтобы протестировать **разрешение** имен на компьютере клиента SecureNAT

Табл. 5.4. (окончание)

Применение DNS к клиентам SecureNAT	Следствие
Клиент SecureNAT не может установить соединение с серверами во внутренней сети	Чаще всего неспособность клиента SecureNAT установить соединение с локальными ресурсами с помощью имен хостов DNS объясняется сбоем в разрешении имен. Нужно проверить, настроен ли DNS-сервер на клиенте SecureNAT так, чтобы выполнять разрешение имен во внутренней сети. Если клиент SecureNAT настроен на использование DNS-сервера в Интернете (например, DNS-сервера интернет-провайдера), то клиент SecureNAT не сможет разрешать имена локальных DNS хостов. Этого можно избежать, если настроить клиент SecureNAT на использование внутреннего DNS-сервера, который может разрешать имена локальных хостов и хостов в Интернете, или если использовать альтернативный метод разрешения имен хостов во внутренней сети
Клиенты SecureNAT должны быть настроены на использование DNS-сервера во внутренней сети	Хотя в небольших организациях не всегда имеется DNS-сервер, отвечающий за разрешение имен во внутренней сети, следует избегать использования общего DNS-сервера для клиентов SecureNAT. Вместо этого нужно настроить брандмауэр ISA Server 2004, чтобы использовать DNS-сервер в режиме только кэширования на брандмауэре ISA Server 2004. Настройте DNS-сервер в режиме только кэширования на брандмауэре ISA Server 2004, чтобы использовать надежный DNS-сервер, например DNS-сервер интернет-провайдера, в качестве механизма продвижения данных. Это снижает риск, присутствующий, если клиенты SecureNAT напрямую взаимодействуют с DNS-серверами в Интернете. DNS-сервер в режиме только кэширования на брандмауэре ISA Server 2004 можно настроить, чтобы предотвратить атаки на DNS, такие как фальсификация кэша.

Клиент брандмауэра ISA Server 2004

Программное обеспечение клиента брандмауэра является вспомогательным программным продуктом, который можно установить на любую совместимую операционную систему Windows для обеспечения расширенных функций защиты и предоставления доступа. Программное обеспечение клиента брандмауэра добавляет следующие функции клиентам Windows:

- позволяет выполнять строгую пользовательскую/групповую проверку подлин ности для всех приложений Winsock, использующих протоколы TCP и UDP;
- позволяет вносить в системные журналы брандмауэра ISA Server 2004 инфор мацию о пользователях и приложениях;
- обеспечивает расширенную поддержку сетевых приложений, включая сложные протоколы, требующие вторичных соединений;

- обеспечивает DNS-поддержку компьютеров клиентов брандмауэра;
- позволяет публиковать серверы, требующие использования сложных протоколов без помощи фильтров приложений;
- маршрутная инфраструктура сети прозрачна для клиента брандмауэра.

Выполнение строгой пользовательской/групповой проверки подлинности для всех приложений Winsock, использующих протоколы TCP и UDP

Программное обеспечение клиента брандмауэра отправляет информацию о пользователе на брандмауэр ISA Server 2004 в прозрачном режиме. Это позволяет создавать правила доступа, которые применяются к пользователям и группам и разрешают или запрещают доступ к любому протоколу, сайту или содержимому, основываясь на учетной записи пользователя или на членстве в группе. Такой жесткий контроль исходящего пользовательского/группового доступа очень важен. Не всем пользователям следует предоставлять одинаковый уровень доступа, им следует предоставлять доступ только к тем протоколам, сайтам и содержимому, которое им необходимо для выполнения их работы.

> ПРИМЕЧАНИЕ Принцип, состоящий в том, чтобы разрешать пользователям доступ только к тем протоколам, сайтам и содержимому, которые им необходимы, называется принципом наименьшего уровня привилегий. Этот принцип применяется как к входящему, так и к исходящему доступу. В случае входящего доступа правила Web-публикации и публикации серверов разрешают трафик от внутренних хостов к ресурсам во внешней сети только под жестким контролем и наблюдением. То же относится и к исходящему доступу. В традиционных сетях входящий доступ сильно ограничен, а внешний доступ разрешен практически ко всем ресурсам. Такой подход к контролю исходящего доступа может подвергнуть риску не только корпоративную сеть, но и другие сети, поскольку интернет-черви могут с легкостью обойти брандмауэры, которые не ограничивают исходящий доступ.

Клиент брандмауэра автоматически отправляет верительные данные пользователя (имя пользователя и пароль) на брандмауэр ISA Server 2004. Пользователь должен выполнить вход в систему с помощью учетной записи пользователя, которая находится либо в домене Windows Active Directory, либо в домене NT, или же учетная запись пользователя должна быть зеркально отображена на брандмауэре ISA Server 2004. Например, если имеется домен Active Directory, то пользователи должны выполнять вход на этот домен, а брандмауэр ISA Server 2004 должен быть членом этого домена. Брандмауэр ISA Server 2004 способен выполнить проверку подлинности пользователя и разрешить или запретить доступ на основании верительных данных пользователя.

Программное обеспечение клиента брандмауэра можно использовать для контроля исходящего доступа для пользователей/групп, даже если домена Windows нет.

В этом случае нужно зеркально отобразить учетные записи, с помощью которых пользователи выполняют вход на свои рабочие станции, в учетные записи, хранящиеся в локальном SAM (Security Account Manager, администратор учетных данных в системе защиты) на компьютере брандмауэра ISA Server 2004.

Например, в небольших офисах не используется служба Active Directory, но нужен жесткий контроль исходящего доступа для пользователей/групп. Пользователи выполняют вход на свои компьютеры с помощью локальных учетных записей. Можно ввести те же имена пользователей и пароли на брандмауэр ISA Server 2004, и он сможет проверять подлинность пользователей, основываясь на информации об используемой учетной записи.

Внесение в системные журналы брандмауэра ISA Server 2004 информации о пользователях и приложениях

Основное преимущество использования клиента брандмауэра состоит в том, что когда имя пользователя пересылается на брандмауэр ISA Server 2004, это имя пользователя включается в системные журналы брандмауэра ISA Server 2004. Это позволяет с легкостью выполнить запрос к системным журналам, указав имя пользователя, и получить точную информацию о том, что этот пользователь делал в Интернете.

В данном случае клиент брандмауэра не только обеспечивает высокий уровень защиты, позволяя контролировать исходящий доступ на основании учетных записей пользователей/групп, но также дает возможность создавать различные отчеты. Пользователи будут менее охотно делиться своей информацией об учетной записи, если они будут знать, что их работа в Интернете отслеживается по имени учетной записи и за то, что они делают в Интернете, им придется нести ответственность.

Расширенная поддержка сетевых приложений, в том числе сложных протоколов, требующих вторичных соединений

В отличие от клиента SecureNAT, которому необходим фильтр приложения для поддержки сложных протоколов, требующих вторичных соединений, клиент брандмауэра может поддерживать практически любое приложение Winsock с помощью протоколов TCP или UDP независимо от количества первичных или вторичных соединений и без помощи фильтра приложения.

Брандмауэр ISA Server 2004 позволяет легко настроить определения протоколов, отражающие несколько первичных или вторичных соединений, а затем создать правила доступа на основании этих определений протоколов. Это обеспечивает существенное преимущество с точки зрения полной стоимости владения, потому что не придется покупать приложения, работающие с SOCKS прокси, и тратить время на создание собственных фильтров приложения для поддержки сторонних интернет-п риложен и й.

DNS-поддержка компьютеров клиента брандмауэра

В отличие от клиента SecureNAT клиент брандмауэра не нужно настраивать с DNS-сервером, который будет разрешать имена хостов в Интернете. Брандмауэр ISA Server 2004 может выполнять функцию поддержки клиентов брандмауэра вместо DNS.

Например, когда клиент брандмауэра отправляет запрос на ftp://ftp.microsoft.com, этот запрос отправляется напрямую на брандмауэр ISA Server 2004. Брандмауэр ISA Server 2004 разрешает имя для клиента брандмауэра, основываясь на настройках DNS на сетевых интерфейсных картах брандмауэра ISA Server 2004, затем возвращает IP-адрес компьютеру клиента брандмауэра, а компьютер клиента брандмауэра отправляет FTP-запрос на этот IP-адрес к FTP-сайту ftp.microsoft.com. Брандмауэр ISA Server 2004 также кэширует результаты DNS-запросов, которые он направляет клиентам брандмауэра. Это ускоряет разрешение имен для последующих соединений клиента брандмауэра с теми же сайтами. На рис. 5.6 показана последовательность действий при разрешении имен для клиента брандмауэра.

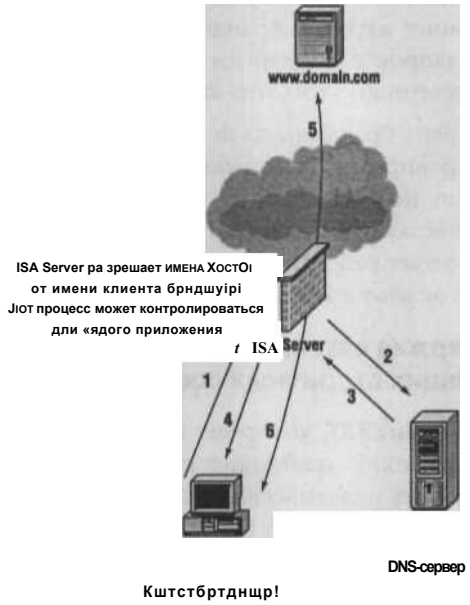


Рис. 5.6. Последовательность действий при разрешении имен

1. Клиент брандмауэра посылает запрос на ftp.microsoft.com.
2. Брандмауэр ISA Server 2004 отправляет DNS-запрос на внутренний DNS-сервер.
3. DNS-сервер разрешает имя ftp.microsoft.com в его IP-адрес и возвращает результат на брандмауэр ISA Server 2004.
4. Брандмауэр ISA Server 2004 возвращает IP-адрес ftp.microsoft.com клиенту бранд мауэра, который выполнил этот запрос.

5. Клиент брандмауэра отправляет запрос на IP-адрес для ftp.microsoft.com, и со единение устанавливается.
6. Интернет-сер вер возвращает запрошенную информацию клиенту брандмауэра по соединению между клиентом брандмауэра и брандмауэром ISA Server 2004.

Маршрутная инфраструктура сети прозрачна для клиента брандмауэра

Еще одно преимущество клиента брандмауэра состоит в том, что маршрутная инфраструктура является практически прозрачной для компьютера клиента брандмауэра. В отличие от клиента SecureNAT, зависящего от основного шлюза и от настроек основного шлюза на маршрутизаторах корпоративной сети, компьютеру клиента брандмауэра нужно знать только маршрут к IP-адресу на внутреннем интерфейсе брандмауэра ISA Server 2004.

Компьютер клиента брандмауэра пересылает запросы напрямую на IP-адрес брандмауэра ISA Server 2004. Поскольку маршрутизаторы в корпоративной сети обычно имеют информацию обо всех остальных маршрутизаторах корпоративной сети, нет необходимости вносить изменения в маршрутную инфраструктуру для поддержки соединения клиента брандмауэра с Интернетом. На рис. 5.7 показана передача таких соединений напрямую на компьютер брандмауэра ISA Server 2004. В табл. 5.5 представлены преимущества приложения клиента брандмауэра.

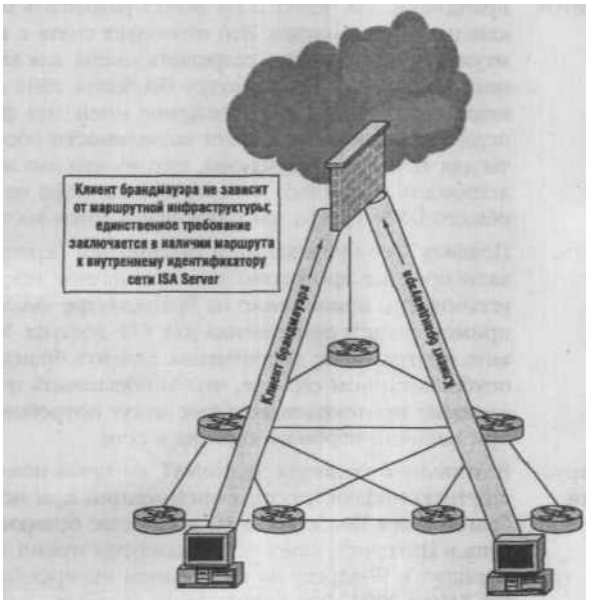


РИС. 5.7. Соединения клиента брандмауэра с брандмауэром ISA Server 2004 не зависят от конфигурации основного шлюза на промежуточных маршрутизаторах

Табл. 5.5. Преимущества конфигурации клиента брандмауэра

Преимущество клиента брандмауэра	Следствие
Пользовательская/групповая проверка подлинности для протоколов Winsock TCP и UDP	Пользовательская/групповая проверка подлинности для приложений Winsock, использующих протоколы TCP и UDP, позволяет осуществлять жесткий контроль исходящего доступа и реализовать принцип наименьшего уровня привилегий применительно не только к своей сети, но и к сетям других организаций
Информация об имени пользователя и приложениях сохраняется в журналах брандмауэра ISA Server 2004	Жесткий пользовательский/групповой контроль доступа повышает защиту сети, а сохранение информации об именах пользователей и приложениях в журнале брандмауэра ISA Server 2004 позволяет вести отчетность и отслеживать, к каким сайтам, протоколам и приложениям получали доступ пользователи с программным обеспечением клиента брандмауэра
Расширенная поддержка сетевых приложений и протоколов	Клиент брандмауэра может получить доступ практически к любому протоколу TCP/UDP, даже к сложным протоколам, требующим несколько первичных и/или вторичных соединений. Напротив, клиенту SecureNAT требуется фильтр приложения на брандмауэре ISA Server 2004 для поддержки сложных протоколов. *В* общем использование клиента брандмауэра позволяет снизить общую стоимость владения брандмауэра ISA Server 2004
DNS-поддержка клиентов брандмауэра	Брандмауэр ISA Server 2004 может разрешать имена от имени клиентов брандмауэра. Это позволяет снять с клиента брандмауэра необходимость разрешать имена для хостов в Интернете и позволяет брандмауэру ISA Server 2004 иметь DNS-кэш недавних запросов на разрешение имен. Эта функция DNS-поддержки также расширяет возможности обеспечения защиты для клиента брандмауэра, потому что она исключает необходимость настройки клиента брандмауэра на использование общего DNS-сервера для разрешения имен хостов в Интернете
Позволяет публиковать серверы, которым нужны сложные сетевые протоколы	Правила Web-публикации и публикации серверов поддерживают простые протоколы за исключением тех, для которых установлено приложение на брандмауэре ISA Server 2004, например фильтр приложения для FTP доступа. Можно установить программное обеспечение клиента брандмауэра на опубликованном сервере, чтобы обеспечить поддержку сложных протоколов, которые могут потребоваться при наличии игрового сервера в сети
Маршрутная инфраструктура сети практически прозрачна для клиента брандмауэра	В отличие от клиента SecureNAT, который полагается на маршрутную инфраструктуру организации при использовании брандмауэра ISA Server 2004 в качестве брандмауэра для доступа в Интернет, клиенту брандмауэра нужно знать только маршрут к IP-адресу на внутреннем интерфейсе брандмауэра ISA Server 2004. Это существенно снижает административные трудозатраты на поддержку клиента брандмауэра по сравнению с клиентом SecureNAT

Принцип работы клиента брандмауэра

В книгах корпорации Microsoft нет подробного описания принципов работы программного обеспечения клиента брандмауэра. Известно лишь, что клиент брандмауэра ISA Server 2004, в отличие от предыдущих версий, использует только TCP 1745 для контрольного канала клиента брандмауэра. По этому контрольному каналу клиент брандмауэра осуществляет взаимодействие со службой брандмауэра ISA Server 2004 для выполнения разрешения имен и команд сетевых приложений (например, команд, используемых FTP и Telnet). Служба брандмауэра использует информацию, полученную по контрольному каналу, и устанавливает соединение между клиентом брандмауэра и сервером-адресатом в Интернете.

ПРИМЕЧАНИЕ Стоит отметить, что клиент брандмауэра только устанавливает соединение по контрольному каналу при соединении с ресурсами, расположенными не во внутренней сети.

В ISA Server 2004 внутренняя сеть определялась таблицей локальных адресов (Local Adress Table, LAT). Брандмауэр ISA Server 2004 не использует LAT, потому что обладает расширенными возможностями по работе с несколькими сетями. Тем не менее клиент брандмауэра должен обладать неким другим механизмом для определения того, какие соединения нужно направлять на службу брандмауэра на брандмауэре ISA Server 2004, а какие следует направлять напрямую к хосту назначения, с которым хочет установить соединение клиент брандмауэра.

Клиент брандмауэра решает эту проблему с помощью адресов, определенных во внутренней сети. Внутренняя сеть для конкретного клиента брандмауэра состоит из всех адресов, доступ к которым можно получить с сетевого интерфейса, соединенного с сетью клиента брандмауэра. Особый случай представляет собой брандмауэр ISA Server 2004 с тремя сетевыми интерфейсами, в котором есть несколько внутренних сетей, связанных с различными сетевыми адаптерами. В общем все хосты, расположенные за одним сетевым адаптером (независимо от идентификатора сети) рассматриваются как часть одной внутренней сети, а все взаимодействия между хостами в одной внутренней сети должны обходить клиента брандмауэра.

Адреса для внутренней сети определяются в процессе установки программного обеспечения брандмауэра ISA Server 2004, но по желанию можно создать другие внутренние сети.

Замечание о защите ISA Server 2004

На одном компьютере с брандмауэром ISA Server 2004 может быть несколько интерфейсов. Однако только одна сеть может называться внутренней. Она состоит из группы компьютеров, безоговорочно доверяющих друг другу (хотя бы настолько, чтобы не пользоваться сетевым брандмауэром для контроля взаимодействия между ними). Может иметься несколько внутренних сетей,

(см. след. стр.)

но они не могут включаться в диапазон внутренних адресов другой внутренней сети.

Это означает, что нельзя использовать централизованно созданный диапазон сетевых адресов, настроенный для внутренней сети и дополнительных внутренних сетей, чтобы обойти клиента брандмауэра при соединении с внутренними сетями, подключенными к брандмауэру ISA Server 2004 через разные сетевые интерфейсы. Однако можно использовать файл с LAT (locallat.txt) для того, чтобы подменить настройки главной внутренней сети,

Внутренние сети с точки зрения брандмауэра ISA Server 2004 более подробно рассматриваются в главе 4.

Наиболее важным улучшением клиента брандмауэра ISA Server 2004 по сравнению с предыдущими версиями клиента брандмауэра (Winsock Proxy Client 2.0 и клиент брандмауэра ISA Server 2000) является возможность использовать зашифрованный канал между клиентом брандмауэра и брандмауэром ISA Server 2004. Не стоит забывать о том, что клиент брандмауэра отправляет верительные данные пользователя на брандмауэр ISA Server 2004 в прозрачном режиме. Клиент брандмауэра ISA Server 2004 зашифровывает канал так, что верительные данные пользователя не могут быть перехвачены теми, кто прослушивает сеть с помощью сетевого анализатора (например, Microsoft Network Monitor или Ethereal). Кроме того, имеется возможность настроить брандмауэр ISA Server 2004 так, чтобы разрешался как зашифрованный, так и незашифрованный обмен данными по контрольному каналу.

Подробное практическое исследование взаимодействия приложения клиента брандмауэра *и* службы брандмауэра в ISA Server 2000, представлено в статье Стефана Поусила (Stefaan Pouseele) «Understanding the Firewall Client Control Channel» (Контрольный канал клиента брандмауэра) на сайте: www.isaserver.org/articles/Understanding_the_Firewall_Client_Control_Channel.html.

ПРИМЕЧАНИЕ Если в сети включен транспортный режим IPSec, так что компьютер клиента брандмауэра использует транспортный режим IPSec для соединения с брандмауэром ISA Server 2004, то это может привести к необычным и непредсказуемым ситуациям при установке соединения. Если клиент брандмауэра в сети ведет себя как-то необычно, отключите вариант IP routing (IP-маршрутизация) в консоли брандмауэра ISA Server 2004. В консоли управления Microsoft Internet Security and Acceleration Server 2004 разверните сервер, а затем разверните узел Configuration (Настройка) и щелкните узел General (Общие). На панели инструментов щелкните Define IP Preferences (Определить IP-предпочтения). Убедитесь, что на вкладке IP Routing (IP-маршрутизация) не установлен флажок в поле Enable IP Routing (Включить IP-маршрутизацию).

Установка общего ресурса клиента брандмауэра

Общий ресурс клиента брандмауэра содержит установочные файлы для клиента брандмауэра. Вне зависимости от способа распространения клиента брандмауэра необходимо установить общий ресурс клиента брандмауэра либо на брандмауэре ISA Server 2004, либо на файловом сервере во внутренней сети. Не рекомендуется устанавливать программное обеспечение клиента брандмауэра на брандмауэре ISA Server 2004.

Когда общий ресурс клиента брандмауэра установлен на брандмауэре ISA Server 2004, создается правило системной политики брандмауэра (тип правила доступа, обрабатываемое перед применением определенных правил доступа), разрешающее нескольким потенциально опасным протоколам получать доступ на компьютер брандмауэра. К таким протоколам относятся:

- Microsoft CIFS (Common Internet File System, общий протокол доступа к файлам Интернет) (TCP);
- Microsoft CIFS (UDP);
- дейтаграмма NetBIOS (NetBIOS Datagram);
- служба имен NetBIOS (NetBIOS Name Service);
- сеанс NetBIOS (NetBIOS Session).

Кроме того, на внутреннем интерфейсе должны быть включены возможности совместного использования файлов и принтеров. Эти службы и протоколы Microsoft для совместного использования файлов и принтеров, а также служба клиента для сетей Microsoft (Client for Microsoft Networks) могут представлять серьезную угрозу для брандмауэра ISA Server 2004, и их следует по возможности отключить на всех сетевых интерфейсах ISA Server 2004. Эти службы можно отключить и при этом оставить общий ресурс клиента брандмауэра доступным для пользователей в сети. Для этого нужно установить общий ресурс клиента брандмауэра на другом компьютере в корпоративной сети.

Для установки общего ресурса клиента брандмауэра на файловом сервере во внутренней сети выполните следующие действия:

1. Вставьте компакт-диск с ISA Server 2004 в дисковод для компакт-дисков на файловом сервере и подождите, пока появится меню **Autorun** (Автозапуск). Щелкните **Install ISA Server 2004** (Установить ISA Server 2004).
2. Щелкните **Next** (Далее) на странице **Welcome to the Installation Wizard for Microsoft ISA Server 2004** (Вас приветствует мастер установки Microsoft ISA Server 2004).
3. Щелкните **I accept the terms** (Согласен) в окне лицензионного соглашения и щелкните **Next** (Далее).
4. Введите имя пользователя, название организации и серийный номер продукта в соответствующие текстовые поля. Щелкните **Next** (Далее).

5. На странице **Setup Type** (Тип установки) выберите **Custom** (Пользовательская) и щелкните **Next** (Далее).
6. Щелкните на значке **Firewall Services** (Службы брандмауэра) и щелкните **This feature will not be available** (Эта функция будет недоступна). Щелкните на значке **ISA Server Management** (Управление ISA Server) и щелкните **This feature will not be available** (Эта возможность будет недоступна). Щелкните на значке **Firewall Client Installation Share** (Общий ресурс для установки клиента брандмауэра) и щелкните **This feature, and all the subfeatures, will be installed on local hard drive** (Эта функция и все подфункции будут установлены на локальном жестком диске) (рис. 5.8). Щелкните **Next** (Далее).

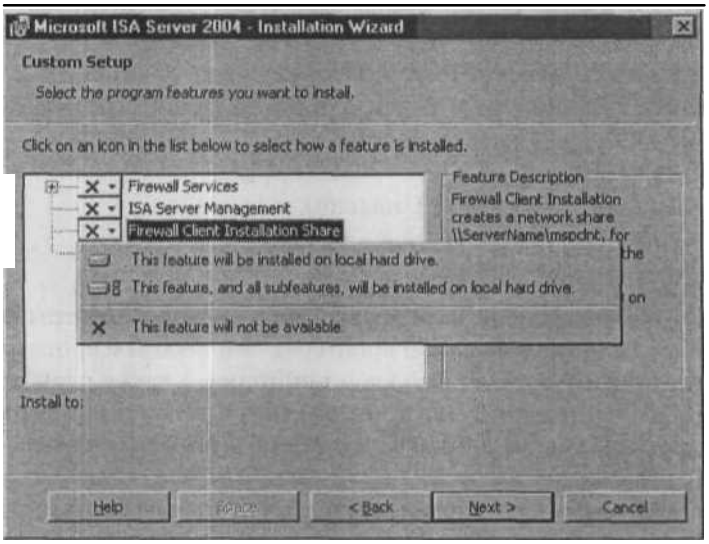


Рис. 5.8. Установка клиента брандмауэра

7. Щелкните **Install** (Установить) на странице **Ready to Install the Program** (Готов к установке программы).
8. Щелкните **Finish** (Готово) на странице **Installation Wizard Completed** (Завершение работы мастера установки).
9. Закройте страницу **Autorun** (Автозапуск).

Общий ресурс для установки клиента брандмауэра готов. По умолчанию путь к нему такой: %System%\Program Files\...\Microsoft ISA Server\clients. Имя общего ресурса: mspclnt. По умолчанию для этой папки параметр **Share Permissions** (Полномочия общего ресурса) установлен на **Everyone Read** (Чтение). По умолчанию для этого общего ресурса действительны следующие NTFS-полномочия: ■ для администраторов — Full Control (Полный контроль);

- для пользователей, прошедших проверку подлинности, — **Read&Execute** (Чтение и Выполнение), **List Folder Contents** (Просмотр содержимого папок) и **Read** (Чтение);
- для системы — **Full Control** (Полный контроль).

Установка клиента брандмауэра

Существует несколько методов установки программного обеспечения клиента брандмауэра:

- с использованием SMB/CIFS-соединения с общим ресурсом на файловом сервере;
- установка с применением групповых политик в среде с Active Directory;
- установка без вмешательства пользователей с помощью сценариев;
- установка с помощью SMS-сервера (Systems Management Server, сервер управления системами).

В этом разделе показано, как устанавливать клиент брандмауэра вручную. Пользователи, выбравшие этот метод установки программного обеспечения клиента брандмауэра, должны быть локальными администраторами компьютера, на котором они устанавливают программное обеспечение. Например, если речь идет о ноутбуке, который также является членом корпоративного домена, нужно убедиться в том, что у пользователя ноутбука имеется локальная учетная запись, которая является членом группы администраторов. Необходимо, чтобы пользователь вышел из домена и зашел на локальный компьютер. Затем пользователь может установить соединение с общим ресурсом клиента брандмауэра на сетевом файловом сервере. Пользователю, возможно, придется ввести сетевые верительные данные при соединении с файловым сервером, если учетная запись ноутбука, с которой пользователь в данный момент зарегистрировался в системе, не отображена на файловом сервере или в службе Active Directory (при условии, что файловый сервер и пользователь являются членами одного домена Active Directory).

Все пользователи этого компьютера имеют доступ к программному обеспечению клиента брандмауэра, после того как оно было установлено. Это означает, что пользователь может выйти из локальной учетной записи и войти вновь с доменными верительными данными, продолжая пользоваться программным обеспечением клиента брандмауэра.

Если пользователям не разрешено быть членами группы администраторов на их локальных компьютерах, то нужно использовать один из методов автоматической установки, который устанавливает программное обеспечение клиента брандмауэра, прежде чем пользователь выполнит вход в систему. Для этого можно воспользоваться установкой с применением групповых политик в среде с Active Directory или SMS-сервером.

При установке программного обеспечения клиента брандмауэра нужно учесть следующее:

- не следует устанавливать программное обеспечение клиента брандмауэра на компьютер брандмауэра ISA Server 2004;
- не следует устанавливать программное обеспечение клиента брандмауэра на контроллер домена или другие сетевые серверы. Единственным исключением из этого правила является случай, когда **нужно** опубликовать сервер, который требует поддержки сложных протоколов. Например, многие игровые серверы требуют несколько первичных и вторичных соединений. В таком случае клиент брандмауэра должен быть установлен на опубликованном сервере;
- программное обеспечение клиента брандмауэра **начинает** работать сразу же после завершения установки;
- клиента брандмауэра можно установить на базе любой версии Windows (за исключением Windows 95) при условии, что установлен Internet Explorer 5.0.

Для установки программного обеспечения клиента брандмауэра с общего ресурса во внутренней сети выполните следующие действия:

1. Щелкните **Start** (Пуск), а затем **Run** (Выполнить).
2. В диалоговом окне **Run** (Запуск программы) введите \\FILESERVER\mspclnt\setup (где FILESERVER — имя брандмауэра ISA Server 2004) и щелкните OK.
3. Щелкните **Next** (Далее) на странице **Welcome to the Install Wizard for Micro soft Firewall Client** (Вас приветствует мастер установки клиента брандмауэра Microsoft).
4. Щелкните **Next** (Далее) на странице **Destination Folder** (Путь установки).
5. На странице **ISA Server Computer Selection** (Выбор компьютера ISA Server) вы берите **Connect to this ISA Server computer** (Установить соединение с этим компьютером ISA Server) и введите remoteisa.msfirewall.org в текстовое поле под этой надписью. Щелкните **Next** (Далее).
6. Щелкните **Install** (Установить) на странице **Ready to Install the Program** (Ус тановка программы).
7. Щелкните **Finish** (Готово) на странице **Install the Wizard Completed** (Завер шение работы мастера установки).
8. В области уведомлений появится значок клиента брандмауэра (рис 5.9). Если имеется активное TCP или UDP-соединение с сетью, которая не является внут ренней сетью, то на значке будет зеленая стрелка вверх.

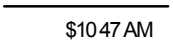


Рис. 5.9. Значок клиента брандмауэра

СОВЕТ VPN-клиенты могут устанавливать программное обеспечение клиента брандмауэра при соединении с сетью с помощью клиентского VPN-подключения.

Замечание о защите ISA Server 2004

Настройки, указанные при установке клиента брандмауэра, применяются ко всем учетным записям пользователя на компьютере клиента. Изменения, внесенные в диалоговое окно клиента брандмауэра на компьютере клиента брандмауэра после установки, применяются только к учетным записям пользователей, с которых выполнен вход в систему. Изменения не касаются других пользователей или приложений, работающих с системными учетными записями. Чтобы изменить настройки клиента брандмауэра для всех учетных записей после завершения установки, внесите изменения в файлы Common.ini и Manage men t.ini, расположенные в папке Documents and Settings\All Users\ Local Settings\Application Data\Microsoft\Firewall Client 2004. После изменения файла Common.ini следует перезагрузить службу клиента брандмауэра (FwcAgent) на компьютерах на базе ОС Windows Server 2003, Windows XP, Windows 2000 и Windows NT. Нужно перезагрузить компьютер на базе ОС Windows 9x. Изменения, внесенные в файл Management.ini, не требуют перезапуска службы или компьютера. Более подробно конфигурационные файлы Management.ini и Common.ini рассматриваются далее в этой главе.

Конфигурирование клиента брандмауэра

Программное обеспечение клиента брандмауэра можно настроить либо в консоли управления **Microsoft Internet Security and Acceleration Server 2004,** либо непосредственно на компьютере клиента брандмауэра. Изменения в настройках, выполненные в консоли управления **Microsoft Internet Security and Acceleration Server 2004,** применяются ко всем компьютерам клиента брандмауэра, а изменения, выполненные на отдельном клиентском компьютере, применяются только к этому клиенту.

Варианты централизованной настройки на компьютере брандмауэра ISA Server 2004

Варианты централизованной настройки клиента брандмауэра находятся в консоли управления **Microsoft Internet Security and Acceleration Server 2004.** Настройка клиента брандмауэра производится для каждой сети, настроенной на поддержку соединений клиентов брандмауэра. Клиенты брандмауэра могут выполнять соединения из:

- сетей периметра;
- внутренних сетей.

Все остальные типы сетей не поддерживают соединения клиентов брандмауэра. Если для сети разрешены соединения клиентов брандмауэра, то разрешены входящие соединения с портами TCP и UDP 1745 к интерфейсу, соединенному с этой сетью.

Доступ к интерфейсу конфигурирования клиента брандмауэра можно получить с консоли управления **Microsoft Internet Security and Acceleration Server 2004,** развернув имя сервера, а затем развернув узел **Configuration** (Настройка). В узле Configuration (Настройка) щелкните узел **Networks** (Сети), а затем щелкните вкладку **Networks** (Сети) на панели **Details** (Подробно). Правой кнопкой мыши щелкните внутреннюю сеть и щелкните **Properties** (Свойства).

На вкладке **Firewall Client** (Клиент брандмауэра) установите флажок в поле **Enable Firewall client support for this network** (Разрешить поддержку клиента брандмауэра для этой сети), как показано на рис. 5.10. В разделе **Firewall client configuration** (Настройка клиента брандмауэра) введите имя компьютера брандмауэра ISA Server 2004 в текстовое поле **ISA Server name or IP address** (Имя или IP-адрес ISA Server).

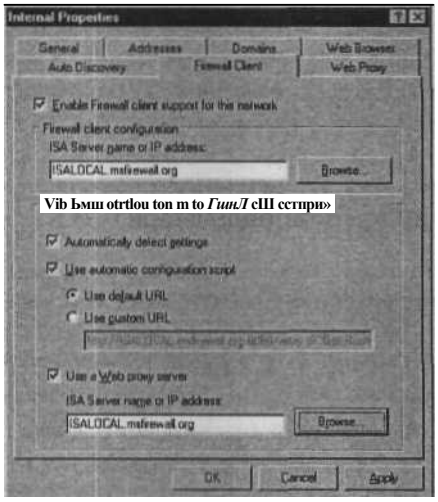


Рис. 5.10. Диалоговое окно внутренних свойств

Стандартная настройка предполагает использование компьютера (так называемое NetBIOS-имя). Однако NetBIOS-имя следует заменить FQDN-именем (Fully Qualified Domain Name, полное имя домена) брандмауэра ISA Server 2004 Когда имя компьютера будет заменено на FQDN-имя, компьютеры клиента брандмауэра смогут использовать службу DNS для корректного разрешения имени брандмауэра **ISA** Server 2004. Это позволит избежать одного из самых распространенных сбоев в работе клиента брандмауэра. Следует убедиться в том, что для этого имени имеется запись на DNS-сервере во внутренней сети. По умолчанию все интерфейсы на брандмауэре ISA Server 2004 автоматически регистрируют свои имена в DNS, но если DNS-сервер не поддерживает динамическое обновление, то придется вручную вводить запись хоста (A) для брандмауэра ISA Server 2004.

ПРИМЕЧАНИЕ Чаще всего при работе с клиентом брандмауэра администраторы брандмауэра ISA Server 2004 сталкиваются с проблемами, связанными с разрешением имен для брандмауэра ISA Server 2004. Если в сети нет DNS-сервера, следует использовать IP-адрес брандмауэра ISA Server 2004 в текстовом поле **ISA Server name or IP address** (Имя или IP-адрес ISA Server). Никогда не следует использовать имя по умолчанию, которое программное обеспечение вводит в это текстовое поле автоматически. Это часто становится причиной сбоев в работе клиента брандмауэра.

Настройки клиента Web-прокси приводятся в разделе **Web browser configuration on the Firewall client computer** (Конфигурирование Web-браузера на компьютере клиента брандмауэра). Эти настройки автоматически конфигурируют Web-браузер в качестве клиента Web-прокси *при установке клиента брандмауэра*. Позже можно изменить эти настройки, тогда Web-браузеры автоматически обновят свои настройки.

Вариант **Automatically detect settings** (Автоматически обнаруживать настройки) позволяет Web-браузеру автоматически обнаруживать службу Web-прокси и конфигурироваться на основании настроек, введенных на вкладке **Web Browser** (Web-браузер) диалогового окна **Internal Properties** (Внутренние свойства). Следует отметить, что автообнаружение основывается на **WPAD-записях** (Web Proxy Auto-Discovery, автобнаружение Web-прокси), размещенных в DNS или DHCP.

Вариант **Use automatic configuration script** (Использовать сценарий автоматической настройки) позволяет присваивать адрес файла PAC (Proxy Autoconfiguration, автоконфигурация прокси) Web-браузеру. Затем Web-браузер установит соединение с указанным ресурсом или с ресурсом по умолчанию. Ресурсом по умолчанию является компьютер брандмауэра ISA Server 2004. Обратите внимание, что при использовании ресурса по умолчанию полученная информация совпадет с информацией, которая была бы получена при настройке браузера на применение варианта **Automatically detect settings** (Автоматически обнаруживать настройки).

Вариант **Use default URL** (Использовать URL по умолчанию) автоматически настраивает браузер на установку соединения с брандмауэром ISA Server 2004 для получения информации об автоматической настройке. Если нужно создать собственный файл PAC, который переписывает настройки *в* автоматически сгенерированном файле на брандмауэре ISA Server 2004, можно воспользоваться вариантом **Use custom URL** (Использовать определяемый пользователем URL). Более подробная информация о файле PAC и файлах автоматической настройки клиента прокси приводится в статье **Using** Automatic **Configuration and Automatic Proxy** (Использование автоматической настройки и автоматического прокси) на сайте www.microsoft.com/resources/documentation/ie/5/all/reskit/en-us/part5/ch21auto.mspx.

Вариант **Use a Web Proxy server** (Использовать сервер Web-прокси) позволяет настроить Web-браузер так, чтобы он использовал брандмауэр ISA Server 2004 в

качестве своего Web-прокси, но при этом он не может воспользоваться возможностями сценариев автоматического конфигурирования. Эта настройка обеспечивает улучшенную производительность Web-браузера по сравнению **с** конфигурацией клиента SecureNAT, но **при** этом нельзя воспользоваться настройками, содержащимися в сценарии автоматического конфигурирования PAC. Наиболее важная настройка в сценарии автоматического конфигурирования включает имена и адреса узлов, которые должны использоваться *для прямого доступа.* Поэтому следует избегать использования этого варианта за исключением тех случаев, когда нужно использовать прямой доступ для того, чтобы обойти Web-прокси при установке соединения с выбранными Web-сайтами.

ПРИМЕЧАНИЕ Конфигурация клиента Web-прокси для поддержки прямого доступа позволяет обходить Web-прокси при установке соединения с выбранными Web-сайтами. Некоторые Web-сайты не соответствуют интернет-стандартам (например, сайты Java), и поэтому они не могут корректно работать с серверами Web-прокси. Эти сайты можно настроить для прямого доступа, тогда клиентские компьютеры не будут пользоваться Web-прокси при установке соединения с этим сайтами, а будут применять альтернативные методы соединения с ними. Для того чтобы клиент использовал альтернативный метод соединения, клиентский компьютер должен быть настроен как клиент брандмауэра и/или клиент SecureNAT.

Щелкните вкладку **Domains** (Домены), как показано на **рис.** 511.

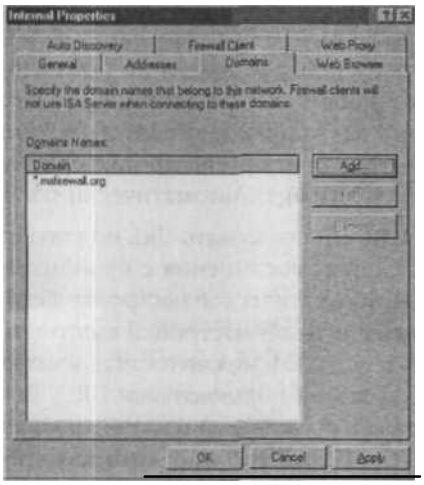


Рис. 5.11. Вкладка Domains (Домены)

На вкладке **Domains** (Домены) указаны домены, при установке соединения с которыми компьютер клиента брандмауэра не будет использовать программное обеспечение клиента брандмауэра. Записи на вкладке **Domains** (Домены) равно-

значны добавлению компьютеров из этих доменов к внутренней сети (или к сети, для которой настроены свойства клиента брандмауэра). Когда клиент брандмауэра устанавливает соединение с хостом, расположенным в одном из доменов, указанных на вкладке **Domains** (Домены), программное обеспечение клиента брандмауэра не используется, а компьютер клиента брандмауэра пытается установить соединение напрямую с хостом-адресатом.

Домены можно добавить, щелкнув кнопку **Add** (Добавить) и выбрав их из диалогового окна **Domain Properties** (Свойства домена), как показано на рис. **5.12.**

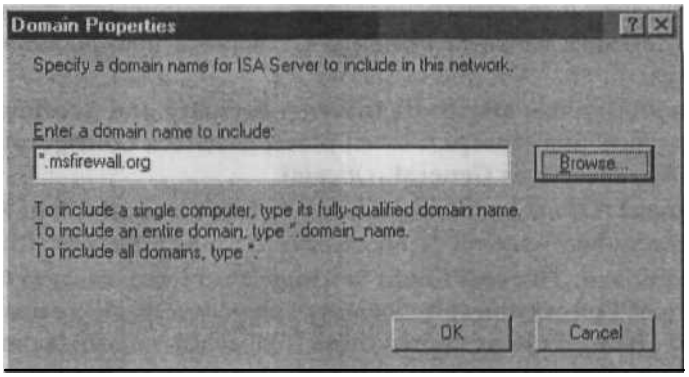


Рис. 5.12. Диалоговое окно **Domain Properties** (Свойства домена)

При указании домена можно использовать групповые символы. Если нужно указать отдельный компьютер, то достаточно ввести FQDN-имя этого хоста. Если необходимо добавить все хосты в отдельном домене, используется звездочка (*) в левой части FQDN-имени. Если нужно, чтобы клиент брандмауэра не применялся ни к каким доменам, следует просто ввести звездочку. После внесения записи щелкните ОК.

На вкладке **Domains** (Домены) нужно всегда вводить все домены внутренней сети, это объясняется тем, что прямые соединения с хостами, расположенными в одном домене, обычно разрешаются.

Например, если члены домена расположены в нескольких подсетях на одном сетевом интерфейсе, представляющем отдельную сеть на брандмауэре ISA Server 2004, то хостам в этой сети для соединения с другими хостами той же сети не нужно использовать брандмауэр ISA Server 2004. Это могло бы привести к ненужной нагрузке на брандмауэр, к тому же в функции сетевого брандмауэра не входит осуществление контроля таких соединений.

Включение поддержки унаследованного клиента брандмауэра/клиентов Winsock-прокси

Клиент брандмауэра ISA Server 2004 использует новый и улучшенный протокол удаленного Winsock-прокси (Remote Winsock Proxy Protocol), который зашифро-

вывает канал соединения между клиентом брандмауэра и службой брандмауэра ISA Server 2004. Это позволяет повысить безопасность, потому что верительные данные пользователя передаются на брандмауэр ISA Server 2004 в прозрачном режиме, когда клиент брандмауэра выполняет запрос на исходящее соединение.

Однако также имеется возможность разрешить незашифрованные соединения клиента Web-прокси с брандмауэром ISA Server 2004. Это может дать время для обновления существующего клиента брандмауэра или клиентов Winsock Proxy 2.0 до программного обеспечения клиента брандмауэра ISA Server 2004.

Чтобы разрешить поддержку незашифрованных соединений клиента брандмауэра для действующих клиентов брандмауэра/Winsock-прокси, выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Конфигурация). Щелкните узел **General** (Общие).
2. В узле **General** (Общие) щелкните ссылку **Define Firewall Client Settings** (Определить настройки клиента брандмауэра) на панели **Details** (Подробно).
3. В диалоговом окне **Firewall Client Settings** (Настройки клиента брандмауэра) щелкните узел **Connection** (Соединение). Установите флажок в поле **Allow non-encrypted Firewall client connections** (Разрешить незашифрованные соединения клиента брандмауэра).
4. Щелкните **Apply** (Применить), а затем щелкните ОК.
5. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
6. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Настройка клиента брандмауэра на стороне клиента

У пользователей, на компьютерах которых установлено программное обеспечение клиента брандмауэра, имеется несколько вариантов настройки. Доступ к этим вариантам можно получить, щелкнув правой кнопкой мыши значок клиента брандмауэра на панели задач и щелкнув команду **Configure** (Настроить).

На вкладке **General** (Общие) (рис. 5.13) диалогового окна **Microsoft Firewall Client for ISA Server 2004** (Клиент брандмауэра Microsoft для ISA Server 2004) установите флажок в поле **Enable Microsoft Firewall Client for ISA Server 2004** (Включить клиент брандмауэра Microsoft для ISA Server 2004).

В варианте **Automatically detect ISA Server** (Автоматически обнаруживать ISA Server) используется WPAD-запись на DHCP- или DNS-сервере для автоматического обнаружения местоположения брандмауэра ISA Server 2004, а затем для автоматического получения конфигурационной информации клиента брандмауэра.

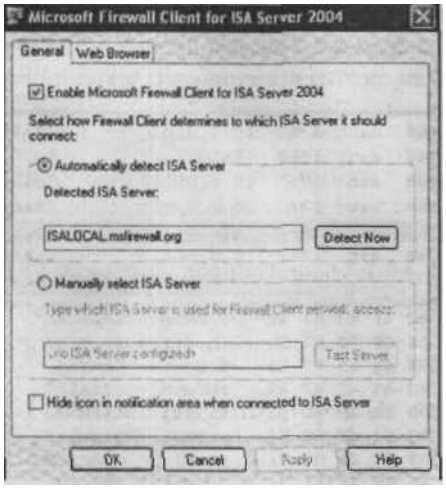


Рис. 5.13. Диалоговое окно **Firewall Client Configuration** (Конфигурация клиента брандмауэра)

На рис. 5.14 показан результат нажатия кнопки **Detect Now** (Обнаружить сейчас).

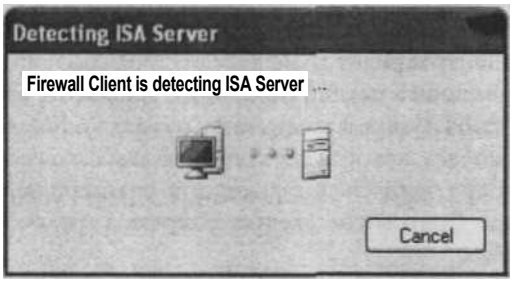


Рис. 5.14. Диалоговое окно Detecting **ISA** Server (Обнаружение ISA Server)

Важно помнить о том, что автообнаружение возможно, только если на DHCP- или DNS-сервере была настроена запись протокола WPAD. Более подробно о том, как настраивать записи протокола WPAD, рассказывается далее в этой главе.

Еще имеется вариант **Manually select ISA Server** (Выбрать ISA Server вручную), позволяющий ввести IP-адрес или DNS-имя брандмауэра ISA Server 2004, а затем щелкнуть кнопку **Test Server** (Протестировать сервер), чтобы найти брандмауэр. Когда вводится IP-адрес, клиент отправляет запрос на порт TCP 1745 и получает информацию об автоматическом конфигурировании напрямую с брандмауэра ISA Server 2004. В информацию об автоматическом конфигурировании включается имя брандмауэра ISA Server 2004, которое приводится в диалоговом окне **Detecting ISA Server** (Обнаружение ISA Server).

Запись монитора сети, представленная на рис. 5.1б, показывает, что соединение выполняется клиентом брандмауэра, а часть информации, полученной клиентом брандмауэра, показана на панели шестнадцатеричного декодирования (Hex decode pane).

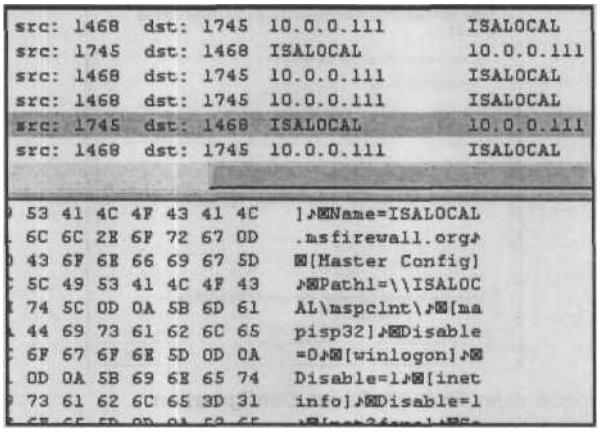


Рис. 5.16. Отслеживание пакетов клиента брандмауэра

Щелкните вкладку **Web Browser** (Web-браузер). Здесь имеется вариант **Enable Web browser automatic configuration** (Включить автоматическое конфигурирование Web-браузера). Этот вариант извлекает информацию из конфигурации Web-браузера, ранее настроенной в панели управления **Microsoft Internet Security and Acceleration Server 2004.** Пользователи могут нажать кнопку **Configure Now** (Выполнить настройку сейчас), которая позволяет пользователям, случайно изменившим настройки браузера, вернуться к исходной оптимальной конфигурации одним нажатием кнопки. Поэтому не следует убирать значок клиента брандмауэра из области уведомления.

СОВЕТ Можно убрать значок клиента брандмауэра из области уведомления, установив флажок в поле Hide icon in notification area when connected to ISA Server (Скрыть значок в области уведомления при соединении с ISA Server). Этот процесс можно автоматизировать, добавив в файл management. ini, расположенный в папке \Documents and Settings\user_name\Local Settings\Application Data\Microsoft\Firewall Client 2004, следующую запись [TrayIcon] TrayIconVisualState=1

Можно использовать сценарий входа в систему для размещения этого файла в каталоге пользователя. Более подробная информация о настройках конфигурационного файла клиента брандмауэра представлена в следующем разделе.

Файлы конфигурации клиента брандмауэра

Программное обеспечение клиента брандмауэра принимает централизованные настройки, установленные на компьютере ISA Server 2004. Эти настройки определяют такие параметры, как автоматическая конфигурация клиентов Web-прокси, имя ISA Server и автоматическое обнаружение ISA Server. После установки программного обеспечения клиента брандмауэра ISA Server обновляет эти настройки клиента всякий раз, когда компьютер клиента перезапускается, и каждые шесть часов после выполнения начального обновления. Эти настройки также обновляются всякий раз, когда пользователь нажимает кнопку **Test Server** (Протестировать сервер).

Помимо этих настроек ISA Server автоматически обновляет на клиенте брандмауэра информацию об IP-адресах, которые клиент должен считать локальными (имеется в виду «внутренняя сеть» для этого конкретного клиента брандмауэра).

Практически для всех приложений Winsock подходит стандартная конфигурация клиента брандмауэра, и в нее не нужно вносить никаких изменений. Однако иногда бывают ситуации, когда нужно изменить стандартные настройки. Клиента брандмауэра можно настроить для каждого пользователя и для каждого компьютера на компьютере клиента брандмауэра, путем внесения изменений в ini-файлы, установленные на компьютере клиента брандмауэра.

Для всех компонентов после установки можно изменить их стандартные настройки. Новые настройки вступят в силу только после обновления конфигурации клиента.

Файлы конфигурации

Информация о конфигурации хранится в группе файлов, которые устанавливаются на компьютере клиента брандмауэра. Когда производится установка клиента брандмауэра, на компьютере клиента брандмауэра создаются следующие файлы (они также показаны на рис. 5.17):

- файл **common.ini,** определяющий общую конфигурацию для всех приложений;
- файл management.ini, определяющий настройки управления клиентом бранд мауэра.

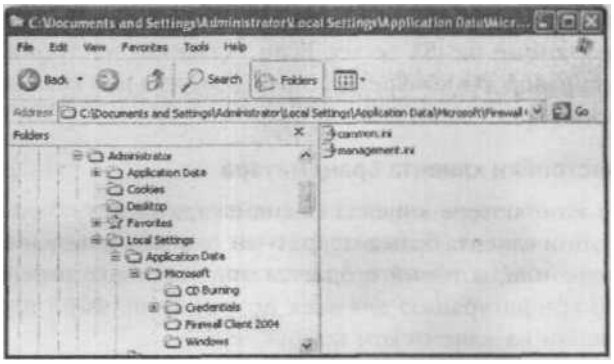


Рис. 5.17. Файлы конфигурации клиента брандмауэра

Эти файлы создаются для всех пользователей, выполняющих вход на компьютер, могут создаваться для каждого пользователя компьютера по отдельности. Настройки для каждого пользователя замещают общие настройки, которые применяются ко всем пользователям одного и того же компьютера клиента брандмауэра. Эти файлы создаются в разных местах в зависимости от операционной системы. К сожалению, у нас есть только информация о том, где расположены эти файлы на компьютере на базе ОС Windows XP. Для конкретной версии Windows можно определить расположение этих файлов с помощью функции **Search** (Поиск).

В компьютерах на базе ОС Windows XP эти файлы расположены в папке:

- \Documents and Settings\All Users\\Local Settings\Application Data\Microsoft\Firewall Client 2004;
- \Documents and *Settmgs\uMa_nojib3oeamejia\Loc2L* Settings\Application Data\Microsoft\Firewall Client 2004.

Помимо этих файлов пользователь может создать еще один файл под названием application.ini, содержащий информацию о конфигурации конкретных приложений.

Существует порядок предшествования, определяющий, как файлы configuration.ini обрабатываются клиентом брандмауэра:

1. Первыми обрабатываются ini-файлы в папке пользователя. Все настройки из этих файлов используются клиентом брандмауэра для определения поведения кли ента брандмауэра и приложений, зависящих от клиента брандмауэра.
2. Затем клиент брандмауэра обращается к папке **Documents and Settings\All Users.** Применяются все *дополнительные* конфигурационные настройки. Нсли указанная настройка противоречит настройкам, установленным для конкретного пользователя, то брандмауэр ее игнорирует. Настройки в папке пользователя всегда обрабатываются первыми.
3. Клиент брандмауэра обнаруживает компьютер ISA Server, с которым он должен установить соединение, и получает настройки с компьютера брандмауэра ISA Server 2004.
4. После получения настроек с брандмауэра ISA Server 2004, клиент брандмауэра проверяет настройки уровня сервера. Применяются все конфигурационные настройки, указанные на ISA Server. Если указанная настройка противоречит настройке, указанной для конкретного пользователя или компьютера, то бранд мауэр ее игнорирует.

Расширенные настройки клиента брандмауэра

Пользователь на компьютере клиента брандмауэра может создавать и изменять файлы конфигурации клиента брандмауэра и настраивать поведение клиента брандмауэра. Файл *common.ini,* который создается при установке клиента брандмауэра, содержит общую конфигурацию для всех приложений. Файл *application.ini* контролирует настройки на клиентском компьютере.

Эти файлы могут быть созданы для всех клиентов, выполняющих вход на компьютер, и для отдельных пользователей на одном компьютере. Настройки отдельных пользователей имеют больший приоритет, чем настройки, применяемые ко всем пользователям компьютера. Также можно воспользоваться консолью управления Microsoft Internet Security and Acceleration Server 2004 для изменения настроек клиента брандмауэра.

В табл. 5.6 показаны записи, которые можно включить при настройке приложений клиента брандмауэра. В первом столбце приводятся ключи, которые можно добавить в файлы конфигурации. Второй столбец описывает значения, которые можно присвоить этим ключам.

Не следует забывать о том, что некоторые настройки можно установить *только на компьютере клиента брандмауэра,* а не в консоли управления Microsoft Internet Security and Acceleration Server 2004. Табл. 5.6. Настройки файла конфигурации клиента брандмауэра

Запись	Описание
Serve rName	Указывается имя компьютера ISA Server, с которым должен установить соединение клиент брандмауэра Возможные значения: 0 и 1. Если установлено значение 1, приложение клиента брандмауэра отключается для конкретного приложения клиента
Disable	Возможные значения: 0 и 1. Если установлено значение 1, клиент брандмауэра отключается для конкретного приложения клиента. Применяется только к клиенту брандмауэра для ISA Server 2004. Если эта запись задана, то запись Disable не учитывается
DisahlcEx	(Устанавливается только на компьютере клиента брандмауэра). Возможные значения: 0 и 1. При установке значения 1, приложение клиента брандмауэра автоматически находит компьютер ISA Server, с которым оно должно установить соединение
Autodetection N	Возможные значения: L или R. По умолчанию десятичное представление с разделительными точками или имена доменов Интернета перенаправляются на компьютер ISA Server, чтобы пройти разрешение имен, а все остальные имена разрешаются на локальном компьютере. При установке значения R, все имена перенаправляются на компьютер ISA Server для разрешения. При установке значения L, все имена разрешаются на локальном компьютере
a meResol u do n	Указывается локальный TCP-порт, список или диапазон
	Указывается локальный UDP-порт, список или диапазон
LocalBindTcpPorts	Указывается удаленный TCP-порт, список или диапазон
LocalBindUdpPorts	Указывается удаленный UDP-порт, список или диапазон
Rem o te B i ndTcp Ports	Указывается TCP-порт, список или диапазон для всех портов,
Re mo teB indUdpPor ts	которые должны принимать несколько подключений
Se rve rB in dTcpPorts	

(см. след. стр.)

Табл. 5.6 (окончание)

Запись	Описание
Persistent	Возможные значения: 0 и 1. При установке значения 1 на компьютере ISA Server сохраняется определенное состояние сервера при остановке и перезапуске службы и если сервер не отвечает. Если сервер не отвечает, клиент попытается восстановить состояние прослушивающих сокетов после перезапуска сервера
ForceCredentials	(Устанавливается только на компьютере клиента брандмауэра). Используется при запуске службы Windows или серверного приложения в качестве приложения клиента брандмауэра. Если значение установлено на 1, то для проверки подлинности используются альтернативные верительные данные пользователя, хранящиеся на компьютере, на котором запущена эта служба. Верительные данные пользователя хранятся на клиентском компьютере с помощью приложения Credtool.exe, поставляемого вместе с программным обеспечением клиента брандмауэра. Верительные данные пользователя должны соответствовать учетной записи пользователя, подлинность которой может быть проверена ISA Server. Учетная запись пользователя обычно не имеет срока действия. Иначе пришлось бы обновлять верительные данные пользователя всякий раз, когда срок действия учетной записи заканчивается
NameResolution ForLocalHost	Возможные значения: L (по умолчанию), P или E. Используется для того, чтобы указать, как разрешается локальное имя компьютера (клиента) **при** вызове gethostbyname API. Имя компьютера LocalHost разрешается при вызове функции Winsock API gethosbyname с помощью строки LocalHost, пустой строки или нулевого указателя строки. Приложения Winsock вызывают gethostbyname (LocalHost), чтобы узнать свои локальные IP-адреса и отправить их на Интернет-сервер. Если установлено значение L, gethostbynameO возвращает IP-адреса компьютера локального хоста. Если установлено значение P, gethostbynameO возвращает только внешние IP-адреса компьютера ISA Server — IP-адреса, не входящие в таблицу локальных адресов
ControlChannel	Возможные значения: Wsp.udp или Wsp.tcp (стандартное значение). Указывается тип используемого контрольного канала

Секреты ISA Server 2004

Файлы конфигурации клиента брандмауэра могут оказаться очень полезными в нескольких случаях, один из которых — публикация серверов с помощью программного обеспечения клиента брандмауэра и файла конфигурации. Например, с помощью ISA Server 2000 и Proxy Server 2.0, можно было создать файл wspcfg.ini на опубликованном сервере и разместить этот файл

в том же каталоге, что и приложение, которое нужно было опубликовать. Это позволяет публиковать сложные протоколы, не пользуясь фильтрами приложений. Однако для ISA Server 2004 не существует документации по созданию аналогичного файла wspcfg.ini.

Настройка клиента брандмауэра на брандмауэре ISA Server 2004

Файлы конфигурации, расположенные на компьютере локального клиента брандмауэра, во время написания данной книги остаются не совсем понятными, а централизованная настройка клиента брандмауэра, выполняемая в консоли управления **Microsoft Internet Security and Acceleration Server 2004,** остается такой же полезной, как и в брандмауэре ISA Server 2000. Доступ к интерфейсу централизованной настройки клиента брандмауэра можно получить, открыв консоль управления **Microsoft Internet Security and Acceleration Server 2004,** а затем развернув имя сервера и узел **Configuration** (Настройка). Щелкните узел **General** (Общие), а затем щелкните ссылку **Define Firewall Client Settings** (Определить настройки клиента брандмауэра) (см. рис. 518).

Define Firewall Client Settings

Рис. 5.18. Ссылка Define Firewall Client Settings (Определить настройки клиента брандмауэра)

Щелкните вкладку **Application Settings** (Настройки приложения). Список настроек встроенного приложения клиента брандмауэра показан на рис. 5-19.

Рис. **5.19.** Диалоговое окно **Firewall Client Settings** (Настройки клиента брандмауэра)

Эти настройки применяются ко всем клиентам брандмауэра, которые получают свои настройки с брандмауэра ISA Server 2004. Например, имеется настройка outlook Disable 0 (показана настройка outlook Disable 1). Эта настройка указывает программному обеспечению клиента брандмауэра не использовать настройки клиента брандмауэра для приложения Microsoft Outlook. Эта важная настройка позволяет клиенту Outlook получать правильные уведомления о новой почте

Одна особая функция настроек клиента брандмауэра состоит в том, чтобы блокировать приложения. Например, нужно запретить пользователям применять приложение kazaa.exe. Чтобы заблокировать это приложение, можно использовать ключ Disable. Для этого выполните следующие действия:

1. В диалоговом окне **Firewall Client Settings** (Настройки клиента брандмауэра) на вкладке **Application Settings** (Настройки приложения) щелкните **New** (Новый).
2. В диалоговом окне **Application Entry Settings** (Настройки записи приложения) введите **Kazaa** (Без расширения файла) в текстовое поле **Application** (Прило жение). Выберите **Disable** (Запретить) из выпадающего списка **Key** (Ключ). Вы берите значение 1 из списка **Value** (Значение).
3. Щелкните ОК.
4. В списке **Settings** (Установки) появится новая запись **kazaa.** Щелкните **Apply** (Применить), а затем ОК.
5. Щелкните **Apply** (рис. 5-20), чтобы сохранить изменения и обновить политику брандмауэра.

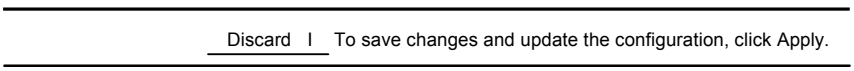


Рис. 5.20. Применение изменений к конфигурации брандмауэра

6. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Теперь все пользователи, у которых установлено программное обеспечение клиента брандмауэра, не смогут пользоваться приложением kazaa.exe.

ПРЕДУПРЕЖДЕНИЕ Пользователи могут избежать использования подобной конфигурации, переименовав исполняемый файл. Для того чтобы полностью заблокировать приложение kazaa, нужно настроить фильтр защиты HTTP и ограничить доступ пользователей протоколом HTTP или купить фильтр приложения стороннего производителя, например Akonix L7, для продукта ISA Server (www.akonix.com), который может определять одноранговые приложения.

Клиент Web-прокси ISA Server 2004

В качестве клиента Web-прокси может выступать любой компьютер, браузер которого настроен на использование брандмауэра ISA Server 2004 в качестве своего сервера Web-прокси. Для того чтобы настроить компьютер в качестве клиента Web-прокси, не нужно устанавливать на нем никакое новое программное обеспечение. Единственное требование состоит в том, чтобы настроить браузер на клиентском компьютере на использование брандмауэра ISA Server 2004 в качестве его Web-прокси. Web-браузер является не единственным приложением, которое может быть настроено в качестве клиента Web-прокси. Другие приложения, например программы обмена сообщениями или клиенты электронной почты, также могут быть настроены в качестве клиентов Web-прокси.

Далее перечислены преимущества конфигурации клиента Web-прокси:

- улучшенная производительность конфигурации клиента брандмауэра и клиента SecureNAT для обеспечения Web-доступа;
- способность использовать сценарий автоматического конфигурирования, чтобы обходить сайты с помощью прямого доступа;
- позволяет обеспечивать Web-доступ (HTTP/HTTPS/FTP), не разрешая пользователям доступ к другим протоколам;
- позволяет осуществлять пользовательский/групповой контроль доступа для Web-доступа;
- поддерживает проверку подлинности RADIUS для исходящих запросов клиента Web-прокси;
- позволяет ограничить количество исходящих соединений клиента Web-прокси;
- поддерживает создание цепочек Web-прокси, которые могут ускорить доступ к Интернету.

Улучшенная производительность конфигурации клиента брандмауэра и клиента SecureNAT для обеспечения Web-доступа

Компьютеры клиента Web-прокси взаимодействуют с брандмауэром ISA Server 2004 напрямую через фильтр Web-прокси брандмауэра. Клиент Web-прокси устанавливает прямое соединение с портом TCP 8080 на брандмауэре ISA Server 2004. Порт TCP 8080 используется приемником Web-прокси брандмауэра ISA Server 2004. Приемник прослушивает исходящие Web-запросы, а затем применяет к этим соединениям политики доступа брандмауэра. Это повышает производительность, потому что соединения с клиентов брандмауэра и SecureNAT должны передаваться на фильтр Web-прокси вместо того, чтобы фильтр получал их напрямую. В процессе тестирования становится ясно, что компьютеры клиента Web-прокси получают доступ к Web-содержимому заметно быстрее.

Способность использования сценария автоматического конфигурирования, чтобы обходить сайты с помощью прямого доступа

Одна из наиболее полезных функций конфигурации клиента Web-прокси состоит в ее способности использовать прямой доступ для того, чтобы обходить фильтр Web-прокси для выбранных Web-сайтов. Предполагается, что компьютер клиента Web-прокси настроен на использование сценария автоматического конфигурирования. Существуют два способа настройки клиента Web-прокси для использования сценария автоматического конфигурирования:

- ручная настройка клиента на использование сценария автоматического конфи гурирования;
- настройка WPAD-записей в DNS и/или DHCP и настройка клиента Web-прокси на использование автоматического обнаружения для получения доступа к кон фигурационной информации;

Можно вручную настроить браузер клиента Web-прокси на использование сценария автоматического конфигурирования. Любое приложение, которое извлекает свою конфигурацию из настроек Web-браузера, также может воспользоваться преимуществом сценария автоматического конфигурирования. Приложения, которые не извлекают свою конфигурацию из Web-браузера, вряд ли могут воспользоваться настройками сценария автоматического конфигурирования.

Более эффективный метод применения сценария автоматического конфигурирования к клиентам Web-прокси состоит в том, чтобы использовать WPAD-заииси а DNS и/или DHCP. Информация из WPAD-записей указывает клиенту Web-прокси на IP-адрес брандмауэра ISA Server 2004, с которого клиент Web-прокси получает настройки автоматического конфигурирования.

Поддержка сценария автоматического конфигурирования очень важна для тех клиентов Web-прокси, которые хотят получить доступ к определенным узлам Java и также к электронной почте Hotmail. Автоматическое конфигурирование обеспечивает централизованный список Web-сайтов, к которым можно получить доступ с помощью Direct Access (прямой доступ). Когда эти сайты настроены на прямой доступ, компьютер клиента Web-прокси будет использовать не фильтр Web-прокси, а другие методы, например конфигурацию клиента SecureNAT или брандмауэра для установки соединения с этим Web-сайтом.

Возможность обеспечения Web-доступа (HTTP/HTTPS/FTP) без разрешения пользователям доступа к другим протоколам

Конфигурация клиента Web-прокси позволяет предоставлять доступ к Интернету пользователям, которым не требуется весь набор протоколов Интернета для установления соединения с ним. Клиент Web-прокси поддерживает только протоколы HTTP, HTTPS (SSL/TLS-over-HTTP) и FTP-загрузки по HTTP-туннелю. Если компью-

тер пользователя настроен *только* как клиент Web-прокси, то пользователь этого компьютера имеет доступ только к этим протоколам.

Клиенты Web-прокси используют туннельное соединение, когда они отправляют свои интернет-запросы на брандмауэр ISA Server 2004. Например, когда пользователь отправляет запрос к сайту **www.microsoft.com,** клиент Web-прокси добавляет к этому запросу еще один HTTP-заголовок, в котором в качестве адреса назначения указан внутренний интерфейс компьютера брандмауэра ISA Server 2004, а в качестве порта назначения — порт TCP 8080. Когда брандмауэр ISA Server 2004 получает этот запрос, он отбрасывает заголовок клиента Web-прокси и перенаправляет запрос на сервер **www.microsoft.com** в Интернете.

Точно так же, когда клиент Web-прокси отправляет FTP-запрос на узел типа **ftp://ftp.microsoft.com,** клиент Web-прокси добавляет к этому FTP-запросу такой же HTTP-заголовок, в котором в качестве адреса назначения указан внутренний интерфейс брандмауэра ISA Server 2004, а в качестве порта назначения — порт TCP 8080. Когда брандмауэр ISA Server 2004 получает этот запрос, он удаляет HTTP-заголовок и перенаправляет запрос на FTP-сервер ftp.microsoft.com в виде FTP-запроса, а не HTTP-запроса. Поэтому поддержка протокола FTP клиентом Web-прокси обозначается как поддержка FTP по HTTP-туннелю.

> ПРИМЕЧАНИЕ При использовании клиента Web прокси для FTP-соединений клиент Web-прокси может выполнить только *загрузку* по протоколу FTP. Для того чтобы клиентский компьютер мог поддерживать размещение данных по протоколу FTP, он должен быть настроен как клиент SecureNAT или клиент брандмауэра.

Возможность осуществления пользовательского/группового контроля доступа для Web-доступа

Клиент Web-прокси способен отправлять верительные данные пользователя на компьютер брандмауэра ISA Server 2004, только когда это необходимо, в отличие от клиента брандмауэра, который отправляет верительные данные пользователя на брандмауэр ISA Server 2004 всегда. Это улучшает производительность, т. к. проверка подлинности выполняется только по требованию. Если клиент Web-прокси имеет доступ к правилу доступа, которое разрешает доступ к сайту и содержимому, указанному в запросе, и если это правило доступа разрешает анонимный доступ (разрешает доступ к этому правилу для всех пользователей), то клиент Web-прокси не отправляет верительные данные и соединение разрешается.

Эта функция объясняет большое количество анонимных записей, появившихся в системных журналах брандмауэра. Когда клиент Web-прокси отправляет запрос на брандмауэр ISA Server 2004, первая попытка соединения не включает в себя верительные данные пользователя клиента Web-прокси. Этот запрос обрабатывается как анонимный. Если доступ к узлу предполагает предъявление верительных

данных пользователя, то брандмауэр ISA Server 2004 отправит сообщение «access denied» (доступ запрещен) на компьютер клиента Web-прокси и потребует проверки подлинности пользователя. Как показано на рис. 5.21, в данной ситуации клиент Web-прокси может пройти проверку подлинности, используя ряд различных протоколов проверки подлинности.

Для сеанса Web-прокси можно использовать следующие протоколы проверки подлинности:

- интегрированный протокол проверки подлинности Windows;
- протокол базовой проверки подлинности;
- протокол проверки подлинности Digest;
- протокол проверки подлинности клиентских сертификатов;
- протокол проверки подлинности RADIUS.

ПРЕДУПРЕЖДЕНИЕ Web-браузеры могут использовать интегрированную, базовую проверку подлинности, проверку подлинности Digest, RADIUS и клиентских сертификатов. Важно отметить, что Web-браузеры могут использовать только проверку подлинности клиентских сертификатов при установке соединения с опубликованными ресурсами по правилу Web-публикации. Клиенты Web-браузера, выступающие в роли клиентов Web-прокси, не могут использовать проверку подлинности клиентских сертификатов при получении доступа к ресурсам через брандмауэр ISA Server 2004 по правилу доступа.

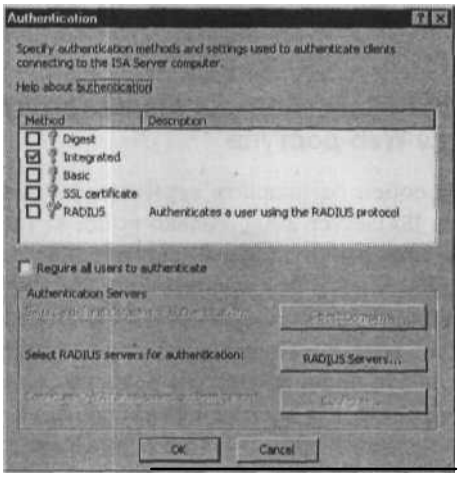


Рис. 5.21. Диалоговое окно проверки подлинности

Верительные данные передаются на брандмауэр ISA Server 2004 в прозрачном режиме, если включена интегрированная проверка подлинности. Однако и брандмауэр ISA Server 2004, и клиент Web-прокси должны быть членами одного домена,

или же брандмауэр ISA Server 2004 должен использовать проверку подлинности RADIUS для того, чтобы установить соединение с Active Directory или базой данных учетных записей пользователей Windows NT 4.0. Добиться прозрачной проверки подлинности можно также, если зеркально отобразить учетные записи пользователей в локальный SAM на компьютере брандмауэра ISA Server 2004. Однако для всех более-менее крупных организаций административные трудозатраты и риск от зеркального отображения учетных записей пользователей могут быть неоправданно большими.

Проверка подлинности по SSL-сертификатам в настоящее время недоступна для браузера для соединений сервера Web-прокси. Проверку подлинности по SSL-сертификатам можно использовать при настройке создания цепочек Web-прокси. В таком случае нижестоящий сервер Web-прокси перенаправляет Web-запросы на вышестоящий сервер Web-прокси. Нижестоящий сервер Web-прокси ISA Server 2004 может пройти проверку подлинности на вышестоящем сервере, представив ему клиентский сертификат. Благодаря этому конфигурация цепочки Web-прокси становится очень защищенной. При использовании других решений Web-прокси не так просто добиться такого же результата.

Имя пользователя и пароль пользователи должны вводить, только если используется базовая проверка подлинности. Если клиент Web-прокси и брандмауэр ISA Server 2004 не являются членами одного домена или не используется служба проверки подлинности RADIUS, то базовая проверка подлинности является наилучшим вариантом.

Новая функция ISA Server 2004 — способность использовать RADIUS для проверки подлинности Web-прокси. Когда RADIUS используется в качестве протокола проверки подлинности для клиентов Web-прокси, брандмауэр ISA Server 2004 не должен быть членом домена пользователя. Это обеспечивает немного более высокий *уровень* безопасности, потому что атакующий, которому удалось завладеть управлением брандмауэром ISA Server 2004, не сможет использовать доменные верительные данные, чтобы атаковать пользователей в защищенной сети брандмауэра ISA Server 2004. Когда пользователь домена пытается пройти проверку подлинности для установления соединения с Интернетом, брандмауэр ISA Server 2004, который не является членом домена пользователя, перенаправляет запрос на проверку подлинности на сервер RADIUS во внутренней сети. Сервер RADIUS перена-правляет запрос на сервер проверки подлинности, а затем возвращает ответ на брандмауэр ISA Server 2004.

Следует обратить внимание, что при настройке брандмауэра ISA Server 2004 для поддержки проверки подлинности RADIUS брандмауэр становится клиентом RADIUS. Можно использовать любой сервер RADIUS, включая реализацию службы RADIUS от Microsoft — сервер IAS (Internet Authentication Server, сервер проверки подлинности для Интернета).

Проверка подлинности RADIUS не требует создания сервера RADIUS во внутренней сети и настройки приемника Web-прокси для сети клиента Web-прокси на использование сервера RADIUS. Кроме того, должно иметься правило доступа, разрешающее брандмауэру ISA Server 2004 взаимодействовать с сервером RADIUS по протоколу RADIUS. Существует стандартная системная политика брандмауэра, разрешающая сообщения от службы RADIUS во внутреннюю сеть. Если сервер RADIUS не расположен во внутренней сети, то нужно настроить системную политику брандмауэра, чтобы разрешить протокол RADIUS к серверу RADIUS в другом месте.

Далее в этой главе рассматриваются методики создания сервера RADIUS и настройки клиента RADIUS. Для обеспечения поддержки клиентов Web-прокси необходимо выполнить следующие действия:

- настроить приемник исходящих Web-запросов на использование проверки подлинности RADIUS;
- настроить учетную запись пользователя для разрешения удаленного доступа (Remote Access Permission) или настроить политики удаленного доступа для разрешения доступа;
- настроить политику удаленного доступа для поддержки проверки подлиннос ти по протоколу PAP (Password Authentication Protocol, протокол аутентифика ции пароля).

Для того чтобы настроить приемник Web-прокси в сети клиента Web-прокси на использование RADIUS, нужно сделать следующее:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Конфи гурация). Щелкните узел **Networks** (Сети) и правой кнопкой мыши щелкните **Internal network** (Внутренняя сеть) (при условии, что клиенты Web-прокси рас положены во внутренней сети). Щелкните **Properties** (Свойства).
2. В диалоговом окне **Internal Properties** (Внутренние свойства) щелкните вкладку **Web Proxy** (Web-прокси).
3. На вкладке **Web Proxy** (Web-прокси) щелкните кнопку **Authentication** (Про верка ПОДЛИННОСТИ),
4. В диалоговом окне **Authentication** (Проверка подлинности) снимите флажки во всех полях. Появятся диалоговое окна, сообщающие о том, что других мето дов проверки подлинности нет в наличии. Подтвердите, что выбран только ва риант RADIUS (рис. 5.22).
5. Щелкните **RADIUS Servers** (Серверы RADIUS).
6. В диалоговом окне **Add RADIUS Server** (Добавить сервер RADIUS) (рис. 5.23) вве дите имя или IP-адрес для сервера **RADIUS** в текстовое поле **Server** name (Имя сервера). Введенное имя должно быть FQDN-именем, и брандмауэр ISA Server 2004 должен быть способен разрешить это имя в правильный IP-адрес. Введите опи сание сервера в текстовое поле Server description (Описание сервера). Оставьте в полях **Port** (Порт) и **Time-out** (seconds) (Тайм-аут, секунды) значения по умол-

чанию, если нет причин их менять. Установите флажок в поле Always use message authenticator (Всегда использовать удостоверения сообщений).

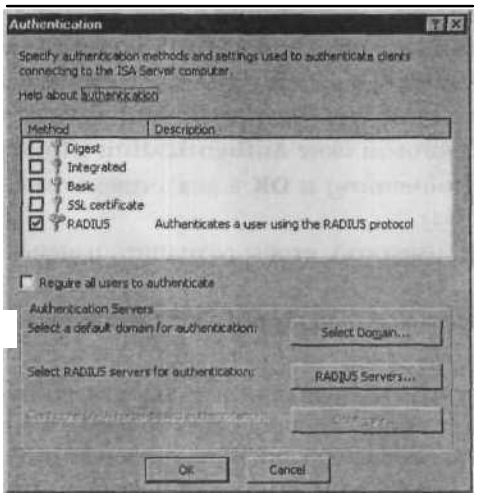


Рис. 5.22. Диалоговое окно Authentication (Проверка подлинности)

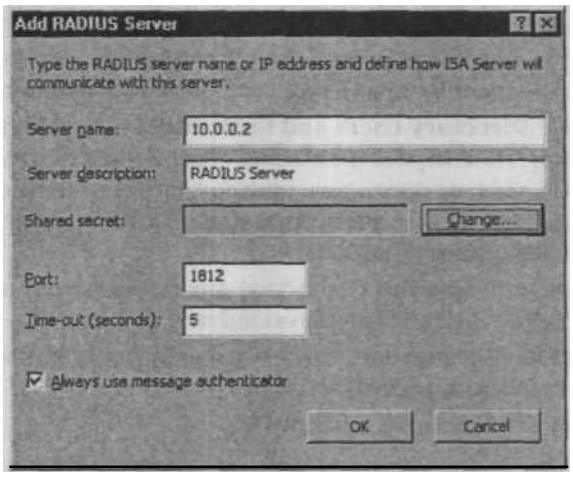


Рис. 5.23. Диалоговое окно Add RADIUS Server (Добавить сервер RADIUS)

7. Щелкните Change (Изменить).
8. В диалоговом окне Shared Secret (Общий пароль) введите и подтвердите па роль в текстовые поля New secret (Новый пароль) и Confirm new secret (Под твердить новый пароль). Этот пароль используется для проверки подлинности сервера RADIUS и клиента RADIUS. Это должен быть тот же пароль, что исполь зовался при настройке клиента RADIUS на сервере RADIUS для внутренней сети.

Щелкните OK. (Обратите внимание: пароль RADIUS должен быть длинным и сложным; в идеале пароль RADIUS должен состоять из 24 символов, и он создается с помощью приложения генерации паролей.)

9. Щелкните OK в диалоговом окне **Add RADIUS Server** (Добавить сервер RADIUS).
10. Теперь в списке появится запись для сервера RADIUS. Можно создать несколько серверов RADIUS, в списке они будут располагаться друг за другом.
11. Щелкните OK в диалоговом окне **Authentication** (Проверка подлинности).
12. Щелкните **Apply** (Применить) и OK в диалоговом окне **Internal Properties** (Внутренние свойства).
13- Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
14. Щелкните OK в диалоговом окне **Apply New** Configuration (Применить новую конфигурацию).

Теперь нужно настроить учетную запись пользователя, чтобы разрешить соединение через телефонную линию. Эта процедура не требуется, если домен находится в автономном режиме Windows 2000 или Windows Server 2003. Это объясняется тем, что политику доступа можно контролировать с помощью политики удаленного доступа, а стандартная настройка для учетных записей контролирует доступ посредством политики удаленного доступа, когда домен находится в автономном режиме. Поэтому настоятельно рекомендуется включить автономный режим для доменов Windows для того, чтобы не нужно было настраивать каждую учетную запись пользователя на применение соединения через телефонную линию.

1. В консоли **Active Directory Users and Computers** (Пользователи и компьюте ры Active Directory) на контроллере домена, содержащем учетные записи пользо вателей, которые должны проходить проверку подлинности с помощью служ бы RADIUS, дважды щелкните учетную запись, для которой необходимо разре шить проверку подлинности RADIUS.
2. В диалоговом окне **Properties** (Свойства) для пользователя щелкните вкладку **Dial-in** (Соединение через телефонную линию).
3. На вкладке **Dial-in** (Соединение через телефонную линию) выберите вариант **Allow access** (Разрешить доступ).
4. Щелкните **Apply** (Применить), а затем OK.

Теперь учетная запись пользователя будет использовать службу RADIUS для проверки подлинности Web-прокси.

Наконец, нужно настроить политику удаленного доступа так, чтобы для проверки подлинности RADIUS клиента Web-прокси поддерживался протокол PAR Важно отметить, что проверка подлинности по протоколу PAP не является безопасной, и нужно использовать методы защиты верительных данных, передаваемых между брандмауэром ISA Server 2004 и сервером RADIUS. Предпочтительный метод защиты верительных данных состоит в применении соединения в транспортном режиме IPSec.

Для настройки политики удаленного доступа выполните следующее:

1. На IAS-сервере (Internet Authentication Server, сервер аутентификации Интернета) во внутренней сети щелкните **Start** (Пуск) и выберите **Administrative Tools** (Панель управления). Щелкните **Internet Authentication Services** (Службы проверки подлинности Интернет).
2. В консоли **Internet Authentication Services** (Службы проверки подлинности Интернет) щелкните узел **Remote Access Policies** (Политики удаленного доступа) на левой панели консоли.
3. *В* узле **Remote Access Policies** (Политики удаленного доступа) на правой панели консоли размещаются две политики удаленного доступа. Первая политика применяется только к RAS-соединениям от коммутируемых и VPN-клиентов. Вторая политика, **Connections to other access servers** (Соединения с другими серверами доступа), используется клиентами Web-прокси. Дважды щелкните вторую политику.
4. В диалоговом окне **Connections to other access servers Properties** (Свойства соединений с другими серверами доступа) щелкните **Edit Profile** (Редактировать профиль).
5. В диалоговом окне **Edit Dial-in Profile** (Изменить профиль набора) щелкните вкладку **Authentication** (Проверка подлинности).
6. На вкладке **Authentication** (Проверка подлинности) установите флажок в поле **Unencrypted authentication** (PAP, SPAP) (Незашифрованная проверка подлинности, PAP, SPAP).
7. Щелкните **Apply** (Применить) и OK.

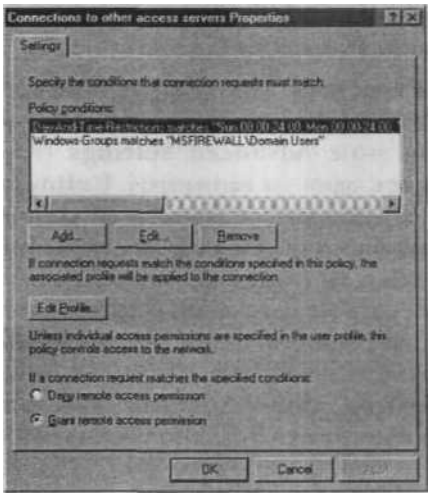


Рис. 5.24. Диалоговое окно Connections to other Access Servers Properties (Свойства соединений с другими серверами доступа)

8. В диалоговом окне **Connections to other access servers Properties** (Свойства соединений с другими серверами доступа) (рис. 5.24) проверьте, что добавлена запись Windows-Groups matches..., включающая группы пользователей, которые будут получать доступ к службе Web-прокси после прохождения проверки подлинности RADIUS. Используйте кнопку **Add** (Добавить), чтобы добавить группу. Также должен быть выбран вариант **Grant remote access permission** (Разрешить удаленный доступ).
9. Щелкните **Apply** (Применить) и ОК в диалоговом окне **Connections to other access server Properties** (Свойства соединений с другими серверами доступа).

Эта политика сразу же вступит в силу, никакое оборудование перезапускать не нужно.

Возможность ограничения количества исходящих соединений клиента Web-прокси

Количество соединений клиента Web-прокси может быть ограничено определенным числом. Это может оказаться полезным, если пропускная способность ограничена или нужно сделать так, чтобы лишь определенное количество пользователей получало доступ к Интернету одновременно.

Установить значение количества одновременных соединений клиента Web-прокси можно в диалоговом окне **Properties** (Свойства) сети, из которой клиенты Web-прокси получают доступ к Интернету. В панели управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Конфигурация). Щелкните узел **Networks** (Сети) в левой панели консоли и правой кнопкой мыши щелкните сеть на панели **Details** (Подробно). Щелкните команду **Properties** (Свойства).

В диалоговом окне **Properties** (Свойства) сети щелкните вкладку **Web Proxy** (Web-прокси). На вкладке **Web Proxy** (Web-прокси) щелкните **Advanced** (Расширенные). В диалоговом окне **Advanced Settings** (Расширенные настройки) (рис. 5.25) можно выбрать один из вариантов: **Unlimited** (Неограниченное) и **Maximum** (Максимальное). При выборе варианта **Maximum** (Максимальное) можно ввести значение максимального количества одновременных **соединений.** Имеется также значение **Connection timeout (seconds)** (Тайм-аут соединения, секунды), которое тоже можно изменить. По умолчанию установлено 120 секунд. Можно уменьшить или увеличить это значение по своему желанию. Если окажется, что незанятые соединения сокращают количество разрешенных одновременных соединений, то можно уменьшить значение тайм-аута. Если же пользователи жалуются на то, что сеансы работы в Интернете слишком быстро прерываются, можно увеличить значение тайм-аута.

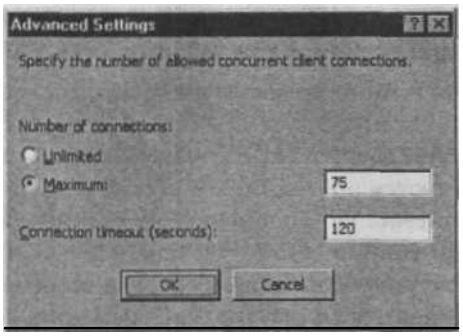


Рис. 5.25. Диалоговое окно **Advanced Settings** (Расширенные настройки)

Поддержка создания цепочек Web-прокси, которые могут ускорить доступ к Интернету

Создание цепочек Web-прокси позволяет соединить ISA Server 2004, брандмауэр ISA Server 2004 и серверы Web-прокси друг с другом. Соединение брандмауэра ISA Server 2004 и серверов Web-прокси представляет собой цепочку, в которой сервер Web-прокси, наиболее удаленный от центральной точки доступа в Интернет, является наиболее «нижестоящим» (downstream) сервером Web-прокси и брандмауэра, а брандмауэр ISA Server 2004 и сервер Web-прокси, ближайший к центральному соединению с Интернетом, является самым «вышестоящим» (upstream) сервером Web-прокси брандмауэра ISA Server 2004.

Создание цепочек Web-прокси применяется в нескольких случаях:

- если филиалы соединяются с сервером брандмауэра Web-прокси ISA Server 2004 главного офиса;
- в университетских сетях, состоящих из нескольких ЛВС рабочих групп/отделений, соединенных с серверами Web-прокси брандмауэра ISA Server 2004, расположенными выше в основной сети университета или сети служб;
- в конфигурациях брандмауэра ISA Server 2004 с последовательным подключением (back-to-back), когда нижестоящий брандмауэр ISA Server 2004 использует цепочку Web-прокси, чтобы перенаправлять запросы Web-прокси из корпоративной сети на внешний брандмауэр ISA Server 2004. Такая конфигурация повышает и без того хорошую защиту конфигурации брандмауэра ISA Server 2004 с последовательным подключением.

Эти конфигурации более подробно рассматриваются в главе 10.

Конфигурирование ISA Server 2004 с клиентами разных типов

Многие администраторы брандмауэра ISA считают, что отдельный компьютер нельзя настроить одновременно в качестве клиента Web-прокси, клиента брандмауэра и

клиента SecureNAT. Это заблуждение. Возможно, а иногда и предпочтительно настраивать на одном компьютере все три типа клиентов ISA.

Другое дело, что один компьютер нельзя настроить так, чтобы он выступал *в* роли клиента брандмауэра и клиента SecureNAT. Это объясняется тем, что когда компьютер настроен как клиент брандмауэра, все взаимодействия по протоколам Winsock TCP и UDP перехватываются программным обеспечением клиента брандмауэра. Поэтому у клиента SecureNAT нет доступа к этим соединениям. Для других соединений и для всех соединений не по протоколам TCP и UDP клиент SecureNAT будет выполнять обработку запросов. Например, если компьютер настроен как клиент SecureNAT и как клиент брандмауэра одновременно, конфигурация клиента SecureNAT обрабатывает все соединения ping, tracert и PPTP. Утилиты Ping и tracert используют протокол ICMP, а PPTP использует GRE. Ни ICMP, ни GRE не используют в качестве транспортных протоколов TCP или UDP.

В табл. 5.7 представлено поведение компьютеров, на которых настроено несколько типов клиентов.

Табл. 5.7. Работа приложений на компьютерах с установленными клиентами разных типов

Конфигурация клиентов на брандмауэре **ISA Server 2004**	**Работа приложения**
Клиент Secure NAT и клиент брандмауэра	Клиент брандмауэра обрабатывает все соединения по протоколам TCP и UDP от приложений на базе Winsock. Клиент SecureNAT обрабатывает все соединения по протоколам TCP/UDP от других приложений и все соединения не по протоколам TCP/UDP
Клиент SecureNAT и клиент Web-прокси	Клиент Web-прокси обрабатывает все соединения по протоколам HTTP/HTTPS/FTP (по протоколу ПТ только скачивание) от приложений клиента Web-прокси. От других приложений клиент SecureNAT обрабатывает соединения по протоколам HTTP/HTTPS/FTP (как скачивание, так и закачивание). Если браузер, настроенный как клиент Web-прокси, не способен получить доступ к ресурсам по протоколу FTP, то будет использоваться конфигурация клиента SecureNAT, Все остальные протоколы обрабатываются конфигурацией клиента SecureNAT
Клиент брандмауэра и клиент Web-прокси	Клиент Web-прокси обрабатывает все соединения по протоколам HTTP/HTTPS/FTP (только скачивание) от приложений клиента Web-прокси. Клиент брандмауэра обрабатывает все остальные соединения по протоколам Winsock TCP и UDP, включая протоколы HTTP/HTTPS/FTP (скачивание и закачивание) от приложений, не настроенных как клиенты Web-прокси. Скачивание по протоколу РГР от клиентов Web-прокси может обрабатываться конфигурацией клиента брандмауэра. Для приложений не на базе Winsock нет доступа к протоколам TCP и UDP и к другим протоколам, отличным от TCP и UDP

Табл. 5.7. (окончание)

Конфигурация клиентов на брандмауэре ISA Server 2004	Работа приложения
Клиент SecureNAT, клиент брандмауэра и клиент Web-прокси	Имеется доступ к протоколам HTTP/HTTPS/FTP (скачивание) посредством конфигурации клиента Web-прокси для приложений, настроенных как клиенты Web-прокси. Для скачивания по протоколу FTP, если конфигурация клиента Web-прокси не поддерживает соединение, используется клиент брандмауэра. Все соединения по протоколам TCP/UDP от приложений на базе Winsock обрабатываются клиентом брандмауэра. Все остальные соединения обрабатываются конфигурацией клиента SecureNAT

Выбор типа клиента ISA Server 2004

Выбор типа клиента ISA Server 2004 зависит от необходимого уровня функциональности и защиты (см. табл. 5.8) приводится оценка различных клиентов ISA Server 2004 на основании уровня их функциональности, безопасности и простоты в применении и управлении, а также совместимости с операционной системой.

Табл. 5.8. Оценка безопасности, функциональности, простоты в применении и совместимости различных типов клиента ISA Server 2004

Уровень функциональности	Уровень безопасности	Простота в применении и управлении	Совместимость с операционной системой
Клиент брандмауэра	Клиент брандмауэра	Клиент SecureNAT	Клиент SecureNAT
Клиент SecureNAT	Клиент Web-прокси	Клиент Web-прокси	Клиент Web-прокси
Клиент Web-прокси	Клиент SecureNAT	Клиент брандмауэра	Клиент брандмауэра

В табл. 5.9 представлен ряд параметров, которые следует учитывать при выборе типа клиента ISA Server 2004-

Табл. 5.9. Выбор подходящего типа клиента ISA Server 2004

Требование	Подходящий тип клиента ISA Server 2004
Не применять для сетевых клиентов никакое специальное программное обеспечение	Клиент SecureNAT и клиент Web-прокси. Клиент SecureNAT не предполагает установку программного обеспечения, нужно лишь задать правильный адрес основного шлюза. Клиент Web-прокси также не предполагает установку клиентского программного обеспечения. Нужно лишь настроить приложения Web-прокси на использование брандмауэра в качестве их сервера Web-прокси

(см. след. стр.)

Табл. 5.9. (продолжение)

Требование	Подходящий тип клиента ISA Server 2004
Использование только протоколов Интернета HTTP, HTTPS и FTP для скачивания через Web-браузер и другие приложения, работающие с Web-прокси, з также поддержка Web-кэширования	Клиент Web-прокси или клиент SecureNAT. Оба эти типа клиента способны использовать кэш Web-прокси на брандмауэре ISA Server 2004. Преимущество использования клиента Web-прокси по сравнению с клиентом SecureNAT в этом случае состоит в том, что клиент Web-прокси отправляет информацию о пользователе на брандмауэр ISA Server 2004 и поддерживает жесткий контроль пользовательского/группового доступа и доступа пользователей в Интернет
Проверка подлинности до разрешения доступа. Имя пользователя включается в журналы	Клиент брандмауэра или клиент Web-прокси. Клиент Web-прокси позволяет осуществлять жесткий контроль пользовательского/группового доступа для соединений по протоколам HTTP/HTTPS/FTP (скачивание) через приложения клиента Web-про кс и. Клиент брандмауэра позволяет контролировать пользовательский/групповой доступ для всех приложений на базе Winsock по протоколам TCP и UDP. Всякий раз, когда пользователь проходит проверку подлинности ш брандмауэре ISA Server 2004, имя этого пользователя включается в системный журнал
Публикация серверов в Интернете с помощью правил Web-публикации или публикации серверов	Клиент SecureNAT или любой клиент, не являющийся клиентом ISA Server 2004. Опубликованный сервер должен быть настроен как клиент SecureNAT, если исходный IP-адрес клиента из Интернета сохраняется в соединении, устанавливаемом с опубликованным сервером. Это стандартная конфигурация для правил публикации серверов. Для правил Web-публикации по умолчанию нужно заменить исходный IP-адрес клиента на IP-адрес внутреннего-интерфейса брандмауэра ISA Server 2004 (интерфейса, который находится в той же сети, что и опубликованный сервер). Когда исходный IP-адрес источника заменяется на IP-адрес брандмауэра ISA Server 2004, опубликованный сервер должен знать только маршрут к внутреннему IP-адресу брандмауэра ISA Server 2004, который перенаправил запрос. Для правил Web-публикации и публикации серверов имеется возможность сохранить исходный IP-адрес клиента
Поддержка операционных систем сторонних производителей	Клиент SecureNAT и клиент Web-прокси. Все операционные системы поддерживают конфигурацию клиента SecureNAT, потому что клиент SecureNAT требует только установки правильного адреса основного шлюза. Все операционные системы, работающие с приложениями, поддерживающими конфигурацию клиента Web-прокси, могут соединяться с брандмауэром ISA Server 2004 посредством конфигурации клиента Web-прокси
Поддержка интернет-игр	Клиент брандмауэра. Большинство интернет-игр предполагает несколько первичных и вторичных соединений. Только клиент брандмауэра поддерживает сложные протоколы, которые требуют вторичных соединений (при условии, что на брандмауэре ISA Server 2004 не установлен фильтр приложения, который поддерживает это приложение)

Табл. 5.9. (окончание)

Требование	Подходящий тип клиента ISA Server 2004
Поддержка голосовых/ видеоприложений	Голосовые/видеоприложения, которые не требуют протокол **SIP,** обычно предполагают установку вторичных соединений (ISA Server 2004 не поддерживает передачу сигналов SIP). Только клиент брандмауэра поддерживает вторичные соединения без помощи фильтра приложения

Автоматизация инициализации клиента ISA Server 2004

Существует несколько методов автоматизации конфигурирования клиента Web-прокси и клиента брандмауэра:

- настройка DHCP-серверов для поддержки автоматического обнаружения кли ента Web-прокси и клиента брандмауэра;
- настройка DNS-серверов для поддержки автоматического обнаружения клиен та Web-прокси и клиента брандмауэра;
- автоматизация конфигурирования клиента Web-прокси с помощью групповой политики;
- автоматизация конфигурирования клиента Web-прокси с помощью набора ин струментальных средств IEAK для Internet Explorer.

В следующих разделах обсуждается, как автоматизировать конфигурирование клиентов Web-прокси и брандмауэра с помощью протокола WPAD и групповой политики Active Directory. В этой книге не приводится подробное описание того, как использовать набор инструментальных средств IEAK (Internet Explorer Administration Kit, инструментальные средства администрирования Internet Explorer) для автоматизации конфигурирования клиента Web-прокси.

Существуют два основных метода поддержки автоматического обнаружения для клиентов Web-прокси и клиента брандмауэра: DNS и DHCP. В табл. 5.10 представлена информация, которая поможет выбрать наиболее подходящий из этих методов.

Табл. 5.10. Поддержка DNS и DHCP для автоматического обнаружения клиента Web-прокси и брандмауэра

DHCP	DNS
Клиент должен быть клиентом DHCP	Клиент должен быть способен разрешать DNS-имена во внутренней сети
Требуется Internet Explorer 5.0 и выше	Требуется Internet Explorer 5.0 и выше
Должен быть способен отправлять DHCPINFORM-запросы (только для Windows 2000, Windows XP и Windows Server 2003)	Должен быть способен правильно квалифицировать имя WPAD с доменным именем, чтобы получить FQDN-имя, которое разрешается во внутренний IP-адрес брандмауэра ISA Server 2004

(см. след. стр.)

Табл. 5.10. (окончание)

DHCP	**DNS**
Пользователь должен выполнить вход в систему как локальный администратор	Каждый домен должен быть настроен со своей WPAD-записью
Брандмауэр ISA Server 2004 может публиковать информацию об автоматическом обнаружении на любом доступном порте	Брандмауэр ISA Server 2004 должен публиковать информацию об автоматическом обнаружении на порте TCP 80
Каждый DHCP-сервер должен быть настроен с WPAD-записью	Каждый DNS-сервер должен быть настроен с WPAD-записью. В филиалах может потребоваться специальное конфигурирование, чтобы клиенты филиала не использовали WPAD-запись, указывающую на брандмауэры ISA Server 2004 в главном офисе

ПРИМЕЧАНИЕ Более подробная информация о протоколе WPAD (Web Proxy Auto discover y Protocol) представлена в справочном файле ISA Server 2004 по адресу: **www.microsoft.com/technet/treeview/ default.asp?url=/techn9t/** prodtechnol/isa/ roddocs/isadocs/CMT_AutoDetect.asp Более подробная информация о конфигурировании IEAK для автоматизации конфигурирования клиента Web-прокси приводится в главе 26 «Using Automatic Configuration, Automatic Proxy, and Automatic Detection» (Использование автоматического конфигурирования, автоматического прокси и автоматического обнаружения) на сайте: **www.microsoft.com/resources/documentation/ie/6/all/reskit/en**-us/pa rt6/c26ie6rk.mspx.

Настройка DHCP-серверов для поддержки автоматического обнаружения клиента Web-прокси и клиента брандмауэра

Клиенты DHCP могут получать информацию об автоматическом конфигурировании с компьютера брандмауэра ISA Server 2004, используя информационные сообщения DHCP. Клиент брандмауэра и программное обеспечение Web-браузера могут создавать информационные сообщения DHCP, в которых у DHCP-сервера запрашивается адрес компьютера, содержащего информацию об автоматическом конфигурировании. DHCP-сервер возвращает адрес этого компьютера, а клиент брандмауэра или программное обеспечение Web-браузера запрашивает автоматическое конфигурирование с полученных адресов.

DHCP-сервер использует специальный вариант DHCP для предоставления этой информации. Для получения информации об автоматическом конфигурировании с помощью WDAD выполняют следующие этапы:

- установка DHCP-сервера;
- создание диапазона действия DHCP;

- создание варианта диапазона действия DHCP 252;
- настройка клиента в качестве DHCP-клиента;
- настройка клиентского браузера на использование автоматического обнаружения;
- настройка брандмауэра ISA Server 2004 на публикацию информации об авто матическом обнаружении;
- установка соединения.

Установка DHCP-сервера

Процедуры установки DHCP-сервера рассматривались в главе 4.

Создание диапазона действия DHCP

Диапазон действия DHCP - это набор IP-адресов, которые могут использоваться DHCP-сервером для присваивания адресов DHCP-клиентам в сети. Кроме того, диапазон действия DHCP может включать дополнительные настройки TCP/IP, присваиваемые клиентам, которые называются DHCP-вариантами (DHCP options). DHCP-варианты могут присваивать DHCP-клиентам различные настройки TCP/IP, например адрес DNS-сервера, адрес WINS-сервера и первичное имя домена.

Для того чтобы активировать DHCP-сервер и создать диапазон действия DHCP, выполните следующие действия:

1. Щелкните **Start** (Пуск), выберите **Administrative Tools** (Администрирование), щелкните **DHCP.**
2. В левой панели консоли **DHCP** щелкните правой кнопкой мыши имя сервера. Щелкните команду **Authorize** (Разрешить) (рис. 5.26).

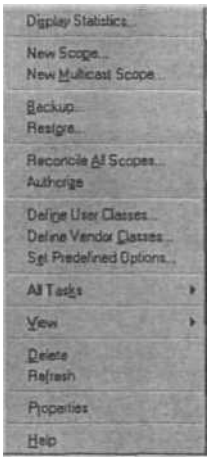


Рис. 5.26. Расположение команды Authorize (Разрешить)

3. Щелкните **Refresh** (Обновить) на линейке кнопок консоли. Значок слева от имени сервера изменится: красная стрелка, направленная вниз, превратится в зеленую стрелку, направленную вверх.
4. Правой кнопкой мыши щелкните еще раз имя сервера в левой панели консоли и щелкните команду **New Scope** (Новая область действия).
5. Щелкните **Next** (Далее) на странице **Welcome to the New Scope Wizard** (Вас приветствует мастер создания новой области действия).
6. Введите имя диапазона действия на странице **Scope Name** (Имя диапазона действия). Это имя несет только описательную нагрузку и не влияет на функциональность диапазона действия. Также можно ввести описание диапазона действия в поле **Description** (Описание). Щелкните **Next** (Далее).
7. Введите диапазон IP-адресов, которые могут присваиваться DHCP-клиентам, на странице **IP Address Range** (Диапазон IP-адресов). Введите первый адрес диапазона в текстовое поле **Start IP-address** (Начальный IP-адрес) и последний IP-адрес диапазона в текстовое поле **End IP-address** (Конечный IP-адрес). Введите маску подсети для диапазона IP-адресов в текстовое поле **Subnet mask** (Маска подсети).
8. В примере, показанном на рис. 5.27, внутренняя сеть имеет идентификатор сети 10.0.2/24. В диапазон действия DHCP будут включаться не все IP-адреса этого идентификатора сети, а **лишь** часть. Поэтому в этом примере в качестве начального IP-адреса в поле **Start IP address** (Начальный IP-адрес) указано значение 10.0.2.100, а в качестве конечного значения — 10.0.2.150 и использована 24-битная маска подсети. В производственных сетях часто лучше присвоить весь идентификатор сети диапазону IP-адресов, используемых в диапазоне действия. Затем можно задать исключения для хостов в сети, которые имеют статически присвоенные IP-адреса, содержащиеся в этом диапазоне действия. Это позволяет централизованно управлять присвоением IP-адресов и конфигурированием с помощью DHCP. Щелкните **Next** (Далее).

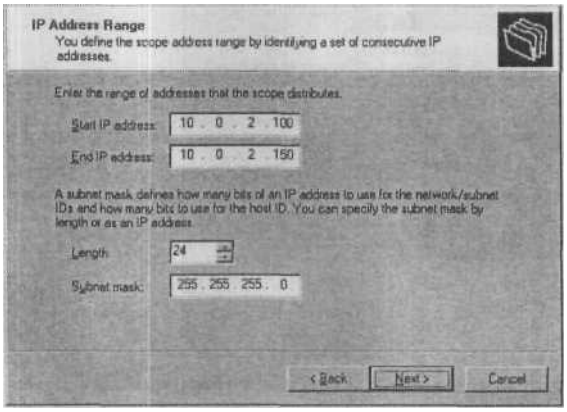


Рис. 5.27. Настройка диапазона IP-адресов для диапазона действия DHCP

9. Не вводите никакие исключения в диалоговом окне **Add Exclusions** (Добавить исключения). Щелкните **Next** (Далее).
] 0. Примите настройки по умолчанию на странице **Lease Duration** (Продолжительность владения) и щелкните **Next** (Далее).
11. На странице **Configure DHCP Options** (Настроить режимы DHCP) выберите **Yes, I want to** configure **these options now** (Да, я хочу настроить эти режимы сей час) и щелкните **Next** (Далее).
12. Ничего не вводите на странице **Router (Default Gateway)** (Маршрутизатор, ос новной шлюз). Если бы в сети использовался клиент SecureNAT, то на этой стра нице следовало бы ввести IP-адрес внутреннего интерфейса брандмауэра. Од нако в данной конфигурации используется только клиент Web-прокси и кли ент брандмауэра. Щелкните **Next** (Далее).
13- На странице **Domain Name and DNS Servers** (Имя домена и DNS-серверы) введите в поле **Primary domain name** (Первичное имя домена) первичное имя домена, которое будет присваиваться DHCP-клиентам, и в поле **DNS server address** (Адрес DNS-сервера) адрес DNS-сервера, который будут использовать DHCP-клиенты.
14. Первичное имя домена является важной настройкой для клиента брандмауэра и клиента Web-прокси. Для того чтобы автоматическое обнаружение выполнялось корректно для клиента брандмауэра и клиента Web-прокси, эти клиенты должны правильно полностью квалифицировать неполное имя WPAD. Более подробно этот вопрос рассматривается далее. В данном примере введите в текстовое поле **Parent domain** (Родительский домен) msfirewall.org (рис. 5.28). Это позволяет присвоить DHCP-клиентам первичное имя домена msfirewall.org, которое будет присоединено к неполным именам. Введите IP-адрес DNS-сервера в текстовое поле IP address. В этом примере IP-адрес DNS-сервера — **10.0.2.2.** Щелкните **Add** (Добавить) после ввода IP-адреса. Щелкните **Next** (Далее).

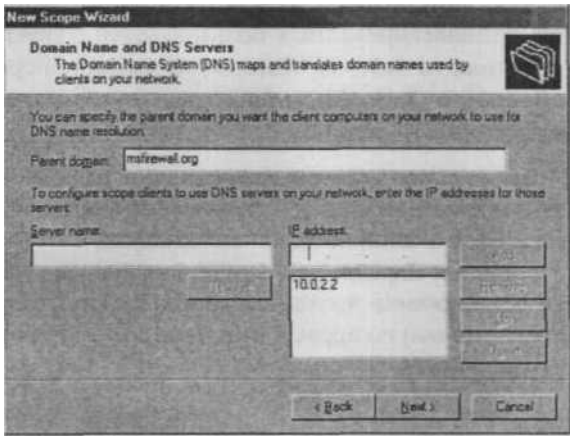


Рис. 5.28. Настройка основного имени домена для DHCP-клиентов

15. Не вводите адрес WINS-сервера на странице **WINS Servers** (WINS-серверы). В этом примере не используется WINS-сервер. Однако WINS-серверы очень полезны в среде VPN-сервера, если нужно разрешить VPN-клиентам просматривать университетскую сеть с помощью приложения **My Network Places** (Сетевые подключения) или **Network Neighborhood** (Сетевое окружение). Щелкните **Next** (Далее).
16. На странице **Activate Scope** (Включить диапазон действия) выберите Yes, **I want to activate this scope now** (Да, я хочу включить этот диапазон действия сей час) и щелкните **Next** (Далее).
17. Щелкните **Finish** (Готово) на странице **Completing the New Scope Wizard** (За вершение работы мастера создания нового диапазона действия).
18. В правой панели консоли DHCP будут отображены два варианта DHCP, созданные с помощью мастера (см. рис. 5.29).

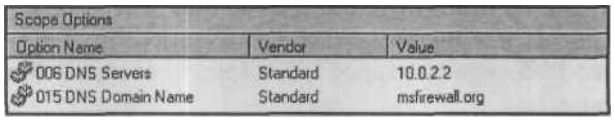


Рис. 5.29. Просмотр вариантов диапазона действия

Следующий шаг — создание варианта DHCP, который позволит DHCP-клиентам автоматически обнаруживать настройки клиента Web-прокси и клиента брандмауэра.

Создание варианта диапазона действия DHCP 252 и добавление его к области действия

Вариант диапазона действия DHCP 252 может использоваться для автоматического конфигурирования клиентов Web-прокси и брандмауэра. Клиент Web-прокси или клиент брандмауэра должны быть настроены как DHCP-клиент, а пользователь, выполнивший вход в систему, должен быть членом группы локальных администраторов или группы привилегированных пользователей (Power users group) (для Windows 2000). В системах на базе ОС Windows XP группа операторов настройки сети (Network Configuration Operators group) также имеет разрешение создавать DHCP-запросы (сообщения DHCPINFORM).

> ПРИМЕЧАНИЕ Более подробная информация об ограничениях при использовании DHCP для автоматического обнаружения совместно с Internet Explorer 6.0 представлена в Базе знаний Microsoft в статье под названием «Automatic Proxy Discovery in Internet Explorer with DHCP Requires Specific Permissions» (Автоматическое обнаружение прокси в Internet Explorer с помощью DHCP требует особых полномочий) по адресу: http://support.microsoft.com/default.aspx?scid=kb;en-us;312864.

Для **создания** специального варианта DHCP выполните следующие действия на DHCP-сераерс:

1. Откройте консоль DHCP в меню **Administrative Tools** (Администрирование) и щелкните правой кнопкой мыши имя сервера в левой панели консоли. Щелкните команду **Set Predefined Options** (Установить предопределенные варианты) (рис. 530).

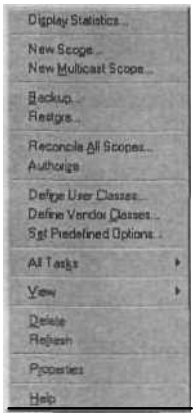


Рис. 5.30. Выбор команды Set Predefined Options (Установить предопределенные варианты)

2. В диалоговом окне **Predefined Options and Values** (Предопределенные варианты и значения) (рис. 531) щелкните **Add** (Добавить).

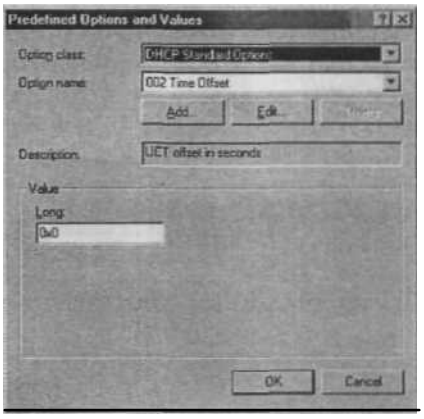


Рис. 5.31. Диалоговое окно Predefined Options and Values (Предопределенные варианты и значения)

3. В диалоговом окне **Option** Type (Тип варианта) (рис. 5.32) введите следующую информацию: D **Name** (имя): wpad D **Data type** (тип данных): String

a Code (код): 252
n Description (описание): wpad entry
Щелкните OK.

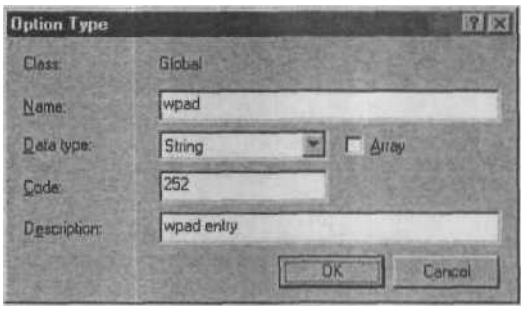


Рис. 5.32. Диалоговое окно Option **Type** (Тип варианта)

В разделе **Value** (Значение) введите URL брандмауэра ISA Server 2004 в текстовое поле **String** (Строка). Это значение имеет следующий формат: **http://ISA-Serve** r **nam e:Au to discovery Port Number/wpad.dat.** Номер стандартного порта для автоматического обнаружения — TCP 80. Это значение можно изменить в консоли **ISA Management.** Более подробно эта тема рассматривается далее. Как показано на рис. 533, введите следующее значение в текстовое поле **String** (Строка): http://isa2.msfirewall.org:80/wpad.dat. Запись wpad.dat должна быть выполнена строчными буквами. Более подробная информация по этой теме содержится в Базе знаний к статье «Automatically Detect Settings Does not Work if You Configure DHCP Option 252» (Настройки автоматического обнаружения не работают, если настроен вариант DHCP 252) по адресу: http://support.microsoft.com/default.aspx?scid=kb,en-us;307502. Щелкните **OK.**

5.

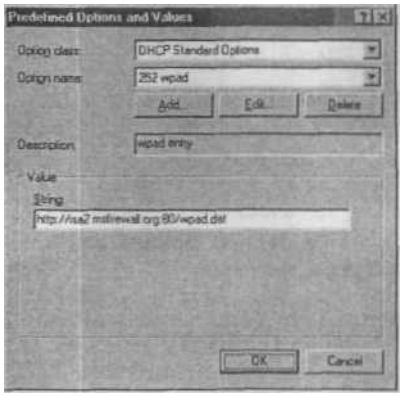


Рис. 5.33. Диалоговое окно Predefined Options and Values (Предопределенные варианты и значения)

6. Щелкните правой кнопкой мыши узел **Scope Options** (Варианты диапазона дей ствия) в левой панели консоли и щелкните команду **Configure Options** (Настро ить варианты).
7. В диалоговом окне **Scope Options** (Варианты диапазона действия) (рис. 5.34) прокрутите список **Available Options** (Доступные варианты) и установите фла жок в поле **252 wpad.** Щелкните **Apply** (Применить) *и* ОК.

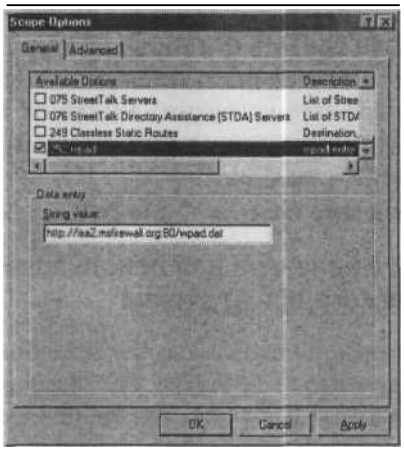


Рис. 5.34. Диалоговое окно Scope Options (Варианты диапазона действия)

Теперь в правой панели консоли DHCP в списке **Scope options** (Варианты диапазона действия) появится запись **252 wpad.** 9. Закройте консоль **DHCP.**

Настройка клиента как DHCP-клиента

Для того чтобы использовать DHCP для получения информации об автоматическом обнаружении для клиента Web-прокси и клиента брандмауэра, клиентский компьютер должен быть настроен как DHCP-клиент.

ПРИМЕЧАНИЕ В этом примере компьютер на базе ОС Windows 2000 настроен в качестве DHCP-клиента. Процедура может несколько отличаться в зависимости от операционной системы клиентского компьютера. Все операционные системы Windows TCP/IP используют DHCP в качестве стандартной конфигурации IP-адресов.

Для того чтобы настроить клиентский компьютер в качестве DHCP-клиента, выполните следующие действия на клиентском компьютере: 1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на

рабочем столе и щелкните команду **Properties** (Свойства).

8

2. Правой кнопкой мыши щелкните запись **Local Area Connection** (Подключение по локальной сети) в окне **Network and Dial-up Connections** (Сетевые подключения) и щелкните команду **Properties** (Свойства).
3. В диалоговом окне **Local Area Connection Properties** (Подключение по локальной сети — свойства) щелкните запись **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) и щелкните **Properties** (Свойства).
4. В диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета, TCP/IP) выберите **Obtain an IP address automatically** (Получить IP-адрес автоматически) *и* **Obtain DNS server address automatically** (Получить адрес DNS-сервера автоматически). Щелкните OK
5. Щелкните OK в диалоговом окне **Local Area Connection Properties** (Подключение по локальной сети — свойства).
6. Закройте окно **Network and Dial-up Connections** (Сетевые подключения).

Настройка клиентского браузера для использования DHCP для автоматического обнаружения

Браузер должен быть **настроен** на использование автообнаружения до того, как он сможет воспользоваться вариантом DHCP-сервера 252 для автоматического самоконфигурирования. Это стандартная настройка для Internet Explorer 6.0, но с течением времени эта стандартная настройка может быть изменена в браузере на конкретном компьютере. В этом примере браузер настроен вручную на использование автоматического обнаружения для самоконфигурирования. Далее будут представлены методы, которые можно использовать для автоматической установки этого варианта.

На компьютере клиента Web-прокси выполните следующие действия:

1. Щелкните правой кнопкой мыши значок **Internet Explorer** на рабочем столе и щелкните **Properties** (Свойства).
2. В диалоговом окне **Internet Properties** (Свойства обозревателя) щелкните вкпадку **Connections (Соединения).** Щелкните кнопку **LAN Settings** (Настройки ЛВС).
3. В диалоговом окне **Local Area Network (LAN) Settings** (Настройки ЛВС) установите флажок в поле **Automatically detect settings** (Автоматически обнаруживать настройки). Щелкните OK.
4. Щелкните OK в диалоговом окне **Internet Properties** (Свойства обозревателя).

Брандмауэр ISA Server 2004 должен быть настроен на публикацию информации об автоматическом обнаружении, прежде чем клиент Web-прокси сможет получить информацию о конфигурировании. Это нужно сделать в следующую очередь.

Настройка брандмауэра ISA Server 2004 на публикацию информации об автоматическом обнаружении

Все настройки, необходимые Web-браузеру для самоконфигурирования, содержатся на компьютере брандмауэра ISA Server 2004. По умолчанию этот вариант отклю-

чен. Можно включить публикацию информации об автоматическом обнаружении на компьютере брандмауэра ISA Server 2004 так, чтобы клиент Web-прокси мог получить настройки для автоматического конфигурирования.

Для того, чтобы компьютер брандмауэра ISA Server 2004 предоставлял информацию об автоматическом конфигурировании автоматически обнаруживаемым клиентам Web-прокси и брандмауэра, выполните следующие действия:

1. На этом компьютере брандмауэра ISA Server 2004 откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004.** Разверните имя сервера в левой панели консоли, а затем разверните узел **Configuration** (На стройка). Щелкните узел **Networks** (Сети).
2. В узле **Networks** (Сети) щелкните вкладку **Networks** (Сети) на панели **Details** (Подробно).
3. Правой кнопкой мыши щелкните внутреннюю сеть на вкладке **Networks** (Сети) и щелкните **Properties** (Свойства) (рис. 5.35).

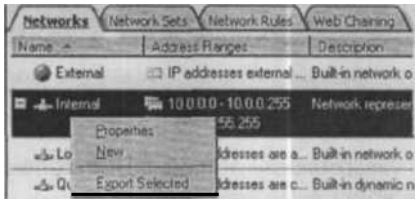


Рис. 5.35. Открытие диалогового окна Internal Network Properties (Внутренние свойства сети)

4. В диалоговом окне **Internal Properties** (Внутренние свойства) установите фла жок в поле **Publish automatic discovery information** (Опубликовать инфор мацию об автоматическом обнаружении). В текстовом поле **Use this port for automatic discovery request** (Использовать этот порт для запросов автомати ческого обнаружения) оставьте стандартную установку: порт 80.
5. Щелкните **Apply** (Применить) и ОК.
6. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
7. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Установка соединения

Теперь Web-браузер может автоматически установить соединение со службой Web-прокси брандмауэра ISA Server 2004 с помощью автоматического обнаружения.

На компьютере клиента Web-прокси нужно сделать следующее: 1. Откройте **Internet Explorer** и введите URL сайта ISA Server Microsoft **www.mic-rosoft.com/isaserver.**

2. Записи монитора сети показывают информационные сообщения DHCP, отправленные клиентом Web-прокси. Клиент Web-прокси использует информационное сообщение DHCP (как на рис. 5.36) для получения адреса автоматического обнаружения, содержащегося в записи варианта DHCP 252.

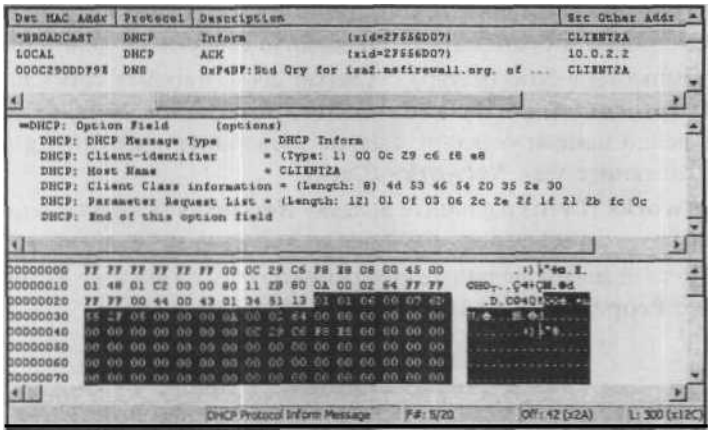


Рис. 5.36. Просмотр запроса DHCPINFORM

3. На рис. 5.37 показано уведомление ACK на DHCP-сообщение клиента Web-прокси. В нижней панели консоли монитора сети видно, что DHCP-сервер вернул адрес, который был настроен в записи варианта DHCP 252.

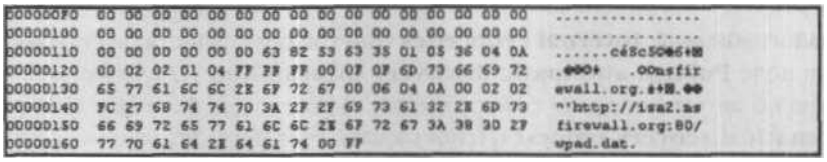


Рис. 5.37. Просмотр содержимого запроса DHCPINFOBM

После того как клиент Web-прокси получает адрес ISA Server 2004, содержащий настройки автоматического обнаружения, следующий шаг состоит в том, чтобы разрешить имя брандмауэра ISA Server 2004 в его внутренний IP-адрес. Разрешение имен является очень важным для многих аспектов функционирования ISA Server 2004. Этот факт подтверждается следующим примером. В мониторе сети (рис. 5.38) видно, что клиент Web-прокси создал запрос к isa2.msfirewall.org, к URL, который содержался в варианте DHCP 252.

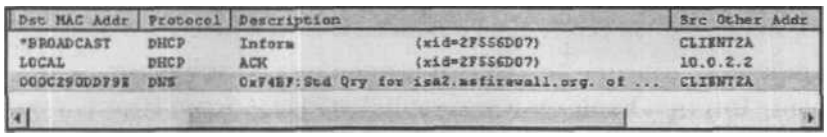


Рис. **5.38.** Просмотр DNS-запроса WPAD

Конфигурирование DNS-серверов для поддержки автоматического обнаружения клиента Web-прокси и клиента брандмауэра

Другой способ передачи информации об автоматическом обнаружении клиентам Web-прокси и клиентам брандмауэра состоит в использовании DNS-серверов. Можно создать WPAD-запись псевдонима в DNS и позволить клиентам браузера использовать эту информацию для автоматического самоконфигурирования. Этот метод отличается от применения DHCP тем, что в случае DHCP пользователи, выполнившие вход в систему, должны были быть членами конкретной группы в операционной системе Windows.

Разрешение имен является основным компонентом, обеспечивающим корректную работу этого метода автоматического обнаружения клиента Web-прокси и клиента брандмауэра. В этом случае операционная система клиента должна быть способна правильно полностью квалифицировать WPAD-имя. Это объясняется тем, что клиент Web-прокси и клиент брандмауэра знает лишь то, что он должен разрешить WPAD-имя, но он не знает, какое именно имя домена он должен добавить к запросу, чтобы разрешить WPAD-имя. Далее этот вопрос рассматривается более подробно.

> ПРИМЕЧАНИЕ В отличие от применения DHCP для присваивания информации об автоматическом обнаружении клиентам Web-прокси и брандмауэра, при использовании DNS не предусмотрен вариант использования настраиваемого номера порта для публикации информации об автоматическом обнаружении. При использовании DNS информация об автоматическом обнаружении должна публиковаться на порт TCP 80.

Для того чтобы информация об автоматическом обнаружении предоставлялась клиенту Web-прокси и клиенту брандмауэра с помощью DNS, нужно сделать следующее:

- создать WPAD-записи в DNS;
- настроить клиента на использование полного WPAD-псевдонима;
- настроить браузер клиента на использование автоматического обнаружения;
- установить соединение.

Создание WPAD-записи в DNS

Первый шаг состоит в создании WPAD-записи псевдонима в DNS. Этот псевдоним указывает на запись хоста (A) для брандмауэра ISA Server 2004, который разрешает имя брандмауэра ISA Server 2004 во внутренний IP-адрес брандмауэра. Запись хоста (A) должна быть создана до создания записи псевдонима CNAME. Если включена автоматическая регистрация в DNS, запись брандмауэра ISA Server 2004 уже будет введена в DNS. Если автоматическая регистрация не включена, то нужно создать запись хоста (A) для брандмауэра ISA Server 2004 вручную. В следующем примере брандмауэр ISA Server 2004 автоматически зарегистрировался в DNS.

На DNS-сервере контроллера домена во внутренней сети выполните следующие действия:

1. Щелкните **Start** (Пуск) и выберите **Administrative Tools** (Администрирование). Щелкните запись **DNS.** В консоли управления DNS (рис. 5.39) щелкните правой кнопкой мыши зону прямого просмотра для вашего домена и щелкните команду **New Alias (CNAME)** (Новый псевдоним, CNAME).

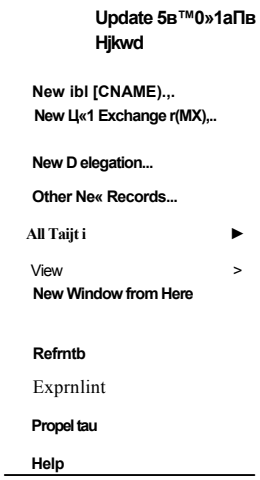


Рис. 5.39. Выбор команды New **Alias (CNAME)** (Новый псевдоним, CNAME)

2. В диалоговом окне **New Resource Record** (Запись нового ресурса) (рис. 5.40) введите wpad в текстовое поле **Alias name** (Псевдоним) (если в это поле ничего не ввести, то будет использоваться родительский домен). Щелкните кнопку **Browse** (Обзор).

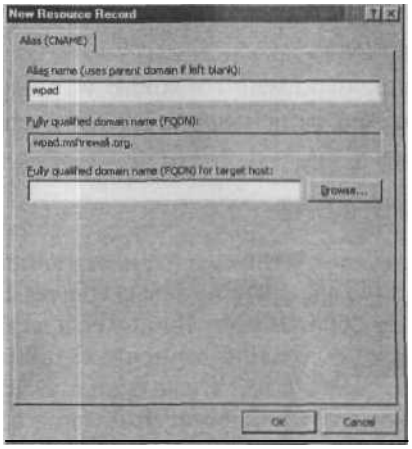


Рис. 5.40. Диалоговое окно New Resource Record (Запись нового ресурса)

3. В диалоговом окне **Browse** (Обзор) дважды щелкните имя сервера в списке **Records** (Записи).
4. В диалоговом окне **Browse** (Обзор) дважды щелкните запись **Forward Lookup Zone** (Зона прямого просмотра) в разделе Records (Записи).
5. В диалоговом окне **Browse** (Обзор) дважды щелкните имя зоны прямого про смотра в разделе **Records** (Записи).
6. В диалоговом окне **Browse** (Обзор) выберите имя брандмауэра ISA Server 2004 в разделе **Records** (Записи). **Щелкните ОК** (рис. 5.41).

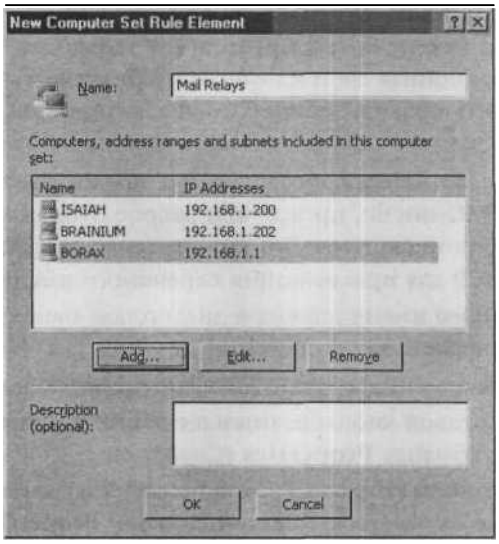


Рис. 5.41. Диалоговое окно **New Resource** (Новый ресурс)

7. Щелкните ОК в диалоговом окне **New Resource Record** (Запись **нового** ресурса).
8. Запись **CNAME (alias)** появится в правой панели консоли управления DNS(рис. 5.42).

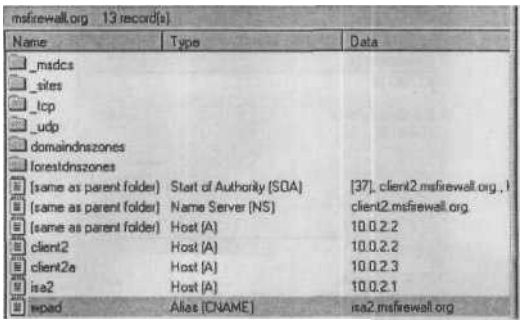


Рис. 5.42. Просмотр псевдонима WPAD в DNS 9.

Закройте консоль **DNS Management.**

Конфигурирование клиента на использование полного псевдонима WPAD

Клиент Web-прокси и клиент брандмауэра должны быть способны правильно разрешать WPAD-имя. Конфигурации клиента Web-прокси и клиента брандмауэра не знают, какой домен содержит WPAD-псевдоним. Операционная система клиента Web-прокси и клиента брандмауэра должна быть способна предоставить эту информацию клиенту Web-прокси и клиенту брандмауэра.

Прежде чем запрос отправляется на DNS-сервер, DNS-запросы должны быть полностью квалифицированы. Полный запрос содержит имя хоста и имя домена. Клиент Web-прокси и клиент брандмауэра знают только часть запроса, содержащую имя хоста. Операционная система клиента Web-прокси и клиента брандмауэра должна предоставить правильное имя домена, которое она добавляет к WPAD-имени хоста, прежде чем она перешлет DNS-запрос на DNS-сервер.

Существует несколько методов, позволяющих предоставить имя домена, которое добавляется к WPAD-имени, прежде чем запрос отправляется на DNS-сервер клиентской операционной системы. Вот два наиболее распространенных метода:

- использование DHCP для присваивания первичного имени домена;
- настройка первичного имени домена в диалоговом окне сетевой идентификации клиентской операционной системы.

Для реализации этих методов нужно выполнить следующие действия:

1. На рабочем столе правой кнопкой мыши щелкните My computer (Мой компьютер) и щелкните команду Properties (Свойства).
2. В диалоговом окне System Properties (Свойства системы) щелкните вкладку Network Identification (Имя компьютера). Щелкните кнопку Properties (Изменить).
3. В диалоговом окне Identification Changes (Изменение имени компьютера) (рис. 5.43) щелкните More (Дополнительно).

Рис. 5.43. Диалоговое окно Identification Changes (Изменение имени компьютера)

4. В диалоговом окне **DNS Suffix and NetBIOS Computer Name** (DNS-суффикс и NetBIOS-имя компьютера) (рис. 544) введите имя домена, содержащее WPAD-запись, в текстовое поле **Primary DNS suffix of this computer** (основной DNS-суффикс этого компьютера). Это то самое имя домена, которое операционная система добавит к WPAD-имени, прежде чем отправлять DNS-запрос на DNS-сервер. По умолчанию основное имя домена — это то же имя домена, к которому относится данный компьютер. Если компьютер не является членом домена, то это текстовое поле будет пустым. **Нужно** отметить, что вариант **Change primary DNS suffix when domain membership changes** (Изменить основной DNS-суффикс, когда изменяется членство в домене) включен по умолчанию. В данном примере компьютер не является членом домена. Нажмите **Cancel** (Отмена) в каждом из этих диалоговых окон, чтобы не настраивать основное имя домена.

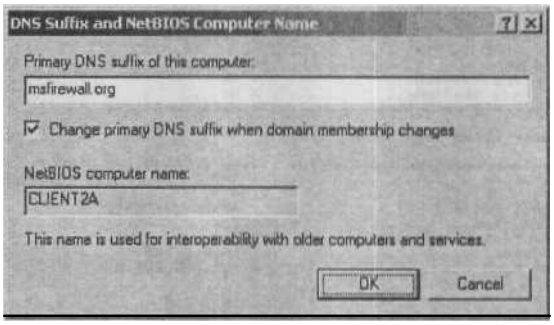


Рис. 5.44. Диалоговое окно DNS Suffix and NetBIOS Computer Name (DNS-суффикс и NetBIOS-имя компьютера)

5. Еще один способ присвоения компьютеру основного имени домена состоит в использовании DHCP. DHCP-сервер можно настроить так, чтобы он предоставлял DHCP-клиентам основное имя домена. Для этого нужно настроить вариант области действия DHCP. Как это сделать, было показано ранее при создании области действия на DHCP-сервере с помощью мастера создания области действия DHCP. В данном примере вариант области действия **DNS Domain Name** (DNS-имя домена) был установлен так, чтобы предоставлять DHCP-клиентам доменное имя msfirewall.org. Применение этого варианта (рис. 5.45) дает тот же результат, что и ручная настройка основного имени домена. DHCP-клиенты добавляют это имя к неквалифицированным DNS-запросам (например, WPAD), прежде чем отправлять DNS-запрос на DNS-сервер.

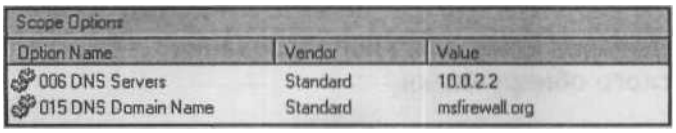


Рис. 5.45. Варианты области действия

6. Перейдите в систему DHCP-клиента и откройте командную строку. В командной строке введите ipconfig/all и нажмите клавишу <Enter>. Обратите внимание, что в поле Connection-specific DNS Suffix (DNS-суффикс для соединения) для этого компьютера было введено значение msfirewall.org.

DHCP является наиболее эффективным способом присвоения основного DNS-суффикса клиентам сети (рис. 5.46). Эта функция позволяет автоматически настроить DNS-суффикс на DHCP-клиен тах, соединенных с сетью, которые не являются членами домена Active Directory. Эти клиенты тем не менее могут корректно разрешать WPAD-имя на основании текущей DNS-инфраструктуры. При этом им ненужно присоединяться к этому домену и нет необходимости в их настройке вручную.

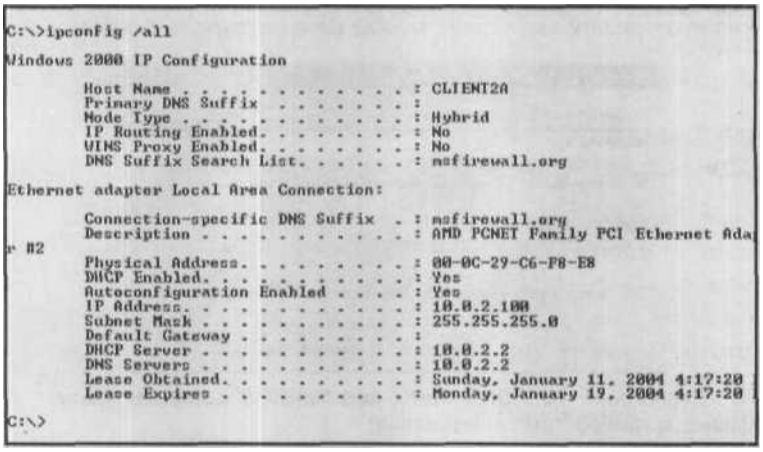


Рис. 5.46. Конфигурация DHCP-клиента

Если во внутренней сети имеется несколько доменов и клиентов, принадлежащих к нескольким доменам, то нужно создать запись WPAD-псевдонима CNAME для каждого домена. Кроме того, поддержка DNS для WPAD-записей может быть немного проблематичной, когда имеется лишь один внутренний сетевой домен, который охватывает ссылки WAN. Можно ввести лишь одну WPAD-запись для каждого домена, а все хосты, которые полностью квалифицируют WPAD-запись с этим именем домена, получат тот же адрес сервера. Это может привести к тому, что хосты филиалов попытаются получить доступ к Интернету через ISA Server 2004, расположенный в главном офисе. В такой ситуации лучше всего создать дочерние домены в DNS, которые поддерживают клиентов филиалов.

Настройка браузера клиента на использование автоматического обнаружения

Следующий шаг состоит в том, чтобы настроить браузер на использование автоматического обнаружения. Если это еще не сделано, настройте Web-браузер на исполь-

зование автоматического обнаружения для того, чтобы он автоматически выполнял самонастройку на применение службы Web-прокси брандмауэра ISA Server 2004.

1. Правой кнопкой мыши щелкните значок **Internet Explorer** на рабочем столе и щелкните **Properties** (Свойства).
2. В диалоговом окне **Internet Properties** (Свойства обозревателя) щелкните вкладку **Connections** (Подключения). Щелкните кнопку LAN **Settings** (Настройка LAN).
3. В диалоговом окне **Local Area Networks (LAN) Settings** (Настройка локальной сети) установите флажок в поле **Automatically detect settings** (Автоматическое определение параметров). Щелкните ОК.
4. Щелкните **Apply** (Применить), а затем щелкните ОК в диалоговом окне **Internet Properties** (Свойства обозревателя).

Теперь нужно настроить брандмауэр ISA Server 2004 на публикацию информации об автоматическом обнаружении для клиентов Web-прокси и брандмауэра.

Настройка брандмауэра ISA Server 2004 на публикацию информации об автоматическом обнаружении

Для того чтобы брандмауэр ISA Server 2004 предоставлял информацию об автоматическом обнаружении клиентам Web-прокси и брандмауэра, выполните следующие действия на компьютере брандмауэра ISA Server 2004:

1. На компьютере брандмауэра ISA Server 2004 откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004.** Разверните имя сервера пи левой панели консоли, а затем разверните узел **Configuration** (Настройка). Щелкните узел **Networks** (Сети).
2. **В** узле **Networks** (Сети) щелкните вкладку **Networks** (Сети) на панели **Details** (Подробно).
3. Правой кнопкой мыши щелкните внутреннюю сеть на вкладке **Networks** (Сети) и щелкните **Properties** (Свойства) (рис. 5.47).

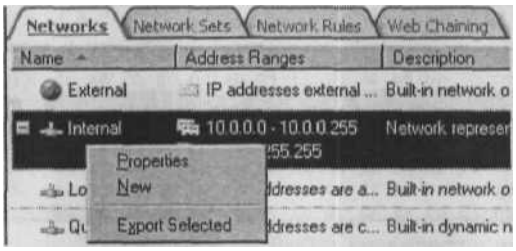


Рис. 5.47. Диалоговое окно Internal Network Properties (Внутренние свойства сети)

В диалоговом окне **Internal Properties** (Внутренние свойства) установите флажок в поле **Publish automatic discovery information** (Публиковать информацию об автоматическом обнаружении). В текстовом поле **Use this port for**

automatic discovery request (Использовать этот порт для запросов на автоматическое обнаружение) оставьте стандартное значение 80.

5. Щелкните **Apply** (Применить) и ОК.
6. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить поли тику брандмауэра.
7. Щелкните ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Установка соединения с использованием DNS для автоматического обнаружения

Теперь компьютер клиента Web-прокси и клиента брандмауэра может использовать DNS для получения информации об автоматическом конфигурировании Выполните следующие действия на компьютере клиента Web-прокси:

1. Откройте Internet Explorer и перейдите на домашнюю страницу **www.microsoft. com/isaserver.**
2. Запись монитора сети показывает, что клиент Web-прокси выполняет DNS-запрос к wpad.msfirewall.org. DNS-сервер отвечает на запрос, отправляя IP-адрес (рис. 5.48) компьютера брандмауэра ISA Server 2004.

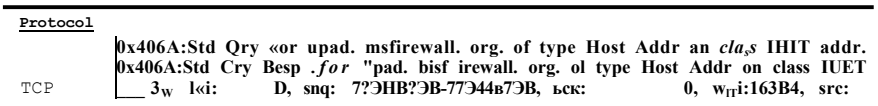


Рис. 5.48. Просмотр DNS-запросов WPAD

3. После того как клиент Web-прокси получит IP-адрес компьютера брандмауэра ISA Server 2004 и" порт, с которого он может получить информацию об автоконфигурировании, он направляет запрос (рис. 549) информации об автоконфигурировании WPAD. Этот запрос показан в нижней панели окна монитора сети: GET/wpad.dat HTTP/1.1.

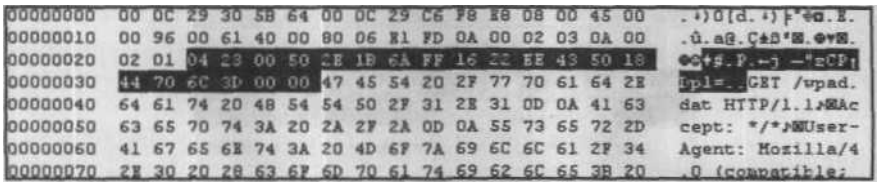


РИС. 5.49. Просмотр информации о DNS-запросе WPAD

Автоматизация установки клиента брандмауэра

Программное обеспечение клиента брандмауэра может быть установлено практически на любой 32-битной операционной системе семейства Windows за исключением Windows 95. Существует несколько убедительных причин, по которым программное обеспечение клиента брандмауэра следует устанавливать на всех компьютерах, которые оно поддерживает.

- Клиент брандмауэра позволяет создавать правила контроля пользовательского/группового доступа для всех протоколов TCP и UDP. Этим он отличается от клиента Web-прокси, который поддерживает только протоколы HTTP, HTTPS и FTP.
- Клиент брандмауэра имеет доступ ко всем протоколам на базе TCP и UDP, включая протоколы, требующие вторичных соединений. А клиент SecureNAT поддерживает протоколы приложений, требующие вторичных соединений, только при наличии фильтра приложения, который поддерживает такие протоколы.
- Клиент брандмауэра обеспечивает гораздо более высокую производительность, чем клиент SecureNAT.
- Клиент брандмауэра пересылает информацию о приложении службе брандмауэра ISA Server 2004; это позволяет служебным журналам брандмауэра собирать информацию об использовании приложений и помогает определить, какие приложения используются для получения доступа к узлам и службам Интернета.
- Клиент брандмауэра отправляет информацию о пользователе службе брандмауэра; это позволяет брандмауэру ISA Server 2004 контролировать доступ на основе учетной записи пользователя и записывать информацию о пользователе в служебные журналы брандмауэра. Эта информация может быть извлечена и представлена в форме отчета.

Благодаря этим функциям клиент брандмауэра обеспечивает непревзойденный уровень функциональности и контроля доступа в своем классе. Поэтому рекомендуется всегда устанавливать клиент брандмауэра на любой компьютер, поддерживающий программное обеспечение клиента брандмауэра.

Однако, поскольку конфигурирование клиента брандмауэра предполагает установку программного обеспечения клиента брандмауэра, многие администраторы сетей сомневаются в том, что стоит устанавливать клиент брандмауэра. Многие администраторы брандмауэра ISA Server 2004 не имеют ни времени, ни средств на то, чтобы вручную устанавливать программное обеспечение клиента брандмауэра на каждом компьютере корпоративной сети.

В качестве решения этой проблемы предлагается автоматизировать установку клиента брандмауэра. Для этого существуют два способа, которые не подразумевают покупку дополнительного программного обеспечения, но могут существенно упростить установку программного обеспечения клиента брандмауэра на большом количестве компьютеров в корпоративной сети:

- установка и управление с применением групповых политик;
- сценарий установки без вмешательства **пользователя.**

Далее описаны эти методы, а также основные параметры конфигурации клиента ISA Server, которые нужно **установить** в консоли **ISA** Management.

Конфигурирование клиента брандмауэра и клиента Web-прокси в консоли управления ISA

Существует несколько параметров конфигурации, которые следует задать для клиента брандмауэра до настройки групповой политики или сценария установки без вмешательства пользователя для установки программного обеспечения клиента брандмауэра. Эти параметры, задаваемые в консоли управления **Microsoft Internet Security and Acceleration Server 2004,** определяют такие факторы, как автоматическое обнаружение клиента брандмауэра и то, как настраивается Web-браузер в процессе установки клиента брандмауэра.

Для настройки этих параметров выполните следующие действия на компьютере брандмауэра ISA Server 2004:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера, а затем разверните узел **Configuration** (Настройка).
2. Щелкните узел **Networks** (Сети), а затем щелкните **Networks** (Сети) на вкладке **Details** (Подробно). Правой кнопкой мыши щелкните внутреннюю сеть и щелкните **Properties** (Свойства).
3. В диалоговом окне **Internal Properties** (Внутренние свойства) щелкните вкладку **Firewall Client** (Клиент брандмауэра).
4. На вкладке **Firewall Client** (Клиент брандмауэра) установите флажок в поле **Enable Firewall client support for this network** (Разрешить поддержку клиента брандмауэра для этой сети). В разделе **Firewall client configuration** (Конфигурация клиента брандмауэра) введите имя компьютера брандмауэра ISA Server 2004 в текстовое поле **ISA Server name or IP-address** (Имя или IP-адрес ISA Server). Стандартной настройкой является имя компьютера. Однако нужно заменить имя компьютера (NetBIOS-имя) FQND-именем брандмауэра ISA Server 2004. Когда имя компьютера заменяется на FQDN-имя, компьютеры клиента брандмауэра могут использовать DNS для того, чтобы правильно разрешить имя брандмауэра ISA Server 2004. Это позволяет избежать одной из наиболее распространенных проблем с установкой соединения клиента брандмауэра. На DNS-сервере во внутренней сети должна быть запись, соответствующая этому имени.

Параметры конфигурации клиента Web-прокси представлены в разделе **Web browser configuration on the Firewall client computer** (Конфигурация Web-браузера на компьютере клиента брандмауэра). Эти параметры позволяют автоматически настроить Web-браузер в качестве клиента Web-прокси. Позже можно из-

менить эти настройки, тогда Web-браузеры автоматически обновят свои параметры в соответствии с новыми настройками.

Вариа нт Automatically detect settings (Автоматически обнаруживать параметры) позволяет Web-браузеру обнаруживать службу Web-прокси и самоконфигурироваться в соответствии с настройками, которые указываются на вкладке Web Browser (Web-браузер) диалогового окна Internal Properties (Внутренние свойства), показанного на рис. 5.50.

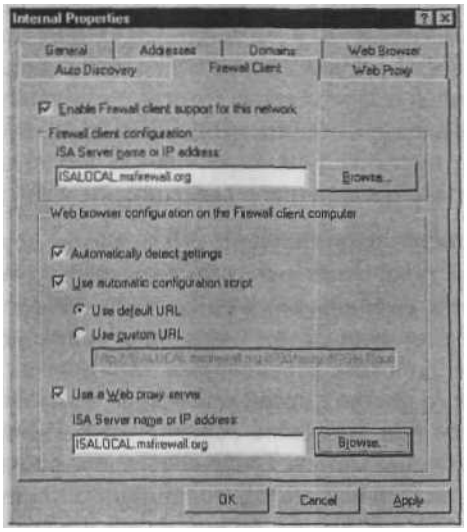


Рис. 5.50. Диалоговое окно Internal Properties (Внутренние свойства)

Вариант **Use automatic configuration script** (Использовать сценарий автоматического конфигурирования) позволяет присваивать адрес файла PAC Web-браузеру. Затем Web-браузер установит соединение с указанным ресурсом или с ресурсом по умолчанию. Ресурсом по умолчанию является компьютер брандмауэра ISA Server 2004. Обратите внимание, что при использовании ресурса по умолчанию полученная информация совпадет с информацией, которая была бы получена при настройке браузера на применение варианта **Automatically detect settings** (Автоматически обнаруживать настройки).

Вариант **Use default URL** (Использовать URL по умолчанию) автоматически настраивает браузер на установку соединения с брандмауэром ISA Server 2004 для получения информации об автоматической настройке. Если нужно создать собственный файл PAC, замещающий настройки в автоматически сгенерированном файле на брандмауэре ISA Server 2004, можно воспользоваться вариантом **Use custom URL** (Использовать назначенный URL). Более подробная информация о файле PAC и файлах автоматической настройки клиента прокси приводится в статье «Using

Automatic Configuration and Automatic Proxy» (Использование автоматической настройки и автоматического прокси) на сайте **www.microsoft.com/resources/documentation/ie/5/all/reskit/en-us/part5/ch21auto. mspx.**

Вариант **Use** a **Web Proxy server** (Использовать сервер Web-прокси) позволяет настроить Web-браузер так, чтобы он использовал брандмауэр ISA Server 2004 в качестве своего Web-прокси, но при этом он не может воспользоваться возможностями сценариев автоматической настройки. Эта настройка обеспечивает улучшенную производительность Web-браузера по сравнению с конфигурацией клиента SecureNAT, но при этом нельзя воспользоваться настройками, содержащимися в сценарии автоматической настройки. Наиболее важная настройка в сценарии автоматической настройки включает имена и адреса узлов, которые должны использоваться *для прямого доступа.* Поэтому следует избегать использования этого варианта за исключением тех случаев, когда нужно использовать прямой доступ для того, чтобы обойти Web-прокси при установке соединения с выбранными Web-сайтами.

> ПРИМЕЧАНИЕ Конфигурация клиента Web-прокси для поддержки Direct Access (прямого доступа) позволяет обходить службу Web-прокси при установке соединения с выбранными Web-сайтами. Некоторые Web-сайты не соответствуют интернет-стандартам (например, сайты Java), и поэтому они не могут корректно работать с серверами Web-прокси. Эти сайты можно настроить для прямого доступа, тогда клиентские компьютеры не будут пользоваться Web-прокси при установке соединения с этими сайтами, а будут применять альтернативные методы соединения с ними. Для того чтобы клиент использовал альтернативный метод соединения, клиентский компьютер должен быть настроен как клиент брандмауэра и/или клиент SecureNAT.

1. Щелкните вкладку **Web Browser** (Web-браузер). В этом диалоговом окне (рис. 5.51) имеется несколько настроек для конфигурирования клиентов Web-прокси с помощью сценария автоматического конфигурирования. Следует отметить, что для того чтобы эти варианты вступили в силу, нужно настроить клиентов Web-прокси на использование сценария автоматического конфигурирования либо с помощью автоматического обнаружения и автоматического конфигурирования, либо вручную, указав местоположение сценария автоматического конфигурирования.

   Вариант **Bypass proxy for Web server in this network** (Не использовать прокси для Web-сервера в этой сети) позволяет Web-браузеру использовать прямой доступ для прямого соединения с серверами, которые доступны посредством одиночного имени типа метки. Например, если пользователь получает доступ к Web-серверу во внутренней сети с адресом **URL http://SERVERl,** то браузер клиента Web-прокси не будет отправлять запрос на брандмауэр ISA Server 2004. Вместо этого Web-браузер установит прямое соединение с компьютером SERVER1. Это уменьшает нагрузку на брандмауэр ISA Server 2004 и позволяет пользовате-

лям избегать замыкания через брандмауэр ISA Server 2004 для получения доступа к ресурсам внутренней сети.

Вариант **Directly access computers specified in the Domains tab** (Напрямую устанавливать доступ к компьютерам, указанным на вкладке Домены) позволяет настраивать прямой доступ к компьютерам, содержащимся на вкладке **Domains** (Домены), которые используются клиентом брандмауэра для определения того, какие хосты являются частью внутренней сети, и для обхода брандмауэра ISA Server 2004 при установке соединения с хостами, являющимися частью того же домена. Клиент Web-прокси также может использовать домен из этого списка для прямого доступа. Рекомендуется всегда устанавливать этот вариант, потому что он уменьшает нагрузку на брандмауэр ISA Server 2004, так как клиенты Web-прокси не обращаются к брандмауэру для доступа к ресурсам внутренней сети.

Список **Directly access these servers or domains** (Напрямую устанавливать доступ к этим серверам или доменам) представляет собой список адресов компьютеров или имен доменов, которые можно настроить для прямого доступа. Щелкните кнопку **Add** (Добавить).

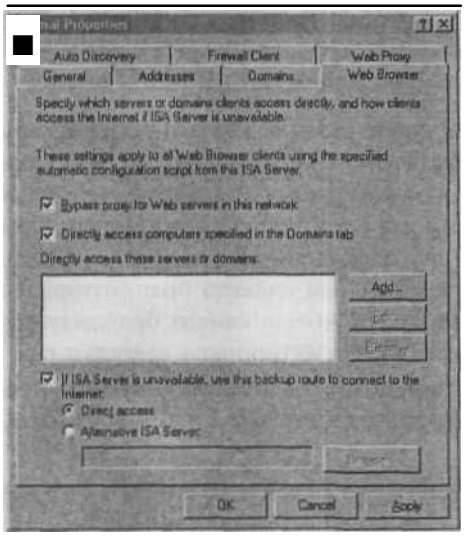


Рис. 5.51. Вкладка **Web** Browser (Web-браузер) в диалоговом окне **Internal Properties** (Внутренние свойства)

2. В диалоговом окне **Add Server** (Добавить сервер), показанном на рис. 5.52, можно выбрать вариант **IP address within this range** (IP-адрес из этого диапазона), а затем ввести IP-адрес или диапазон IP-адресов компьютеров, к которым нужно разрешить прямой доступ. Также можно выбрать вариант **Domain or computer** (Домен или компьютер) и ввести имя компьютера или полное доменное имя ком-

пьютера, к которому нужно установить прямой доступ. Обычно для прямого доступа вводят имя домена msn.com, потому что этот домен, наряду с доменами passport.com и hotmail.com, должен быть настроен для прямого доступа, чтобы упростить соединения клиента Web-прокси с узлом Microsoft Hotmail.

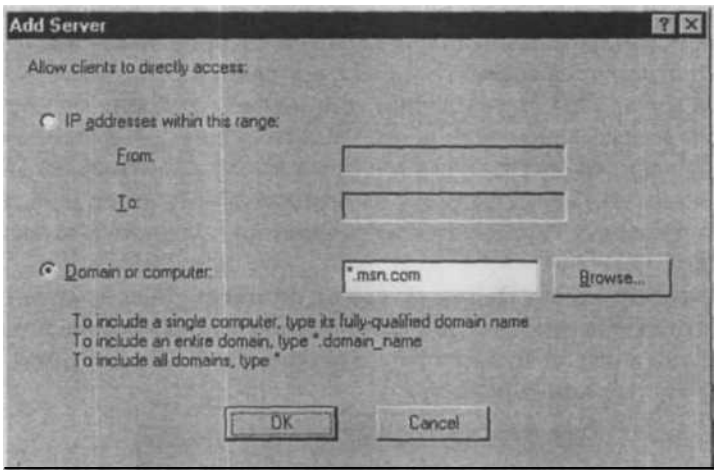


Рис. 5.52. Диалоговое окно Add Server (Добавить сервер)

3. Если ISA Server недоступен, вариант **Use this backup route to connect to the Internet** (Использовать этот запасной маршрут для соединения с Интернетом) позволяет компьютерам, настроенным в качестве клиентов Web-прокси, использовать другие средства для соединения с Интернетом. Обычно это означает, что **клиент** Web-прокси для соединения с Интернетом будет использовать конфигурацию клиента SecureNAT или клиента брандмауэра. Если компьютер не настроен как клиент SecureNAT и/или клиент брандмауэра, то любой доступ будет невозможен, когда служба Web-прокси недоступна.
4. Щелкните Apply (Применить), а затем щелкните OK, после того как были внесены изменения в конфигурацию в диалоговом окне **Internal Properties** (Внутренние свойства).
5. Щелкните **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.

Конфигурирование клиента брандмауэра и клиента Web-прокси завершено, теперь можно установить клиента брандмауэра на клиентских компьютерах под защитой брандмауэра ISA Server 2004, и эти параметры будут автоматически настроены на клиентских компьютерах.

Установка программного обеспечения с помощью групповой политики

В некоторых случаях не нужно устанавливать клиент брандмауэра на всех компьютерах сети. Например, контроллеры доменов и опубликованные серверы не нужно настраивать как клиенты брандмауэра. Можно создать отдельное подразделение для клиентов брандмауэра, а затем настроить групповую политику для подразделения, чтобы установка клиента брандмауэра выполнялась только на компьютерах, входящих в это подразделение. Таким образом осуществляется контроль установки программного обеспечения с помощью групповой политики.

> ПРИМЕЧАНИЕ Добавление компьютеров в подразделение клиентов брандмауэра является одним из возможных решений. При наличии необходимых знаний об Active Directory можно связать объект групповой политики с более высоким уровнем (доменом или сайтом). При этом не придется перемещать компьютер в другое подразделение и создавать групповую политику для каждого подразделения. Однако возможно потребуется отфильтровать объект групповой политики с помощью фильтров групп или фильтров WMI (Windows Management Instrumentation, инструментальные средства управления средой Windows), что предполагает административные трудозатраты. По умолчанию все компьютеры размещаются в контейнере компьютеров (это не то же, что подразделение); нужно либо связать групповую политику с этим доменом или сайтом, либо создать подразделение и добавить компьютеры к этому подразделению, а затем связать с объектом групповой политики. Стоит отметить, что не все компьютеры настраиваются как клиенты брандмауэра, поскольку контроллеры домена и другие серверы не должны использовать клиента брандмауэра без крайней необходимости.

Выполните следующие действия на контроллере домена, чтобы создать подразделение, а затем настройте установку и управление программным обеспечением так, чтобы установить клиент брандмауэра на компьютерах, входящих в это подразделение:

1. Щелкните **Start** (Пуск) и выберите меню **Administrative Tools** (Администри рование). Щелкните **Active Directory Users and Computers** (Пользователи и компьютеры Active Directory). Правой кнопкой мыши щелкните имя домена и щелкните **Organizational Unit** (Подразделение).
2. В диалоговом окне **New Object — Organizational Unit** (Новый объект — под разделение) введите имя подразделения в текстовое поле **Name** (Имя). В этом примере подразделение называется **FWCLIENTS.** Щелкните ОК.
3. Щелкните узел **Computers** (Компьютеры) в левой панели консоли. Правой кноп кой мыши щелкните клиентский компьютер и команду **Move** (Переместить).
4. В диалоговом окне **Move** (Переместить) щелкните подразделение **FWCLIENTS,** затем ОК.

5. Щелкните подразделение **FWCLIENTS.** В нем должен быть компьютер, который был в него перемещен.
6. Правой кнопкой мыши щелкните подразделение **FWCLIENTS** и щелкните команду **Properties** (Свойства).
7. Щелкните вкладку **Group Policy** (Групповая политика) в диалоговом окне **FW CLIENTS.** Щелкните кнопку **New** (Новый), чтобы создать **New Group PolicyObject** (Новый объект групповой политики). Выберите **New Group Policy Object** (Новый объект групповой политики) и щелкните **Edit** (Редактировать).
8. Разверните узел **Computer Configuration** (Конфигурирование компьютера), а затем разверните узел **Software Settings** (Настройки программного обеспечения). Правой кнопкой мыши щелкните **Software installation** (Установка программного обеспечения), установите курсор мыши на **New** (Новый) и щелкните **Package** (Пакет).
9. В текстовом поле **Open** (Открыть) введите путь к установочному пакету Microsoft для клиента брандмауэра (msi-файл) в текстовое поле **File name** (Имя файла). В этом примере путь к нему такой: \\isa2\mspclnt\MS_FWC.MSI, где isa2 — это NetBIOS-имя компьютера брандмауэра ISA Server 2004 или имя файлового сервера, на котором находятся установочные файлы клиента брандмауэра; mspclnt — это имя совместно используемого ресурса на компьютере брандмауэра ISA Server 2004, в котором находятся установочные файлы клиента брандмауэра, а MS_FWC.MSI — это имя установочного пакета Microsoft для клиента брандмауэра. После ввода пути щелкните **Open** (Открыть) (рис. 5.53).

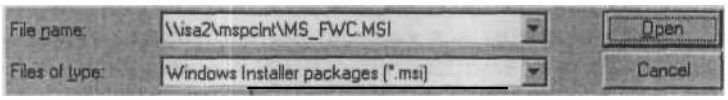


Рис. 5.53. Ввод пути к установочному пакету

10. В диалоговом окне **Deploy Software** (Развертывание программного обеспечения) выберите вариант Assigned (Назначенный) (рис. 5-54) и щелкните ОК Следует отметить, что при установке программного обеспечения с помощью узла **Computer Configuration** (Конфигурирование компьютера) нет варианта **Published** (Опубликованный). Программное обеспечение устанавливается до того, как пользователь выполнит вход в систему. Это важно, поскольку только локальные администраторы могут устанавливать программное обеспечение клиента брандмауэра при наличии пользователя, зарегистрированного в системе. Вместо этого можно назначить программное обеспечение компьютерам без пользователей, зарегистрированных в системе. Щелкните ОК.

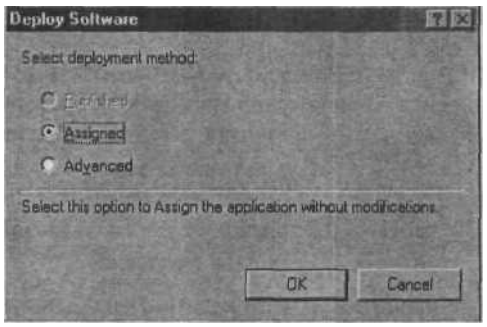


Рис. 5.54. Выбор варианта **Assigned** (Назначенный)

11. На правой панели консоли появится новый пакет программного обеспечения. На всех компьютерах в подразделении после их перезагрузки будет установлено программное обеспечение клиента брандмауэра. Также можно осуществлять управление программным обеспечением клиента брандмауэра, как это показано на рис. 5.55.

ПРИМЕЧАНИЕ Более подробно *о* том, как пользоваться всеми возможностями установки и сопровождения программного обеспечения с помощью групповой политики, рассказывается в статье «Step-by-Step Guide to Software Installation and Maintenance» (Пошаговая инструкция по установке и сопровождению программного обеспечения) на сайте: **ww w.microsoft.com/win-**do ws2000/techinfo/planning/management/swinstall.asp.

Рис. 5.55. Управляемое программное обеспечение

12. Закройте **Group Policy Object Editor** (Редактор объекта групповой политики) и консоль **Active Directory Users and Computers** (Пользователи и компьюте ры Active Directory).
13. После перезагрузки компьютеров в подразделении FWCLIENTS появится диало говое окно (рис. 5.56), которое показывает, как управляемое программное обес печение устанавливается на клиентских операционных системах Windows.

Рис. 5.56. Вход в систему

Сценарий установки без вмешательства пользователя

Еще один полезный метод, который можно использовать для установки программного обеспечения клиента брандмауэра на компьютерах, не являющихся членами домена, состоит в применении сценария установки без вмешательства пользователя (silent installation script). Этот метод может оказаться полезным, если пользователь, выполнивший вход в систему, является членом локальной группы администраторов. Сценарий установки без вмешательства пользователя не предлагает пользователю вводить данные и принимать решения.

Откройте документ **Notepad** (Блокнот); скопируйте следующую строку в новый текстовый документ и сохраните файл с именем fwcinstall.cmd: msiexec /i \\ISA2\mspclnt\MS_FWC.msi /qn /l'v c :\mspclnt_i.log. Запись //ISA2 — это имя компьютера брандмауэра ISA Server 2004, она зависит от того, куда производится установка. Остальная часть строки используется точно в таком виде. Затем пользователи могут перейти на Web-страницу или щелкнуть ссылку в сообщении электронной почты, указывающую на этот командный файл. Этот процесс очень прост, от пользователя требуется лишь щелкнуть ссылку для запуска сценария. Установка полностью прозрачна, единственное, что видит пользователь, — быстро появляющееся и исчезающее окно с командной строкой, а по окончании процедуры в области уведомления появится значок клиента брандмауэра.

> ПРЕДУПРЕЖДЕНИЕ Для установки программного обеспечения клиента брандмауэра пользователь должен иметь права администратора. Если у пользователя нет прав администратора, то программное обеспечение не будет установлено. В такой ситуации можно назначить программное обеспечение клиента брандмауэра компьютерам. Программное обеспечение устанавливается до того, как пользователь выполнит вход в систему, поэтому в таком случае в процессе установки не имеет значения, какие права есть у пользователя, выполняющего вход в систему.

SMS-сервер

Организации, в которых установлен SMS 2003 (Systems Management Server, сервер управления системами), могут воспользоваться функцией распределения программного обеспечения для развертывания программного обеспечения клиента брандмауэра. Процедура распределения программного обеспечения в SMS 2003 обеспечивает способность развертывания файлов программы установки Windows (msi-файлов) на любом компьютере, который назначен в среде SMS так же, как и в функции управления программным обеспечением с помощью групповой политики в Active Directory. Для развертывания клиента брандмауэра с помощью SMS 2003 выполните следующее.

1. Создайте группу, включающую все компьютеры, на которых нужно установить клиент брандмауэра. SMS-группа (collection) представляет собой группу сетевых

объектов, например компьютеров или пользователей, которые рассматриваются как **группа** SMS-управления. Можно настроить такие требования, как IP-адрес, конфигурация аппаратного обеспечения или добавить клиентов напрямую по имени, чтобы сгруппировать все компьютеры, на которых необходимо установить программное обеспечение клиента брандмауэра.

2. Создайте пакет, импортировав файл Windows клиента брандмауэра (MS_FWC.msi). Файл программы установки Windows автоматически включает различные варианты назначенной и неназначенной установки, которые мо гут использоваться для систем и пользователей. Также создаются программы для удаления клиента. Программы для систем настраиваются на установку кли ента с административными правами независимо от того, зарегистрирован ли пользователь в системе. Программы для пользователей устанавливают клиент, используя верительные данные зарегистрированного в системе пользователя. Этот метод имеет свои преимущества по сравнению с методом групповой политики, который не позволяет временно повышать права для установки приложения клиента брандмауэра.
3. Создайте SMS-уведомление, в котором указывается целевая группа и програм мы для установки. Чтобы контролировать развертывание, можно задать время, когда программа будет представлена членам группы.

Выводы

Сервер без клиентов приносит мало пользы, но ISA Server отличается тем, что есть несколько различных способов его настройки в качестве клиента ISA. Фактически различают три типа клиентов ISA: клиент SecureNAT, клиент брандмауэра и клиент Web-прокси. Выбор наиболее подходящего типа клиента за висит от ряда факторов, включая операционную систему клиента, поддерживаемые протоколы, и от того, нужно ли устанавливать на клиентских компьютерах клиентское программное обеспечение.

Клиент SecureNAT не требует установки никакого программного обеспечения и изменения настроек Web-браузера на клиентском компьютере. Нужно всего лишь изменить настройки TCP/IP клиентского компьютера так, чтобы в качестве основного шлюза выступал шлюз ISA Server. Так любой компьютер на базе любой популярной операционной системы может пользоваться защитой брандмауэра ISA Server 2004. Это относится к операционным системам сторонних производителей типа Linux/UNIX и Macintosh, а также к более ранним версиям операционных систем семейства Windows типа Windows 95, Windows 3x и MS-DOS, которые не поддерживаются программным обеспечением клиента брандмауэра. Клиент SecureNAT поддерживает все простые протоколы и даже сложные протоколы при условии установки фильтров приложения на компьютере ISA Server. Выбор клиента SecureNAT является логичным, если на клиентских компьютерах установлены различные операционные системы, которым нужно обеспечить защиту с помощью ISA, и если

клиентской системе необходимо обеспечить доступ к другим протоколам помимо HTTP/HTTPS или FTP.

Клиент Web-прокси также работает со всеми операционными системами при наличии совместимого Web-браузера (такого, который можно настроить на использование прокси-сервера). Однако клиент Web-прокси является намного более ограниченным в плане поддерживаемых протоколов — HTTP/HTTPS и FTP по HTTP-туннелю. Во многих случаях этого вполне достаточно, и в сущности это ограничение играет роль дополнительной меры по обеспечению безопасности, т. к. оно запрещает доступ к другим приложениям. Клиент Web-прокси имеет одно преимущество по сравнению с клиентом SecureNAT: он может обеспечивать проверку подлинности на брандмауэре ISA (если брандмауэр запросит верительные данные). Клиенты SecureNat могут обеспечить проверку подлинности только для клиентских приложений, поддерживающих SOCKS 5, и только если на компьютере ISA Server установлен фильтр приложения SOCKS 5.

Клиент брандмауэра является идеальным выбором для клиентских компьютеров на базе современных операционных систем Windows. Его можно установить на базе Windows 98 и более поздних версий операционных систем Windows, он поддерживает все приложения на базе Winsock, использующие протоколы TCP/UDP, включая приложения, которые предполагают использование сложных протоколов. Не нужны никакие фильтры приложений; это уменьшает административные трудозатраты при обслуживании сервера. Самое главное: клиент брандмауэра позволяет осуществлять жесткий контроль пользовательского/группового доступа, поскольку верительные данные направляются на брандмауэр ISA Server для проверки подлинности, причем не нужно специально конфигурировать клиент или предпринимать другие действия. Клиент брандмауэра также дает возможность администраторам осуществлять более тщательный контроль благодаря записи в журналы информации о пользователях и приложениях.

Чаще всего причиной проблем с получением доступа и обеспечением безопасности являются ошибки в конфигурации клиента. Однако конфигурирование клиента Web-прокси и установка клиента брандмауэра не требуют много времени и усилий. Эти процессы могут быть автоматизированы. DHCP- и DNS-серверы можно настроить для поддержки автоматического обнаружения клиента Web-прокси и клиента брандмауэра. Установка может быть автоматизирована с помощью групповой политики или сценария установки без вмешательства пользователя, или же можно использовать набор средств IEAK, чтобы настроить клиента Web-прокси. Если в сети имеется SMS-сервер, его можно использовать для развертывания клиента брандмауэра.

Выбор правильной конфигурации клиента и правильная настройка клиентских компьютеров является важной составной частью успешного развертывания ISA Server 2004, поэтому важно понимать три типа клиента и пошаговый процесс настройки каждого типа, прежде чем устанавливать ISA Server.

Краткое резюме по разделам

Клиент SecureNAT ISA Server 2004

0 Клиент SecureNAT не требует установки программного обеспечения. Единственное требование — клиентская операционная система должна быть настроена с адресом основного шлюза, который может маршрутизировать соединения с Интернетом через брандмауэр ISA Server 2004.

И Клиент SecureNAT поддерживает все протоколы, не требующие вторичных соединений. Протоколы, требующие вторичных соединений (например, FTP) предполагают наличие фильтра приложения на брандмауэре ISA Server 2004.

0 Клиент SecureNAT поддерживает только протоколы, входящие в список протоколов (Protocol list) брандмауэра ISA Server 2004. Если для протокола нет определения протокола, то клиент SecureNAT не может получить доступ к этому протоколу, даже если имеется правило доступа, которое разрешает компьютеру клиента SecureNAT доступ ко всем протоколам.

й Все операционные системы могут быть настроены как клиенты SecureNAT.

И Клиент SecureNAT не поддерживает клиент-серверные отношения. На клиенте SecureNAT нет программного обеспечения, которое напрямую взаимодействует с брандмауэром ISA Server 2004.

0 Клиент SecureNAT не пересылает информацию о пользователе или приложении на брандмауэр ISA Server 2004. Брандмауэр записывает исходный IP-адрес соединения и размещает в системных журналах только эту информацию.

0 Клиент SecureNAT является единственным клиентом, имеющим доступ к протоколам, отличным от TCP/UDP, например ЮМР (используемый командами ping и tracert) и PPTP (требуемый GRE, не использующий протоколы TCP или UDP в качестве транспортного протокола).

И Поскольку клиент SecureNAT не поддерживает отправку информации о пользователе на брандмауэр ISA Server 2004, невозможно обеспечить безопасную пользовательскую/групповую проверку подлинности при помощи протоколов, отличных от TCP/UDP.

0 Клиент SecureNAT предназначен для операционных систем сторонних производителей. На базе всех операционных систем Microsoft, которые поддерживают клиента брандмауэра, должен быть установлен клиент брандмауэра. Исключением являются опубликованные серверы и серверы сетевой инфраструктуры, типа контроллеров домена, DHCP-, DNS- и IAS-серверов.

0 В общем, все опубликованные серверы должны быть настроены как клиенты SecureNAT. Исключением является случай, когда правило Web-публикации или публикации серверов настроено на замену исходного клиентского IP-адреса на IP-адрес брандмауэра ISA Server 2004.

0 Клиент SecureNAT может воспользоваться возможностями кэша Web-прокси брандмауэра ISA Server 2004, если клиент SecureNAT получает доступ в Интернет по правилу, в котором активирован фильтр Web-прокси.

И Клиент SecureNAT в значительной степени зависит от текущей инфраструктуры маршрутизации; все маршрутизаторы на пути между клиентом SecureNAT и Интернетом должны быть осведомлены о том, что все запросы, связанные с Интернетом, должны исходить с внутреннего IP-адреса брандмауэра ISA Server 2004.

Клиент Web-прокси ISA Server 2004

И Все приложения, рассчитанные на поддержку Web-прокси, можно настроить в качестве клиентов Web-прокси.

0 Конфигурация клиента Web-прокси не требует установки программного обеспечения; единственное требование состоит в том, чтобы приложение, которое поддерживает соединения Web-прокси, было настроено на использование брандмауэра ISA Server 2004 в качестве сервера Web-прокси.

0 Клиент Web-прокси может отправлять верительные данные пользователя на брандмауэр; это позволяет осуществлять жесткий контроль пользовательского/группового доступа для клиентов Web-прокси.

0 Клиент Web-прокси поддерживает только соединения по протоколам HTTP, HTTPS (SSL/TLS) и загрузки по FTP.

0 С помощью клиента Web-прокси нельзя размещать данные по протоколу FTP.

И Клиент Web-прокси автоматически пользуется возможностями кэша Web-прокси на брандмауэре ISA Server 2004.

И Клиент Web-прокси напрямую взаимодействует с брандмауэром ISA Server 2004, что делает его независимым от инфраструктуры маршрутизации. Единственное требование состоит в том, чтобы компьютер клиента Web-прокси был осведомлен о маршруте к внутреннему интерфейсу брандмауэра ISA Server 2004.

0 Клиент Web-прокси можно автоматически настроить на соединение с Интернетом через брандмауэр ISA Server 2004 с помощью протокола WPAD и автоматического обнаружения клиента Web-прокси. Это позволяет всем Web-браузерам в сети автоматически знать, какой IP-адрес использовать для своей конфигурации клиента Web-прокси, и администратору не приходится настраивать каждого клиента отдельно.

И Возможно, у клиента Web-прокси не получится установить соединение с некоторыми Web-сайтами, например использующими Java и встроенные частные адреса для обмена данными или другим способом нарушающими работу Web-прокси, регламентированную RFC. Для таких сайтов можно настроить прямой доступ.

0 Клиент Web-прокси можно настроить на использование сценария автоматического конфигурирования. Сценарий автоматического конфигурирования предоставляет клиенту Web-прокси информацию об имени брандмауэра ISA Server 2004

и об узлах, которые должен обходить клиент Web-прокси с помощью механизма прямого доступа.

0 Исходящие соединения клиента Web-прокси проходят через брандмауэр по SSL-туннелю. В отличие от Web-публикаций, когда доступ к опубликованному Web-серверу осуществляется через мост SSL-SSL, брандмауэр ISA Server 2004 не может оценить содержимое, передаваемое по SSL-туннелю через брандмауэр.

Клиент брандмауэра ISA Server 2004

0 Клиент брандмауэра может отправлять информацию о пользователе и приложении на брандмауэр ISA Server 2004, эта информация сохраняется в файлах журналов.

0 Клиент брандмауэра поддерживает вторичные соединения без помощи фильтра приложения.

И Клиент брандмауэра не требует определения протокола для доступа к протоколу. Если настроено правило доступа, разрешающее доступ ко всем протоколам, то клиент брандмауэра сможет получить доступ ко всем протоколам TCP и UDP даже при отсутствии определения протокола для конкретного протокола.

0 Клиент брандмауэра перехватывает все соединения по протоколам TCP и UDP с приложений на базе Winsock и перенаправляет их напрямую на брандмауэр ISA Server 2004. Это позволяет клиенту брандмауэра быть относительно независимым от текущей инфраструктуры маршрутизации. Единственное требование состоит в том, чтобы компьютер клиента брандмауэра знал **маршрут к** внутреннему интерфейсу брандмауэра ISA Server 2004.

И Клиент брандмауэра может автоматически находить брандмауэр ISA Server 2004 с помощью WPAD-записей в DHCP или **DNS.**

0 Клиент брандмауэра можно развернуть с помощью групповой политики Active Directory, с помощью SMS-сервера или сценария установки по умолчанию.

0 Если SMS-сервер не применяется, то пользователь, выполнивший вход в систему, должен быть членом локальной группы администраторов, чтобы установить программное обеспечение клиента брандмауэра.

0 При установленном программном обеспечении клиента брандмауэра можно также автоматически настроить Web-браузер в качестве клиента Web-прокси.

И Клиент брандмауэра требует установки программного обеспечения; это программное обеспечение поддерживается всеми 32-битными операционными системами семейства Windows за исключением Windows 95.

И Клиент брандмауэра совместим со всеми типами клиентов ISA Server 2004. Однако один компьютер не может выступать в роли клиента SecureNAT и клиента брандмауэра для приложений на базе Winsock, соединение с которыми выполняется по протоколам UDP или TCP.

Автоматизация инициализации клиента ISA Server 2004

И Клиентов SecureNAT можно настроить автоматически, применив DHCP для назначения соответствующего адреса основного шлюза.

И Клиент Web-прокси можно автоматически настроить на использование брандмауэра ISA Server 2004 с помощью WPAD-записей в DNS и/или DHCP.

0 Клиент Web-прокси можно автоматически настроить при установке клиента брандмауэра.

И Клиент Web-прокси не требует установки программного обеспечения; приложения, поддерживающие соединения Web-прокси, могут быть настроены как клиенты Web-прокси для брандмауэра ISA Server 2004.

Автоматизация установки клиента брандмауэра

И Программное обеспечение клиента брандмауэра можно установить с помощью SMS-сервера, групповой политики Active Directory или сценария установки без вмешательства пользователя.

0 Клиент брандмауэра может автоматически обнаруживать брандмауэр ISA Server 2004 с помощью WPAD-записей в DNS и/или DHCP.

И Клиент брандмауэра можно вручную настроить на установку соединения с конкретным брандмауэром ISA Server 2004.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма «Ask the Author»), Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: компьютер настроен как клиент SecureNAT. Невозможно установить соединение с узлом FTP. В чем проблема?

О: Брандмауэр ISA Server 2004 включает фильтр приложения FTP, который разрешает соединения *с* узлами FTP без применения клиента брандмауэра. Это означает, что для поддержки вторичных соединений для применения протокола FTP не нужно устанавливать программное обеспечение клиента брандмауэра на клиентском компьютере. Нужно изучить другие причины невозможности установки соединения с узлами FTP, потому что установка программного обеспечения клиента брандмауэра не решит эту проблему.

В: Компьютер настроен как клиент брандмауэра. Используется программа Microsoft Outlook, но невозможно установить соединение с сервером POP3- Почему можно

установить соединение с серверами с помощью других протоколов, а с помощью POP3 нельзя?

Oл При использовании Outlook стандартные настройки клиента брандмауэра предусматривают обход клиента брандмауэра. Поэтому для доступа к POP3-серверу у клиента должен быть альтернативный механизм. Нужно настроить клиент также как клиент SecureNAT или настроить клиент брандмауэра так, чтобы в Outlook использовался клиент брандмауэра. Это можно сделать в настройках клиента брандмауэра в консоли управления Microsoft Internet Security and Acceleration Server 2004.

B: Компьютер настроен как клиент Web-прокси. Попытки установить соединение с чатами и другими сайтами Java оканчиваются неудачей. Что нужно сделать, чтобы соединение было установлено?

O: Есть несколько причин, объясняющих, почему соединения с этими узлами не устанавливаются. Скорее всего, код Java не совместим с RFC Web-прокси серверами. Поскольку ISA Server 2004 является RFC-совместимым Web-прокси сервером, он не всегда может получить содержимое с сайтов, не являющихся совместимыми. Кроме того, некоторые чаты и другие приложения, работающие в режиме онлайн, используют дополнительные протоколы помимо HTTP. В такой ситуации нужно настроить клиент как клиент SecureNAT или клиент брандмауэра для поддержки дополнительных протоколов. Сайты, не совместимые с RFC Web-прокси серверами, можно настроить так, чтобы клиенты Web-прокси использовали прямой доступ через конфигурации клиента SecureNAT и/или клиента брандмауэра.

B: На DHCP-сервере настроена WPAD-запись, и некоторые клиенты могут автоматически получать информацию об автоматическом конфигурировании для настроек клиента Web-прокси и клиента брандмауэра. Однако большинство компьютеров не могут получить эту информацию с DHCP-сервера. Почему?

O: Не забывайте, что при использовании DHCP-сервера для присвоения информации об автоматическом конфигурировании с помощью WPAD-записей только пользователи, зарегистрированные как локальные администраторы, могут получать информацию по WPAD- протоколу. Для пользователей, не зарегистрированных Б качестве членов локальной группы администраторов, нужно настроить WPAD-запись в DNS для поддержки их соединений.

B: Мне нужен доступ к Интернет-играм и нескольким голосовым приложениям в Интернете, например к игре Yahoo и голосовому чату Yahoo. Мои клиенты настроены как клиенты SecureNAT, но пользователи не могут установить соединение. Что нужно сделать, чтобы разрешить такие типы приложений?

Os Для поддержки приложений, требующих вторичных протоколов, нужно установить клиент брандмауэра. Большинство голосовых приложений и многие интернет-игры требуют вторичных соединений. Хотя для этих типов приложений

может использоваться клиент SecureNAT, нужно создать фильтр приложения для поддержки каждого интернет-приложения, требующего использования сложных протоколов. Также, если приложение клиента поддерживает прокси SOCKS 4, можно настроить это приложение на использование SOCKS 4 для установки соединения с фильтром SOCKS 4 на компьютере брандмауэра ISA Server 2004.

В: Мне нужно установить соединение с Web-сайтом по SSL-протоколу с помощью порта TCP 8081, но клиент Web-прокси отказывается устанавливать соединение. Что нужно сделать, чтобы установить соединение с Web-сайтом по протоколу SSL, используя другой порт?

О: Ознакомьтесь с информацией на Web-сайте Джима Харрисона (Jim Harrison) www.isatools.org. На этом сайте Джим предлагает замечательное инструментальное средство, позволяющее расширить диапазон портов для SSL-туннеля и включить в него любые порты по желанию. Во время написания этой книги этот файл назывался isa2k4_ssl_tpr.zip.

В: Клиенты SecureNAT не могут установить соединение с Интернетом. Клиенты Web-прокси и клиенты брандмауэра устанавливают соединение с Интернетом без проблем. Основной шлюз настроен правильно. Почему клиенты брандмауэра и Web-прокси могут установить соединение с Интернетом, а клиенты SecureNAT не могут?

О: Скорее всего, это объясняется тем, что клиенты SecureNAT не настроены на использование DNS-сервера, который может разрешать имена хостов в Интернете. В отличие от клиентов Web-прокси и клиентов брандмауэра, за которых разрешение имен выполняется брандмауэром ISA Server 2004, клиент SecureNAT должен сам выполнять разрешение имен. Тщательно проверьте настройки DNS на клиенте SecureNAT и настройте его на использование DNS-сервера, разрешающего имена хостов в Интернете.

Глава

Установка и конфигурирование брандмауэра ISA

Основные темы главы:

- **Задачи и анализ действий перед установкой брандмауэра ISA**
- **Установка брандмауэра ISA «с нуля» на компьютере с несколькими сетевыми адаптерами**
- **Стандартная конфигурация брандмауэра ISA после установки**
- **Настройка системной политики после установки брандмауэра ISA**
- **Установка обновления брандмауэра ISA**
- **Установка брандмауэра ISA на компьютере с одним сетевым адаптером (брандмауэр ISA с одним сетевым интерфейсом)**
- **Конфигурирование брандмауэра ISA для быстрого старта**
- **Улучшение базовой конфигурации брандмауэра ISA и базовой операционной системы**

Задачи и анализ действий перед установкой брандмауэра ISA

Прежде чем устанавливать программное обеспечение брандмауэра ISA, нужно рассмотреть несколько ключевых моментов:

- системные требования;
- настройка таблицы маршрутизации;
- размещение DNS-сервера;
- конфигурирование сетевых интерфейсов брандмауэра ISA;
- автоматизированная установка;
- установка с помощью режима администрирования службы терминалов.

Системные требования

Компьютер, на котором будет установлено программное обеспечение брандмауэра ISA, должен удовлетворять следующим требованиям:

- процессор Intel или AMD с частотой 550 МГц и выше;
- операционная система Windows 2000 или Windows Server 2003;
- минимум 256 Мб памяти; минимум 512 Мб памяти для систем без функции Web-кэширования и 1 000 Мб памяти для брандмауэра ISA с Web-кэшированием;
- хотя бы один сетевой адаптер; два и более сетевых адаптера необходимы для обеспечения функций фильтрации с отслеживанием соединений и проверки на уровне приложения с отслеживанием соединений;
- дополнительный сетевой адаптер для каждой сети, соединенной с компьютером ISA Server;
- один локальный жесткий диск, отформатированный с файловой системой NTFS, и хотя бы 150 Мб свободного пространства на жестком диске (за вычетом пространства на жестком диске, предназначенного для кэширования);
- дополнительное пространство на диске; в идеале, на отдельном;
- дополнительное свободное пространство на диске; *в* идеале, отдельный диск, если планируется использовать функцию Web-кэширования брандмауэра ISA.

При установке программного обеспечения брандмауэра ISA на базе Windows 2000 нужно учесть несколько моментов:

- нужно установить пакет исправлений Windows 2000 Service Pack 4 (SP4) или более поздней версии;
- нужно установить Internet Explorer 6 или более поздней версии;
- при использовании Windows 2000 SP4 SplitStream[1] нужно также установить обновление, указанное в статье 821 887 «Events for Authorization Roles Are Not

[1] Совместный исследовательский проект университета Райе и корпорации Microsoft, предусматривающий создание распределенной сети доставки содержимого, которая позволяет загружать крупные файлы даже клиентам с низкой скоростью подключения. — *Прим. пер.*

Logged in the Security Log When You Configure Auditing for Windows 2000 Authorization Manager Runtime» в Базе знаний Microsoft (http://support.microsoft.com/default.aspx?scid=kb;enus;821887);

- общий ключ L2TP IPSec настроить нельзя;
- при использовании политики RADIUS не поддерживается изолирование VPN-подключений;
- все службы ISA Server работают с помощью учетной записи локальной системы.

Еще одним важным вопросом является планирование ресурсов. Приведенный ранее список отражает минимальные системные требования для установки и запуска программного обеспечения брандмауэра ISA, идеальную конфигурацию можно получить, соразмеряя возможности аппаратного обеспечения для оптимизации производительности программного обеспечения брандмауэра ISA на конкретном компьютере. В табл. 6.1 представлены основные требования при выборе процессора, памяти, емкости жесткого диска и сетевого адаптера на основании скорости канала связи с Интернетом.

Табл. 6.1. Основные требования к процессору, памяти, емкости жесткого диска и сетевому адаптеру в зависимости от скорости канала связи с Интернетом

Скорость канала связи с Интернетом	До 7,5 Мбит/с	До 25 Мбит/с	До 45 Мбит/с	Примечания
Количество процессоров	1	1	1	
Тип процессора	Pentium III 550 МГц (и больше)	Pentium IV с частотой 2,0-3,0 ГГц	Хеоп с частотой 2,0-3,0 ГГц	В реализациях, требующих только фильтрации с отслеживанием соединений («проверка с отслеживанием соединений» означает, что не нужно обеспечивать более безопасную проверку с отслеживанием соединений на уровне приложения), использование процессоров Pentium IV и Хеоп позволяет достичь скорости кабельных ЛВС
Память	256 Мб	512 Мб	1 Гб	При включенном режиме Web-кэширования указанный объем памяти нужно увеличить примерно на 256-512 Мб
Свободное пространство на жестком диске	150 Мб	2,5 Гб	5 Гб	Сюда не включается пространство жесткого диска, необходимое для кэширования и ведения журналов
Сетевой адаптер	10/100 Мбит/с	10/100 Мбит/с	100/1000 Мбит/с	Это требования для сетевых адаптеров, не подключенных к Интернету

(см. след. стр.)

Табл. 6.1. (окончание)

Скорость канала связи с Интернетом	До 7,5 Мбит/с	До 25 Мбит/с	До 45 Мбит/с	Примечания
Одновременные VPN-подключения удаленного доступа	150	700	850	Standard Edition брандмауэра ISA поддерживает жестко запрограммированный максимум в 1000 одновременных VPN-подключений. Enterprise Edition поддерживает столько подключений, сколько поддерживает базовая операционная система, и не имеет жестко закодированных ограничений

Подробный анализ производительности брандмауэра ISA и оценки базовых ресурсов представлен в документе «Microsoft ISA Server 2004 Performance Best Practices» (Производительность ISA Server 2004) на сайте www.microsoft.com/technet/prodtechnol/isa/2004/plan/bestpractices.mspx.

Настройка таблицы маршрутизации

Таблица маршрутизации на компьютере брандмауэра ISA должна быть настроена до установки программного обеспечения брандмауэра ISA. Таблица маршрутизации должна включать маршруты ко всем сетям, которые не являются локальными для сетевых интерфейсов брандмауэра ISA. Эти записи в таблице маршрутизации необходимы, потому что у брандмауэра ISA может быть только один основной шлюз. Обычно основной шлюз настроен на сетевом интерфейсе, используемом для инешней сети. Поэтому, если имеется внутренняя сеть или другая сеть, содержащая несколько дочерних сетей, нужно настроить записи в таблице маршрутизации так, чтобы брандмауэр ISA мог взаимодействовать с компьютерами и другими устройствами в соответствующих дочерних сетях. Сетевой интерфейс с основным шлюзом используется для соединения с Интернетом напрямую или с помощью вышестоящих маршрутизаторов.

Записи в таблице маршрутизации являются критически важными для поддержки конфигураций брандмауэра ISA «сеть-в-Сети», которые представляют собой идентификатор сети, расположенной «за» сетевой интерфейсной картой брандмауэра ISA, т. е. не в локальной сети.

Например, на рис. 6.1 представлен образец простой конфигурации «сеть-в-Сети».

В этой схеме IP-адресов небольшой организации используется два идентификатора сети: 192.168.1.0/24 и 192.168.2.0/24. Сеть, локальная по отношению к внутреннему интерфейсу брандмауэра ISA, имеет идентификатор сети 192.168.1.0/24. Сеть, удаленная от внутреннего интерфейса брандмауэра ISA, — 192.168.2.0/24. Маршрутизатор корпоративной сети разделяет сеть и маршрутизирует пакеты между этими двумя идентификаторами сети.

|1аг.1бв.1.гд11

Рис. 6.1. Сеть в Сети

Сетевая модель брандмауэра ISA включает обе эти сети как часть одной Сети («Сеть» с заглавной буквы означает сеть, определенную на брандмауэре ISA). Можно предположить, что 192.168.1.0/24 является Сетью, определенной на брандмауэре ISA, потому что она включает в себя весь идентификатор сети, но также можно предположить, что идентификатор сети 192.168.2.0/24 определяется как вторая Сеть, определенная на брандмауэре ISA. Однако это неверно, потому что сетевая модель брандмауэра ISA включает все сети *(все* IP-адреса), доступные с конкретного интерфейса брандмауэра ISA, как часть одной и той же сети.

Это объясняется тем, что хосты в одной определенной на брандмауэре ISA Сети не используют брандмауэр ISA для взаимодействия между собой. Брандмауэр ISA не выступает в качестве посредника при взаимодействии между хостами с идентификаторами сети 192.168.1.0/24 и 192.168.2.0/24, потому что в этом случае хосты будут использовать брандмауэр для получения доступа к хостам, с которыми они могут взаимодействовать напрямую.

В этом примере должна быть запись в таблице маршрутизации на брандмауэре ISA, указывающая, что для получения доступа к идентификатору сети 192.168.2.0/24, соединение должно быть перенаправлено на IP-адрес 192.168.2.1 на корпоративном маршрутизаторе. Можно использовать консоль RRAS (Routing and Remote Access Service, служба маршрутизации и удаленного доступа) или команды ROUTE и netsh в командной строке для добавления записи в таблицу маршрутизации.

Брандмауэр ISA должен знать маршрут к каждому внутреннему идентификатору сети. Если окажется, что соединения направляются через брандмауэр ISA к хостам в корпоративной сети неправильно, нужно проверить записи в таблице маршрутизации на брандмауэре ISA: они должны указывать правильный шлюз для каждого из этих идентификаторов сети.

> СОВЕТ Можно существенно упростить определения сетей и таблицу маршрутизации брандмауэра ISA, создав корректную инфраструктуру IP-адресации с дочерними сетями, что позволит суммировать маршруты.

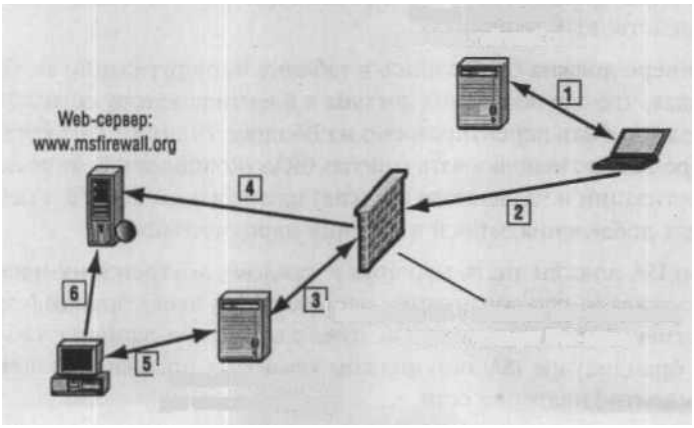
Размещение DNS-сервера

Чаще всего проблемы соединения с брандмауэром ISA связаны с DNS-сервером и разрешением имени хоста. Если инфраструктура разрешения имен в организации настроена неправильно, то одним из первых от неправильного разрешения имен пострадает брандмауэр ISA.

Брандмауэр ISA должен правильно разрешать как корпоративные DNS-имена, так и имена из Интернета. Брандмауэр ISA выполняет разрешение имен для клиентов Web-прокси и для клиентов брандмауэра. Если брандмауэр не может правильно выполнять разрешение имен, то клиентам Web-прокси и клиентам брандмауэра не удастся установить соединение с Интернетом.

Правильное разрешение имен для ресурсов корпоративной сети также является критически важным, потому что брандмауэр ISA должен правильно разрешать имена для ресурсов корпоративной сети, опубликованных по правилам Web-публикации. Например, при создании правила Web-публикации по протоколу SSL брандмауэр ISA должен правильно перенаправлять входящие запросы на соединение на FQDN-имя (Fully Qualified Domain Name, полное имя домена), используемое для обычного имени на сертификате Web-сайта, связанного с опубликованным Web-сервером в корпоративной сети.

Идеальной инфраструктурой разрешения имен является расщепленная DNS, позволяющая внешним хостам разрешать имена в общедоступные адреса, а хостам корпоративной сети разрешать имена в частные адреса. На рис. 6.2 показано, как действует расщепленная инфраструктура DNS при разрешении имен для хостов в корпоративной сети, а также хостов, «блуждающих» между корпоративной сетью и удаленными узлами в Интернете.



Общий DNS-сервер
для www.msfirewall.org
[1] Брандмауэр ISA с правилом Web-публикации,
который публикует Web-сервер

[2] Частный DNS-сервер для
www.msfirewall.org

Рис. 6.2. Работа расщепленной инфраструктуры DNS

1. Удаленному пользователю нужно получить доступ к ресурсам на корпоративном Web-сервере www.msfirewall.org, который обслуживается в Сети под защитой брандмауэра ISA и опубликован с помощью правила Web-публикации брандмауэра ISA. Удаленный пользователь отправляет запрос на www.msfirewall.org, и общий DNS-сервер, отвечающий за этот домен, выполняет разрешение имени в IP-адрес на внешнем интерфейсе брандмауэра ISA с помощью Web-приемника, указанного в правиле Web-публикации.

2. Удаленный Web-клиент отправляет запрос на IP-адрес на внешнем интерфейсе, используемом Web-приемником для правил Web-публикации.
3. Брандмауэр ISA разрешает имя www.msfirewall.org в реальный IP-адрес, связан ный с Web-сайтом www. msfirewall.org в корпоративной сети, отсылая запрос на DNS-сервер внутренней сети, отвечающий за домен msfirewall.org.
4. Брандмауэр ISA перенаправляет соединение на реальный IP-адрес, связанный с Web-сайтом www.msfirewall.org в корпоративной сети.
5. Хосту в корпоративной сети нужно получить доступ к ресурсам на Web-сайте www.msfirewall.org. Пользователь корпоративной сети отправляет запрос на корпоративный DNS-сервер, отвечающий за домен msfirewall.org. Корпоратив ный DNS-сервер разрешает имя www.msfirewall.org в реальный IP-адрес, связан ный с Web-сайтом www.msfirewall.org в корпоративной сети.
6. Web-клиент в корпоративной сети устанавливает прямое соединение с Web-сервером www.msfirewall.org. Web-клиент не выполняет замыкание через бранд мауэр ISA для получения доступа к Web-сайту www.msfirewall.org в корпоратив ной сети, потому что клиенты Web-прокси настроены на прямой доступ к ре сурсам в домене msfirewall.org.

Расщепленная инфраструктура DNS обеспечивает прозрачный доступ для пользователей независимо от того, где они находятся. Пользователи могут перемещаться между корпоративной сетью и удаленными узлами и использовать одно и то же имя для доступа к корпоративным ресурсам. Им не нужно менять настройки своих почтовых клиентов, новостных клиентов и других приложений, потому что для доступа к ресурсам используется одно и то же имя независимо от их местоположения. В любой организации, которой нужно обеспечить поддержку пользователей, «блуждающих» между корпоративной сетью и удаленными узлами, должна использоваться расщепленная инфраструктура DNS.

Требования к расщепленной инфраструктуре DNS включают в себя:

- DNS-сервер, отвечающий за домен, который разрешает имена для ресурсов этого домена во внутренние адреса, используемые для доступа к этим ресурсам;
- DNS-сервер, отвечающий за домен, который разрешает имена для ресурсов в этом домене в общие адреса, используемые для доступа к этим ресурсам;
- удаленным пользователям должны быть присвоены адреса DNS-сервера, кото рые перенаправляют запросы к домену на общий DNS-сервер. Это легко осуще ствить с помощью DHCP;
- корпоративным пользователям должны быть присвоены адреса DNS-сервера, которые перенаправляют запросы к домену на частный DNS-сервер. Это легко осуществить с помощью DHCP;
- брандмауэр ISA должен разрешать имена опубликованных ресурсов и других ресурсов Сети под защитой брандмауэра ISA в частный адрес, используемый для доступа к этому ресурсу.

В большинстве организаций, использующих брандмауэр ISA, есть один или несколько внутренних DNS-серверов. Хотя бы один из этих DNS-серверов должен быть настроен на разрешение имен внутренних хостов и хостов в Интернете, а брандмауэр ISA должен быть настроен на использование этого DNS-сервера. Если имеется DNS-сервер во внутренней сети, то не следует настраивать интерфейсы брандмауэра ISA на использование внешнего DNS-сервера. Это распространенная ошибка, которая ведет к замедлению разрешения имен или к ошибкам.

СОВЕТ В статье Джима Харрисона (Jim Harrison) *Designing An ISA Server Solution on a Complex Network* (Разработка решений для ISA Server в сложной сети) на сайте http://isa server. org/tutorial s/Designi ng_An„S A_Server_Solution_on_a_Complex_Network.html представлена информация о сетевых конфигурациях, поддерживающих брандмауэры ISA.

Конфигурирование сетевых интерфейсов брандмауэра ISA

Наверное, наименее понятно при конфигурировании брандмауэра ISA, как правильно настраивать информацию об IP-адресах на сетевых интерфейсах брандмауэра ISA, потому что разрешение имен является настолько сложным, что начинающие администраторы брандмауэра часто не уделяют вопросам разрешения имен хостов DNS и NetBIOS-имен достаточно времени и, как следствие, делают ошибки.

Существуют два основных типа конфигурации сетевого интерфейса:

- отлаженная инфраструктура разрешения имен в корпоративной сети под защи той брандмауэра ISA;
- отсутствие отлаженной инфраструктуры разрешения имен в корпоративной сети под защитой брандмауэра ISA.

В табл. 6.2 и *6.3* показана правильная информация об IP-адресах для этих двух типов конфигурации для брандмауэра ISA с двумя сетевыми интерфейсами.

Табл. 6.2. Отлаженная инфраструктура разрешения имен в корпоративной сети

Параметры	Внутренний интерфейс	Внешний интерфейс
Клиент для сетей Microsoft Networks	Включен	Выключен
Совместное использование файлов и принтеров для Microsoft Networks	Включено, только если брандмауэр ISA поддерживает общие ресурсы для клиентов брандмауэра	Выключено
Драйвер монитора сети	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)

Табл. 6.2. (окончание)

Параметры	Внутренний интерфейс	Внешний интерфейс
Протокол Интернета (TCP/IP)	Включен	Включен
IP-адрес	Действительный IP-адрес в сети, *к* которой подключен внутренний интерфейс	Действительный IP-адрес в сети, к которой подключен внешний интерфейс, общий или частный *в* зависимости от сетевой инфраструктуры
Маска подсети	Действительная маска подсети в сети, к которой подключен внутренний интерфейс	Действительная маска подсети в сети, к которой подключен внешний интерфейс
Основной шлюз	Отсутствует. Никогда не следует настраивать основной шлюз на любом внутреннем интерфейсе или интерфейсе DMZ на брандмауэре ISA	IP-адрес вышестоящего маршрутизатора (либо *в* корпоративной сети, либо интернет-провайдера в зависимости от следующего перехода), обеспечивающего доступ в Интернет
Основной DNS-сервер	Внутренний DNS-сервер, который может разрешать имена хостов внутренней сети и Интернета	Отсутствует. Не указывайте адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA
Альтернативный DNS-сервер	Второй внутренний DNS-сервер, который может разрешать имена хостов внутренней сети и Интернета	Отсутствует. Не указывайте адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA
Регистрация адресов соединения в DNS	Отключена. Нужно вручную создавать записи на DNS-сервере во *в* нутре н ней сети, чтобы разрешить клиентам разрешать имя внутреннего интерфейса брандмауэра ISA	Отключена
WINS	Введите IP-адрес еще одного DNS-сервера во внутренней сети. Особенно пригодится для VPN-клиентов, которые хотят просматривать серверы во внутренней сети с помощью NetBIOS-имени/службы браузера	Отсутствует
Настройки WINS NetBIOS	Стандартные	Отключить NetBIOS поверх TCP/IP
Порядок интерфейса	Верх списка интерфейса	Под внутренним интерфейсом

Табл. 6.3. Отсутствие отлаженной инфраструктуры разрешения имен в корпоративной сети

Параметры	Внутренний интерфейс	Внешний интерфейс
Клиент для сетей Microsoft Networks	Включен	Выключен
Совместное использование файлов и принтеров для Microsoft Networks	Включено, только если брандмауэр ISA поддерживает общие ресурсы для клиентов брандмауэра	Выключено
Драйвер монитора сети	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)
Протокол Интернета (TCP/IP)	Включен	
IP-адрес	Действительный IP-адрес в сети, к которой подключен внутренний интерфейс	Включен Действительный IP-адрес в сети, к которой подключен внешний интерфейс, общий или частный в зависимости от сетевой инфраструктуры. Или же DHCP, если это требование интернет-провайдера
Маска подсети	Действительная маска подсети в сети, к которой подключен внутренний интерфейс	Действительная маска подсети в сети, *к* которой подключен внешний интерфейс. Может назначаться интер нет-провай дером посредством DHCP
Основной шлюз	Отсутствует. Никогда не следует настраивать основной шлюз на любом внутреннем интерфейсе или интерфейсе DMZ на брандмауэре ISA	IP-адрес вышестоящего маршрутизатора (либо в корпоративной сети, либо Интернет-провайдера в зависимости от следующего перехода), обеспечивающего доступ в Интернет. Может назначаться интернет-провайдером с помощью DHCP
Основной DNS-сервер	Внешний DNS-сервер, который может разрешать имена хостов Интернета. Обычно это DNS-сервер интернет-провайдера. Примечание: если для получения информации об IP-адресах для внешнего интерфейса используется DHCP, то не следует указывать DNS-сервер на внутреннем интерфейсе брандмауэра ISA	Отсутствует. Может быть назначен интернет-провайдером посредством DHCP

Табл. 6.3. (окончание)

Параметры	Внутренний интерфейс	Внешний интерфейс
Альтернативный DNS-сервер	Второй внешний DNS-сервер, который может разрешать имена хостов Интернета. Примечание: если для получения информации об IP-адресах от интернет-провайдера для внешнего интерфейса используется DHCP, то не следует указывать DNS-сервер на внутреннем интерфейсе брандмауэра ISA	Отсутствует. Не следует вводить адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA за исключением случая, когда он назначен интернет-провайдером посредством DHCP
Регистрация адресов соединения в DNS	Выключен	Выключен
WINS	Отсутствует	Отсутствует
Настройки WINS NetBIOS	Стандартные	Отключить NetBIOS поверх TCP/IP
Порядок интерфейса	Верх списка интерфейса. Примечание: если для получения информации об IP-адресе для внешнего интерфейса от интернет-провайдера используется DHCP, то не нужно перемещать внутренний интерфейс вверх списка	Верх списка интерфейса при использовании DHCP-сервера интернет-провайдера для назначения адресов DNS-сервера

Важно не только уметь конфигурировать информацию об IP-адресах для интерфейсов сервера Windows, но и знать, как изменять порядок интерфейса. Порядок интерфейса необходим для того, чтобы определить предпочтительный сервер имен, адреса которого будут использоваться.

> СОВЕТ Можно отследить, с какой сетью соединяется тот или иной интерфейс, переименовав сетевые интерфейсы в пользовательском интерфейсе Network and dial-up connections (Сетевые подключения). Правой кнопкой мыши щелкните сетевой интерфейс и нажмите кнопку Rename (Переименовать). Введите новое имя интерфейса. Например, для простого брандмауэра с тремя сетевыми интерфейсами обычно интерфейсы называются LAN (ЛВС), WAN (ГВС) и DMZ (демилитаризованная зона).

Для изменения порядка интерфейса выполните следующие действия: 1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и выберите в контекстном меню пункт **Properties** (Свойства).

2. В окне **Network and Dial-up Connections** (Сетевые подключения) щелкните мышью меню **Advanced** (Дополнительно), а затем нажмите кнопку **Advanced Settings** (Дополнительные параметры).
3. В диалоговом окне **Advanced Settings** (Дополнительные параметры) (рис. 6.3) щелкните мышью внутренний интерфейс в списке **Connections** (Подключения) на вкладке **Adapters and Bindings** (Адаптеры и привязки). Выбрав внутренний интерфейс, щелкните мышью стрелку вверх, чтобы переместить этот внутренний интерфейс наверх списка интерфейсов.

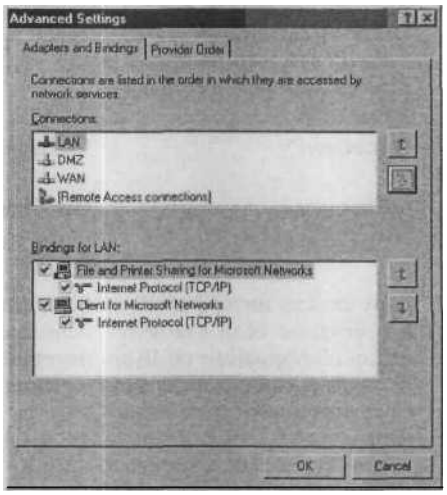


Рис. 6.3. Диалоговое окно Advanced Settings (Дополнительные параметры)

4. Нажмите **кнопку OK** в диалоговом окне **Advanced Settings** (Дополнительные параметры).

Автоматизированная установка

Для упрощения подготовки к работе нескольких брандмауэров ISA с общей схемой установки и конфигурирования можно выполнить автоматизированную установку брандмауэра ISA. Автоматизированная установка зависит от **правильной** конфигурации файла msiund.ini, в котором содержится конфигурационная информация, используемая программой установки брандмауэра ISA в автоматизированном режиме.

ПРИМЕЧАНИЕ Следует обратить особое внимание на последнюю запись в табл. 6.4, показывающую, как можно включить заготовку политики брандмауэра ISA в автоматизированную установку. Это позволяет автоматизировать установку и конфигурирование брандмауэра ISA для тысяч брандмауэров ISA путем выполнения простой команды из командной строки.

Стандартный файл msisaund.ini находится на компакт-диске ISA Server 2004 в каталоге \FPC. В табл. 6.4 содержатся наиболее важные записи и значения, настраиваемые *в* файле msisaund.ini.

Табл. 6.4. Записи *и* значения в файле msisaund.ini

Запись	Описание
PIDKEY	Указывается ключ программного продукта
INTERNALNETRANGES	Указывается диапазон адресов во внутренней сети. В Msisaund.ini должен **быть** указан хотя бы один IP-адрес. Иначе установка не будет выполнена. Синтаксис следующий: N Froml-Tol,Frorn2-To2,..FromN-ToN, где N — число диапазонов, а FromI и Tol являются начальным и конечным адресом каждого диапазона
InstallDir « {Install_directory}	Указывается каталог установки для ISA Server. Если не указано, то по умолчанию установка производится на первый диск с достаточным свободным пространством. Синтаксис следующий: ДискДПапка. По умолчанию используется папка %Program Files%\Microsoft ISA Server
COMPANYNAME = Company_Name	Указывается название компании, выполняющей установку программы
DONOTDELLOGS = {0|1}	Значение 1 означает, что файлы журналов не удаляются с компьютера. По умолчанию устанавливается значение 0
DONOTDELCACHE = {0|1}	Значение 1 означает, что файлы кэша на компьютере не удаляются. По умолчанию устанавливается значение 0
ADDLOCAL = (MSFirewall_ Management}, {MSFirewall_ Services}, {Message_Screener}, {Publish_Share_Directory}, {MSDE}	Указывается список компонентов (разделенных запятыми), которые должны быть установлены на компьютере. Для установки всех компонентов введите ADDLOCAL = ALL
REMOVE = {MSFirewall_ Management}, (MSFirewall Services}, {Message_Screener}, {Publish_Share_Directory}, {MSDE}	Указывается список компонентов (разделенных запятыми), которые должны быть удалены с компьютера. Для удаления всех компонентов введите REMOVE = AL_L
IMPORT_CONFIG_FILE = Importfile.xml	Указывается файл *конфигурации* для **импорта**

Для изменения автоматизированной установки брандмауэра ISA необходимо выполнить следующие действия:

1. Изменить файл Msisaund.ini.
2. В командной строке ввести:

```
PathToISASetup\Setup.exe [/[X|R]] /V" /q[b|n]
FULLPATHANSWERFILE=Y'PathToINIFile\MSISAUND. INI\""
```

D Параметр PathToISASetup означает путь к установочным файлам ISA Server 2004 (корневая папка на установочном диске ISA Server или общая папка в сети, содержащая файлы ISA Server).

D Параметр /q[b|n] выполняет тихую скрытую автоматизированную установку. Значение b означает, что процесс установки будет отображаться. Если указать значение n, то не будут выводиться никакие диалоговые окна.

a Параметр /R выполняет повторную автоматизированную установку.

a Параметр /X выполняет автоматизированное удаление программы.

□ Параметр PathToINIFile указывает путь к папке, содержащей информацию для автоматизированной установки.

При выполнении автоматизированной установки нужно учесть несколько моментов.

- Для выполнения автоматизированной установки нужно быть членом группы администраторов.
- Невозможно выполнить автоматизированную установку на компьютере с уста новленным ISA Server 2000.
- Запись INTERNALNETRANGES в файле Msisaund.ini должна содержать хотя бы один диапазон IP-адресов, который включает один из IP-адресов компьютера с ISA Server. Иначе установка не будет выполнена.
- Образец файла (Msisaund.ini) представлен на установочном компакт-диске в папке FPC.
- Например, команда CD\FPC\setup.exe /v" /qn FULLPATHANSWERFILE=\"G\ MSISA-UND.INI\"" выполняет автоматизированную установку ISA Server с помощью файла Msisaund.ini, расположенного в папке c:\.
- Установка компонента MSDE при установке функции **Advanced logging** проходит некорректно, если выполняется удаленная установка брандмауэра ISA с помо щью служб терминалов в режиме сервера приложения. Для корректной устанэвки MSDE следует использовать службы терминалов в режиме администрирования.

Установка служб терминалов в режиме администрирования

Брандмауэр ISA можно установить с помощью соединения со службами терминалов в режиме администрирования. После завершения установки правило системной политики настраивается так, чтобы соединения по протоколу RDP (Remote Desktop Protocol, протокол удаленного рабочего стола) были разрешены только с IP-адреса компьютера, который был подключен в процессе установки программного обеспечения брандмауэра ISA. Это отличается от стандартной настройки системной политики при установке программного обеспечения брандмауэра ISA с консоли, когда любой хост во внутренней сети может инициировать RDP-соединение с внутренним интерфейсом брандмауэра ISA.

Установка брандмауэра ISA «с нуля» на компьютере с несколькими сетевыми адаптерами

Следующая последовательность действий показывает, как установить программное обеспечение ISA Server 2004 на компьютере с двумя сетевыми интерфейсами (двумя картами Ethernet) на базе ОС Windows Server 2003. Это «чистый компьютер» в том смысле, что на нем установлено только программное обеспечение Windows Server 2003 и настроена информация об IP-адресах на каждом из интерфейсов компьютера. Также на этом компьютере настроена таблица маршрутизации.

Для того чтобы установить программное обеспечение брандмауэра ISA на компьютере с несколькими сетевыми интерфейсами, выполните следующие действия:

1. Вставьте установочный компакт-диск ISA Server 2004 в привод для компакт-дисков или установите соединение с общим сетевым ресурсом, в котором находятся установочные файлы ISA Server 2004. Если процесс установки не запустится автоматически, дважды щелкните мышью файл isaautomn.exe в корневом ката логе папки с установочными файлами.
2. На странице **Microsoft Internet Security and Acceleration Server 2004** щел кните мышью ссылку **Review Release Notes** (Информация о версии) и прочти те информацию об этой версии. Информация о версии содержит очень важные и актуальные сведения об изменениях в основных функциях программного обес печения брандмауэра. Эта информация может не входить в файл справки, по этому настоятельно рекомендуется ее прочесть. После прочтения этой инфор мации щелкните мышью ссылку **Read Setup and Feature Guide** (Прочитать ру ководство по установке и функциям). Можно прочитать это руководство сразу, просмотреть только основные темы или распечатать его. Щелкните мышью ссылку **Install ISA Server 2004** (Установить ISA Server 2004).
3. Нажмите кнопку **Next** (Далее) на странице **Welcome to the Installation Wizard for Microsoft ISA Server 2004** (Мастер установки Microsoft ISA Server 2004).
4. Выберите вариант **I accept the terms in the license agreement** (Я согласен с условиями лицензионного соглашения) на странице **License Agreement** (Ли цензионное соглашение). Нажмите кнопку **Next** (Далее).
5. На странице **Customer Information** (Информация о пользователе) введите ваше имя и название организации в текстовые поля **User Name** (Имя) **и Organization** (Организация). Введите серийный номер в текстовое поле **Product Serial Num ber** (Серийный номер). Если вы уже устанавили оценочную версию програм много обеспечения брандмауэра ISA, а сейчас устанавливаете лицензионную вер сию, то создайте резервную копию конфигурации с помощью интегрирован ного инструмента создания резервной копии брандмауэра ISA и удалите оце ночную версию. Перезапустите установку лицензионной версии программно го обеспечения. Нажмите кнопку **Next** (Далее).

6. На странице **Setup** Type (Тип установки) (рис. 6.4) выберите **Custom** (Пользовательский). Если вы не хотите устанавливать программное обеспечение ISA Server 2004 на диске C:, нажмите кнопку **Change (Изменить),** чтобы изменить место установки программы на жестком диске. При выборе варианта **Typical** (Обычная) не устанавливаются общие ресурсы для клиентов брандмауэра и средство просмотра сообщений SMTP. При выборе **варианта Complete** (Полная) устанавливается программное обеспечение брандмауэра ISA, консоль управления Microsoft Internet Security and Acceleration Server 2004, средство просмотра сообщений SMTP и общие ресурсы для клиентов брандмауэра. Нажмите кнопку **Next** (Далее).

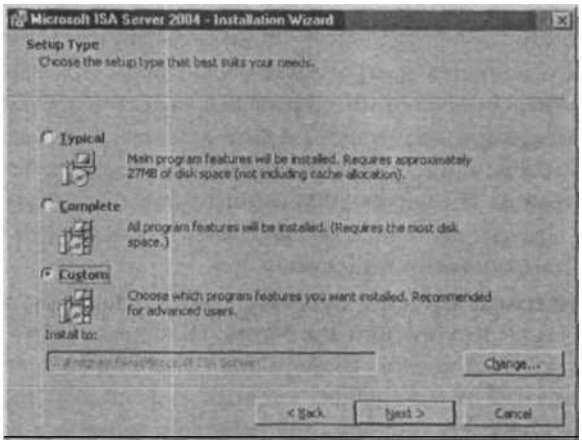


Рис. 6.4. Страница Setup Type (Тип установки)

7. На странице **Custom Setup** (Пользовательская установки) (рис. 6.5) выберите компоненты, которые должны быть установлены. По умолчанию при выборе варианта **Custom** (Пользовательская) устанавливаются **функции** брандмауэра Firewall Services, функции управления ISA Server Management и функция расширенных возможностей создания журналов Advanced Logging. Advanced Logging — это создание журналов в формате БД MSDE, обеспечивающее улучшенные возможности поиска по журналам и фильтрации информации в журналах. Средство просмотра сообщений SMTP Message Screener, которое используется для того, чтобы контролировать поступление в сеть и отправку из сети спама и сообщений электронной почты с определенными типами вложений, по умолчанию не устанавливается. Прежде чем устанавливать Message Screener, следует установить SMTP-службу IIS 6.0 или IIS 5.0 на компьютере брандмауэра ISA. Если попытаться установить средство просмотра сообщений SMTP на брандмауэр ISA до установки SMTP-службы *IIS,* то появится сообщение об ошибке и нужно будет перезапустить установку брандмауэра ISA. Используйте стандартные настройки и нажмите кнопку **Next** (Далее).

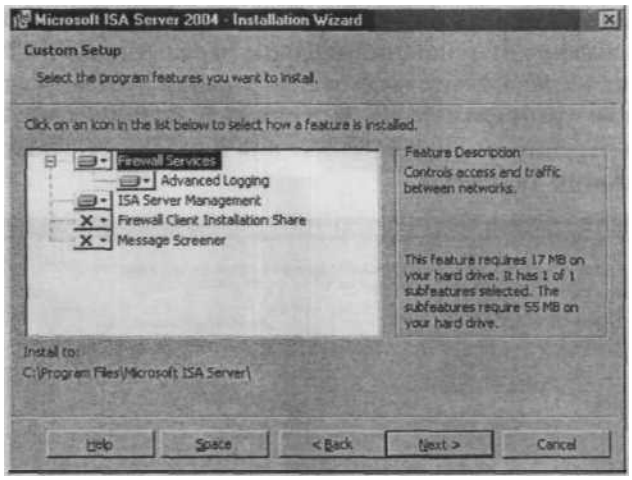


Рис. 6.5. Страница **Custom Setup** (Пользовательская установка)

8. На странице **Internal Network** (Внутренняя сеть) (рис. 6.6) нажмите кнопку **Add** (Добавить). Эта внутренняя сеть отличается от внутренней сети, которая использовалась в таблице LAT в ISA Server 2000. В случае ISA Server 2004 внутренняя сеть содержит доверяемые сетевые службы, с которыми должен взаимодействовать брандмауэр ISA. В качестве примера таких служб можно привести контроллеры домена Active Directory, DNS-серверы, DHCP-серверы, серверы терминалов и рабочие станции управления. Системная политика брандмауэра использует внутреннюю сеть для нескольких правил системной политики. Системная политика рассматривается далее в этой главе.
9. Определите адреса, входящие во внутреннюю сеть по умолчанию, на странице установки внутренней сети. Можно вручную ввести адреса, которые будут входить во внутреннюю сеть, указав первый и последний адрес диапазона адресов внутренней сети в текстовых полях **From** (От) и To (Кому) и щелкнув кнопку **Add** (Добавить). Но лучше настроить внутреннюю сеть по умолчанию, используя вариант **Select Network Adapter** (Выбрать сетевой адаптер). Это позволяет программе установки брандмауэра ISA воспользоваться таблицей маршрутизации, чтобы определить адреса, используемые для внутренней сети по умолчанию. Поэтому важно правильно настроить записи таблицы маршрутизации, прежде чем устанавливать брандмауэр ISA. Щелкните мышью **Select Network Adapter** (Выбрать сетевой адаптер) (рис. 6.6).
10. В диалоговом окне **Configure Internal Network** (Настроить внутреннюю сеть) снимите флажок в поле **Add the following private ranges...** (Добавить следующие частные диапазоны...). Лучше снять этот флажок, потому что во многих организациях используются подсети сетевых идентификаторов для частных адресов в различных сетях, определенных на брандмауэре ISA. Оставьте флажок в

поле **Add address ranges based on the Windows Routing Table** (Добавить адресные диапазоны на основании таблицы маршрутизации Windows), как показано на рис. 6.7. Установите флажок в поле рядом с сетевым адаптером, представляющим внутреннюю сеть по умолчанию. В данном случае сетевые интерфейсы были переименованы так, чтобы имя интерфейса отражало его расположение. Нажмите кнопку OR

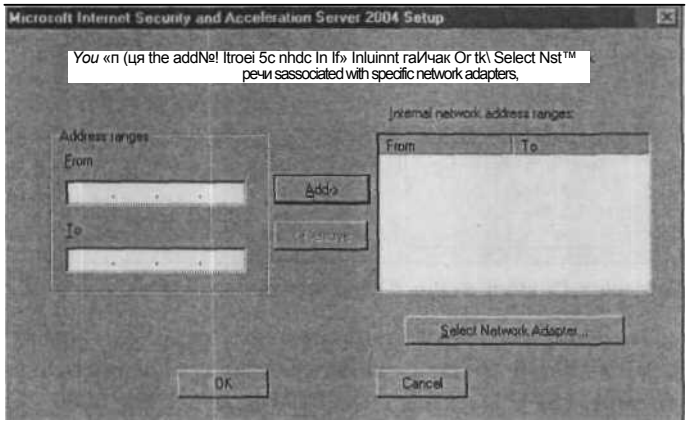


Рис. 6.6. Страница Internal Network Address (Адрес внутренней сети)

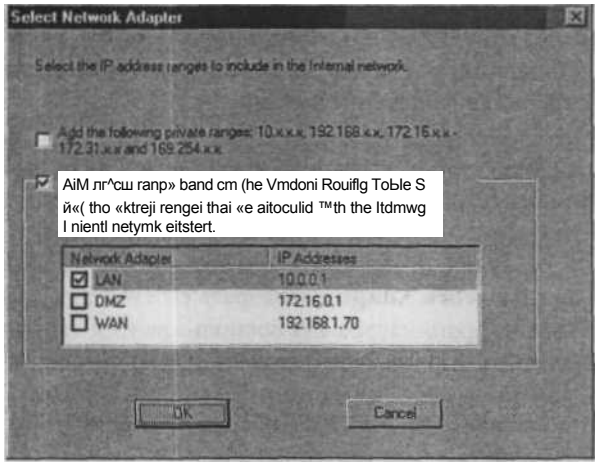


Рис. 6.7. Страница Select Network Adapter (Выбрать сетевой адаптер)

11. Нажмите кнопку OK в диалоговом окне **Setup Message** (Сообщение об установке) (рис. 6.8), сообщающем, что The Internal network was defined, based on the Windows routing table (Внутренняя сеть была определена на основе таблицы маршрутизации Windows).

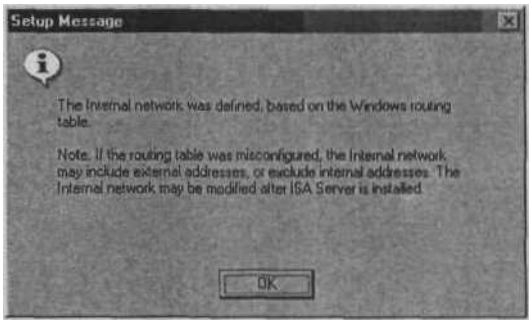


Рис. 6.8. Диалоговое окно Setup Message (Сообщение об установке)

12. Нажмите кнопку OK в диалоговом окне **Internal network address ranges** (Диапазоны адресов внутренней сети), как показано на рис. 6.9.

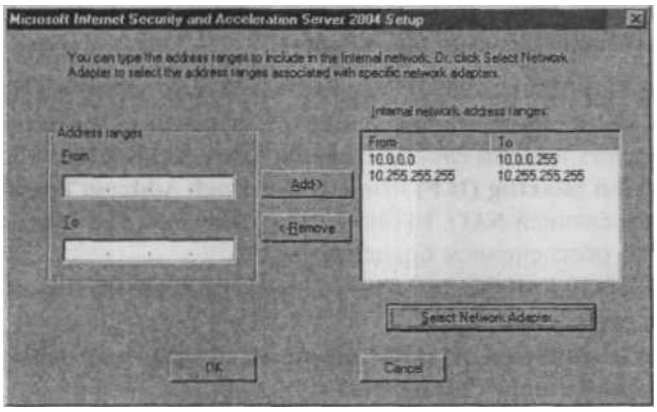


Рис. 6.9. Страница Internal network address ranges (Диапазоны адресов внутренней сети)

13. Нажмите кнопку **Next** (Далее) на странице **Internal Network** (Внутренняя сеть).
14. Установите флажок в поле **Allow computers running earlier versions of Fire wall Client software to connect** (Разрешить соединения компьютерам с более ранними версиями клиента брандмауэра) (рис. 6.10), если нужно обеспечить поддержку клиентов брандмауэра, работающих с предыдущими версиями Winsock Proxy (Proxy Server 2.0) или программным обеспечением клиента брандмауэра ISA Server 2000. Это позволит и дальше использовать программное обеспечение клиента брандмауэра ISA Server 2000 после перехода на ISA Server 2004. При переходе на клиент брандмауэра версии ISA 2004 канал между клиентами бранд мауэра и брандмауэром ISA будет шифроваться. Программное обеспечение кли ента брандмауэра ISA Server 2004 шифрует верительные данные пользователя, которые пересылаются с компьютера клиента брандмауэра на брандмауэр ISA в прозрачном режиме. Нажмите кнопку **Next** (Далее).

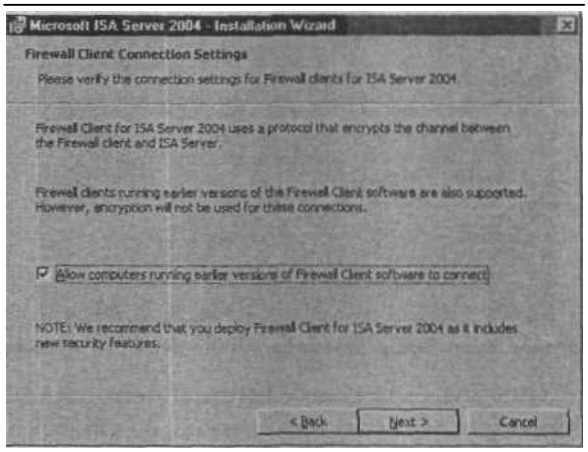


Рис. 6.10. Страница Firewall Client Connection Settings (Настройка соединения клиента брандмауэра)

15. На странице **Services** (Службы) укажите, что службы **SNMP** и **IIS Admin Servi ce** должны быть остановлены в процессе **установки.** Если на компьютере с бран дмауэром ISA установлены службы **Internet Connection Firewall (ICF) / Inter net Connection Sharing (ICF)** и/или **IP Network Address Translation** (Служ ба RRAS с трансляцией NAT), то они будут отключены, т. к. они конфликтуют с программным обеспечением брандмауэра ISA.
16. Нажмите кнопку **Install** (Установить) на странице **Ready to Install the Program** (Установка программы).
17. На странице **Installation Wizard Completed** (Завершение работы мастера ус тановки) нажмите кнопку **Finish** (Готово).
18. Нажмите кнопку **Yes** (Да) в диалоговом окне Microsoft ISA Server с предупрежде нием о необходимости перезапуска системы (рис. 6.11). Обратите внимание, что не нужно перезапускать компьютер, если программное обеспечение брандмау эра ISA устанавливалось на этом компьютере раньше. Необходимость переза пуска объясняется тем, что стек протоколов TCP/IP изменяется так, что дина мический диапазон портов драйвера TCP/IP расширяется до 65 535- Если про грамма установки определит, что этот диапазон уже был расширен, то переза пуск не нужен.

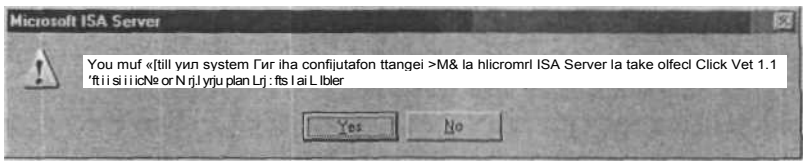


Рис. 6.11. Диалоговое окно с предупреждением о необходимости перезапуска системы

19 После перезапуска компьютера выполните вход в систему с учетной записью администратора.

20. Нажмите **кнопку Start** (Пуск) и переместите указатель на **All Programs** (Все программы). Переместите указатель на **Microsoft ISA Server** и щелкните мышью **ISA Server Management** (Управление ISA Server). Откроется консоль **Microsoft Internet Security and Acceleration Server 2004, и** появится страница **Welcome to Microsoft Internet Security and Acceleration Server 2004.**

СОВЕТ Можно установить консоль управления ISA на любом компьютере на базе Windows XP или Windows Server 2003. Системную политику необходимо настроить так, чтобы компьютер, на котором устанавливается MMC-оснастка удаленного управления, был добавлен к подмножеству компьютеров Remote Management Computers (Компьютеры удаленного управления).

На компьютере брандмауэра ISA создаются три журнала установки:

- ISAWRAP_'.log предоставляет информацию об успешной или неуспешной установке и установке журнала в формате MSDE;
- ISAMSDE_'.log содержит подробную информацию об установке MSDE, если была выбрана функция Advanced Logging;
- ISAFWSV_*.log содержит подробную информацию обо всем процессе установки брандмауэра ISA.

Если некоторые компоненты, например общие ресурсы для клиентов брандмауэра или функцию **Advanced Logging** (Создание журналов MSDE), устанавливать не нужно, то можно использовать апплет **Add/Remove Programs** (Установка/Удаление программ) панели управления, чтобы перезапустить программу установки и установить эти дополнительные компоненты потом.

ПРЕДУПРЕЖДЕНИЕ Если в процессе установки на компьютере работает служба IAS, то после завершения установки нужно перезапустить службу IAS. Кроме того, установка на одном компьютере IAS и брандмауэра ISA не поддерживается ОС Windows 2000.

Стандартная конфигурация брандмауэра ISA после установки

Программа установки брандмауэра ISA включает в себя настройки, которые пользователь вводит в процессе работы мастера установки. Программа установки также задает несколько стандартных настроек для полномочий пользователя (User Permissions), настроек сети (Network Settings), политики брандмауэра (Firewall Policy) и др. В табл. 6.5 представлены настройки, которые не задаются явно в процессе установки. Вкратце стандартную конфигурацию брандмауэра можно представить так:

- системные политики разрешают выборочный трафик с/на брандмауэр IS_A;
- запрещен весь трафик через брандмауэр ISA, потому что есть только одно за прещающее правило;
- между сетями VPN/VPN-Q и внутренней сетью установлены отношения типа «маршрут»;
- между внутренней сетью и внешней сетью по умолчанию задано отношение трансляции адресов NAT;
- только администраторы могут менять политику брандмауэра ISA.

Табл. 6.5. Настройки брандмауэра ISA после его установки

Функция	Настройка после установки брандмауэра
Полномочия пользователя	Члены группы администраторов на локальном компьютере могут настраивать политику брандмауэра. Если брандмауэр ISA является членом домена, то администраторы домена автоматически добавляются к группе локальных администраторов
Настройки сети	Мастер установки создает следующие правила для сети (Network Rules): *Правило доступа к локальному хосту* определяет отношение маршрутизации между сетью локального хоста и другими сетями. Дгся разрешенных соединений с брандмауэра ISA к другим хостам задано отношение типа «маршрут» (не NAT, которое не используется между локальным хостом и другими сетями). *Правило доступа в Интернет* задает отношение NAT из внутренней сети, сети изолированных VPN-клиентов и сети VPN-клиентов во внешнюю сеть. Отношение NAT распространяется на все соединения из этих трех типов сетей к внешней сети. Доступ разрешен, только если правильно настроена соответствующая политика доступа. Правило отношения из сети VPN-клиентов во внутреннюю сеть определяет отношение типа «маршрут» между сетью VPN-клиентов и внутренней сетью. Доступ разрешен, только если разрешен доступ для VPN-клиентов
Политика брандмауэра	Стандартное правило доступа (под названием «запрещающее правило» (Default Rule)) запрещает трафик между всеми сетями
Системная политика	По умолчанию брандмауэр ISA полностью защищен. Некоторые правила системной политики включаются для того, чтобы разрешить необходимые службы. Нужно просмотреть конфигурацию системной политики и настроить ее так, чтобы были включены только наиболее важные для данной реализации функции
Создание Web-цепочек	Стандартное правило (Default Rule) определяет, что все запросы клиентов Web-прокси обрабатываются непосредственно из Интернета. То есть по умолчанию создание Web-цепочек не задано. Правила создания Web-цепочек назывались правилами Web-маршрутизации в ISA Server 2000
Кэширование	Размер кэша установлен равным 0. Таким образом, кэширование отключено. Для включения кэширования нужно определить диск, на котором будет расположен кэш
Оповещения	Большинство оповещений включены. Нужно просмотреть и настроить оповещения в соответствии с потребностями конкретной сети

Табл. 6.5. (окончание)

Функция	Настройка после установки брандмауэра
Конфигурация клиента	По умолчанию для клиентов брандмауэра и Web-прокси включено автоматическое обнаружение. Web-браузеры на клиентах брандмауэра настраиваются при установке клиента брандмауэра
Автообнаружение для клиентов брандмауэра Web-прокси	По умолчанию публикация информации об автоматическом обнаружении отключена. Нужно включить публикацию информации об автоматическом обнаружении и подтвердить порт, на котором эта информация публикуется

Настройка системной политики после установки брандмауэра ISA

Политика брандмауэра ISA — набор правил, контролирующих доступ в/из сети локального хоста. Системная политика контролирует доступ в/из системы, она не настраивается для сетевого доступа между другими хостами. Одна из наиболее распространенных ошибок, совершаемых неопытными администраторами брандмауэра ISA, — использование системной политики для контроля доступа с хостов защищенной сети к хостам незащищенной сети.

В табл. *6.6* представлен список правил системной политики и их статуса после установки программного обеспечения брандмауэра ISA. Столбец Номер/Комментарии включает рекомендации по настройке конкретного правила системной политики.

Табл. 6.6. Стандартная системная политика после установки брандмауэра ISA

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
1. Является ли брандмауэр ISA членом домена? Если нет, отключить это правило	Разрешить доступ к службам каталогов с целью проверки подлинности	Разрешить	LDAP, ШАР (UDP), ШАР GC (Global Catalog), LDAPS, LDAPS GC (Global Catalog)	Локальный хост	Внутренняя сеть	Все пользователи
2, Если удаленная MMC-оснастка для управления брандмауэром ISA не используется, отключить это правило	Разрешить удаленный доступ с выбранных компьютеров с помощью MMC-оснастки	Разрешить	Microsoft FirewallControl, программа NetBIOS, служба имен NetBIOS, сеанс NetBIOS, EPC (все интерфейсы)	Компьютеры удаленного управления	Локальный хост	Все пользователи

(см. след. стр.)

Табл. 6.6. (продолжение)

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
3. Подтверждает, что подмножество компьютеров удаленного управления имеет адреса хостов, которые будут управлять брандмауэром ISA. Чтобы не разрешать управление брандмауэром ISA по протоколу RDP, отключите это правило	Разрешает удаленное управление с выбранных компьютеров с помощью сервера терминалов	Разрешить	RDP (службы терминалов)	Компьютеры удаленного управления	Локальный хост	Все пользователи
4. (По умолчанию отключено). Включите это правило, если нужно захо дить на SQL-серверы	Разрешает удаленный вход на доверяемые серверы с помощью NetBIOS	Разрешить	Дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Локальный хост	Внутренняя сеть	Все пользователи
5. Если не будет использоваться проверка подлинности с помощью RADIUS, то это правило следует отключить	Разрешить проверку подлинности RADIUS с ISA Server на доверяемые серверы RADIUS	Разрешить	RADIUS RADIUS Accounting	Локальный хост	Внутренняя сеть	Все пользователи
6. Если на брандмауэре ISA не будет производиться проверка подлинности, то отключите это правило	Разрешить проверку подлинности Kerberos с ISA Server к доверяемым серверам	Разрешить	Kerberos-Sec (TCP), Kerberos-Sec (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
7. Это правило необходимо включить, чтобы брандмауэр ISA мог инициировать DNS-запросы	Разрешить DNS-запросы с ISA Server к выбранным серверам	Разрешить	DNS	Локальный хост	Везде	
8. Если брандмауэр ISA не будет выступать в роли DHCP-клиента, отключите это правило	Разрешить DHCP-запросы с ISA Server ко всем сетям	Разрешить (запрос)	DHCP	Локальный хост	Везде	Все пользователи

Табл. 6.6. (продолжение)

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
9. Если брандмауэр ISA не будет выступать в роли DHCP-ото DHCP-клиента, отключите это правило	Разрешить DHCP-ответы от DHCP-сервера к ISA Server	Разрешить	DHCP (ответ)	Внутренняя сеть	Локальный хост	Все пользователи
10. Подтверждает, что для подмножества компьютеров удаленного управления правильно настроены IP-адреса	Разрешает ICMP (PING) запросы от выбранных компьютеров к ISA Server	Разрешить	Ping	Компьютеры удаленного управления	Локальный хост	**Все** пользователи
11. Это правило необходимо включить для того, чтобы брандмауэр ISA мог выполнять задачи по управлению сетью с помощью ICMP	Разрешить ICMP-запросы с ISA Server к выбранным серверам	Разрешить	Запрос информации ICMP, временная метка ICMP, Ping	Локальный хост	Все сети (и сеть локального хоста)	**Все** пользователи
12. (Отключено по умолчанию). Это правило автоматически включается при включении компонента VPN-сервера брандмауэра ISA	Весь трафик VPN-клиента на ISA Server	Разрешить	PPTP	Внешняя сеть	Локальный хост	Все пользователи
13- (Отключено по умолчанию). Это правило автоматически включается при включении VPN-подключений «узел-в-узел» с этим брандмауэром ISA	Разрешить VPN-подключения «узел-в-узел» с ISA Server	Разрешить	Нет	Внешние удаленные шлюзы **IPSec**	Локальный хост	Все пользователи
14. (Отключено по умолчанию). Это правило автоматически включается при включении VPN-подключений «узел-в-узел>> с этим брандмауэром ISA	Разрешить VPN-подключения «узел-в-узел» с ISA Server	Разрешить	Нет	Локальный хост	Внешние удаленные шлюзы IPSec	Все пользователи

(см. след. стр.)

Табл. 6.6. (продолжение)

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
15. Если не нужен доступ с брандмауэра ISA к папкам общего доступа, то это правило следует отключить	Разрешить соединения по протоколу CIFS с ISA Server к доверяемым серверам	Разрешить	Microsoft CIFS (TCP), Microsoft CIFS (UDP)	Локальный хост	Внутренняя сеть	Вес пользователи
16. (Отключено по умолчанию). Включите это правило, если нужно входить в систему с помощью SQL	Разрешить удаленный вход в систему с помощью SQL с ISA Server на выбранные серверы	Разрешить	Microsoft SQL (TCP) Microsoft SQL (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
17. Включите это правило, если нужно разрешать брандмауэру ISA самостоятельно устанавливать соединение с сайтом Windows Update. Некоторые предпочитают скачивать обновления, просматривать их, а затем копировать их на брандмауэр ISA и устанавливать	Разрешить HTTP/HTTPS запросы с ISA Server на указанные сайты	Разрешить	HTTP, HTTPS	Локальный хост	Сайты, разрешенные системной политикой	Все пользователи
18. (По умолчанию отключено). Это правило включается при создании верификатора связи по протоколам HTTP/HTTPS	Разрешить запросы по протоколам HTTP/HTTPS с ISA Server к выбранным серверам для верификаторов связей	Разрешить	HTTP, HTTPS	Локальный хост	Все сети (и локальная сеть пользователи локального хоста)	Вес
19. (По умолчанию отключено). Это правило включается, если на брандмауэре ISA устанавливается общий ресурс клиента	Разрешить доступ с надежных компьютеров к общему ресурсу с установочными файлами клиента брандмауэра на ISA Server	Разрешить	Microsoft CIFS (TCP), Microsoft CIFS (UDP), дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Внутренняя сеть	Локальный хост	Все пользователи

Табл. 6.6. (продолжение)

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
20. (Отключено по умолчанию). Включите это правило, если нужно выполнять удаленный мониторинг производительности брандмауэра ISA	Разрешить удаленный мониторинг производительности ISA Server с доверяемых серверов	Разрешить	Дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Компьютеры удаленного управления	Локальный хост	Все пользователи
21. Включите это правило, если нужно обеспечить доступ к общим папкам с брандмауэра ISA	Разрешить NetBIOS с ISA Server к доверяемым серверам	Разрешить	Дейтаграмма NetBIOS, служба имен NetBIOS, сеансы NetBIOS	Локальный хост	Внутренняя сеть	Все пользователи
22. Включите это правило, если нужно использовать протокол RPC для соединения с другими серверами	Разрешить RPC-соединения с ISA Server к доверяемым серверам	Разрешить	RPC (все интерфейсы)	Локальный хост	Внутренняя сеть	Все пользователи
23. Это правило разрешает брандмауэру ISA отправлять сообщения об ошибках в корпорацию Microsoft	Разрешить сообщения об ошибках по протоколам HTTP/HTTPS с ISA Server к указанным сайтам Microsoft	Разрешить	HTTP, HTTPS	Локальный хост	Сайты Microsoft по обработке сообщений об ошибках	Все пользователи
24. (Отключено по умолчанию). Это правило следует включить, если включена проверка подлинности SecurlD	Разрешить проверку подлинности SecurlD с ISA Server к доверяемым серверам	Разрешить	SecurlD	Локальный хост	Внутренняя сеть	Все пользователи
25. (Отключено по умолчанию). Включите это правило, если нужно использовать MOM (Microsoft Operations Manager, менеджер операций Microsoft) для мониторинга брандмауэра ISA	Разрешить удаленный мониторинг с ISA Server на доверяемые серверы с помощью агента MOM	Разрешить	Microsoft Operations Manager Agent	Локальный хост	Внутренняя сеть	Все пользователи

(см. след. стр.)

Табл. 6.6. (окончание)

Номер/ комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
26. (Отключено по умолчанию). Включите это правило, если нужно обеспечить доступ брандмауэра ISA к CRL	Разрешить весь HTTP-трафик с ISA Server ко всем сетям (для загрузок CRL) (он необходим, если брандмауэр ISA завершает любые SSL-соединения)	Разрешить	HTTP	Локальный хост	Все сети (и локальный хост)	Все пользователи
27. Это правило следует изменить, разрешив контакт с доверяемым NTP-сервером организации	Разрешить NTP-соединения с ISA Server к доверяемым NTP-серверам	Разрешить	NTP (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
28. Это правило еледует отключить, если не нужно **вешшг** зовать протокол SMTP для отправки оповещений. В противном случае нужно заменить внутренний адресат (Internal Destination) конкретным компьютером, который будет принимать SMTP-сообщения с брандмауэра ISA	Разрешить SMTP-соединения с ISA Server к доверяемым серверам	Разрешить	SMTP	Локальный хост	Внутренняя сеть	Все пользователи
29. (Отключено по умолчанию). Это правило автоматически включается при включении загрузку содержимого	Разрешить HTTP-соединения с ISA Server к вычислительным компьютерам с целью выполнения заданий на загрузку	Разрешить	HTTP	Локальный хост	Все сети (и локальный хост)	Системная и сетевая служба
30. Это правило нужно включить, если планируется использовать удаленную MMC-оснастку	Разрешить брандмауэру контролировать соединения с выбранными компьютерами	Разрешить	Весь исходящий трафик	Локальный хост	Компьютеры удаленного доступа	Все пользователи

Правила системной политики брандмауэра ISA оцениваются прежде всех задаваемых пользователями правил доступа в том порядке, как они перечислены в табл. 6.6. Системную политику брандмауэра ISA можно просмотреть, щелкнув мышью **Firewall Policy** (Политика брандмауэра) в левой панели консоли, а затем щелкнув вкладку **Tasks** (Задачи). На вкладке Tasks (Задачи) щелкните мышью **Show System Policy Rules** (Показать правила системной политики). Щелкните мышью **Hide System Policy Rules** (Скрыть правила системной политики), когда закончите просматривать системную политику брандмауэра.

ПРЕДУПРЕЖДЕНИЕ Можно внести изменения лишь в некоторые компоненты стандартной системной политики брандмауэра ISA. Есть несколько случаев, когда невозможно внести изменения в системную политику брандмауэра ISA с помощью редактора системной политики System Policy Editor.

Изменить системную политику брандмауэра ISA можно, **щелкнув** мышью пункт **Edit System Policy** (Редактировать системную политику) на вкладке **Tasks** (Задачи). Откроется окно редактора системной политики **System Policy Editor** (Редактор системной политики) (рис. 6.12). Для каждого правила системной политики имеются вкладки **General** (Общие) *и* **From** (От) или **To** (К). Вкладка **General** (Общие) для каждой **Configuration Group** (Группы конфигурирования) содержит объяснение правил(а), а вкладки From (От) и To (К) позволяют контролировать доступ от/к компьютеру брандмауэра ISA.

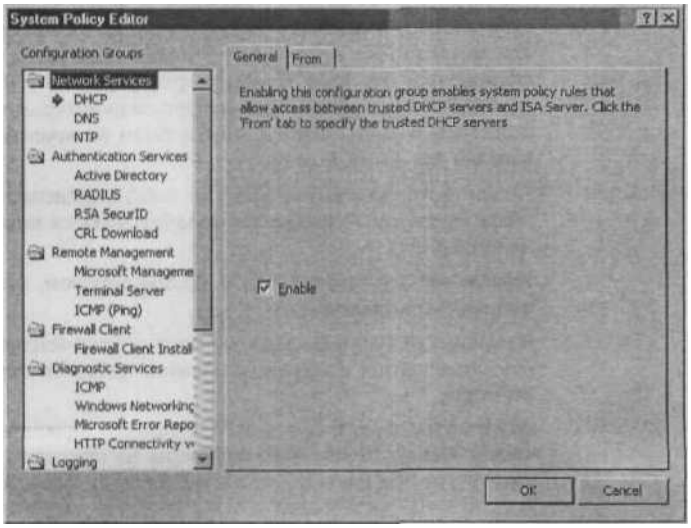


Рис. 6.12. Диалоговое окно **System** Policy **Editor** (Редактор системной политики)

Табл. 6.7. Стандартная конфигурация системы брандмауэра ISA после его установки

Функция	Стандартное значение
Полномочия пользователей	Члены группы администраторов на локальном компьютере могут конфигурировать политику брандмауэра. Если брандмауэр ISA является членом домена, то глобальная группа администраторов домена автоматически включается в локальную группу администраторов
Определение внутренней сети	Внутренняя сеть содержит IP-адреса, указанные в процессе установки программного обеспечения брандмауэра ISA
Сетевые правила	Правило доступа к локальному хосту определяет отношения типа «маршрут» (а не NAT) между сетью локального хоста и всеми остальными сетями. Правило доступа к Интернету определяет отношения NAT между внутренней сетью, сетью изолированных VPN-клиентов и сетью VPN-клиентов с одной стороны и внешней сетью с другой. Соединение этих трех типов сетей с Интернетом осуществляется с помощью NAT. Доступ разрешается, только если настроены соответствующие правила доступа. Правило отношений между сетью VPN-клиентов и внутренней сетью определяет отношение типа «маршрут» между этими сетями. Доступ разрешается, только **если** разрешен доступ для VPN-клиентов
Политика брандмауэра	Правило по умолчанию (Default Rule) запрещает трафик между всеми сетями
Системная политика	По умолчанию ISA Server является хорошо **защищенным,** при этом он разрешает работу нескольких важных служб После установки некоторые правила системной политики включаются для того, чтобы разрешить работу необходимых служб. Рекомендуется просмотреть конфигурацию системной политики и настроить ее, чтобы были включены службы, важные для данной сети
Создание Web-цепочек	Правило по умолчанию (Default Rule) определяет, что все запросы клиентов Web-прокси обрабатываются непосредственно из Интернета
Кэширование	Размер кэша установлен на 0. Таким образом, кэширование полностью отключено
Оповещения	Большинство оповещений включено. Рекомендуется настроить оповещения в соответствиями с потребностями конкретной сети
Конфигурация клиента	Для клиента брандмауэра и Web-прокси включено автоматическое обнаружение. Web-браузеры на клиентах брандмауэра конфигурируются при установке клиента брандмауэра

Установка обновления брандмауэра ISA

На компьютере с установленным ISA Server 2000 можно обновить программное обеспечение брандмауэра следующим образом:

- выполнить обновление только на этом компьютере;
- перенести текущие настройки ISA Server 2000 на установленный «с нуля» ISA Server 2004.

Перенос настроек и обновление ISA Server 2000 — это сложная тема; прежде чем переносить настройки или обновлять брандмауэр, нужно учесть несколько моментов. При перенесении настроек и обновлении возникает несколько осложнений, потому ЧТО:

- сетевая модель ISA Server 2004 полностью отличается от сетевой модели ISA Server 2000;
- в новом брандмауэре ISA не поддерживаются правила для распределения пропускной СПОСОбнОСТИ;
- в новом брандмауэре ISA не поддерживается активное кэширование;
- настройки полномочий не переходят в новый брандмауэр ISA;
- настройки создания журналов и отчетов не наследуются;
- конфигурация фильтрации пакетов не наследуется, потому что в новом брандмауэре ISA нет и не требуется конфигурация фильтрации пакетов;
- фильтры приложения и Web-фильтры для ISA Server 2000 не совместимы с новым брандмауэром ISA;
- в ISA Server 2000 и ISA Server 2004 полностью отличаются функции и интеграция маршрутизации и удаленного доступа.

Эти и другие моменты могут усложнить процесс обновления. В сложных случаях рекомендуется обращаться к справочной системе ISA Server 2004, чтобы получить информацию об установке обновления. В справочной системе содержится информация о различиях брандмауэров ISA Server 2004 и ISA Server 2000.

Однако, следуя рекомендациям этой книги, лучше создать копию конфигурации ISA Server 2000, а затем воспроизвести политики после того, как станет ясен принцип работы нового брандмауэра ISA и то, как он совместим с политикой брандмауэра ISA Server 2000.

> ПРЕДУПРЕЖДЕНИЕ Брандмауэр ISA Server 2000 Standard Edition можно обновить только до ISA Server 2004 Standard Edition. Для ISA Server 2000 Enterprise Edition не предусмотрено встроенных инструментов обновления и перенесения настроек, чтобы переместить текущие политики брандмауэра в ISA Server 2004 Standard Edition. В ISA Server 2004 Enterprise Edition имеется инструмент, позволяющий обновлять или переносить настройки ISA Server 2000 Enterprise Edition в ISA Server 2004 Enterprise Edition.

Установка брандмауэра ISA на компьютере с одним сетевым адаптером (брандмауэр ISA с одним сетевым интерфейсом)

Программное обеспечение брандмауэра ISA можно установить на компьютере с одной сетевой интерфейсной картой. Такая конфигурация имитирует конфшурацию Proxy Server 2.0 или брандмауэр ISA Server 2000 в режиме только кэширования. Брандмауэр ISA Server 2004 не может работать в режиме только кэширования, но при установке этого брандмауэра на компьютере с одним сетевым адаптером можно лишить брандмауэр существенной части его функций.

Если брандмауэр ISA устанавливается в режиме с одним сетевым адаптером, теряются следующие его функции:

- поддержка клиентов брандмауэра;
- поддержка полной защиты и функциональности клиента SecureNAT;
- правила публикации серверов;
- поддержка всех протоколов, за исключением HTTP, HTTPS и FTP, по HTTP-тунелю (Web-прокси);
- VPN-подключения удаленного доступа;
- VPN-подключения «узел-в-узел»;
- функции поддержки работы с несколькими сетями (все адресное пространство IPv4 в одной сети);
- проверка на уровне приложения для всех протоколов, кроме HTTP.

Хотя такая сокращенная версия брандмауэра ISA сохраняет лишь часть сзоей способности выступать в роли сетевого брандмауэра для защиты хостов в корпоративной сети, она тем не менее способна обеспечить собственную защиту, как и полнофункциональный брандмауэр. Брандмауэр ISA будет напрямую доступен для внешних и внутренних хостов только в том случае, если будут включены правила системной политики, разрешающие этот доступ.

Для конфигурации сетевой интерфейсной карты на брандмауэре ISA с одним сетевым интерфейсом в качестве адреса основного шлюза должен быть указан IP-адрес любого шлюза в сети, позволяющий брандмауэру ISA с одним сетевым интерфейсом получить доступ к Интернету. Все прочие нелокальные маршруты должны быть настроены в таблице маршрутизации брандмауэра ISA с одним сетевым интерфейсом.

Если нужно только, чтобы служба Web-прокси работала в прямом и обратном режиме, то следует установить программное обеспечение брандмауэр ISA на компьютере с одной сетевой интерфейсной картой. Процесс установки немного отличается от установки брандмауэра ISA на компьютере с несколькими сетевыми интерфейсными картами:

1. Вставьте установочный компакт-диск ISA Server 2004 в привод для компакт-дисков или установите соединение с общим ресурсом, содержащим установочные файлы ISA Server 2004. Если программа установки не запустится автоматически, дваж ды щелкните мышью файл isaautorun.exe в корне дерева папок с установочны ми файлами.
2. На странице **Microsoft Internet Security and Acceleration Server 2004** щел кните мышью **Review Release Notes** (Информация о версии) и прочтите ин формацию о версии. Эта информация о версии содержит очень важные данные об изменениях в основной функциональности программного обеспечения бранд мауэра. Эта информация не обязательно входит в файл справки, поэтому насто ятельно рекомендуется прочитать ее на этом этапе. После просмотра инфор мации о версии щелкните мышью **Read Setup and Feature Guide** (Прочитать руководство по установке и функциям). Руководство можно прочитать сразу, про смотреть основные темы или распечатать. Щелкните мышью **Install ISA Server 2004** (Установить ISA Server 2004).
3. Нажмите кнопку **Next** (Далее) на странице **Welcome to the Installation Wizard for Microsoft ISA Server 2004** (Мастер установки Microsoft ISA Server 2004).
4. Выберите вариант **I accept the terms in the license agreement** (Я принимаю условия лицензионного соглашения) на странице **License Agreement** (Лицен зионное соглашение). Нажмите кнопку **Next** (Далее).
5. На странице **Customer Information** (Информация о пользователе) введите ваше имя и название организации в текстовые поля **User Name** (Имя) и **Organization** (Организация). Введите серийный номер в текстовое поле **Product Serial Num ber** (Серийный номер продукта). Если была установлена оценочная версия про граммного обеспечения, а сейчас устанавливается лицензионная версия, то соз дайте резервную копию конфигурации с помощью встроенного в брандмауэр ISA инструмента создания резервных копий и удалите оценочную версию. Пе резапустите установку лицензионной версии программного обеспечения бранд мауэра ISA. Нажмите кнопку **Next** (Далее).
6. На странице **Setup Type** (Тип установки) щелкните мышью вариант **Custom** (Пользовательская).
7. На странице **Custom Setup** (Пользовательская установка) варианты **Firewall Services, Advanced Logging** и **ISA Server Management** выбраны по умолчанию. Хотя можно установить общий ресурс клиента брандмауэра, следует учесть, что брандмауэр ISA с одним сетевым интерфейсом не поддерживает клиентов бранд мауэра и SecureNAT. Единственный поддерживаемый тип клиента — это клиент Web-прокси. Однако если в сети имеются полнофункци ональные брандмауэры ISA, то можно установить общий ресурс клиента брандмауэра на этом компью тере и разрешить клиентам сети скачивать программное обеспечение клиента брандмауэра с брандмауэра ISA с одним сетевым интерфейсом. Нет смысла ус танавливать средство просмотра SMTP-сообщений на брандмауэре ISA с одним

сетевым интерфейсом, потому что такой режим не поддерживает правила публикации серверов. Нажмите кнопку **Next** (Далее).

8. На странице **Internal Network** (Внутренняя сеть) нажмите кнопку **Add** (Добавить). На странице **Address Ranges for Internal Network** (Диапазоны адресов для внутренней сети) щелкните мышью **Select Network Adapter** (Выбрать сетевой адаптер) (рис. 6.1 3).
9- На странице **Select Network Adapter** (Выбрать сетевой адаптер) выбраны варианты **Add the following private ranges** (Добавить следующие частные диапазоны) и **Add address ranges based on the Windows Routing Table** (Добавить диапазоны адресов на основании таблицы маршрутизации Windows) Рекомендуется снять флажок в поле **Add the following private ranges** (Добавить следующие частные диапазоны) и установить флажок в поле рядом с одной сетевой интерфейсной картой, установленной на брандмауэре ISA с одним сетевым интерфейсом. Нажмите кнопку ОК.
10. Нажмите кнопку ОК в диалоговом окне **Setup** Message (Информация об уста новке), сообщающем, что внутренняя сеть была определена на основании таб лицы маршрутизации. Это диалоговое окно в действительности не относится к брандмауэру ISA с одним сетевым интерфейсом, потому что все IP-адреса в ад ресном диапазоне IPv4 (за исключением идентификаторов сети локального хоста) включаются в определение внутренней сети. Идентификатор сети локаль ного хоста не включается в определение внутренней сети, потому что этот ад рес включается в определение сети локального хоста.
11. В диалоговом окне адресного диапазона внутренней сети (рис. 6.13) показаны все IP-адреса, входящие в определение внутренней сети. Нажмите кнопку ОК.

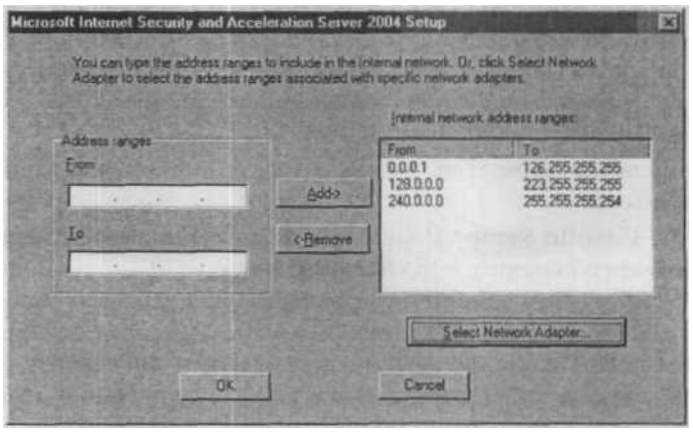


Рис. 6.13. Определение внутренней сети на брандмауэре ISA с одним сетевым интерфейсом

12. Нажмите кнопку **Next** (Далее) на странице **Internal Network** (Внутренняя сеть).

13. Нажмите кнопку **Next** (Далее) на странице **Firewall Client Connection Settings** (Настройки соединения клиента брандмауэра). Эти настройки ничего не значат, потому что брандмауэр ISA с одним сетевым интерфейсом не поддерживает клиенты брандмауэра.
14. Нажмите кнопку **Next** (Далее) на странице **Services** (Службы).
15. Нажмите кнопку **Install** (Установить) на странице **Ready to Install the Program** (Установка программы).
16. Установите флажок в поле **Invoke ISA Server Management when the wizard closes** (Активировать ISA Server Management по окончании работы мастера ус тановки) и нажмите кнопку **Finish** (Готово).

Брандмауэр ISA с одной сетевой интерфейсной картой имеет ряд важных ограничений, потому что он не определяет внешнюю сеть, не поддерживает клиент брандмауэра и т, д. Некоторые особенности применения брандмауэра ISA с одним сетевым интерфейсом и политики доступа для этой конфигурации обсуждаются в главе 7.

Конфигурирование брандмауэра ISA для быстрого старта

Многие администраторы хотели бы установить и настроить брандмауэр ISA как можно быстрее, а позже углубиться в детали конфигурирования брандмауэра ISA. Они хотят установить брандмауэр ISA в сети, создать соединение с Интернетом, установить программное обеспечение и создать правило, которое разрешает всем хостам частной сети быстрый доступ ко всем протоколам в Интернете. После того как брандмауэр ISA работает, а соединение с Интернетом установлено, в свободное время они могут изучить остальную часть этой книги и узнать об интересных и мощных возможностях конфигурирования брандмауэра ISA.

Поэтому в эту книгу был добавлен раздел, посвященный быстрой установке и конфигурированию. В этом руководстве по быстрой установке и конфигурированию брандмауэра используется сеть, к которой предъявляются следующие требования:

- в этой сети нет других серверов Windows. Это руководство включает в себя инструкции по установке служб DNS и DHCP на брандмауэре ISA. Если в сети уже имеется DNS- или DHCP-сервер, на брандмауэре ISA их устанавливать не нужно;
- установка брандмауэра ISA Server 2004 производится на базе ОС Windows Server 2003;
- на компьютере установлена ОС Windows Server 2003 со стандартными настрой ками и нет другого программного обеспечения;
- на компьютере на базе Windows Server 2003 установлено два сетевых адаптера. Одна сетевая интерфейсная карта соединена с внутренней сетью, а другая на-

прямую соединяется с Интернетом через сетевой маршрутизатор или же п>;ред ней есть DSL или кабельный NAT-омаршрутизатор»;

- компьютеры во внутренней сети настроены как DHCP-клиенты и будут исполь зовать компьютер брандмауэра ISA Server 2004 в качестве своего DHCP-сервера;
- компьютер на базе ОС Windows Server 2003, на котором устанавливается про граммное обеспечение брандмауэра ISA Server 2004, не является членом доме на Windows. Хотя позже рекомендуется сделать брандмауэр ISA членом домена, компьютер, на котором установлено программное обеспечение брандмауэра ISA, не обязательно должен быть членом домена. Это требование необходимо в дан ном руководстве, потому что предполагается, что в данной сети нет других сер веров на базе Windows (но в ней могут быть серверы на базе Linux, Netware и других производителей).

На рис. 6.14 показан брандмауэр ISA и его отношения с внутренней и внешней сетью. Внутренний интерфейс подключен к концентратору или коммутатору внутренней сети, а внешний интерфейс подключен к концентратору или коммутатору, который также подключен к маршрутизатору.

Внешний интерфейс брандмауэра ISA и интерфейс маршрутизатора, связанный с ЛВС, находятся на одном идентификаторе сети. В зависимости от типа сети это можн бить общий или частный идентификатор сети

Рис. 6.14. Физические связи между брандмауэром ISA Server 2004, внутренней и внешней сетью

Для быстрой установки и конфигурирования брандмауэра ISA нужно выполнить следующие действия:

- настроить сетевые интерфейсы брандмауэра ISA;
- установить и настроить DNS-сервер на компьютере брандмауэра ISA Server 2004;
- *ш* установить и настроить DHCP-сервер на компьютере брандмауэра ISA Server 2004;
- установить и настроить программное обеспечение ISA Server 2004;

Все клиенты внутренней иги настроены *как* клиенты SecureNAT

- настроить компьютеры внутренней сети как DHCP-клиенты.

Конфигурирование сетевых интерфейсов брандмауэра ISA

У брандмауэра ISA должен быть хотя бы один внутренний сетевой интерфейс и один внешний сетевой интерфейс. Чтобы правильно настроить сетевые интерфейсы на брандмауэре ISA, нужно сделать следующее:

- назначить IP-адреса внутреннему и внешнему сетевым интерфейсам;
- назначить адрес DNS-сервера внутреннему интерфейсу брандмауэра ISA;
- поместить внутренний интерфейс в верх списка сетевых интерфейсов.

Назначение IP-адресов и DNS-сервера

Прежде всего нужно назначить статические IP-адреса внутреннему и внешнему интерфейсу брандмауэра ISA. Для брандмауэра ISA также требуется адрес DNS-сервера, связанного с его внутренним интерфейсом. Для всех сетевых интерфейсов брандмауэра ISA не используется DHCP-сервер, потому что у внутреннего интерфейса должен всегда быть статический IP-адрес, а внешний интерфейс не поддерживает динамические адреса, поскольку он находится за маршрутизатором.

Если в учетной записи Интернета используется DHCP для присвоения общего адреса, то DSL или кабельный маршрутизатор могут получать и обновлять общий адрес. Кроме того, еош для соединения с интернет-провайдером используется PPPoE (Point-to-Point Protocol over Ethernet, протокол «точка-точка» через Ethernet) или VPN, то маршрутизатор также может выполнять эти задачи.

В этом разделе рассматриваются следующие темы:

- конфигурирование **внутреннего** сетевого интерфейса;
- конфигурирование внешнего сетевого интерфейса.

Конфигурирование внутреннего сетевого интерфейса

Внутренний интерфейс должен иметь IP-адрес с того же идентификатора сети, что и другие компьютеры во внутренней сети. Этот адрес должен входить в адресный диапазон частной сети и не должен уже использоваться в сети.

Брандмауэр ISA будет настроен на использование адреса внутреннего интерфейса в качестве адреса DNS-сервера.

На брандмауэре ISA должен быть статический IP-адрес, связанный с его внутренним интерфейсом. На компьютере на базе ОС Windows Server 2003 нужно выполнить следующие действия:

1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и выберите в контекстном меню пункт **Properties** (Свойства).
2. В окне **Network Connections** (Сетевые подключения) правой кнопкой мыши щелкните внутренний сетевой интерфейс и выберите в контекстном меню пункт **Properties** (Свойства).

3. В диалоговом окне сетевого интерфейса **Properties** (Свойства) щелкните правой кнопкой мыши **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) и выберите в контекстном меню пункт **Properties** (Свойства).
4. В диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства: Протокол Интернета, TCP/IP) выберите **Use the following IP address** (Использовать следующий IP-адрес). Введите IP-адрес внутреннего интерфейса в текстовое поле **IP address** (IP-адрес). Введите маску подсети для внутреннего интерфейса в текстовом поле **Subnet mask** (Маска подсети). Не вводите основной шлюз для внутреннего интерфейса.
5. Выберите **Use the following DNS server addresses** (Использовать следующие адреса DNS-серверов). Введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовом поле **Preferred DNS server** (Предпочитаемый DNS-сервер). Это тот же адрес, который был введен в текстовое поле **IP-address** (IP-адрес) в п. 4. Нажмите кнопку OK в диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства: Протокол Интернета, TCP/IP).
6. Нажмите кнопку OK в диалоговом окне **Properties** (Свойства) внутреннего интерфейса.

ПРЕДУПРЕЖДЕНИЕ Если во внутренней сети уже есть DNS-сервер, то следует настроить внутренний интерфейс брандмауэра ISA на использование IP-адреса DNS-сервера внутренней сети. Затем следует настроить DNS-сервер во внутренней сети так, чтобы он разрешал имена хостов в Интернете. DNS-сервер Microsoft автоматически разрешает имена хостов s Интернете, пока файл корневых ссылок заполняется корневыми серверами DNS Интернета. Стандартное правило доступа, создание которого описано в конце этого раздела, разрешает DNS-серверу исходящий доступ к DNS-серверам Интернета с целью разрешения имен хостов.

ПРЕДУПРЕЖДЕНИЕ Никогда не указывайте адрес основного шлюза на внутреннем интерфейсе. У брандмауэра ISA может быть лишь один интерфейс с основным шлюзом. Даже если на одном брандмауэре ISA установлено 17 сетевых интерфейсных карт, только одна из них может быть настроена с адресом основного шлюза. Все другие шлюзы должны настраиваться в таблице маршрутизации Windows.

Конфигурирование внешнего сетевого интерфейса

Для того чтобы настроить информацию об IP-адресах на внешнем интерфейсе брандмауэра ISA, выполните следующие действия:

1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт **Properties** (Свойства).
2. В окне **Network Connections** (Сетевые подключения) правой кнопкой мыши щелкните внешний сетевой интерфейс и в контекстном меню выберите пункт **Properties** (Свойства).
3. В диалоговом окне сетевого интерфейса **Properties** (Свойства) щелкните мы шью **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) и выберите пункт меню **Properties** (Свойства).
4. В диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства: прото кол Интернета, TCP/IP) выберите **Use the following IP address** (Использовать следующий IP-адрес). Введите IP-адрес внешнего интерфейса в текстовое поле **IP address** (IP-адрес). Введите маску подсети для внешнего интерфейса в тек стовое поле **Subnet mask** (Маска подсети). Введите основной шлюз для внеш него интерфейса в текстовое поле **Default gateway** (Основной шлюз). Основ ной шлюз — это адрес маршрутизатора в сети.
5. Нажмите кнопку OK в диалоговом окне **Properties** (Свойства) внешнего интер фейса.

> СОВЕТ Не нужно настраивать адрес DNS-сервера на внешнем интерфейсе. Необходим лишь адрес DNS-сервера на внутреннем интерфейсе.

Порядок сетевых интерфейсов

Внутренний интерфейс компьютера с ISA Server 2004 помещается вверху списка сетевых интерфейсов, чтобы обеспечить лучшую производительность при разрешении имен. Выполните следующие действия, чтобы настроить сетевой интерфейс на компьютере на базе ОС Windows Server 2003:

1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт **Properties** (Свойства).
2. В окне **Network and Dial-up Connections** (Сетевые подключения) щелкните мышью меню **Advanced** (Дополнительно), а затем щелкните мышью **Advanced Settings...** (Дополнительные параметры...).
3. В диалоговом окне **Advanced Settings** (Дополнительные параметры) (рис. 6.15) щелкните мышью внутренний интерфейс в списке **Connections** (Подключения) на вкладке **Adapters and Bindings** (Адаптеры и привязки). После того как выб ран внутренний интерфейс, щелкните мышью стрелку вверх, чтобы перемес тить его в верх списка интерфейсов.

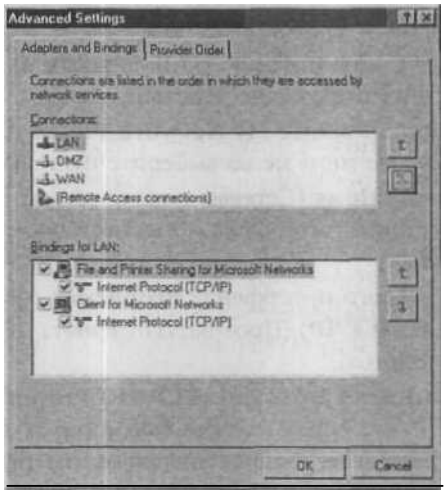


Рис. 6.15. Диалоговое окно Advanced Settings (Дополнительные параметры)

4. Нажмите кнопку OK в диалоговом окне **Advanced Settings** (Дополнительные параметры).

Установка и конфигурирование DNS-сервера на брандмауэре ISA

На брандмауэре ISA будет установлен DNS-сервер в режиме только кэширования. Это позволит компьютерам во внутренней сети и брандмауэру ISA разрешать имена хостов в Интернете. Отметим, что если во внутренней сети уже есть DNS-сервер, то устанавливать его еще раз не нужно. Если во внутренней сети есть DNS-сервер, то можно попробовать настроить компьютер брандмауэра ISA как DNS-сервер в режиме только кэширования, а затем настроить компьютеры во внутренней сети так, чтобы они использовали компьютер с ISA Server 2004 в качестве DNS-сервера или применяли DNS-сервер внутренней сети, а DNS-сервер внутренней сети настроить так, чтобы он использовал брандмауэр ISA в качестве сервера пересылок DNS.

Установка службы DNS

Служба DNS-сервера не устанавливается по умолчанию в операционных системах Windows для серверов. Сначала нужно установить службу DNS-сервера на компьютере на базе Windows Server 2003, который будет играть роль брандмауэра ISA.

Установка службы DNS-сервера на базе Windows Server 2003

Выполните следующие действия, чтобы установить службу DNS на компьютере с Windows Server 2003:

1. Нажмите кнопку **Start** (Пуск), установите курсор мыши на **Control Panel** (Панель управления) и щелкните мышью **Add or Remove Programs** (Установка и удаление программ).
2. В окне **Add or Remove Programs** (Установка и удаление программ) щелкните мышью **Add/Remove Windows Components** (Установка компонентов Windows).
3. В диалоговом окне **Windows Components Wizard** (Мастер компонентов Windows) выберите **Networking Services** (Сетевые службы) из списка **Components** (Компоненты Windows). Не устанавливайте флажок в поле! Выделив запись **Networking Services** (Сетевые службы), нажмите кнопку **Details** (Состав).
4. В диалоговом окне **Networking Services** (Сетевые службы) установите флажок в поле **Domain Name System (DNS) и** нажмите кнопку ОК.
5. Нажмите кнопку **Next** (Далее) в диалоговом окне **Windows Components** (Компоненты Windows).
6. Нажмите кнопку ОК в диалоговом окне **Insert Disk** (Вставка диска). В диалоговом окне **Files Needed** (Требуемые файлы) укажите путь к папке i386 на установочном компакт-диске Windows Server 2003 в текстовом поле **Copy files from** (Размещение файлов) и нажмите кнопку ОК.
7. Нажмите кнопку **Finish** (Готово) на странице **Completing the Windows Components Wizard** (Завершение работы мастера компонентов Windows).
8. Закройте окно **Add or Remove Programs** (Установка и удаление программ).

Конфигурирование службы DNS на брандмауэре ISA

DNS-сервер на компьютере с брандмауэром ISA выполняет DNS-запросы имен хостов в Интернете от имени компьютеров внутренней сети. DNS-сервер на брандмауэре ISA настроен в режиме только кэширования. DNS-сервер в режиме только кэширования не имеет информации об общих или частных DNS-именах и доменах. Он разрешает имена хостов в Интернете и кэширует результаты; он не отвечает на DNS-запросы имен в частной DNS-зоне **внутренней** сети или в общей DNS-зоне.

> ПРИМЕЧАНИЕ Изучение DNS — это сложная тема, и не стоит огорчаться, если не все принципы работы DNS понятны. После выполнения приведенных в этом разделе рекомендаций DNS-служба будет правильно настроена на разрешение имен хостов в Интернете.

Если во внутренней сети имеется DNS-сервер, поддерживающий домен Active Directory, то расположенный на брандмауэре ISA DNS-сервер можно настроить в режиме только кэширования так, чтобы направлять клиентские запросы к домену внутренней сети на DNS-сервер внутренней сети. В итоге DNS-сервер в режиме только кэширования на компьютере брандмауэра ISA Server 2004 не будет мешать текущей установке DNS-сервера.

Конфигурирование службы DNS в Windows Server 2003

Для того чтобы настроить службу DNS на компьютере с Windows Server 2003 выполните следующие действия:

1. Нажмите кнопку **Start** (Пуск) и установите курсор мыши на **Administrative** Tools (Администрирование). Щелкните мышью запись **DNS.**
2. Правой кнопкой мыши щелкните имя сервера в левой панели консоли, устано вите курсор мыши на **View** (Вид) и щелкните пункт **Advanced** (Расширенный).
3. Разверните все узлы в левой панели консоли **DNS.**
4. Правой кнопкой мыши щелкните имя сервера в левой панели консоли **DNS** и в контекстном меню выберите пункт **Properties** (Свойства).
5. В диалоговом окне **Properties** (Свойства) сервера щелкните мышью вкладку **Interfaces** (Интерфейсы). Выберите вариант **Only the following IP addresses** (Только по указанным IP-адресам). Щелкните мышью любой IP-адрес, не связан ный с внутренним интерфейсом компьютера. Выделив такой IP-адрес, нажмите кнопку **Remove** (Удалить). Нажмите кнопку **Apply** (Применить).
6. Щелкните мышью вкладку **Forwarders** (Пересылка) (рис. б.16). Введите IP-ад рес DNS-сервера интернет-провайдера в текстовое поле **Selected domain's forwarder IP address list** (Список IP-адресов серверов пересылки для выбран ного домена), а затем нажмите кнопку **Add** (Добавить). Установите флажок в поле **Do not use recursion for this domain** (Не использовать рекурсию для этого домена). Этот вариант запрещает попытки DNS-сервера на брандмауэре ISA вы полнять разрешение имен самостоятельно. В итоге, если сервер пересылки не может разрешить имя, запрос на разрешение имени отвергается. Нажмите кнопку **Apply** (Применить).

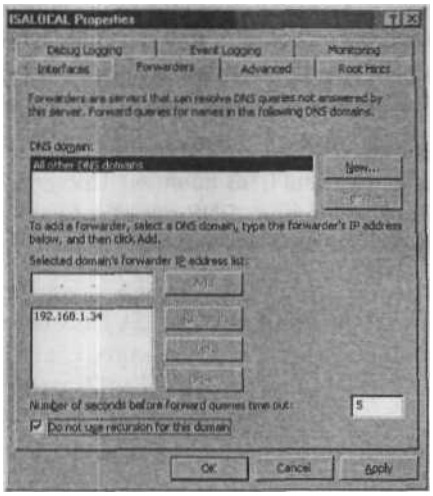


РИС. 6.16. Вкладка Forwarders (Пересылка)

СОВЕТ Если производительность разрешения имен оставляет желать лучшего, отключите запись Forwarders (Пересылка). Хорошо настроенный DNS-сервер интернет-провайдера может существенно улучшить производительность разрешения имен, а плохо настроенный DNS-сервер интернет-провайдера может снизить способность локального брандмауэра ISA по разрешению имен хостов в Интернете. Чаще всего лучшей производительности можно добиться, используя DNS-сервер интернет-провайдера, потому что его кэш с разрешенными именами хостов больше, чем кэш на DNS-сервере в режиме только кэширования на локальном брандмауэре ISA.

7. Нажмите кнопку OK в диалоговом окне **Properties** (Свойства).
8. Правой кнопкой мыши щелкните имя сервера, установите курсор на **All Tasks** (Все задачи) и нажмите кнопку **Restart** (Перезапустить).
   Эти действия нужно выполнять, только если во внутренней сети нет DNS-сервера, который используется для поддержки домена Active Directory. Если во внутренней сети нет DNS-сервера и нет необходимости в разрешении DNS-имен внутренней сети, то пропустите следующий раздел, посвященный конфигурированию зоны-заглушки.

   ПРЕДУПРЕЖДЕНИЕ Если во внутренней сети уже есть DNS-сервер, то не нужно выполнять указанные далее действия. Их нужно выполнять только в тех сетях, где уже есть домены Active Directory в среде Windows 2000 Server или Windows Server 2003.
9. Сначала нужно создать зону обратного просмотра для внутренней сети, в которой расположен идентификатор внутреннего DNS-сервера. Правой кнопкой мыши щелкните узел **Reverse Lookup Zones** (Зоны обратного просмотра) в левой панели консоли и нажмите кнопку **New Zone** (Создать новую зону).
10. Нажмите кнопку **Next** (Далее) на странице **Welcome to the New Zone Wizard** (Вас приветствует мастер создания новой зоны).
11. На странице **Zone Type** (Тип зоны) выберите **Stub zone** (Зона-заглушка) и нажмите кнопку **Next** (Далее).
12. Выберите **Network ID** (Идентификатор сети ID). На странице **Reverse Lookup Zone Name** (Имя **зоны** обратного просмотра) введите в текстовое поле **Network ID** (Идентификатор сети ID) идентификатор сети, в которой расположен DNS-сервер внутренней сети (рис. 6.17). Нажмите кнопку **Next** (Далее).
13- На странице **Zone File** (Файл зоны) оставьте стандартное имя файла и нажмите кнопку **Next** (Далее).
14. На странице **Master DNS Servers** (Основные DNS-серверы) введите IP-адреса DNS-сервера внутренней сети и нажмите кнопку **Add** (Добавить). Щелкните мышью кнопку **Next** (Далее).
15. Нажмите кнопку **Finish** (Готово) на странице **Completing the New Zone Wizard** (Завершение мастера создания новой зоны).

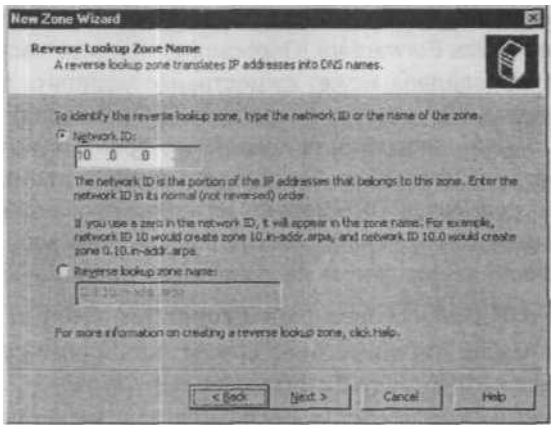


РИС. 6.17. Страница Reverse Lookup Zone Name (Имя зоны обратного просмотра)

] 6. Затем нужно создать зону прямого просмотра для зоны-заглушки. Правой кнопкой мыши щелкните узел **Forward Lookup Zones** (Зоны прямого просмотра) в левой панели консоли и выберите пункт **New Zone...** (Создать новую зону...).

17. Нажмите кнопку **Next** (Далее) на странице **Welcome to the New Zone Wizard** (Мастер создания новой зоны).

18. На странице **Zone** Type (Тип зоны) выберите **Stub zone** (Зона-заглушка) и щелкните кнопку **Next** (Далее).

19. На странице **Zone name** (Имя зоны) введите имя домена внутренней сети в текстовое поле **Zone** name (Имя зоны). Нажмите кнопку **Next** (Далее).

20. На странице **Zone File** (Файл зоны) (рис. 6.18) оставьте стандартное имя файла зоны и щелкните кнопку **Next** (Далее).

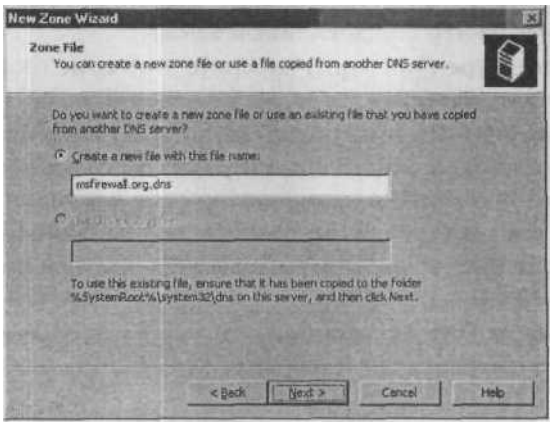


Рис. 6.18. Страница Zone File (Файл зоны)

21. На странице **Master DNS Servers** (Основные DNS-серверы) введите IP-адрес DNS-сервера внутренней сети и нажмите кнопку **Add** (Добавить). Нажмите кнопку **Next** (Далее).
22. Нажмите кнопку **Finish** (Готово) на странице **Completing the New Zone Wizard** (Завершение мастера создания новой зоны).
23. Правой кнопкой мыши щелкните имя сервера в левой панели консоли; установите курсор мыши на пункт **All Tasks** (Все задачи) и нажмите кнопку **Restart** (Перезапустить).

Конфигурирование службы DNS на DNS-сервере внутренней сети

Если в организации имеется инфраструктура DNS, то следует настроить DNS-сервер внутренней сети на использование DNS-сервера на брандмауэре ISA Server 2004 в качестве сервера пересылки в DNS. Такая конфигурация DNS является более безопасной, потому что DNS-сервер внутренней сети никогда напрямую не взаимодействует с не вызывающим доверия DNS-сервером в Интернете.

DNS-сервер внутренней сети пересылает DNS-запросы на DNS-сервер на брандмауэре ISA Server 2004, а DNS-сервер на брандмауэре ISA Server 2004 разрешает имя, сохраняет результат в своем кэше, а затем возвращает IP-адрес на DNS-сервер во внутренней сети.

> ПРЕДУПРЕЖДЕНИЕ Перечисленные далее действия следует выполнять, только если во внутренней сети имеется DNS-сервер, а внутренний интерфейс брандмауэра ISA был настроен на использование внутреннего DNS-сервера. Если внутреннего DNS-сервера нет, то эти действия выполнять не нужно.

Выполните следующие действия на DNS-сервере внутренней сети, чтобы настроить его на использование DNS-сервера на брандмауэре ISA в качестве сервера пересылок:

1. Нажмите кнопку **Start** (Пуск) и установите курсор мыши на **Administrative tools** (Администрирование) и щелкните пункт **DNS.**
2. В консоли **DNS Management** (Управление DNS-сервером) правой кнопкой мыши щелкните имя сервера в левой панели консоли и в контекстном меню выберите пункт **Properties** (Свойства).
3. В диалоговом окне **Properties** (Свойства) щелкните мышью вкладку **Forwarders** (Пересылка) (рис. 6.19).
4. На вкладке **Forwarders** (Пересылка) введите IP-адрес внутреннего интерфейса брандмауэра ISA Server 2004 в текстовое поле **Selected domain's forwarder IP address list** (Список IP-адресов серверов пересылки для выбранного домена). Нажмите кнопку **Add** (Добавить).
5. IP-адрес внутреннего интерфейса брандмауэра ISA Server 2004 появится в списке адресов серверов пересылки (рис. 6.19).

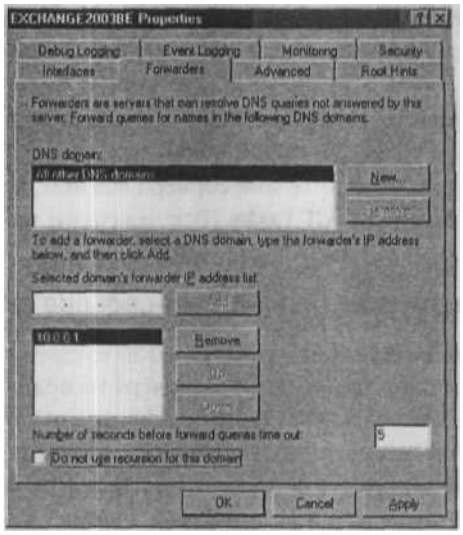


Рис. 6.19. Вкладка Forwarders (Пересылка)

6. Установите флажок в поле Do not use recursion for this domain (Не использовать рекурсию для этого домена) (рис. 6.20). Этот параметр запрещает DNS-серверу внутренней сети разрешать имя самостоятельно в случае, если сервер пересылок на брандмауэре ISA не способен разрешить имя.

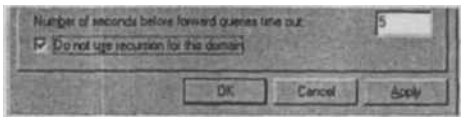


Рис. 6.20. Отключение рекурсии

Обратите внимание, что DNS-сервер во внутренней сети еще не способен разрешать имена хостов в Интернете. Еще нужно создать правило доступа, которое разрешает DNS-серверу доступ к DNS-серверу на брандмауэре ISA. Далее в этом разделе показано, как создавать такое правило доступа.

Установка и конфигурирование DHCP-сервера на брандмауэре ISA

У каждого компьютера должен быть IP-адрес и другая информация, позволяющая ему взаимодействовать с другими компьютерами в сети и в Интернете. Служба DHCP-сервера может быть установлена на брандмауэре ISA, она предоставляет информацию об IP-адресах компьютерам во внутренней сети. Предположим, что брандмауэр ISA будет использоваться в качестве DHCP-сервера. Если в сети уже есть DHCP-сервер, то следующий раздел можно пропустить.

ПРЕДУПРЕЖДЕНИЕ В сети не должно быть других DHCP-серверов. Если в сети есть еще один компьютер, выступающий в роли DHCP-сервера, то нужно отключить на нем службу DHCP так, чтобы брандмауэр ISA Server 2004 выступал в роли единственного DHCP-сервера в сети.

Установка службы DHCP

Службу DHCP-сервера можно установить на базе ОС Windows 2000 Server и Windows Server 2003. Процесс установки немного отличается для этих двух операционных систем. В этом разделе рассматривается установка службы DHCP-сервера на базе Windows 2000 Server и Windows Server 2003.

Установка службы DHCP-сервера на базе Windows Server 2003

Для того чтобы установить службу DNS-сервера на базе Windows Server 2003, выполните следующие действия:

1. Нажмите кнопку **Start** (Пуск), установите курсор мыши на **Control Panel** (Панель управления) и выберите пункт **Add or Remove Programs** (Установка и удаление программ).
2. В окне **Add or Remove Programs** (Установка или удаление программ) щелкните мышью **Add/Remove Windows Components** (Установка/Удаление компонентов Windows).
3. В диалоговом окне **Windows Components Wizard** (Мастер компонентов Windows) выберите **Networking Services** (Сетевые службы) из списка Components (Компоненты Windows). Не уста на вливайте флажок в поле! Выделив запись **Networking Services** (Сетевые службы) нажмите кнопку **Details...** (Состав...).
4. В диалоговом окне **Networking Services** (Сетевые службы) (рис. 6.21) установите флажок в поле **Dynamic Host Configuration Protocol (DHCP)** и нажмите кнопку OK

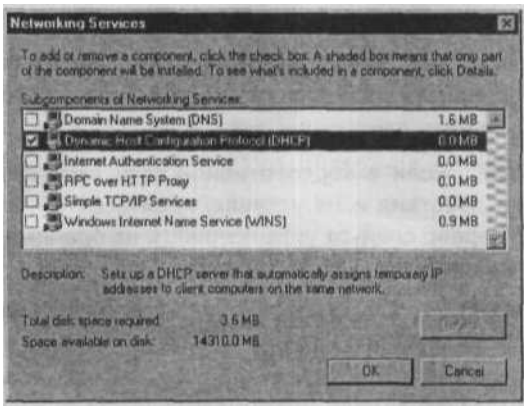


Рис. 6.21. Диалоговое окно **Networking Services** (Сетевые службы)

5. Нажмите кнопку **Next** (далее) в диалогором окне **Windows Components** (Ком поненты Windows).
6. Нажмите кнопку **Finish** (Готово) на странице **Completing the Windows Compo nents Wizard** (Завершение мастера компонентов Windows).
7. Закройте окно **Add or Remove Programs** (Установка или удаление программ).

Конфигурирование службы DHCP

DHCP-сервер должен быть сконфигурирован с набором IP-адресов, которые он может присваивать компьютерам в частной сети. DPICP-сервер также предоставляет дополнительную информацию помимо IP-адреса, включающую адрес DNS-сервера, основной шлюз и первичное имя домена.

Адреса DNS-сервера и основного шлюза, назначаемые компьютеру, совпадают с IP-адресом внутреннего интерфейса брандмауэра ISA. DHCP-сервер использует область DHCP, чтобы предоставить эту информацию клиентам внутренней сети. Необходимо создать область DHCP, которая предоставляет клиентам внутренней сети правильную информацию об IP-адресах.

> ПРИМЕЧАНИЕ DHCP-сервер не должен назначать адреса, которые уже используются в сети. Нужно создать исключения для этих IP-адресов. В качестве примера можно привести статические или зарезервированные адреса, назначенные печатным, файловым, почтовым или Web-серверам, это лишь несколько примеров устройств или серверов, которые постоянно используют одни и те же назначенные им на постоянной основе IP-адреса. Если для этих адресов не создать исключения, то DHCP-сервер выполнит разрешение адресов, а когда он обнаружит, что эти адреса уже используются, то он поместит их в группу плохих адресов (bad address group). Кроме того, хорошо сконфигурированная сеть сгруппирует компьютеры в смежные блоки IP-адресов. Например, все компьютеры, которым должны быть назначены статические IP-адреса, входят в один блок.

Для того чтобы настроить DHCP-сервер на базе Windows Server 2003 с областью, которая будет назначать правильную информацию об IP-адресах клиентам внутренней сети, выполните следующие действия:

> ПРЕДУПРЕЖДЕНИЕ Если в корпоративной сети уже есть DHCP-сервер, не выполняйте эти действия и не устанавливайте DHCP-сервер на брандмауэре ISA. DHCP-сервер следует устанавливать на брандмауэре ISA, только если во внутренней сети нет DHCP-сервера.

1. Нажмите кнопку **Start** (Пуск) и установите курсор мыши на **Administrative Tools** (Администрирование). Нажмите кнопку **DHCP.**
2. Разверните все узлы в левой панели консоли **DHCP.** Правой кнопкой мыши щелк ните имя сервера в левой панели консоли и нажмите кнопку **New Scope** (Соз дать область).

3. Нажмите кнопку **Next** (Далее) на странице **Welcome to the New Scope Wizard** (Вас приветствует мастер создания области).
4. Введите **SecureNAT Client Scope** (Область для клиента SecureNAT) в текстовом поле **Name** (Имя) на странице **Scope Name** (Имя области). Нажмите кнопку **Next** (Далее).
5. На странице **IP Address Range** (Диапазон адресов) введите первый IP-адрес и последний IP-адрес диапазона в текстовые поля **Start IP address** (Начальный IP-адрес) и **End IP address** (Конечный IP-адрес). Например, при использовании иден тификатора сети 192.168.1.0 с маской подсети 255.255.255.0 введите начальный IP-адрес 192.168.1.1, а конечный IP-адрес 192.168.1.254. Нажмите кнопку **Next** (Далее).
6. На странице **Add Exclusions** (Добавление исключений) введите IP-адрес внут реннего интерфейса брандмауэра ISA в текстовое поле **Start IP address** (Началь ный IP-адрес) и нажмите кнопку **Add** (Добавить). Если в сети имеются серверы или рабочие станции со статическими IP-адресами, которые не нужно менять, добавьте эти адреса в список исключений. Нажмите кнопку **Next** (Далее), после того как будут добавлены все адреса, которые нужно исключить из области **DHCP.**
7. На странице **Lease Duration** (Срок действия аренды адреса) оставьте стандартное значение и нажмите кнопку **Next** (Далее).
8. На странице **Configuring DHCP Options** (Настройка параметров DHCP) выбе рите **Yes, I want to configure these options now** (Да, настроить эти парамет ры сейчас) и щелкните кнопку **Next** (Далее).
9. На странице **Router** (Маршрутизатор, основной шлюз) введите IP-адрес внут реннего интерфейса брандмауэра ISA и нажмите кнопку **Add** (Добавить). Нажмите кнопку **Next** (Далее).
10. На странице **Domain Name and DNS Servers** (Имя домена и DNS-серверы) вве дите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовое поле **IP address** (IP-адрес) и нажмите кнопку **Add** (Добавить). Если во внутренней сети имеется домен **Active Directory,** введите имя домена внутренней сети в текстовое поле **Parent domain** (Родительский домен). Не вводите имя домена в тексто вое поле **Parent domain** (Родительский домен), если во внутренней сети нет домена **Active Directory.** Щелкните кнопку **Next** (Далее).
11. Не вводите никакую информацию на странице **WINS Servers** (WINS-серверы), если во внутренней сети нет WINS-сервера. Если во внутренней сети имеется WINS-сервер, введите этот IP-адрес в текстовое поле **IP address** (IP-адрес). На жмите кнопку **Next** (Далее).
12. Выберите **Yes, I want to activate this scope now** (Да, **я** хочу активировать эту область сейчас) на странице **Activate Scope** (Активировать область) и нажми те кнопку **Yes** (Да).
13. Нажмите кнопку **Finish** (Готово) на странице **Completing the New Scope Wizard** (Завершение мастера создания области).

Установка и конфигурирование программного обеспечения ISA Server 2004

Теперь можно приступить к установке программного обеспечения брандмауэра ISA.

Чтобы установить программное обеспечение брандмауэра ISA на компьютере на базе ОС Windows Server 2003 с двумя сетевыми адаптерами, выполните следующие действия:

1. Вставьте установочный компакт-диск для ISA Server 2004 в дисковод для компакт-дисков или установите соединение с общим сетевым ресурсом, в котором находятся установочные файлы ISA Server 2004. Если программа установки не запустится автоматически, дважды щелкните мышью файл isaautorun.exe в корне дерева установочных файлов.
2. На странице **Microsoft Internet Security and Acceleration Server 2004** щелкните мышью **Review Release Notes** (Информация о версии) и прочтите информацию о версии. Эта информация о версии содержит полезные данные о важных моментах и возможностях конфигурирования. После просмотра информации о версии щелкните мышью **Read Setup and Feature Guide** (Прочесть руководство по установке и функциям). Не обязательно читать все руководство сразу, его можно распечатать и прочесть потом. Щелкните мышью **Install ISA Server 2004** (Установить ISA Server 2004).
3. Нажмите кнопку **Next** (Далее) на странице **Welcome to the Installation Wizard for Microsoft ISA Server 2004** (Мастер установки Microsoft ISA Server 2004).
4. Выберите вариант **I accept the terms in the license agreement** (Я согласен) на странице **License Agreement** (Лицензионное соглашение). Нажмите кнопку **Next** (Далее).
5. На странице **Customer Information** (Информация о пользователе) введите имя пользователя и название организации в текстовые поля **User Name (Имя)** и **Organization** (Организация). Введите серийный номер в текстовое поле **Product Serial Number** (Серийный номер). Щелкните кнопку **Next** (Далее).
6. На странице **Setup Type** (Тип установки) щелкните мышью вариант **Custom** (Пользовательская). Если не нужно устанавливать программное обеспечение брандмауэра ISA на диске C:, щелкните мышью кнопку **Change** (Изменить), чтобы изменить место установки программы на жестком диске. Нажмите кнопку **Next** (Далее).
7. На странице **Custom Setup** (Пользовательская установка) выберите устанавливаемые компоненты. По умолчанию устанавливаются компоненты **Firewall Services, Advanced Logging** и **ISA Server Management.** Средство контроля SMTP-сообщений (Message Screener), которое используется для того, чтобы контролировать спам и вложения, поступающие в сеть и исходящие из нее, не устанавливается по умолчанию. Прежде чем устанавливать Message Screener, нужно установить SMTP-службу IIS 6.0 на компьютере брандмауэра ISA Server 2004. В данном случае будет установлен общий ресурс с установочными файлами для кли-

ента брандмауэра Firewall Client Installation Share, чтобы впоследствии можно было установить клиент брандмауэра на других компьютерах во внутренней сети. Щелкните мышью значок x слева от параметра **Firewall Client Installation Share** и щелкните мышью **This feature, and all subfeatures, will be installed on the local hard drive** (Эта функция и все подфункции будут установлены на локальном жестком диске) (рис. 6.22). Использование клиента брандмауэра позволяет лучше защитить сеть, по возможности следует всегда устанавливать клиент брандмауэра на клиентских компьютерах во внутренней сети. Более подробно этот вопрос обсуждается в главе 5. Нажмите кнопку **Next** (Далее).

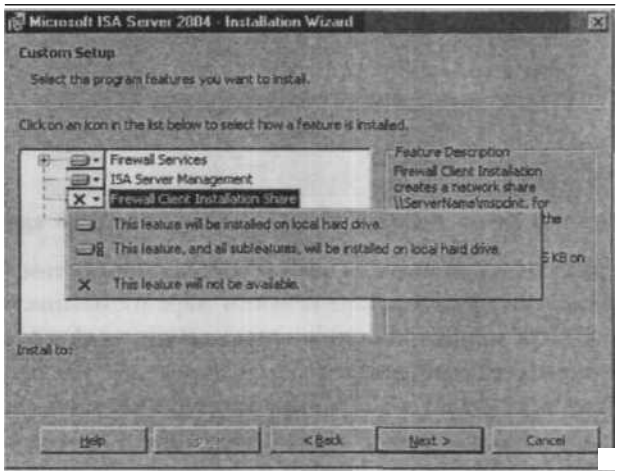


Рис. 6.22. Страница Custom Setup (Пользовательская установка)

8. На странице **Internal Network** (Внутренняя сеть) нажмите кнопку **Add** (Добавить). Внутренняя сеть отличается от таблицы локальных адресов (LAT, Local Address Table), которая использовалась в брандмауэре ISA Server 2000. Внутренняя сеть включает в себя доверяемые сетевые службы, с которыми должен взаимодействовать брандмауэр ISA. В качестве примера таких служб можно привести контроллеры домена Active Directory, DNS, DHCP, службы терминалов и др. Системная политика брандмауэра использует определение внутренней сети во многих правилах системной политики.
9. На странице **Internal Network** (Внутренняя сеть) нажмите кнопку **Select Network Adapter** (Выбрать сетевой адаптер).
10. На странице **Configure Internal Network** (Настроить внутреннюю сеть) снимите флажок в поле **Add the following private ranges...** (Добавить следующие частные диапазоны...). Оставьте флажок в поле **Add address ranges based on the Windows Routing Table** (Добавить диапазоны адресов на основе таблицы маршрутизации Windows) (рис. 6.23). Установите флажок в поле рядом с адаптером, соединенным со внутренней сетью. В данном случае сетевые интерфей-

сы были переименованы так, чтобы имя интерфейса отражало его расположение. Нажмите кнопку OK.

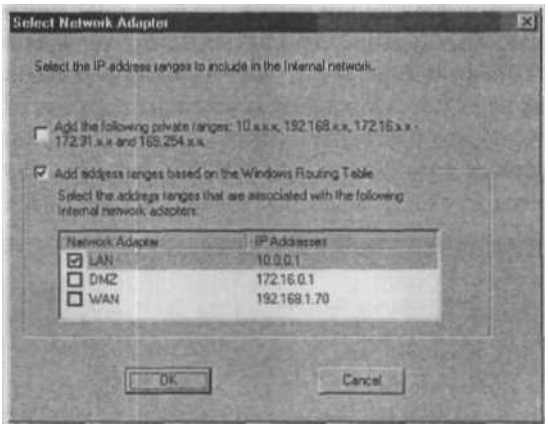


Рис. 6.23. Страница Select Network Adapter (Выбрать сетевой адаптер)

11. Нажмите кнопку OK в диалоговом окне с сообщением о том, что внутренняя сеть была определена на основании таблицы маршрутизации Windows.
12. Щелкните кнопку OK в диалоговом окне **Internal network address ranges** (Ди апазоны адресов внутренней сети).
13. Нажмите кнопку **Next** (Далее) на странице **Internal Network** (Внутренняя сеть).
14. Не устанавливайте флажок в поле **Allow computers running earlier versions of Firewall Client software to connect** (Разрешить соединения компьютерам с более ранними версиями программного обеспечения клиента брандмауэра). Этот параметр предполагает применение клиента брандмауэра нового бранд мауэра ISA. Предыдущие версии клиента брандмауэра (входящие в Proxy 2.0 и ISA Server 2000) не поддерживаются. Этот параметр также разрешает клиенту брандмауэра отправлять верительные данные пользователя по зашифрованно му каналу на брандмауэр ISA и проходить проверку подлинности на брандмау эре ISA в прозрачном режиме. Щелкните кнопку **Next** (Далее).
15. На странице **Services** (Службы) отметьте, чтобы службы SNMP и IIS Admin Service были остановлены на время установки. Если на компьютере брандмауэра ISA Server 2004 установлены **службы Internet Connection Firewall (ICF)/Internet Connection Sharing (ICF)** и/или служба **IP Network Address Translation,** то они будут отключены, т. к. они конфликтуют с программным обеспечением бранд мауэра ISA Server 2004.
16. Щелкните кнопку **Install** (Установить) на странице **Ready to Install the Program** (Установка программы).
17. На странице **Installation** Wizard **Completed** (Завершение работы мастера ус тановки) нажмите кнопку **Finish** (Готово).

18. Щелкните кнопку **Yes** (Да) в диалоговом окне **Microsoft ISA Server,** в котором сообщается, что нужно перезапустить сервер.
19. Выполните вход в систему как администратор после перезапуска компьютера.
20. Нажмите кнопку **Start** (Пуск) и установите курсор на **All Programs** (Програм мы). Установите курсор на **Microsoft ISA Server** и выберите пункт **ISA Server Management.** Откроется консоль управления **Microsoft Internet Security and Acceleration Server 2004,** и появится страница **Welcome to Microsoft Internet Security and Acceleration Server 2004.**

Конфигурирование брандмауэра ISA

Теперь можно настроить политику доступа на брандмауэре ISA. Нужно создать пять правил доступа:

- правило, разрешающее клиентам внутренней сети доступ к DHCP-серверу на брандмауэре ISA;
- правило, разрешающее брандмауэру ISA отправлять DHCP-сообщения хостам во внутренней сети;
- правило, разрешающее DNS-серверу внутренней сети использовать брандмау эр ISA в качестве своего DNS-сервера. Это правило следует создавать, только если во внутренней сети имеется DNS-сервер;
- правило, разрешающее клиентам внутренней сети доступ к DNS-серверу в ре жиме только кэширования на брандмауэре ISA. Это правило используется, только если во внутренней сети нет DNS-сервера или если нужно использовать бранд мауэр ISA в качестве DNS-сервера в режиме только кэширования с зоной-за глушкой, указывающей на домен внутренней сети;
- правило «все открыто», разрешающее клиентам внутренней сети доступ ко всем протоколам и узлам Интернета.

В табл. 6.8-6.12 представлена подробная информация о каждом из этих правил.

Табл. 6.8. Правило для запроса к DHCP-серверу

Название	DHCP Request to Server (запрос к DHCP-серверу)
Действие	Разрешающее
Протоколы	DHCP (запрос)
Источник	Любой
Адресат	Локальный хост
Пользователи	Все
График	Всегда
Типы содержимого	Все
Назначение	Это правило разрешает DHCP-клиентам отправлять DHCP-запросы на DHCP-сервер, установленный на брандмауэре ISA

Табл. 6.9. Правило для DHCP-ответа от сервера

Название	DHCP Reply from Server (DHCP-ответ от сервера)
Действие	Разрешающее
Протоколы	DHCP (ответ)
Источник	Локальный хост
Адресат	Внутренняя сеть
Пользователи	Все
График	Всегда
Типы содержимого	Все
Назначение	Это правило разрешает DHCP-серверу на брандмауэре ISA отвечать на DHCP-запросы от DHCP-клиентов внутренней сети

Табл. 6.10. Правило перенаправления запросов от внутреннего DNS-сервера к серверу пересылок

Название	Internal DNS Server to Forwarder (перенаправление запросов от внутреннего DNS-се рв ера к серверу пересылок (DNS))
Действие	Разрешающее
Протоколы	DNS
Источник	DNS-сервер'
Адресат	Локальный хост
Пользователи	Все
График	Всегда
Типы содержимого	Все
Назначение	Это правило разрешает внутреннему DNS-серверу перенаправлять запросы на сервер пересылок (DNS) на компьютере брандмауэра ISA Server 2004. Это правило следует создавать только в том случае, если во внутренней сети имеется DNS-сервер

' Определенный пользователем.

Табл. 6.11. Правило доступа из внутренней сети к DNS-серверу

Название	Internal Network to DNS Server (правило доступа из внутренней сети к DNS-серверу)
Действие	Разрешающее
Протоколы	DNS
Источник	Внутренняя сеть
Адресат	Локальный хост
Пользователи	Все
График	Всегда
Типы содержимого	Все

Табл. 6.11. (окончание)

Название	Internal Network to DNS Server (правило доступа из внутренней сети к DNS-серверу)
Назначение	Это правило разрешает клиентам внутренней сети доступ к DNS-серверу в режиме только кэширования на брандмауэре ISA. Это правило нужно создавать только в том случае, если во внутренней сети нет DNS-сервера или если DNS-сервер в режиме только кэширования будет использоваться в качестве сервера пересылок в режиме только кэширования для всех клиентов внутренней сети, даже если при этом во внутренней сети имеется DNS-сервер

Табл. 6.12. Правило «All Open»

Название	All Open («Все открыто»)
Действие	Разрешающее
Протоколы	Весь исходящий трафик
От	Внутренняя сеть
Для	Внешняя сеть
Пользователи	Все
График	Всегда
Типы содержимого	Все
Назначение	Это правило разрешает клиентам внутренней сети доступ ко всем протоколам и узлам в Интернете

ПРЕДУПРЕЖДЕНИЕ Последнее правило, «все открыто», используется только для того, чтобы начать работу. Это правило позволяет протестировать способность брандмауэра ISA устанавливать соединение с Интернетом, но оно не обеспечивает никакого контроля исходящего доступа, как это делают большинство аппаратных брандмауэров с фильтрацией пакетов. Брандмауэр ISA способен обеспечить контроль входящего и исходящего трафика, поэтому нужно выключить это правило и создать правила для пользователей/групп, для протоколов и для узлов после того, как базовые соединения с Интернетом через брандмауэр ISA окажутся успешными.

Помимо этих правил доступа, следует настроить системную политику брандмауэра, чтобы разрешить DHCP-ответы с DHCP-серверов внешней сети.

Правило «DHCP Request to Server»

Для того чтобы создать правило «DHCP Request to Server» (DHCP-запрос к серверу), выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера и щелкните пункт **Firewall Policy** (Политика брандмауэра).

В узле **Firewall Policy** (Политика брандмауэра) щелкните вкладку **Tasks** (Задачи). На панели задач щелкните мышью пункт **Create a New Access Rule** (Создать новое правило доступа).

3. На странице **Welcome to the New Access Rule Wizard** (Мастер создания нового правила доступа) введите **DHCP Request to Server** (DHCP-запрос к серверу) в текстовое поле **Access Rule name** (Имя правила доступа). Щелкните кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите **Allow** (Разрешающее) и нажмите кнопку Next (Далее).
5. На странице **Protocols** (Протоколы) выберите вариант **Selected protocols** (К выбранным протоколам) из списка **This rule applies to** (Это правило применяется) и щелкните кнопку **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) (рис. 6.24) щелкните папку **Infrastructure** (Инфраструктура). Дважды щелкните мышью запись **DHCP (request)** (DHCP, запрос) и нажмите кнопку **Close** (Закрыть).

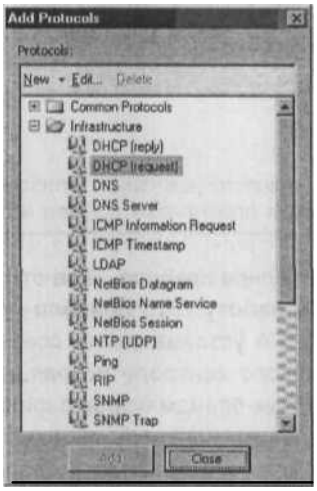


Рис. 6.24. Диалоговое окно Add Protocols (Добавить протоколы)

7. Нажмите кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники для правила доступа) щелкните кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computer Sets** (Подмножества компьютеров). Дважды щелкните мышью запись **Anywhere** (Везде) и нажмите кнопку **Close** (Закрыть).
10. Нажмите кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники для правила доступа).

11. На странице **Access Rule Destinations** (Адресаты правила доступа) щелкните кнопку **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью **Local Host** (Локаль ный хост). Щелкните кнопку **Close** (Закрыть).
13- Нажмите кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адреса- ты правила доступа).
14. На странице **User Sets** (Подмножества пользователей) оставьте значение по умол чанию **All Users** (Все пользователи) и щелкните, кнопку **Next** (Далее).
15. На странице **Completing the New Access Rule Wizard** (Завершение работы ма стера создания нового правила доступа) проверьте настройки и нажмите кноп ку **Finish** (Готово).

Правило «DHCP Reply from Server»

Для создания правила **«DHCP Reply from Server»** (DHCP-ответ от сервера) выполните следующие **действия:**

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера и нажмите **кнопку Firewall Policy** (Политика бранд мауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните мышью вкладку **Tasks** (Задачи) на панели задач. На панели задач щелкните мышью **Create a New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Мастер создания ново го правила доступа) введите **DHCP Reply from Server** (DHCP-ответ от серве ра) в текстовое поле **Access Rule name** (Имя правила доступа). Щелкните кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите **Allow** (Разрешающее) и щелкните кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите вариант **Selected protocols** (К выбранным протоколам) из списка **This rule applies to** (Это правило при меняется) и щелкните кнопку **Add** (Добавить) (рис. 6.25).
6. В диалоговом окне **Add Protocols** (Добавить **протоколы)** щелкните мышью пап ку **Infrastructure** (Инфраструктура). Дважды щелкните мышью **запись DHCP (reply)** (DHCP, ответ) и нажмите кнопку Close (Закрыть).
7. Нажмите кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники для правила доступа) щелкните кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети). Дважды щелкните мышью запись **Local Host** (Ло кальный хост) и нажмите кнопку **Close** (Закрыть).

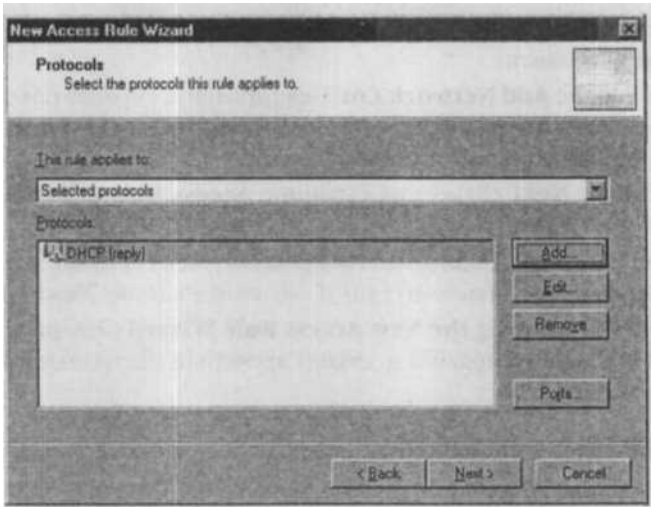


Рис. 6.25. Страница Protocols (Протоколы)

10. Нажмите кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники для правила доступа).
11. На странице **Access Rule Destinations** (Адресаты для **правила** доступа) щелк ните кнопку **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью запись **Internal** (Внутренняя). Нажмите кнопку **Close** (Закрыть).
13. Нажмите кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адреса ты правила доступа).
14. На странице **User Sets** (Подмножества пользователей) оставьте значение по умол чанию **(All Users** (Все пользователи)) и щелкните кнопку **Next** (Далее).
15. На странице **Completing the New Access Rule Wizard** (Завершение работы ма стера создания нового правила доступа) проверьте настройки и нажмите кноп ку **Finish** (Готово).

Правило «Internal DNS Server to DNS Forwarder»

Для создания правила **«Internal DNS Server to DNS Forwarder»** (От внутреннего DNS-сервера к серверу пересылок DNS) выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера и щелкните мышью пункт **Firewall Policy** (Поли тика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните мышью вкладку **Tasks** (Задачи) на панели задач. На панели задач щелкните мышью пункт **Create a New Access Rule** (Создать новое правило доступа).

3. На странице **Welcome to the New Access Rule Wizard** (Мастер создания ново го правила доступа) введите **Internal DNS Server to DNS Forwarder** (От внут реннего DNS-сервера к серверу пересылок DNS) в текстовом поле **Access Rule name** (Имя правила доступа). Нажмите кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите **Allow** (Разрешающее) и щелкните кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите вариант **Selected protocols** (К выбранным протоколам) из списка **This rule applies to** (Это правило при меняется) и щелкните кнопку **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **Infrastructure** (Инфраструктура). Дважды щелкните мышью запись **DNS** и щелкните кнопку **Close** (Закрыть). Нажмите кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники для правила доступа) щелкните кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) (рис. 6.26) щелкните мышью меню **New** (Новый), а затем **Computer** (Компьютер).

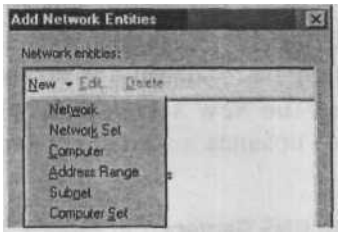


Рис. 6.26. Выбор **Computer** (Компьютер)

10. В диалоговом окне **New Computer Rule Element** (Новый элемент правила для компьютера) введите **Internal DNS Server** (Внутренний DNS-сервер) в тексто вое поле **Name** (Имя). Введите 10.0.0.2 в текстовое поле **Computer IP Address** (IP-адрес компьютера). Нажмите кнопку OK.
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) (рис. 6.27) щелкните мышью папку **Computers** (Компьютеры) и дважды щелкните мышью запись **Internal DNS Server** (Внутренний DNS-сервер). Нажмите кнопку **Close** (Закрыть).
12. Нажмите кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники для правила доступа).
13. Нажмите кнопку **Add** (Добавить) на странице **Access Rule Destinations** (Адресаты правила доступа).
14. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью **Local Host** (Локальный хост). Нажмите кнопку Close (Закрыть).

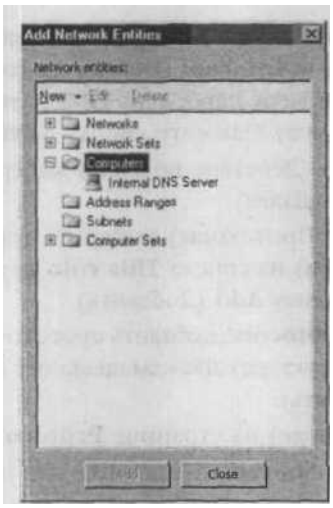


Рис. 6.27. Выбор нового объекта Computer (Компьютер)

15. Нажмите кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты правила доступа).
16. На странице **User Sets** (Подмножества пользователей) оставьте значение по умолчанию **All Users** (Все пользователи) и нажмите кнопку **Next** (Далее).
17. На странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку **Finish** (Готово).

Правило «Internal Network to DNS Server»

Для создания правила **«Internal Network to DNS Server»** (Из внутренней сети к DNS-серверу) выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера и щелкните мышью **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните мышью вкладку **Tasks** (Задачи) на панели задач. На панели задач щелкните мышью **Create a New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Мастер создания ново го правила доступа) введите **Internal Network to DNS Server** (Из внутренней сети к DNS-серверу) в текстовое поле **Access Rule name** (Имя правила досту па). Нажмите кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите **Allow** (Разрешающее) и нажмите кнопку **Next** (Далее).

5. На странице **Protocols** (Протоколы) выберите вариант **Selected protocols (К** выбранным протоколам) из списка **This rule applies to** (Это правило при меняется) и нажмите кнопку **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **Common Protocols** (Общие протоколы). Дважды щелкните мышью запись **DNS** и нажмите кнопку **Close** (Закрыть).
7. Нажмите кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники для правила доступа) нажмите кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети). Дважды щелкните мышью **Internal** (Внутренняя сеть) и нажмите кнопку **Close** (Закрыть).
10. Нажмите кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники для правила доступа).
11. Нажмите кнопку **Add** (Добавить) на странице **Access Rule Destinations** (Адре саты правила доступа).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью **Local Host** (Локаль ный хост). Нажмите кнопку **Close** (Закрыть).
13. Нажмите кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адреса ты правила доступа).
14. На странице **User Sets** (Подмножества пользователей) оставьте значение по умолчанию **All Users** (Все пользователи) и нажмите кнопку **Next** (Далее).
15. На странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила **доступа)** проверьте настройки и нажмите кнопку **Finish** (Готово).

Правило »АИ Open»

Для создания правила **«All Open»** (Все открыто) выполните следующие действия:

1. В консоли управления **Microsoft Internet Security and Acceleration Server 2004** разверните имя сервера и щелкните мышью **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните мышью вкладку **Tasks** (Задачи) на панели задач. На панели задач щелкните мышью **Create a New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила **доступа)** введите **All Open** (Все открыто) в текстовое поле **Access Rule name** (Имя правила доступа). Нажмите кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите **Allow** (Разрешающее) и нажмите кнопку **Next** (Далее).

5. На странице **Protocols** (Протоколы) выберите вариант **All outbound traffic** (Ко всему исходящему трафику) из списка **This rule applies to** (Это правило при меняется) и нажмите кнопку **Next** (Далее).
6. Нажмите кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
7. На странице **Access Rule Sources** (Источники для правила доступа) нажмите кнопку **Add** (Добавить).
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети). Дважды щелкните мышью **Internal** (Внутрен няя) и нажмите кнопку **Close** (Закрыть).
9. Нажмите кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники для правила доступа).
10. Нажмите кнопку **Add** (Добавить) на странице **Access Rule Destinations** (Адре саты правила доступа).
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью **External** (Внешняя). Нажмите кнопку **Close** (Закрыть).
12. Нажмите кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адреса ты правила доступа).
13. На странице **User Sets** (Подмножества пользователей) оставьте значение по умолчанию **All Users** (Все пользователи) и нажмите кнопку **Next** (Далее).
14. На странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила доступа) проверьте настройки и нажмите кнопку **Finish** (Готово).

Правило доступа должно выглядеть, как на рис. 6.28. В данном случае не нужно менять порядок правил. При создании расширенных правил доступа для контроля исходящего и входящего доступа, возможно, потребуется изменить порядок правил, чтобы добиться желаемых результатов.

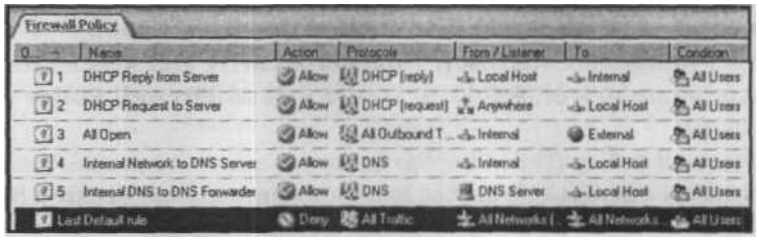


Рис. 6.28. Политика брандмауэра

Конфигурирование компьютеров внутренней сети

Компьютеры внутренней сети настраиваются как клиенты SecureNAT ISA Server. Клиент SecureNAT — это компьютер, адрес основного шлюза которого настроен как

IP-адрес сетевого устройства, маршрутизирующего запросы из Интернета на внутренний IP-адрес брандмауэра ISA Server 2004.

Когда компьютеры внутренней сети имеют тот же идентификатор сети, что и внутренний интерфейс брандмауэра ISA, основной шлюз компьютеров внутренней сети настраивается как внутренний IP-адрес на компьютере брандмауэра ISA. Так настраивается область DHCP на DHCP-сервере, расположенном на брандмауэре ISA.

В этом разделе описывается конфигурирование компьютеров внутренней сети, имеющих тот же идентификатор сети, что и внутренний интерфейс брандмауэра ISA Server 2004, и клиентов, которые могут иметь другой идентификатор сети. Чаще всего второй случай встречается в крупных сетях, в которых для внутренней сети есть более одного идентификатора сети.

ПРИМЕЧАНИЕ «Идентификатор сети» является частью IP-адреса. Обычно сети класса SOHO имеют только один идентификатор сети. Если же в сети за брандмауэром ISA есть маршрутизатор, то нужно учитывать идентификаторы сети.

Настройка клиентов внутренней сети как DHCP-клиентов

DHCP-клиенты запрашивают информацию об IP-адресах с DHCP-сервера. В этом разделе описывается, как настроить клиент Windows 2000 (Server или Professional) как DHCP-клиент. Эта процедура схожа для всех клиентов на базе Windows. Для того чтобы настроить клиент внутренней сети как DHCP-клиент, выполните следующие действия:

1. Правой кнопкой мыши щелкните значок **My Network Places** (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт **Properties** (Свойства).
2. В окне **Network Connections** (Сетевые подключения) правой кнопкой мыши щелкните внешний сетевой интерфейс и выберите пункт **Properties** (Свойства).
3. В диалоговом окне **Properties** (Свойства) сетевого интерфейса щелкните мышью запись **Internet Protocol (TCP/IP)** (Протокол Интернета, TCP/IP) и щелкните мышью пункт меню **Properties** (Свойства).
4. В диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства протокол Интернета TCP/IP) (рис. 6.29) выберите **Obtain an IP-address automatically** (Получить IP-адрес автоматически).
5. Выберите **Use the following DNS server addresses** (Использовать следующие адреса DNS-серверов). Введите IP-адрес внутреннего интерфейса в текстовое поле **Preferred DNS server** (Предпочитаемый DNS-сервер). Нажмите кнопку OK в диалоговом окне **Internet Protocol (TCP/IP) Properties** (Свойства протокола Интернета TCP/IP).

- требования к службам для выполнения распространенных задач на брандмауэ ре ISA. Выполнение ряда задач по обслуживанию брандмауэра ISA зависит от функций базовой операционной системы. В этом разделе рассматриваются некоторые такие функции и службы;
- роли клиентов брандмауэра ISA. Для различных сетевых служб брандмауэр ISA должен играть роль клиента сети. В этом разделе рассматриваются некоторые роли клиента сети и службы операционной системы, необходимые для того, чтобы брандмауэр ISA мог выполнять эти роли;
- административные роли и полномочия брандмауэра ISA. Не все администрато ры брандмауэра ISA имеют равные права. В этом разделе обсуждаются админи стративные роли брандмауэра ISA и то, как предоставить пользователям более тщательный контроль конфигурации и управления брандмауэром ISA;
- режим блокировки брандмауэра ISA. Брандмауэр ISA должен защитить себя и за висящую от него сеть в случае, если в результате атаки будет отключена служба брандмауэра ISA. В этом разделе обсуждается режим блокировки брандмауэра ISA.

Зависимость брандмауэра ISA от служб

Для пользователей брандмауэра ISA Server 2000 особую сложность представляло отсутствие четкой информации о том, какие службы необходимы для полной функциональности брандмауэра ISA. Многие сторонники брандмауэра ISA пытались выяснить, от каких служб зависит брандмауэр, но никакого руководства по этому вопросу так и не было создано. Более того, шаблоны улучшения системы System Hardening Templates для ISA Server 2000 постоянно прерывали работу ключевых функций брандмауэра и базовой операционной системы.

В новом брандмауэре ISA все эти проблемы решены. Теперь имеется точная информация о необходимых для программного обеспечения брандмауэра ISA служ-бах. В табл. 6.13 перечислены наиболее важные службы, которые должны быть ЕКЛЮ-чены для ISA Server, чтобы он мог нормально функционировать.

> ПРЕДУПРЕЖДЕНИЕ Не используйте никакие стандартные шаблоны безопасности, входящие в версию Windows, на базе который было установлено программное обеспечение брандмауэра ISA. Следует создать собственную политику безопасности на брандмауэре ISA, а затем на основе этой политики создать шаблон.

Табл. 6.13. Службы, от которых зависит работа брандмауэра ISA

Название службы	Объяснение	Тип запуска
COM+ Event System (Сие-тема событий COM+)	Базовая операционная система	Вручную
Cryptographic Services (Службы криптографии)	Базовая операционная система (безопасность)	Авто

Табл. 6.13. (продолжение)

Название службы	Объяснение	Тип запуска
Event Log (Журнал событий)	Базовая операционная система	Авто
IPScc Services (Службы IPSec)	Базовая операционная система (безопасность)	Авто
Logical Disk Manager (Диспетчер логических дисков) Logical Disk Manager Administrative Service (Служба администрирования диспетчера логических дисков)	Базовая операционная система (управление дисками)	Авто
	Базовая операционная система (управление дисками)	Вручную
Microsoft Firewall (Брандмауэр Microsoft)	Необходим для нормального функционирования ISA Server	Авто
Microsoft ISA Server Control (Контроль ISA Server Microsoft)	Необходим для нормального функционирования ISA Server	Авто
Microsoft ISA Server Job Scheduler (Планировщик заданий ISA Server Microsoft)	Необходим для нормального функционирования ISA Server	Авто
Microsoft ISA Server Storage (Служба хранения ISA Server Microsoft)	Необходима для нормального функционирования ISA Server	Авто
MSSQLJMSFW	Необходима, когда для ISA Server используются журналы MSDE	Авто
Network Connections (Сетевые подключения)	Базовая операционная система (сетевая инфраструктура)	Вручную
NTLM Security Support Provider (Поставщик поддержки безопасности NTLM)	Базовая операционная система (безопасность)	Вручную
Plug and Play	Базовая операционная система	Авто
Protected Storage (Защищенное хранилище)	Базовая операционная система (безопасность)	Авто
Remote Access Connection Manager (Диспетчер подключений удаленного доступа)	Необходима для нормального функционирования ISA Server	Вручную
Remote Procedure Call (Удаленный вызов процедур (RPC))	Базовая операционная система	Авто
Secondary Logon (Вторичный вход в систему)	Базовая операционная система (безопасность)	Авто
Security Accounts Manager (Диспетчер учетных записей безопасности)	Базовая операционная система	Авто

(см. след. стр.)

Табл. 6.13. (окончание)

Название службы	Объяснение	Тип запуска
Server (Сервер)	Необходима для общего ресурса клиента брандмауэра ISA Server (в зависимости от сети)'	Авто
Smart Card (Смарт-карты)	Базовая операционная система (безопасность)	Вручную
SQLAgentSMSFW	Необходима, когда для ISA Server используется создание журналов MSDE (при выборе параметра Advanced Logging в процессе установки не устанавливается)	Вручную
System Event Notification (Уведомление о системных событиях)	Базовая операционная система	Авто
Telephony (Телефония)	Необходима для нормального функционирования ISA Server	Вручную
Virtual Disk Service (Служба администрирования диспетчера логических дисков)	Базовая операционная система (управление дисками)	Вручную
Windows Management Instrumentat ion (Инструментарий управления Windows (WMI))	Базовая операционная система (WMI)	Авто
WMI Performance Adapter (Адаптер производительности WMI)	Базовая операционная система (WMI)	Вручную

" Тип запуска для службы сервера должен быть настроен на Авто в следующих случаях:

- на брандмауэре ISA устанавливается общий ресурс с установочными файлами клиента брандмауэра;
- для настройки виртуальной частной сети (VPN) используется служба маршрутизации и удаленного доступа, а не диспетчер ISA Server. Такой режим запуска необходим, если нужно использовать проверку подлинности пользователей на основе сертификатов EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации) для VPN-подключений по требованию и поиск и устранение неисправностей таких подключений;
- если служба сервера нужна для других задач или ролей;
- режим запуска для службы маршрутизации и удаленного доступа — « вручную». ISA Server запускает эту службу, только если включен VPN. Следует отметить, что служба сервера необходима, только если нужно обеспечить доступ *к* консоли маршрутизации и удаленного доступа (а не к консоли Microsoft Internet Security and Acceleration Server 2004) для настройки VPN-подключений удаленного доступа и «узел-в-узел».

Требования к службам для выполнения распространенных задач на брандмауэре ISA

Некоторые службы должны быть включены, для того чтобы брандмауэр ISA мог выполнять необходимые задачи. Все неиспользуемые службы должны быть отключены. В табл. 6.14 приводится ряд задач, которые должна выполнять базовая one-

рационная система брандмауэра ISA. Включите службы, необходимые для выполнения задач на брандмауэре ISA, и отключите службы, которые не потребуются.

Табл. 6.14. Службы, необходимые для выполнения распространенных задач на брандмауэре ISA

Задача	Применение службы	Необходимые службы	Тип запуска
Установка приложения на локальном компьютере с помощью Windows Installer	Необходима служба установки Microsoft для установки, удаления или восстановления приложений. Часто требуется устанавливать надстройки брандмауэра ISA для расширения функциональности брандмауэра и усиления его защиты	Windows Installer	Вручную
Резервирование	Необходима при использовании NTBackup или других программ резервирования на брандмауэре ISA	MS Software Shadow Copy Provider	Вручную
Резервирование	Необходима при использовании NTBackup или других программ резервирования на брандмауэре ISA	Volume Shadow Copy (Теневое копирование тома)	Вручную
Резервирование	Необходима при использовании NTBackup или других программ резервирования на брандмауэре ISA	Removable Storage Service (Служба управления съемными запоминающими устройства ми)	Вручную
Сообщение об ошибках	Необходима служба для сообщениях об ошибках, которые позволяют повысить надежность Windows, сообщая о критических ошибках Microsoft	Error Reporting Service (Служба регистрации ошибок)	Авто
Помощь и поддержка	Позволяет сохранять данные работе компьютера, исполь- случае возникнове- службами поддержки продуктов Microsoft	Help and Support о (Помощь зуемые в и поддержка) ния сбоев	ABTD
Поддержка общего установочного ресурса клиента брандмауэра	Необходима, чтобы разрешить компьютерам соединения с брандмауэром ISA по протоколам SMB/CIFS для установки программного обеспечения клиента брандмауэра	Server (Сервер)	**а,что**

(см. след. стр.)

Табл. 6.14. (окончание)

Задача	Применение службы	Необходимые службы	Тип запуска
Запись журналов в формате MSDE	Необходима для создания журналов с помощью баз данных MSDE. Если не включать соответствующую службу, то можно создавать журналы в базах данных SQL или в файлах. Однако в таком случает нельзя пользоваться оснасткой Event Viewer (Просмотр событий) в автономном режиме. Необходима только при установке функции Advanced logging	MSSQLSMSFW	Авто
Мониторинг производительности, сбор данных	Позволяет в фоновом режиме собирать данные о производительности брандмауэра ISA	Performance Logs and Alerts (Журналы и оповещения производительности)	Авто
Печать на удаленном компьютере	Разрешает печать с компьютера ISA Server (не рекомендуется отправлять задания на печать с брандмауэра ISA)	Workstation (Рабочая станция)	Авто
Удаленное управление Windows	Разрешает удаленное управление сервером Windows (не требуется для удаленного управления программным обеспечением брандмауэра ISA)	Server (Сервер)	Авто
Удаленное управление Windows	Разрешает удаленное управление сервером Windows (не требуется для удаленного управления программным обеспечением брандмауэра ISA)	Remote Registry (Удаленный реестр)	Авто
Синхронизация	Разрешает брандмауэру ISA соединение с NTP-сервером для синхронизации часов. Точный ход часов важен для аудита событий и других протоколов защиты	Windows Time (Служба времени Windows)	Авто
Удаленный помощник	Разрешает использовать функцию удаленной справки на этом компьютере (не рекомендуется запускать сеанс удаленной справки с брандмауэра ISA) Позволяет использовать функцию удаленной справки на компьютере	Remote Desktop Help Session Manager (Диспетчер сеанса справки для удаленного рабочего стола)	Вручную
Удаленный помощник		Terminal Services (Службы терминалов)	Вручную

Роли клиента для брандмауэра ISA

Для сетевых служб, расположенных в защищенных и незащищенных сетях, брандмауэру ISA иногда приходится играть роль клиента сети, для этого необходимы службы клиента сети. В табл. 6.15 перечислены возможные роли клиента сети для брандмауэра ISA, описывается, когда это может потребоваться, и приводятся службы, которые должны быть включены для конкретной роли.

ПРИМЕЧАНИЕ При использовании в сети серверов WUS или SUS нужно также включить службы автоматического обновления.

Табл. 6.15. Необходимые службы для того, чтобы брандмауэр ISA выполнял различные роли клиентов

Роль клиента	Применение	Необходимые службы	**Тип** запуска
Клиент автоматического обновления	Эта роль назначается, чтобы разрешить автоматическое обнаружение и обновление с помощью службы обновления Microsoft Windows	Automatic Updates (Авто матичес кое обновление)	Авто
Клиент автоматического обновления	Эта роль назначается, чтобы разрешить автоматическое обнаружение и обновление с помощью службы обновления Microsoft Windows	Background Intelligent Transfer Service (Фоновая интеллектуальная служба передачи)	Вручную
Клиент DHCP	Эта роль назначается, если компьютер ISA Server автоматически получает IP-адрес от DHCP-сер вера	DHCP Client (DHCP-клиент)	Авто
Клиент DNS	Эта роль назначается, если компьютеру ISA Server нужно получать информацию о разрешении имен с других серверов	DNS Client (DNS-клиент)	Авто
Член домена	Эта роль назначается, если компьютер ISA Server является членом домена	Network location awareness (NLA) (Служба сетевого расположения)	Вручную
Член домена	Эта роль назначается, если компьютер ISA Server является членом домена	Net logon (Сетевой вход в систему)	Авто
Член домена	Эта роль назначается, если компьютер ISA Server является членом домена	Windows Time (Служба времени Windows)	Авто

(см. след. стр.)

Табл. 6.15. (окончание)

Роль клиента	Применение	Необходимые службы	Тип запуска
Динамическая регистрация DNS	Эта роль назначается, если компьютер ISA Server должен устанавливать соединение с другими клиентами Windows. Если эту роль не выбрать, то компьютер ISA Server не получит доступ к общим ресурсам на удаленных компьютерах; например для публикации отчетов	TCP/IP NetBIOS Helper (Модуль поддержки NetBIOS через TCP/IP)	Авто
Клиент сетей Microsoft	Эта роль назначается, если компьютер ISA Server должен устанавливать соединение с другими клиентами Windows. Если эту роль не выбрать, то компьютер ISA Server не получит доступ к общим ресурсам на удаленных компьютерах; например для публикации отчетов	Workstation (Рабочая станция)	Авто
Клиент WINS	Эта роль назначается, если компьютер ISA Server использует разрешение имен WINS	TCP/IP NetBIOS Helper (Модуль поддержки NetBIOS через TCP/IP)	Авто

Сконфигурировав службы для брандмауэра ISA, можно сохранить их конфигурацию в файле шаблона безопасности Windows (.inf). На сайте www.isaserver.org приведено несколько примеров шаблонов безопасности, предназначенных для наиболее распространенных сетевых моделей.

Административные роли и полномочия брандмауэра ISA

Не у всех администраторов брандмауэра должен быть одинаковый уровень контроля конфигурации и управления брандмауэром ISA. Брандмауэр ISA позволяет настроить три уровня контроля программного обеспечения брандмауэра в зависимости от роли, назначенной пользователю.

Административные роли брандмауэра ISA:

- ISA Server Basic Monitoring (базовый мониторинг ISA Server);
- ISA Server Extended Monitoring (расширенный мониторинг ISA Server);
- ISA Server Full Administrator (администратор ISA Server).

В табл. 6.16 приводится описание функций каждой из этих ролей.

Табл. **6.16.** Административные роли брандмауэра ISA

Роль	Описание
ISA Server Basic Monitoring	Пользователи и группы, которым назначена эта роль, могут выполнять мониторинг работы ISA Server и сети, но не могут настраивать функции мониторинга
ISA Server Extended Monitoring	Пользователи и группы, которым назначена эта роль, могут выполнять все типы мониторинга, включая конфигурирование журналов, оповещений и других функций, разрешенных для этой роли
ISA Server Full Administrator	Пользователи и группы, которым назначена эта роль, могут выполнять любые настройки на ISA Server, включая конфигурирование правил, применение сетевых шаблонов и мониторинг

Пользователи, которым назначены эти роли, могут быть созданы в подсистеме SAM (Security Account Manager, администратор учетных данных в системе защиты) брандмауэра ISA, или это могут быть пользователи домена, если брандмауэр ISA является членом домена Active Directory внутренней сети. Административные роли брандмауэра ISA могут быть назначены любым пользователям, для этого не нужны никакие особые права или полномочия. Единственным исключением является случай, когда пользователю нужно выполнять мониторинг счетчиков производительности ISA Server с помощью монитора производительности (PerfMon) или инструментальной панели ISA Server; в таком случае пользователь должен быть членом группы Performance Monitors User в Windows Server 2003.

Для каждой роли ISA Server имеется список разрешенных действий. В табл. 6.17 перечислены некоторые действия и административные роли, которым разрешено выполнять каждое из них. **Табл. 6.17.** Действия, разрешенные для различных административных ролей брандмауэра ISA

Действие	Полномочия Basic Monitoring	Полномочия Extended Monitoring	Полномочия Full Administrator
Просмотр инструментальной панели, связи, сеансов и служб	X	X	X
Квитирование оповещений	X	X	X
Просмотр информации в журналах		X	X
Создание определений оповещений		X	X
Создание отчетов		X	X
Остановка и запуск сеансов и служб		X	X
Просмотр политики брандмауэра		X	X
Конфигурирование политики брандмауэра			X
Конфигурирование кэша			X
Конфигурирование VPN			X

ПРЕДУПРЕЖДЕНИЕ Пользователи с полномочиями Extended Monitoring (расширенное наблюдение) могут экспортировать и импортировать любую информацию о конфигурации, включая секретную. Это означает, что потенциально они могут расшифровать секретную информацию.

Для того чтобы назначить административные роли, выполните следующие действия:

1. Нажмите кнопку **Start** (Пуск), установите курсор на **All** Programs (Все программы), установите курсор на **Microsoft ISA Server** и щелкните мышью **ISA Server Management.**
2. Щелкните имя сервера в левой панели консоли управления **Microsoft Internet Security and Acceleration Server 2004.** Щелкните **Define Administrative Roles** (Определить административные роли) на вкладке **Tasks** (Задачи).
3. На странице **Welcome to the ISA Server Administration Delegation Wizard** (Вас приветствует мастер делегирования административных полномочий ISA Server) нажмите кнопку **Next** (Далее).
4. На странице **Delegate Control** (Делегировать контроль) нажмите кнопку **Add** (Добавить).
5. В диалоговом окне **Group (recommended) or User** (Группа (рекомендуется) или пользователь) введите имя группы или пользователя, которому будут предоставлены административные полномочия. Щелкните мышью стрелку вниз в выпадающем списке **Role** (Роль) и выберите соответствующую административную роль. Нажмите кнопку OK.
6. Нажмите кнопку **Next** (Далее) на странице **Delegate Control** (Делегировать контроль).
7. Нажмите кнопку **Finish** (Готово) на странице **Completing the Administration Delegation Wizard** (Завершение работы мастера делегирования административных полномочий).
8. Нажмите кнопку **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра.
9. Нажмите кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Режим блокировки

В брандмауэре ISA имеется новая функция, которая позволяет отключить службы брандмауэра, чтобы защитить брандмауэр и все защищенные сети в случае, если брандмауэр ISA был атакован.

Режим блокировки активируется:

- когда атака или другое событие в сети или на локальном хосте вызовет выключение службы брандмауэра, например из-за ошибки или ситуации, когда пользователь намеренно настраивает оповещения и действия при оповещении так, что

служба брандмауэра выключается в ответ на событие, которое спровоцировало это оповещение;

- когда служба брандмауэра выключается вручную. Также можно выключить службу брандмауэра для эффективной реакции на атаку в случае, когда в процессе конфигурирования брандмауэра ISA и сети становится известно о готовящейся атаке.

Функциональность брандмауэра в режиме блокировки

При переходе в режим блокировки брандмауэр ISA сохраняет следующие функции:

1. Механизм пакетной фильтрации (Packet Filter Engine) брандмауэра ISA (fweng) применяет политику режима блокировки брандмауэра.
2. Правила политики брандмауэра разрешают исходящий трафик из сети локального хоста ко всем сетям (если они так настроены). Если устанавливается исходящее соединение, то это соединение может использоваться для ответа на входящий трафик. Например, DNS-ответ на DNS-запрос может быть принят по одному соединению. Это не означает, что режим блокировки разрешает расширить существующую политику для исходящего доступа из сети локального хоста. Допустимы только существующие правила, разрешающие исходящий доступ из сети локального хоста.
3. Новые первичные соединения с самим брандмауэром ISA разрешаются только в том случае, когда включено правило системной политики, которое разрешает именно такой трафик. Исключением является DHCP-трафик, который разрешен всегда. DHCP-запросы (на порт UDP 67) разрешены из сети локального хоста во все сети, а DHCP-ответы (на порт UDP 68) разрешены в обратном направлении.
4. VPN-клиенты удаленного доступа не смогут устанавливать соединение с брандмауэром ISA. VPN-соединения "узел-в-узел» также будут запрещены.
5. Любые изменения в конфигурации сети в режиме блокировки применяются только после перезапуска службы брандмауэра и выходе из режима блокировки брандмауэра ISA.
6. ISA Server не будет инициировать никаких оповещений.

Ограничения соединений

Брандмауэр ISA вводит ограничение на количество соединений, выполняемых с брандмауэром или через него в любой момент времени. Ограничение количества соединений позволяет брандмауэру ISA блокировать соединения через брандмауэр для клиентов, которые могут быть заражены червями, пытающимися установить большое количество соединений через брандмауэр ISA. В качестве примера таких червей можно привести черви массовой рассылки и червь Blaster.

В правилах Web-публикации можно настроить ограничение общего количества соединений, указав максимальное количество одновременных соединений в свойствах Web-приемника. Когда будет достигнуто максимальное количество соедине-

ний, настроенное для Web-приемника, любые новые запросы от клиентов будут отвергаться.

Можно ввести ограничение общего количества UDP, ICMP **и** других Raw IP сеансов в секунду, разрешенных правилом публикации серверов или правилом доступа. Эти ограничения не относятся к TCP-соединениям. Когда будет превышено определенное количество соединений, новые **соединения** не будут устанавливаться, а существующие соединения не будут разрываться.

Начать нужно с настройки нижних порогов количества соединений. Это позволит брандмауэру ISA запретить злоумышленникам расходовать ресурсы компьютера ISA Server.

По умолчанию количество не TCP-соединений настроено на 1000 соединений в секунду на одно правило и 160 соединений на один клиент.

Ограничение для TCP-соеди нений начинается со 160 соединений на один клиент.

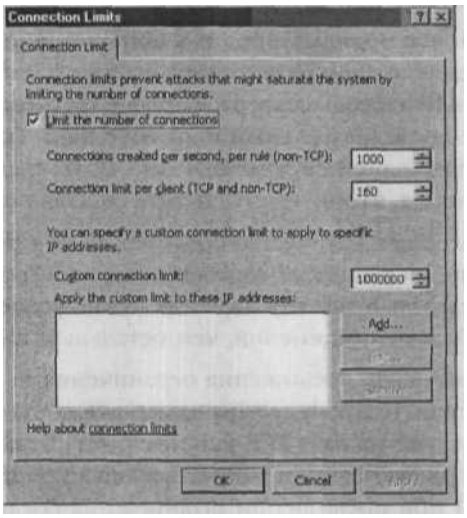
Это значение следует изменить в том случае, если становится заметно, что блокируются соединения с легальных хостов из-за слишком низкого значения порога. Определить, что хост заблокирован, потому что он превысил свой лимит соединений, можно по соответствующему оповещению. В оповещении указывается IP-адрес хоста, превышающего разрешенное количество соединений.

Для того чтобы настроить ограничение количества соединений, выполните следующие действия:

1. Нажмите кнопку **Start** (Пуск), установите курсор на **All Programs** (Программы), установите курсор на **Microsoft ISA Server** и щелкните мышью **ISA Server Management.**
2. Разверните имя сервера в левой панели консоли управления **Microsoft Internet Security and Acceleration Server 2004** и разверните узел **Configuration** (Кон фигурация). Щелкните мышью узел **General** (Общие).
3. Щелкните мышью **Define Connection Limits** (Определить ограничение коли чества соединений) на панели **Details** (Подробности).
4. На вкладке **Connection Limit** (Ограничение количества соединений) (рис. 6.32) установите флажок в поле **Limit the number of connections** (Ограничит!) ко личество соединений). Затем можно настроить количество соединений в секунду и поле **Connections created per second** (Количество соединений, устанавли ваемых в секунду), на одно правило (для не TCP-соединений) в поле **Connections created per rule (non-TCP)** (Количество соединений не по протоколу TCP, ус танавливаемых на одно правило) и на клиента (для TCP- и не TCP-соединений) в поле **Connections limit per client (TCP and non-TCP)** (Ограничение коли чества соединений на одного клиента по протоколу TCP и по другим протоко лам). Для некоторых компьютеров нужно разрешить превышение этих значе ний, например для сильно загруженных печатных серверов. В этом случае можно щелкнуть **Add** (Добавить) и выбрать **Computer Set** (Подмножество компьюте-

Рис. 6.32. Диалоговое окно Connection Limits (Ограничение количества соединений)

ров), чтобы применить значение **Customer connection limit** (Пользовательское ограничение количества соединений).



После того как указанное количество соединений превышено, новые соединения устанавливаться не будут. Однако существующие соединения также не будут разорваны. На одно правило и в секунду по умолчанию разрешено до 1000 новых соединений. Когда это значение по умолчанию превышено, создается оповещение.

Когда превышается это значение, создается запись в журнале:

- предпринятое действие: **Connection Denied** (Соединение запрещено);
- код: **FWXERULE_QUOTA_EXCEEDED_DROPPED.**

Для предотвращения атак переполнения следует ограничить количество соединений, устанавливаемых хостами. Во время атаки переполнения UDP или IP многие запросы отправляются с ложных (spoofed) исходных адресов, что может стать причиной отказа в обслуживании.

Когда ограничение превышено, попытайтесь сделать следующее:

- если атакующий трафик исходит из сети, защищенной брандмауэром ISA, это может означать, что некий хост в защищенной сети заражен вирусом или чер вем. Нужно сразу же отключить этот компьютер от сети;
- если атакующий трафик исходит из небольшого диапазона IP-адресов внешней сети, то следует создать правило, запрещающее доступ для подмножества ком пьютеров, включающих эти исходные IP-адреса;
- если трафик исходит с большого диапазона IP-адресов, оцените общее состоя ние сети. Рассмотрите возможность установки меньшего значения для ограни чения соединений, так чтобы брандмауэр ISA мог обеспечить лучшую защиту сети.

Если предел был превышен в результате большого объема трафика, попробуйте установить большее значение для количества соединений на одно правило исходя из требований конкретной сети.

При создании цепочек брандмауэров и в конфигурациях брандмауэра ISA с последовательным подключением нужно задать настраиваемые ограничения количества соединений для IP-адресов сервера, входящего в цепочку, или брандмауэра ISA в конфигурации с последовательным подключением. Также, если во внешней сети опубликовано более одной службы UDP или IP, то следует установить меньшее значение ограничения, чтобы защитить сеть от атак переполнения.

Можно ограничить общее количество соединений по протоколам UDP, ICMP и Raw IP на один клиент. Для разных IP-адресов можно настроить конкретные ограничения. Это можно сделать в том случае, когда нужно разрешить некоторым серверам устанавливать больше соединений, чем остальным клиентам.

Для TCP-соединений после превышения ограничения не разрешается устанавливать новые соединения. Поэтому нужно назначить достаточно большие зиачения ограничений для служб на базе TCP, например SMTP, так чтобы SMTP-сернеры могли отправлять исходящую почту и получать входящую почту. Для других соединений (Raw IP и UDP) при превышении ограничения соединений более ранние соединения разрываются для того, чтобы можно было создать новые.

Предотвращение атак имитации соединения на DHCP

Некоторые администраторы брандмауэров предпочитают использовать DHCP-сервер на внешнем интерфейсе брандмауэра ISA, чтобы он мог получать информацию об IP-адресах с DHCP-сервера компании по кабельному или DSL-соединению. Но если внешний интерфейс настроен на использование DHCP для получения информации об IP-адресах, то при получении IP-адреса на внешнем интерфейсе могут возникнуть проблемы. Чаще всего их причиной является механизм предотвращения атак имитации соединения (spoofing attack) на DHCP.

Чтобы решить эту проблему, важно понимать принцип работы этого механизма. Для каждого адаптера, на котором включена служба DHCP, на брандмауэре ISA имеется список разрешенных адресов. Вот как выглядит раздел реестра для каждого включенного адаптера с DHCP:

```
HKLM\SYSTEM\Cu r rentCont rolSet\Se r vices\Fweng\Pa rameters\DhcpAdapte rs\<Adapte r' s
MAC>/<Adapter's  hardware type>
```

Значения параметров в разделе реестра (рис 6.33) следующие:

1. Имя адаптера.
2. Сетевое имя адаптера на брандмауэре ISA.
3. MAC-адрес адаптера.

4. Сетевой адрес ISA Server.
5. Тип аппаратного обеспечения адаптера.

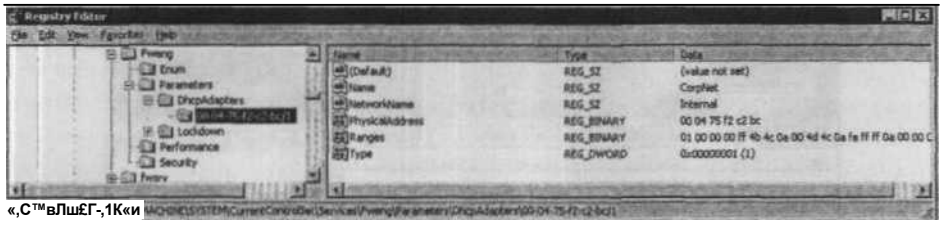


Рис. 6.33. Раздел реестра для предотвращения атак на DHCP

Когда драйвер брандмауэра ISA видит сообщение-приглашение от DHCP, он проверяет достоверность этого сообщения следующим образом:

1. Используя поля DHCP «Client Ethernet Address» (Ethernet-адрес клиента) и «Hard ware Type» (тип устройства), драйвер находит соответствующий раздел реестра для этого адаптера.
2. Если такого раздела реестра нет, то пакет пропускается (так происходит в на чале установки программного обеспечения брандмауэра ISA).
3. Драйвер проверяет, содержится ли в поле «Your IP-Address» (IP-адрес) в DHCP-приглашении IP-адрес из диапазона адресов, отведенных в сети для адаптера (со гласно записи в реестре).
4. Если проверка не была успешной, то пакет отбрасывается, а на брандмауэре ISA создается оповещение.

На рис. 6.34 показан пример пакета DHCP-приглашения (соответствующие поля отмечены).

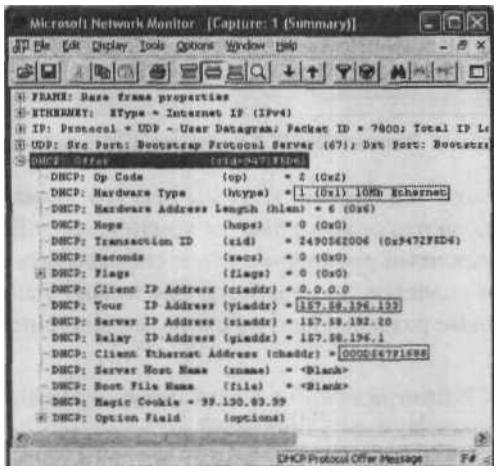


Рис. 6.34. Запись монитора сети о пакете DHCP-приглашения

Информация, содержащаяся в оповещении, показана на рис. 6.35.

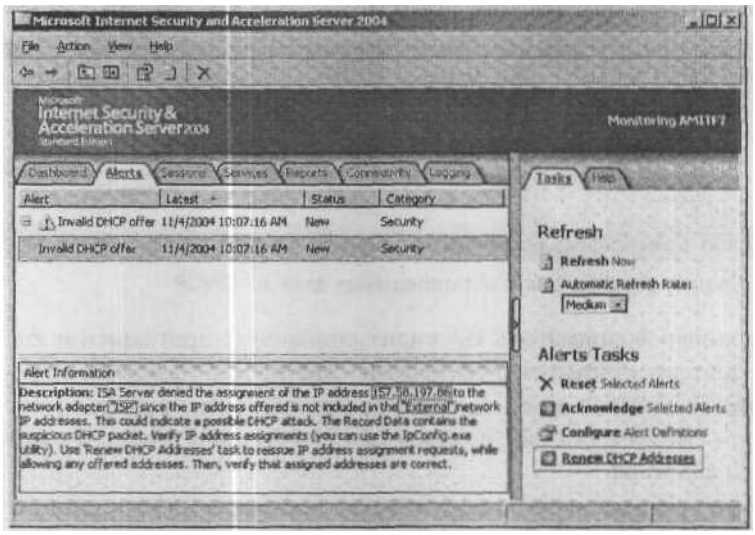


Рис. 6.35. Оповещение о недостоверном DHCP-приглашении

Если сетевой адаптер все же должен принять предлагаемый адрес, то администратору следует использовать параметр «Renew DHCP addresses» (обновить адреса DHCP) на панели задач консоли брандмауэра ISA. На рис. *6.36* показано диалоговое окно с предупреждением, появляющимся, если щелкнуть **Renew DHCP Addresses** (Обновить адреса DHCP) на панели задач.

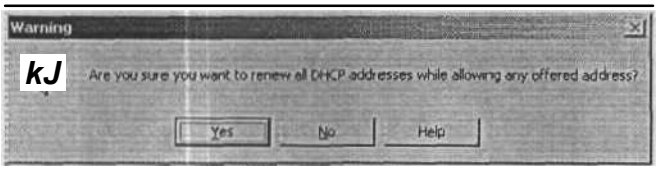


Рис. 6.36. Предупреждение Renew DHCP Addresses (Обновить адреса DHCP)

После нажатия кнопки **Yes** (Да) все разделы реестра, связанные с предотвращением атак на DHCP, удаляются, и выполняется команда ipconfig /renew. Это означает, что в этот период времени драйвер не будет отбрасывать никакие адреса приглашений (потому что разделов реестра нет). Как только у адаптеров появятся адреса, будут созданы новые разделы реестра с новыми значениями, и этот механизм будет запущен вновь.

Отбрасывание DHCP-приглашений в целях предотвращения атак на DHCP может происходить в следующих ситуациях:

1. Если имеются два DHCP-адаптера, которые поменялись ролями. Например, адап тер, ранее подключенный к внутренней сети, теперь подключен к внешней сети, и наоборот.
2. DHCP-адаптер был перенесен в другую сеть. Например, внешний сетевой адап тер брандмауэра ISA имел соединение с домашней сетью, в которой другой маршрутизатор осуществлял соединение с интернет-провайдером (и Интерне том), а теперь этот маршрутизатор пытаются заменить на внешний сетевой адаптер брандмауэра ISA для соединения с интернет-провайдером.

В таких случаях нужно использовать задачу Renew DHCP Addresses (обновить адреса DHCP), чтобы разрешить назначение адресов DHCP. Это нужно делать лишь один раз. Эта процедура необходима только при изменении положения DHCP-адаптера, при котором он становится членом другого элемента сети брандмауэра ISA.

Резюме

В этой главе было рассмотрено много вопросов, связанных с планированием и установкой брандмауэра ISA. Также обсуждалась стандартная системная политика и конфигурация брандмауэра после завершения установки. Описание конфигурации для быстрого старта, приведенное в этой главе, позволяет быстро приступить к работе с брандмауэром ISA.

Краткое резюме по разделам

Задачи и анализ действий перед установкой брандмауэра ISA

0 Наиболее важным параметром при оценке ресурсов сервера, на котором будет установлен брандмауэр ISA, является скорость интернет-соединений.

И Перед установкой брандмауэра ISA должна быть правильно настроена таблица маршрутизации.

0 Расщепленная инфраструктура DNS обеспечивает наилучшее и наиболее прозрачное разрешение имен для всех организаций, которым нужен удаленный доступ к корпоративным ресурсам.

0 Правильная настройка DNS на сетевых интерфейсах брандмауэра ISA является важным фактором, позволяющим оптимизировать скорость и точность доступа в Интернет.

0 При определении требований к памяти и объему жесткого диска для аппаратного обеспечения брандмауэра ISA нужно учесть, будет ли использоваться прямое и обратное кэширование.

0 Запись журналов в базы данных MSDE и в файлы производится на самом брандмауэре ISA. Для этого нужно отвести достаточное пространство на диске.

Установка брандмауэра ISA «с нуля» на компьютере с несколькими сетевыми адаптерами

0 Если на сервере с брандмауэром ISA будет работать средство просмотра SMTP-сообщений, то перед установкой брандмауэра ISA на этом компьютере следует установить службу IIS SMTP.

0 Внутренняя сеть определяется как сеть, основные сетевые службы которой используются брандмауэром ISA, например Active Directory, DNS, DHCP и службы сертификации.

Ш Если включено шифрование для клиента брандмауэра, то поддерживаются только компьютеры с установленной версией клиента брандмауэра ISA 2004.

0 Если на компьютере уже была установлена любая версия брандмауэра ISA, то после установки брандмауэра ISA его не нужно перезапускать.

Стандартная конфигурация брандмауэра ISA после установки

И Стандартное правило доступа (правило по умолчанию) блокирует весь трафик, проходящий через брандмауэр ISA, и является единственным правилом доступа, которое включается программой установки.

0 Стандартное сетевое правило (правило по умолчанию) между внутренней сетью и Интернетом устанавливается на NAT.

0 После установки Web-кэширование отключено по умолчанию. Его можно включить, создав диск для кэширования.

0 Публикация информации об автоматическом обнаружении отключена по умолчанию.

Установка обновления брандмауэра ISA

0 Многие функции, входящие в ISA Server 2000, не вошли в ISA Server 2004. Это может осложнить процесс обновления и перехода с одной версии на другую.

0 Можно обновлять только подобные версии ISA Server: ISA Server 2000 Standard Edition обновляется до ISA Server 2004 Standard Edition, а ISA Server 2000 Enterprise Edition — до ISA Server 2004 Enterprise Edition.

Установка брандмауэра ISA на компьютере с одним сетевым адаптером

0 В конфигурации с одним сетевым адаптером большая часть функциональности брандмауэра ISA утрачивается.

0 Конфигурация брандмауэра ISA с одним сетевым адаптером напоминает Proxy Server 2.0.

0 При установке в режиме с одним сетевым адаптером брандмауэр ISA может обеспечить собственную защиту и защиту соединений по протоколам HTTP, HTTPS и FTP.

0 В режиме с одной сетевой картой не поддерживаются клиенты брандмауэра и SecureNAT.

Конфигурация брандмауэра ISA для быстрого старта

0 Приведенная в этой главе конфигурация для быстрого старта позволяет быстро установить и настроить брандмауэр ISA в режиме с двумя сетевыми интерфейсными картами и быстро установить соединение с Интернетом.

0 Конфигурация для быстрого старта не является оптимальной для брандмауэра ISA. Ее нужно рассматривать как базовую конфигурацию, которой следует пользоваться до тех пор, пока не станет понятен принцип работы брандмауэра ISA.

Улучшение базовой конфигурации брандмауэра ISA и базовой операционной системы

И Безопасность базовой операционной системы можно усилить, отключив службы, которые не нужны для брандмауэра ISA.

В Некоторые службы нужно включить, чтобы обеспечить нормальное функционирование брандмауэра ISA.

И Административные роли брандмауэра ISA, назначаемые пользователям и группам, обеспечивают доступ к конфигурации брандмауэра и компонентам управления.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма ***«Ask* the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Не удается создать правило доступа, разрешающее соединения из внутренней сети во внешние сети на брандмауэре ISA с одним сетевым интерфейсом. Почему?

О: Для брандмауэра ISA с одним сетевым интерфейсом не существует внешней сети. Это объясняется тем, что все IP-адреса в адресном диапазоне IPv4 (за исключением адресов на идентификаторе сети локального хоста) считаются частью внутренней сети по умолчанию. Если нужно создать правило доступа от хостов корпоративной сети к другим хостам, эти хосты должны быть расположены во внутренней сети. Рекомендуется использовать брандмауэр ISA в режиме с несколькими сетевыми интерфейсами так, чтобы он мог обеспечить полнофункциональную защиту сетей.

В: Нужно ли устанавливать DNS- и DHCP-сервер на брандмауэре ISA? О: Нет. На брандмауэре ISA не нужно устанавливать DNS-сервер или DHCP-сервер. В этой главе описывается образец конфигурации сети, в которой брандмауэр

ISA выступал в роли DNS- и DHCP-сервера. Эта конфигурация позволяла брандмауэру ISA имитировать функциональность нескольких простых брандмауэров с фильтрацией пакетов, предназначенных для малого бизнеса. Однако если в корпоративной сети уже есть DNS- или DHCP-сервер, то не нужно устанавливать эти серверы на брандмауэре ISA.

В: Попытки перехода с конфигурации ISA Server 2000 на ISA Server 2004 оказались безуспешны. Почему?

О: Существует ряд причин, по которым процесс перехода с одной версии на другую может не быть успешным. Чаще всего это происходит при местном обновлении. Рекомендуется создать копию настроек ISA Server 2000, а затем дублировать эти настройки на вновь установленном брандмауэре ISA. Однако если производится местное обновление или нужно перейти с одной версии на дру!ую с помощью специального инструмента ISA, то следует ознакомиться с принципами перехода и с тем, какие функции поддерживаются при переходе с ISA Server 2000 на ISA Server 2004, в справочной системе ISA Server 2004.

В: Что могут делать клиенты сети, когда брандмауэр находится в режиме блокировки? Смогут ли хакеры напасть на сеть или на брандмауэр, когда он находится в режиме блокировки?

О: Хакеры не смогут атаковать сеть, когда брандмауэр находится в режиме блокировки. Во время блокировки через брандмауэр ISA не устанавливаются новые соединения. Но и существующие соединения не **будут** разорваны. Брандмауэр ISA переходит в режим блокировки, когда службы брандмауэра выходят из строя. Режим блокировки является примером того, как брандмауэр ISA блокируется при сбое.

В: Нужно ли использовать расщепленную инфраструктуру DNS? (Уже имеется домен самого высокого уровня .local).

О: Использовать расщепленную инфраструктуру DNS совсем не обязательно, не она может сильно облегчить жизнь пользователям, перемещающимся между корпоративной сетью и удаленными рабочими местами. Применение расщепленной инфраструктуры DNS упрощается, если имя внутреннего домена также доступно с внешних узлов, однако это не жесткое требование. Например, если внутренний домен называется domain.local, то можно создать общий домен с именем domain.com. Затем создается ресурс, записанный в домене domain.com, который соответствует ресурсам, используемым удаленными пользователями для доступа к внутренним ресурсам с помощью правил Web-публикации и публикации серверов на брандмауэре ISA. И внешние, *и* внутренние пользователи получают доступ к ресурсам, используя одно и то же имя, например owa.domain, com, но внешняя зона DNS будет разрешать имя в общий адрес на брандмауэре ISA, который используется для публикации сайта, а для внутренней зоны имя owa.domain.com будет разрешаться в реальный внутренний адрес OWA-сайта в корпоративной сети.

В: В корпоративной сети имеется несколько идентификаторов сети. Нужно ли создавать отдельную сеть для каждого из них?

О: Нет. Помните, что все IP-адреса, расположенные за одной сетевой интерфейсной картой, являются частью одной и той же сети брандмауэра ISA. Например, если за одним интерфейсом на брандмауэре ISA имеется пять идентификаторов сети, то брандмауэр ISA рассматривает все эти идентификаторы как часть одной сети. Можно создать объекты подсетей или объекты подмножеств адресов, чтобы сгруппировать идентификаторы сети, если нужно контролировать доступ на брандмауэре ISA на основании этих идентификаторов сети.

Глава

Создание и применение политики доступа в брандмауэре ISA Server 2004

Основные темы главы:

- **Элементы правил доступа брандмауэра ISA**
- **Конфигурирование правил доступа для исходящих соединений через брандмауэр ISA**
- **Использование сценариев для заполнения наборов имен доменов**
- **Создание и конфигурирование трехадаптернои сети DMZ с общедоступными адресами**
- **Разрешение в ну три доменных соединений через брандмауэр ISA**

Введение

Политика доступа брандмауэра ISA (известная так же как политика брандмауэра) включает правила публикации Web-сервера (Web Publishing Rules), правила публикации сервера (Server Publishing Rules) и правила доступа (Access Rules). Правила публикации Web-сервера и обычного сервера используются для предоставления входящего доступа (inbound access), а правила доступа применяются для управления исходящим доступом (outbound access).

Концепции входящего и исходящего доступа в новом брандмауэре ISA более запутаны по сравнению с интерпретацией этих понятий в ISA Server 2000. Это объясняется тем, что ISA Server 2000 базировался на таблице локальных адресов (Local Address Table, LAT) и определения входящего и исходящего доступа были связаны с этой таблицей. Входящий доступ определялся как входящие соединения хоста, не имеющего таблицы локальных адресов, с хостами (внешними и внутренними) на базе LAT. У нового брандмауэра ISA нет таблицы локальных адресов и не существует концепции «внутренней» сети, подобной внутренней сети в ISA Server 2000, определяемой таблицей локальных адресов.

Вообще правила публикации Web-севеpов и обычных серверов следует применять, если необходимо разрешить соединения хоста, не входящего в сеть, защищенную брандмауэром ISA, с хостом, размещенным в сети, защищенной брандмауэром ISA. Правила доступа применяются для управления соединениями между любыми двумя сетями. Существует единственное ограничение — нельзя создать правила доступа для управления соединением между сетями, использующими средства преобразования сетевых адресов (Network Address Translation, NAT), если инициирующий связь хост находится в узле сетевого соединения, не применяющего NAT.

Предположим, что имеется связь с преобразованием сетевых адресов между стандартной внутренней сетью (internal network) и Интернетом. Можно создать правила доступа, которые управляют соединением между внутренней сетью и Интернетом, потому что инициирующие связь хосты находятся на стороне, использующей преобразование сетевых адресов. Но невозможно сформировать правило доступа для соединения и н тер нет-хоста и внутренней сети, поскольку интернет-хосты находятся на стороне соединения, не применяющего средства NAT.

Если определен маршрут между сетью-источником информации, или исходной сетью, и сетью-адресатом информации, можно создать правила доступа, действующие в *обоих* направлениях. Допустим, что определен маршрут между сегментом DMZ и Интернетом. В этом случае можно создать управляемый правилами доступа трафик между сегментом DMZ и Интернетом и сформировать правила доступа, которые управляют этим трафиком.

Главная задача брандмауэра ISA — контроль трафика между сетью-источником информации и сет ью-адреса том. Политика доступа (Access Policy) брандмауэра ISA

позволяет клиентам сети-и сточ ника получить доступ к хостам сети-адресата информации, а правила доступа можно сконфигурировать для блокировки соединений хостов исходной сети с хостами сети-адресата. Политика доступа определяет способ доступа хостов к хостам других сетей.

Ключевая идея — исходные и конечные хосты должны принадлежать разным сетям. Брандмауэр ISA никогда не должен быть связующим звеном в соединениях хостов одной и той же сети ISA. Такой тип конфигурации называется «петлей (looping back) через брандмауэр ISA». Никогда не следует создавать подобные петли через брандмауэр ISA для доступа к ресурсам одной и той же сети.

Когда брандмауэр ISA перехватывает запрос на исходящее соединение, он проверяет как сетевые правила, так и правила политики брандмауэра для того, чтобы определить, разрешен ли доступ. Первыми проверяются сетевые правила. Если нет сетевого правила, определяющего преобразование сетевых адресов (NAT) или маршрут между сетью-источником и сетью-адресатом, попытка соединения окажется безуспешной. Это обычная причина неудавшихся соединений, и именно ее следует искать, когда политика доступа приводит к неожиданным результатам.

Правила доступа можно сконфигурировать для определенного исходного или конечного хостов. Клиенты могут быть заданы IP-адресом (например, используя сетевые объекты компьютера или набора компьютеров) или именем пользователя. Брандмауэр ISA обрабатывает запросы по-разному, в зависимости от типа клиента, запрашивающего объект, и варианта настройки правил доступа.

Когда брандмауэр ISA получает запрос на соединение, он, прежде всего, проверяет наличие сетевого правила, определяющего маршрут между сетью-источником информации и сетью-адресатом. Если такого сетевого правила нет, брандмауэр ISA предполагает, что сеть-источник и сеть-адресат *не соединены*. При наличии правила, определяющего маршрут между ними, брандмауэр ISA обрабатывает правила политики доступа.

После того, как брандмауэр ISA подтвердил соединение сети-источника и сети-адресата, рассматривается политика доступа. Брандмауэр ISA обрабатывает правила доступа в политике доступа сверху вниз (системная политика реализуется до выполнения политики доступа, определенной пользователем).

Если с запросом исходящего соединения связано разрешающее правило (Allow rule), брандмауэр ISA разрешит выполнение запроса. Для выполнения разрешающего правила необходимо, чтобы характеристики соединения в запросе соответствовали характеристикам, определенным в правиле доступа. Правило доступа соответствует запросу на соединение, если в правиле доступа следующие параметры совместимы с параметрами запроса на соединение:

- протокол;
- от кого (местонахождение источника, включающее номер порта источника);
- расписание или время работы;

- кому (местонахождение адресата, включающее адреса, имена, URL-адреса и другие сетевые объекты);
- пользователи;
- группы содержимого (content groups).

Если каждый из перечисленных параметров совместим с одноименным параметром запроса на соединение, то к соединению применяется правило доступа. Если запрос на соединение не соответствует параметрам в правиле доступа, брандмауэр ISA переходит к рассмотрению следующего правила в политике доступа брандмауэра.

ПРЕДУПРЕЖДЕНИЕ Если не задана системная политика или определенные пользователем правила доступа, предназначенные для запроса на соединение, то применяется последнее правило по умолчанию (Last Default rule). Это правило блокирует все коммуникации через брандмауэр ISA.

Если правило доступа соответствует параметрам запроса на соединение, то брандмауэр снова проверяет сетевые правила, чтобы выяснить, не применяются ли NAT-средства или не определен ли маршрут между сетью-источником и сетью-адресатом. Брандмауэр ISA для определения способа обслуживания запроса также проверяет наличие правил построения цепочек связывания в Web (Web chaining rules) (если клиент Web-прокси запросил объект) или возможную конфигурацию связывания (если клиент SecureNAT (безопасное преобразование сетевых адресов) или клиент брандмауэра затребовали объект).

СОВЕТ Правила построения цепочек связывания в Web и построение цепочек связывания брандмауэра представляют методы маршрутизации брандмауэра ISA. Правила построения Web-цепочек можно сконфигурировать для направления запросов от клиентов Web-прокси к определенным узлам, таким как предшествующие брандмауэру на пути следования запросов (upstream) Web-прокси серверы. Построение цепочек брандмауэра позволяет запросы от клиентов SecureNAT и брандмауэра отправлять на предшествующие на пути следования запросов (upstream) брандмауэры ISA. Построение и Web-цепочек связывания, и связующих цепочек брандмауэра дает возможность брандмауэру ISA обойти конфигурацию по умолчанию его шлюза для определенных запросов на соединение от клиентов Web-прокси и клиентов брандмауэра.

Например, имеется брандмауэр ISA с двумя сетевыми картами (network interface card, NIC): одна из них соединена с Интернетом, а другая — с внутренней сетью. Создано единственное правило доступа «All Open» (Все открыто), которое разрешает всем пользователям доступ с помощью любых протоколов к любым интернет-сайтам.

Такая политика включала бы следующие правила для брандмауэра ISA:

- сетевое правило, определяющее маршрут между сетью-источником (внутренняя сеть) и сетью-адресатом (Интернетом);
- правило доступа, позволяющее внутренним клиентам доступ ко всем сайтам в любое время и с помощью любого протокола.

Конфигурация по умолчанию использует средства преобразования сетевых адресов (NAT) между внутренней сетью, установленной по умолчанию, и Интернетом. Однако по желанию можно использовать определение маршрута для связи внутренней сети (или любой другой сети) с Интернетом (пока у вас есть общедоступные или открытые адреса — public addresses — в сети).

Элементы правил доступа брандмауэра ISA

Правила доступа конструируются с помощью элементов политики (Policy Elements). Одно из основных улучшений в новом брандмауэре ISA по сравнению с ISA Server 2000 — возможность создания элементов политики «на лету». Это означает, что можно сформировать все элементы политики в мастере создания нового правила доступа (New Access Rule Wizard). Он существенно усовершенствован по сравнению с мастером в ISA Server 2000, в котором нужно заранее спланировать элементы политики, а затем, *после* конфигурирования элементов, создать правила для протоколов и правила публикации.

В брандмауэр ISA включены следующие элементы политики:

- протоколы;
- наборы пользователей;
- типы содержимого;
- расписания или часы работы;
- сетевые объекты.

Протоколы

В состав брандмауэра ISA входит ряд встроенных протоколов, которые можно использовать для создания правил доступа, правил публикации Web-серверов и правил публикации серверов.

Помимо встроенных протоколов можно создать собственные протоколы, используя мастер создания новых протоколов (New Protocol Wizard) брандмауэра ISA. Заготовленные заранее, встроенные протоколы нельзя модифицировать или удалить. Но можно редактировать и удалять созданные протоколы. Существует несколько протоколов, которые устанавливаются вместе с прикладными фильтрами, их нельзя модифицировать, но можно удалить. Существует возможность устранить связь прикладных фильтров с этими протоколами. Например, если нежелательно пересылать Web-запросы для клиентов SecureNAT и клиентов брандмауэра на фильтр Web-про-

кси, то можно удалить связь протокола HTTP с фильтром Web-прокси. Позже в этой главе мы рассмотрим эту задачу более подробно.

При создании определения нового протокола нужно задать следующую информацию.

- **Тип протокола** Протокол TCP (Transmission Control Protocol, протокол управления передачей), UDP (User Data Protocol, пользовательский протокол данных), ICMP (Internet Control Message Protocol, протокол управляющих сообщений в сети Internet) или протокол IP-уровня (Internet protocol, интернет-протокол или протокол сетевого уровня). Если задается ICMP-протокол, необходимо включить тип ICMP и код. Имейте в виду, что нельзя создавать публикации в сети с помощью протоколов ICMP и **IP-уровня.**
- **Направление** Для протокола UDP включаются элементы Send, Receive, Send Receive или Receive Send. Для протокола TCP — элементы Inbound и Outbound. Для протоколов ICMP и IP-уровня — элементы Send и Receive.
- **Диапазон портов** (для протоколов TCP и UDP) Это диапазон портов от 1 до 65535, который применяется для начального соединения. Протоколы ICM? и IP-уровня не используют порты, так как порты — элемент заголовка транспортного уровня.
- **Номер протокола** (для протоколов IP-уровня) Например, GRE (Generic Routing Encapsulation, Обобщенная инкапсуляция маршрутизации) использует IP-протокол **с** номером 47.
- **Свойства ICMP** (для протоколов ICMP) К ним относятся код ICMP и тип.
- **Вторичные соединения** (необязательные) Диапазон портов, типы протоколов и направление, применяемые для вторичных соединений или пакетов, следующих за исходным (первичным) соединением. Можно конфигурировать одно или несколько вторичных соединений. Вторичные соединения могут быть входящими (inbound), исходящими (outbound) или одновременно входящими и исходящими.

ПРИМЕЧАНИЕ Нельзя определять вторичные соединения для первичных (primary) протоколов IP-уровня.

Наборы пользователей

Для управления исходящим доступом можно создать правила доступа и применить их к конкретным IP-адресам (Internet Protocol addresses) или определенным пользователям или группам пользователей. Когда правила доступа применяются к пользователям или группам, **пользователи** должны подтвердить подлинность с помощью протокола аутентификации (authentication protocol). Клиент брандмауэра всегда использует интегрированную аутентификацию и всегда отправляет незаметно для пользователя его верительные данные — имя и пароль (credentials). Клиент Web-прокси может применять ряд разных методов подтверждения подлинности или аутентификации.

Брандмауэр ISA позволяет группировать пользователей и группы пользователей в наборы пользователей (User Set), которые, нам кажется, лучше называть «группами брандмауэра». Наборы пользователей включают один или несколько пользователей или группы пользователей с любой схемой аутентификации, поддерживаемой брандмауэром ISA. Например, набор пользователей может содержать пользователь Windows, пользователь из пространства имен RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного пользователя) и еще один пользователь из пространства имен SecurlD (Система двухфакторной аутентификации). ОС Windows и пространства имен RADIUS и SecurlD используют разные схемы подтверждения подлинности, но все их пользователи могут включаться в один набор пользователей.

Брандмауэр ISA поставляется со следующими заранее сконфигурированными наборами пользователей.

- **Все подтвердившие свою подлинность пользователи** (All Authenticated Users) Этот предопределенный набор содержит все подтвердившие подлинность пользователи, независимо от избранного метода аутентификации. Правило до ступа, использующее этот набор, применяется ко всем подтвердившим под линность пользователям. При этом соединения от клиентов SecureNAT будут заканчиваться неудачей. За исключением случая, когда клиент SecureNAT одно временно является и VPN-клиентом (Virtual Private Network, виртуальная част ная сеть). Когда пользователь создает VPN-соединение с брандмауэром ISA, VPN-клиент автоматически становится клиентом SecureNAT. Хотя обычно клиент SecureNAT не может посылать имя и пароль брандмауэру ISA, когда он одновре менно становится VPN-клиентом, регистрационные данные VPN могут приме няться для подтверждения подлинности пользователя.
- **Все** пользователи (ЛИ Users) Этот предопределенный набор пользователей представляет всех пользователей, как подтвердивших подлинность, так и не сделавших этого, и никаких имен и паролей не требуется для доступа к прави лу, использующему этот набор пользователей. Но клиент брандмауэра всегда должен посылать имя и пароль брандмауэру ISA, даже если не требуется аутен тификации. Подтверждение этому можно найти на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер 2004 защищенного быстрого доступа к сети Интернет) — на вкладке Sessions (Сеансы связи) ря дом с именем пользователя стоит вопросительный знак.
- **Системный и сетевой сервис** (System and Network Service) Этот заранее под готовленный пользовательский набор представляет локальный системный и сетевой сервисы на машине брандмауэра ISA. Он применяется в некоторых правилах системной политики.

Типы содержимого

Типы содержимого задают типы MIME (Multipurpose Internet Mail Extensions, многоцелевые расширения электронной почты в сети Интернет) электронной корреспонденции и расширения файлов. При создании правила доступа для протокола HTTP можно ограничить типы содержимого, к которым оно будет применяться. Контроль типа содержимого позволяет очень детально конфигурировать политику доступа, поскольку можно управлять доступом, основываясь не только на протоколах и адресатах, но и на конкретном содержимом.

Управление типом содержимого возможно только для HTTP-трафика и туннельного (tunneled) FTP-трафика. Управление и контроль типа содержимого не работают для FTP-трафика, не обработанного фильтром Web-прокси брандмауэра ISA.

Когда на хосте, принадлежащем сети, защищенной брандмауэром ISA, создается FTP-запрос, брандмауэр ISA проверяет расширение файла в запросе. Затем он определяет, применяется ли правило к типу содержимого, включающему запрашиваемое расширение файла, и обрабатывает правило соответствующим образом. Если тип содержимого не соответствует правилу, правило игнорируется и выполняется проверка следующего правила политики доступа.

Когда хост сети, защищенной брандмауэром ISA, создает исходящий HTTP-запрос, брандмауэр ISA посылает запрос на Web-сервер через фильтр Web-прокси (по умолчанию). При возврате Web-сервером запрошенного Web-объекта брандмауэр ISA проверяет MIME-тип объекта (который находится в данных заголовка HTTP) или его расширение файла (в зависимости от информации в заголовке, который возвращается Web-сервером). Брандмауэр ISA определяет, применяется ли правило к заданному типу содержимого, включая расширение файла, и обрабатывает правило соответствующим образом.

Брандмауэр ISA поставляется с предопределенным встроенным списком типов содержимого, которые можно использовать. Можно также создать собственные типы содержимого, задавая как MIME-тип, так и расширение файла.

Например, для включения всех файлов программного пакета Director в тип содержимого, выберите следующие расширения файлов и MIME-типы:

- .dir;
- .dxr;
- *ЛСТ*;
- application/x-director.

При задании MIME-типа можно использовать звездочку (*) как символ-маску. Например, для включения всех типов приложений введите **application/*.**

> СОВЕТ Символ-маску можно применять только для MIME-типов. *Нельзя* использовать символ-маску при задании расширений файлов. Он применяется только в заключительной части задания MIME-типа после слэша (/).

Брандмауэр ISA поставляется *со* следующими предопределенными типами содержимого:

- Application (Приложение);
- Application data files (Файлы данных приложения);
- Audio (Аудио-файлы);
- Compressed files (Сжатые файлы);
- Documents (Документы);
- HTML documents (HTML-документы);
- Images (Изображения);
- Macro documents (Макродокументы);
- Text (Текст);
- Video (Видео);
- VRML (Virtual Reality Modeling Language, язык моделирования виртуальной ре альности).

Управление доступом с помощью MIME-типа может быть сложной задачей, поскольку разные MIME-типы связаны с различными расширениями имен файлов. Причина заключается в том, что Web-сервер контролирует MIME-тип, связанный с Web-объектом, который возвращается пользователю. Несмотря на то, что существует общее соглашение о способах определения MIME-типов, администратор Web-сайта полностью управляет MIME-типом, связывая его с любым содержимым, поддерживаемым его Web-сервером. Поэтому иногда видно, что содержимое, которое считается заблокированным с помощью типов содержимого, на самом деле не заблокировано. Можно определить MIME-тип, используемый Web-сервером, возвращая ответ на запрос с помощью трассировки или отслеживания, выполненного службой Network Monitor (Сетевой монитор). HTTP-за головок покажет возвращенный Web-сервером MIME-тип для Web-содержимого, запрошенного клиентом.

В табл. 7.1. приведены связи, принятые по умолчанию в информационном сервисе Интернета (Internet Information Services, IIS). Их можно использовать для справки.

Табл. 7.1. Принятые по умолчанию в IIS MIME-типы для общепринятых расширений файлов

Расширение имени файла	MIME-тип
.hta	Application/hta
.isp	Application/x-internet-sign
.crd	Application/x-mscardfile
.pmc	Application/x-perfmon
.spc	Application/x-pkcs7-certific
,sv4crc	Application/x-sv4crc
.bin	Application/octet-stream
.cl$_p$	Application/x-msclip
.nrny	Application/x-msmoney
.clp	Application/x-msclip
,mny	Applica tion/x-msmoney

Расширение имени файла	**MIME-тип**
.hta	Application/hta
.isp	Application/x-internet-signu
.crd	Application/x-mscardfile
.pmc	Application/x-perfmon
яре	Application/x-pkcs7-certifica
,sv4crc	Application/x-sv4crc
.bin	Application/octet-stream

(см. след. стр.)

Табл. 7.1. (продолжение)

Расширение имени файла	MIME-тип
.P7r	Application/x-pkcs7-certreqresp
.evy	Application/envoy
,P7s	Applica tion/pkcs7-signa ture
.eps	Application/postscript
.setreg	Application/set-registration-initiation
,xlm	Application/vnd.ms-excel
.cpio	Application/x-cpio
.dvi	Application/x-dvi
.p7b	Application/x-pkcs7-certificates
.doc	Applica tion/msword
.dot	Application/msword
,P7c	Applica tion/pkcs7-mime
.pa	Applica tion/postscript
.wps	Applica tion/vnd.ms-works
.csh	Applica tion/x -csh
ifl	Application/x-iphone
.pmw	Application/x-perfmon
.man	Application/x-troff-man
.hdf	Application/x-hdf
.mvb	Application/x-msmediaview
.texi	Applica tio n /x-texinfo
.setpay	Applica tion/set-payment-ini tiation
.stl	Application/vndms-pkistl
.mdb	Applicat ion/x-msaccess
,oda	Applica tion/oda
.hip	Applica tion/winhlp
,nc	Appl ication/x-netcdf
,sh	Application/x-sh
.shar	Applica tion/x-shar
.tcl	Applica tion/x- tcl
,ms	Applica tion/x-troff-ms
ods	Application/oleobject
.axs	Application/olescript
.xla	Application/vnd.ms- exce l
,mpp	Application/vnd.ms-project
.dir	Applica tion/x-director
.sit	Application/x-stuffit

Табл. 7.1. (продолжение)

Расширение имени файла	MIME-тип
•	Application/octet-stream
.crl	Application /pkix -crl
.al	Appl ica tion/postscript
JCIS	Application/vnd.ms-excel
.*wks*	Appl ication/vnd.ms-works
.ins	Application/x-internct-signup
pub	Application/x-mspublisher
.wri	Application/x-mswrite
.spl	Application/futuresplash
.hqx	Application/mac- bi nhex40
.plO	Application/pkes 10
JttlC	Applica tion/vnd.ms-excel
.xlt	Application/vnd.ms-excel
.dxr	Application/x-director
■is	Application/x-javascript
,ml3	Appl ica t ion/x-msmediaview
.trm	Application/x-msterminal
.pml	Application/x-perfmon
.me	Application/x-troff-me
.won	Application/vnd.ms- works
.latex	Application/x-latex
,ml4	Appl icat ion/x-msmedia view
.wmf	Application/x-msmetafile
,cer	Applica t ion/x-x 5 09-ca-cert
.zip	Application/x-zip-compressed
,pl2	Application/x-pkcs12
.pfx	Application/x-pkcs12
.der	Applica tion/x-x 509-ca-cert
.pdf	Application/pdf
.xlw	Application/vnd.ms-excel
.texinfo	Application/x-texinfo
.p7m	Applicat ion/pkcs7 -mime
•PPS	Application/vnd.ms-powerpoint
.dcr	Application/x-director
gtar	Application/x-gtar
so.	**text/scriptlet**
tit	Application/fractals

(см. след. стр.)

Табл. 7.1. (продолжение)

Расширение имени файла	MIME-тип
.cxe	Application/octet-stream
№	Application/vnd.ms-powerpoint
m	Application /vnd ms - pk icert s tore
.pko	Application/vndms-pkipko
.scd	Application/x-msschedule
.tar	Application/x-tar
.roff	Application/x-troff
.t	Application/x-troff
prf	Application/pics-rules
.rtf	Applica tion/rtf
.pot	Application/vnd.ms-powerpoint
.wdb	Application/vnd.ms-works
.bcpio	Application/x-bcpio
.dll	Application/x-msdownload
.pma	Application/x-perfmon
.pmr	Application/x-perfmon
и	Application/x-troff
.src	Application/x-wais-source
.acx	Application/internet-property-stream
.cat	Application/vndms-pkiseccat
	Application/x-cdf
tgz	Application/x-compressed
,sv4cpio	Application/x-sv4cpio
.tex	Application/x-tex
.ustar	Application/x-ustar
.crt	Application /x -x 5 09- ca -cert
X*	audio/x-pn-realaudio
.mid	audio /mid
.au	audio/basic
snd	audio/basic
.wav	audio/wav
.alfc	audio/aiff
,m3u	audio/x-mpegurl
.ram	audio/x-pn-reala udio
яла	audio/a iff
.rmi	audio/mid
,alf	audio/x-aiff

Табл. 7.1. (окончание)

Расширение имени файла	MIME-тип
тр3	audio /m peg
•gz	Appl i c a tio n /x -gz ip
z	Appl i c a tio n/x - c ompre ss
.isv	tex t /t a b-s epara ted - va lu es
.xml	text/xml
.323	text/h323
.htt	tex t /we bv iewht ml
.stm	text/html
.html	text/html
.xsl	text/xml
.htm	text/html
.cod	image/cis-cod
(cf	image/ief
.pbm	image/x-portable-bitmap
as	image/tiff
.ppm	image/x-portable-pixmap
rgb	image/x-rgb
.dib	image/bmp
-Ipeg	image/jpeg
,crax	image/x-cmx
.pnm	image/x-portable-anymap
■lpe	image/jpeg
.jfif	image/pjpeg
.tif	image/tiff
-]P8	image/jpeg
.xbm	image/x-xbitmap
.ras	image/x-cmu-raster
•gif	image/gif

Часы работы или расписание

Можно задать расписание (Schedule), управляющее временем применения правила. Имеются три встроенных расписания:

- **Work Hours** (Рабочие часы) разрешает доступ в период с 09:00 утра до 17:00, начиная с понедельника и заканчивая пятницей (для данного правила);
- **Weekends** (Выходные дни) разрешает доступ в любое время в субботу и вос кресенье (для данного правила);

- **Always** (Всегда) разрешает доступ в любое время (для данного правилг).

Обратите внимание на то, что правила могут быть разрешающими и запрещающими. Расписания применяются ко всем правилам доступа, а не только к разрешающим правилам.

ПРЕДУПРЕЖДЕНИЕ Расписания управляют только новыми соединениями, применяющими правило доступа. На уже установленные соединения расписания не влияют. Например, если задано расписание доступа Work Hours (Рабочие часы) для сайта партнера, пользователи не будут отключены после 17:00. Необходимо будет вручную отключить их или написать сценарий рестарта службы брандмауэра.

Сетевые объекты

Сетевые объекты применяются для контроля над источниками и адресатами соединений, проходящих через брандмауэр ISA. Мы обсуждали эти элементы политики в главе 4.

Конфигурирование правил доступа для исходящих соединений через брандмауэр ISA

К исходящим соединениям всегда применяются правила доступа. Только протоколы с первичным соединением в исходящем направлении или направлении отправки можно использовать в правилах доступа. Правила публикации Web-серверов и правила публикации серверов, наоборот, всегда применяют протоколы с первичным соединением во входящем направлении или направлении получения (receive). Правила доступа управляют доступом от источника к адресату с помощью исходящих протоколов.

В этом разделе мы подробно рассмотрим процесс создания правила доступа и каждый из его параметров, доступных в мастере создания нового правила **(New Access Rule Wizard),** наряду с дополнительными характеристиками из команды Properties, относящейся к правилу доступа.

Для начала откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004,** раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач и ссылку **Create New Access Rule** (Создать новое правило доступа). На экране появится страница с заголовком **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа). Введите имя правила в текстовое поле ввода **Access Rule name** (Имя правила доступа). В этом примере мы создадим правило доступа «All Open (Все открыто)», пропускающее весь трафик хостов внутренней сети (Internal Network),

установленной по умолчанию, в выбранную по умолчанию внешнюю сеть (External Network). Щелкните мышью по кнопке **Next** (Далее).

ПРЕДУПРЕЖДЕНИЕ Мы создаем правило «All Open» (Все открыто) в этом примере только как демонстрационное, служащее для первоначального тестирования брандмауэра. После того как вы убедитесь, что ваш брандмауэр ISA успешно соединяет вас с Интернетом, следует заблокировать правило «All Open (Все открыто)» и создать правила доступа, соответствующие вашей политике использования сети. Управление исходящим доступом так же важно для состояния общей безопасности, как и управление входящим доступом. Действительно, мощный контроль над исходящим доступом, основанный на пользователях/группах, — одна из функциональных возможностей, которая отличает брандмауэр ISA от любых других брандмауэров, представленных на рынке.

Страница Rule Action

На странице **Rule Action** (Действие правила) есть два варианта: **Allow** (Разрешить) или **Deny** (Запретить). В отличие от ISA Server 2000 в новом брандмауэре ISA вариант **Deny** (Запретить) установлен по умолчанию. В нашем примере мы выберем вариант **Allow** (Разрешить) и щелкнем мышью кнопку **Next** (Далее), как показано на рис. 7.1.

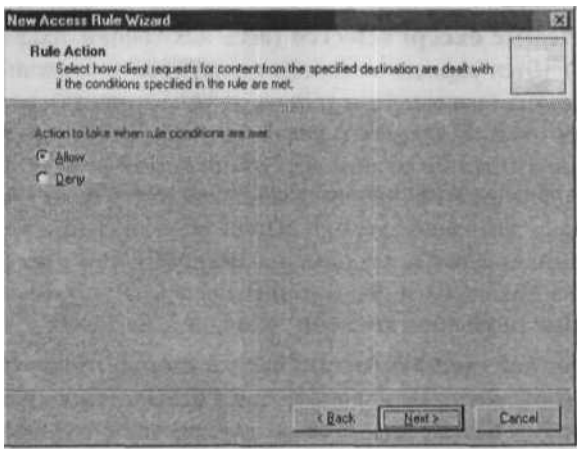


Рис. 7.1. Страница Rule Action (Действие правила)

Страница Protocols

На странице **Protocols** (Протоколы) выбираются протоколы, которые следует разрешить для исходящего соединения сети-источника с адресатом. В списке **This rule applies to** (Это правило применяется к) есть три возможных варианта.

- **All outbound traffic** (весь исходящий трафик) Этот вариант разрешает исполь зовать все протоколы для исходящего доступа. Результат применения этого ва рианта зависит от типа клиента, использующего данное правило для доступа. Для клиентов брандмауэра такой выбор разрешает исходящий доступ с помо щью всех протоколов, включая дополнительные, или вторичные (secondary), протоколы, определенные в брандмауэре ISA, и некоторые не определенные. Если же клиент SecureNAT пытается соединиться с помощью правила, использующе го этот вариант, исходящий доступ будет разрешен только для протоколов, вклю ченных в список брандмауэра **ISA Protocols** (Протоколы). Если клиент SecureNAT не может подключиться к ресурсу, когда используется данный протокол, попро буйте создать новое определение протокола (Protocol Definition) в брандмауэ ре ISA для поддержки соединения клиента SecureNAT. Когда требуются вторич ные соединения, например в случае с FTP-соединением, следует применить кли ент брандмауэра или создать прикладной фильтр (application filter), обеспечи вающий поддержку этого протокола для клиентов SecureNAT.
- **Selected protocols** (выбранные протоколы) Этот вариант позволит выбрать конкретные протоколы, к которым применяется данное правило. Можно выб рать из списка протоколов по умолчанию, включенного в брандмауэр ISA и го тового к использованию, или создать новое определение протокола (Protocol Definition) «на лету». Для одного правила можно выбрать один или несколько протоколов.
- **All outbound traffic except selected** (весь исходящий трафик за исключени ем выбранных) Этот вариант позволит сделать все протоколы доступными для исходящего доступа (зависящими только от типа клиента), *за исключением* оп ределенных протоколов для исходящего доступа. Например, можно разрешить клиентам брандмауэра исходящий доступ посредством всех протоколов за ис ключением тех, которые необходимо явно запретить из-за корпоративной по литики безопасности, такие как AOL Instant Messenger (протокол мгновенного обмена сообщениями службы Америка онлайн), MSN Messenger (протокол службы сообщений сети Microsoft) и IRC (Internet Relay Chat, протокол общения в Ин тернете в режиме реального времени) (см. рис. 7.2).

Выделите строку **Selected Protocols** (Выбранные протоколы) и щелкните мышью кнопку **Add** (Добавить). На экране появится диалоговое окно **Add Protocols** (Добавить протоколы). В этом диалоговом окне вы увидите список папок, в которых сгруппированы протоколы в зависимости от основной сферы их применения. Например, папка **Common Protocols** (Общие протоколы) содержит протоколы, которые обычно применяются для подключения к Интернету, а в папке **Mail Protocols** (Почтовые протоколы) собраны протоколы, которые, как правило, используются для доступа через брандмауэр ISA к сервисам электронной почты. Папка **User-Defined** (Определенные пользователем) включает все персональные протоколы, созданные пользователем вручную в брандмауэре ISA. Папка **All Protocols** (Все про-

токолы) содержит все протоколы, как встроенные, так и определенные пользователем, включенные в конфигурацию брандмауэра ISA.

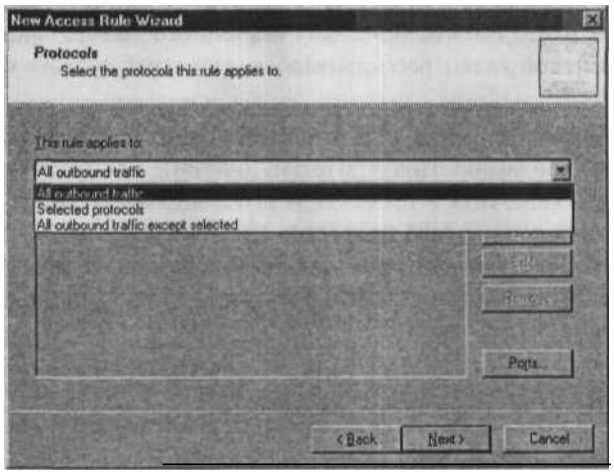


Рис. 7.2. Страница Protocols (Протоколы)

После щелчка кнопкой мыши папки All Protocols (Все протоколы) появятся все протоколы, сконфигурированные в брандмауэре ISA. Брандмауэр ISA поставляется с определениями ста протоколов, которые можно использовать в правилах доступа, как показано на рис. 7.3.

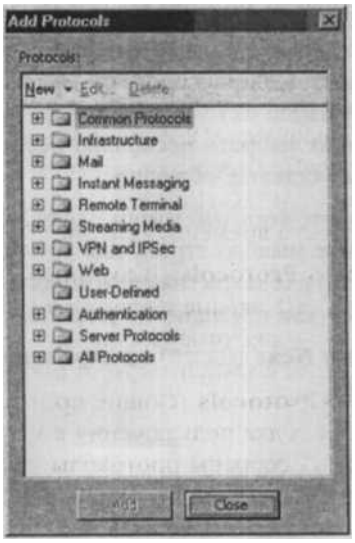


Рис. 7.3. Диалоговое окно Add Protocols (Добавить протоколы)

Если нужно использовать протокол, определения которого еще нет, можно создать новое определение, щелкнув кнопкой мыши пункт меню **New** (Новое). Выбор этого пункта меню позволит создать **Protocol** (Протокол) или **RPC Protocol** (Remote Procedure Call Protocol, протокол удаленного вызова процедуры). В предыдущих разделах этой главы рассказывалось о том, как создать новые определения протоколов.

После определения протокола, который необходимо включить в правило, дважды щелкните его кнопкой мыши. Повторите это действие для других протоколов, которые необходимо включить в правило, и затем щелкните мышью кнопку (Лове (Закрыть) диалогового окна **Add Protocols** (Добавить протоколы). В нашем примере мы хотим разрешить доступ для всех протоколов, поэтому щелкните мышью кнопку закрытия диалогового окна **Add Protocols** (Добавить протоколы).

На странице **Protocols** (Протоколы) выберите вариант **All outbound traffic** (Весь исходящий трафик) ш списка **This rule applies to** (Это правило применяется к) и щелкните мышью кнопку **Next** (Далее).

Страница Access Rule Sources

На странице **Access Rule Sources** (Источники в правиле доступа) выберите местонахождение источника информации, к которому следует применить правило доступа. Щелкните мышью кнопку **Add** (Добавить), чтобы вставить источник связи, к которому будет применяться данное правило.

В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) можно выбрать местонахождение источника информации для данного правила. Если в диалоговом окне не перечислены подходящие местонахождения источников, можно создать новый сетевой объект, щелкнув кнопкой мыши пункт меню **New** (Новый). Дважды щелкните кнопкой мыши источник, к которому нужно применить правило. Имейте в виду, что можно выбрать несколько источников информации двойным щелчком мыши разных сетевых объектов.

В нашем примере щелкните кнопкой мыши папку **Networks** (Сети), чтобы раскрыть ее, и дважды щелкните мышью строку для сети **Internal** (Внутренняя). Нажмите кнопку **Close** (Закрыть) для закрытия диалогового окна **Add Network Entities** (Добавить сетевые объекты), как показано на рис. 7.4.

Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).

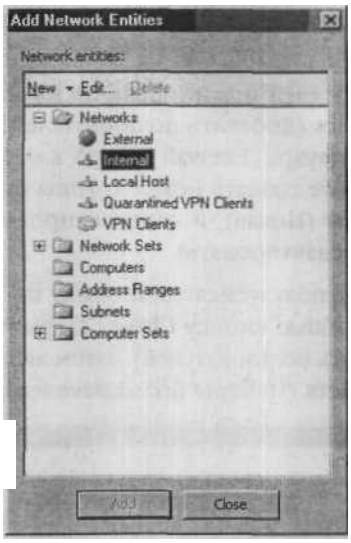


Рис. 7.4. Диалоговое окно **Add Network** Entities (Добавить сетевые объекты)

Страница Access Rule Destinations

На странице Access Rule Destinations (Адресаты в правиле доступа) выберите адресат информации, к которому нужно применить данное правило. Щелкните мышью кнопку Add (Добавить), чтобы добавить местонахождение адресата. На экране появится диалоговое окно Add Network Entities (Добавить сетевые объекты), в нем можно выбрать сетевой объект в качестве адресата информации, к которому будет применяться данное правило доступа. Как и на предыдущей странице мастера создания нового правила доступа, можно создать новый адресат, щелкнув кнопкой мыши пункт меню New (Новый) и указав новый объект.

В нашем примере мы щелкнем кнопкой мыши папку Networks (Сети), а далее двойным щелчком кнопки мыши выберем строку External (Внешняя). Щелкните мышью кнопку Close (Закрыть), чтобы закрыть диалоговое окно Add Network Entities (Добавить сетевые объекты). Затем щелкните мышью кнопку Next (Далее) на странице Access Rule Destinations (Адресаты в правиле доступа).

Страница User Sets

На странице User Sets (Наборы пользователей) можно задать пользователей, к которым применяется данное правило. Установка по умолчанию — набор All Users (Все пользователи). Если нужно удалить этот набор пользователей или любой другой из списка пользователей, к которым применяется данное правило, выберите набор пользователей и щелкните мышью кнопку Remove (Удалить). Можно также

отредактировать набор пользователей, приведенный в списке, щелкнув мышью кнопку **Edit** (Редактировать).

Добавить набор пользователей можно, щелкнув мышью кнопку **Add** (Добавить). В диалоговом окне **Add** Users (Добавить пользователей) нужно двойным щелчком мыши указать группу брандмауэра (Firewall Group), к которой требуется применить данное правило. Можно также создать новые группы брандмауэра, щелкнув кнопкой мыши пункт меню **New** (Новая), и отредактировать существующие группы, выбрав пункт меню **Edit** (Редактировать).

В нашем примере мы воспользуемся установкой по умолчанию **All Users** (Все пользователи). Щелкните мышью кнопку **Close** (Закрыть), чтобы закрыть диалоговое окно **Add Users** (Добавить пользователей). Затем щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователей), как показано на рис. 7.5.

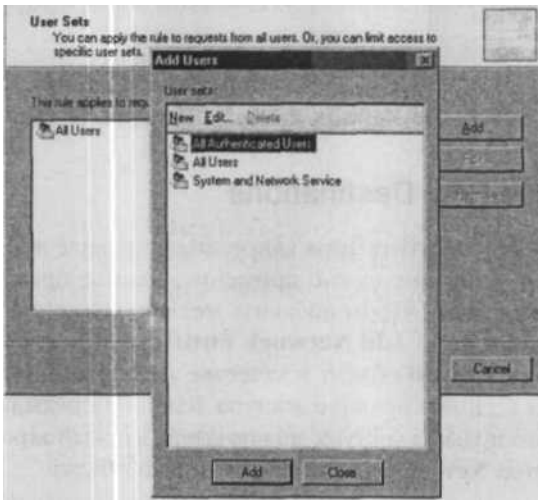


Рис. 7.5. Страница User Sets (Наборы пользователей)

Далее появляется страница **Completing the New** Access **Rule Wizard** (Завершение мастера создания нового правила). Проверьте сделанные установки и щелкните мышью кнопку **Finish** (Готово).

ПРИМЕЧАНИЕ Когда создается правило, разрешающее исходящий доступ для набора All Users (Все пользователи), разрешаются соединения через брандмауэр ISA, не требующие подтверждения подлинности. Правило, применяемое к набору All Users (Все пользователи), может использоваться клиентами SecureNAT. Если правило доступа требует аутентификации, попытка соединения клиента SecureNAT потерпит неудачу, так как клиент SecureNAT не может подтвердить подлинность.

Свойства правила доступа

Существует несколько параметров, не доступных в мастере создания нового правила доступа, которые можно установить в диалоговом окне **Properties** (Свойства) правила доступа.

Диалоговое окно **Properties** (Свойства) правила доступа содержит следующие вкладки:

- General (Общие);
- Action (Действие);
- Protocols (Протоколы);
- From (От кого);
- To (Кому);
- Users (Пользователи);
- Schedule (Расписание);
- Content Types (Типы содержимого).

Щелкните правило доступа правой кнопкой мыши и выберите команду **Properties** (Свойства).

Вкладка General

Первая открывшаяся вкладка — вкладка **General** (Общие). Можно изменить название правила доступа, введя новое название в текстовое поле ввода Name (Название). Правило можно сделать действующим или заблокировать, установив или сбросив флажок **Enable** (Разрешить).

Вкладка Action

Вкладка **Action** (Действие) предоставляет несколько параметров, не отображающихся в мастере создания нового правила. На этой вкладке представлены следующие параметры.

- **Allow** (Разрешить) Выберите этот вариант, если необходимо разрешить все соединения через брандмауэр ISA, характеристики которых совпадают с характеристиками данного правила доступа.
- Deny (Запретить) Выберите этот вариант, если необходимо запретить все соединения через брандмауэр ISA, характеристики которых совпадают с характеристиками данного правила доступа.
- **Redirect HTTP requests to this Web page** (перенаправлять HTTP-запросы на данную Web-страницу) Выберите этот вариант, если хотите все HTTP-запросы, соответствующие характеристикам данного правила доступа, перенаправлять на другую Web-страницу. Этот параметр доступен только для запрещающего правила (Deny). Когда пользователь пытается получить доступ к запрещенному сайту, запрос автоматически перенаправляется на Web-страницу, которая зада-

на в текстовом поле, расположенном под этим параметром. Убедитесь, что введен полный URL-адрес, на который необходимо перенаправить запрос пользователя, такой как http://corp.domain.com/accesspolicy.htm. **Log requests matching this rule** (записывать в журнал запросы, соответствующие данному правилу) Попытки соединений, соответствующих **правилу** доступа, автоматически рег истрируются после создания правила. Иногда не нужно регистрировать все соединения, соответствующие определенному правилу Например, когда создаются протоколы, соответствующие правилу, нет нужды отслеживать широковещательные оповещения NetBIOS. Позже в этой главе мы опишем процедуру, которую можно использовать для уменьшения размеров регистрационных журналов за счет создания правила доступа, которое не регистрирует соединения для широковещательной рассылки по протоколу NetBIOS (Network Basic Input Output System, сетевая базовая система ввода-вывода — NetBIOS broadcast protocols).

На рис. 7.6 показана вкладка **Action** (Действие).

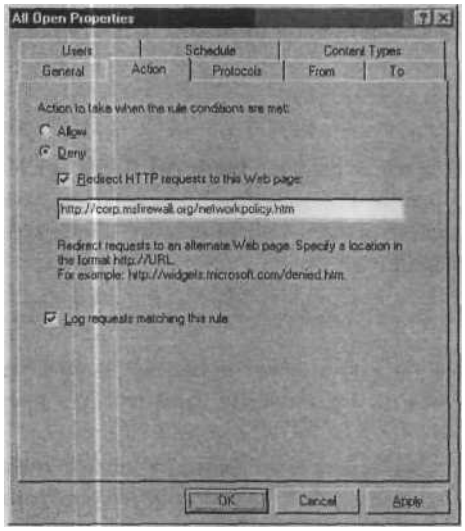


Рис. 7.6. Вкладка Action (Действие)

Вкладка Protocols

Вкладка **Protocols** (Протоколы) предлагает многие из параметров, доступных в мастере создания нового **правила** доступа. В списке **This rule applies to** (Данное правило применяется к) содержатся те же варианты: **Allow all outbound traffic** (Разрешить весь исходящий трафик), **Selected protocols** (Выбранные протоколы) и **All outbound traffic except selected** (Весь исходящий трафик за исключением выбранных). Можно использовать кнопку **Add** (Добавить) для вставки новых про-

токолов в список. Применяйте кнопку **Remove** (Удалить) для исключения протоколов, выбранных в списке **Protocols** (П ротоколы), и щелкните мышью по кнопке **Edit** (Редактировать) для корректировки протоколов, выбранных в списке **Protocols** (Протоколы).

ПРИМЕЧАНИЕ Можно редактировать только протоколы, определенные пользователем.

Существуют прикладные фильтры, которые можно **настраивать** для использования любых протоколов, включенных в список **Protocols** (Протоколы) на вкладке Protocols (Протоколы). Какие из фильтров будут доступны, определяется протоколами, содержащимися в списке. Щелкните мышью по кнопке **Filters** (Фильтры), чтобы увидеть фильтры, которые можно настроить, при существующем списке протоколов, включенных в правило доступа, как показано на рис. 7.7.

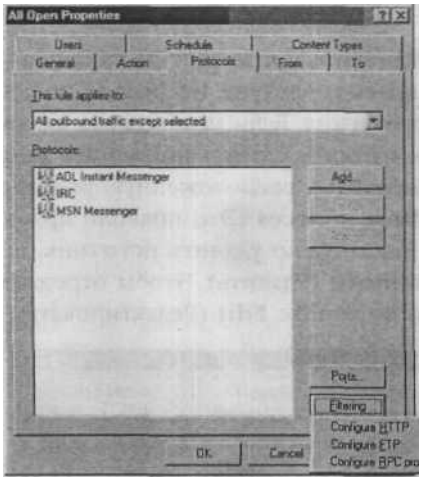


Рис. 7.7. Вкладка Protocols (Протоколы)

Имеется также возможность в каждом правиле доступа управлять портами источника информации, предоставляющими доступ к ресурсам через брандмауэр ISA. Щелкните мышью кнопку **Ports** (Порты), появится диалоговое окно **Source Ports** (Порты источника). *По* умолчанию выбран режим **Allow traffic from any allowed source port** (Разрешить трафик через любой разрешенный порт источника). Однако если есть приложения, в которых необходимо контролировать исходный порт, или такие, в которых применяются порты источника, установленные по умолчанию (например, протокол SMTP), можно ограничить порты, доступные для применения правила, выбрав режим **Limit access to traffic from this range of source ports** (Ограничить доступ к трафику заданным диапазоном портов источника), и ввести номера портов в поля **From** (От) и **To** (До), представляющие первый и последний порты в диапазоне портов источника, которым нужно разрешить доступ (см. рис. 7.8).

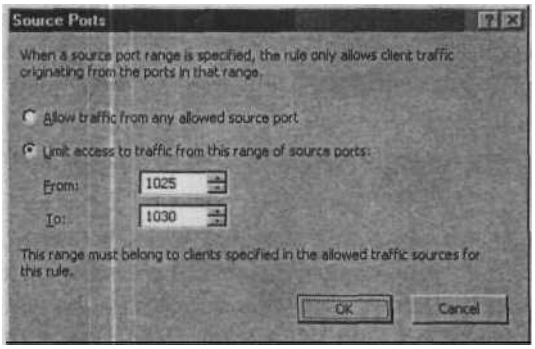


Рис. 7.8. Диалоговое окно Source **Ports** (Порты источника)

Вкладка From

На вкладке **From** (От) в основном представлены параметры, которые имеются в мастере создания нового правила доступа. Но режим, не доступный в мастере, — возможность создания исключения. Если необходимо включить дополнительные источники информации, к которым следует применить данное правило, щелкните мышью кнопку **Add** (Добавить), расположенную рядом со списком This rule applies **to traffic from** these sources (Это правило применяется к трафику из следующих источников). Если нужно удалить источник, щелкните мышью этот элемент, а затем кнопку Remove (Удалить). Чтобы отредактировать свойства источника, щелкните мышью по кнопке **Edit** (Редактировать).

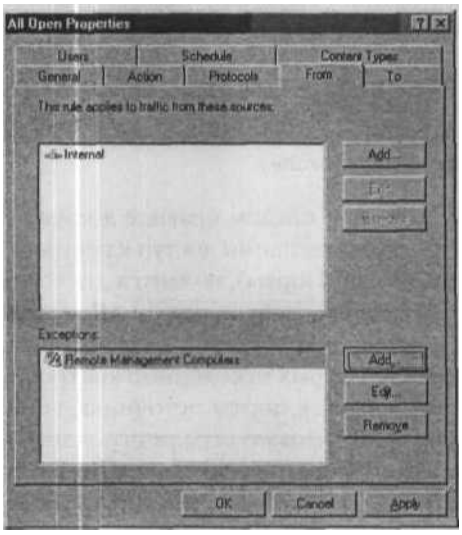


Рис. 7.9. Вкладка **From** (От)

Можно применять данное правило ко всем источникам информации, перечисленным в списке **This rule applies to traffic from these sources** (Это правило применяется к трафику из следующих источников) *за исключением* определенных местонахождений источников, которые задаются в списке **Exceptions** (Исключения). Предположим, что правило доступа запрещает всем компьютерам внутренней сети исходящий доступ по протоколу **PPTP** (Point-to-Point Tlinneling Protocol, сквозной туннельный протокол) для сети **VPN** (Virtual Private Network, виртуальная частная сеть). Но необходимо разрешить доступ по этому протоколу машинам, принадлежащим набору компьютеров **Remote Management Computers** (Удаленно управляемые компьютеры). Можно включить этот набор компьютеров в список **Exceptions** (Исключения), щелкнув мышью кнопку **Add** (Добавить). Пользуйтесь кнопками **Remove** (Удалить) и **Edit** (Редактировать) в списке **Exceptions** (Исключения) для удаления и редактирования источников, приведенных в этом списке, как показано на рис. 7.9.

Вкладка To

Вкладка To (Кому) предоставляет те же функциональные возможности, что и страница **Access Rule Destination** (Адресаты в правиле доступа) мастера создания нового правила доступа. Однако имеется дополнительная возможность задать исключения для адресатов информации, включенных в список **This rule applies to traffic sent to these destinations** (Данное правило применяется к трафику, отправленному следующим адресатам).

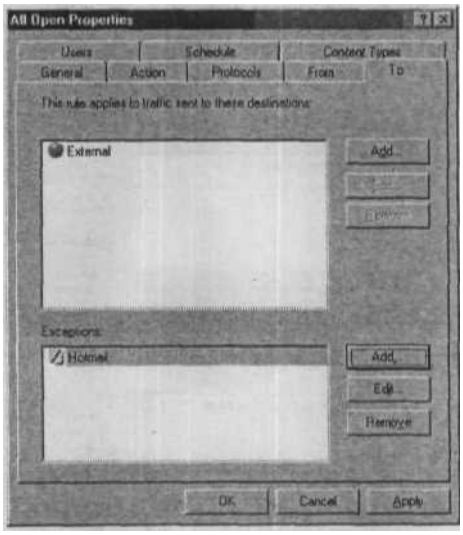


Рис. 7.10. Вкладка To (Кому)

Предположим, что создается правило доступа, разрешающее исходящий доступ ко всем сайтам **External** (Внешние). Однако необходимо не разрешать пользователям посещать почтовый Web-сайт Hotmail. Можно создать набор имен доменов (Domain Name Set) для доменов, необходимых для доступа к Hotmail, и затем использовать кнопку **Add** (Добавить) в разделе **Exceptions** (Исключения) для вставки набора имен доменов Hotmail. После этого правило будет разрешать доступ по протоколу HTTP ко всем сайтам за исключением сайта Hotmail (см. рис. 7.10).

Вкладка Users

Вкладка **Users** (Пользователи) позволяет добавлять группы брандмауэра, к которым необходимо применить правило доступа, как показано на рис. **7.11.** Кроме того, есть возможность добавить исключения к группе, для которой действует правило. Например, можно установить правило, применяемое к группе **All Authenticated Users** (Все подтвердившие свою подлинность пользователи), но исключить другие группы брандмауэра, такие как встроенная группа **System and Network Service** (Системный и сетевой сервис).

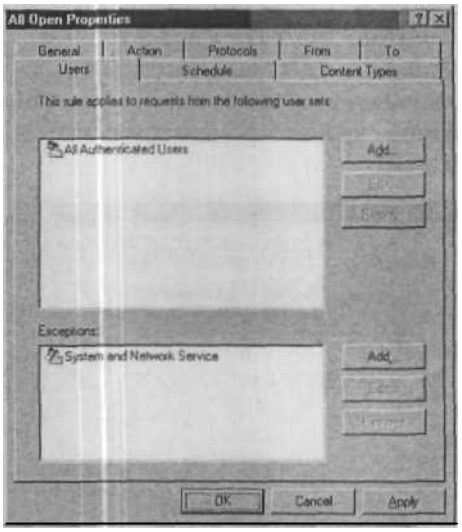


Рис. 7.11. Вкладка Users (Пользователи)

Вкладка Schedule

На вкладке **Schedule** (Расписание) задается период времени, в течение которого будет применяться правило. Интерфейс мастера создания нового правила (New Access Rule Wizard) не предоставляет параметры для определения расписания. Можно воспользоваться одним из трех встроенных **расписаний: Always** (Всегда), **Weekends**

(В выходные дни) или **Work hours** (В рабочие часы), или создать новое расписание, щелкнув мышью по кнопке New (Новое), как показано на рис. 7.12.

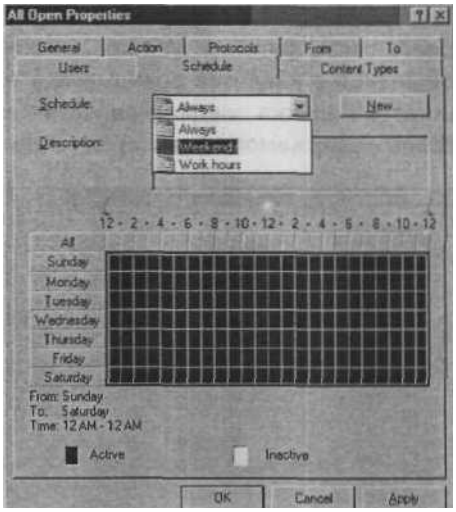


Рис. 7.12. Вкладка Schedule (Расписание)

ПРЕДУПРЕЖДЕНИЕ После задания расписания правило будет применяться только к новым соединениям, соответствующим характеристикам правила. Действующие соединения, к которым применяется данное правило, не будут разорваны. Эта ситуация подобна установке **Logon Hours** (Часы регистрации) в службе каталогов Active Directory. Придется ждать, пока пользователи отсоединятся или их сеансы связи превысят допустимое время, либо необходимо завершить сеансы связи вручную на консоли управления **Microsoft Internet Security and Acceleration Server 2004** или с помощью сценария.

Вкладка Content Types

Еще один элемент политики, не представленный в мастере создания нового правила (New Access Rule Wizard), — возможность контроля типа содержимого во время соединения. На вкладке **Content Types** (Типы содержимого) вы можете задать типы содержимого, используемые в правиле. Ограничения типов содержимого применяются только к HTTP-соединениям, все остальные протоколы игнорируют установки, сделанные на вкладке **Content Types** (Типы содержимого).

Установка по умолчанию — применять правило к **All content types** (Все типы содержимого). Вы можете ограничить типы содержимого, к которым применяется правило, выбрав параметр **Selected content types** (with this option selected, the rule is applicable only HTTP traffic) (Выбранные типы содержимого (если выбран этот

параметр, правило применяется только к HTTP-трафику) и установив флажки, расположенные рядом с типами содержимого, к которым вы хотите применять данное правило (рис. 7.13).

СОВЕТ Если разорвать связь фильтра Web-прокси с HTTP-протоколом, а затем разрешить соединениям клиентов брандмауэра или SecureNAT доступ к данному правилу, то попытка соединения может завершиться неудачей, поскольку контроль содержимого зависит от фильтра Web-прокси.

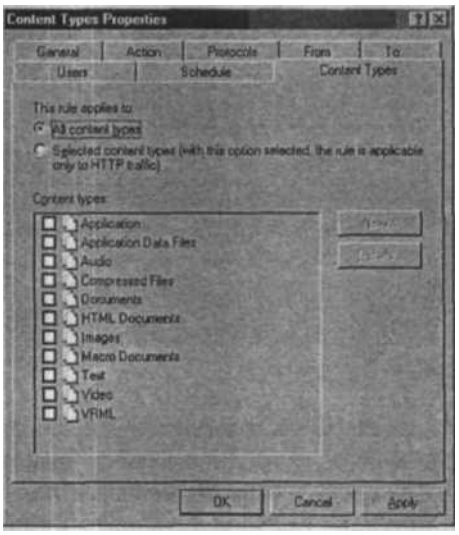


Рис. 7.13. Вкладка Content Types (Типы содержимого)

ПРИМЕЧАНИЕ Название правила доступа появляется в строке заголовка диалогового окна **Properties** (Свойства) данного правила. И это остается справедливым при переходе с вкладки на вкладку в диалоговом окне **Properties** (Свойства) правила. Однако, если щелкнуть кнопкой мыши вкладку **Content Types** (Типы содержимого), а затем другие вкладки в диалоговом окне **Properties** (Свойства), название правила в строке заголовка изменится на **Content Types Properties** (Свойства типов содержимого). При этом закрытие диалогового окна не приведет к действительному изменению названия правила. Мы склонны воспринимать это скорее как «пасхальное яйцо», а не как ошибку[1].

[1] Сленг, запрятанное в объектном коде шуточное послание, которое может быть обнаружено только в результате тщательной «очистки скорлупы» программного модуля *или* при определенном стечении обстоятельств. — *Примеч. пер.*

Команды контекстного меню правила доступа

При щелчке правой кнопкой мыши на правиле доступа появляются следующие команды контекстного меню, из которых можно выбрать требуемую.

- **Properties** (Свойства) Эта команда выводит на экран диалоговое окно **Properties** (Свойства).
- **Delete** (Удалить) Эта команда удаляет правило доступа.
- **Copy** (Копировать) Эта команда позволяет скопировать правило доступа, а затем вставить копию правила в политику брандмауэра.
- **Paste** (Вставить) Эта команда дает возможность вставить правило доступа, которое предварительно было скопировано.
- **Export Selected** (Экспортировать выбранные) Благодаря этой команде можно экспортировать правило доступа в файл с расширением xml. Затем можно импортировать этот файл на другой брандмауэр ISA для дублирования правила на другой машине.
- **Import to Selected** (Импортировать в выбранное) Эта команда позволяет импортировать правило доступа из xml-файла в правило, выбранное в политике доступа (Access Policy).
- **Move Up** (Переместить вверх) Эта команда позволяет переместить правило на одну строку вверх в списке правил доступа.
- **Move Down** (Переместить вниз) Эта команда позволяет переместить правило на одну строку вниз в списке правил доступа.
- **Disable** (Заблокировать) Благодаря этой команде можно заблокировать правило доступа, сохраняя его в списке правил доступа, чтобы снова разрешить его позже, когда потребуется.
- **Enable** (Разрешить) С помощью этой команды можно сделать доступным для использования то правило доступа, которое раньше было заблокировано командой **Disable** (Заблокировать).
- **Configure HTTP** (Настроить HTTP) Эта команда появляется, когда в правило доступа включается протокол HTTP. Команда **Configure HTTP** (Настроить HTTP) позволяет настроить H^T TP-фильтр защиты (HTTP Security Filter) для влияния на управление доступом через HTTP-соединения с помощью средств расширенного контроля прикладного уровня, входящих в брандмауэр ISA.
- **Configure FTP** (Настроить FTP) Эта команда появляется, когда правило доступа содержит FTP-протокол. Если она выбрана, на экране появляется диалоговое окно, позволяющее разрешить или запретить загрузку на удаленный компьютер с помощью этого протокола.
- **Configure RPC Protocol** (Настроить RPC-протокол) Эта команда появляется, когда в правило доступа включен RPC-протокол (Remote Procedure Call Protocol, протокол удаленного вызова процедуры). Когда она выбрана, на экране появляется диалоговое окно, позволяющее активизировать или заблокировать строгое

RPC-соответствие (strict RPC compliance), которое в свою очередь разрешает **или** блокирует соединения DCOM (Distributed Component Object Model, распределенная модель компонентных объектов).

СОВЕТ Команда **Copy** (Копировать) очень полезна, если нежелательно использовать мастер создания нового правила (New Access Rule Wizard) для создания новых правил. Щелкните правой кнопкой мыши существующее правило и затем левой кнопкой команду **Copy** (Копировать). Еще раз щелкните правой кнопкой мыши то же самое правило и выберите левой кнопкой команду **Paste** (Вставить). У вставленной копии будет то же самое название, что и у правила-оригинала, за исключением символов (1), добавленных в конец названия. Далее можно щелкнуть правой кнопкой мыши новое правило и выбрать команду **Properties** (Свойства) или дважды щелкнуть левой кнопкой мыши правило и изменить его название и другие характеристики. Если новое правило работает не так, как ожидалось, можно удалить его и вернуться к первоначальному правилу. Попробуйте скопировать и вставить правила несколько раз и посмотрите, насколько этот процесс вам подходит.

Настройка RPC-политики

Когда создается правило доступа, разрешающее исходящий RPC-доступ, имеется возможность настроить политику RPC-протокола. Правила доступа, которые разрешают **All IP Traffic** (Весь IP-трафик), также содержат RPC-протоколы. Для настройки RPC-политики щелкните правой кнопкой мыши правило доступа и выберите команду **Configure RPC Protocol** (Настроить RPC-протокол).

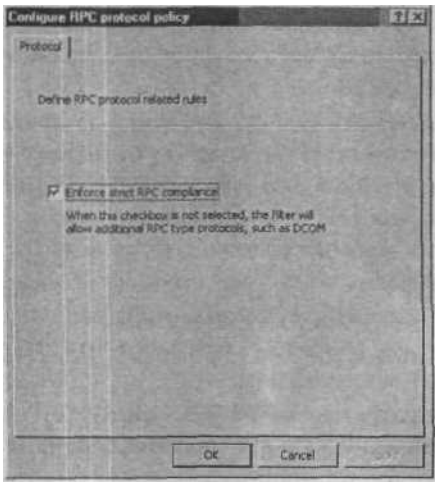


Рис. 7.14. Диалоговое окно Configure RPC protocol policy (Настройка политики RPC-протокола)

В диалоговом окне **Configure RPC protocol policy** (Настройка политики RPC-протокола), показанном на рис. 7.14, есть только один переключатель **Enforce strict RPC compliance** (Требовать строгого RPC-соответствия). По умолчанию он установлен. Если же флажок сброшен, RPC-фильтр разрешит использовать RPC- протоколы дополнительных типов, такие как DCOM. Если обнаружится, что некоторые протоколы, основанные на удаленном вызове процедуры, работают некорректно, проходя через брандмауэр ISA, попробуйте сбросить описанный переключатель.

RPC-политика брандмауэра настраивается для каждого протокола. Например, можно добиться строгого RPC-соответствия в одном правиле доступа и отказаться от этого в другом правиле в брандмауэре ISA.

Настройка FTP-политики

Если создано правило доступа, разрешающее использование FTP-протокола, то имеется команда для настройки FTP-политики. Щелкните правой кнопкой мыши правило доступа и выберите левой кнопкой мыши команду **Configure FTP** (Настроить FTP). При этом на экране появится диалоговое окно **Configures FTP protocol policy** (Настройка политики FTP-протокола), показанное на рис. 7.15. По умолчанию установлен флажок **Read Only** (Только чтение). В этом случае загрузки файлов с удаленных компьютеров по протоколу FTP будут блокироваться. Если нужно разрешить пользователям загружать файлы с помощью FTP, сбросьте этот флажок.

FTP-политика настраивается для каждого правила.

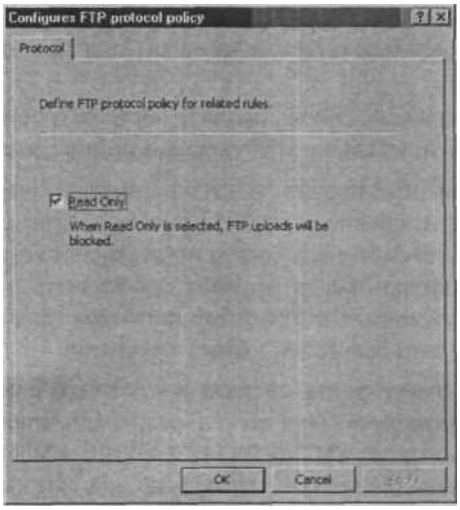


Рис. 7.15. Диалоговое окно Configures FTP protocol policy (Настройка политики FTP-протокола)

Настройка HTTP-политики

Когда бы ни создавалось правило доступа, разрешающее HTTP-соединения, всегда имеется возможность настроить HTTP-политику. Параметры HTTP-политики управляют HTTP-фильтром защиты. Подробному обсуждению параметров конфигурации, доступных в HTTP-фильтре защиты, посвящена глава 10.

Расстановка и упорядочивание правил доступа

Расположение правил доступа важно для гарантии корректной работы разработанной вами политики доступа. Мы рекомендуем следующий порядок размещения правил доступа.

- Располагайте правила публикации Web-серверов (Web Publishing Rules) и правила публикации серверов (Server Publishing Rules) в начале или в верхней части списка.
- Размещайте анонимные запрещающие (Deny) правила доступа под правилами публикации Web-серверов и правилами публикации серверов. Эти правила не требуют подтверждения подлинности пользователей и местонахождения клиентов в определенном месте (например, в составе набора компьютеров).
- Располагайте анонимные разрешающие (Allow) правила доступа под анонимными запрещающими правилами доступа. Эти правила не требуют подтверждения подлинности пользователей и местонахождения клиентов в определенном месте (например, в составе набора компьютеров).
- Размещайте запрещающие (Deny) правила доступа, требующие подтверждение подлинности пользователей (аутентификации), под анонимными разрешающими правилами.
- Располагайте разрешающие (Allow) правила доступа, требующие аутентификации, под запрещающими правилами, требующими подтверждения подлинности

Важно, чтобы анонимные правила доступа, применяемые к тому же протоколу, что и правила доступа, требующие аутентификации, применялись первыми, если необходимо разрешить анонимный доступ по этому протоколу. Если не поместить анонимное правило доступа прежде правила, требующего подтверждения подлинности, то запрос на соединение по данному протоколу для анонимного пользователя (как правило, клиента SecureNAT) будет отвергнут.

Предположим, что имеются два правила доступа: одно разрешает всем пользователям доступ по протоколу HTTP, а второе разрешает членам группы брандмауэра EXECS доступ по протоколам HTTP, HTTPS, FTP, IRC и MSN Messenger. Если поместить правило, разрешающее доступ группе EXECS, до анонимного правила доступа, то от всех HTTP-соединений для исходящего доступа потребуется аутентификация, а анонимное правило доступа, расположенное ниже правила, требующего аутентификации, будет игнорироваться. Однако, если имеется анонимное прави-

ло доступа для протокола NNTP (Network News Transfer Protocol, сетевой протокол передачи новостей), расположенное ниже правила, разрешающего группе EXECS исходящий доступ по протоколам HTTP, HTTPS, FTP, IRC и MSN Messenger, то анонимное соединение по протоколу NNTP будет разрешено, потому что этот протокол не соответствует параметрам, заданным для правила, разрешающего исходящий доступ группе EXECS.

Мы считаем, что на первый взгляд эта модель слегка запутана. Когда мы начинали работать с брандмауэром ISA, то предполагали, что, когда правило применяется к конкретной группе брандмауэра, запрос на соединение от пользователя, который не предоставил верительных данных (credentials) брандмауэру ISA, будет проигнорирован и брандмауэр продолжит обработку списка правил сверху вниз до тех пор, пока не будет найдено анонимное правило доступа, соответствующее параметрам соединения. На самом деле это *не* так. Анонимные пользователи могут считаться членами группы «Anonymous Users (Анонимные пользователи)», и эта группа не соответствует ни одной группе, от которой мы можем потребовать подтверждения подлинности. Поскольку группа «Anonymous Users» (Анонимные пользователи) не соответствует ни одной реальной группе, любое правило, соответствующее запросу на соединение, но требующее аутентификации, будет запрещено.

Как препятствовать регистрации в журнале соединений для выбранных протоколов

Допустим, что необходимо помешать брандмауэру ISA записывать в журнал информацию о соединениях по определенным протоколам, достигших брандмауэра. Обычным примером могут быть широковещательные протоколы NetBIOS: NetBIOS Name Service (служба имен NetBIOS) и NetBIOS Datagram (дейтаграмма NetBIOS). Оба эти протокола регулярно пересылают сообщения на широковещательный адрес локальной подсети и могут заполнить журнал регистрации службы брандмауэра ISA информацией, не представляющей большого интереса для администратора брандмауэра ISA.

Можно создать правило доступа, включающее эти протоколы, а затем настроить его так, чтобы не записывать в журнал информацию о соединениях, связанных с данным правилом. Например, можно выполнить следующую процедуру, препятствующую записи в журнал сведений об этих протоколах NetBIOS.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. На панели задач щелкните кнопкой мыши вкладку **Tasks** (Задачи) и далее щелк ните кнопкой мыши вариант **Create** New Access **Rule** (Создать новое правило доступа).

3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере мы назовем правило **Block NetBIOS logging** (Запретить запись в журнал соединения NetBIOS). Щелкните мышью кнопку **Next** (Далее).
4. Выберите вариант **Deny** (Запретить) на странице **Rule Action** (Действие правила) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите вариант **Selected protocols** (Выбранные протоколы) в списке **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните кнопкой мыши папку **Infrastructure** (Инфраструктура). Дважды щелкните кнопкой мыши элементы **NetBIOS Datagram** (Дейтаграмма NetBIOS) и **NetBIOS Name Service** (Служба имен NetBIOS). Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) **щелкните** кнопкой мыши папку **Computer Sets** (Наборы компьютеров) и затем дважды щелкните мышью элемент **Anywhere** (Везде). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).
11. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните **КНОПКОЙ** мыши папку **Computer Sets** (Наборы компьютеров). Дважды щелкните мышью элемент **Anywhere** (Везде) и далее щелкните мышью кнопку **Close** (Закрыть).
13. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
14. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователей).
15. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила доступа).
16. Щелкните правой кнопкой мыши правило **Block NetBIOS Logging** (запретить запись в журнал соединения NetBIOS) и щелкните кнопкой мыши команду **Properties** (Свойства).
17. В диалоговом окне **Block NetBIOS Logging Properties** (Свойства запрета записи в журнал NetBIOS) сбросьте флажок **Log requests matching this rule** (Регистрировать в журнале запросы, соответствующие данному правилу).

18. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK.
19. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра. 20. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Правило, созданное в этом примере, не только препятствует записи в журнал широковещательных сообщений по протоколу NetBIOS, но и не позволяет этим сообщениям проходить через брандмауэр в обоих направлениях (от него и к нему). Таким образом, одно правило дает двойной выигрыш!

Запрет автоматических соединений Web-прокси для клиентов SecureNAT

Бывают ситуации, в которых клиентам брандмауэра и клиентам SecureNAT (средства безопасного преобразования сетевых адресов) выгодно отказаться от сервиса Web-прокси. По умолчанию HTTP-соединения от клиентов брандмауэра и SecureNAT автоматически направляются на фильтр Web-прокси. Благодаря этой конфигурации клиенты как SecureNAT, так и брандмауэра получают выигрыш от использования кэширования Web-прокси брандмауэра ISA (если кэширование разрешено в брандмауэре ISA).

Проблема в том, что некоторые Web-сайты плохо написаны и не согласуются с CERN-совместимым (CERN compliant) Web-прокси. Можно решить эту проблему, настроив такие сайты на прямой доступ (Direct Access), а затем разорвав связь фильтра Web-прокси с HTTP-протоколом.

Выполните следующие шаги, запрещающие автоматические соединения с Web-прокси для клиентов брандмауэра и SecureNAT.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра) на левой панели консоли.
2. На панели задач щелкните кнопкой мыши вкладку **Toolbox** (Инструментальная панель). На этой вкладке щелкните кнопкой мыши папку **Command Protocols** (Протоколы команды) и дважды щелкните протокол **HTTP.**
3. В диалоговом окне **HTTP Properties** (Свойства HTTP) щелкните кнопкой мыши вкладку **Parameters** (Параметры).
4. На вкладке **Parameters** (Параметры) сбросьте флажок **Web Proxy Filter** (Фильтр Web-прокси). Щелкните мышью кнопку **Apply** (Применить) и затем кнопку OK.
5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

С одной стороны обход фильтра Web-прокси приводит к тому, что HTTP-политика не применяется к клиентам SecureNAT и брандмауэра. Однако HTTP-политика применяется к машинам, которые явно настроены как клиенты Web-прокси, даже когда клиенты брандмауэра, SecureNAT и Web-прокси получают доступ к сайту, использующему то же самое правило доступа.

Например, создается правило, названное **HTTP Access** (Доступ по HTTP), которое разрешает всем пользователям внутренней сети доступ ко всем сайтам внешней сети с помощью протокола HTTP. Допустим, что в HTTP-политику этого правила вносится запрет соединений с доменом www.spyware.com. Когда клиенты Web-прокси попытаются соединиться с www.spyware.com, соединение будет заблокировано правилом доступа **HTTP Access** (Доступ по HTTP). Однако, если клиенты SecureNAT и брандмауэра попытаются получить доступ к домену www.spyware.com с помощью правила **HTTP Access** — доступ по HTTP — (когда фильтр Web-прокси отсоединен от протокола HTTP), это правило разрешит доступ клиентам SecureNAT и брандмауэра.

С другой стороны, отсоединение фильтра Web-прокси от определения протокола HTTP приводит к удалению конфигурационного интерфейса (диалогового окна **Configure HTTP policy for rule** — настройка HTTP-политики для правила) для HTTP-фильтра с консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет). Во всех правилах, имеющих уже настроенную HTTP-политику, она будет продолжать действовать на клиентов Web-прокси. Для того чтобы изменить HTTP-политику в уже существующем правиле или настроить ее в новых правилах доступа, придется снова связать определение HTTP-протокола с фильтром Web-прокси. После конфигурирования HTTP-политики можно опять разорвать связь фильтра Web-прокси с HTTP-протоколом.

Конечно, можно сконфигурировать все клиенты как клиенты Web-прокси (мы рекомендуем сделать это!) и избежать административных издержек.

> ВНИМАНИЕ Когда фильтр Web-прокси отсоединен от определения HTTF'-протокола, интерфейс настройки HTTP-политики также удаляется из правил Web-прокси.

Использование сценариев для заполнения наборов имен доменов

Одна из сильных сторон брандмауэра ISA — его исключительный, отслеживающий соединения контроль прикладного уровня (stateful application layer inspection). Кроме выполнения основной задачи — фильтрации с отслеживанием соединений (которую может выполнять и простой «аппаратный» брандмауэр) — возможность строгого контроля и отслеживания соединений на прикладном уровне позволяет брандмауэру ISA на самом деле анализировать проходящие через брандмауэр протоко-

лы. В отличие от традиционных аппаратных брандмауэров второго поколения брандмауэр ISA — представитель третьего поколения брандмауэров, обладающих сведениями не только о сети, но и о прикладных протоколах.

Механизм отслеживающего состояние соединения прикладного контроля позволяет управлять доступом не непосредственно к «портам», а к реальным протоколам, проходящим через эти порты. В то время как традиционный «аппаратный» брандмауэр получает информацию о проходящих пакетах благодаря простым механизмам фильтрации, отслеживающим соединения, которые стали доступны с середины 1990-х гг., средства контроля прикладного уровня, отслеживающие состояние соединения, переносят брандмауэр ISA в XXI век и действительно управляют доступом протоколов уровня приложения. Эти средства делают возможным управление входящим и исходящим доступом, основанное на информации прикладного уровня, известной брандмауэру, в отличие от простого «открытия и закрытия» портов.

Один яркий пример — возможность задания сайтов, к которым пользователи могут получить доступ через брандмауэр ISA. Эту возможность можно сочетать как с мощным контролем доступа, основанным на пользователях/группах, так и с управлением протоколами.

Например, если имеется группа пользователей, названная «Web Users» (Web-пользователи), и необходимо запретить этим пользователям доступ к списку из 1 500 URL-адресов или доменов. Можно создать правило доступа, блокирующее доступ только к заданным 1 500 сайтам и разрешающее доступ ко всем остальным после подтверждения подлинности пользователей этой группы в брандмауэре ISA.

Другой пример: необходимо создать список запрета из 5 000 доменов, доступ к которым по любому протоколу запрещен всем пользователям за исключением администраторов доменов. Можно создать набор имен доменов (Domain Name Set) и применить этот набор в правиле доступа, блокирующем доступ к этим сайтам.

Задача заключается в поиске способа занесения тысяч имен доменов или URL-адресов в наборы имен доменов или наборы URL-адресов. Конечно, можно вводить их вручную, используя встроенные средства консоли управления ISA, но удобнее импортировать их из текстового файла. В Интернете есть ряд мест, где можно найти такие файлы (мы не хотели бы упоминать их, поскольку не хотим неявно их рекламировать). Как только появится текстовый файл, возможно, потребуется использовать сценарий для импорта строк текстового файла в набор URL-адресов или набор имен доменов.

Давайте начнем со сценариев. Первый сценарий, приведенный в листинге 7.1, применяется для импорта элементов из текстового файла в набор URL-адресов. Скопируйте информацию в текстовый файл и сохраните его с именем Import-URLs.vbs.

Листинг 7.1. Сценарий для импорта элементов текстового файла в **набор URL-адресов**

```
< ------начните со строки,  расположенной под этой —>
Set Isa = CreateObjectC'FPC.Root")
Set CurArray = Isa.GetContainingArray
Set RuleElements = CurArray.RuleElements
Set URLSets = RuleElements.URLSets
Set URLSet = URLSets.Item("Urls")
Set FileSys = CreateObjectC'Scripting.FileSystemObject")
Set UrlsFile = FileSys.OpenTextFileCurls.txt", 1)
For i = 1 to URLSet.Count
   URLSet.Remove 1 Next Do While
UrlsFile.AtEndOfStream <> True
   URLSet.Add UrlsFile.ReadLine
Loop
WScript. Echo "Saving..."
CurArray.Save
WScript.Echo "Done"
< ---Закончите строкой, расположенной над этой->
```

Две строки в этом файле, которые вам придется изменить в вашем варианте, выделены жирным шрифтом.

В строке:

```
Set URLSet = URLSets.ItemfUrls")
```

измените элемент **Urls** на имя набора URL-адресов, который вы хотите создать в брандмауэре ISA.

В строке: Set UrlsFile = FileSys.

```
OpenTextFileCurls.txt",  1)
```

измените элемент **urls.txt** на имя текстового файла, содержащего URL-адреса, которые вы хотите импортировать в конфигурацию брандмауэра ISA.

Следующий сценарий применяется для импорта коллекций имен доменов, содержащихся в текстовом файле. Сохраните содержимое листинга *7.2* в текстовом файле *и* назовите его ImportDomains.vbs.

Листинг 7.2. Сценарий для импорта элементов текстового файла в набор имен доменов

```
< ------ начните со строки,  расположенной под этой —>
Set Isa = CreateObjectC'FPC.Root"
Set CurArray = Isa.GetContainingArray
Set RuleElements = CurArray.RuleElements
Set DomainNameSets = RuleElements.DomainNameSets
Set DomainNameSet = DomainNameSets. Item("Domains")
```

```
Set FileSys = CreateObject ("Scripting.FileSystemObject")
Set DomainsFile = FileSys. OpenTextFile("domains.txt", 1)
For i = 1 to DomainNameSet.Count
    DomainNameSet.Remove  1 NextDo While
DomainsFile.AtEndOfStream o True
    DomainNameSet. Add   DomainsFile.ReadLine
Loop
WScript.Echo   "Saving..." CurArray.Save WScript.Echo
"Done" < ——Закончите строкой,   расположенной над
этой—>
```

Две строки в этом файле, которые придется изменить в вашем варианте, приведены далее.

```
В строке: Set DomainNameSet =

DomainNameSets.Item("Domains")
```

замените элемент Domains на имя набора имен доменов, который вы хотите создать в брандмауэре ISA.

В строке:

```
Set  DomainsFile  = FileSys.OpenTextFileC domains.txt",   1)
```

замените элемент domains.txt на имя текстового файла, содержащего домены, которые вы хотите импортировать в конфигурацию брандмауэра ISA.

Использование сценариев импорта

Теперь давайте посмотрим, как работают сценарии. Первое, что необходимо сделать, — создать набор URL-адресов или набор имен доменов на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет). Это простая процедура, состоящая всего из нескольких шагов.

Сначала создадим набор URL-адресов, названный URLs, поскольку это имя по умолчанию, использованное в нашем сценарии. Помните, что можно изменить имя набора URL-адресов; только сначала обязательно создайте набор URL-адресов с выбранным вами именем на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет).

Для создания набора URL-адресов с именем URLs выполните следующие шаги.

- На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).

В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вкладку **Toolbox** (Инструментальная панель) на панели задач. На вкладке **Toolbox** (Инструментальная панель) щелкните мышью вкладку **Network Objects** (Сетевые объекты).

На вкладке **Network Objects** (Сетевые объекты) щелкните кнопкой мыши последовательность команд меню **New** (Новый) / **URL Set** (Набор URL-адресов). В диалоговом окне **New URL Set Rule Element** (Новый элемент правила для набора URL-адресов), показанном на рис. 7.16, введите **URLs** в **текстовое поле Name** (Имя). Щелкните мышью кнопку OK.

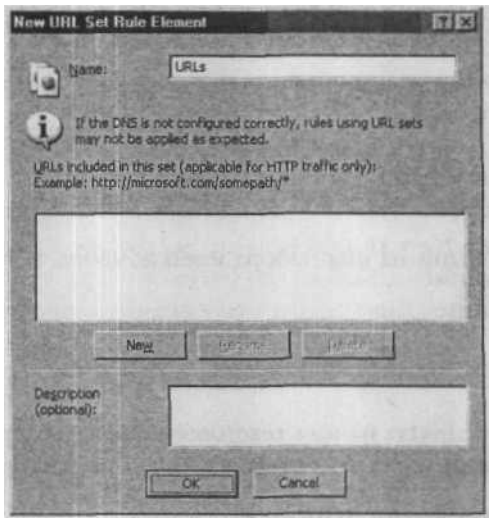


Рис. 7.16. Диалоговое окно New URL Set Rule Element (Новый элемент правила для набора URL-адресов)

Теперь набор URL-адресов появится в списке наборов URL-адресов, показанном на рис. 7.17.

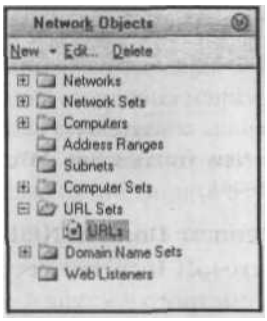


Рис. 7.17. Список наборов URL-адресов

Следующий шаг — создание набора имен доменов с именем **Domains,** именем набора по умолчанию, использованном в сценарии ImportDomains. Помните, что можно использовать другое имя набора имен доменов; только убедитесь, что оно такое же, как в сценарии.

Для создания набора имен доменов с именем **Domains** выполните следующие шаги.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вкладку **Toolbox** (Инструментальная панель) на панели задач. На вкладке **Toolbox** (Ин струментальная панель) щелкните мышью вкладку **Network Objects** (Сетевые объекты).
3. На вкладке **Network Objects** (Сетевые объекты) щелкните кнопкой последователь ность команд меню **New** (Новый) / **Domain Name Set** (Набор имен доменов).
4. В диалоговом окне **New Domain Name Set Policy Element** (Новый элемент политики наборов имен доменов), показанном на рис. 7.18, введите **Domains** в текстовое поле **Name** (Имя). Щелкните мышью кнопку OK.

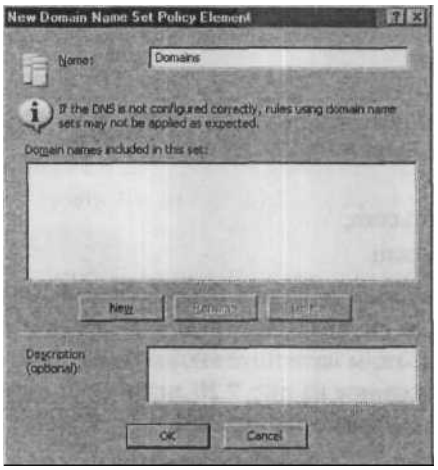


Рис. 7.18. Диалоговое окно New Domain Set Policy Element (Новый элемент политики наборов имен доменов)

Новый элемент появится в списке **Domain Name Sets** (Наборы имен доменов), показанном на рис. 7.19.

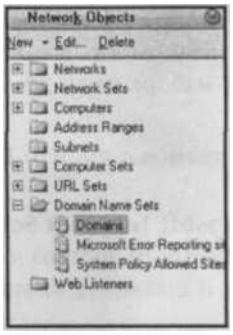


Рис. 7.19. Список Domain Name Sets (Наборы имен доменов)

я Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.

- Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Теперь **нужно** создать **два** текстовых файла: **urls.txt и domains.txt.** Это текущие **имена,** использованные в сценариях. Можно изменить имена файлов, но только убедитесь, что они соответствуют именам, заданным в сценариях.

Файл **domains.txt** будет содержать следующие домены:

- stuff.com;
- blah.com;
- scumware.com.

Файл **urls.txt** будет содержать следующие URL-адреса:

- http://www.cisco.com;
- http://www.checkpoint.com;
- http://www.sonicwall.com.

Далее скопируйте файлы сценариев и текстовые файлы в один и тот же каталог. В нашем примере мы скопируем файлы сценариев и текстовые файлы в корневой каталог диска C:. Дважды щелкните кнопкой мыши по файлу **Import URLs .vbs.** Сначала вы увидите показанное на рис. 7.20 диалоговое окно с сообщением: **Saving** (Сохранение). Щелкните мышью кнопку OK.

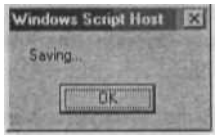
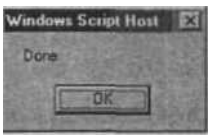


Рис. 7.20. Сохранение информации

В зависимости от количества импортируемых вами URL-адресов может пройти от нескольких секунд до нескольких минут, прежде чем вы увидите показанное на

Рис. 7.21. Завершение процедуры

рис. 7.21 следующее диалоговое окно, информирующее о том, что импорт завершен. Щелкните мышью кнопку OK.



Теперь импортируем домены. Щелкните дважды кнопкой мыши файл **Import-Domains.vbs.** Снова появится диалоговое окно **Saving** (Сохранение). Щелкните мышью кнопку OK. Через несколько секунд или минут вы увидите диалоговое окно **Done** (Сделано). Щелкните мышью кнопку OK.

Закройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет), если она открыта. Теперь откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет) и перейдите на узел **Firewall Policy** (Политика брандмауэра) на левой панели консоли.

ПРИМЕЧАНИЕ Можно обойтись без закрытия и повторного открытия консоли Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет), если щелкнуть на ней мышью кнопку Refresh (Обновить).

Щелкните кнопкой мыши вкладку **Toolbox** (Инструментальная панель) на панели задач и строку **Network Objects** (Сетевые объекты). Щелкните кнопкой мыши папку **URL Sets** (Наборы URL-адресов). Дважды щелкните кнопкой мыши набор URL-адресов с именем URLs. Вы увидите, что набор URL-адресов заполнен элементами из вашего текстового файла, как показано на рис. 7.22.

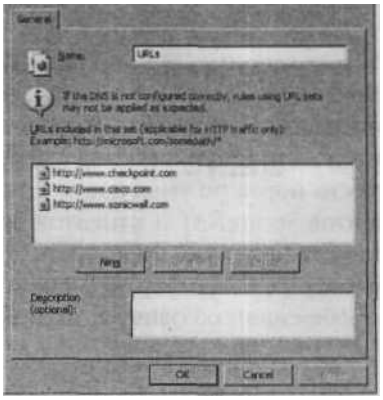


Рис. 7.22. Элементы набора URL-адресов

Щелкните кнопкой мыши папку **Domain Name Sets** (Наборы имен доменов). Дважды щелкните строку **Domains.** Вы увидите, что набор имен доменов заполнен доменами, доступ к которым необходимо запретить или разрешить, в зависимости от потребностей. В нашем примере мы включили в набор показанные на рис. 7.23 домены, доступ к которым хотели бы заблокировать.

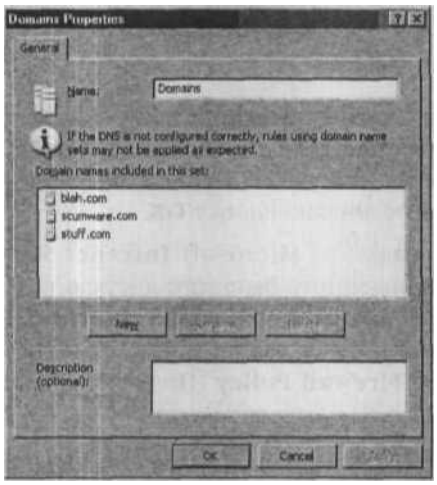


Рис. 7.23. Свойства набора имен доменов

Когда накопится больше URL-адресов, вы сможете добавить их в тот же текстовый файл и выполнить сценарий снова. Новые элементы будут вставлены без создания дубликатов URL-адресов или имен доменов, которые уже включены в набор URL-адресов или набор имен доменов.

Расширение диапазона портов туннелирования SSL-соединения для Web-доступа к дополнительным SSL-портам

Возможны ситуации, в которых клиентам Web-прокси понадобится соединение по протоколу SSL (Secure Sockets Layer, протокол защищенных сокетов) с Web-сайтами, использующее дополнительные порты для SSL-связи. Например, пользователи могут попытаться получить доступ к банковскому сайту, который требует SSL-соединения на порт 4433 вместо порта по умолчанию с номером 443. Это окажется проблематичным для клиентов SecureNAT и клиентов брандмауэра, поскольку установка по умолчанию брандмауэра ISA — направлять HTTP-соединения клиентов SecureNAT и клиентов брандмауэра на фильтр Web-прокси. Клиенты увидят пустую страницу или страницу с сообщением об ошибке, указывающим на невозможность отображения страницы.

В данном случае проблема заключается в том, что фильтр Web-прокси направляет SSL-соединения только на порт 443- Если клиенты попытаются соединиться с SSL-сайтом через порт, отличный от TCP-порта 443, попытка соединения закончится неудачей. Можно решить эту проблему, расширяя диапазон портов туннелирования SSL-соединения. Однако для этого потребуется загрузить сценарий Джима Харрисона (Jim Harrison) с сайта http://www.isatools.org и ввести диапазон портов туннелирования, который, по вашему мнению, должен использовать компонент Web-прокси брандмауэра ISA.

Выполните следующие шаги для расширения в брандмауэре ISA диапазона портов туннелирования SSL-соединения.

- Зайдите на сайт www.isatools.org и загрузите на ваш компьютер файл isa_tpr.js, ско пируйте этот файл в брандмауэр ISA. Не используйте обозреватель на компьютере с брандмауэром. Загрузите файл с сайта на управляющую рабочую станцию, про смотрите файл и затем скопируйте его на съемное устройство и поместите его в брандмауэр. Помните, на самом брандмауэре никогда не следует использовать кли ентские приложения, такие как обозреватели, почтовые клиенты и т. д.
- Дважды щелкните кнопкой мыши файл isa_tpr.js. Первое диалоговое окно, которое вы увидите, утверждает: This is your current Tunnel Port Range list (Это ваш текущий список диапазона портов туннелирования). Щелкните мышью кнопку ОК.
- Отображается NNTP-порт (Network News Transfer Protocol, сетевой протокол передачи новостей). Щелкните мышью кнопку ОК.
- Отображается SSL-порт (Secure Sockets Layer, протокол защищенных сокетов). Щелкните мышью кнопку ОК.
- Теперь скопируйте файл isa_tpr.js в корневой каталог диска C:. Откройте окно ввода командной строки и введите следующую строку:

  ```
  isa_tpr.js /?
  ```

- Откроется диалоговое окно, показанное на рис. 7.24.
- Для вставки нового порта туннелирования, например 8848, введите следующую команду и нажмите клавишу <ENTER>:

  ```
  Cscript isa.tpr.js /add Ext8848 8848
  ```

- После успешного выполнения команды откроется окно, похожее на приведен ное на рис. 7.25.

Рис. **7.24.** Пояснительная информация к сценарию файла isa_pr.js

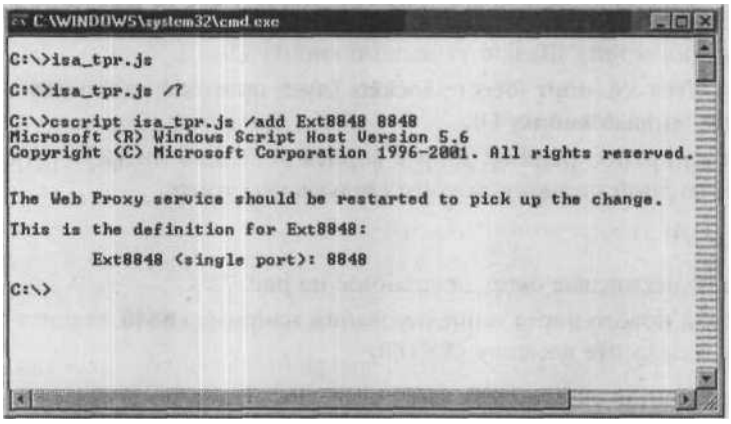


Рис. 7.25. Выполнение сценария для добавления порта к диапазону портов туннелирования SSL-соединения

Можно воспользоваться альтернативным вариантом: загрузите с сайта www.isa-tools.org файл **ISATpre.zip,** содержащий приложение .NET, написанное Стивеном Соекрасно (Steven Soekrasno), и установите это приложение на брандмауэре ISA. Приложение предлагает легкий в использовании графический интерфейс, позволяющий расширить диапазон портов туннелирования SSL-соединения. На рис. 1.26 показан интерфейс GUI (graphical user interface, графический интерфейс пользователя) этого приложения.

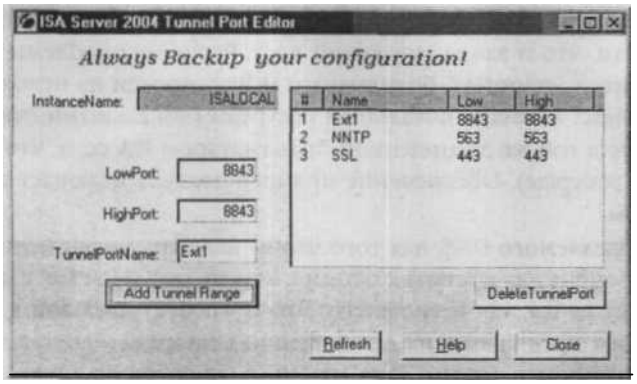


Рис. 7.26. Применение приложения .NET Стивена Соекрасно (Steven Soekrasno) для расширения диапазона портов туннелирования

Исключение петель через брандмауэр ISA для соединения с внутренними ресурсами

Обычная ошибка администраторов брандмауэра ISA — разрешение хостам из сети, защищенной брандмауэром ISA, создавать петлю (loop back) при получении доступа к ресурсам той же самой сети, в которой размещается клиент.

ПРИМЕЧАНИЕ Петля через брандмауэр ISA может как снизить его общую производительность, так и нарушить все соединения.

Предположим, что имеется брандмауэр ISA с простой конфигурацией, у которого есть один внутренний и один внешний интерфейсы. Во внутренней сети, расположенной за внутренним интерфейсом, имеется клиент SecureNAT и Web-сервер. Вы опубликовали Web-сервер в Интернете с помощью правила публикации Web-сервера. Web-сервер доступен внутренним клиентам по URL-адресу http://webl и внешним клиентам по URL-адресу http://www.msfirewall.org.

Что произойдет, когда пользователи внутренней сети попытаются соединиться с Web-сервером, используя URL-адрес http://www.msfirewall.org? Если у вас нет в нужном месте разделяемого DNS (Domain Name Server, сервер доменных имен), клиенты внутренней сети будут разрешать ссылку www.msfirewall.org на IP-адрес через внешний интерфейс брандмауэра ISA, который ждет (прослушивает) входящие подключения к www.msfirewall. org. Далее хост попытается подключиться к внутреннему ресурсу с помощью петли через брандмауэр ISA, используя правило публикации Web-сервера. Если клиент является клиентом SecureNAT, попытка соединения может оказаться неудачной (в зависимости от конфигурации брандмауэра ISA) или значительно снизится общая производительность брандмауэра ISA, поскольку он обрабатывает в этом случае подключения к внутренним ресурсам.

Всегда следует избегать петель через брандмауэр ISA для ресурсов, размещенных в той же сети, что и запрашивающий хост. Решение проблемы заключается в настройке клиентов SecureNAT, брандмауэра и Web-прокси на использование прямого доступа (Direct Access) к локальным ресурсам (локальными считаются ресурсы, размещенные в той же защищенной брандмауэром ISA сети, что и хост, запрашивающий эти ресурсы). Обеспечение прямого доступа включает в себя следующие компоненты.

- Создание разделяемого DNS, для того чтобы клиенты могли использовать одно и то же имя домена для доступа к одним и тем же ресурсам как с помощью внутреннего интерфейса, так и внешнего. Это потребует двух зон в двух серверах DNS. Одна зона предназначена для внешних клиентов, а другая зона используется внутренними клиентами. Зона внешних клиентов преобразует имена в адреса, доступные через внешний интерфейс, а внутренняя зона — в адреса, доступные через внутренний интерфейс. Суть в том, что зоны отвечают за одно и то же доменное имя.
- Настройка свойств сети, в которой размещается клиент Web-прокси защищенной сети, использующий прямой доступ для достижения как IP-адресов внутренней сети, так и имен доменов внутренней сети. Настройка выполняется на вкладке Web-прокси.
- Настройка свойств сети, в которой располагается клиент брандмауэра защищенной сети, использующий прямой доступ для внутренних доменов.

Подробности такой настройки включены в описание установки и сопровождения клиента ISA в главе 5 и в описание проекта организации сети брандмауэра ISA в главе 4.

Появление анонимных запросов в журнале регистрации соединений, даже при обязательной аутентификации, заданной для Web-доступа (HTTP-соединений)

Обычный вопрос, который задают администраторы брандмауэра ISA, связан с появлением анонимных подключений от клиентов Web-прокси в регистрационных журналах Web-прокси брандмауэра ISA. Эти подключения появляются несмотря на то, что все правила настроены на обязательную аутентификацию. Короткий ответ на этот вопрос — это нормальная и предсказуемая ситуация.

Подробный ответ включает объяснение способа обычных соединений клиентов Web-прокси с проверяющими подлинность серверами Web-прокси. Из соображений производительности первоначальный запрос от клиента Web-прокси посылается *без* верительных данных (имени и пароля) пользователя. Если есть правило, разрешающее анонимное соединение, то соединение разрешается. Если клиент должен сначала подтвердить свою подлинность, сервер Web-прокси посылает обратно клиенту Web-прокси сообщение об отказе в соединении (ошибка 407) с запросом верите-

ных данных. Затем клиент Web-прокси посылает верительные данные брандмауэру ISA и имя пользователя появляется в файлах журналов регистрации.

На рис. 7.27 показан HTTP-ответ с ошибкой 407, возвращенный клиенту Web-прокси. В правой части рисунка представлен декодированный в ASCII-код кадр (frame), взятый из записи трассировки Network Monitor (сетевой монитор). В пятой сверху строке вы найдете **HTTP/1.1407 Proxy Authentication Required** (HTTP/1.1 407 требуется аутентификация прокси). Это и есть ответ 407, получаемый клиентами Web-прокси, когда правило доступа требует аутентификации для подключения к Web-сайту через брандмауэр ISA.

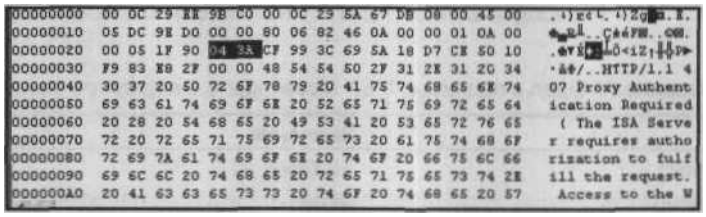


Рис. 7.27. Ответ 407, возвращенный клиенту Web-прокси

Блокирование протокола MSN Messenger с помощью правила доступа

Блокирование опасных приложений — обычная задача брандмауэра ISA. Существует ряд способов, которые можно использовать для блокирования опасных приложений.

- Используйте фильтр защиты HTTP (HTTP Security Filter) для блокирования приложения, использующего Web (HTTP)-соединение для доступа к сайту.
- Применяйте наборы имен доменов и URL-адресов для блокирования сайтов, в доступе к которым нуждается опасное приложение для установки соединения.
- Блокируйте протоколы или запрещайте доступ по протоколу, который требуется опасному приложению, если оно использует определенный пользователем (custom) протокол.
- Если приложение может использовать определенный пользователем протокол и Web-соединение для выхода в Интернет, блокируйте определенный пользователем протокол и затем используйте наборы имен доменов и URL-адресов для блокирования возможности доступа в Интернет с помощью Web-соединения.
- Упростите свою жизнь, применяя принцип минимума полномочий или прав (Principle of Least Privilege). Когда применяются минимальные полномочия, можно создать правила, разрешающие доступ. Все, что явно не разрешено, заблокировано. В этом случае, почти никогда не понадобится создавать какие бы то ни было запрещающие правила.

Для демонстрации одного из способов, которые можно использовать при блокировании опасных приложений, мы создадим политику доступа, которая блоки-

рует приложение, устанавливающее соединение по протоколу MSN Messenger 6.2 (протокол службы сообщений сети Microsoft). Решение состоит из следующих шагов:

1 создание запрещающего (Deny) правила, которое блокирует протокол MSN Messenger; ■ создание правила доступа, которое блокирует HTTP-заголовок протокола MSN Messenger.

В данном примере мы создадим правило «all open» (все открыто), разрешающее всем протоколам исходящий доступ, но включим в фильтр защиты HTTP подпись (signature), которая заблокирует протокол MSN Messenger. Второе правило блокирует протокол MSN Messenger. В табл. 7.2 и 7.3 приведены свойства каждого правила доступа.

Табл. 7.2. Правило All Open с подписью MSN Messenger 6.2 в фильтре защиты HTTP

Свойство	Значение
Name (Название)	All Open -1
Action (Действие)	Allow
Protocols (Протоколы)	HTTP and HTTPS
From /Listener (От/Слушаюший процесс)	Internal
To (Кому)	External
Condition (Условие)	All Users
Purpose (Назначение)	Это правило разрешает любой трафик через брандмауэр ISA всем пользователям ко всем сайтам. HTTP-подпись (HTTP signature) создается для блокирования HTTP-за головки протокола MSN Messenger 6.2

Табл. 7.3. Правило доступа, запрещающее протокол MSN Messenger

Свойство	Значение
Name (Название)	Deny Messenger Protocol
Action (Действие)	Deny
Protocols (Протоколы)	MSN Messenger
From/Listener (От/Слушающий процесс)	Internal
To (Кому)	External
Condition (Условие)	All Users
Purpose (Назначение)	Блокирует соединение по протоколу MSN Messenger через TCP-порт 1863

Можно использовать информацию, приведенную ранее в этой главе, для создания правил доступа, описанных в табл. 7.2 и 7.3. Правило **Deny Messenger Protocol** (Запретить протокол Messenger) должно находиться над правилом **All Open** (Все открыто). Запрещающие правила следует всегда помещать над разрешающими правилами. Ваша политика доступа должна быть похожа на показанную на рис. 7.28.

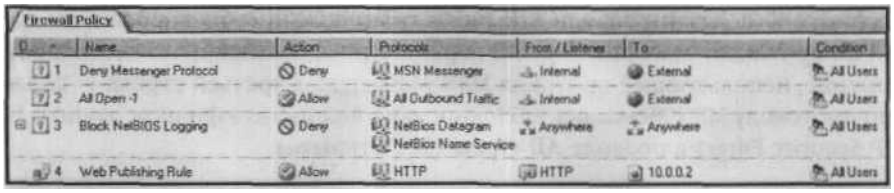


Рис. 7.28. Политика брандмауэра для блокирования протокола MSN Messenger

После создания правила доступа щелкните правой кнопкой мыши правило доступа **All Open -1** и щелкните левой кнопкой мыши команду **Configure HTTP** (Настроить HTTP). В диалоговом окне **Configure HTTP policy for rule** (Настроить HTTP-политику для правила) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Signature** (Подпись), показанном на рис. 7.29, введите следующую информацию:

Name: (Имя:) введите имя подписи, блокирующей протокол MSN Messenger;

Description (optional): (Описание необязательное:) введите описание правила;

Search in: (Искать в:) выберите строку **Request headers** (Заголовки запросов) в раскрывающемся списке;

HTTP Header: (HTTP-заголовок:) введите **User-Agent:** (Пользователь-агент:) в текстовое поле;

Signature: (Подпись:) введите **MSN Messenger** в текстовое поле.

Щелкните мышью кнопку ОК, чтобы сохранить подпись, затем щелкните мышью кнопку ОК в диалоговом окне **Properties** (Свойства). Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра, затем щелкните мышью *кнопку* ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Рис. 7.29. Диалоговое окно **Signature** (Подпись)

На рис. 7.30 показаны записи в журнале регистрации о блокированном соединении по протоколу MSN Messenger. В первой строке показано, что заблокировано соединение, использующее протокол MSN Messenger, в третьей строке — соединение по протоколу MSN Messenger заблокировано подписью в фильтре защиты HTTP (HTTP Security Filter) в правиле **All Open** (Все открыто).

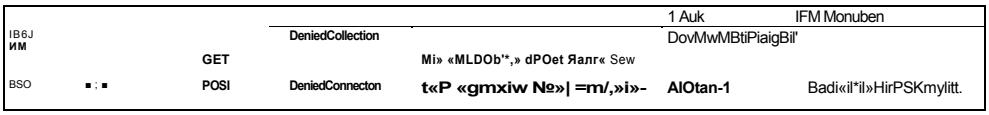


Рис. 7.30. Строки файла журнала регистрации, показывающие блокирование фильтром защиты HTTP соединения по протоколу MSN Messenger

СОВЕТ Для фильтрования этих типов событий, связанных с фильтром **защиты** HTTP полезно добавить столбец **HTTP Status** (Состояние HTTP) в журнал мониторинга в реальном времени брандмауэра ISA.

Разрешение исходящего доступа по протоколу MSN Messenger через Web-прокси

Протокол MSN Messenger может получить доступ к Интернету по своему собственному протоколу или с помощью туннелирования своих соединений в HTTP-заголовке. Но вы столкнетесь с проблемами, если захотите предоставить доступ клиентам Web-прокси к сайту, использующему MSN Messenger, из-за трудностей аутентификации, преследующих, как протокол MSN Messenger, так и приложения Hotmail.

Когда протокол MSN Messenger посылает верительные данные (credentials) сайту, использующему MSN Messenger, эти же сведения посылаются и брандмауэру ISA. Если имя пользователя и пароль, применяемые пользователем для доступа к сайту с протоколом MSN Messenger, отличаются от верительных данных этого пользователя в корпоративной сети, соединение не устанавливается. Если разрешить анонимный доступ к сайту, использующему протокол MSN Messenger, проблем не возникнет, поскольку никакие верительные данные не посылаются брандмауэру ISA, который в этом случае не должен запрашивать у пользователя сведения, подтверждающие его подлинность.

Эту проблему можно обойти, разрешив правило анонимного доступа для клиентов Web-прокси, чтобы они могли применять протоколы HTTP и HTTPS (Hypertext Transmission Protocol, Secure, протокол защищенной передачи гипертекстов) для соединения с сайтами, затребованными протоколом MSN messenger. Это ограничит возможность внешнего воздействия, поскольку анонимный доступ разрешен не ко всем сайтам, а только к использующим MSN Messenger. Но контроль доступа, основанный на пользователях/группах, будет потерян. Эту проблему легко решить, применяя клиент брандмауэра на хостах, требуя аутентификации через клиент

брандмауэра и настраивая сайты MSN (Microsoft Network, сеть Microsoft) для прямого доступа (Direct Access).

Потребуется разрешить анонимный доступ по HTTP-протоколу к следующим сайтам;

- Config. messenger. msn.com;
- Gateway.messenger.hotma il.com;
- Loginnet.passport.net;
- Loginnet.passport.com;
- 207.46.110.0/24 (this is a Subnet Network Object).

Эту информацию мы получили, просматривая записи файла регистрационного журнала в программе просмотра соединений в реальном времени (real time log viewer) консоли брандмауэра ISA. Подсеть и домены могут измениться со временем, поэтому, если правило перестанет работать, нужно проверить файлы журнала регистрации и посмотреть, какие сайты затребованы протоколом MSN Messenger.

В табл. 7.4 приведены установки в правиле доступа, разрешающем клиентам Web-прокси доступ к сайтам, использующим протокол MSN Messenger.

Табл. 7.4. Установки в правиле доступа клиентов Web-прокси по протоколу MSN Messenger

Параметр	**Значение**
Name (Имя)	MSN Messenger Web Proxy Access
Action (Действие)	Allow
Protocols (Протоколы)	HTTP and HTTPS
From/Listener (От/Приемник)	Internal
To (Кому)	Messenger Subnet
	Messenger Sites (сайты, использующие MSN Messenger)
Condition (Условие)	All Users
Purpose (Назначение)	Это правило разрешает клиентам Web-прокси доступ к сайтам, использующим протокол MSN Messenger, без необходимости аутентификации. Данное правило должно располагаться над всеми другими правилами, требующими аутентификации по протоколам HTTP и HTTPS

Изменения политики брандмауэра ISA влияют только на новые соединения

После инициации запроса клиентом брандмауэр ISA поддерживает для сеанса связи активное состояние в таблице состояния брандмауэра (firewall state table), позволяющее вернуть ответ клиенту. Активное состояние предоставляет клиенту возможность отправлять новые запросы. Брандмауэр ISA удаляет активное состояние

из таблицы состояния, если сеанс бездействует в течение точно не установленного периода времени (обычно 1-2 мин).

Например, попробуйте выполнить следующие действия.

- Откройте окно командной строки на хосте защищенной сети и проверьте дос тупность хоста через брандмауэр ISA, воспользовавшись командой «ping -n IP address». Ключ -n разрешает команде ping продолжать работу без ослабления в течение вашего теста. После завершения теста команду ping можно остановить комбинацией клавиш <CTRL>+<C>. Убедитесь, что существует правило доступа, разрешающее связать хост командой ping с хостом через брандмауэр ISA.
- В брандмауэре ISA примените запрещающее (Deny) правило к протоколу Ping и поместите его над всеми правилами, которые в данный момент разрешают выполнять команду ping через брандмауэр *ISA*.
- Команда ping будет продолжать работать, не ослабевая, даже после применения запрещающего правила. Это происходит потому, что существует запись в таб лице состояния для команды ping отданного клиента к адресу назначения.
- Откройте второе окно командной строки для того же самого клиента, связыва ющегося с удаленным хостом. Введите команду ping ко второму хосту через брандмауэр ISA. Запросы команды будут отвергнуты, поскольку в таблице состо яния нет записи для протокола этой команды ping от данного хоста к хосту-адресату.
- Если вы попытаетесь связать с хостом другого клиента командой ping, ей будет отказано в доступе.

Правила доступа начинают действовать немедленно для *новых* соединений, как только вы щелкнете мышью кнопку **Apply** (Применить), чтобы сохранить изменения и обновить политику брандмауэра. Для того чтобы применить сделанные изменения ко всем существующим соединениям, следует выполнить следующие шаги.

- Прервите существующие сеансы связи на вкладке **Sessions** (Сеансы связи) узла **Monitoring** (Мониторинг). Для разрыва соединения откройте консоль управ ления **Microsoft Internet Security and Acceleration Server 2004** (Сервер за щищенного быстрого доступа к сети Интернет 2004) и щелкните кнопкой мыши узел **Monitoring,** щелкните мышью вкладку **Sessions** на средней панели, щелк ните мышью сеанс связи, который вы хотите прервать, а затем щелкните мы шью **Disconnect Session** (Разорвать сеанс связи) на вкладке **Tasks** (Задачи).
- Другой способ — перезапуск службы Microsoft Firewall. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** щелкните кнопкой мыши узел **Monitoring,** щелкните мышью вкладку **Services** (Службы), щелкни те мышью службу **Microsoft Firewall,** на вкладке **Tasks** (Задачи) щелкните кноп кой мыши **Stop Selected Service** (Остановить выбранную службу), а затем на этой же вкладке щелкните кнопкой мыши **Start Selected Service** (Запустить выбранную службу).

Создание и конфигурирование трехадаптерной сети DMZ с общедоступными адресами

Одно из значительных улучшений брандмауэра ISA Server 2004 по сравнению с брандмауэром ISA Server 2000 — возможность функционирования в разнородных сетях (multinetworking). Как обсуждалось в главе 4, эта способность определяется тем, как брандмауэр ISA Server 2004 «воспринимает окружающее», В отличие от брандмауэра ISA Server 2000, который «делит мир» на «доверенные и не заслуживающие доверия» (основанные на таблице локальных адресов (LAT) и "не базирующиеся на таблице LAT соответственно (not-LAT)), брандмауэр ISA Server 2004 считает все сети не заслуживающими доверия и применяет политику брандмауэра ко всем соединениям, установленным через брандмауэр ISA Server 2004, включая хосты, соединяющиеся через клиенты VPN (Virtual Private Network, виртуальная частная сеть) удаленного доступа или шлюзовое подключение VPN.

Функционирование ISA Server 2004 в разнородных сетях позволяет соединять различные интерфейсы (или многочисленные виртуальные интерфейсы с помощью тегирования (сопровождения данных тегами) VLAN (virtual LAN, виртуальная локальная сеть)) и полностью контролировать трафик между сетями, соединенными брандмауэром ISA Server 2004. Подобная модель резко отличается от сетевой модели ISA Server 2000, в которой трафик между внутренними сетями не доступен политике брандмауэра и необходимо создавать «свою защитную зону», используя фильтры пакетов RRAS (Routing and Remote Access Service, сервис маршрутизации и удаленного доступа).

В этом разделе мы рассмотрим, как опубликовать хосты на сегменте DMZ с общедоступными адресами. Как вы помните, ISA Server 2000 требовал применения общедоступных или открытых адресов в сегменте DMZ. Сегмент DMZ брандмауэра ISA Server 2000 должен был использовать общедоступные адреса или адреса интернет-пространства; не было возможности применять частные адреса, поскольку брандмауэр ISA Server 2000 прокладывал маршрут (вместо применения средств преобразования сетевых адресов, NAT) для соединений с сегментом DMZ трехадаптерной защитной сети, используя простые, отслеживающие соединения пакетные фильтры (stateful packet filters) (как традиционный брандмауэр, фильтрующий пакеты). Брандмауэр ISA Server 2004 предоставляет возможность решить, как устанавливать соединения между любыми двумя сетями, определяя маршрут или используя средства NAT.

Применение общедоступных адресов иногда необходимо, если установлен сегмент DMZ с многочисленными хостами, использующими общедоступные адреса, и при этом нежелательно менять схему адресации из-за дополнительных накладных расходов, связанных с внесением соответствующих изменений в общедоступный сервер имен доменов (DNS). Требуется использовать текущую схему IP-адресации на серверах, чтобы интернет-хосты получали доступ к серверам DMZ, применяя те же адреса (в действительности, те же самые DNS-отображения), которые исполь-

зовались раньше. Это можно сделать с помощью брандмауэра ISA Server 2004, настроив маршрутную связь между Интернетом и сегментом DMZ, содержащим серверы, которые нужно «опубликовать» в сети.

Обратите внимание на то, что слово «опубликовать» заключено в кавычки. Для этого есть причина. Политика брандмауэра ISA предоставляет два метода, которые можно использовать для контроля трафика, проходящего через брандмауэр: правила доступа и правила публикации. Правила доступа могут участвовать в связях, устанавливаемых как с помощью маршрута, так и с помощью средств NAT. Правила публикации всегда преобразуют сетевые адреса для установки соединения, даже если используется сегмент с общедоступными адресами и есть маршрутная связь между хостом-источником и хостом-адресатом.

Приведенные объяснения могут сбить с толку, особенно если пользователь привык к принятому в ISA Server 2000 способу, который требует обязательного преобразования сетевых адресов (т. е. применения средств NAT) для соединения не заслуживающих доверия и доверенных хостов. Прежде чем углубиться в подробности публикации серверов в сегменте с общедоступными адресами, рассмотрим некоторые особенности новой сетевой модели брандмауэра ISA.

На рис. 7.31 показан пример сети, который мы будем использовать в поясняющей части раздела. На рисунке показана маршрутная связь между Интернетом и сегментом DMZ. Когда клиент-«карманный» PC-компьютер PDA (Personal Digital Assistant, «карманный» компьютер, предназначенный для выполнения некоторых специальных функций) соединяется с сервером сегмента DMZ, имя, которое он использует для подключения, преобразуется в действительный IP-адрес DMZ-хоста, в нашем случае 172.16.0.2. Маршрутная связь позволяет сделать это и сохранить существующие записи DNS, отображающие DMZ-хост В его действительный IP-адрес. Применение правил доступа ISA Server 2004 делает DMZ-хост доступным для интернет-клиентов.

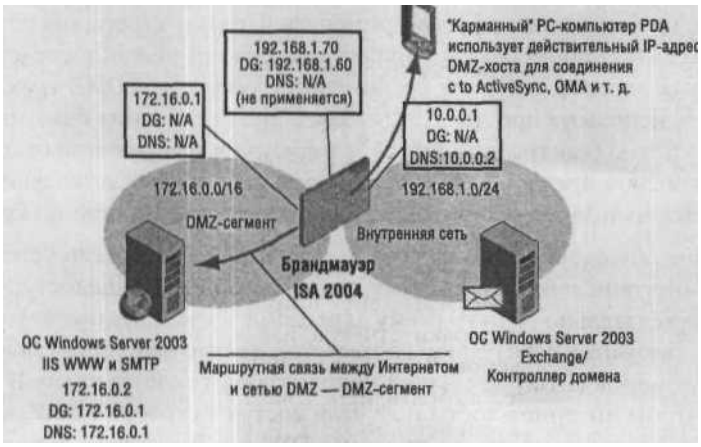
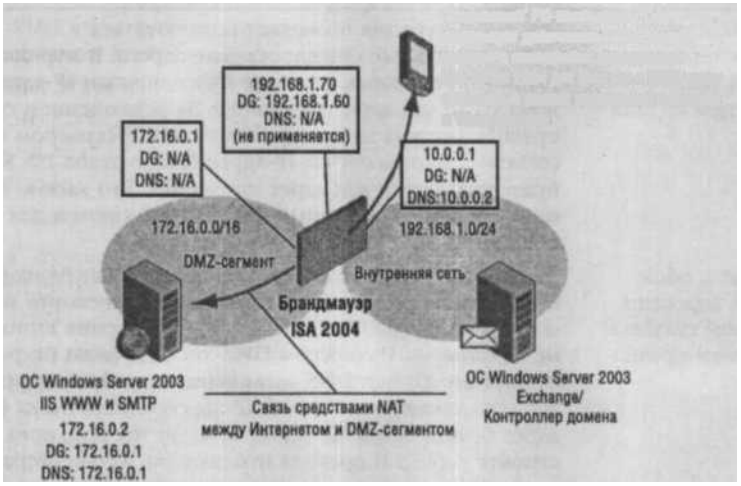


Рис. 7.31. Пример сегмента DMZ, использующего общедоступный адрес

Сделать доступным для пользователей Интернета хост сегмента DMZ, использующего общедоступный адрес, можно и с помощью правил публикации. В данном случае карманный PC-компьютер PDA, хост сети Интернет, применяет IP-адрес во *внешнем интерфейсе* брандмауэра ISA для доступа к DMZ-хосту, как показано на рис. 7.32. Обратите внимание, что у DMZ-хоста по-прежнему общедоступный адрес. Не смотря на то, что мы используем общедоступные адреса, выполняется преобразование сетевых адресов (NAT), поскольку мы применяем правило публикации. Это позволяет интернет-хосту соединиться с IP-адресом через внешний интерфейс брандмауэра ISA и эффективно *спрятать* IP-адрес DMZ-хоста. Подобное *NAT-сокрытие (NAT hiding)* — обычная мера защиты для общедоступных серверов.



"Карманный" PC-компьютер PDA использует действительный IP-адрес внешнего интерфейса брандмауэра ISA Server SOM для доступа к DMZ-хосту с помощью правил публикации серверов и Web-серверов

Рис. 7.32. Общедоступная сеть позволяет выполнять NAT-сокрытие

Обратите внимание, что на рис. 7.31-7.32 IP-адрес использовался DMZ-хостом как адрес сервера DNS. Адрес **172.16.0.1** — это IP-адрес интерфейса DMZ. Причина применения IP-адреса вместо дейст ви тельного адреса сервера DNS состоит в том, что мы публикуем DNS-сервер во внутренней сети. Правило публикации DNS-сервера ожидает (прослушивает) IP-адрес в DMZ-интерфейсе. Вы познакомитесь с подробностями этой конфигурации позже в этом разделе.

Один из главных недостатков сценариев Web-публикации ISA Server 2000 заключался в том, что IP-адрес брандмауэра ISA Server 2000 всегда получался в журналах регистрации публикуемых Web-серверов. Это существенная проблема для организаций, вложивших большие суммы денег в программное обеспечение анализа журналов регистрации и подготовки отчетов, извлекающее информацию из журналов регистрации Web-серверов. В ISA Server 2004 учтена эта проблема, и новая версия брандмауэра позволяет выбрать, передавать ли опубликованному Web-серверу исходный адрес клиента или использовать IP-адрес брандмауэра ISA. Это спра-

ведливо для правил публикации в сетях DMZ, применяющих общедоступные и частные адреса, для обоих типов правил публикации: как для Web-серверов, так и для серверов.

В табл. 7.5 описывается поведение брандмауэра ISA, разрешающее удаленный доступ к сегментам DM2 с использованием общедоступного адреса и частных адресов.

Табл. 7.5. Удаленный доступ к DMZ-серверу с применением частных или общедоступных адресов, средств NAT или маршрута, правил доступа и правил публикации

Схема адресации — Маршрутная связь — Тип правила	Результат и объяснение
Сегмент DMZ с общедоступными адресами, маршрутной связью и с применением правил доступа	Эта **конфигурация позволяет** подключаться к DMZ-хостам, используя реальные общедоступные адреса. В журналах регистрации публикуемых серверов будет показан **IP-адрес** удаленного хоста как адрес источника. За исключением создания правила доступа для соединения с HTTP-се рве ром в DMZ-сегменте. В этом случае IP-адрес брандмауэра ISA Server 2004 будет появляться как адрес источника. Это можно исправить, если сделать **недоступным** фильтр Web-прокси для данного правила
DMZ-сегмент с общедоступными адресами и маршрутной связью и *с* применением правил публикации"	Эта конфигурация требует соединения с опубликованным DMZ-хостом по IP-адресу, связанному с внешним интерфейсом брандмауэра ISA Server 2004. Соединения выполняются не с реальным IP-адресом DMZ-хоста, и ваши открытые или публичные записи DNS, возможно, потребуют корректировки для отражения этого факта. IP-адресом источника будет IP-адрес брандмауэра ISA Server 2004 до тех пор, пока вы не настроите сервер и правила публикации Web-сервера для пересылки IP-адреса источника (у вас есть выбор между пересылкой на опубликованный сервер исходного IP-адреса клиента или IP-адреса брандмауэра ISA Server 2004)
Сегмент DMZ с общедоступными адресами, использующий для связи средства NAT и применяющий правила доступа	Эта конфигурация требует соединения с опубликованным DMZ-хостом по IP-адресу, связанному с внешним интерфейсом брандмауэра ISA Server 2004. Соединения выполняются не с реальным IP-адресом DMZ-хоста и ваши открытые или публичные записи DNS, возможно, потребуют корректировки для отражения этого факта. IP-адресом источника будет IP-адрес брандмауэра ISA Server 2004 до тех пор, пока вы не настроите сервер и правила публикации Web-сервера для пересылки IP-адреса источника (возможен выбор между пересылкой на опубликованный сервер исходного IP-адреса клиента или IP-адреса брандмауэра ISA Server 2004). В результате этот вариант подобен предыдущему

Табл. 7.5. (окончание)

Схема адресации — Маршрутная связь — Тип правила	Результат и объяснение
DMZ-сегмент с общедоступными адресами, использующий для связи средства NAT и применяющий правила публикации"	Эта конфигурация требует соединения с опубликованным DMZ-хостом по IP-адресу, связанному с внешним интерфейсом брандмауэра ISA Server 2004. Соединения выполняются не с реальным IP-адресом DMZ-хоста, и ваши открытые или публичные записи DNS, возможно, потребуют корректировки для отражения этого факта. IP-адресом источника будет IP-адрес брандмауэра ISA *Server* 2004 до тех пор, пока вы не настроите сервер и правила публикации Web-сервера для пересылки IP-адреса источника (у вас есть выбор между пересылкой на опубликованный сервер исходного IP-адреса клиента или IP-адреса брандмауэра ША Server 2004). *Звучит* похоже?
DMZ-сегмент с частными адресами, использующий для связи средства NAT и применяющий правила публикации"	Эта конфигурация требует соединения с опубликованным DMZ-хостом по IP-адресу, связанному с внешним интерфейсом брандмауэра ISA Server 2004. Соединения выполняются не с реальным IP-адресом DMZ-хоста, *и* ваши открытые или публичные записи DNS, возможно, потребуют корректировки для отражения этого факта. IP-адресом источника будет IP-адрес брандмауэра ISA Server 2004 до тех пор, пока вы не настроите сервер и правила публикации Web-сервера для пересылки IP-адреса источника (у вас есть выбор между пересылкой на опубликованный сервер исходного IP-адреса клиента или IP-адреса брандмауэра ISA Server 2004). То же самое, что и в двух предыдущих вариантах

' Обратите внимание, что во всех конфигурациях с применением правил публикации соединение устанавливается средствами NAT. Ни при каких обстоятельствах не задается маршрут для соединения, если используются правила публикации Web-серверов или серверов.

Есть несколько интересных результатов, зависящих от того, разрешен или заблокирован фильтр Web-прокси в правиле доступа. Мы рассмотрим их позже в этом разделе.

В заключение обсуждения следует упомянуть, что в некоторых сценариях степень защиты снижается, если для разрешения доступа к DMZ-хостам использовать правила доступа вместо правил публикации, в этих случаях брандмауэр ISA обеспечивает чуть больше защиты, чем традиционный брандмауэр с фильтрацией пакетов. Можно предпочесть применение правил публикации по следующим причинам. ■

Правила Web-публикации серверов позволяют запретить пользователям применять IP-адреса вместо полностью определенных имен доменов (Fully Qualified Domain Name, FQDN) для доступа к ресурсам DMZ-хоста. Множество вирусов-червей (worms) атакуют серверы, базирующиеся на IP-адресах, и редко используют полностью определенные имена доменов.

- Правила Web-публикации серверов позволяют настроить пользовательские Web-приемники (Web listeners), обеспечивающие такие функциональные возможности, как основанная на формах аутентификация в Exchange, делегирование базовой аутентификации (delegation of basic authentication) и аутентификация SecurID с применением алгоритма шифрования открытым ключом (RSA).
- Правила Web-публикации серверов позволяют выполнять стыковку SSL к SSL (Secure Sockets Layer, протокол защищенных сокетов), мешающую злоумышленникам использовать в своих целях туннель SSL. При использовании моста от SSL к SSL брандмауэр ISA Server 2004 «разворачивает» SSL-туннель, проверяет соединение собственными серьезными, отслеживающими состояние соединения, средствами контроля прикладного уровня и разрывает соединения, содержащие следы действий злоумышленников и имеющие подозрительные характеристики. Соединения, кажущиеся безопасными, затем снова кодируются и отправляются на опубликованный Web-сервер через вторую SSL-ссылку, которая создается между брандмауэром ISA Server 2004 и опубликованным Web-сервером.
- Правила Web-публикации серверов подвергают входящие соединения обработке с помощью фильтров прикладного уровня, предназначенных для защиты определенных сервисов. Примерами могут служить SMTP-фильтр, блокирующий атаки переполнения буфера, DNS-фильтр, запрещающий ряд DNS-атак, и POP3-фильтр, препятствующий переполнению буфера POP3 (Post Office Protocol v. 3, почтовый протокол Интернета). Если используются правила доступа для публикации хоста DMZ-сегмента, применяющего общедоступные адреса, то фильтры прикладного уровня не защитят от перечисленных атак.
- Хотя Web-сервер с общедоступным адресом публикуется в DMZ-сегменте с помощью правил доступа, тем не менее защита обеспечивается фильтром защиты HTTP. Этот фильтр обеспечивает очень серьезную проверку прикладного уровня для всех HTTP-соединений, проходящих через брандмауэр ISA Server 2004. Фильтр защиты HTTP предоставляет возможность детального контроля и может быть сконфигурирован для отдельного правила, таким образом отсутствует привязка к единой политике фильтра защиты HTTP для всех правил брандмауэра ISA Server 2004. Это существенный шаг вперед по сравнению с методом URLScan фильтрования проходящих через брандмауэр HTTP-соединений, применявшимся в брандмауэре ISA Server 2000 для контроля состояние HTTP-соединения.

В оставшейся части раздела описывается применение правил доступа при публикации DMZ-хоста с общедоступным адресом. Этот способ позволяет продолжать применять общедоступный адрес, который использовался вашими серверами, и при этом не снижать мощи фильтрации прикладного уровня, полностью отслеживающей состояния соединений в брандмауэре ISA Server 2004. В отличие от традиционных брандмауэров, базирующихся на фильтрации пакетов, брандмауэр ISA выполняет отслеживающую соединения фильтрацию и контроль прикладного уровня с отслеживанием состояния соединения для всех соединений, проходящих че-

рез брандмауэр; эти средства обеспечивают наивысшую степень защиты и контроля по сравнению с любым другим брандмауэром, представленным на рынке.

Для достижения поставленной цели придется выполнить следующие шаги:

- настроить таблицу маршрутизации на маршрутизаторе, предшествующем бран дмауэру на пути потока информации;
- настроить сетевые адаптеры;
- установить программное обеспечение брандмауэра ISA Server 2004;
- установить и настроить на сервере DMZ сервисы IIS (Internet Information Services, Информационная служба Интернета) WWW и SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты);
- создать сеть DMZ;
- создать сетевые правила, действующие между сетью DMZ и внешней сетью, а также между DMZ и внутренней сетью;
- создать правило публикации сервера, разрешающее использовать DNS при со единении из DMZ с внутренней сетью;
- создать правило доступа, разрешающее использовать DNS для соединений внут ренней сети с внешней сетью;
- создать правило доступа, разрешающее HTTP-подключения из внешней сети к сети DMZ;
- создать правило доступа, разрешающее SMTP-подключения из внешней сети к сети DMZ;
- протестировать правила доступа из внешней сети к сети DMZ;
- изменить правило доступа из внешней сети к сети DMZ, сделав недоступным фильтр Web-прокси.

Настройка таблицы маршрутизации на предшествующем брандмауэру маршрутизаторе

Общая проблема, с которой сталкиваются администраторы брандмауэра ISA, соединяющие сегменты DMZ с применением общедоступных адресов, связана с записями в таблице маршрутизации на предшествующем брандмауэру маршрутизаторе. Когда создается сегмент DMZ с общедоступным адресом, необходимо выделить подсети для общедоступного блока и присвоить одну из подсетей сегменту DMZ. Затем можно связать первый допустимый адрес выделенного в подсеть блока с интерфейсом DMZ, а первый допустимый адрес другого блока подсети с общедоступным интерфейсом.

Именно в этот момент большинство администраторов сталкивается с проблемами. Необходимо настроить на предшествующем брандмауэру маршрутизаторе маршрут к сегменту DMZ. Делается это с помощью указания в маршрутизаторе IP-адреса внешнего интерфейса брандмауэра ISA Server 2004 как адреса шлюза для

сетевого идентификатора (ID) сегмента DMZ. Если эта запись пропущена в таблице маршрутизации предшествующего маршрутизатора, то никакие первичные входящие соединения и отклики на входящие соединения, приходящие на сегмент DMZ и отправляемые с него, не будут функционировать.

В используемом примере этого раздела у хоста внешней сети тот же самый сетевой идентификатор, что и у внешнего интерфейса брандмауэра ISA, равный 192.168.1.0/24. Внешний IP-адрес в брандмауэре ISA — 192.168.1.70 и внешний хост будет использовать IP-адрес, присвоенный в той же подсети (тот же сетевой ID). Сегмент DMZ использует сетевой ID 172.16.0.0/16. Таким образом, для хоста внешней сети с ОС Windows XP, который применяется в этом разделе, в записи таблицы маршрутизации мы указали на необходимость использования внешнего IP-адреса брандмауэра ISA Server 2004 для соединения с подсетью, имеющей сетевой ID, равный 172.16.0.0/16. Далее показано, что именно мы сделали:

```
route add 172.16.0.0 MASK 255.255.0.0 192.168.1.70
```

Обратите внимание, что в этом примере не применяется подсеть блока эбщедоступных адресов (public address block). В вашей производственной среде вам нужно выделить в подсеть блок, использующий общедоступные адреса, и создать для вашего выделенного в подсеть сегмента DMZ запись в таблице маршрутизации маршрутизатора, предшествующего брандмауэру ISA Server 2004. Это означает, что осуществляется контроль через предшествующий маршрутизатор, который делает сегменты DMZ спорной областью для учетных записей, предоставляемых непрофессиональными ISP (Internet Service Provider, поставщик услуг Интернета). Но ничто не мешает создать сегменты DMZ с частным адресом непрофессионального ISP.

Конфигурирование сетевых адаптеров

Конфигурация сетевого адаптера всегда была спорным вопросом для администраторов ISA Server 2000 и, вероятно, будет им оставаться. Для этого есть ряд причин, первая из которых связана с тем, поддерживаются собственные сервисы DNS или нет.

DNS — важный вопрос для брандмауэра ISA, поскольку брандмауэр может выполнять разрешение имен прокси для клиентов Web-прокси и клиентов брандмауэра. Брандмауэр ISA использует DNS-установки своих сетевых адаптеров для запроса подходящего DNS-сервера. Если конфигурация DNS-сервера некорректна, то это приведет к медленному разрешению имен или полному его отсутствию, что создаст у конечного пользователя представление о том, что «брандмауэр ISA не работает».

Корректную конфигурацию DNS на брандмауэре ISA можно определить, используя следующие общие рекомендации.

- Если во внутренней сети имеется DNS-сервер, то его нужно настроить для поддержки разрешения имен интернет-хостов.

- Если принято решение не разрешать DNS-серверу во внутренней сети выполнять разрешение имен интернет-хостов, то необходимо поместить на брандмауэр ISA или в сегмент DMZ только кэширующий DNS-сервер.
- Если выбрано размещение в сегменте DMZ DNS-сервера, наделенного полномочиями для общедоступных доменов, не разрешайте этому серверу участвовать *в* DNS-разрешении имен. Это означает, что наделенный полномочиями DNS-сервер должен только отвечать на запросы для поддерживаемых доменов и возвращать ошибку пользователям, пытающимся разрешать другие имена с помощью этого сервера.
- Если нежелательно поддерживать собственные DNS-серверы и при этом не используется DNS-сервис во внутренней сети, нужно настроить брандмауэр ISA на применение общедоступного DNS-сервера, такого как DNS-сервер, предлагаемый провайдером интернет-услуг. Следует иметь в виду, что такая конфигурация вызовет проблемы с разрешением имен для хостов внутренней сети и также может вызвать проблемы с клиентскими соединениями Web-прокси и брандмауэра. По этой причине следует выбрать другой брандмауэр для рабочей среды SOHO (Small Office/Home Office, класс программного обеспечения, предназначенного для малого или домашнего офиса), не имеющей установленной DNS-инфраструктуры. Однако в рабочей среде малого офиса или домашнего офиса при наличии DNS-сервера брандмауэр ISA — идеальный выбор для защиты информационных активов компании.
- Никогда не указывайте общедоступный адрес DNS-сервера в установочных параметрах сетевого адаптера, в настройках которого задан частный адрес DNS-сервера!
- Адрес DNS-сервера должен быть задан в интерфейсе, указанном первым в списке окна **Network and Dial-up Connections** (Сетевые подключения). Например, если имеется трехадаптерный брандмауэр ISA и интерфейс DMZ, внутренний интерфейс и общедоступный интерфейс, внутренний адаптер должен быть в верхней строке списка и IP-адрес DNS-сервера должен быть задан в этом интерфейсе. Это справедливо при использовании внутреннего DNS-сервера, DNS-сервера в сегменте DMZ или общедоступного DNS-сервера, такого как DNS-сервер вашего провайдера интернет-услуг.

Если приведенные правила покажутся непонятными, проконсультируйтесь со специалистом. DNS-установки важны: если на брандмауэре DNS-конфигурация некорректна, то возможно возникновение коммуникационных проблем, которые трудно будет устранить, и у пользователя может сложиться неверное представление о неработоспособности брандмауэра ISA.

СОВЕТ Определитесь с DNS-конфигурацией перед публикацией в Интернете ваших серверов сегмента DMZ, использующего общедоступные адреса.

Установка программного обеспечения ISA Server 2004

После того, как ситуация с DNS разрешена и сетевые интерфейсы брандмауэра ISA Server 2004 настроены должным образом — все готово к установке программного обеспечения брандмауэра ISA Server 2004. Так как теперь поздно говорить людям: «пожалуйста, посмотрите такую-то инструкцию» ([потом]у что вы потеряете много времени, пытаясь понять, как инструкции решают конкретную возникшую проблему), в данном случае мы сошлемся на главу 5, в которой описывается установка брандмауэра ISA.

Установка и настройка сервисов IIS WWW и SMTP на DMZ-сервере

В этом разделе мы поместим машину с ОС Windows Server 2003 в сегмент DMZ с применением общедоступных адресов. На компьютере будет установлен сервис IIS 6.0 WWW (W3SVC) и сервис IIS 6.0 SMTP. Мы опубликуем оба эти сервиса в Интернете с помощью правил доступа. В вашей рабочей сети вы установите и настроите сервисы, которые нужны вам; к ним могут относиться: внешний Exchange Server publishing OWA (Outlook Web Access, Web-доступ через Outlook), OMA (Object Management Architecture, архитектура объектного управления), ActiveSync (программа для синхронизации и взаимодействия настольного компьютера с карманным компьютером), RPC over HTTP (удаленный вызов процедуры по протоколу HTTP) и другие сервисы.

Хост в сегменте DMZ использует IP-адрес, годный для вашего блока подсети, применяемого в сегменте DM2. Опубликованный DMZ-хост использует IP-адрес DMZ-интерфейса в брандмауэре ISA Server 2004 в качестве его шлюза по умолчанию. DMZ-хост не применяет IP-адрес внутренней сети как его шлюз по умолчанию, потому что у него нет доступа к адресам внутренней сети, пока мы не предоставим ему такой доступ, чего мы делать не собираемся.

Адрес DNS-сервера в сетевом адаптере DMZ-хоста будет равен IP-адресу DMZ-интерфейса в брандмауэре ISA. Мы используем эту конфигурацию, поскольку будем настраивать средства NAT для связи между сегментом DMZ и внутренней сетью, и правило публикации сервера, которое публикует DNS-сервер по IF-адресу DMZ-интерфейса.

DNS-сервер внутренней сети настроен на разрешение имен интернет-хостов. Это полезно, если желательно использовать SMTP-сервер в сегменте DMZ как исходящий SMTP-ретранслятор (SMTP relay). SMTP-ретранслятор должен быть способен разрешать имя домена MX (mail exchange, обмен почтовой корреспонденцией) для каждого исходящего сообщения электронной почты, и для этого может использовать DNS-сервер во внутренней сети.

Создание сети DMZ

После завершения настройки DMZ-сервера можно вызвать на экран консоль управления ISA Server 2004 и создать правила, чтобы все заработало. Первый шаг — создание сети DMZ. Брандмауэру ISA нужно знать IP-адреса, используемые в сети, и маршрутную связь, которую ему следует применить для соединения с любой другой сетью. В нашем примере, сеть DMZ мы назовем **DMZ** и присвоим ей диапазон IP-адресов для ее сетевого идентификатора (network ID). В конкретной рабочей сети необходимо включить все IP-адреса в блоке подсети, созданном для сегмента DMZ.

ПРЕДУПРЕЖДЕНИЕ Возможно, вы заметили, что брандмауэр ISA поставляется с несколькими шаблонами сети (Network Templates), существенно упрощающими конфигурирование трехадаптерной сети DMZ. Однако мы советуем отказаться от использования этих шаблонов, поскольку в них сделаны допущения о маршрутной связи между сетями и требуется настроить политики доступа брандмауэра, которые не очень хорошо описаны и не слишком понятны большинству администраторов ISA Server 2004. Мы уже сталкивались со множеством конфигураций сети и проблем выявления неисправностей, связанных с применением сетевых шаблонов. Этих проблем можно избежать, если вручную настроить брандмауэр. Отказавшись от применения сетевых шаблонов, вы будете уверены в том, что создана безопасная конфигурация и что эта конфигурация брандмауэра и его политики доступа в точности такие, какими они, по вашему мнению, должны быть.

Выполните следующие шаги для создания сети DMZ.

- На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и узел **Configuration** (Конфигурация). Щелкните кнопкой мыши узел **Networks** (Сети).
- В узле **Networks** щелкните кнопкой мыши вкладку **Networks** на панели **Details** (Подробности) консоли. На вкладке **Tasks** (Задачи) щелкните кнопкой мыши ссылку **Create a New Network** (Создать новую сеть).
- На странице **Welcome to the New Network Wizard** (Вас приветствует мастер создания новой сети), показанной на рис. 7.33, введите название сети в текстовое поле **Network name** (Имя сети). В нашем примере мы назовем сеть **DMZ.** Щелкните мышью кнопку **Next** (Далее).
- На странице **Network Type** (Тип сети) выберите вариант **Perimeter Network** (Сеть периметра). Щелкните мышью кнопку **Next** (Далее).
- На странице **Network Addresses** (Адреса сети) щелкните мышью кнопку **Add Adapter** (Добавить адаптер).

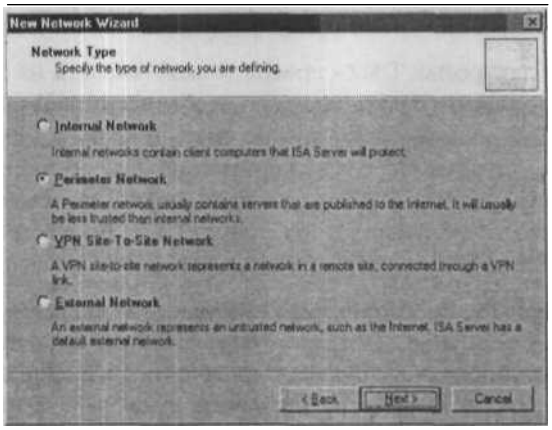


Рис. 7.33. Мастер New Network Wizard

В диалоговом окне **Select Network Adapters** (Выберите сетевые адаптеры), показанном на рис. 7.34, выберите сетевой интерфейс **DMZ** и установите флажок для этого интерфейса. Имейте в виду, что можно установить флажок без предварительного выбора интерфейса. Но если не выбрать интерфейс, то не будет видна корректная информация **Network Interface Information** (Сведения о сетевом интерфейсе) в нижней части диалогового окна. Щелкните мышью кнопку OK.

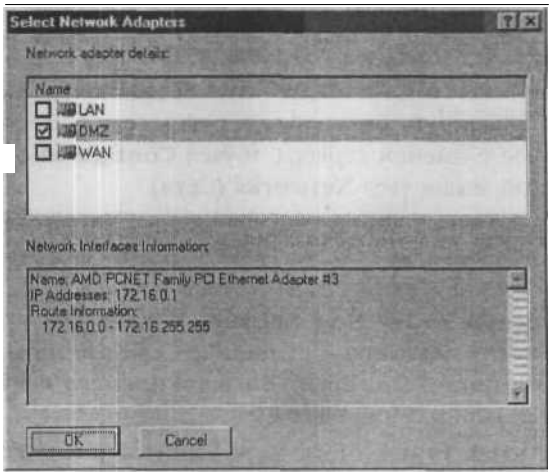


Рис. 7.34. Диалоговое окно Select Network Adapters (Выберите сетевые адаптеры)

- Щелкните мышью **кнопку Next** (Далее) на странице **Network Addresses** (Адреса сети).

■ Проверьте сделанные установки на странице **Completing the** New **Network Wizard** (Завершение мастера создания новой сети) и щелкните мышью кнопку **Finish** (Готово).

Создание сетевых правил для связи между DMZ и внешней сетью и DMZ и внутренней сетью

Теперь, когда сеть DMZ определена, нужно настроить маршрутные связи между сетью DMZ, внутренней сетью и Интернетом (который является внешней сетью, этот термин применяется к любой сети, для которой мы не определили характеристики сети).

В нашем примере мы хотим установить маршрутную связь между сетью DMZ и Интернетом и связь средствами NAT (network address translation, преобразование сетевых адресов) между сетью DMZ и внутренней сетью. Это позволит применять правила доступа для разрешения внешним хостам обращаться к сегменту DMZ и правило публикации сервера для сокрытия IP-адреса DNS-сервера во внутренней сети. Имейте в виду, что даже если мы используем маршрутную связь между сетью DMZ и внутренней сетью, в с е равно можно создать правило публикации сервера (Server Publishing Rule) для разрешения доступа DMZ-хоста к DNS-серверу во внутренней сети. Важно применять правило публикации сервера вместо правила доступа, для того чтобы DNS-фильтр мог защитить DNS-сервер во внутренней сети.

Выполните следующие шаги для создания сетевого правила, управляющего маршрутной связью между сетью DMZ и Интернетом.

1. В узле **Networks** (Сети), расположенном на левой панели консоли, щелкните кнопкой мыши вкладку **Network Rules** (Сетевые правила) на панели **Details** (Подробности). Щелкните кнопкой мыши ссылку **Create a New Network Rule** (Создать новое сетевое правило) на вкладке **Tasks** (Задачи), расположенной на панели задач.
2. На странице **Welcome to the New Network Rule Wizard** (Вас приветствует ма стер создания нового сетевого правила) введите название правила в текстовое поле **Network rule name** (Название сетевого правила). В этом примере мы назовем сетевое правило **DMZOExternal.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Network Traffic Sources** (Источники сетевого трафика) щелкни те мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и затем дважды щелкните сеть **DMZ.** Щелкните мышью кнопку **Close** (Закрыть).
5. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Sources** (Источники сетевого трафика).
6. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелк ните мышью кнопку **Add** (Добавить).

7. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и затем дважды щелкните сеть **External** (Внешняя). Щелкните мышью кнопку **Close** (Закрыть).
   - о Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Destinations** (Адресаты сетевого трафика), о На странице **Network Relationship** (Связь сетей) выберите вариант **Route** (Маршрут) и щелкните мышью кнопку **Next** (Далее).
   - о Проверьте ваши установки на странице **Completing the New Network Wizard** (Завершение мастера создания нового сетевого правила) и щелкните мышью кнопку **Finish** (Готово).

Следующий шаг — создание маршрутной связи между сетью DMZ и внутренней сетью. В данном случае мы будем использовать средства преобразования сетевых адресов для задания маршрута между сетью DMZ и внутренней сетью.

Выполните следующие шаги для создания средствами NAT маршрутной связи между сетью DMZ и внутренней сетью.

1. В узле **Networks** (Сети), расположенном на левой панели консоли, щелкните кнопкой мыши вкладку **Network Rules** (Сетевые правила) на панели **Details** (Подробности). Щелкните кнопкой мыши ссылку **Create a New Network Rule** (Создать новое сетевое правило) на вкладке **Tasks** (Задачи), расположенной на панели задач.
2. На странице **Welcome to the New Network Rule Wizard** (Вас приветствует ма стер создания нового сетевого правила) введите название правила в текстовое поле **Network rule name** (Название сетевого правила). В этом примере мы назовем сетевое правило **DMZOInternal.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Network Traffic Sources** (Источники сетевого трафика) шелкните мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и затем дважды щелкните сеть **Internal.** Щелк ните мышью кнопку **Close** (Закрыть).
5. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Sources** (Источники сетевого трафика).
6. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелк ните мышью кнопку **Add** (Добавить).
7. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и затем дважды щелкните сеть **DMZ.** Щелкните мышью кнопку **Close** (Закрыть).
8. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Destina tions** (Адресаты сетевого трафика).

9. На странице **Network** Relationship (Связь сетей) выберите вариант **Route** (Маршрут) и щелкните мышью кнопку **Next** (Далее).

Проверьте ваши установки на странице **Completing the New Network Wizard** (Завершение мастера создания нового сетевого правила) и щелкните мышью кнопку **Finish** (Готово).

Создание правила публикации сервера, разрешающего использование DNS в соединениях сегмента DMZ с внутренней сетью

DMZ-хосту может понадобиться разрешение имен интернет-хостов. Такая ситуация возникает каждый раз, когда DMZ-хост нуждается в установке новых исходящих соединений с серверами в сети Интернет, базирующихся на имени хоста-адресата. Примером может служить SMTP-ретранслятор (SMTP relay) в сегменте DMZ, применяемый для ретрансляции исходящей почты вашей организации.

Мы используем правило публикации в этом примере для того, чтобы применить с помощью DNS-фильтра защиту соединений DMZ-хоста с DNS-сервером во внутренней сети.

Выполните следующие шаги для создания правила публикации сервера.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). На панели задач щелкните вкладку **Tasks** (Задачи) и затем *ссылку* **Create a New Server Publishing Rule** (Создать новое правило публикации).
2. На странице **Welcome to the New Server Publishing Rule Wizard** (Вас приветствует мастер создания нового правила публикации сервера), показанной на рис. 7.35, введите название правила в текстовое поле **Server publishing rule name** (Название правила публикации сервера). В этом примере мы назовем правило **Publish Internal DNS Server.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Select Server** (Выберите сервер) введите IP-адрес DNS-сервера, находящегося во внутренней сети. В этом примере IP-адрес DNS-сервера внутренней сети равен **10.0.0.2.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Select Server** (Выберите сервер) выберите протокол **DNS Server** в списке выбранных протоколов. Щелкните мышью кнопку **Next** (Далее).
5. На странице **IP Addresses** (IP-адреса) установите флажок **DMZ.** Это интерфейс, в котором правило публикации сервера будет ожидать запросы на входящие соединения с DNS-сервером внутренней сети. Щелкните мышью кнопку **Next** (Далее).
6. Проверьте сделанные установки на странице **Completing the New Server Publishing Rule** (Завершение создания нового правила публикации сервера) и щелкните мышью кнопку **Finish** (Готово).

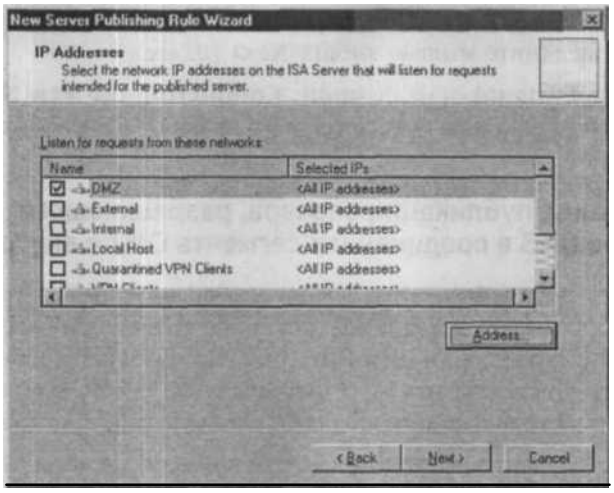


Рис. 7.35. Мастер New Server Publishing Rule Wizard

Создание правила доступа, разрешающего использование DNS в соединениях внутренней сети с внешней сетью

DNS-сервер внутренней сети должен иметь право запрашивать DNS-сервер в Интернете для разрешения имен интернет-хостов. Можно создать правило DNS-доступа, разрешающее DNS-серверу внутренней сети запрашивать DNS-серверы в Интернете по DNS-протоколу.

Выполните следующие шаги для создания правила DNS-доступа для DNS-сервера.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), расположенный на левой панели консоли.
2. На панели задач щелкните кнопкой мыши вкладку **Tasks** (Задачи) и затем ссылку **Create a New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В этом примере мы назовем правило **Outbound DNS Internal DNS Server.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** *(Это* правило применяется к). Щелкните мышью кнопку **Add** (Добавить).

6. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **Common Protocols** (Общие протоколы) и затем дважды щелкните элемент **DNS.** Щелкните мышью **кнопку Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью кнопку **New** (Новый), затем элемент **Computer** (Компьютер).
10. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите имя компьютера в текстовое поле **Name** (Имя). В этом при мере мы введем имя **Internal DNS Server.** В текстовое поле **Computer IP Address** (IP-адрес компьютера) введите IP-адрес внутреннего DNS-сервера, в нашем при мере **10.0.0.2.** Щелкните мышью кнопку OK.
11. Щелкните мышью папку **Computers** (Компьютеры) и дважды щелкните элемент **Internal DNS Server** (Внутренний DNS-сервер). Щелкните мышью кнопку **Close** (Закрыть).
12. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Next** (Далее).
13. На странице Access **Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add (Добавить).**
14. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети). Дважды щелкните элемент **External** (Внешняя), щелкните кнопку **Close** (Закрыть).
15. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
16. Ш странице **User Sets** (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Да лее).
17. Проверьте установки на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила доступа) и щелкните мышью кнопку **Finish** (Готово).

Создание правила доступа, разрешающего HTTP-подключение из внешней сети к сети DMZ

Следующий шаг — создание правила доступа, разрешающего HTTP-доступ из внешней сети к DMZ-хосту. Несмотря на то, что вы не получаете выигрыша от набора функциональных возможностей брандмауэра, предоставляемых правилом публикации Web-сервера, этот вариант позволяет представить действительный IP-адрес Web-севера в Интернет и продолжать обеспечивать безопасность с помощью фильтра защиты HTTP, применяемого к правилу доступа. Базовая конфигурация фильтра

защиты HTTP предоставляет хороший уровень безопасности, и кроме того вы можете настроить фильтр защиты HTTP, чтобы повысить уровень безопасности опубликованного Web-сервера, к которому применяется правило доступа.

Выполните следующие шаги для публикации вашего Web-сервера из сети DMZ с использованием правила доступа.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), расположенный на левой панели консоли, и затем щелкните ссылку **Create *a* New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) панели задач.
2. На странице Welcome **to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В этом примере мы назовем правило **Inbound to DMZ Web Server.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **Common Protocols** (Общие протоколы) и затем дважды щелкните элемент **HTTP.** Щелкните мышью кнопку Close (Закрыть).
6. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
7. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети), дважды щелкните элемент **External** (Внешняя). Щелкните мышью кнопку **Close** (Закрыть).
9. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Next** (Далее).
10. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью кнопку **New** (Новый). Щелкните элемент **Computer** (Компьютер).
12. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер), показанном на рис. 7.36, введите имя компьютера в текстовое поле **Name** (Имя). В этом примере введем имя **DMZ Web Server.** В текстовое поле **Computer IP Address** (IP-адрес компьютера) введите IP-адрес Web-сервера сети DMZ, в нашем примере 172.16.0.2. Щелкните мышью кнопку OK.

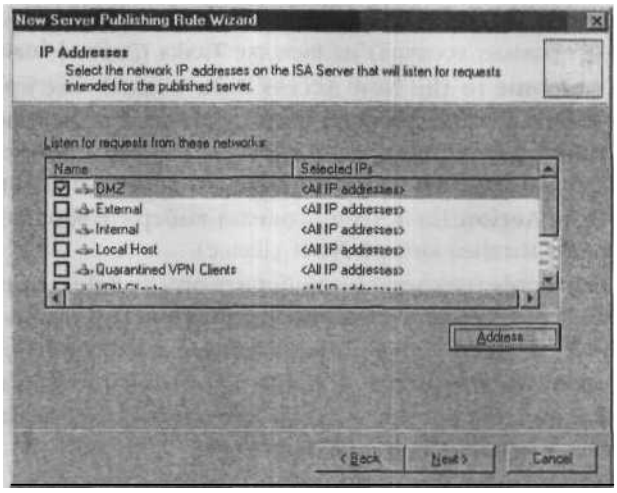


Рис. 7.36. Диалоговое окно New Computer Rule Element (Новый элемент правила, компьютер)

13-В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computers** (Компьютеры) и дважды щелкните элемент **DMZ Web Server** (Web-сервер сети DMZ). Щелкните мышью кнопку **Close** (Закрыть).

14. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).

15. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умол чанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).

16. Проверьте установки на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила доступа) и щелкните мышью кнопку **Finish** (Готово).

Создание правила доступа, разрешающего SMTP-подключение из внешней сети к сети DMZ

Теперь, когда Web-сервер опубликован, создадим другое правило, разрешающее входящий доступ к SMTP-серверу в сети DMZ. Снова воспользуемся правилом доступа. Учтите, что когда применяется правило доступа вместо правила публикации сервера, нельзя воспользоваться защитой, предоставляемой SMTP-фильтром.

Выполните следующие шаги для создания правила доступа, разрешающего входящий доступ к SMTP-серверу.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), расположенный

на левой панели консоли, затем щелкните ссылку **Create a New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) панели зада[ч].

2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В этом примере мы назовем правило **Inbound to DMZ SMTP Server.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разре шить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (П ротоколы) выберите строку **Selected protocols** (Выб ранные протоколы) из списка **This rule applies to** (Это правило применяется к), как показано на рис. 7.37, и щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью **папку Common Protocols** (Общие протоколы) и затем дважды щелкните элемент **SMTP.** Щелкните мышью кнопку **Close** (Закрыть).

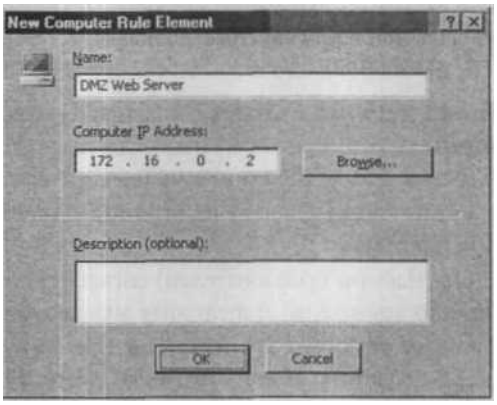


Рис. 7.37. Мастер New Access Rule Wizard

6. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
7. На странице **Access Rule Sources** (Источники **в** правиле доступа) щелкните мышью кнопку **Add** (Добавить).
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети) и дважды щелкните элемент **External** (Внешняя). Щелкните мышью кнопку **Close** (Закрыть).
9. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Next** (Далее).
10. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить).
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computers** (Компьютеры) и дважды щелкните элемент **DM.Z Web Server** (Web-сервер сети DMZ). Щелкните мышью кнопку **Close** (Закрыть).

12. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
13 На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
14. Проверьте установки на странице **Completing the** New Access **Rule Wizard** (Завершение мастера создания нового правила доступа) и щелкните мышью кнопку **Finish** (Готово).
15. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
16. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Созданная политика брандмауэра должна быть похожа на политику, показанную на рис. 7.38.

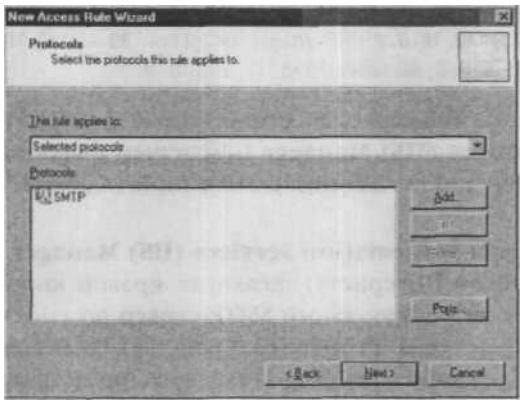


Рис. 7.38. Политика брандмауэра

Тестирование правил доступа для соединения внешней сети с сетью DMZ

Теперь мы готовы тестировать правила доступа. Далее перечислены шаги теста.

1. Откройте Web-обозреватель на внешнем хосте и введите IP-адрес Web-сервера из сети DMZ. В нашем случае IP-адрес Web-сервера из сети DMZ — **172.16.0.2,** поэтому мы введем **http://172.l6.0.2** в строку адреса в обозревателе и нажмем клавишу <ENTER>.
2. По умолчанию появляется Web-страница Web-сайта IIS (Internet Information Services, информационные сервисы Интернета). В этом примере мы не создали специальную Web-страницу по умолчанию, поэтому увидим страницу **Under Construction** (В разработке). Это доказывает, что правило доступа, разрешающее входящий доступ к Web-сайту сети DMZ, работает корректно.

3. Теперь давайте посмотрим, что показывает регистрационный журнал Web-сайта. Откройте **Windows Explorer** (Проводник) и перейдите в каталог **C:\WINDOWS\system32\LogFiles\W3SVCl.** Дважды щелкните кнопкой мыши регистрационный журнал с текущей датой. Вы увидите что-то похожее на строки, приведенные далее. Обратите внимание на элементы, выделенные жирным шрифтом. Они показывают IP-адрес источника, записанный в журнал Web-сервера. В этом примере IP-адрес источника — это IP-адрес DMZ-интерфейса компьютера, на котором находится брандмауэр ISA Server 2004. Он может быть не таким, каким вы ожидали его увидеть. Причина заключается в том, что фильтр Web-прокси автоматически связан с протоколом HTTP. Мы узнаем, как разорвать связь фильтра с протоколом, позже в этой главе.

```
«Software: Microsoft Internet Information Services 6,0
«Version: 1.0
#Date: 2004-06-18 05:47:14
2004-06-18 05:56:21 172.16.0.2 GET /iisstart.htm - 80 - 172.16.0.1 Mozilla/
4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
2004-06-18 05:56:25 172.16.0.2 GET /pagerror.gif - 80 - 172.16.0.1 Mozilla/
4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
```

4. Далее перейдите на Web-сервер в сегменте DMZ и откройте консоль **Internet Information Services (IIS) Manager** (Диспетчер информационных сервисов Интернета) из пункта меню **Administrative Tools** (Администрирование) в меню **Start** (Пуск).
5. На консоли **Internet Information Services (IIS) Manager** (Диспетчер информационных сервисов Интернета) щелкните правой кнопкой мыши **Default Virtual SMTP Server** (Виртуальный SMTP-сервер по умолчанию) и щелкните левой кнопкой строку меню **Properties** (Свойства). На вкладке **General** (Общие) установите флажок **Enable Logging** (Разрешить регистрацию). Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK.
6. На компьютере внешнего хоста откройте окно командной строки. Введите в нем команду **telnet 172.16.0.2 25** и нажмите клавишу <ENTER>.
7. Вы увидите появление баннера SMTP-сервиса. Введите команду **help** и нажмите клавишу <ENTER>. На экране появится список команд, поддерживаемых SiMTP-сервером, как показано на рис. 7.39. Введите команду **quit** для отсоединения от SMTP-сервера.

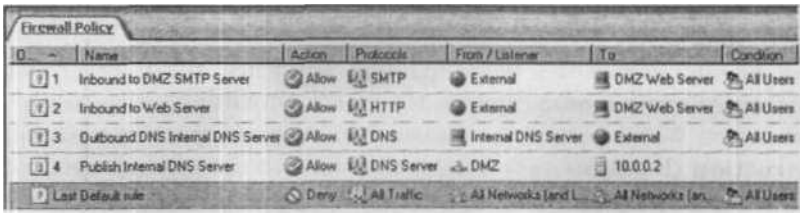


Рис. 7.39. Команды, поддерживаемые SMTP-сервером

8. Перейдите в каталог **C:\WINDOWS\system32\LogFiles\SMTPSVCl** на компьютере, служащем DMZ-хостом. Откройте журнал регистрации с текущей датой. Вы увидите строки, похожие на приведенные далее. Обратите внимание на выделенный жирным шрифтом IP-адрес. Это адрес внешнего хоста, выполнившего входящий запрос к Web-серверу в сети DMZ. В данном случае истинный IP-адрес клиента сохранен, потому что нет прикладного фильтра, представляющего соединение и заменяющего начальный IP-адрес IP-адресом брандмауэра ISA.

```
((Software:  Microsoft Internet Information Services 6.0
((Version:  1.0
#Date:  2004-06-18 06:07:22
«Fields: time c-ip cs-method cs-uri-stem sc-status
06:07:22 192.168.1.187 QUIT - 240
```

Тестирование правила DNS для соединения сегмента DMZ с внутренней сетью

С помощью процедур, описанных в предыдущем разделе, мы продемонстрировали, что правила доступа, управляющие входящим доступом из Интернета к DMZ-хосту, работают корректно. Следующий шаг — подтверждение того, что правило публикации сервера, разрешающее DMZ-хосту доступ к DNS-серверу во внутренней сети, также работает правильно.

Выполните следующие шаги для тестирования правила публикации DNS-сервера.

1. На DMZ-хосте откройте окно командной строки. В этом окне введите команду nslookup **www.hotmail.com** и нажмите клавишу <ENTER>.
2. Вы увидите результаты выполнения команды **nslookup,** которые выглядят, как показано на рис. 7.40. Обратите внимание, что первые две строки запустили правило **Publish Internal DNS Server,** а следующие строки запустили правило **Outbound DNS Internal DNS Server.** Из рис. 7.41 видно, что DMZ-хост сделал DNS-запрос к DNS-серверу во внутренней сети и этот DNS-сервер затем послал запросы DNS-серверам в Интернете для разрешения имени.

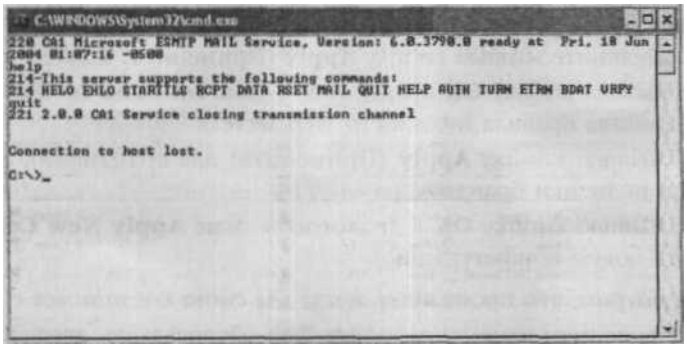
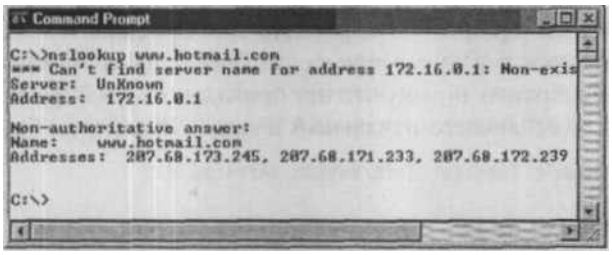


РИС. **7.40.** Результаты выполнения команды nslookup

Рис. 7.41. Строки журнала мониторинга

3. В журнале мониторинга в режиме реального времени (real time log monitcr) вы увидите строки, похожие на приведенные на рис. 7.41.



Блокирование фильтра Web-прокси, изменяющее правило доступа, разрешающее соединение внешней сети с сетью DMZ

Возможно потребуется видеть истинный IP-адрес хоста внешней сети вместо IP-адреса брандмауэра ISA Server 2004 при публикации Web-сервера с помощью правила доступа. Этого можно достичь, если заблокировать фильтр Web-прокси в свойствах правила HTTP-доступа, созданного вами ранее.

Выполните следующие шаги для блокирования фильтра Web-прокси.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа *к* сети Интернет 2004) щелкните правой кнопкой мыши правило **Inbound to Web Server** и левой кнопкой щелк ните команду **Properties** (Свойства).
2. В диалоговом окне **Inbound to Web Server Properties** (Свойства правила In bound to Web Server) щелкните кнопкой мыши вкладку **Protocols** (Протоколы).
3. На вкладке **Protocols** (Протоколы) щелкните кнопкой мыши элемент **HTTP** в списке **Protocols** (Протоколы) и кнопку **Edit** (Редактировать).
4. В диалоговом окне **HTTP Properties** (Свойства HTTP) щелкните кнопкой мыши вкладку **Parameters** (Параметры). На вкладке **Parameters** сбросьте флажок **Web Proxy Filter** (Фильтр Web-прокси) в области **Application Filters** (Прикладные фильтры). Щелкните мышью кнопку **Apply** (Применить) и затем кнопку ОК.
5. Щелкните мышью кнопку ОК в диалоговом окне **Inbound to Web Server Pro perties (Свойства** правила Inbound to Web Server).
6. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
7. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Теперь посмотрим, что произойдет, когда мы снова соединимся с Web-сайтом. 1. На машине внешнего клиента откройте Web-обо зре вате ль, введите в адресную строку **http://172.l6.0.2 и** нажмите клавишу <ENTER>.

2. Появится страница **Under Construction** (В разработке). Удерживая нажатой клавишу <CTRL>, щелкните мышью кнопку **Refresh** (Обновить) на инструмен тальной панели обозревателя.
3. Вернитесь на Web-сервер сети DMZ и откройте регистрационный журнал сер виса WWW Web-сервера. Вы увидите что-то похожее на строки, приведенные далее. Обратите внимание на выделенные жирным шрифтом IP-адреса. Началь ный IP-адрес теперь появляется в журнале регистрации.

```
«Software: Microsoft Internet Information Services 6.0
«Version: 1.0
(•Date: 2004-06-18 07:42:37
«Fields:  date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip
cs(User-Agent)  sc-status  sc-substatus sc-win32-status
2004-06-18  07:42:37  172.16.0.2 GET /iisstart.htm - 80  -  192.168.1.187 Mozilla/
4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)  200  0  0
2004-06-18 07:42:37 172.16.0.2 GET /pagerror.gif - 80 - 192.168.1.187 Mozilla/
4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
```

Несмотря на то, что блокирование фильтра Web-прокси для соединений по протоколу HTTP решает проблему **контроля** IP-адреса источника в правиле доступа опубликованного Web-сервера, при этом мы лишаемся фильтра Web-прокси для *всех* Web-соединений, устанавливаемых не с помощью конфигурации клиента Web-прокси. Это означает, что исходящие соединения от клиентов SecureNAT и клиентов брандмауэра не будут обрабатываться фильтром Web-прокси и не получат преимуществ от использования кэша Web-прокси и других функциональных возможностей, предоставляемых фильтром Web-прокси. Кроме того, могут возникнуть побочные эффекты, влияющие на правила публикации Web-сервера. Имейте в виду, что мы пока не протестировали основательно побочные эффекты от блокирования фильтра Web-прокси для HTTP-протокола, поэтому не можем знать наверняка, каковы эти непреднамеренные влияния.

Альтернативой может быть создание собственного определения протокола, которое описывается как **TCP** 80 Outbound. Можно применить это пользовательское определение протокола для **публикации** HTTP-сервера сети DM2 с помощью правила доступа. Большая проблема такого подхода заключается в том, что при этом мы лишаемся защиты фильтра Web-прокси или фильтра защиты HTTP. При таком сценарии мы имеем действительно традиционный брандмауэр с фильтрацией пакетов!

Разрешение внутридоменных соединений через брандмауэр ISA

В новом брандмауэре ISA улучшенная поддержка присоединенных непосредственно сетей DMZ привела *к* множеству вопросов о том, как разрешить внутридоменные соединения через брандмауэр ISA одной сети с другой. Теперь можно создать МН о-

гочисленные напрямую присоединенные сети периметра и разрешить контролируемый доступ к этим сетям и из них. Кроме того, можно, не рискуя, размещать машины, члены домена, в этих сегментах DM2 для поддержки множества новых сценариев, таких как сегменты специализированных сетевых сервисов, реализующие сегментацию домена.

Например, необходимо поместить обращенный к Интернету Exchange Server или входной аутентифицирующий SMTP-ретранслятор в сегмент сетевых сервисов. Для того чтобы воспользоваться базой данных пользователей в службе каталогов Active Directory, нужно присоединить эти машины к домену службы каталогов Active Directory во внутренней сети. Поскольку контроллеры домена внутренней сети находятся в сети, контролируемой брандмауэром ISA, необходимо настроить брандмауэр ISA для разрешения протоколов, требуемых для внутридоменных коммуникаций.

СОВЕТ Обратите внимание, что вы не «открываете порты» в брандмауэре ISA. Термин «открыть порты» берет свое начало в простых аппаратных брандмауэрах с фильтрацией пакетов. Поскольку у брандмауэра ISA ес~ь информация о протоколах, он может выполнять отслеживающие состояние соединений фильтрацию и проверку прикладного уровня всех соединений, проходящих через брандмауэр. Мы настоятельно рекомендуем не доверять защиту важных корпоративных ресурсов лишь простому аппаратному брандмауэру с фильтрацией пакетов.

Базовая сетевая конфигурация, использованная в данном примере, показана на рис. 7.42.

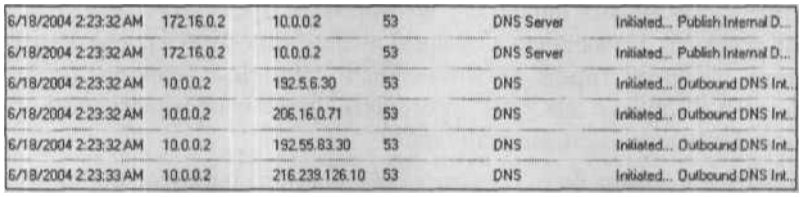


Рис. 7.42. Базовая сетевая конфигурация для трехадаптерной сети DMZ

В табл. 7.6 приведены протоколы, необходимые для внутридоменных коммуникаций, и другие параметры, включенные в правило доступа, которое мы создадим для поддержки этих соединений.

Табл. 7.6. Протоколы, требуемые для внутри доменных коммуникаций

Имя	**Внутридоменные соединения**
Action (Действие)	Allow
Protocols (Протоколы)	ADLogon/DirRep* Direct Host (TCP 445)" DNS Kerberos-Adm (UDP) Kerberos-Sec (TCP)

Табл. 7.6. (окончание)

Имя	Внутридоменные соединения
	Kerberos-Sec (UDP) ШАР (TCP) LDAP (UDP) LDAP GC (Global Catalog) RPC Endpoint Mapper (TCP 135)*" NTP Ping
From (От)	DM2 Member Server Internal Network DC (Контроллер домена внутренней сети)
To (К)	Internal Network DC DM2 Member Server (Сервер-член DM2)
Users (Пользователи)	All
Schedule (Расписание)	Always
Content Types (Типы содержимого)	All content types

ADLogon/DirRep: Первичное соединение: 50000 TCP исходящее (требуется задание ключа RPC на внутреннем Exchange Server).

" Direct Host: Первичное соединение: 445 TCP исходящее (требуется для демонстрации проблемы, обсуждаемой в этом разделе).

"• RPC Endpoint Mapper: Первичное соединение: 135 TCP исходящее (требуется для демонстрации проблемы, обсуждаемой в этом разделе).

Сервисы RPC (Remote Procedure Call, удаленный вызов процедуры) самонастраиваются в реестре с помощью универсального уникального идентификатора (universally unique identifier, UUID), который функционально подобен глобальному уникальному идентификатору (globally unique identifier, GUID). Идентификаторы RPC UUID хорошо известны (по крайней мере, сервисам RPC) и уникальны для каждого сервиса.

Когда сервис RPC стартует, он получает неиспользуемый верхний (high) порт или динамически распределяемый порт с большим номером (больше 1024) и регистрирует его с помощью идентификатора UUID сервиса RPC. Некоторые сервисы выбирают случайный верхний порт, в то время, как другие пытаются всегда применять один и тот же верхний порт, если он в это время не используется. Назначение верхнего порта статическое по отношению ко времени жизни сервиса и меняется только после рестарта машины или сервиса.

Когда клиент связывается с сервисом RPC, он заранее не знает, какой верхний порт, или порт с большим номером, использует сервис. Приложение-клиент RPC устанавливает соединение с сервисом серверного RPC-распределителя конечной точки (на порт 135) и запрашивает нужный сервис, используя его UUID. RPC-рас-

пределитель конечной точки возвращает номер соответствующего верхнего порта клиенту и закрывает соединение с распределителем конечной точки.

В заключение клиент создает новое соединение с сервером, используя номер порта, полученный от распределителя конечной точки.

Поскольку невозможно заранее узнать, какой порт будет использовать сервис RPC, брандмауэру необходимо разрешить соединения через все порты с большими номерами.

Мы хотим ограничить порты, запрашиваемые сервисом RPC, единственным портом. Это позволит нам знать заблаговременно, какой порт использовать и задать его в брандмауэре. В противном случае нам пришлось бы разрешить использовать все порты с большими номерами для соединений сети DM2 с внутренней сетью. Мы можем ограничить допустимые порты единственным портом, внеся изменение в Реестр на каждом контроллере домена. Далее приведен ключ реестра:

```
HKEY_LOCAL_MACHINE\SYSTEM\Cu r rentCont rolSet\Services\NTDS\Pa ramete rs\
```

> ПРИМЕЧАНИЕ В действительности нет необходимости делать это, так как RPC-фильтр брандмауэра ISA может управлять динамически доступом к порту. RPC-фильт ждет RPC-согласований (RPC negotiations) и затем динамически открывает требуемый верхний порт. Однако мы предпочитаем установить порт вручную, чтобы облегчить анализ регистрационных журналов и отслеживание RPC-соединений, устанавливаемых между сегментом DMZ и внутренней сетью. Если административные издержки от установки конкретного верхнего порта для RPC-коммуникаций слишком велики, то можно воспользоваться RPC-фильтром и не беспокоиться об этом. Вот что мы имели в виду, когда утверждали, что брандмауэр ISA не «открывает порты» — он действительно анализирует требуемые *протоколы.*

Вам нужно добавить значение типа DWORD, названное **TCP/IP Port** (порт TCP/IP) и задать номер порта, который вы хотите использовать. Придется выполнить эту процедуру на каждом контроллере домена.

Проделайте следующие шаги на каждом контроллере домена для того, чтобы ограничить порт RPC-репликации номером **50000.**

1. Щелкните мышью кнопку меню **Start** (Пуск) и выберите команду **Run** (Выпол нить). В текстовое поле **Open** (Открыть) введите **Regedit** и щелкните мышью кнопку ОК.
2. Перейдите к следующей ветви реестра: HKEY_LOCAL_MACHI NE\SYSTEM\Cu r rent-Con trolSe t\Services\NTDS\Para meters\
3. Щелкните мышью пункт меню **Edit** (Редактировать) и укажите на команду **New** (Новый). Щелкните кнопкой мыши вариант **DWORD Value** (Значение типа DWORD).

4. Замените имя элемента **New Value *1 на** имя **TCP/IP Port** и дважды щелкните его кнопкой мыши.
5. В диалоговом окне **Edit DWORD Value** (Редактирование значения типа DWORD) выберите вариант **Decimal** (Десятичное). Введите 50000 в текстовое поле **Value data** (Значение). Щелкните мышью кнопку OK.
6. Перезапустите контроллер домена.

Брандмауэр ISA разрешает управлять маршрутной связью между любыми двумя сетями, в данном примере мы воспользуемся типом связи ROUTE (маршрут) между сетью DMZ и внутренней сетью. Имейте в виду, что, когда применяется сетевой шаблон (Network Template) для создания сегмента DMZ, по умолчанию устанавливается маршрутная связь типа NAT (преобразование сетевых адресов). Несмотря на то, что применение связи типа NAT предоставляет некоторые минимальные преимущества, они компенсируются ограничениями, налагаемыми в данном сценарии. Если используется сетевой шаблон, убедитесь в том, что в сетевом правиле, управляющем коммуникациями между сетью DMZ и внутренней сетью, выбран тип связи ROUTE (маршрут), как показано на рис. 7.43.

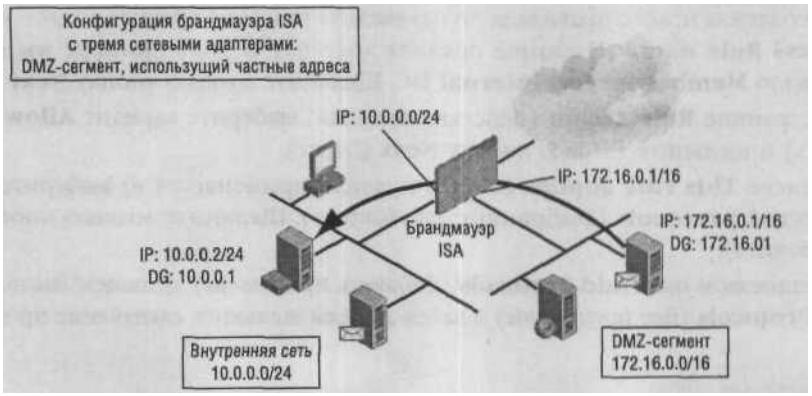


Рис. 7.43. Настройка сетевой связи

В следующем примере создается правило, разрешающее внутридоменные коммуникации между отдельным сервером-членом сети DMZ и отдельным контроллером домена во внутренней сети. Мы применяем этот сценарий для простоты, но ничто не мешает разрешить соединения между отдельными серверами.

Например, у вас может быть несколько машин с серверами-членами сети DMZ и многочисленные контроллеры домена во внутренней сети. В этом случае, вместо создания сетевых объектов, представляющих отдельные машины, следует создать один набор компьютеров для серверов-членов сети DMZ и другой набор компьютеров для контроллеров домена во внутренней сети. Затем можно использовать наборы компьютеров для указания местоположения источника и адресата в правиле внутридоменных коммуникаций.

ПРИМЕЧАНИЕ В следующем упражнении вы создадите два определения протоколов (Protocol Definitions), которые на самом деле *не нужны,* поскольку имеются встроенные определения протоколов для обеспечения ваших требований. Однако мы создадим эти определения протоколов для иллюстрации некоторых важных моментов, обсуждаемых в конце раздела.

Выполните следующие шаги для создания правила внутридоменных соединений, которое разрешит машинам в сегменте DMZ связываться с контроллерами домена во внутренней сети.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните мышью вкладку **Tasks** (Задачи) на панели задач. Щелкните кнопкой мыши ссылку **Create a New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В этом примере мы назовем правило **Member Serveralnternal DC.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. В списке **This rule applies to** (Это правило применяется к) выберите строку **Selected protocols** (Выбранные протоколы). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **All Protocols** (Все протоколы) и затем дважды щелкните следующие протоколы:

   DNS
   Kerberos-Adm (UDP)
   Kerberos-Sec (TCP)
   Kerberos-Sec (UDP)
   LDAP
   LDAP (UDP)
   LDAP GC (Global Catalog)
   NTP (UDP)
   Ping

7. Щелкните мышью пункт меню **New** (Новый) и строку **Protocol** (Протокол).
8. На странице **Welcome to the New Protocol Definition Wizard** (Вас приветствует мастер определения нового протокола) введите имя **AD Logon /DirRep** в текстовое поле **Protocol Definition name** (Имя определение протокола). Щелкните мышью кнопку **Next** (Далее).

9- На странице Primary Connection Information (Информация о первичном соединении) щелкните кнопкой мыши кнопку New (Новый).

10. На странице New/Edit Protocol Connection (Новое/Редактировать соединение по протоколу) выберите TCP в списке Protocol type (Тип протокола). Выберите Outbound (Исходящее) в списке Direction (Направление). В области Port Range (Диапазон портов) введите 50000 в текстовые поля From (От) и To (До), как показано на рис. 7.44. Щелкните мышью кнопку OK.

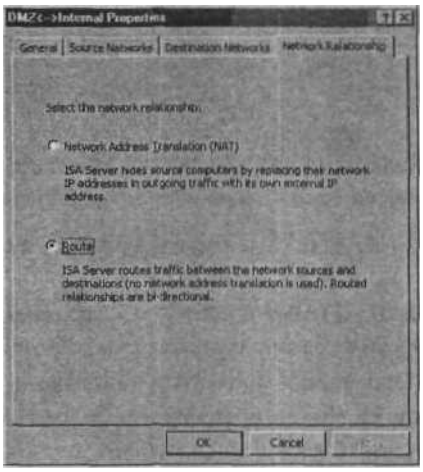


Рис. 7.44. Создание новых определений протоколов

11. Щелкните мышью кнопку Next (Далее) на странице Primary Connection Information (Информация о первичном соединении).

12. Выберите вариант No (Нет) на странице Secondary Connections (Вторичные соединения).

13-Щелкните мышью кнопку Finish (Готово) на странице Completing the New Protocol Definition Wizard (Завершение мастера определения нового протокола).

14. Щелкните кнопкой мыши пункт меню New (новый) и Protocol (Протокол).

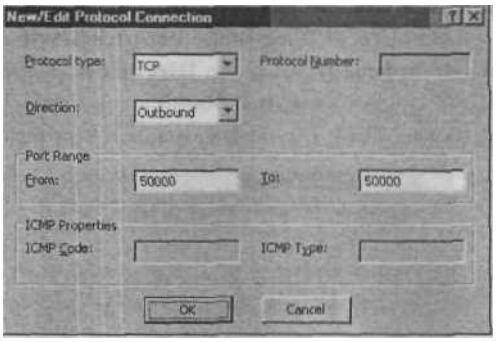
15. На странице Welcome to the New Protocol Definition Wizard (Вас приветствует мастер определения нового протокола) введите имя Direct Host в текстовое поле Protocol Definition name (Имя определения протокола). Щелкните мышью кнопку Next (Далее).

16. На странице Primary Connection Information (Информация о первичном соединении) щелкните кнопкой мыши пункт New (Новый).

17.На странице New/Edit Protocol Connection (Новое/Редактировать соединение по протоколу) выберите TCP в списке Protocol type (Тип протокола). Выберите Outbound (Исходящее) в списке Direction (Направление). В области Port Range (Диапазон портов) введите 445 в текстовые поля From (От) и To (До). Щелкните мышью кнопку OK.

Рис. 7.45. Настройка первичного соединения для определения протокола

18. Щелкните мышью кнопку **Next** (Далее) на странице **Primary Connection Information** (Информация о первичном соединении), как показано на рис.



19. Выберите **вариант No (Нет)** на странице **Secondary Connections (Вторичные** соединения).
20. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Protocol Definition Wizard** (Завершение мастера определения нового протокола).
21. Щелкните кнопкой мыши пункт меню New (Новый) и **Protocol** (Протокол).
22. На странице **Welcome to the New Protocol Definition Wizard** (Вас привет ствует мастер определения **нового** протокола) введите имя **RPC Endpoint Mapper (TCP 135)** в текстовое поле **Protocol Definition name (Имя определения** про токола). Щелкните мышью кнопку **Next** (Далее).
23. На странице **Primary Connection Information** (Информация о первичном соединении) щелкните кнопкой мыши кнопку **New** (Новый).
24. На странице **New/Edit Protocol Connection** (Новое/Редактировать соедине ние по протоколу) выберите **TCP** в списке **Protocol type** (Тип протокола). Вы берите **Outbound** (Исходящее) в списке **Direction** (Направление). В области **Port Range** (Диапазон портов) введите 135 в текстовые поля **From** (От) и **To** (До). Щелкните мышью кнопку ОК.
25. Щелкните мышью кнопку **Next** (Далее) на странице **Primary Connection Infor mation** (Информация **о** первичном соединении).
26. Выберите вариант **No** (Нет) на странице **Secondary Connections** (Вторичные соединения).
27. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Protocol Definition Wizard** (Завершение мастера определения нового протокола).
28. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните кнопкой мыши папку **User-Defined** (Определенный пользователем). Дважды щелкните кнопкой мыши протоколы: **ADLogon/DirRep, Direct Access** и **RPC Endpoint Mapper (TCP 135).** Щелкните мышью кнопку **Close** (Закрыть).

29. Щелкните мышью кнопку **Next** (Далее) на станице **Protocols** (Протоколы).
30. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
31. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New** (Новый). Щелкните кнопкой мыши **Computer** (Компьютер).
32. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите **DMZ Member Server** в текстовое поле **Name** (Имя). Введите адрес **172.16.0.2** в текстовое поле **Computer IP Address** (IP-адрес компьютера). Щелкните мышью кнопку ОК.
33. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New (Новый)** и **Computer** (Компьютер).
34. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите **Internal DC** в текстовое поле **Name** (Имя). Введите адрес **10.0.0.2** в текстовое поле **Computer IP Address** (IP-адрес компьютера). Щелкните мышью кнопку ОК.
35. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните кнопкой мыши элемент **DMZ Member Server.** Щелкните мышью кнопку **Close** (Закрыть).
36. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).
37. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
38. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните кнопкой мыши элемент **Internal DC.** Щелкните мышью кнопку **Close** (Закрыть).
39. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
40. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
41. Проверьте установки на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила) щелкните мышью кнопку **Finish** (Готово).
42. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
43. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию), далее вы увидите на вкладке **Firewall Policy** (Политика брандмауэра) то, что показано на рис. 7.46.

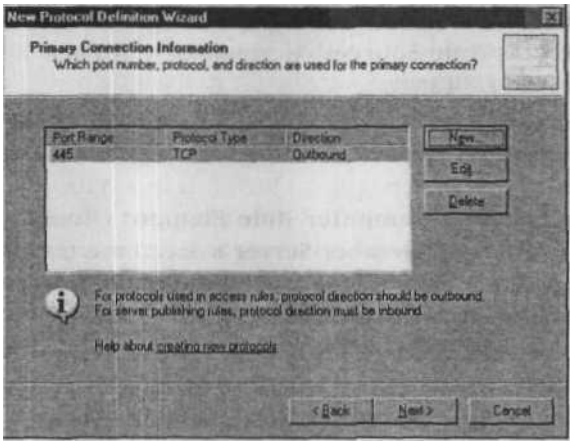
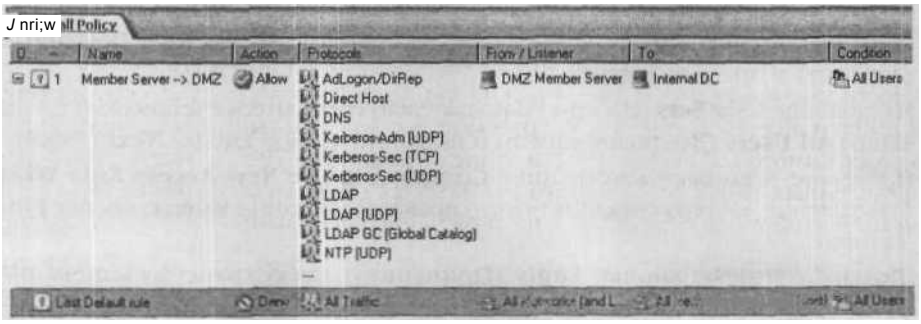


Рис. 7.46. Вкладка Firewall Policy (Политика брандмауэра)

Можно протестировать правило, соединив машину в сети DMZ с доменом службы каталогов Active Directory во внутренней сети и затем зарегистрировавшись а домене после его присоединения. Имейте в виду, что данное правило не разрешает соединение по всем протоколам от серверов-членов к контроллерам доменов. Вам потребуется создать другие правила доступа для других протоколов и дополнительные правила доступа для коммуникаций с другими машинами в других сетях.

На рис. 7.47 показаны некоторые записи в журнале регистрации для соединений сервера-члена с контроллером домена во внутренней сети. Есть среди них записи, подчеркивающие некоторые недокументированные проблемы, связанные с брандмауэром ISA и его конфигурацией.



^On **!;.^A1TмЛ«** 4eti>okj**|ind**L .'^ MtJ«tMC»ktEeryJLoCJiHocll * **AlUttn**

Рис. 7.47. Записи в журнале регистрации, показывающие соединения между серв ерами-членами и контроллером домена

Обратите внимание на первую запись соединения по протоколу TCP к порту 445. В столбце протокола указано имя протокола **Microsoft CIFS (TCP)** (Common Internet File System, общий протокол доступа к файлам Интернет), а не **Direct Host,** имя

определения протокола, которое мы создали для этого протокола. Причина в том, что предпочтение отдается встроенным протоколам в том случае, если создано определение протокола, параметры которого совпадают с встроенным определением протокола.

В пятой строке сверху можно увидеть соединение к TCP-порту 135. В столбце **Protocol** (Протокол) приведен протокол **RCP (all interfaces)** (RCP-протокол, все интерфейсы) вместо протокола **RCP Endpoint Mapper,** который мы создали. Причина та же — существует встроенный протокол **RCP (all interfaces),** который брандмауэр предпочел созданному нами протоколу. Кроме того, это встроенное определение протокола автоматически связано с RPC-фильтром брандмауэра ISA, значительно повышающим уровень защиты RPC-соединений.

Мы видим, что одно из наших пользовательских определений протоколов действительно использовано в четвертой строке сверху. Определение протокола **ADLogon/DirRep** применяется для связи с пользовательским RPC-портом, настроенным нами в реестре контроллера домена.

Резюме

В этой главе мы рассмотрели, как функционирует политика доступа и как настраиваются правила доступа для управления исходящим доступом через брандмауэр ISA. Мы также обсудили ряд специальных особенностей политики доступа брандмауэра ISA, которые можно использовать для будущей защиты вашей сети.

Мы рассказали об элементах, создающих правила доступа брандмауэра ISA, включая протоколы, наборы пользователей, типы содержимого, расписания и сетевые объекты. Были обсуждены способы создания собственных протоколов или использование встроенных в брандмауэр ISA Server. Мы также рассмотрели наборы пользователей (группы брандмауэра), которые поставляются как предварительно сконфигурированные в брандмауэре ISA Server: all authenticated users (все подтвердившие свою подлинность пользователи), all users (все пользователи) и system and network service (системный и сетевой сервис). Мы рассказали о том, как выполняется контроль типов содержимого в HTTP-трафике и туннелированном FTP-трафике, а также о предопределенных типах содержимого и о том, как создать собственные типы содержимого. В этой главе обсуждалось и применение расписаний в правилах доступах.

Далее мы представили подробное пошаговое описание создания правил доступа и все параметры, доступные в процессе создания и настройки правила. Было показано, *как* обойти мастер и создать новые правила с помощью копирования и вставки, а затем внести изменения в существующее правило. Мы рассказали, как настроить RPC-, FTP- и HTTP-политики и как упорядочить и разместить правила доступа.

Мы обсудили использование сценариев для заполнения наборов имен доменов и предложили простой сценарий, позволяющий импортировать компоненты в набор имен доменов или набор URL-адресов из текстового файла.

Вы познакомились с некоторыми конкретными примерами задач, которые вам возможно захочется выполнить, **такими** как блокирование протокола MSN Messenger с помощью правила доступа и разрешение исходящего доступа по протоколу MSN Messenger через Web-прокси.

В следующем разделе мы обсудили подробности создания и конфигурирования трехадаптерной сети DMZ (или сети периметра) с применением общедоступных адресов. Мы рассмотрели причины применения правил доступа вместо правил публикации для разрешения доступа к DMZ-хостам и описали публикацию хоста сети DMZ с общедоступными адресами с помощью правил доступа, а также способы тестирования правил.

В заключение мы показали, как разрешать внутридоменные коммуникации через брандмауэр ISA Server. Мы обсудили протоколы, необходимые для внутридоменных соединений, и показали вам, как редактировать Реестр на ваших контроллерах домена для замены диапазона портов, необходимых для RPC-соединений, одним портом, для того чтобы упростить анализ журналов регистрации соединений.

Краткое резюме по разделам

Конфигурирование правил доступа для исходящих соединений через брандмауэр ISA

0 В правилах доступа можно применять только протоколы для первичного соединения в исходящем, или send , направлении. Правила публикации Web-сервера и правила публикации сервера, наоборот, всегда используют протоколы для первичных соединений входящего, или receive, направления. Правила доступа управляют доступом от источника к адресату с помощью исходящих протоколов.

0 На странице **Rule Action** (Действие правила) есть два варианта: **Allow** (Разрешить) или **Deny** (Запретить). В отличие от ISA Server 2000 в новом брандмауэре ISA вариант **Deny** (Запретить) установлен по умолчанию.

0 Брандмауэр ISA поставляется более чем с сотней встроенных определений протоколов, которые вы можете использовать в своих правилах доступа.

0 Есть несколько параметров, которые можно настроить в правиле доступа, но которые не представлены в **New Access Rule Wizard** (Мастер создания нового правила доступа). Можно получить к ним доступ в диалоговом окне **Properties** (Свойства) правила доступа.

0 Когда задается расписание для правила доступа, правило применяется только к новым соединениям, характеристики которых соответствуют параметрам правила. Активные соединения, к которым применяется данное правило, не будут разорваны.

0 Команда **Copy** (Копировать) очень полезна, если нужно использовать **New Access Rule Wizard** (Мастер создания нового правила доступа) для создания новых

правил. Щелкните правой кнопкой мыши существующее правило и затем левой кнопкой мыши щелкните команду Copy (Копировать). Щелкните правой кнопкой мыши то же правило и затем левой кнопкой мыши выберите команду **Paste** (Вставить).

0 Общая ошибка администраторов брандмауэра ISA — разрешение хостам в сети, защищенной брандмауэром ISA, создавать петлю через брандмауэр для доступа к ресурсам той же сети, в которой находится клиент. Петля через брандмауэр ISA может снизить общую производительность брандмауэра или полностью нарушить коммуникации.

0 Всегда следует избегать создания петель через брандмауэр ISA для доступа к ресурсам, находящимся в той же сети, что и запрашивающий хост. Решение этой проблемы заключается в настройке клиентов SecureNAT, клиентов брандмауэра и клиентов Web-прокси для применения прямого доступа (Direct Access) к локальным ресурсам (локальные ресурсы — это ресурсы, содержащиеся в той же сети брандмауэра ISA, что и затребовавший их клиент).

0 Блокирование опасных приложений — основная задача брандмауэра ISA. Существует ряд методов, которые вы можете использовать для блокирования опасных приложений.

0 Когда протокол MSN Messenger посылает верительные данные на сайт MSN Messenger, эти данные также посылаются на брандмауэр ISA. Если имя пользователя и пароль, применяемые пользователем для доступа к сайту MSN Messenger, не совпадают с верительными данными, которые пользователь применяет в корпоративной сети, соединение не будет установлено.

0 После того, как клиент инициирует запрос, брандмауэр ISA сохраняет состояние соединения в таблице состояния брандмауэра в течение сеанса связи, что дает возможность клиенту получить ответ. Активное состояние соединения позволяет клиенту посылать новые запросы. Брандмауэр ISA удаляет активное состояние из таблицы состояния после простоя сеанса в течение точно не установленного периода времени (обычно 1-2 мин).

Использование сценариев для заполнения наборов имен доменов

0 Кроме выполнения базовой задачи — фильтрования, отслеживающего состояние соединений (что может делать и простой «аппаратный» брандмауэр), функциональная возможность строгой проверки прикладного уровня позволяет брандмауэру ISA действительно распознавать протоколы, проходящие через брандмауэр.

0 Механизм отслеживающей состояние соединений проверки прикладного уровня брандмауэра ISA дает вам возможность контролировать доступ не прямо к «портам», а к действующим протоколам, проходящим через эти порты.

И Первое, что необходимо сделать при использовании сценариев для импорта, — создать набор URL-адресов или имен доменов на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004).

И По мере появления новых URL-адресов вы можете добавить их в те же текстовые файлы и выполнить сценарий снова. Новые компоненты будут включены без дублирования доменов или URL-адресов, которые уже содержатся в наборе имен доменов или наборе URL-адресов.

Создание и конфигурирование трехадаптерной сети DMZ с общедоступными адресами

И В отличие от брандмауэра ISA Server 2000, который видел мир разделенным на доверенных и не заслуживающих доверия (включенных в таблицу локальных адресов (LAT) и не включенных в нее), брандмауэр ISA Server 2004 считает все сети не заслуживающими доверия или непроверенными и применяет политику брандмауэра ко всем соединениям, установленным через брандмауэр ISA Server 2004, включая хосты, соединяющиеся с помощью клиентов удаленного доступа VPN (Virtual Private Network, виртуальная частная сеть) или шлюзовых VPN-соеди нений.

В Функционирование брандмауэра ISA Server 2004 в разнородных сетях позволит вам соединить многочисленные интерфейсы (или множественные виртуальные интерфейсы с помощью сопровождения данных тегами VLAN (virtual LAN, виртуальная локальная сеть)) и иметь полный контроль над трафиком, который передается между сетями, соединенными брандмауэром ISA Server 2004.

0 Иногда использование общедоступных адресов необходимо, например, если у вас установлен сегмент DMZ с многочисленными хостами, использующими общедоступные адреса, и нежелательно менять схему адресации из-за расходов, связанных с внесением соответствующих изменений в общедоступную систему доменных имен (DNS).

0 Политика брандмауэра ISA Server 2004 предоставляет два метода, которые можно использовать для контроля трафика, проходящего через брандмауэр: правила доступа и правила публикации. Правила доступа могут применяться к связи, устанавливаемой с помощью определения маршрута, и к связи, устанавливаемой средствами NAT (network address translation, преобразование сетевых адресов). Правила публикации применяются только к соединениям с помощью NAT, даже если используется сегмент с общедоступным адресом и имеется определение маршрута между хостами источника и адресата.

И Один из главных недостатков сценариев публикации Web-серверов брандмауэра ISA Server 2000 состоял в том, что вы всегда получали IP-адрес брандмауэра ISA Server 2000 в журналах регистрации опубликованных Web-серверов. В брандмауэре ISA Server 2004 эта проблема устранена и можно либо передавать дей-

ствительный IP-адрес клиента на опубликованный Web-сервер, либо использовать IP-адрес брандмауэра ISA Server 2004.

0 Когда создается сегмент DMZ с применением общедоступных адресов, необходимо выделить подсети в общедоступном блоке и назначить одну из подсетей сегменту DMZ. Затем можно связать первый допустимый адрес выделенного в подсеть блока интерфейсу DMZ и первый допустимый адрес другого выделенного в подсеть блока общедоступному интерфейсу.

0 Можно сконфигурировать предшествующий брандмауэру маршрутизатор, определив маршрут к сегменту DMZ. Делается это с помощью использования IP-адреса во внешнем интерфейсе брандмауэра ISA Server 2004 как адреса шлюза для сетевого идентификатора (ID) сегмента DMZ. Если эта запись таблицы маршрутизации пропущена на предшествующем маршрутизаторе, никакие первичные входящие соединения и никакие отклики на входящие соединения с сегментом DMZ (к нему и из него) не будут работать.

И Сервис DNS (Domain Name System, служба имен доменов) очень важен для брандмауэра ISA Server 2004, поскольку брандмауэр может выполнять разрешение имен для Web-прокси и клиентов брандмауэра. Брандмауэр ISA Server 2004 использует установочные DNS-параметры своих сетевых адаптеров для запроса подходящего DNS-сервера. Если DNS-конфигурация некорректна, то можно столкнуться как с медленным разрешением имен, так и с полным его отсутствием.

0 После того, как сеть DMZ определена, следующий шаг — настройка маршрутных связей между сетью DMZ, внутренней сетью и Интернетом (который служит внешней сетью, определяемой как любая сеть с не заданными сетевыми параметрами).

0 DMZ-хосту может понадобиться разрешение имен интернет-хостов. Такая ситуация возникает каждый раз, когда DMZ-хосту надо установить новые исходящие соединения с серверами в Интернете, основанные на имени хоста-адресата.

В DNS-сервер внутренней сети должен быть способен запрашивать DNS-сервер в Интернете для разрешения имен интернет-хостов. Мы можем создать правило доступа для DNS, которое позволит DNS-серверу внутренней сети обращаться к DNS-серверам в Интернете по DNS-протоколу.

0 Возможно при публикации Web-сервера с помощью правила доступа возникнет желание увидеть действительный IP-адрес хоста внешней сети вместо IP-адреса брандмауэра ISA Server 2004. Этого можно добиться, если заблокировать фильтр Web-прокси.

Разрешение внутридоменных соединений через брандмауэр ISA

0 Теперь можно создавать множественные непосредственно присоединенные сети периметра и разрешать контролируемый доступ к этим сетям периметра и из них. Появилась возможность безопасного размещения машин, членов домена,

в сегменте DMZ для поддержки ряда новых сценариев, таких как сегменты специализированных сетевых сервисов (dedicated network services), реализующие сегментацию домена.

И Может возникнуть желание поместить доступный из Интернета Exchange Server или SMTP-ретранслятор входной аутентификации в сегменте сетевого сервиса. Для того чтобы получить выигрыш от применения базы данных пользователей в службе каталогов Active Directory, понадобится присоединить эти машины к домену Active Directory во внутренней сети.

И RPC-сервисы настраивают самих себя в реестре с помощью универсального уникального идентификатора (UUID), который функционально подобен глобальному уникальному идентификатору (GUID). RPC-идентификаторы UUID — хорошо известные **идентификаторы** (по крайней мере, для RPC-сервисов) и уникальны в каждом сервисе.

0 RPC-фильтр брандмауэра ISA может динамически контролировать доступ к порту. RPC-фильтр ожидает (прослушивает) RPC-обращения (RPC negotiations) и затем динамически открывает требуемый верхний порт (high port).

0 Когда применяется сетевой шаблон (Network Template) для создания сегмента DMZ, по умолчанию устанавливается тип маршрутной связи — средства NAT.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»),** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Я использую специализированную FTP-программу для соединения с FTP-сервером моей компании. Я могу выполнить аутентификацию и загрузить информацию с FTP-сайта, но я не могу загрузить данные на удаленный компьютер. У меня есть правило доступа, которое разрешает хосту доступ к FTP-протоколу. Почему же я не могу загрузить информацию на удаленную машину?

О: Щелкните правой кнопкой мыши правило доступа, разрешающее исходящее соединение по FTP-протоколу, и щелкните левой кнопкой мыши команду **Configure FTP** (Настроить FTP). Затем настройте FTP-политику для разрешения FTP-загрузки на удаленный компьютер.

В: Я хочу получать подтверждение **подлинности** всех соединений, проходящих через брандмауэр ISA. **Действительно ли** мне следует использовать клиент брандмауэра?

О: Клиент брандмауэра существенно улучшает и безопасность, и производительность брандмауэра ISA. Без клиента брандмауэра вы не сможете выполнить аутентифи-

кацию соединений, установленных через брандмауэр ISA приложениями Winsock (Windows Sockets, сетевой программный интерфейс). Если вы настроите клиенты как клиенты Web-прокси, *вы* получите только информацию о пользователях для соединений по протоколам: **HTTP,** HTTPS и HTTP туннелированный FTP. Мы рекомендуем вам установить клиент брандмауэра на всех клиентских операционных системах и настроить правила доступа на требование аутентификации.

В: Я создал на брандмауэре ISA правило доступа, которое разрешает анонимный доступ с помощью FTP-протокла к FTP-сайту нашей компании. Но пользователи не могут установить FTP-соединения с сайтом. В журнале обслуживания брандмауэра ISA я вижу, что правило требует аутентификации и отвергает запрос. Почему в запросе отказано, если я создал правило для анонимного доступа, разрешающее запрос?

О: Возможно, проблема связана с упорядочиванием ваших правил. Если у вас есть правило, которое применяется к FTP-протоколу и также требует аутентификации, и это правило расположено в списке правил над правилом анонимного доступа, анонимный запрос будет отвергнут, потому что это правило будет обрабатываться прежде, чем правило анонимного доступа. Мы рекомендуем указывать анонимные запрещающие правила первыми, затем располагать анонимные разрешающие правила. После анонимных разрешающих правил поместите запрещающие правила, требующие подтверждения подлинности. И в конце вашего списка правил доступа приведите разрешающие правила, требующие аутентификации.

В: Я создал пользовательское определение протокола для пользовательского приложения, которое мы используем у себя в компании. Определение протокола включает исходящий TCP-порт *4467* и вторичные соединения для входящих портов 5587-5600. Я создал правило доступа, разрешающее всем пользователям исходящий доступ по этому протоколу, но соединение отвергается правилом доступа по умолчанию (Default Access Rule). Наши клиенты настроены как клиенты SecureNAT и клиенты Web-прокси. Что мне нужно сделать, чтобы заставить это правило работать?

О: Проблема, с которой вы столкнулись, заключается в том, что клиенты SecureNAT не могут реализовывать вторичные соединения без помощи прикладного фильтра. Вы должны поручить вашим разработчикам создать прикладной фильтр для поддержки вашего местного пользовательского протокола. Но гораздо лучшее решение проблемы — установка клиента брандмауэра на ваши клиентские операционные системы. Клиент брандмауэра может устанавливать вторичные соединения, потому что в брандмауэре ISA он взаимодействует напрямую с сервисом брандмауэра.

В: Я создал правило доступа, разрешающее нашим клиентам SecureNAT исходящий доступ к Web-серверу в нашей внутренней сети, который мы **опублиĸовали** с помощью правила публикации Web-сервера. У внешних пользователей нет проблем при об-

ращении к опубликованному серверу с помощью правила публикации Web-сервера, наши клиенты SecureNAT во внутренней сети не могут соединиться с Web-сай-том. Что нужно сделать для того, чтобы правило доступа выполнялось корректно? О: По существу проблема связана не с вашим правилом доступа, а с петлей, которую вы создали через брандмауэр ISA для доступа к ресурсам внутренней сети. Мы предполагаем, что опубликованный Web-сервер и клиенты SecureNAT все находятся в одной и той же сети ISA. Хосты, находящиеся в одной сети ISA, должны всегда взаимодействовать друг с другом напрямую, не создавая петлю через брандмауэр ISA. Из вашего описания следует, что клиенты SecureNAT выполняют разрешение имени сайта в IP-адрес во внешнем интерфейсе брандмауэра ISA. Для решения проблемы вам нужно создать разделяемый DNS, чтобы внешние хосты преобразовывали имя Web-сайта в IP-адрес во внешнем интерфейсе брандмауэра ISA, как это делается правилом публикации Web-сервера, а клиенты SecureNAT во внутренней сети разрешали IP-адрес опубликованного Web-сайта в действительный IP-адрес Web-сервера (как это делается во внутренней сети).

В: Клиенты в моей внутренней сети сконфигурированы как клиенты Web-прокси. Я создал правило доступа, разрешающее исходящий доступ для аутентифицированных пользователей по протоколам HTTP и HTTPS. Это правило отлично работает, за исключением пользователей, которым необходимо соединиться с MSN Messenger (служба сообщений сети Microsoft) по протоколу HTTP. Каждый раз, когда клиенты Web-прокси пытаются соединиться с MSN Messenger через Web-прокси, попытка соединения заканчивается неудачей. Почему это происходит и как я могу исправить это?

О: Проблема заключается в том, что MSN Messenger отправляет верительные данные учетной записи пользователя MSN брандмауэру ISA, когда запрос аутентификации Web-прокси возвращается службе MSN Messenger. Поскольку невероятно, чтобы верительные данные пользователя MSN Messenger совпадали с верительными данными пользователя домена, попытка аутентификации оказывается неудачной, Для решения этой проблемы вам нужно обойти ответ HTTP 407, возвращаемый фильтром Web-прокси на брандмауэр ISA. Лучшее решение — настроить клиенты как клиенты брандмауэра и затем сконфигурировать сайты MSN Messenger для прямого доступа. Прямой доступ можно настроить в диалоговом окне **Properties** (Свойства) сети (или сетей), из которой клиенты соединяются с сайтом MSN. После того, как прямой доступ к сайтам MSN Messenger разрешен, клиент Web-прокси игнорирует соединения с этими сайтами и перебрасывает их клиентской конфигурации клиента брандмауэра или клиента SecureNAT. Если вы хотите потребовать аутентификацию для исходящего доступа, следует установить клиент брандмауэра на всех клиентских операционных системах. Клиент брандмауэра незаметно (прозрачно) посылает пользовательские верительные данные сервису брандмауэра ISA.

Глава 8

Публикация сетевых служб в Интернете с помощью ISA Server 2004

Основные темы главы:

Обзор публикаций Web-серверов и серверов

Создание и настройка правил публикации Web-сервера по протоколу, отличному от SSL

Создание и настройка правил публикации Web-сервера по протоколу SSL

Создание правил публикации сервера Создание

правил публикации почтового сервера

Обзор публикаций Web-серверов и серверов

Правила публикации Web-сервера и сервера позволяют делать серверы и сервисы в сетях, защищенных брандмауэром ISA, доступными для пользователей как защищенных, так и незащищенных сетей. Эти правила предоставляют возможность сделать популярные сервисы, такие как SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты), NNTP (Network News Transfer Protocol, сетевой протокол передачи новостей), POP3 (Post Office Protocol v. 3, почтовый протокол в сети Интернет), IMAP4 (Internet Message Access Protocol v. 4, протокол доступа к сообщениям в сети Интернет), Web («всемирная паутина»), OWA (Outlook Web Access, Web-доступ в Outlook),Terminal Services (службы терминалов) и многие другие, более доступными для пользователей удаленных сетей или других внутренних сетей или сетей периметра (Perimeter Networks).

Правила публикации Web-сервера и правила публикации сервера предоставляют разные наборы свойств и применяются для разных целей. Вообще правила публикации Web-сервера следует использовать для публикации Web-серверов и сервисов, а правила публикации сервера должны применяться для публикации серверов и сервисов не-Web. Существуют исключения из этого правила, и мы обсудим их в этой главе.

Начнем главу с обсуждения свойств и функциональных возможностей правил публикации Web-серверов и серверов. После общего обзора перейдем к деталям создания и настройки правил публикации Web-серверов и серверов. И завершим главу несколькими сценариями, демонстрирующими применение правил публикации Web-серверов и серверов в производственных сетях.

Правила публикации Web-сервера

Правила публикации Web-сервера используются для публикации Web-сайтов и сервисов. Web-публикацию иногда называют «реверсивным представительством» (reverse proxy). Когда публикуется Web-сайт, фильтр Web-прокси брандмауэра ISA всегда перехватывает запрос и затем представляет запрос к Web-сайту, опубликованному с помощью правила публикации Web-сервера.

Правила публикации Web-сервера предоставляют следующие функциональные возможности:

- обеспечение доступа через прокси к Web-сайтам, защищенным брандмауэром ISA;
- серьезный контроль прикладного уровня над соединениями, устанавливаемыми с опубликованными Web-сайтами;
- перенаправление маршрута (Path redirection);
- предварительная аутентификация соединений, устанавливаемых с опубликованными Web-сайтами (Forward basic authentication credentials, передача основных аутентификационных данных);

- обратное кэширование (Reverse Caching) опубликованных Web-сайтов;
- возможность публикации нескольких Web-сайтов с помощью единственного IP-адреса;
- возможность с помощью Link Translator (Транслятор ссылок) брандмауэра ISA перезаписывать URL-адреса, возвращаемые опубликованным Web-сайтом;
- поддержка передачи на Web-сайт как IP-адреса брандмауэра ISA, так и действи тельного IP-адреса клиента;
- поддержка системы аутентификации SecurlD;
- поддержка системы подтверждения подлинности RADIUS;
- возможность задания расписания, в соответствии с которым разрешаются со единения с опубликованными Web-сайтами;
- переадресация (redirection) портов и протоколов.

Рассмотрим каждую из этих функций подробно.

Обеспечение доступа через прокси к Web-сайтам, защищенным брандмауэром ISA

Правила публикации Web-сервера обеспечивают доступ через прокси к Web-сайтам, находящимся в сети, защищенной брандмауэром ISA. Любая сеть, не являющаяся частью внешней сети по умолчанию, рассматривается как сеть, защищенная брандмауэром ISA. Соединение через прокси более безопасно, чем соединение с определением маршрута или соединение средствами NAT (network address translation, преобразование сетевых адресов), поскольку соединение разбивается на части и восстанавливается брандмауэром ISA. Оно позволяет брандмауэру ISA выполнять на уровне приложений глубокую проверку Web-запросов к Web-сайтам, опубликованным с помощью правил публикации Web-серверов.

Фильтр Web-прокси брандмауэра ISA обрабатывает все входящие Web-соединения, устанавливаемые с применением правил публикации Web-сервера. Даже если отсоединить фильтр Web-прокси от определения протокола HTTP, он все равно останется доступным для правил публикации Web-сервера. Это решение, принятое разработчиками брандмауэра ISA, связано с безопасностью. Определено, что не прошедшие через прокси входящие подключения к Web-серверам защищенной сети должны всегда обрабатываться прокси для обеспечения наивысшего уровня защиты опубликованных Web-серверов.

Серьезный контроль прикладного уровня над соединениями, устанавливаемыми с опубликованными Web-сайтами

Одно из главных преимуществ применения правил публикации Web-сервера для публикации Web-сайтов в защищенных сетях — возможность брандмауэра ISA выполнять на прикладном уровне глубокую проверку всех соединений с опубли-

кованными Web-сайтами. Подобный контроль на уровне приложений препятствует отправке атакующим злонамеренных команд или кода на опубликованный Web-сайт. Это позволяет брандмауэру ISA останавливать атаки на уровне сети периметра и мешает атакующему попасть на опубликованный Web-сервер.

За глубокий контроль на прикладном уровне Web-запросов отвечает **HTTP-фильтр** в брандмауэре ISA. HTTP-фильтр позволяет контролировать практически любой аспект HTTP-соединения и блокировать или разрешать соединения, основанные на почти любом компоненте HTTP-коммуникаций.

Способы контроля соединения с опубликованными Web-сайтами включают:

- установку максимальной длины пользовательских данных (payload length);
- блокирование символов верхних битов (high-bit characters);
- проверку нормализации (verifying normalization);
- блокирование ответов, содержащих исполняемый контент Windows;
- настройку точно соответствующих HTTP-методов, которые нужно разрешить, и блокирование всех остальных;
- разрешение только определенного списка расширений файлов;
- разрешение только определенных заголовков запроса (request) или ответа (response);
- создание точно настроенных подписей (signatures), которые способны блокировать соединения, основываясь на URL-адресах запроса, заголовках запроса, теле запроса, заголовках ответа или теле ответа.

Мы рассмотрим некоторые подробности функционирования фильтра защиты HTTP (HTTP Security Filter) или HTTP-фильтра позже в этой главе и вернемся к подробному обсуждению фильтра защиты HTTP в главе 10 при изучении набора характеристик фильтрации уровня приложений в брандмауэре ISA.

Перенаправление маршрута

Допустим, что пользователь посылает запрос на сайт www.msfirewall.org/kits. Вы хотите направить этот запрос на сервер с именем **WEBSERVER1** и в каталог на сервере, названный **/deployment_kits.** Можно настроить правило публикации Web-сервера для замены маршрута в запросе (который установлен **/kits)** на маршрут на внутреннем Web-сервере, **/deployment_kits.**

Также можно использовать перенаправление маршрута для отправки запроса целиком на другой Web-сервер. Например, пользователи предлагают запросы к следующим сайтам;

- www.msfirewall.org/scripts;
- www.msfirewall.org/deploymentkits.

Вы можете создать два правила публикации Web-сервера: одно для входящих запросов к www. msfirewall.org/scripts и одно — для доступа к www.msfirewall.org/

deployment_kits. Запрос к www.msfirewall.org/script может быть перенаправлен к Web-серверу WEBSERVER1, а другой запрос — к Web-серверу WEBSERVER2. Можно даже перенаправить запрос по дополнительным маршрутам на каждый Web-сервер.

Мы рассмотрим несколько примеров перенаправления маршрута в разделе сценариев этой главы.

Предварительная аутентификация соединений, устанавливаемых с опубликованными Web-сайтами

Правила публикации Web-сервера можно настроить для пересылки верительных данных (credentials) базовой аутентификации (базовое делегирование, basic delegation). Это означает, что можно заранее установить подлинность пользователя на брандмауэре ISA. Предварительная аутентификация мешает неавторизованным соединениям добираться до Web-сервера. Предварительная аутентификация не позволяет атакующим и злоумышленникам применять неаутентифицированные соединения для использования известных и неизвестных слабых мест в Web-серверах и приложениях.

Очень популярно применение предварительной аутентификации на Web-сайтах OWA. Вместо того, чтобы разрешать не подтвердившим подлинности соединениям обращаться к Web-сайтам 0WA, правило публикации Web-сервера брандмауэра ISA может быть настроено на аутентификацию пользователя. Если пользователь успешно подтвердил свою подлинность на брандмауэре ISA, запрос на соединение передается Web-сайту 0WA. Если пользователь не сумел аутентифицироваться на брандмауэре ISA, попытка соединения прерывается на брандмауэре и никогда не доходит до опубликованного Web-сайта.

Предварительная аутентификация также позволяет контролировать пользователей, обращающихся к Web-сайтам. Можно настроить правила публикации Web-серверов для разрешения только определенным группам пользователей получать доступ к опубликованному Web-сайту. Итак, даже если пользователи способны успешно подтвердить свою подлинность, они смогут получить доступ к опубликованному Web-сайту только при наличии разрешения на это. В данном случае правила публикации Web-серверов брандмауэра ISA разрешают аутентификацию и авторизацию (проверку полномочий) для получения доступа к опубликованным Web-сайтам.

Возможность делегирования базовой аутентификации в брандмауэре ISA позволяет брандмауэру установить подлинность пользователя и затем переслать его верительные данные на опубликованный Web-сайт, если Web-сайт требует верительных данных. Это исключает двойное напоминание пользователю о вводе верительных данных. Вместо ответа пользователя на запрос аутентификации, посылаемый Web-сайтом, на него отвечает брандмауэр после успешной аутентификации пользователя.

Обратное кэширование опубликованных Web-сайтов

Брандмауэр ISA умеет кэшировать ответы Web-сайтов, опубликованных с помощью правил публикации Web-сервера. Когда пользователь запросил первый раз содержимое опубликованного Web-сайта, это содержимое может кэшироваться (храниться) брандмауэром ISA. Если несколько пользователей последовательно запрашивают одно и то же содержимое с опубликованного Web-сервера, это содержимое предоставляется из Web-кэша брандмауэра ISA вместо его извлечения непосредственно с Web-сервера.

Кэширование ответов с опубликованных Web-сайтов снижает нагрузку на опубликованный Web-сервер и на любой сетевой сегмент, расположенный между брандмауэром ISA и опубликованным Web-сервером. Поскольку содержимое поступает из Web-кэша брандмауэра ISA, опубликованный Web-сервер не подвергается дополнительной обработке, необходимой для обслуживания Web-запросов. По этой же причине уменьшается сетевой трафик между брандмауэром ISA и опубликованным Web-сайтом, что приводит к росту общей сетевой производительности корпоративной сети.

Можно также управлять содержимым при обратном **кэшировании.** Можно предоставлять пользователям самые свежие версии содержимого, размещенного в определенных местах на вашем опубликованном Web-сервере, в то же время разрешая брандмауэру ISA кэшировать другое содержимое на опубликованных Web-серверах за определенный заранее заданный период времени. Есть возможность создать правила кэширования на брандмауэре ISA для того, чтобы иметь точно настроенный контроль над типом кэшируемого содержимого и временем его кэширования.

Возможность публикации нескольких Web-сайтов с помощью единственного IP-адреса

Правила публикации Web-сервера позволяют публиковать многочисленные Web-сайты, используя один IP-адрес во внешнем интерфейсе брандмауэра ISA. Это возможно благодаря способности брандмауэра ISA выполнять на уровне приложений проверку, отслеживающую соединения. Частью механизма такой проверки **служит** способность брандмауэра ISA анализировать заголовок хоста во входящем запросе и принимать решение об обработке входящего запроса на основе информации заголовка хоста.

Предположим, что имеется единственный IP-адрес во внешнем интерфейсе брандмауэра ISA. Необходимо опубликовать два Web-сервера в сети, защищенной брандмауэром ISA. Пользователи будут обращаться к Web-сайтам с помощью URL-адресов www.msfirewall.org и www.tacteam.net. Все, что потребуется, — создать два правила публикации Web-сервера. Одно из них будет ожидать (прослушивать) входящие соединен і ия к сайту www.msfirewall.org и передавать эти запросы на сервер msfirewall.org

в сети, защищенной брандмауэром ISA, а другое правило публикации Web-сервера будет ожидать запросы к сайту www.tacteam.net и пересылать их Web-сайту в сети, защищенной брандмауэром ISA, ответственному за Web-сайт www.tacteam.net.

Главное при решении этой задачи (мы будем обсуждать ее чуть позже в этой главе) быть уверенным в том, что общедоступный DNS-сервер преобразует (разрешает) полностью определенные имена доменов (fully-qualified domain names) в IP-адрес во внешнем интерфейсе брандмауэра ISA. Как только первый DNS-результат получен, опубликовать два или двести Web-сайтов очень просто, используя правила публикации Web-сервера.

Возможность с помощью Link Translator брандмауэра ISA перезаписывать URL-адреса, возвращаемые опубликованным Web-сайтом

Транслятор ссылок брандмауэра ISA может перезаписывать ответы, которые опубликованные Web-серверы посылают пользователям, сделавшим запрос. Транслятор ссылок полезен при публикации Web-сайтов, включающих в свои ответы жестко закодированные URL-адреса, недоступные с удаленных компьютеров.

Предположим, что публикуется Web-сайт, жестко кодирующий URL-адреса в своих ответах, и эти адреса включают частные имена (private names) серверов в защищенной сети. Такие URL-адреса будут иметь форму http://server l /documents или http:// /webserver2/users. Поскольку это не полностью определенные имена доменов, доступные из Интернета, запрос на соединение завершится неудачей. Это обычная проблема для Web-сайтов SharePoint Portal Server (система управления и совместного использования документов).

Транслятор ссылок решает эту проблему, перезаписывая ответы, возвращаемые обратившемуся к Web-сайту пользователю. Ссылки http://serverl /documents и http:// webserver2/users перезаписываются как http://www.msfirewall.org/documents и http:// www. tacteam.net/users, каждая из которых доступна из Интернета.

Трансляция ссылок также полезна в некоторых SSL-сценариях. Например, если не используется протокол SSL (Secure Sockets Layer, протокол защищенных сокетов) при соединении брандмауэра ISA с Web-сервером, но применяется SSL в соединении Web-клиента из Интернета с брандмауэром ISA, транслятор ссылок может изменить HTTP-ответ, возвращаемый Web-сервером, на SSL-ответ в ссылках, предоставляемых пользователю. Это избавляет пользователей от обнаружения испорченных ссылок на опубликованной Web-странице.

Мы обсудим применение и настройку параметров транслятора ссылок в этой главе и более подробно в главе 10 при описании фильтрации прикладного уровня.

Поддержка передачи на Web-сайт как IP-адреса брандмауэра ISA, так и исходного IP-адреса клиента

Одно из ограничений, связанных с правилами публикации Web-сервера в ISA Server 2000, состояло в том, что журналы регистрации на опубликованном Web-сервере всегда показывали IP-адрес адаптера внутренней сети брандмауэра ISA Server Когда публиковались Web-серверы с применением правил публикации Web-сервера, исходный IP-адрес клиента заменялся внутренним IP-адресом ISA Server. Это было главной преградой для многих потенциальных администраторов ISA Server при выборе брандмауэра, поскольку они уже вложили значительные суммы в установленное на опубликованных Web-серверах программное обеспечение анализа регистрационных журналов. Для них оставалась единственная возможность — применение правил публикации сервера, которую нельзя считать лучшим вариантом, так как правила публикации сервера не дают столь же высокой степени защиты, как правила публикации Web-сервера.

К счастью, новый брандмауэр ISA предоставляет выбор между пересылкой IP-адреса брандмауэра ISA опубликованному Web-серверу и передачей истинного IP-адреса удаленного Web-клиента на опубликованный Web-сервер. Если в журналах регистрации Web-сервера реальный IP-адрес клиента не нужен, можно использовать установку по умолчанию, заменяющую IP-адрес клиента адресом сетевого интерфейса брандмауэра. Чтобы сохранить IP-адрес удаленного Web-клиента, выберите вариант настройки, сохраняющий IP-адрес.

Мы обсудим достоинства и недостатки каждого из названных вариантов настройки, когда будем рассматривать подробности создания и конфигурирования правил публикации Web-сервера позже в этой главе.

Поддержка системы аутентификации SecurID

SecurlD фирмы RSA Security Inc. — это механизм двухфакторной аутентификации, требующий, чтобы пользователь имел кое-что (опознавательный признак или маркер SecurlD) и знал кое-что (верительные данные пользователя). Брандмауэр ISA поставляется со встроенной поддержкой аутентификации SecurlD для Web-серверов и сервисов, опубликованных с помощью правил публикации Web-сервера.

Поддержка системы подтверждения подлинности RADIUS

Некоторые организации решают поместить брандмауэр ISA в место, делающее его членом пользовательского домена, что нельзя считать лучшим вариантом. Например, если имеется каскадная (back-to-back) конфигурация брандмауэров, в которой брандмауэр ISA — входной (front-end) брандмауэр, его не следует делать членом пользовательского домена. Однако можно получить выигрыш от применения пользовательской базы данных домена для аутентификации и авторизации, используя RADIUS (Remote Authentication Dial-In User Service, служба аутентификации уда-

ленного дозванивающегося (коммутируемого) пользователя) для аутентификации в правиле публикации Web-сервера.

Брандмауэр ISA можно сконфигурировать как клиента RADIUS сервера RADIUS, размещенного в корпоративной сети. Затем сервер RADIUS может быть настроен для аутентификации пользователей, базирующейся на службе каталогов Active Directory или любом другом RADIUS-совместимом (RADIUS-compliant) каталоге в корпоративной сети. Аутентификация RADIUS может применяться как для входящих, так и для исходящих соединений через фильтр Web-прокси брандмауэра ISA. Настройка правила публикации Web-сервера для применения системы аутентификации RADIUS очень проста и позволяет брандмауэру ISA поддерживать сценарии каскадного подключения брандмауэров (back-to-back firewall), в которых брандмауэр ISA — входной (или внешний) брандмауэр.

Возможность задания расписания, в соответствии с которым разрешаются соединения с опубликованными Web-сайтами

Правила публикации Web-сервера, определенные в брандмауэре ISA, дают возможность задавать время доступа пользователей к опубликованному Web-сайту. У вас может быть несколько Web-сайтов, к которым необходимо разрешить доступ только в рабочие часы, и другие Web-сайты, имеющие высокие требования к пропускной способности, обращаться к которым вы хотите не в часы пик. Можно определить время доступа пользователей к опубликованным Web-сайтам, применяя как встроенные, так и пользовательские расписания в ваших правилах публикации Web-серверов.

Переадресация портов и протоколов

Правила публикации Web-сервера позволяют выполнять переадресацию или перенаправление как портов, так и протоколов. Переадресация портов дает возможность брандмауэру ISA принять запрос на соединение с одним портом, а затем передать запрос на дублирующий или резервный порт опубликованного Web-сервера. Например, брандмауэр ISA может ожидать входящие запросы с помощью Web-приемника (Web listener) на TCP-порте 80, а затем переадресовывать это соединение на TCP-порт 8888 опубликованного Web-сервера в сети, защищенной брандмауэром ISA.

С помощью правил публикации Web-сервера можно выполнить и переадресацию протоколов. В отличие от переадресации портов, допускающей только изменение порта адресата, поддержка брандмауэром ISA перенаправления протоколов включает возможность публикации FTP-сайтов с помощью правил публикации Web-серверов. Входящий HTTP-запрос GET, сделанный к Web-приемнику правила публикации Web-сервера, преобразуется в FTP GET и пересылается на опубликованный FTP-сайт в сети, защищенной брандмауэром ISA. Правила публикации Web-серверов поддерживают перенаправление HTTP-протокол а в FTP-протокол.

Правила публикации сервера

Как и в случае правил публикации Web-серверов, вы можете применять правила публикации сервера для обеспечения доступа к серверам и сервисам в сетях, защищенных брандмауэром ISA. Правила **публикации** сервера обладают следующими свойствами и возможностями.

- Правила публикации сервера служат формой, обратной средствам NAT или «отображения портов» (Port Mapping), и не обрабатывают соединения с помощью прокси.
- Почти все протоколы IP-уровня и протоколы TCP/UDP можно опубликовать, применяя правила публикации сервера.
- Правила публикации сервера не поддерживают аутентификацию.
- Фильтрация прикладного уровня может применяться к определенному подмножеству протоколов опубликованного сервера.
- Можно сконфигурировать переопределения портов для настройки ожидающих (прослушивающих) портов и переадресации портов. Можно также заблокировать использование исходных портов, запрашиваемых клиентами для соединения с опубликованным сервером.
- Можно использовать IP-адрес для управления доступом *к* опубликованным ресурсам.
- Реальный IP-адрес удаленного клиента можно сохранить или заменить IP-адресом брандмауэра ISA.
- Имеется возможность применять расписания в правиле публикации сервера для ограничения времени доступа к опубликованному серверу.
- Поддерживается «переадресация портов» (Port address translation, PAT, преобразование адресов портов), т. е. можно получать запросы на подключение к одному порту и перенаправлять их на другой порт, обеспечивая функциональные возможности, аналогичные реализованным в «аппаратных» брандмауэрах.

Давайте рассмотрим их более подробно.

Правила публикации сервера служат формой, обратной средствам NAT или «отображения портов» (Port Mapping), и не обрабатывают соединения с помощью прокси

Правила публикации сервера могут быть формой, обратной средствам NAT или отображению портов, в зависимости от типа связи (средствами NAT или определением маршрута), установленной между опубликованным сервером **и** хостом, соединяющимся с этим сервером с применением правила публикации сервера. Правило публикации сервера настраивает брандмауэр ISA для ожидания (прослушивания) запросов к конкретному порту и затем пересылает эти запросы опубликованному серверу, находящемуся в сети, защищенной брандмауэром ISA.

В отличие от правил публикации Web-сервера, обрабатывающих прокси-запросы к опубликованному Web-серверу, правилу публикации сервера только изменяют исходный IP-адрес, прежде чем переслать запрос на соединение опубликованному серверу. Обрабатываемые прокси соединения полностью разбираются и снова компонуются брандмауэром ISA и таким образом предоставляют более высокую степень контроля прикладного уровня по сравнению с правилами публикации сервера.

Почти все протоколы IP-уровня и протоколы TCP/UDP можно опубликовать, применяя правила публикации сервера

Правила публикации Web-сервера принимают только HTTP- и HTTPS-соединения и передают их как HTTP-, HTTPS- или FTP-соединения. Правила публикации сервера, напротив, могут применяться для публикации почти всех протоколов IP-уровня и TCP- или UDP-протоколов. Это существенно повышает гибкость, с которой сервисы можно сделать доступными для хостов благодаря правилам публикации сервера.

Правила публикации сервера не поддерживают аутентификацию

Один из главных недостатков правил публикации сервера по сравнению с правилами публикации Web-сервера заключается в том, что правила публикации сервера не поддерживают предварительную аутентификацию на брандмауэре ISA. Подтверждение подлинности должно выполняться сервером, опубликованным с помощью правила публикации сервера.

Фильтрация прикладного уровня может применяться к определенному подмножеству протоколов опубликованного сервера

HTTP-фильтром брандмауэра ISA на прикладном уровне выполняется глубокая, отслеживающая состояние соединений проверка соединений, установленных с использованием правил публикации Web-серверов. Правила публикации серверов также поддерживают проверку на прикладном уровне с помощью фильтров приложений (Application Filters). Брандмауэр ISA поставляется со следующими фильтрами приложений: м DNS (security filter, фильтр защиты);

- FTP Access Filter;
- H.323 Filter;
- MMS Filter;
- PNM Filter;
- POP Intrusion Detection Filter (фильтр обнаружения вторжений, фильтр защиты);
- PPTP Filter;
- RPC Filter (фильтр защиты);

- RTSP Filter;
- SMTP Filter (фильтр защиты);
- SOCKS v4 Filter;
- Web Proxy Filter (фильтр защиты).

Ряд этих фильтров служит промежуточным звеном для составных протоколов подобно тому, как редакторы средств NAT разрешают применение составных протоколов посредством NAT-устройства. Примерами типов фильтров доступа могут служить фильтр H.323, MMS-фильтр (Microsoft Windows Media, протокол потоковых мультимедийных данных) и RTSP-фильтр (Real Time Streaming Protocol, протокол непрерывной передачи и контроля данных в режиме реального времени). Существует также ряд прикладных фильтров, основная задача которых — защита установленных через брандмауэр ISA соединений с помощью тестирования соответствия (compliance testing) соединения. Примерами таких фильтров защиты могут служить DNS-фильтр, фильтр POP Intrusion Detection (обнаружение вторжений по почтовому протоколу) и RPC-фильтр (Remote Procedure Call, удаленный вызов процедуры).

Некоторые фильтры уровня приложений выполняют обе задачи. Они действуют как посредники для клиентов SecureNAT (средства безопасного преобразования сетевых адресов) в управлении составными протоколами и, кроме того, защищают соединения, для которых служат промежуточным звеном. К фильтрам этой категории относятся фильтр SecureNAT-доступа и RPC-фильтр.

Мы подробно рассмотрим фильтры уровня приложений в главе 10.

Можно сконфигурировать переопределения портов для настройки прослушивающих портов и переадресации портов. Можно также заблокировать использование исходных портов, запрашиваемых клиентами для соединения с опубликованным сервером

В каждом правиле публикации сервера есть возможность управлять прослушивающим, или ожидающим, портом, портом назначения и портом, который может использоваться запрашивающим клиентом как исходный порт для доступа к серверу, опубликованному с помощью правила публикации сервера. Такая возможность обеспечивает скрупулезный контроль переадресации портов (отображения портов) на любом сервере, опубликованном с помощью правила публикации сервера.

Можно использовать IP-адрес для управления доступом к опубликованным ресурсам

Хотя правила публикации сервера не позволяют предварительно аутентифицировать пользователей на брандмауэре ISA, можно настроить правила публикации сервера для ограничения IP-адресов, которые могут соединяться с опубликованным сервером по правилу публикации сервера. Этот способ управления доступом, основанный на IP-адресах, применяется к опубликованным серверам, доступ к кото-

рым следует ограничить, например терминальный сервер (Terminal Server) в корпоративной сети, к которому могут обращаться только администраторы, находящиеся по заранее определенным адресам.

Реальный IP-адрес удаленного клиента можно сохранить или заменить IP-адресом брандмауэра ISA

В брандмауэре ISA Server 2000 правила публикации сервера всегда сохраняли исходный IP-адрес клиента, когда он направлял запрос на соединение с сервером, опубликованным во внутренней сети. В новом брандмауэре ISA возможен выбор между сохранением исходного IP-адреса клиента и замещением этого адреса IP-адресом самого брандмауэра ISA.

Можно применять расписания в правиле публикации сервера для ограничения времени доступа к опубликованному серверу

В правила публикации сервера, как и в правила публикации Web-сервера, можно включить расписание, чтобы соединения с опубликованным сервером могли устанавливаться только в указанные в расписании периоды времени. Можно использовать одно из встроенных расписаний или создавать собственные.

Поддерживается переадресация портов, или **PAT** (Port Address Translation)

Как и правила публикации Web-серверов, правила публикации серверов позволяют настроить способ пересылки соединений на опубликованный сервер и выбрать порты, используемые для доступа и пересылки запросов на соединение. Например, имеется возможность принимать входящие соединения с вашим частным SMTP-сервером на TCP-порт 26 и пересылать их на TCP-порт 27 на опубликованном SMTP-сервере. Сделать это можно благодаря наличию в брандмауэре ISA функциональной возможности переадресации портов (PAT).

Создание и настройка правил публикации Web-сервера по протоколу, отличному от SSL

Можно создавать правила публикации Web-серверов, используя в брандмауэре ISA Мастер создания правила публикации Web-сервера (Web Publishing Rule Wizard), который проведет вас через все этапы создания правила публикации Web-сервера, что позволит публиковать Web-серверы и сервисы в любой сети, защищенной брандмауэром ISA. В этом разделе мы рассмотрим действия мастера создания правила публикации Web-сервера и обсудим предоставляемые им параметры и их смысл.

Сначала сосредоточимся на правилах публикации Web-серверов, не требующих SSL-защищенных соединений. Для SSL-защиты нужны дополнительные шаги, *и* мы

расскажем о них в следующем разделе, посвященном правилам публикации Web-серверов с применением SSL-протокола.

Для запуска мастера создания правила публикации Web-сервера откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел **Firewall policy** (Политика брандмауэра), а затем — вкладку **Tasks** (Задачи). На вкладке **Tasks** (Задачи) щелкните кнопкой мыши ссылку **Publish a Web Server** (Опубликовать Web-сервер).

На экран будет выведена страница **Welcome to the New Web Publishing Rule Wizard** (Вас приветствует мастер создания нового правила публикации Web-сервера). На этой странице в текстовое поле **Web publishing rule name** (Название правила публикации Web-сервера) введите название правила. Щелкните мышью кнопку **Next (Далее).**

Страница Select Rule Action

На странице **Select Rule Action** (Выберите действие правила) можно выбрать **Allow** (Разрешить) или **Deny** (Запретить) соединения с опубликованным Web-сервером. Обратите внимание, что на этой странице по умолчанию выбран вариант **Allow** (Разрешить) в отличие от установки по умолчанию **Deny** (Запретить) в Мастере создания правила доступа. Большинство правил публикации Web-серверов будут разрешать доступ к Web-сайтам и определенные маршруты между этими Web-сайтами. Однако можно создать правила публикации Web-серверов, запрещающие доступ к точно настроенным правилам публикации Web-серверов, разрешающим доступ. Выберите вариант действия **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее). На рис. 8.1 показан выбор по умолчанию на странице **Select Kule Action** (Выберите действие правила).

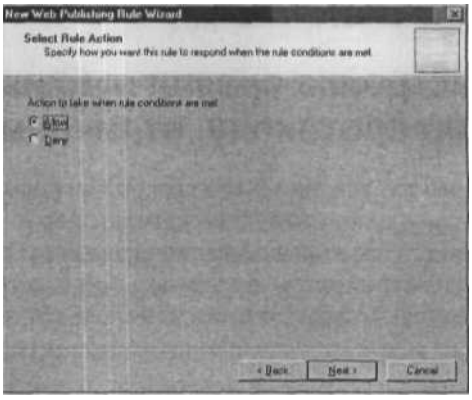


Рис. 8.1. Страница Select Rule Action (Выберите действие правила)

Страница Define Website to Publish

На странице **Define Website to Publish** (Определите Web-сайт для публикации) предоставляется информация о Web-сайте в сети, защищенной брандмауэром ISA. Как видно из рис. 8.2, на этой странице расположены следующие параметры:

- Computer name or IP address (Имя компьютера или IP-адрес);
- Forward the original host header instead of the actual one (specified above) (Пере сылать исходный заголовок хоста вместо фактического, заданного выше);
- Path (Путь);
- Site (Сайт).

В текстовое поле **Computer name or IP address** (Имя компьютера или IP-адрес) введите IP-адрес полностью определенного имени домена (fully-qualified domain name, FQDN) Web-сервера или сети, защищенной брандмауэром ISA. Если используется полностью определенное имя домена, убедитесь, что брандмауэр ISA способен выполнить разрешение этого имени в IP-адрес Web-сервера в корпоративной **сети,** а не в IP-адрес во внешнем интерфейсе брандмауэра ISA. Это очень распространенная ошибка администраторов брандмауэра ISA. Уверенность в том, что имя должным образом преобразовано в частный адрес Web-сервера, обеспечит создание инфраструктуры разделяемого DNS-сервера или включение записи в файл HOSTS на брандмауэре ISA.

Одно из первостепенных преимуществ применения FQDN в поле **Computer name or IP address** (Имя компьютера или IP-адрес) состоит в том, что имя Web-сайта появляется в поле URL журнала регистрации Web-прокси брандмауэра ISA. Если используется IP-адрес, в этом поле появится IP-адрес опубликованного сервера и затруднит эффективный анализ данных журнала регистрации.

Мы обсудим достоинства инфраструктуры разделяемого DNS и способы его создания позже в этой главе.

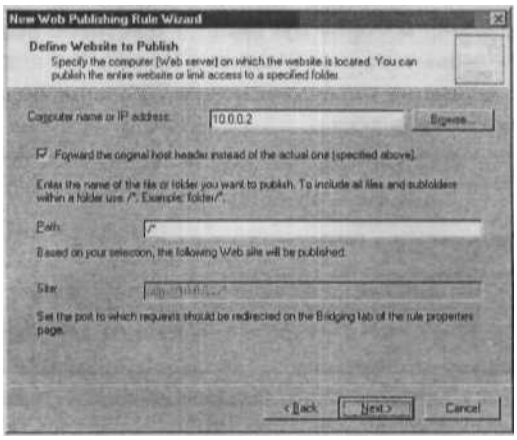


Рис. 8.2. Страница **Define Website to Publish** (Определите Web-сайт для публикации)

Переключатель **Forward the original host header instead of the actual one (specified above)** (Пересылать исходный заголовок хоста вместо фактического, заданного выше) — очень интересный параметр, потому что его смысл до конца не ясен. Можно предположить, что вместо значения заголовка хоста в поле **Computer name or IP address** (Имя компьютера или IP-адрес), посылаемого на опубликованный сервер, действительный заголовок хоста в запросе, посланном внешним клиентом, пересылается на опубликованный Web-сервер. Это важно, если на одном Web-сервере содержится несколько Web-сайтов и Web-сайты используют разные заголовки хостов.

Можно видеть влияние пересылки исходных заголовков хоста или ее отсутствия на рис. 8.3-8.5. На рис. 8.3 показаны заголовки хоста так, как они видны во внешнем интерфейсе брандмауэра ISA из запроса клиента на соединение для **www. msfirewall.org.** Заголовок хоста **HTTP: Host =www.msfirewall.org** появляется в трассировке сетевого монитора.

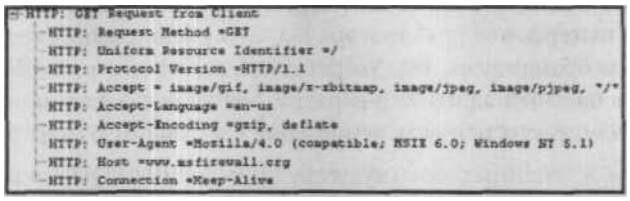


Рис. 8.3. HTTP-заголовки, которые видны во внешнем интерфейсе брандмауэра ISA

Если в правиле публикации Web-сервера не установлен флажок пересылки исходного заголовка хоста и *в* текстовом поле **Computer name or IP address** (Имя компьютера или IP-адрес) задан IP-адрес, то в трассировке сетевого монитора (см. рис. 8.4), полученной на опубликованном Web-сервере, видна запись **HTTP: Host =10.0.0.2,** которая не является заголовком хоста, содержащим исходный адрес клиента. Это просто значение, которое мы ввели в текстовое поле **Computer name or IP address** (Имя компьютера или IP-адрес). На рис. 8.4 показан пример HTTP-заголовков, которые видны на опубликованном Web-сервере, когда не задана пересылка исходных заголовков хоста.

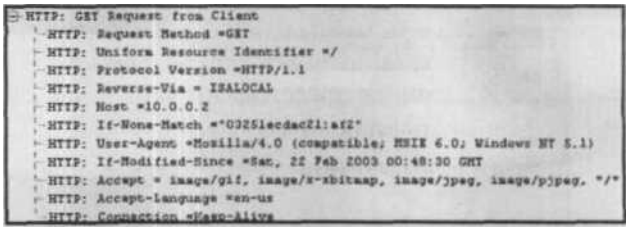


Рис. 8.4. HTTP-заголовки, которые видны на опубликованном Web-сервере, если не задана пересылка исходного заголовка хоста

На рис. 8.5 показано, что появляется на опубликованном Web-сервере, если установлен флажок **Forward the original host header instead of the actual one (specified above)** (Пересылать исходный заголовок хоста вместо фактического, заданного выше). В данном случае в трассировке Сетевого монитора показано, что на Web-сервере будет виден заголовок хоста HTTP: Host =www. msfirewall.org.

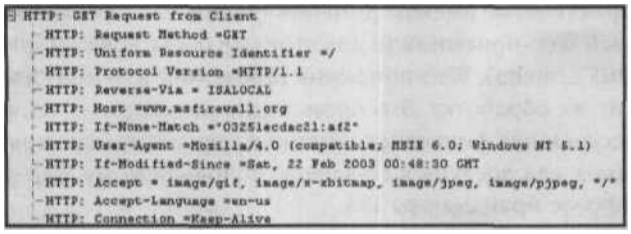


Рис. 8.5. HTTP-заголовки, которые видны на опубликованном Web-сервере, когда пересылается исходный заголовок хоста

В текстовое поле **Path** (Путь) вводятся пути к каталогам, которые нужно сделать доступными на опубликованном Web-сервере. Можно ввести имя конкретной папки или файла или предоставить **доступ** ко всем файлам и папкам внутри папки, используя символьную маску /*. Этот параметр позволяет ограничить доступ определенными файлами и папками. Хотя в этом параметре можно задать единственный путь, позже выяснится, что мы сможем вызвать диалоговое окно **Properties** (Свойства) правила публикации Web-сервера и создать дополнительные пути и даже перенаправления путей.

Поле **Site** (Сайт) не является текстовым полем, и в него ничего нельзя ввести. В нем показан URL-адрес, доступный на опубликованном Web-сайте.

В данном примере мы ввели **10.0.0.2** в поле **Computer name or IP address** (Имя компьютера или IP-адрес) и выбрали пересылку исходного заголовка хоста. Мы ввели путь /*. Теперь щелкнем мышью кнопку **Next** (Далее).

Страница Public Name Details

На странице **Public Name Details** (Параметры общедоступного имени) указывается, какие полностью определенные имена или IP-адреса будут применять пользователи для соединения с опубликованным Web-сайтом с помощью правила публикации Web-сервера. На этой странице представлены следующие параметры:

- Accept requests for (Принимать запросы к);
- Path (optional) (Путь, необязательный);
- Site (Сайт).

Раскрывающийся список **Accept requests for** (Принимать запросы к) предоставляет два варианта **Any domain name** (Любое имя домена) и **This domain name (type below)** (Данное имя домена, ввести ниже). Если вы выбираете **Any domain**

name (Любое имя домена), любые запросы к имени домена или IP-адресу принимаются Web-прием ником для этого правила. Это *очень плохой выбор,* потому что он потенциально может открыть сеть для вирусов, атак червей (worm attacks) или злоумышленников.

Например, некоторые распростра ненные черви будут посылать запросы на ГСР-порт 80 или к фиктивным именам доменов (таким как www.worm.com) на IP-адрес, используемый Web-приемником для этого правила. Если выбрать **Any domain name** (Любое имя домена), Web-приемник примет все эти запросы как правомерные и продолжит их обработку. Это происходит несмотря на то, что не размещаются никакие ресурсы для фиктивного имени домена, которое червь или злоумышленник применяют для доступа к IP-адресу, используемому Web-приемником во внешнем интерфейсе брандмауэра ISA.

Мы рекомендуем всегда использовать в правилах публикации Web-серверон вариант **This domain name (type below)** (Данное имя домена, ввести ниже). В этом случае вводится точное имя домена, который должен быть включен в пользовательский запрос к Web-приемнику. Если желательно принимать запросы только к домену www.msfirewall.org, то входящие запросы кhttp://l.1.1.1 или http://www.worm.com будут удалены, как не соответствующие имени домена, к которому нужно применять данное правило.

Если выбран вариант **This domain name (type below)** (Данное имя домена, ввести ниже), нужно ввести в текстовое поле **Public name** (Общедоступное имя) имя домена, к которому будет применено данное правило. В нашем примере мы ввели полностью определенное имя домена **www.msfirewall.org.** Страница **Public Name Details** (Параметры общедоступного имени) позволяет ввести только одно имя доменг, но можно добавить имена доменов после завершения мастера. Однако мы рекомендуем применять единственное имя домена в каждом правиле публикации Web-сервера.

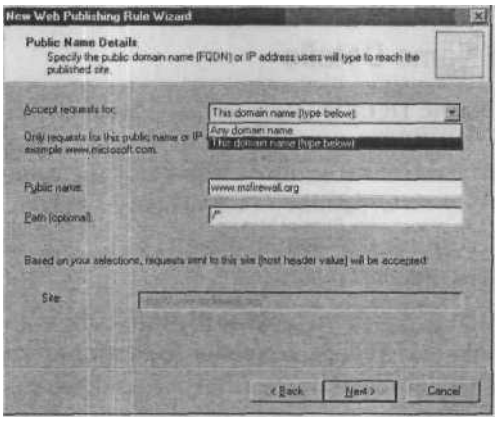


Рис. 8.6. Страница Public Name Details (Параметры общедоступного имени)

Текстовое поле **Path (optional)** (Путь, необязательный) позволяет ограничить путь (пути), разрешающий пользователям доступ с помощью данного правила публикации Web-сервера. Возможно, необходимо разрешить пользователям доступ только к определенным каталогам на вашем Web-сайте, а не к Web-сайту целиком. Несмотря на то, что на странице **Public Name Details** (Параметры общедоступного имени) можно ввести единственный путь (рис. 8.6), дополнительные пути можно будет добавить после завершения мастера, в диалоговом окне **Properties** (Свойства) для данного правила.

Страница Select Web Listener и создание Web-приемника для протокола HTTP

Web-приемникдля правила публикации Web-сервера назначается на странице **Select Web Listener** (Выберите Web-прием ни к). Web-приемник — это сетевой объект, применяемый в правилах публикации Web-серверов. Web-приемник ожидает (прослушивает) входящие подключения к заданному порту в интерфейсе или на выбранном IP-адресе. Например, если создается правило публикации Web-сервера, разрешающее по HTTP- протокол у общий доступ к сайту www.msfirewall.org, то придется создать Web-приемник, ожидающий запросы во **внешнем** интерфейсе брандмауэра ISA, используя IP-адрес, в который внешние пользователи преобразуют www. msfirewall.org.

> ПРИМЕЧАНИЕ В только что приведенном примере предполагается, что у внешнего интерфейса брандмауэра ISA есть связанный с ним общедоступный адрес. Ситуация несколько изменяется, если имеется брандмауэр перед брандмауэром ISA и связь с помощью средств NAT между внешним брандмауэром и брандмауэром ISA. В этом случае внешние клиенты разрешают имя www.msfirewall.org в общедоступный адрес на внешнем брандмауэре, который затем отображается в IP-адрес на Web-приемнике внутреннего брандмауэра ISA.

Если на брандмауэре ISA уже есть сконфигурированные Web-прием ники, на странице **Select Web Listener** (Выберите Web-прием ник) имеются кнопки:

- Edit (Редактировать);
- New (Новый).

Кнопка **Edit** (Редактировать) позволяет настроить существующие Web-приемники, а кнопка **New** (Новый) — создать новый Web-приемник. В данном примере на брандмауэре ISA нет созданных Web-прием ни ко в, поэтому щелкнем мышью кнопку New (Новый).

На странице **Welcome to the** New **Web Listener Wizard** (Вас приветствует мастер создания нового Web-приемника) введите имя Web-приемника в текстовое поле **Web listener** name (Имя Web-приемника). В данном примере мы назовем Web-при-

емник **HTTP Listener** (пока у нас есть только один IP-адрес, связанный с внешним интерфейсом; если бы было несколько адресов, мы могли бы добавить номер в последний байт определения приемника для облегчения идентификации каждого приемника). Щелкните мышью кнопку **Next** (Далее).

На странице **IP Addresses** (IP-адреса) выберите сети и IP-адреса в этих сетях, которые будет проверять приемник. Напомним, что каждый интерфейс брандмауэра ISA представляет сеть и все IP-адреса, доступные из этого интерфейса, считаются частью этой сети. Web-приемник может ожидать запросы в любой сети, определенной в брандмауэре ISA.

В данном примере мы хотим принимать входящие соединения от пользователей Интернета, поэтому установим флажок для сети **External** (Внешняя). С этого момента Web-приемник будет принимать запросы на соединение со всеми адресами, связанными с внешним интерфейсом брандмауэра ISA. Мы рекомендуем при наличии нескольких IP-адресов, связанных с интерфейсом, настроить Web-приемник для использования одного из этих адресов. Такое решение обладает большей гибкостью, поскольку можно настроить свойства каждого приемника. Если разрешить приемнику ожидать запросы со всех адресов интерфейса, приемнику будет назначен единый набор свойств.

На странице **IP Addresses** (IP-адреса) щелкните мышью кнопку **Addresses** (Адреса), как показано на рис. 8.7.

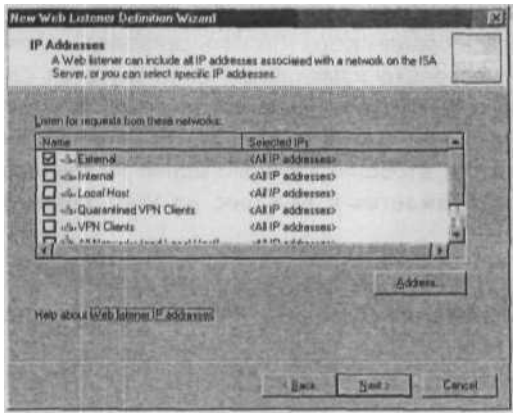


Рис. 8.7. Страница IP Addresses (IP-адреса)

На странице **Network Listener IP Selection** (Выбор IP для приемника сети) (рис. 8.8) есть три варианта:

- All IP addresses on the ISA Server computer that are in the selected network (Все IP-адреса на компьютере с ISA Server, которые находятся в выбранной сети);
- The default IP address on the ISA Server computer in the selected network (IP-адрес по умолчанию на компьютере с ISA Server, находящийся в выбранной сети);

- Specified IP addresses on the ISA Server computer in the selected network (Определенные IP-адреса на компьютере с ISA Server, находящиеся в выбранной сети).

Вариант **АЛ IP addresses on the ISA Server computer that are in the selected network** (Вее IP-адреса на компьютере с ISA Server, которые находятся в выбранной сети) выбран по умолчанию так же, как установка флажка на предыдущей странице без каких-либо дополнительных настроек. Этот вариант позволяет приемнику ожидать запросы на все адреса, связанные с интерфейсом, представляющим сеть (сети), выбранную вами. Если выбрать более одной сети, Web-приемник проверяет IP-адреса, связанные с каждой из выбранных вами сетей.

Вариант **The default IP address on the ISA Server computer in the selected network** (IP-адрес по умолчанию на компьютере с ISA Server, находящийся в выбранной сети) позволяет приемнику принимать подключения к *первичному,* или *основному,* IP-адресу *{primary* IP address), связанному с интерфейсом сети. Первичный адрес — это первый адрес *в* списке адресов, связанных с интерфейсом сети, Это также интерфейс, который используется для соединений, *покидающих* этот интерфейс (исходящих).

Вариант **Specified IP addresses on the ISA Server computer in the selected network** (Определенные IP-адреса на компьютере с ISA Server, находящиеся в выбранной сети) позволяет выбрать конкретные IP-адреса, необходимые для приемника. Доступные для сети IP-адреса появляются в списке **Available IP addresses** (Доступные IP-адреса). Выберите IP-адрес, который должен использовать Web-приемник, и щелкните мышью кнопку **Add** (Добавить), после этого он появится в области **Selected IP Addresses** (Выбранные IP-адреса).

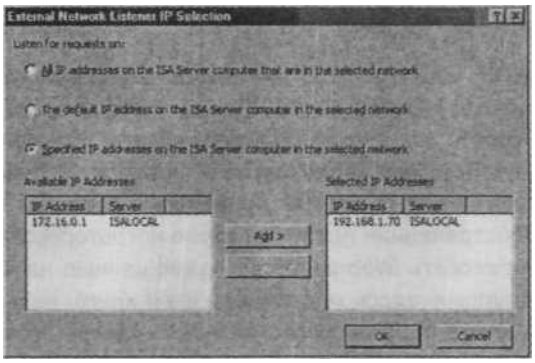


Рис. 8.8. Диалоговое окно External Network Listener IP Selection (Выбор IP для приемника сети)

Пример на рис. 8.8 демонстрирует, что основное внимание в брандмауэре ISA уделяется сети. Прежде чем мы выбрали адрес, оба адреса, **172.16.0.1** и **192.168.1.70,** находились в списке **Available IP Addresses** (Доступные IP-адреса). Эти два адреса в действительности связаны с двумя *разн ыми* адаптерами. Адрес **192.168.1.70** свя-

зан с внешним интерфейсом (интерфейс со сконфигурированным на нем шлюзом по умолчанию), а адрес **172.16.0.1** связан с интерфейсом DMZ (сети периметра) на брандмауэре ISA. Причина, по которой оба адреса включены в список, состоит в том, что внешняя сеть по умолчанию содержит *все IP-адреса, которые не определены как часть сети.* Поскольку мы не определили сеть DMZ, адрес, связанный с DMZ-интерфейсом, является по умолчанию частью внешней сети.

На рис. 8.8 мы выбрали IP-адрес, связанный с внешним интерфейсом брандмауэра ISA. Щелкните мышью кнопку ОК и затем кнопку **Next** (Далее) на странице IP **Addresses** (IP-адреса).

На странице **Port Specification** (Спецификация порта), показанной на рис. 8.9, вы можете определить TCP-порт, на который Web-приемник принимает входящие соединения. По умолчанию задан TCP-порт 80. Вы можете выбрать любой другой порт, но он не должен конфликтовать с сокетом, уже использующимся на брандмауэре ISA.

У вас также есть возможность разрешить Web-приемнику ожидать запросы на ожидающий SSL-порт (SSL listening port). Мы рекомендуем конфигурировать HTTP- и SSL-приемники отдельно. Это новое свойство брандмауэра ISA 2004. Мы изложим подробности конфигурирования SSL-приемников в следующем разделе этой главы.

ПРЕДУПРЕЖДЕНИЕ Нельзя настроить на приемнике SSL-протокол до тех пор, пока у вас нет сертификата машины (machine certificate), находящегося в хранилище сертификатов компьютеров брандмауэра ISA. Мы подробно обсудим эту настройку позже, в этой главе.

В примере, приведенном на рис. 8.9, мы используем порт по умолчанию и щелкаем мышью кнопку **Next** (Далее).

ПРЕДУПРЕЖДЕНИЕ Сокет — это комбинация транспортного протокола (TCP или UDP), IP-адреса и номера порта. Только один процесс может связать себя с сокетом. Если с сокетом, используемым для Web-приемника, связан другой процесс, необходимо заблокировать процесс, использующий сокет, или выбрать другой номер порта для применения в вашем Web-приемнике. Это широко распространенная проблема администраторов брандмауэра ISA, пытающихся опубликовать Web-ресурсы, размещенные на самом брандмауэре ISA. Как уже упоминалось много раз в этой книге, нельзя запускать на брандмауэре ISA какие-либо сервисы, за исключением собственных сервисов брандмауэра ISA, сервисов, от которых зависит брандмауэр ISA, и дополнительных сервисов, улучшающих возможность отслеживающей состояние соединений проверки прикладного уровня на брандмауэре ISA.

Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Web Listener Wizard** (Завершение мастера создания нового Web-приемника). Подробное описание Web-приемника появится на странице **Listener properties** (Свой-

ства приемника). Теперь можно щелкнуть мышью кнопку Edit (Редактировать) для настройки некоторых характеристик Web-приемника.

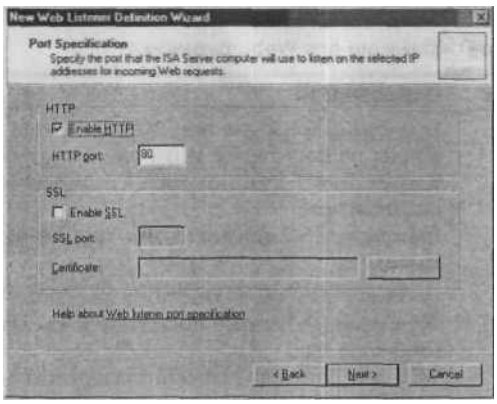


Рис. 8.9. Страница Port Specification (Спецификация порта)

дивидуальные параметры) (рис. 8.10). На этой вкладке можно настроить Aut tication (Аутентификация) и Advanced (Расширенные) свойства приемника.

Щелкните мышью кнопку Edit (Редактировать), а затем вкладку Preferences (Индивидуальные параметры) (рис. 8.10). На этой вкладке можно настроить Authen нтификация) и Advanced (Расширенные) свойства приемника.

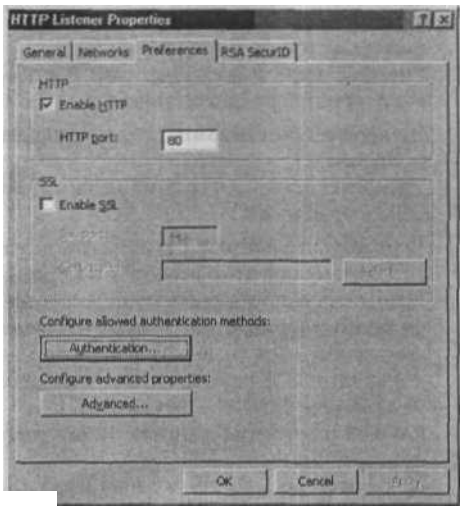


Рис. 8.10. Вкладка Preferences (Индивидуальные параметры)

Щелкните мышью кнопку Authentication (Аутентификация) и в диалоговом окне Authentication (Аутентификация) (рис. 8.11) будут видны параметры аутентификации, доступные для Web-приемника. По умолчанию выбран метод аутентифика-

ции Integrated (Интегрированная). В табл. 8.1 приведены все методы аутентификации, допустимые на Web-приемниках, и дано краткое описание важных характеристик каждого из них.

Табл. 8.1. Методы аутентификации для Web-приемника

Метод аутентификации	Подробности
Basic (Базовая)	Поддерживается для всех Web-клиентов и серверов Имена пользователей и пароли кодируются (Base64), но не шифруются. Легко получить с помощью любого сетевого анализатора Использует SSL-протокол для защиты базовой аутентификации Поддерживает делегирование базовой аутентификации
Digest (На основе хэша)	Верительные данные посылаются как однонаправленный (one-way) хэш Web-обозреватель должен поддерживать протокол HTTP 1.1. Требует на контроллере домена хранения пароля с применением реверсивного шифрования (reversible encryption) Шифрование WDigest также поддерживается (только в Windows Server 2003) Имя пользователя и имя домена чувствительны к состоянию регистра (case sensitive) Когда брандмауэр ISA и контроллер домена работают под управлением ОС Windows Server 2003, шифрование WDigest используется по умолчанию Учетные записи пользователей Windows NT 4.0 не поддерживают аутентификацию Digest
Integrated (Интегрированная)	Использует механизмы аутентификации NTLM, Kerberos и Negotiate Применяется хэширование имени пользователя и пароля перед отправкой
RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя)	Верительные данные регистрирующегося пользователя автоматически отправляются на брандмауэр ISA Если подлинность регистрирующегося в системе пользователя не подтверждается, появляется окно регистрации. Это окно выводится на экран до тех пор, пока правильные имя пользователя и пароль не будут введены или не будет выбрана команда CANCEL (Отменить) RADIUS и аутентифицирует, и авторизует (подтверждает полномочия) Пользователи RADIUS должны ввести верительные данные в формате DOMAIN\User Брандмауэр ISA применяет хэш MD5 совместно используемого пароля (shared secret) для аутентификации с помощью сервера RADIUS, шифрующего имя пользователя, пароль и характеристики соединения

Табл. 8.1. (продолжение)

Метод аутентификации	Подробности
	Рекомендуется применять протокол IPSec (протокол безопасности IP) для защиты канала связи между брандмауэром ISA и сервером RADIUS Серверы RADIUS, сконфигурированные на брандмауэре ISA, применяются ко всем правилам и объектам, использующим аутентификацию RADIUS. Вы не можете сформировать отдельные списки серверов RADIUS для аутентификации в VPN (Virtual Private Network, виртуальная частная сеть) и на Web-приемниках. Однако вы можете выбрать из списка отдельные серверы RADIUS для правил публикации Web-серверов и VPN-аутентификации При использовании аутентификации RADIUS в правилах публикации Web-серверов убедитесь в возможности пересылки верительных данных базовой аутентификации в правило публикации Web-сервера
SecurlD	Двухфакторная аутентификация Требуются физический маркер и персональный идентификационный номер (PIN, personal ID number) На брандмауэре ISA выполняется RSA ACE/Agent RSA ACE/Agent передает верительные данные серверу RSA/ACE Идентификационные данные (Cookie) помещаются в обозреватель пользователя после успешной аутентификации, они хранятся в памяти и не записываются на диск. Пароль удаляется из памяти, когда закрывается обозреватель При использовании аутентификации SecurlD применяйте SSL-протокол для защиты соединения Web-обозревателя с брандмауэром ISA Обратитесь к системе Help брандмауэра ISA Server 2004 для получения подробных сведений о конфигурации Не может применяться *в* комбинации с другими методами аутентификации
OWA Forms-based (OWA, Outlook Web Access, Web-доступ в Outlook, основанный на формах)	Применяется для публикации сервиса Outlook Web Access (OWA, Web-доступ в Outlook) Брандмауэр ISA генерирует форму для регистрации После успешной аутентификации в обозреватель посылаются данные cookie Верительные данные не кэшируются в обозревателе клиента Пользователи должны повторно пройти аутентификацию, если обозреватель закрылся, покинув Web-сайт с сервисом OWA Нельзя задать ограничения времени ожидания сеанса (session time-out limits) Рекомендуется устанавливать SSL-соединен и е между обозревателем и брандмауэром ISA Можно изменять пароль во время сеанса связи, но после смены пароля нужна повторная аутентификация

(см. след. стр.)

Табл. 8.1. (окончание)

Метод аутентификации	Подробности
	Может использоваться только с аутентификацией RADII'S после применения оперативной коррекции (hotfix). Найти подробности этой конфигурации можно по адресу http:// support.microsoft.com/default.aspx?scid=kb;en-us;884560
SSL Certificate (с помощью SSL-сертификата)	Пользователи аутентифицируются, представляя сертификаты пользователя Наиболее безопасная форма аутентификации

Способы аутентификации показаны на рис. 8.11.

Рис. 8.11. Диалоговое окно **Authentication** (Аутентификация)

Выбранный вариант аутентификации действует, только если ограничен доступ пользователю или группе в правиле публикации Web-сервера. Если разрешен доступ всем пользователям (All Users) в правиле публикации Web-сервера, то способ аутентификации игнорируется. Приведенные методы подтверждения подлинности применяются только для аутентификации, выполняемой брандмауэром ISA, но не для аутентификации, которую может потребовать опубликованный Web-сайт.

Все способы аутентификации, за исключением RADIUS требуют, чтобы брандмауэр ISA был членом домена. Это несущественная проблема до тех пор, **пока** не используется каскадная конфигурация брандмауэров, *в* которой внешний, или входной, (front-end) брандмауэр — это брандмауэр ISA (выходной или внутренний брандмауэр может быть любым предпочитаемым вами типом брандмауэра, включая брандмауэры ISA). Если брандмауэр ISA расположен на входе, и необходимо аутентифицировать пользователей на внешнем сервере, мы рекомендуем использовать только аутентификацию RADIUS. Если брандмауэр ISA расположен на выходе (back-end), мы всегда советуем сделать его членом домена службы каталогов Active Directory, чтобы можно было воспользоваться многочисленными преимуществами

защищенности, присущей членству в домене. Если же есть политические причины, препятствующие включению выходного брандмауэра ISA в домен, все равно можно использовать в сценарии преимущества аутентификации RADIUS.

Установите флажок **Require all users to authenticate** (Требуется аутентификация всех пользователей), если необходимо подтверждение подлинности для всех правил публикации Web-серверов, которые будут использовать данный приемник.

ПРЕДУПРЕЖДЕНИЕ Хотя переключатель Require all users to authenticate (Требуется аутентификация всех пользователей) следует устанавливать для Web-приемников, применяемых в правилах публикации Web-серверов, мы не *рекомендуем* делать это для Web-приемников, используемых для исходящего доступа через брандмауэр ISA клиентами Web-прокси. Мы обсуждали этот вывод более подробно в главе 5.

Щелкните мышью кнопку **RADIUS Servers** (Серверы RADIUS), чтобы выбрать или добавить сервер для аутентификации RADIUS.

Щелкните мышью кнопку **Select Domain** (Выбрать домен) для указания домена по умолчанию, если вы хотите выбрать базовую аутентификацию.

Щелкните мышью **кнопку Configure** (Настроить), расположенную справа от строки **Configure OWA forms-based authentication** (Настройте основанную на формах аутентификацию OWA), для того, чтобы настроить параметры cookie для OWA-соединения. Мы обсудим эту задачу более подробно позже в этой главе.

Щелкните мышью **кнопку ОК,** чтобы закрыть диалоговое окно **Authentication** (Аутентификация). В диалоговом окне **HTTP Listener Properties** (Свойства HTTP-приемника) щелкните мышью кнопку **Advanced** (Расширенные). На экране появится диалоговое окно **Advanced Settings** (Расширенные установочные параметры), показанное на рис. 8.12. В этом диалоговом окне вы можете задать **Number of connections** (Количество соединений), которое вы хотите поддерживать на приемнике, и допустимое время бездействия соединения для приемника. Щелкните мышью кнопку ОК, чтобы закрыть диалоговое окно Advanced Settings (Расширенные установочные параметры).

СОВЕТ Без предварительной настройки невозможно использовать аутентификацию RADIUS вместе с основанной на формах аутентификацией. На брандмауэре можно применить оперативную коррекцию (hotfix), которая позволит применять основанную на формах аутентификацию совместно с аутентификацией RADIUS. Для получения более подробной информации откройте статью You cannot use the RADIUS authentication protocol when you use the Outlook Web Access (OWA) Forms-Based Authentication on a Web publishing rule to publish an internal Web site such as OWA in ISA Server 2004 (вы не можете использовать протокол аутентификации RADIUS, если вы используете аутентификацию OWA, основанную на формах, в правиле публикации Web-сервера, применяемом для публикации внутреннего Web-сайта, такого как OWA, в брандмауэре ISA Server 2004) по адресу http://support.microsoft.com/default.aspx?scid=kb;en-us;884560.

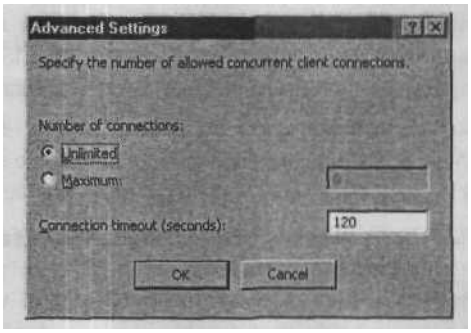


Рис. 8.12. Диалоговое окно **Advanced Settings** (Расширенные установочные параметры)

Щелкните мышью кнопку OK, чтобы закрыть диалоговое окно **HTTP Listener Properties** (Свойства HTTP-приемника), и щелкните мышью кнопку **Next** (Далее) на странице **Select Web Listener** (Выберите Web-приемник).

Страница User Sets

На странице **User Sets** (Наборы пользователей) (рис. 8.13) определяется, нужна ли аутентификация для доступа к Web-серверу, публикуемому с помощью данного правила публикации Web-сервера. Установка по умолчанию — **All Users** (Все пользователи), означающая, что никакой аутентификации не требуется для доступа к Web-серверу, публикуемому с помощью данного правила публикации Web-сервера. Щелкните мышью кнопку **Add** (Добавить), если хотите потребовать аутентификацию. Выводится диалоговое окно **Add Users** (Добавить пользователей), в котором можно выбрать набор пользователей (User Set), содержащий пользователей, к которым нужно применить данное правило.

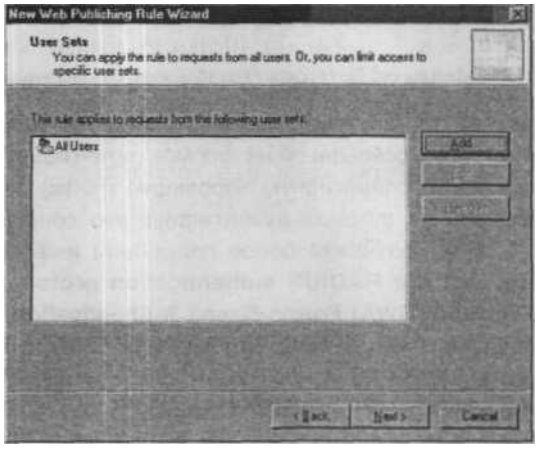


Рис. 8.13. Страница **User** Sets (Набор пользователей)

Имейте в виду, что параметр **All Users** (Все пользователи) означает только, что не требуется аутентификация, когда Web-приемник не настроен на требование подтверждения подлинности. Для настройки правила публикации Web-сервера, разрешающего доступ пользователя с анонимными верительными данными, применяйте набор пользователей **All Users** (Все пользователи).

Мы обсудим наборы пользователей, способы их создания и использования в главе 10. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователей) и затем щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Web Publishing Rule Wizard** (Завершение мастера создания нового правила публикации Web-сервера).

Диалоговое окно Properties правила публикации Web-сервера

Новое правило публикации Web-сервера появляется в списке **Firewall Policy** (Политика брандмауэра). Щелкните правой кнопкой мыши **Web Publishing Rule** (Правило публикации Web-сервера) и левой кнопкой мыши команду **Properties** (Свойства). Окно **Properties** (Свойства) правила публикации Web-сервера содержит вкладки: *ш* General (Общие);

- Action (Действие);
- From (От);
- To (Кому);
- Traffic (Трафик);
- Listener (Приемник);
- Public Name (Общедоступное имя);
- Paths (Пути);
- Bridging (Сопряжение);
- Users (Пользователи);
- Schedule (Расписание);
- Link Translation (Трансляция ссылок).

Давайте рассмотрим параметры каждой из этих вкладок. Оказывается, на этих вкладках есть много параметров, не представленных в мастере создания нового правила публикации Web-сервера.

Вкладка General

На этой вкладке можно изменить название правила публикации Web-сервера, введя название в текстовое поле **Name** (Название). Можно также ввести описание правила в текстовое поле **Description (optional)** (Описание, необязательное). Имеется возможность разрешить или заблокировать правило публикации Web-сервера, установив или сбросив флажок **Enable** (Разрешить), как показано на рис. 8.14.

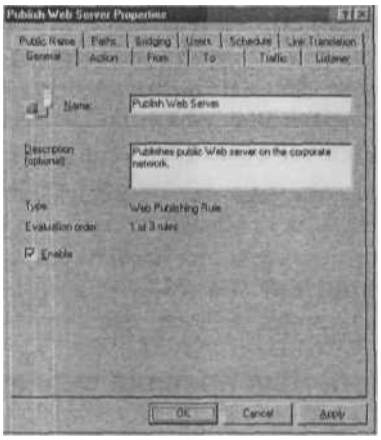


Рис. 8.14. Вкладка **General** (Общие)

Вкладка Action

На вкладке **Action** (Действие) вы разрешаете (Allow) или запрещаете (Deny) доступ к сайту, сконфигурированному в правиле публикации Web-сервера. Есть также возможность **Log requests matching this rule** (Регистрировать запросы, соответствующие правилу). Если окажется, что файлы регистрации становятся слишком большими и сайт, к которому осуществляется доступ с помощью данного правила, не представляет особого интереса, то можно отказаться от регистрации запросов, поддерживаемой этим правилом. Но мы настоятельно рекомендуем не **отказываться** от регистрации в любых правилах публикации, потому что большинство этих правил представляют подключения из непроверенных или не заслуживающих доверия сетей.

Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений, сделанных на этой вкладке (рис. 8.15).

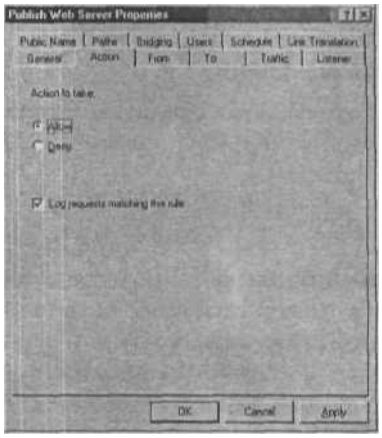


Рис. 8.15. Вкладка **Action** (Действие)

Вкладка From

На вкладке From (От) настраиваются источники, от которых вы хотите с помощью правила публикации Web-сервера принимать запросы на соединения с опубликованным сайтом. По умолчанию выбрано местонахождение Anywhere (Везде), означающее, что любой хост, который может достичь IP-адрес или адреса, используемые на Web-приемнике, получит доступ к этому правилу публикации Web-сервера.

Можно ограничить доступ к данному правилу публикации Web-сервера, щелкнув мышью местонахождение Anywhere (Везде), а затем кнопку Remove (Удалить). После удаления элемента Anywhere (Везде), щелкните мышью кнопку Add (Добавить). В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните кнопкой мыши папку, содержащую сетевой объект, которому нужно разрешить доступ к правилу публикации Web-сервера.

На вкладке From *(От)* есть также параметр для точной настройки доступа к правилу с помощью определения исключений в поле Exceptions (Исключения). Например, можно разрешить доступ к правилу публикации Web-сервера всем сетям, за исключением хостов, находящихся в той же сети, что и опубликованный сервер. Это в общем хорошая идея, поскольку не стоит создавать петли через брандмауэр ISA для хостов корпоративной сети, подключающихся к ресурсам, находящимся в той же корпоративной сети.

Щелкните мышью кнопку Apply (Применить) на вкладке From (От) (рис. 8.16) после внесения изменений.

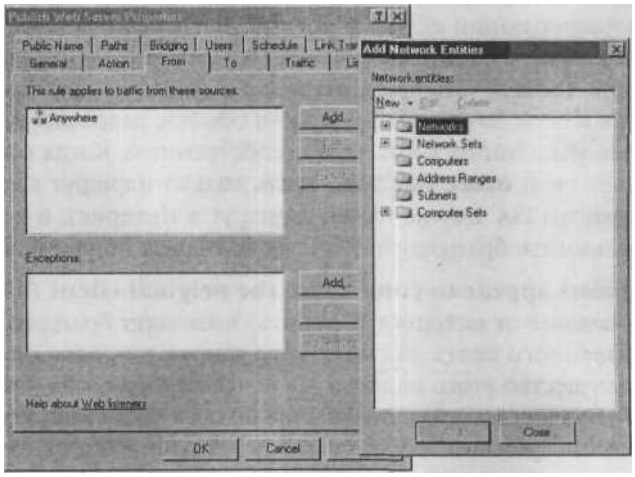


Рис. 8.16. Вкладка From (От)

Вкладка To

Вкладка To (Кому) — одна из самых важных вкладок в диалоговом окне **Properties** (Свойства). Причина заключается в том, что строка, которую вы вводите в текстовое поле **Server** (Сервер) определяет имя хоста в форме URL-адреса, который правило публикации Web-сервера посылает на публикуемый Web-сайт. Текстовая строка из текстового поля **Server** (Сервер) замещает заголовок хоста, включенный в исходный запрос клиента, посланный брандмауэру ISA. Если нежелательно, чтобы брандмауэр ISA заменял строку в заголовке хоста строкой из текстового поля **Server** (Сервер), установите флажок **Forward the original host header instead of the actual one (specified above)** (Пересылать исходный заголовок хоста вместо фактического адреса, заданного выше).

Еще один важный выбор, предлагаемый на вкладке To (Кому), — возможность определить, как брандмауэр ISA обрабатывает с помощью прокси запросы к серверу, приведенному в текстовом поле **Server** (Сервер). Имеется два варианта.

- Requests appear to come from the ISA Server computer (Запросы отображаются как пришедшие с компьютера брандмауэра ISA Server).
- Requests appear to come from the original client (Запросы отображаются как пришедшие от исходного клиента).

Вариант **Requests appear to come from the ISA Server computer** (Запросы отображаются как пришедшие с компьютера брандмауэра ISA Server) полезен, если вы не хотите делать опубликованный Web-сервер клиентом SecureNAT. Один из основных недостатков конфигурации клиента SecureNAT заключается в том, что инфраструктура маршрутизации целиком должна знать, что брандмауэр ISA — шлюз для сети Интернет. Многие организации имеют установленную инфраструктуру маршрутизации, но не хотят делать брандмауэр ISA последним пристанищем в маршрутах всех хостов в сети. Эту проблему можно обойти, разрешив брандмауэру ISA заменять IP-адрес удаленного хоста своим собственным. Когда опубликованный сервер возвращает свой ответ, ему надо знать только маршрут к локальному интерфейсу брандмауэра ISA. Ему не нужен маршрут в Интернет, и у него нет необходимости использовать брандмауэр ISA как свой шлюз по умолчанию.

Вариант **Requests appear to come from the original client** (Запросы отображаются как пришедшие от исходного клиента) позволяет брандмауэру ISA сохранять IP-адрес удаленного хоста, посылающего запрос ресурсов опубликованного Web-сайта. Преимущество этого подхода заключается в том, что можно включать в отчеты реальные IP-адреса хостов, подключившихся к Web-сайту, если на Web-сервере установлено программное обеспечение для формирования отчетов на основе информации журналов регистрации. Если этот вариант не используется, то в журналах регистрации на Web-сайте все соединения будут регистрироваться как пришедшие с ГР-адреса брандмауэра ISA.

С этим вариантом связана одна проблема: если разрешить реверсивное представительство для опубликованного Web-сайта, появится ряд запросов, инициированных непосредственно брандмауэром ISA, и можно неверно истолковать это как неспособность брандмауэра ISA сохранить IP-адрес запрашивающего хоста. Это неверно и в данном случае никак не связано с ошибкой или скрытой проблемой программного обеспечения брандмауэра ISA. Дело в том, что при выполнении реверсивного представительства брандмауэр ISA использует ответы из собственного кэша. Однако брандмауэр ISA в роли реверсивного прокси-сервера должен проверять статус объектов на Web-сайте и в ходе этой проверки с адреса брандмауэра ISA генерируются запросы к опубликованному Web-сайту, которые последовательно появляются в журналах регистрации Web-сайта.

По этой причине мы (и не только мы) предпочитаем анализировать активность Web-сайта на основании журналов регистрации сервиса Web-прокси брандмауэра ISA вместо регистрационных журналов самого Web-сайта. Правда из этого правила есть исключения, но для общедоступных сайтов, к которым не обращаются пользователи внутренней сети, журналы регистрации сервиса Web-прокси на брандмауэре ISA предоставляют наиболее полную и точную информацию.

Параметры вкладки To (Кому) показаны на рис. 8.17.

СОВЕТ Мы рекомендуем использовать полностью определенное имя домена (FQDN) в текстовом поле Server (Сервер) на вкладке To (Кому). Это позволит включить в журнал регистрации Web-прокси записи с этим именем и облегчит контроль доступа к опубликованным серверам. Кроме того, FQDN будет появляться в любом созданном вами отчете.

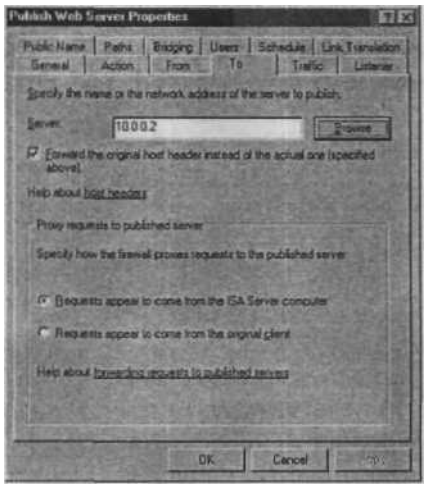


Рис. 8.17. Вкладка To (Кому)

Вкладка Traffic

На вкладке **Traffic** (Трафик) виден список протоколов, разрешенных данным правилом публикации Web-сервера. На этой вкладке протоколы не настраиваются. Напротив, разрешенные протоколы определяются набором поддержки протоколов на Web-приемнике, сконфигурированном для данного правила публикации.

Флажок **Notify HTTP users to use HTTPS instead** (Уведомить пользователей о применении HTTPS-протокола вместо HTTP) в данном примере недоступен, потому что мы не используем SSL-приемник. Установка флажка разрешает брандмауэру ISA возвращать страницу ошибок пользователю, обращающемуся к Web-сайту по правилу публикации Web-сервера, показывая, что вместо HTTP следует использовать HTTPS-протокол (HyperText Transmission Protocol, Secure, протокол защищенной передачи гипертекстов). Ввод HTTP-протокола вместо HTTPS — это широко распространенная ошибка пользователей при обращении к защищенным сайтам. К счастью, потребуется менее трех секунд на вставку символа «s» в обозначение протокола и повторение запроса. Требование применения корректного протокола вынуждает пользователей соблюдать надлежащую «интернет-гигиену».

Переключатель **Require 128-bit encryption for HTTPS traffic** (требовать 128-битное шифрование для HTTPS-трафика) также недоступен, поскольку данное правило не применяется для SSL-публикации. Этот параметр позволяет управлять уровнем защиты с помощью шифрования SSL-соединений к опубликованному Web-сайту. Во все современные клиенты Windows 128-битное шифрование включено в поставку, но есть устаревшие клиенты Windows и клиенты не-Windows, не поддерживающие его; возможно, потребуется блокировать подключения таких относительно небезопасных клиентов.

Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений, сделанных вами на вкладке трафика, показанной на рис. 8.18.

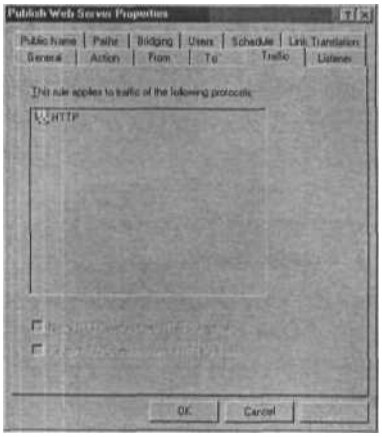


Рис. 8.18. Вкладка Traffic (Трафик)

Вкладка Listener

На вкладке **Listener** (Приемник) можно просмотреть характеристики приемника, используемого в данный момент правилом публикации Web-сервера, и изменить их, щелкнув мышью кнопку **Properties** (Свойства). Можно также создать новый Web-приемник, щелкнув мышью кнопку New (Новый) и затем применив новый приемник к данному правилу публикации Web-сервера.

Если уже создано несколько Web-приемников наданном брандмауэре ISA, можно изменить приемник, применяемый правилом публикации Web-сервера, щелкнув мышью стрелку, направленную вниз, в раскрывающемся списке **This rule applies to requests received on the following listener** (Правило применяется к запросам, получаемым на следующий приемник).

Щелкните мышью кнопку **Apply** (Применить) после внесения изменений на вкладке **Listener** (Приемник) (рис. 8.19).

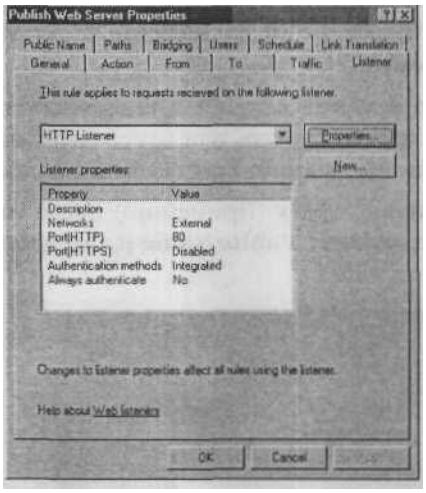


Рис. 8.19. Вкладка **Listener** (Приемник)

Вкладка Public Name

Вкладка **Public Name** (Общедоступное имя) позволяет просмотреть и сформировать имена, которые можно использовать для доступа к Web-серверу, **опубликованному** данным правилом публикации Web-сервера. В правиле публикации, созданном нами в этом примере, выбрано в качестве общедоступного имени имя **www.msfirewall.org,** которое может применяться для доступа к Web-серверу. Если запрос приходит на Web-приемник, используемый данным правилом публикации Web-сервера, с полностью определенным именем домена, отличным от приведенного, правило проигнорирует запрос на соединение. Имейте в виду, если Web-прием ни к

применяется другими правилами публикации Web-серверов, входящий запрос будет сравниваться с компонентами вкладки **Public Name** (Общедоступное имя) в этих других правилах. Если ни в одном из них не найдется общедоступного имени, совпадающего с именем в заголовке хоста (Host header) входящего Web-:ianpoca, соединение будет удалено.

Также обратите внимание на то, что к многочисленным именам хостов может применяться единственное правило публикации Web-сервера. Ключ к успеху — уверенность в том, что каждое из этих имен хостов преобразуется (разрешается) в IP-адрес или адреса, которые ожидает Web-приемник, связанный с этим правилом. Например, Web-приемник данного правила может ожидать IP-адрес, который разрешается в два имени: www.msfirewall.org и www.tacteam.net. В таком случае можно было бы добавить www.tacteam.net в список **Public Name** (Общедоступное имя). Однако это также означает, что одни и те же пути, ретрансляция, пользователи, расписание и другие установочные параметры применялись бы к соединениям, поступающим на Web-сайт www.tacteam.net. Это не всегда может быть правильным, именно поэтому мы советуем создавать отдельные правила публикации Web-сервера для каждого публикуемого сайта.

Можно добавить новое общедоступное имя к списку, щелкнув мышью кнопку **Add** (Добавить), также можно удалить или отредактировать выбранное общедоступное имя, щелкнув мышью кнопки **Edit** (Редактировать) и **Remove** (Удалить).

Щелкните мышью кнопку **Apply** (Применить) после того, как сделаны все необходимые изменения на вкладке **Public Name** (Общедоступное имя), показанной на рис. 8.20.

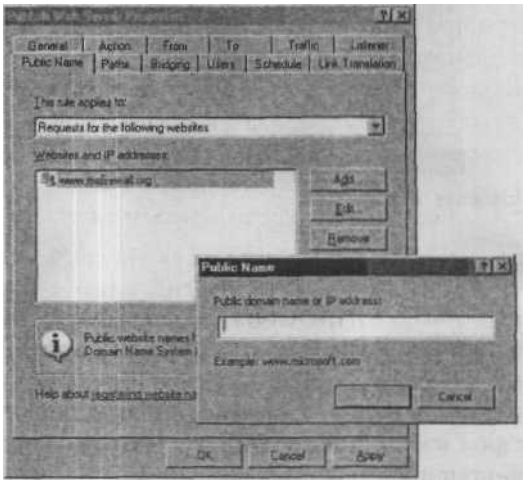


Рис. 8.20. Вкладка Public Name (Общедоступное имя)

Вкладка Paths

Вкладка **Paths** (Пути) позволяет контролировать, как обращения к разным путям, включенные в запросы, обрабатываются правилом публикации Web-сервера. Обратите внимание, что в списке путей есть два столбца: **External Path** (Внешний путь) и **Internal Path** (Внутренний путь).

External Path (Внешний путь) — это путь, указанный пользователем, запрашивающим Web-сайт с помощью правила публикации Web-сервера. Например, если пользователь вводит в обозревателе URL-адрес http://www.msfirewall.org/docs, внешний путь — **/docs.** Если пользователь в обозревателе набирает URL-адрес http://www.tacteam.net/graphics, то внешний путь — **/graphics.**

Internal Path (Внутренний путь) — это базирующийся на содержимом внешнего пути путь, по которому брандмауэр ISA перешлет запрос. Допустим, что мы задали внешний путь как /docs, а внутренний путь — как **/publicdocuments.** Когда пользователь введет в обозревателе URL-адрес http://www.msfirewall.org/docs и Web-приемник для данного правила в брандмауэре ISA установит соединение для запроса, брандмауэр ISA перешлет запрос на сайт, приведенный на вкладке To (Кому) по пути **/publicdocuments.** Если на вкладке To (Кому) указан адрес **10.0.0.2,** брандмауэр ISA пересылает запрос к опубликованному Web-серверу как **http://10.0.0.2/publicdocuments.**

Перенаправление пути придает большую гибкость правилам публикации Web-серверов и позволяет упростить пути, используемые внешними пользователями для доступа к опубликованным ресурсам, не требуя изменения имен каталогов на опубликованном Web-сервере.

Если необходимо получить доступ ко всем папкам и файлам в конкретном каталоге, введите путь в формате: **/path/*.** Если нужно разрешить доступ к единственному файлу в заданном пути, введите путь в формате: **/path.** Например, если необходимо разрешить доступ ко всем файлам в каталоге documents на Web-сервере, введите для внутреннего пути строку **/documents/*.** Если нужно разрешить доступ только к файлу names.htm в каталоге documents, введите путь как **/documents/**names.htm. Пример вкладки **Paths** (Пути) показан на рис. 8.21.

Щелкните мышью кнопку **Add** (Добавить), чтобы добавить новый путь. В диалоговом окне **Path mapping** (Отображение пути) введите *внутренний путь* в текстовое поле **Specify the folder on the Web site that you want to publish. To publish the entire Web site, leave this field blank** (Задайте папку на Web-сайте, которую хотите опубликовать. Для публикации целого Web-сайта оставьте это поле пустым). Далее выберите один из вариантов: **Same as published folder** (Такой же, как опубликованная папка) или **The following folder** (Следующая папка), показанных на рис. 8.22. Если внешние пользователи вводят тот же путь, выберите вариант **Same** as **published folder** (Такой же, как опубликованная папка). Если пользователи

будут указывать другой путь, выберите вариант The following folder (Следующая папка) и введите в текстовое поле заменяющий путь.

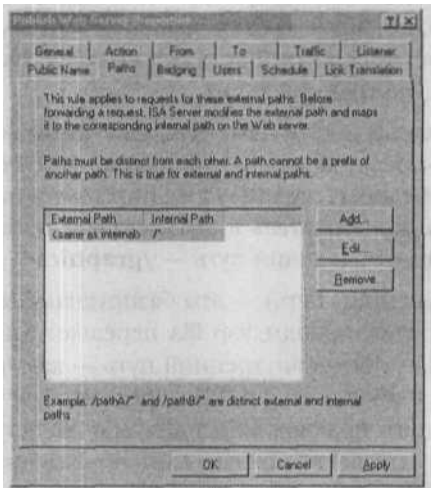


Рис. 8.21. Вкладка Paths (Пути)

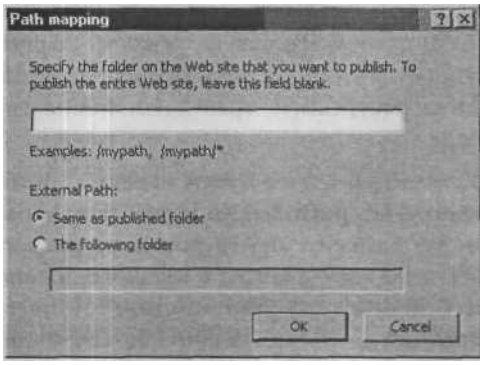


Рис. 8.22. Диалоговое окно **Path Mapping** (Отображение пути)

СОВЕТ Многие администраторы брандмауэра ISA хотят перенаправлять на начальную страницу Web-сайта путь, введенный пользователем. Например, если пользователь вводит URL-адрес http://www.msfirewall.org/firewalldocs, запрос должен быть перенаправлен на начальную страницу Web-сервера **10.0.0.2.** Это можно сделать, введя внешний путь как /firewalldocs/*, а внутренний путь — как / (рис. 8.23). Теперь все подключения к каталогу firewalldocs перенаправляются на начальную страницу сервера, приведенного в списке на вкладке To (Кому), в данном случае **10.0.0.2.**

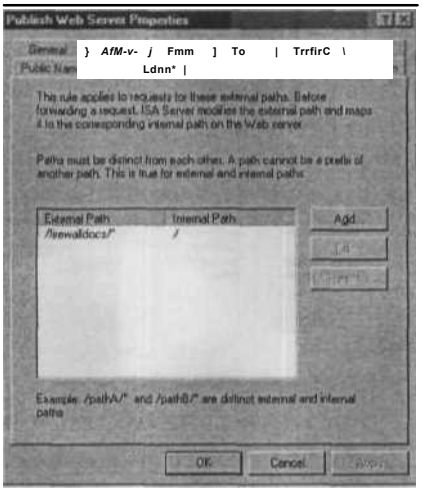


Рис. 8.23. Перенаправление на начальную страницу Web-сайта с помощью указания пути

Общее желание администраторов брандмауэра ISA — перенаправлять соединения с начальной страницей Web-сайта в папку **/Exchange** на Web-сайтах Outlook Web Access (OWA, Web-доступ в Outlook). Это легко сделать с помощью перенаправления пути на вкладке **Paths** (Пути). В этом случае внешний путь — /*, а внутренний — /Exchange\. Учтите, что необходимо использовать обратный слэш (\) в конце пути, потому что уже существует внутренний путь **/Exchange/** после выполнения **Mail Server Publishing Wizard** (Мастер публикации почтового сервера). Об этом мастере мы расскажем больше позже в этой главе. Вкладка **Paths** (Пути) с таким типом конфигурации OWA будет выглядеть, как приведенная на рис. 8.24.

Такой способ срабатывает, потому что Web-сайт OWA благожелательно настроен и готов помочь дилетантам, не видящим разницы между путями UNC (Universal Naming Convention, соглашение об универсальном назначении имен) и HTTP. Web-сайт OWA примет обратный слэш как допустимый запроси преобразует его «на лету» в прямой слэш. Это позволяет использовать два внутренних пути: /Exchange\ и /exchange/* на вкладке **Paths** (Пути), что было бы сделать невозможно, если бы вам пришлось ввести два прямых слэша, так как брандмауэр ISA не разрешает вводить множественные отображения пути, использующие один и тот же префикс (начальную часть) пути. Конфигурация OWA показана на рис. 8.24.

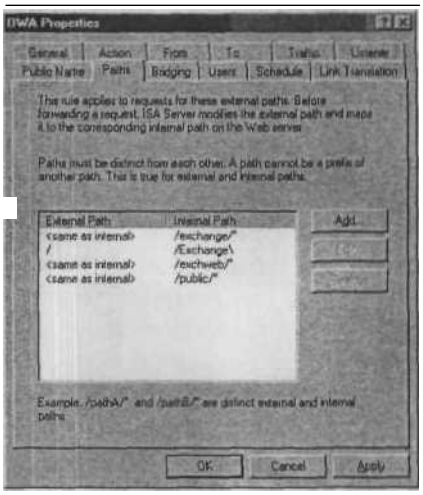


Рис. 8.24. Отображение начальной страницы Web-сайта OWA в папку Exchange

Кроме того, можно перенаправить заданные пути на разные серверы. Например, рассмотрим следующие URL-адреса:

- www.msfirewall.org/scripts;
- www.msf irewall.org/articles;
- www.msfirewall.org/ids-ips.

Все три URL-адреса указывают на одно и то же полностью определенное имя домена и отличаются только путями. Можно создать три правила публикации Web-сервера, в каждом из которых используется одно и то же общедоступное имя **(Public Name),** но содержатся разные конфигурации пути и различные серверы на вкладке To (Кому). Когда пользователь выполняет запрос, используя один из трех URL-адресов, запрос направляется на соответствующий сервер, основываясь на установках, сделанных на вкладках **Public Name** (Общедоступное имя), **Paths** (Пути) и To (Кому).

Вкладка Bridging

Вкладка **Bridging** (Сопряжение), показанная на рис. 8.25, позволяет сконфшурировать переадресацию порта или протокола для правила публикации Web-сервера. На вкладке приведены следующие параметры:

- Web Server (Web-сервер);
- Redirect requests to HTTP port (Перенаправлять запросы на HTTP-порт);
- Redirect requests to SSL port (Перенаправлять запросы на SSL-порт);
- Use a certificate to authenticate to the SSL Web server (Использовать сертификат для аутентификации при SSL-соединении с Web-сервером);
- FTP server (FTP-сервер);

- Use this port when redirecting FTP requests (Использовать данный порт при переадресации FTP-запросов).

Переключатель **Web Server** (Web-сервер) конфигурирует правило публикации Web-сервера на пересылку HTTP- или HTTPS-запросов. С этим параметром не связано перенаправление протоколов.

Установленный флажок **Redirect requests to HTTP port** (Перенаправлять запросы на HTTP-порт) позволяет перенаправить входящие HTTP-запросы для данного правила и Web-приемника опубликованного Web-сервера, используя порт в текстовом поле справа от флажка. По умолчанию установлен TCP-порт 80. Вы можете выбрать любой другой порт для переадресации. Это позволит вам использовать альтернативные номера портов на опубликованных Web-сайтах, в то же время по-прежнему принимая запросы на HTTP-порт по умолчанию, используемый Web-приемником (хотя нет нужды в применении HTTP-порта по умолчанию на Web-приемнике, если сконфигурирован Web-приемник на ожидание запроса к дополнительному порту).

Переключатель **Redirect requests to SSL port** (Перенаправлять запросы на SSL-порт) позволяет переадресовать запросы на заданный SSL-порт. Имейте в виду, что вы можете выбрать оба флажка: и для HTTP-, *и* для SSL-порта. В этом случае входящий трафик маршрутизируется в соответствии с протоколом и портом. Например, если поступает HTTP-запрос, он пересылается на HTTP-порт, а если приходит SSL-запрос, он передается на SSL-порт. Можно изменить SSL-порт, на который перенаправляется запрос, это полезно, если имеются SSL-сайты, опубликованные на дополнительных портах.

Один из самых недооцененных параметров пользовательского интерфейса брандмауэра ISA — флажок **Use a certificate to authenticate to the SSL Web server** (Использовать сертификат для аутентификации при SSL-соединении с Web-сервером). Этот параметр *не* используется брандмауэром ISA для приема входящих SSL-соединений от пользователей, подключающихся к опубликованному Web-серверу. Он позволяет настроить брандмауэр ISA для предоставления *сертификата пользователя* опубликованному Web-сайту, когда последний требует сертификат пользователя для аутентификации. Сертификат пользователя связан с сервисом Firewall на брандмауэре ISA, позволяющим брандмауэру ISA представлять сертификат пользователя для аутентификации на Web-сайте.

Переключатель **FTP server** (FTP-сервер) разрешает правилу публикации Web-сервера выполнять переадресацию протокола. Входящий запрос может быть как HTTP, так и HTTPS; соединение перенаправляется как FTP-запрос GET на опубликованный FTP-сайт. Использование перенаправления SSL-B-FTP полезно, если нужно обеспечить удаленный доступ к FTP-сайтам, требующим аутентификации. Поскольку F^{T}P-сайты поддерживают только базовую аутентификацию, можно защитить вериительные данные пользователя, применяя SSL-ссылку на внешний интерфейс брандмауэра ISA. Вкладка **Bridging** (Сопряжение) показана на рис. 8.25.

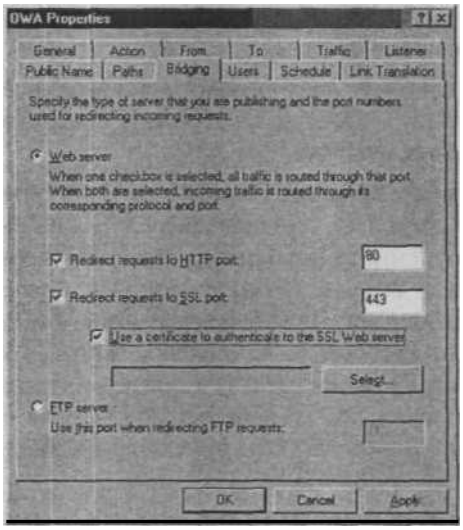


Рис. 8.25. Вкладка Bridging (Сопряжение)

Вкладка Users

Вкладка Users (Пользователи) предоставляет возможность задать пользователей, которые могут обращаться к Web-сайту с помощью правила публикации Web-сервера. Любой может получить доступ к Web-сайту через брандмауэр ISA, если разрешен доступ All Users (Все пользователи). Но это означает, что у всех пользователей есть возможность пройти через брандмауэр ISA и направить неаутентифицированные запросы к опубликованному Web-сайту. Web-сайт может самостоятельно требовать аутентификации, и в этом случае пользователю все же придется подтверждать свою подлинность.

Можно потребовать аутентификации на брандмауэре ISA, удалив группу All Users (Все пользователи) и вставив любую другую группу с помощью кнопки Add (Добавить). По умолчанию в брандмауэр ISA включены следующие группы: All Users (Все пользователи), All Authenticated Users (Все аутентифицированные пользователи) и System and Network Service (Системный и сетевой сервис). Можно добавить собственные группы брандмауэра и точно настроить свою схему аутентификации. Мы подробно рассказывали о группах брандмауэра и о том, как их применять в главе 7. На рис. 8.26 показано, как конфигурировать вкладку Users (Пользователи).

Возможность подтверждать подлинность пользователей на брандмауэре ISA обеспечивает существенное повышение уровня безопасности. Аутентификация на брандмауэре ISA мешает неаутентифицированным соединениям даже доходить до опубликованного Web-сервера. Атакующие злоумышленники, а также злонамеренный код могут использовать неаутентифицированное соединение для атаки на

опубликованный сервер. Подтверждение подлинности на брандмауэре, прежде всего, устраняет потенциальный риск нарушения безопасности.

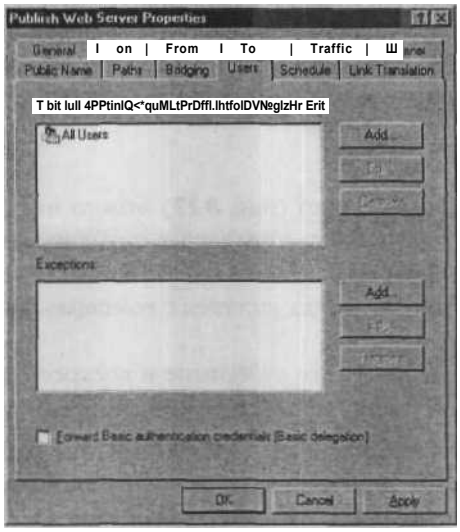


Рис. 8.26. Вкладка **Users** (Пользователи)

Имейте в виду, что можно потребовать аутентификации на Web-сайте для того, чтобы потребовать подтверждения подлинности и на брандмауэре ISA, и на Web-сайте. В некоторых ситуациях пользователи будут представлены двумя диалоговыми окнами регистрации: первый запрос аутентификации, сделанный брандмауэром ISA, а второй — опубликованным Web-сайтом.

Можно избежать двойного приглашения для аутентификации, воспользовавшись свойством одноразового подтверждения подлинности, *делегированием базовой аутентификации,* предоставляемым брандмауэром ISA. Это функциональная возможность станет доступной, если вы установите флажок Forward Basic authentication credentials (Basic delegation) (Пересылать верительные данные базовой аутентификации, базовое делегирование) на вкладке Users (Пользователи).

Делегирование базовой аутентификации дает возможность пользователям подтверждать свою подлинность с помощью брандмауэра ISA, используя базовую аутентификацию. Брандмауэр подтверждает подлинность пользователя. Если попытка аутентификации успешна, запрос пересылается на опубликованный Web-сайт. Если последний требует верительные данные, брандмауэр ISA передает верительные данные пользователя, полученные во время его успешной аутентификации на брандмауэре.

Потребуется разрешить базовую аутентификацию на Web-приемнике, используемом правилом публикации Web-сервера, и Web-сайт, на котором пользователь подтверждает свою подлинность, также должен применять базовую аутентификацию.

ПРЕДУПРЕЖДЕНИЕ Следует всегда разрешать Forward Basic authentication credentials (Basic delegation) (Пересылать верительные данные базовой аутентификации, базовое делегирование), если применяется аутентификация RADIUS в правилах публикации Web-серверов. Если не установить этот флажок, то придется столкнуться с противоречивыми результатами и многочисленными приглашениями регистрации для безуспешных соединений.

Вкладка Schedule

На вкладке **Schedule** (Расписание) (рис. 8.27) можно настроить расписания для управления временем доступа пользователей к опубликованному Web-сайту. Есть три расписания по умолчанию.

- **Always** (Всегда) Web-сайт всегда доступен с помощью правила публикации Web-сервера.
- **Weekends** (Выходные дни) все субботние и воскресные дни.
- **Work hours** (Рабочие часы) с понедельника по пятницу, с 9:00 до 17:00.

Можно также создать собственные пользовательские расписания. Мы рассматривали эту задачу в главе 7 при обсуждении политики исходящего доступа.

Рис. 8.27. Вкладка Schedule (Расписание)

Вкладка Link Translation

Свойство трансляции ссылок брандмауэра ISA позволяет перезаписывать URL-адреса, возвращаемые опубликованными Web-серверами. Перезапись URL-адресов полезна, если публикуются Web-сайты, жестко кодирующие ссылки на Web-страницах, возвращаемых пользователям, и эти ссылки не доступны из внешней сети.

Предположим, что мы посетили Web-сайт с URL-адресом www.msfirewall.org. Начальная страница с этим адресом содержит жестко закодированные ссылки в форме http://serverl/users и http://serverl /computers. Когда интернет-пользователь щелкает мышью одну из этих ссылок, соединение разрывается, поскольку пользователь Интернета не способен корректно разрешить имя **serverl** в IP-адрес во внешнем интерфейсе брандмауэра ISA.

Свойство трансляции ссылок брандмауэра ISA дает возможность перезаписать ссылки, содержащие **serverl,** в ссылки **www.msfirewall.org.** Когда Web-сервер возвращает начальную страницу сайта **www.msfirewall.org,** внешний пользователь больше не видит в них URL-адреса **serverl,** поскольку брандмауэр ISA перезаписал эти URL-адреса, включив **www.msfirewall.org** вместо **serverl.** Теперь внешний пользователь может щелкнуть мышью по ссылкам и получить доступ к содержимому Web-сервера (рис. 8.28).

Мы более подробно рассмотрим транслятор ссылок (Link Translator) брандмауэра ISA в главе 10.

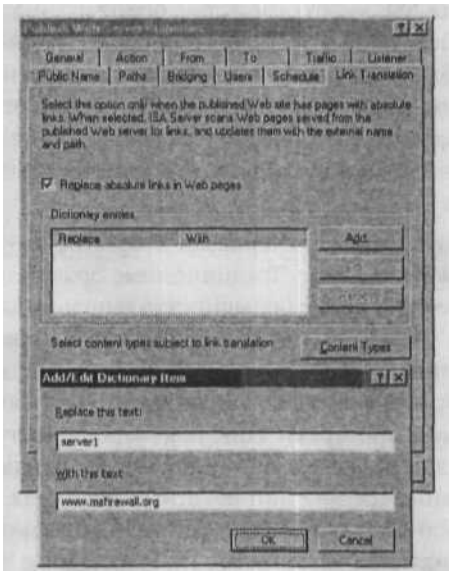


Рис. 8.28. Вкладка Link Translation (Трансляция ссылок)

Создание и настройка правил публикации Web-сервера по протоколу SSL

Можно публиковать защищенные Web-серверы, используя правила публикации Web-серверов по протоколу SSL. Публикация защищенных Web-серверов требует немного больше предварительной работы, поскольку нужно получить сертификат Web-сайта

для публикуемого Web-сайта, связать этот сертификат с Web-сайтом на опубликованном Web-сервере и затем связать сертификат Web-сайта с брандмауэром ISA, чтобы последний мог выдать себя за этот Web-сервер. Это позволяет брандмауэру ISA обеспечивать высокую степень защиты для Web-сайтов, опубликованных с помощью правил публикации Web-серверов по протоколу SSL.

В этом разделе мы обсудим следующие темы:

- сопряжение протокола SSL (SSL Bridging);
- импорт сертификатов Web-сайтов в хранилище сертификатов (certificate store) на машине брандмауэра ISA;
- запрашивание сертификатов Web-сайтов, чтобы брандмауэр представлял защищенные Web-сайты;
- создание правил публикации Web-серверов по протоколу SSL.

Сопряжение протокола SSL

Сопряжение протокола SSL — это свойство брандмауэра ISA, позволяющее ему выполнять на прикладном уровне отслеживающую состояние соединений проверку SSL-соединений с опубликованными с помощью правила публикации Web-сервера Web-серверами в сети, защищенной брандмауэром ISA. Это уникальное свойство дает возможность брандмауэру ISA обеспечить уровень отслеживающего состояние соединений контроля прикладного уровня, недостижимый сегодня другими брандмауэрами этого класса.

Сопряжение протокола SSL предотвращает сокрытие злоумышленниками их деяний в зашифрованном SSL-туннеле. Традиционные брандмауэры с отслеживающей соединения фильтрацией (такие как большинство «аппаратных» брандмауэров, представленных сегодня на рынке) не могут выполнять отслеживающую состояние соединений проверку прикладного уровня SSL-соединений, походя через них. Эти аппаратные брандмауэры с отслеживающей соединения фильтрацией фиксируют входящее SSL-соединение, проверяют список контроля доступа (Access Control List, ACL) брандмауэра и, если существует ACL-инструкция брандмауэру, основанному на отслеживающих состояние соединений пакетных фильтрах, переслать соединение на сервер корпоративной сети, пересылает его опубликованному серверу без какой-либо проверки потенциальных опасностей на прикладном уровне.

Брандмауэр ISA поддерживает два метода SSL-соп ряжения:

- сопряжение SSL-c-SSL (SSL to SSL bridging);
- сопряжение SSL-c-HTTP (SSL to HTTP bridging).

Сопряжение SSL-c-SSL обеспечивает защищенное SSL-соединение от начала до конца. Сопряжение SSL-c-HTTP гарантирует защищенное соединение между Web-клиентом и брандмауэром ISA, а затем разрешает пересылку открытого текста между брандмауэром ISA и опубликованным Web-сервером.

Для того чтобы понять, как брандмауэр ISA работает над защитой Web-сервера, давайте рассмотрим жизненный цикл соединения между Web-клиентом из Интернета и Web-сайтом в сети, защищенной брандмауэром ISA:

1. OWA-клиент из Интернета посылает запрос внешнему интерфейсу брандмауэ ра ISA.
2. Устанавливается сеанс связи между Web-клиентом из Интернета и внешним интерфейсом брандмауэра ISA.
3. *После* того как SSL-сеанс установлен, Web-клиент посылает имя пользователя и пароль брандмауэру ISA. SSL-туннель, который уже установлен между Web-кли ентом и брандмауэром ISA, защищает эти верительные данные.
4. Запрос расшифровывается, *прежде* чем брандмауэр пересылает его опублико ванному Web-серверу. Расшифрованные пакеты, полученные от Web-клиента, проверяются брандмауэром ISA и подвергаются отслеживающему состояние соединения контролю прикладного уровня с помощью HTTP-фильтра защиты или любых других фильтров контроля прикладного уровня, которые вы уста новили на брандмауэр ISA. Если брандмауэр ISA находит проблему в запросе, запрос удаляется.
5. Если запрос приемлемый, брандмауэр ISA Server повторно шифрует соединение и отправляет его через *второе* SSL-соединение, установленное между брандма уэром ISA и Web-сайтом, опубликованным в сети, защищенной брандмауэром.
6. Опубликованный Web-сервер расшифровывает пакет и отвечает брандмауэру ISA. Web-сервер шифрует свой ответ, прежде чем отправить его брандмауэру ISA.
7. Брандмауэр ISA расшифровывает ответ, полученный от опубликованного Web-сервера. Он обрабатывает ответ так же, как описано в п. 4. Если с ответом что-то не так, брандмауэр ISA удаляет его. Если ответ проходит отслеживающую состояние соединения проверку прикладного уровня, брандмауэр ISA снова шифрует сообщение и пересылает ответ Web-клиенту в Интернете, воспользо вавшись SSL-сеансом связи, который Web-клиент из Интернета уже установил с брандмауэром ISA.

Отличие SSL-туннелирования от SSL-сопряжения

Брандмауэр ISA в действительности участвует в двух SSL-сеансах, когда применяется сопряжение SSL-с-SSL:

- SSL-сеанс между Web-клиентом и внешним интерфейсом брандмауэра ISA;
- второй SSL-сеанс между внутренним интерфейсом брандмауэра ISA и опубли кованным Web-сервером.

Типичный отслеживающий состояние соединений брандмауэр с пакетной фильтрацией только выполняет пересылку соединений на опубликованные SSL-сайты. Иногда ее называют «SSL-туннелированием». Традиционный брандмауэр с отслеживающей соединения фильтрацией принимает SSL-сообщения на внешний интер-

фейс и пересылает их опубликованному SSL-серверу. Информация уровня приложения в сообщении полностью скрыта в SSL-туннеле, потому что у брандмауэра, основанного на пакетной фильтрации, нет механизма для расшифровки, проверки и повторного шифрования потока данных. Поскольку традиционные брандмауэры с отслеживающей состояние соединений фильтрацией не способны принимать решения о разрешении или запрете на основании знания содержимого зашифрованного туннеля, они пропускают вирусы, червей, переполнения буфера и другие злоумышленные деяния от Web-клиента к опубликованному Web-сайту.

А что же сопряжение SSL-c-HTTP?

Брандмауэр ISA может также выполнять сопряжение SSL-c-HTTP. В этом сценарии соединение между Web-клиентом и внешним интерфейсом брандмауэра ISA защищается в SSL-туннеле. Соединение между внутренним интерфейсом брандмауэра ISA и Web-сервером, опубликованным в корпоративной сети, устанавливается открытым и не шифруется. Это повышает производительность, поскольку устраняет затраты процессора на вторую SSL-ссылку.

Однако вы должны учитывать последствия сопряжения SSL-c-HTTP. Стив Райли (Steve Riley) (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/askus/auaswho.asp), руководитель проекта в команде ISA Server корпорации Microsoft, подчеркивает, что внешний пользователь, соединяющийся с опубликованным Web-сайтом, используя SSL-протокол, заключает неявное соглашение и рассчитывает на защиту всей транзакции. Мы согласны с этим определением. Внешний Web-клиент заключает то, что можно считать «социальным контрактом», с опубликованным Web-сервером и частью этого контракта является защита соединений от начала до конца.

Сопряжение SSL-c-SSL защищает данные с помощью сервисов SSL и брандмауэра ISA Server на всем протяжении соединения. Сопряжение SSL-c-HTTP защищает данные на отрезке от клиента до брандмауэра ISA и до тех пора пока они находятся на ISA Server, но данные не защищены при пересылке с брандмауэра ISA Server на сайт OWA во внутренней сети.

Центры сертификации предприятия и автономные центры сертификации

Упоминания центров сертификации (ЦС) (CA, Certificate Authorities) и инфраструктуры открытого ключа (PKI, Public Key Infrastructure) достаточно, чтобы многие администраторы отказались даже от обсуждения SSL-протокол а. Для этого есть ряд причин.

- Доступная документация о центрах сертификации и инфраструктуре открытых ключей трудна для понимания.
- Предмет может оказаться крайне сложным.

- Необходимо освоить полностью новую лексику для понимания роли центров сертификации и инфраструктуры открытого ключа. Часто в документации, от носящейся к этим темам, не определяются новые слова или используются зага дочные термины для определения непонятного вам термина.
- Кажется, что нет никакой технической поддержки у администратора сети и брандмауэра, который действительно хочет получить установку центра серти фикации и запустить его, чтобы использовать сертификаты для аутентифика ции по протоколам SSL и L2TP/IPSec (Layer Two Tunneling Protocol, протокол туннелирования на втором уровне модели OSI)/(Internet Protocol Security, про токол безопасности IP) и шифрования.

Мы не собираемся предлагать полный курс по инфраструктуре открытого ключа и серверу сертификации корпорации Microsoft, но хотим действительно помочь понять смысл решений, которые придется принимать при выборе центра сертификации для установки и использования.

При установке Microsoft Certificate Server (Сервер сертификации Microsoft) может быть выбрана одна из четырех ролей:

- Enterprise Root C A (Корпоративный корневой центр сертификации);
- Enterprise Subordinate CA (Корпоративный подчиненный центр сертификации);
- Standalone Root CA (Автономный корневой центр сертификации);
- Standalone Subordinate CA (Автономный подчиненный центр сертификации).

Корневой и подчиненный центры сертификации предприятия могут быть установлены только на серверах-членах службы каталогов Active Directory. Если требуется установить ЦС на компьютер, не член домена, инсталлируйте автономные корневой ЦС или подчиненный ЦС. Если устанавливается единственный сервер сертификации, необходимо инсталлировать его как корневой ЦС предприятия или автономный корневой ЦС. Подчиненные ЦС применяются в организациях, управляющих многочисленными центрами сертификации.

- Можно использовать автономную оснастку (standalone snap-in) **Certificates** (Сер тификаты) консоли управления MMCдля получения сертификатов компьютеров и пользователей — оснастка доступна только компьютерам-членам домена.
- Можно настроить групповую политику для автоматического выпуска сертифи катов компьютеров или пользователей с помощью *авторегистрации* — эта функциональная возможность доступна только компьютерам-членам домена.
- Можно использовать Web-сайт регистрации для получения сертификатов с по мощью Web-интерфейса.

Автономная оснастка **Certificates** (Сертификаты) консоли управления MMC или авто регистрация не могут применяться для получения сертификатов от автономных ЦС. Единственный способ получения сертификата от автономного ЦС — запросить его у Web-сайта регистрации автономного ЦС. Необходимо заполнить форму и предоставить на рассмотрение запрос. Сертификат выдается не моменталь-

но, поскольку ЦС знает о запрашивающем только то, что он указал в форме. Некоторым требуется визуальный контроль запроса, а затем утверждение его вручную. Далее запрашивающему придется использовать обозреватель, для того чтобы вернуться на Web-сайт регистрации и загрузить сертификат.

ЦС предприятия менее въедлив потому, что у него есть информация о запрашивающем. Поскольку запрос предназначен для компьютера или пользователя в домене, кто-то уже проверил пользователь или компьютер домена и счел член домена заслуживающим сертификата. ЦС предприятия предполагает, что у вас есть административный контроль над членами домена: пользователями и компьютерами, и вы можете оценить законность запросов на получение сертификатов с помощью пригодной для этого информации в Active Directory.

По этим причинам мы рекомендуем использовать ЦС предприятия. Далее мы будем предполагать, что используется ЦС предприятия.

Дополнительную информацию о центрах сертификации и инфраструктуре открытого ключа можно найти по адресу www. microsoft.com/windowsserver2 ЭОЗ/ technologies/pki/default.mspx.

Сопряжение SSL-c-SSL и конфигурация Web-сайта сертификатов

Одна из самых распространенных причин, по которой администраторы брандмауэра ISA отмахиваются от SSL- соединен ия и сопряжения SSL-c-SSL, — проблемы, с которыми они столкнулись, пытаясь заставить SSL-подключения выполняться корректно. И основной источник этих проблем — ошибка конфигурации, включающая взаимосвязь между конфигурацией сертификации и правилом публикации Web-сервера, применяемого для публикации Web-сайта.

На рис. 8.29 показаны подробности перенаправленного SSL-в-SSL соединения с общедоступным Web-сайтом Outlook Web Access (Web-доступ в Outlook).

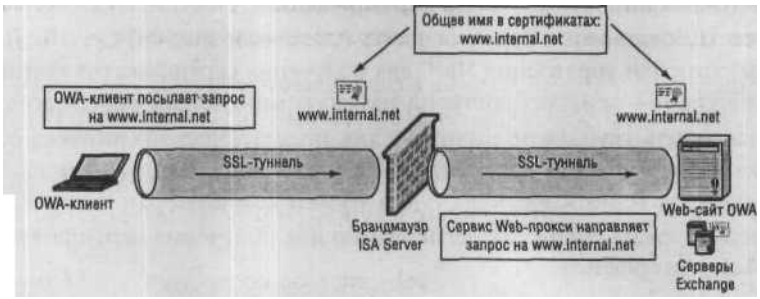


Рис. 8.29. Сопряжение SSL-c-SSL

1. Web-клиент посылает запрос https://www.internal.net/exchange/ на внешний интерфейс брандмауэра ISA Server, публикующего Web-сайт OWA 2003.

2. Брандмауэр ISA проверяет свои правила публикации Web-серверов, чтобы по смотреть, есть ли правило публикации Web-сервера, содержащее адресный **на бор** с полностью определенным именем домена (FQDN) www.internal.net и пу тем **/exchange.** Если есть правило публикации Web-сервера, соответствующее FQDN и пути, соединение будет установлено на основании инструкций пере сылки, включенных в правило публикации Web-сервера. Однако *прежде,* чем брандмауэр ISA сможет определить URL-адрес, должен быть установлен сеанс связи. Параметр **common name** (общее имя) *в сертификате,* который исполь зует брандмауэр ISA, чтобы выдать себя за Web-сайт OWA, должен *совпадать* с FQDN, применяемым Web-клиентом для соединения с сайтом. В данном примере общее имя в сертификате, используемом брандмауэром ISA, должно быть www. internal.net, для того чтобы оно совпало с полностью определенным именем домена, которое внешний клиент OWA применяет в своем запросе.
3. Брандмауэр ISA расшифровывает пакеты, анализирует их, а затем пытается соз дать новое SSL-соединение между собой и внутренним Web-сайтом OWA. Ана логично тому, как внешний клиент OWA соединяется с внешним интерфейсом брандмауэра ISA Server, сервис Web-прокси брандмауэра действует как клиент для Web-сайта OWA 2003 во внутренней сети. Запрос, который сервис Web-прокси посылает сайту OWA 2003 во внутренней сети, должен соответствовать **common name** (общее имя) в сертификате на Web-сайте OWA. Вот почему мы должны конфигурировать запрос, пересылаемый на URL-адрес www.internal.net, когда конфигурируем правило публикации Web-сервера. Мы напомним об этом фак те, когда будем обсуждать конфигурацию правила публикации Web-сервера.
4. После того как установлен SSL-сеанс между брандмауэром ISA и Web-сервером во внутренней сети, пакеты пересылаются на Web-сайт.

ПРИМЕЧАНИЕ Все машины, участвующие в SSL-сеансе (Web-клиент, брандмауэр ISA и Web-сайт) должны иметь сертификат ЦС от корневого центра сертификации в хранилище сертификатов Trusted Root Certification Authorities (Доверенные корневые центры сертификации).

Сеанс разрывается, когда общее имя в сертификате сервера не совпадает с именем, используемым в запросе клиента. Нормальный ход событий в сценарии со пряжения SSL-с-SSL может быть нарушен по двум причинам:

- если общее имя в сертификате, применяемом брандмауэром ISA Server, выдаю щим себя за Web-сайт, не совпадает с именем (FQDN), используемым Web-кли ентом из Интернета;
- если общее имя в сертификате на Web-сайте не соответствует имени (FQDN), применяемому сервисом брандмауэра ISA для пересылки запроса; имя в запро се брандмауэра ISA к опубликованному Web-серверу задается на вкладке To (К) в правиле публикации Web-сервера.

Не забудьте об этом, когда позже мы будем разрабатывать сопряжение SSL-с-SSL в нашем правиле публикации Web-сервера.

ПРЕДУПРЕЖДЕНИЕ Вы столкнетесь с Internal Server Error 500 (Ошибка внутреннего сервера 500), если существует несоответствие между именем в запросе и именем в сертификате.

Импорт сертификатов Web-сайтов в хранилище сертификатов на компьютере брандмауэра ISA

Брандмауэр ISA должен быть способен выдать себя за опубликованный Web-сервер и идентифицировать себя на удаленном клиенте как опубликованный сервер. Ключевым компонентом такой имитации служит общее имя в сертификате Web-сайта. Для выполнения этой задачи нужно установить сертификат Web-сайта на брандмауэре ISA.

Первый шаг — экспорт сертификата Web-сайта с Web-сайта защищенного Web-сервера. В состав консоли IIS (Internet Information Server, информационный сервер Интернета) входит легкий в использовании Certificate Wizard (Мастер сертификата), с помощью которого вы сможете экспортировать сертификат Web-сайта. Когда экспортируете сертификат, убедитесь, что включен секретный ключ. Одна из самых распространенных причин отказа в работе правил публикации Web-серверов — экспорт сертификата Web-сайта без его личного секретного ключа.

Затем сертификат Web-сайта импортируется в хранилище сертификатов на компьютере брандмауэра ISA. Сразу после импортирования сертификата Web-сайта в это хранилище сертификатов, он становится доступным для связывания с Web-приемником. Необходимо помнить, что, если нельзя связать сертификат с Web-приемником, значит сертификат импортирован некорректно.

Выполните следующие шаги для импорта сертификата Web-сайта в хранилище сертификатов на компьютере брандмауэра ISA.

1. Скопируйте сертификат Web-сайта на компьютер брандмауэра ISA.
2. Щелкните мышью кнопку **Start** (Пуск) и затем выберите в меню команду **Run** (Выполнить). В диалоговом окне **Run** (Выполнить) введите mmc в текстовое поле **Open** (Открыть) и щелкните мышью кнопку ОК.
3. На консоли щелкните мышью пункт меню **File** (Файл) и выберите команду **Add/Remove Snap-in** (Добавить/Удалить оснастку).
4. В диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку) щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **Add Standalone Snap-in** (Добавить автономную оснастку) щелкните мышью строку **Certificates** (Сертификаты) в списке **Available Standa lone** Snap-ins (Доступные автономные оснастки) и щелкните мышью кнопку **Add** (Добавить).

6. На странице **Certificates Snap-in** (Оснастка сертификатов) выберите параметр **Computer account** (Учетная запись компьютера) и щелкните мышью кнопку **Next** (Далее).
7. На странице **Select Computer** (Выберите компьютер) выберите **Local computer (the computer this console is running on)** (Локальный компьютер, компьютер, на котором запущена эта консоль), щелкните мышью кнопку **Finish** (Готово).
8. В диалоговом окне **Add Standalone Snap-in** (Добавить автономную оснастку) щелкните мышью кнопку **Close** (Закрыть).
9. Щелкните мышью кнопку ОК в диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку).
10. Раскройте узел **Certificates (Local Computer)** (Сертификаты, локальный ком пьютер) на левой панели консоли.
11. Раскройте узел **Personal** (Персональный) на левой панели консоли.
12. Щелкните правой кнопкой мыши узел **Certificates** (Сертификаты), укажите левой кнопкой мыши строку **All** Tasks (Все задачи) и щелкните левой кнопкой мыши команду **Import** (Импортировать).
13. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Import Wizard** (Вас приветствует мастер импорта сертификатов).
14. На странице **File to Import** (Файл для импорта) используйте кнопку **Browse** (Просмотр) для поиска сертификата, который скопирован на брандмауэр ISA. После того, как сертификат появится в текстовом поле **File name** (Имя файла), щелкните мышью кнопку **Next** (Далее).
15. Введите пароль, который вы назначили сертификату Web-сайта в текстовом поле **Password** (Пароль) на странице **Password** (Пароль). *Не* помечайте сертификат как экспортируемый. Щелкните мышью кнопку Next (Далее).
16. Согласитесь с установкой по умолчанию **Place all certificates in the following store** (Поместить все сертификаты в следующее хранилище) на странице **Certifi cate Store** (Хранилище сертификатов). Щелкните мышью кнопку **Next** (Далее).
17. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certifi cate Import Wizard** (Завершение мастера импорта сертификатов).
18. Щелкните мышью кнопку ОК в диалогогом окне **Certificate Import Wizard** (Мас тер импорта сертификатов).
19. Сертификат Web-сайта и сертификат ЦС появляются на правой панели консоли. У сертификата ЦС то же имя, что и у строки в столбце **Issued by** (Выпущенный).
20. Щелкните правой кнопкой мыши сертификат ЦС и выберите команду **Cut** (Вы резать).
21. Раскройте окно узла **Trusted Root Certification Authorities** (Доверенные кор невые центры сертификации) на левой панели консоли.
22. Щелкните правой кнопкой мыши узел **Certificates** (Сертификаты) и выберите команду **Paste** (Вставить). Если команда **Paste** не появится, повторите пункт 20 и попробуйте еще раз.

23. Вернитесь к узлу **Personal /Certificates** (Персональный/Сертификат) на левой панели и дважды щелкните мышью сертификат Web-сайта.
24. В диалоговом окне **Certificate** (Сертификат) щелкните кнопкой мыши вкладку **Certification Path** (Путь сертификации). На сертификате ЦС не должно быть красного крестика «х». Если же увидите красный крестик на сертификате ЦС, это означает, что он не импортирован должным образом в узел **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации).
25. Закройте диалоговое окно **Certificate** (Сертификат).
26. Закройте консоль mmc Не сохраняйте консоль.

Теперь сертификат Web-сайта импортирован в компьютерное хранилище сертификатов и будет доступен для связывания с Web-приемником в правиле публикации Web-сервера по протоколу SSL.

Запрос сертификата пользователя для представления его брандмауэром ISA защищенным Web-сайтам

Брандмауэр можно сконфигурировать для представления сертификата пользователя Web-сайтам, требующим сертификаты пользователей перед их подключением к сайту. Эти сертификаты пользователей называют также *клиентскими сертификатами (client certificates).* Можно сконфигурировать опубликованный Web-сайт для требования представления клиентского сертификата, прежде чем разрешено соединение. Клиентские сертификаты могут быть сопоставлены с учетными записями пользователей. Это позволяет пользователю подтверждать подлинность с помощью сертификата. Но можно потребовать у пользователей сертификаты, а затем обеспечить регистрацию верительных данных с помощью дополнительных методов аутентификации.

Можно запросить сертификат у пользователя для сервиса Firewall Service брандмауэра ISA, а затем сконфигурировать правило публикации Web-сервера на представление сертификата пользователя, когда Web-сайты требуют клиентские сертификаты. Первый шаг — требование сертификата для учетной записи сервиса Firewall Service брандмауэра ISA.

В следующем примере мы будем использовать консоль сертификатов MMC для импорта сертификата учетной записи сервиса Firewall брандмауэра ISA. Мы не сможем воспользоваться оснасткой **Certificates** (Сертификаты) консоли MMC для запроса сертификата учетной записи, но у нас есть возможность импортировать пользовательский сертификат, применяя Web-сайт регистрации.

Для того чтобы запросить сертификат для брандмауэра ISA с Web-сайта регистрации, мы должны сначала создать учетную запись пользователя для брандмауэра ISA. Создайте учетную запись пользователя с именем **isafirewall** в службе каталогов Active Directory до выполнения следующих процедур.

Выполните следующие шаги, чтобы запросить сертификат для учетной записи сервиса Firewall.

1. На компьютере с брандмауэром ISA откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быст рого доступа к сети Интернет 2004), раскройте окно, связанное с именем сер вера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач консоли. На этой вкладке щелкните кнопкой мыши ссылку **Show System Policy Rules** (По казать правила системной политики).
3. В списке **System Policy Rules** (Правила системной политики) щелкните пра вой кнопкой мыши Правило *2* **Allow all HTTP traffic from ISA Server to all networks (for CRL downloads)** (Разрешить весь HTTP-трафик от брандмауэра **ISA** ко всем сетям, для загрузок CRL) и левой кнопкой мыши команду **Edit System Policy** (Редактировать системную политику).
4. На вкладке **General** (Общие) правила **System Policy Rule for CRL Download** (Правило системной политики для CRL- за грузки) (Certificate Revocation List, список аннулированных сертификатов) установите флажок **Enable** (Разрешить). Щелкните мышью кнопку ОК.
5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
7. Откройте Internet Explorer на брандмауэре ISA и введите URL-адрес http://<certificateserver>/certsrv, где **certificateserver** — имя или IP-адрес ЦС предприятия в корпоративной сети.
8. В диалоговом окне **Connect to** (Соединить с) введите верительные данные учет ной записи **isafirewall** и щелкните мышью кнопку ОК.
9. Щелкните мышью кнопку **Add** (Добавить) в диалоговом окне обозревателя Inter net Explorer для блокировки сайта.
10. Щелкните мышью кнопку **Add** (Добавить) в диалоговом окне **Trusted site** (До веренный сайт), а затем кнопку **Close** (Закрыть).
11. На странице **Welcome** (Добро пожаловать) щелкните кнопкой мыши ссылку **Request a certificate** (Запросить сертификат).
12. На странице **Request a certificate** (Запросить сертификат) щелкните кнопкой мыши ссылку **User Certificate** (Сертификат пользователя).
13. На странице **User Certificate — Identifying Information** (Сертификат пользователя — идентифицирующая информация) щелкните мышью кнопку **Submit** (Предоставить).
14. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).

15. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне, информирующем вас об отправке данных на Web-сервер.
16. На странице **Install this certificate** (Установить данный сертификат) щелкните кнопкой мыши ссылку **Install this certificate** (Установить данный сертификат).
17. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).
18. Щелкните кнопкой мыши пункт меню **Tools** (Сервис) и выберите команду **Internet Options** (Свойства обозревателя).
19. В диалоговом окне **Internet Options** (Свойства обозревателя) щелкните кнопкой мыши вкладку **Content** (Содержание).
20. На вкладке **Content** (Содержание) щелкните мышью кнопку **Certificates** (Сертификаты).
21. В диалоговом окне **Certificates** (Сертификаты) щелкните кнопкой мыши имя isafirewall и затем кнопку **Export** (Экспортировать).
22. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Export Wizard** (Вас приветствует мастер экспорта сертификатов).
23. На странице **Export Private Key** (Экспорт секретного ключа) выберите **Yes, export the private key** (Да, экспортировать секретный ключ) и щелкните мышью кнопку **Next** (Далее).
24. На странице **Export File Format** (Экспортировать формат файла) сбросьте флажок **Enable strong protection** (Разрешить строгую защиту) и установите флажок **Include all certificates in the certification path if possible** (Включите все сертификаты в путь сертификации, если возможно). Щелкните мышью кнопку **Next** (Далее).
25. На странице **Password** (Пароль) введите пароль и подтвердите пароль для файла сертификата. Щелкните мышью кнопку **Next** (Далее).
26. На странице **File to Export** (Файл для экспорта) введите путь в текстовое поле **File name** (Имя файла). В данном примере мы введем имя файла **c:\isafirewall-cert.** Щелкните мышью кнопку **Next** (Далее).
27. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certificate Export Wizard** (Завершение Мастера экспорта сертификатов).
28. **Щелкните** мышью кнопку ОК в диалоговом окне **Certificate Export Wizard** (Мастер экспорта сертификатов).
29. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **Certificates** (Сертификаты).
30. Щелкните мышью кнопку ОК в диалоговом окне **Internet Options** (Свойства обозревателя).

Теперь мы импортируем сертификат в учетную запись сервиса Firewall. 1. Щелкните мышью кнопку **Start** (Пуск) и выберите команду **Run** (Выполнить). В диалоговом окне **Run** (Выполнить) введите в текстовое поле **Open** (Открыть) команду mmc и щелкните мышью кнопку ОК.

2. На консоли выберите пункт меню **File** (Файл) и щелкните кнопкой мыши ко манду **Add/Remove Snap-in** (Добавить/Удалить оснастку).
3. В диалоговом окне **Add/Remove Snap-in** щелкните мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Add Standalone Snap-in** (Добавить автономную оснастку) щелкните мышью строку **Certificates** (Сертификаты) в списке **Available Standa lone Snap-ins** (Доступные автономные оснастки) *и* щелкните мышью кнопку **Add** (Добавить).
5. На странице **Certificates** snap-in (Оснастка сертификатов) выберите параметр **Services account** (Учетная запись сервисов) и щелкните мышью кнопку **Next** (Далее).
6. На странице **Select Computer** (Выберите компьютер) выберите Local **computer (the computer this console is running on)** (Локальный компьютер, компью тер, на котором запущена эта консоль) щелкните мышью кнопку **Next** (Далее).
7. На странице **Select a service account to manage on the local computer** (Вы берите учетную запись сервиса для управления локальным компьютером) вы берите сервис **Microsoft Firewall** (Брандмауэр Microsoft) из списка **Service account** (Учетная запись сервиса) и щелкните мышью кнопку **Finish** (Готово).
8. В диалоговом окне **Add Standalone Snap-in** (Добавить автономную оснастку) щелкните мышью кнопку **Close** (Закрыть).
9. Щелкните мышью кнопку ОК в диалоговом окне **Add/Remove Snap-in** (Доба вить/Удалить оснастку).
10. На консоли раскройте окно узла **Certificates — Service** (Сертификаты — Сер висы) и щелкните правой кнопкой мыши строку **fwsrv\Personal.** Укажите на команду **All Tasks** (Все задачи) и щелкните кнопкой мыши команду **Import** (Импортировать).
11. На странице **Welcome to the Certificate Import Wizard** (Вас приветствует мастер импорта сертификатов) щелкните мышью кнопку **Next** (Далее).
12. На странице **File to Import** (Файл для импорта) щелкните мышью кнопку **Browse** (Просмотр) для поиска файла сертификата пользователя, который экспортирован из обозревателя. Щелкните мышью кнопку **Next** (Далее).
13. Введите пароль, который вы назначили сертификату в текстовом поле **Password** (Пароль). Не устанавливайте флажок **Mark this key as exportable** (Пометить данный ключ как экспортируемый). Возможно, придется удалить сертификат из Web-обозревателя брандмауэра ISA, чтобы его не украли индивидуумы, получив шие физический доступ к брандмауэру. Щелкните мышью кнопку **Next** (Далее).
14. На странице **Certificate Store** (Хранилище сертификатов) примените **установку** по умолчанию **Place all certificates in the following store** (Поместить все сертификаты в следующее хранилище) и щелкните мышью кнопку **Next** (Далее).
15 Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certifi cate Import Wizard** (Завершение мастера импорта сертификатов).
16. В диалоговом окне **Certificate Import Wizard** (Мастер импорта сертификатов) щелкните мышыо кнопку ОК.

Теперь сертификат связан с учетной записью сервиса Firewall. Возможно, возникнет необходимость блокировать правило системной политики, созданное нами ранее, чтобы нечаянно не воспользоваться обозревателем на брандмауэре ISA. Помните о том, что следует избегать применения обозревателя и любых других клиентских приложений на брандмауэре ISA.

Создание правила публикации Web-сервера по протоколу SSL

Когда сертификаты находятся в нужном месте, можно создать правило публикации Web-сервера, защищенного протоколом SSL. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). В раскрытом узле Firewall Policy щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач. На этой панели выберите **Publish a Secure Web Server** (Опубликовать защищенный Web-сервер).

На странице **Welcome to the SSL Web Publishing Rule Wizard** (Вас приветствует мастер публикации Web-сервера по протоколу SSL) введите название правила в текстовое поле **SSL Web publishing rule name** (Название правила публикации Web-сервера по протоколу SSL). В данном примере мы назовем правило **Secure Web Server** (Защищенный Web-сервер) и щелкнем мышью кнопку Next (далее).

Страница Publishing Mode

На странице **Publishing Mode** (Режим публикации) (рис. 8.30) есть два переключателя:

- SSL Bridging (SSL-сопряжение);
- SSL Tunneling (SSL-туннелирование).

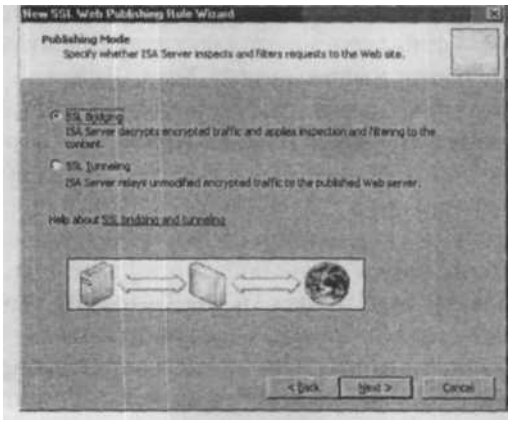


Рис. 8.30. Страница Publishing Mode (Режим публикации)

Вариант **SSL Bridging** (SSL-с оп ряжение) более безопасный. SSL-сопряжение обеспечивает защищенное от начала до конца (end-to-end) шифрованное соединение, в то же время разрешая брандмауэру ISA выполнять как отслеживающую состояние соединений фильтрацию (как любой традиционный «аппаратный» брандмауэр), так и отслеживающую состояние соединения проверку прикладного уровня. Это предпочтительный вариант, и именно его мы будем использовать в данном примере.

Вариант **SSL Tunneling** (SSL-туннелирование) менее безопасный. SSL-туннелирование минует функциональную возможность отслеживающей состояние соединений проверки прикладного уровня на брандмауэре ISA и снижает общий уровень безопасности правила публикации до уровня, обеспечиваемого традиционным «аппаратным» брандмауэром с отслеживающей состояние соединения фильтрацией. Не используйте вариант **SSL Tunneling** (SSL-туннелирование) до тех пор, пока не потребуется опубликовать приложения, не совместимые с Web-прокси HTTP 1.1.

Выберите **SSL Bridging** (SSL-сопряжение) и щелкните мышью кнопку **Next** (Далее).

Страница Select Rule Action

На странице **Select Rule Action** (Выбор действия правила), показанной на рис. 8.31, есть два переключателя: **Allow** (Разрешить) или **Deny** (Запретить). Вариант **Allow** разрешает соединения с опубликованным сервером, а Denyзапрещает соединения с опубликованным сервером. По умолчанию выбран вариант **Allow.** Вы можете применять запрещающие (Deny) правила публикации Web-сервера для точной настройки существующих правил публикации Web-серверов.

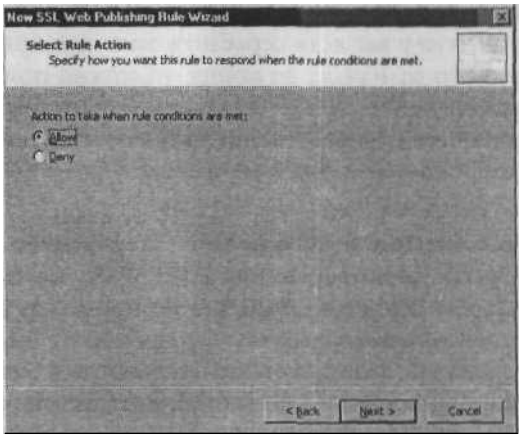


Рис. 8.31. Страница Select Rule Action (Выбор действия правила)

Выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).

Страница Bridging Mode

На странице **Bridging Mode** (Режим сопряжения) есть три переключателя (см. рис. 8.32):

м **Secure connection to clients** (Защищенное соединение с клиентами);
- **Secure connection to Web server** (Защищенное соединение с Web-сервером);
- **Secure connection to clients and Web server** (Защищенное соединение с кли ентами и Web-сервером).

Каждое «защищенное соединение» относится к соединению от брандмауэра ISA.

Вариант **Secure connection to clients** (Защищенное соединение с клиентами) устанавливает соединение как сопряжение SSL-c-HTTR Он защищает соединение Web-клиента с брандмауэром ISA, но разрешает передачу незащищенного открытого текста между брандмауэром ISA и опубликованным Web-сервером. Мы настоятельно рекомендуем отказаться от этой практики, если вы не применяете дополнительный метод защиты соединения между брандмауэром ISA и опубликованным Web-сервером (такой как IPSec безопасность IP) или выделенный канал связи (dedicated link) между брандмауэром ISA и опубликованным Web-сервером, в котором сам кабель нуждался бы в повреждении типа «зуб вампира» («vampire tap»), предусматривающем разрезание кабеля и подсоединение каждого конца витой пары к приемному устройству, действующему как посредник («man in the middle»), или извлечение сигнала с помощью рефлектометра промежутка времени (Time Domain Reflectometer).

Мы понимаем, что на самом деле существует компромисс между безопасностью, производительностью и неявным контрактом, заключенным между вами и пользователями, предполагающими, что их соединение защищено на всем протяжении. Если вы уверены в том, что у вас есть серьезная законная причина отказаться от соединения, защищенного от начала до конца, то можно применить с помощью брандмауэра ISA сопряжение SSL-c-HTTP. В зависимости от публикуемого Web-приложения может понадобиться использование транслятора ссылок (Link Translator) брандмауэра ISA для корректной работы. Мы расскажем больше о трансляторе ссылок в главе 10.

Вариант **Secure connection to Web server** (Защищенное соединение с Web-сервером) позволит выполнить сопряжение HTTP-c-SSL. Соединение между Web-клиентом и брандмауэром ISA устанавливается по протоколу HTTP, а соединение между брандмауэром ISA и Web-сервером — по протоколу SSL Это до некоторой степени необычный сценарий, в котором клиент находится в более доверяемой сети, чем сети на пути между брандмауэром ISA и опубликованным сервером. Примером такого сценария может служить филиал офиса, имеющий брандмауэр ISA, соединяющий этот филиал с центральным офисом по выделенному каналу WAN (Wide-Area Network, глобальная сеть). Можно опубликовать Web-сервер центрального офиса на брандмауэре ISA филиала и защитить соединение через канал WAN с центральным офисом и в конечном счете с Web-сервером как адресатом.

Вариант **Secure connection to clients and Web server** (Защищенное соединение с клиентами и Web-сервером) наиболее защищенный и предпочтительный (рис. 8.32). Он разрешает сопряжение SSL-с-SSL, в котором и соединение Web-клиента с брандмауэром ISA, и соединение между брандмауэром ISA и опубликованным Web-сервером защищаются протоколом SSL. Брандмауэр ISA способен выполнить отслеживающую состояние соединений проверку на прикладном уровне содержимого SSL-соединения при использовании SSL-сопряжения и в то же время обеспечить зашифрованное соединение на всем протяжении.

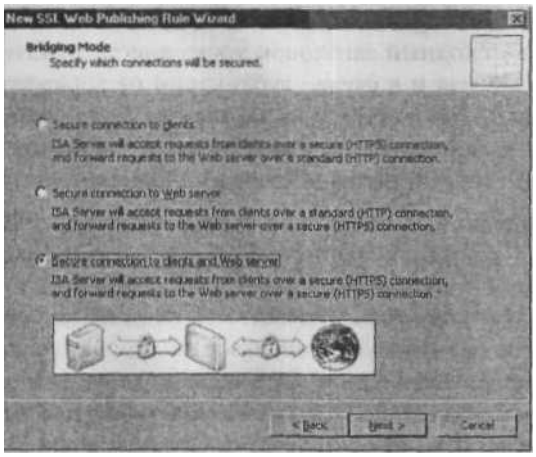


Рис. 8.32. Страница Bridging Mode (Режим сопряжения)

В данном примере мы выберем **Secure connection to clients and Web server** (Защищенное соединение с клиентами и Web-сервером) и щелкнем мышью кнопку **Next** (Далее).

Страница Define Website to Publish

На странице **Define Website to Publish** (Определение Web-сайта для публикации) есть следующие параметры:

- Computer name or IP address (Имя компьютера или IP-адрес);
- Forward the original host header instead of the actual one (specified above) (Пере сылать исходный заголовок хоста вместо фактического, заданного выше);
- Path (Путь);
- Site (Сайт).

Текстовое поле **Computer name or IP address** (Имя компьютера или IP-адрес) включает имя компьютера или IP-адрес публикуемого Web-сервера. Это важный параметр для SSL-публикации, потому что имя в этом поле *должно соответствовать общему имени в сертификате Web-сайта, хранящемся на Web-сервере.* Если

имя, введенное в текстовое поле **Computer name or IP address** (Имя компьютера или IP-адрес), не соответствует общему имени в сертификате Web-сайта, попытка соединения будет неудачной и пользователь увидит ошибку **500 Internal Server.**

Например, если общее имя в сертификате Web-сайта, связанном с опубликованным Web-сайтом, — **owa.msfirewall.org,** *необходимо* ввести **owa.msfirewall.org** в текстовое поле **Computer name or IP address** (Имя компьютера или IP-адрес). Если ввести IP-адрес или NetBIOS-имя сервера, попытка соединения закончится неудачей, потому что это имя не совпадает с общим именем из сертификата Web-сайта.

Вариант **Forward the original host header instead of the actual one** (sped tied **above)** (Пересылать исходный заголовок хоста вместо фактического, заданного выше) работает так же, как и в случае публикации не SSL-сайтов. Но необходимо быть внимательными с этим параметром, потому что если удаленный пользователь использует полностью определенное имя домена, отличающееся от общего имени из сертификата Web-сайта, попытка соединения потерпит неудачу.

Например, если удаленный пользователь введет URL-адрес **ht *tp://* www. ms fire - wall.org** для доступа к опубликованному Web-сайту через брандмауэр ISA, брандмауэр будет использовать www.msfirewall.org вместо owa.msfirewall.org при замещении соединения с опубликованным Web-сайтом и соединение завершится с ошибкой 500. По этой причине мы советуем использовать одно и то же имя от начала до конца в ваших правилах публикации Web-серверов. Однако это не обязательно, поскольку, если не установлен флажок **Forward the original host header instead of the actual one (specified above)** (Пересылать исходный заголовок хоста вместо фактического, заданного выше) и используется одно и то же имя от начала до конца, имя, используемое удаленным пользователем для доступа к Web-сайту, будет тем же, что и общее имя в сертификате Web-сайта.

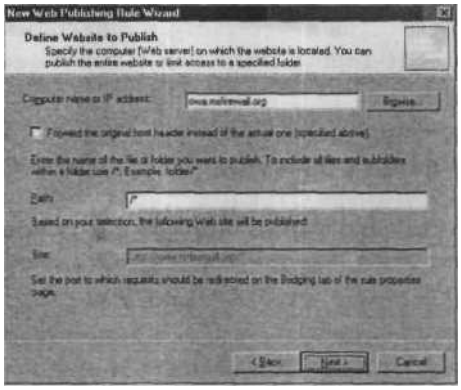
Ключ к успеху — совпадение имени в текстовом поле **Computer name or IP address** (Имя компьютера или IP-адрес) с общим именем *в* сертификате Web-сайта на опубликованном Web-сайте и разрешение брандмауэром ISA имени из текстового поля **Computer name or IP address** (Имя компьютера или IP-адрес) во *внутренний* адрес, а *не* в общедоступный адрес, используемый Web-приемником для этого сайта. В данном примере имя owa.msfirewall.org должно разрешаться во *внутренний,* а не в общедоступный адрес. Другими словами, в действительный адрес, связанный с Web-сайтом в корпоративных сетях.

Текстовое поле **Path** (Путь) применяется так же, как и в случае соединения по протоколу, отличному от SSL Вернитесь к разделу этой главы, описывающему публикацию незащищенных Web-сайтов, для получения подробной информации об этом параметре.

В текстовом поле **Site** (Сайт) приводится URL-адрес сайта, который будет публиковаться во внутренней сети.

Рис. 8.33. Страница Define Website to Publish (Определение Web-сайта для публикации)

Ш рис. 8.33 показана страница **Define Website to Publish** (Определение Web-сайта для публикации) мастера создания правила.



Щелкните мышью кнопку **Next** (Далее) на странице **Define Website to Publish** (Определение Web-сайта для публикации).

Страница Public Name Details

На странице **Public Name Details** (Параметры общедоступного имени) (рис. 8.34) определяется, какие имена могут применять пользователи для доступа к опубликованному Web-сайту с помощью этого правила публикации Web-сервера. Эта страница включает следующие параметры:

- Accept requests for (Принимать запросы к);
- Public name (Общедоступное имя);
- Path (Путь);
- Site (Сайт).

Раскрывающийся список **Accept requests for** (Принимать запросы к) позволяет выбрать либо **This domain name (type below)** (Данное имя домена, набранное ниже), либо **Any domain name** (Любое имя домена). Как мы уже упоминали ранее при обсуждении публикации по протоколу, отличному от SSL, вариант **Any domain name** (Любое имя домена) обеспечивает низкий уровень защиты и его следует избегать, если это возможно. Он позволяет правилу публикации Web-сервера принимать входящие запросы, использующие любой IP-адрес или любое полностью определенное имя домена (FQDN), которые могут достичь IP-адреса, применяемого Web-приемником для правила публикации Web-сервера. Более предпочтителен вариант **This domain name (type below)** (Данное имя домена, набранное ниже). Он ограничивает имена, которые могут использовать удаленные пользователи для доступа к Web-сайту, опубликованному данным правилом публикации Web-сервера.

Можно ввести имя, которое сможет применять удаленный пользователь для доступа к опубликованному Web-сайту, в текстовое поле Public name (Общедоступное имя). Это важный параметр. Необходимо ввести имя, применяемое удаленным пользователем для доступа к Web-сайту, и оно *должно совпадать с общим именем в сертификате Web-сайта, связанного с Web-приемником,* используемым данным правилом.

Мы рекомендуем экспортировать сертификат Web-сайта, связанный с опубликованным Web-сайтом, и импортировать этот сертификат в компьютерное хранилище сертификатов на брандмауэре ISA. После этого можно связать исходный сертификат Web-сайта с Web-приемником, используемым данным правилом публикации Web-сервера. Затем необходимо применять одно и то же имя от начала и до конца соединения.

Например, если в сертификате Web-сайта, используемом на опубликованном Web-сайте, указано общее имя owa.msfirewall.org и экспортируется этот сертификат Web-сайта и связывается с Web-приемником, применяемым правилом публикации Web-сервера, то необходимо использовать то же имя owa.msflrewall.org в текстовом поле Public name (Общедоступное имя). Удаленные пользователи должны быть способны преобразовать это имя в адрес на брандмауэре ISA, на который Web-приемник, используемый этим правилом, принимает входящие защищенные соединения.

Текстовое поле Path (Путь) позволяет указать, какие пути доступны на опубликованном Web-сайте. Более подробные сведения о том, как применять параметр Path (Путь) можно найти в обсуждении этого параметра в разделе этой главы, посвященном правилу публикации Web-сер вер а по протоколу, отличному от SSL

Пример страницы Public Name Details (Параметры общедоступного имени) показан на рис. 8.34.

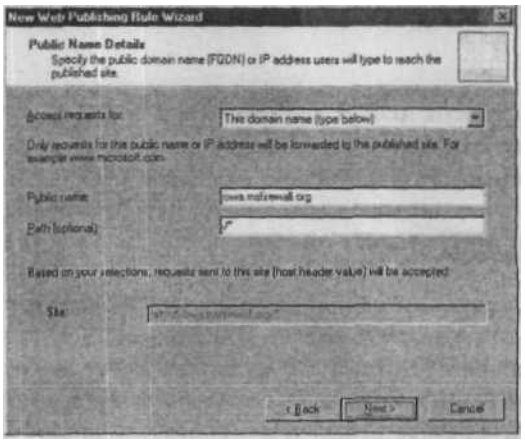


Рис. 8.34. Страница Public Name Details (Параметры общедоступного имени)

Щелкните мышью кнопку **Next** (Далее) на странице **Public Name Details** (Параметры общедоступного имени).

Страница Select Web Listener

На странице **Select Web Listener** (Выбор Web-приемника) (рис. 8.35) можно выбрать Web-приемник, который желательно использовать для данного правила публикации Web-сервера. Если Web-приемник SSL-соединений на этом брандмауэре ISA уже создан, можно выбрать его из списка **Web listener** (Web-приемник). Если Web-приемник SSL-соединений отсутствует, то его можно создать, щелкнув мышью кнопку **New** (Новый).

В данном примере мы создадим новый Web-приемник SSL-соединений для данного правила публикации Web-сервера. Щелкните мышью кнопку **New** (Новый).

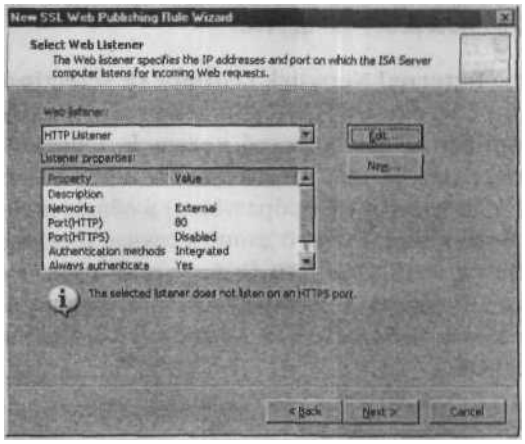


Рис. 8.35. Страница Select Web Listener (Выбор Web-приемника)

На странице **Welcome to the New Web Listener Wizard** (Вас приветствует мастер создания нового Web-приемника) введите имя нового приемника в текстовое поле **Web listener name** (Имя Web-приемника). В данном примере мы назовем его SSL Listener. Щелкните мышью кнопку **Next** (Далее).

На странице **IP Addresses** (IP-адреса) выберите сеть, которую нужно прослушивать с помощью приемника. В нашем примере мы хотим, чтобы приемник ожидал входящие запросы к Web-сайту, опубликованному в интерфейсе **External** (Внешний). Установите флажок, расположенный рядом с сетью, в которой приемник будет ожидать запросы. Но мы не хотим, чтобы Web-приемник ожидал запросы ко всем IP-адресам, присвоенным внешнему интерфейсу (интерфейсам), поэтому мы щелкнем мышью кнопку **Addresses** (Адреса) (см. рис. 8.36).

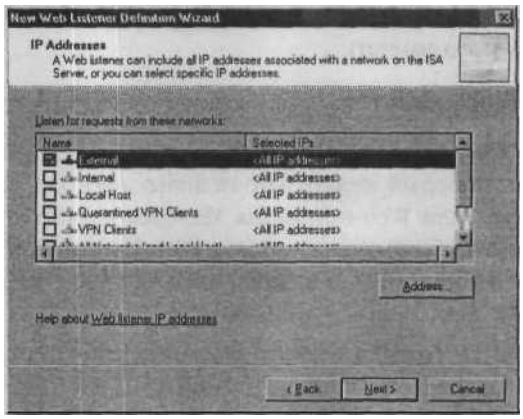


Рис. 8.36. Страница **IP Addresses** (IP-адреса)

В диалоговом окне **External Network Listener IP Selection** (Выбор IP для приемника внешней сети) (см. рис. 8.37) выберите вариант **Specified IP addresses on the ISA Server computer in the selected network** (Определенные IP-адреса на компьютере с ISA Server, находящиеся в выбранной сети). Укажите адрес на брандмауэре ISA, который разрешается (преобразуется) в общее имя в сертификате Web-сайта, связанного с Web-приемником. В данном случае IP-адрес, разрешающийся в имя **owa.msfirewall.org, — 192.168.1.70.** Выберите IP-адрес в списке **Available IP Addresses** (Доступные IP-адреса) и щелкните мышью кнопку **Add** (Добавить), чтобы переместить его в список **Selected IP Addresses** (Выбранные IP-адреса). Щелкните мышью кнопку OK.

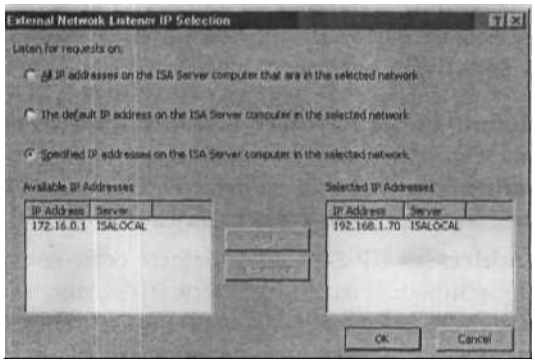


Рис. 8.37. Страница **External Network Listener IP Selection** (Выбор IP для приемника внешней сети)

Щелкните мышью кнопку **Next** (Далее) на странице **The IP Address Selection** (Выбор IP-адреса).

На странице **Port Specification** (Спецификация порта) задайте TCP-порт (порты), с которого Web-приемник будет принимать запросы. Мы советуем всегда создавать отдельные приемники для протоколов HTTP и SSL, потому что такой подход обеспечивает большую гибкость при создании приемников и формировании правил публикации Web-серверов. Поскольку в данном примере мы создаем SSL-tipi емник, сбросьте флажок **Enable HTTP** (Разрешить HTTP), чтобы помешать этому Web-приемнику принимать входящие запросы http-соединений. Установите флажок **Enable** SSL (Разрешить SSL). По умолчанию номер прослушивающего порта для SSL-приемника — 443. Можно изменить этот номер на любой другой, но это заставит пользователей вручную вводить альтернативный порт.

SSL-приемнику **нужен** связанный с ним сертификат Web-сайта, для того чтобы он мог выдать себя за опубликованный Web-сайт. Щелкните мышью кнопку **Select** (Выбрать) для выбора сертификата (рис. 8.38).

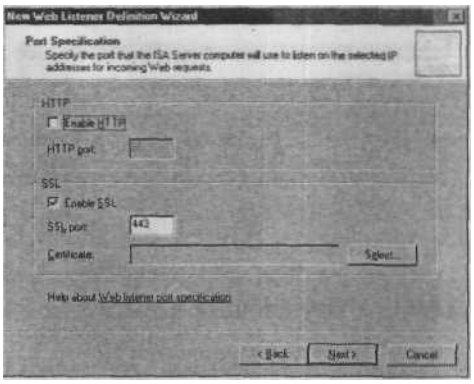


Рис. 8.38. Страница Port Specification (Спецификация порта)

Будет представлен список сертификатов Web-сайтов в диалоговом окне **Select Certificate** (Выберите сертификат). В этом примере мы видим два сертификата: сертификат компьютера, присвоенный брандмауэру ISA и применяемый им для аутентификации пользователей с помощью сертификата на Web-сайтах, требующих сертификаты пользователей, и сертификат для Web-сайта, который мы публикуем. Выберите сертификат Web-сайта (в данном примере сертификат Web-сайта — **owa.msfirewall.org)** и щелкните мышью кнопку ОК. Диалоговое окно выбора сертификата показано на рис. 8.39.

ПРЕДУПРЕЖДЕНИЕ Если в списке Select Certificate (Выберите сертификат) нет вашего сертификата, вероятнее всего, вы не включили секретный ключ при экспорте сертификата Web-сайта. И вторая причина отсутствия вашего сертификата сайта в данном списке — вы импортировали этот сертификат в другое хранилище сертификатов. Сертификат должен быть импортирован в хранилище сертификатов машин, а не в хранилище сертификатов пользователей или сервисов.

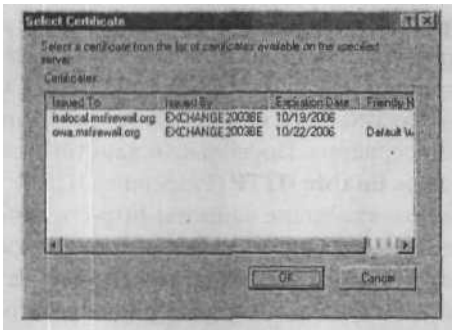


Рис. 8.39. Диалоговое окно Select Certificate (Выберите сертификат)

Сертификат появляется в области **Certificate** (Сертификат) на странице **Port Specification** (Спецификация порта), показанной на рис. 8.40. Щелкните мышью кнопку **Next** (Далее).

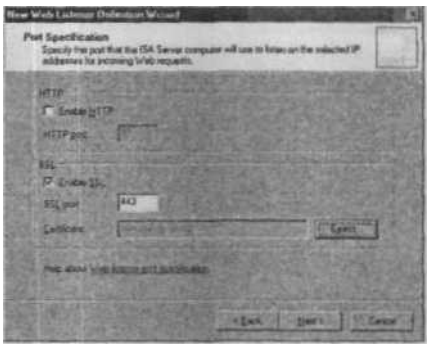


Рис. 8.40. Появление сертификата на странице Port Specification (Спецификация порта)

Щелкните мышью кнопку **Finish** (Готово) на странице Completing **the** New **Web** Listener Wizard (Завершение мастера создания нового Web-приемника). Подробное описание SSL-приемника теперь появится на странице **Select Web Listener** (Выберите Web-приемник) (рис. 8.41). Щелкните мышью кнопку **Next** (Далее).

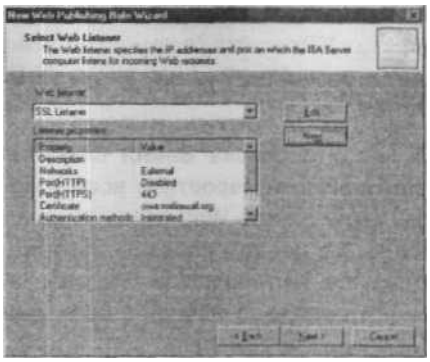


Рис. 8.41. Страница Select Web Listener (Выберите Web-приемник)

Страница User Sets

На странице **User Sets** (Наборы пользователей) выберите пользователей, которым вы хотите предоставить доступ к Web-сайту. Параметры настройки на этой странице одинаковы для публикации по SSL-протоколу и любому другому протоколу. Вернитесь к обсуждению страницы **User Sets** (Наборы пользователей) в разделе этой главы, посвященном публикации Web-сервера по протоколу, отличному от SSL

Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Web Publishing Rule Wizard** (Завершение мастера создания нового правила публикации Web-сервера). Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Диалоговое окно Properties правила публикации Web-сервера по протоколу SSL

Диалоговое окно **Properties** (Свойства) правила публикации Web-сервера по протоколу SSL идентично одноименному окну правила публикации Web-сервера по протоколу, отличному от SSL. Просмотрите еще раз раздел этой главы, посвященный описанию диалогового окна **Properties** правила публикации Web-сервера по протоколу, отличному от SSL.

Создание правил публикации сервера

Создание правил публикации сервера проще по сравнению с формированием правил публикации Web-сервера. Необходимо знать всего лишь следующее:

- протокол или протоколы, которые нужно публиковать;
- IP-адрес, на который брандмауэр ISA принимает входящие соединения;
- IP-адрес сервера из защищенной сети, который нужно опубликовать.

Правило публикации сервера использует протоколы для первичного соединения, установленные как **Inbound** (Входящий), **Receive** (Получить) или Receive/Send (Получить/Отправить). Например, если вы хотите опубликовать SMTP-сервер, должно быть определение протокола для протокола SMTP, TCP-порт 25, входящий. Определения для исходящего протокола применяются в правилах доступа.

Брандмауэр ISA поставляется с набором встроенных в правила публикации определений протоколов. В табл. 8.2 перечислены эти встроенные определения протоколов.

Табл. 8.2. Определения протоколов правил публикации серверов

Определение протокола	Применение
DNS Server	TCP 53 Inbound UDP 53 Receive/Send DNS Security Filter включен Domain Name System Protocol — Server (Протокол системы доменных имен — Сервер). Входящий протокол, используемый для публикации сервера. Это определение протокола также разрешает передачу DNS-зоны (DNS zone transfer)
Exchange RPC Server	TCP 135 Inbound RPC Security Filter включен Представлены только интерфейсы удаленного вызова процедуры сервера Exchange (Exchange RPC UUIDs) Применяется для публикации сервера Exchange для RPC-доступа из внешней сети
FTP Server	TCP 21 Inbound FTP Access Filter включен File Transfer Protocol — Server (Протокол передачи файлов — сервер). Входящий протокол, применяемый для публикации сервера. Поддерживаются режимы PASV и PORT
HTTPS Server	TCP 443 Inbound Secure HyperText Transfer Protocol — Server (Протокол передачи гипертекста — сервер). Входящий протокол, применяемый для публикации сервера. Используется для **публикации** SSL-сайтов, когда правила публикации Web-серверов и улучшенная защита не требуется
IKE Server	UDP 500 Receive/Send Internet Key Exchange Protocol - Server. Входящий протокол, применяемый для публикации сервера. Используется для транзитной пересылки IPSec
IMAP4 Server	TCP 143 Inbound Protocol (ШАР) — Server (Входящий протокол (ШАР) — сервер) Входящий протокол, применяемый для публикации сервера
IMAPS Server	TCP 993 Inbound Secure Interactive Mail Access Protocol (IMAP) — Server (Защищенный интерактивный протокол доступа почты — сервер). Входящий протокол, применяемый для публикации сервера
IPSec ESP Server	IP Protocol 50 Receive/Send IPSec ESP Protocol — Server. Входящий протокол, применяемый для публикации сервера. Используется для транзитной пересылки IPSec UDP 4500 Receive/Send
IPSec NAT-T Server	IPSec NAT-T Protocol — Server. Используется для NAT-обхода (NAT Traversal) по протоколу L2TP/IPSec **и** других RFC (Requests for Comments)-совместимых соединений с NAT-обходом для протокола IPSec

Табл. 8.2. (продолжение)

Определение протокола	Применение
L2TP **Server**	UDP 1701 Receive/Send Layer 2 Tunneling Protocol - Server (Протокол туннелирования уровня 2 — сервер). Входящий протокол, применяемый для публикации сервера. Используется для публикации управляющего канала L2TP/IPSec
Microsoft SQL Server	TCP **1433** Inbound Microsoft SQL Server **Protocol**
MMS Server	TCP 1755 Inbound UDP 1755 Receive MMS Filter включен Microsoft Media Server Protocol — Server **(Протокол** потоковых мультимедийных данных Microsoft — сервер). Входящий протокол, применяемый для публикации сервера
NNTP Server	TCP 119 Inbound Network News Transfer Protocol — Server (Сетевой протокол передачи новостей — сервер). Входящий протокол, применяемый для публикации сервера
NNTPS Server	TCP 563 Inbound Secure Network News Transfer Protocol — Server (Защищенный сетевой протокол передачи новостей — сервер). Входящий протокол, применяемый для публикации сервера TCP 7070
PNM Server	Inbound PNM Filter включен Progressive Networks Streaming Media Protocol — Server. Входящий протокол, применяемый для публикации сервера
POP3 Server	TCP ПО Inbound Post Office Protocol v.3 — Server (Почтовый протокол v.3 — сервер). Входящий протокол, применяемый для публикации сервера
POP3S Server	TCP 995 Inbound Secure Post *Office* Protocol v.3 — Server (Защищенный почтовый протокол v.3 — сервер). Входящий протокол, применяемый для публикации сервера TCP 1723 Inbound PPTP Filter включен
PPTP Server	Point-to-Point Tunneling Protocol — Server (Сквозной туннельный протокол — сервер). Входящий протокол, применяемый для публикации сервера
RDP (Terminal Services) Server	TCP 3389 Inbound Remote Desktop Protocol (Terminal Services) — Server (Протокол удаленного рабочего стала (Службы терминалов) — сервер)

(см. след. стр.)

Табл. 8.2. (окончание)

Определение протокола	Применение
RPC Server (all interfaces)	TCP 135 Inbound RPC Filter включен Remote Procedure Call Protocol — Server (Протокол удаленного вызова процедуры — сервер). Входящий протокол, применяемый для публикации сервера (все RPC-интерфейсы). Прежде всего, используется для внутридоменных соединений через брандмауэр ISA
RTSP Server	TCP 554 Inbound Real Time Streaming Protocol — Server. Входящий протокол, применяемый для публикации сервера. Используется сервисами Windows Media Server ОС Windows Server 2003
SMTP Server	TCP 25 Inbound SMTP Security Filter включен Simple Mail Transfer Protocol — Server (Простой протокол электронной почты — сервер). Входящий протокол, применяемый для публикации сервера
SMTPS Server	TCP 465 Inbound Secure Simple Mail Transfer Protocol — Server (Защищенный простой протокол электронной почты — сервер). Входящий протокол, применяемый для публикации сервера
Telnet Server	TCP 23 Inbound Telnet Protocol — Server. Входящий протокол, применяемый для публикации сервера

Любой из протоколов, приведенных в табл. 8.2, готов для применения в правиле публикации сервера.

В следующем примере мы создадим правило публикации сервера для RDP-сайта (Remote Desktop Protocol, протокол соединения с удаленным рабочим столом) во внутренней сети. RDP-сайт может быть терминальным сервером (Terminal Server) или компьютером под управлением Windows XP, на котором запущен Remote Desktop (Удаленный рабочий стол).

1, На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall policy** (Политика брандмауэра). Щелкните кнопкой мыши вкладку **Tasks** (За дачи) на панели **Tasks** (Задачи), а затем ссылку **Create a New Server Publishing Rule** (Создать новое правило публикации сервера).

2. На странице **Welcome to the New Server Publishing Rule Wizard** (Вас при ветствует мастер создания нового правила публикации) введите название пра вила в текстовое поле **Server Publishing Rule name** (Название правила публи кации сервера). В нашем примере мы назовем правило **SPR — Terminal Server.** Щелкните мышью кнопку **Next** (Далее).

3. На странице **Select Server** (Выберите сервер) введите IP-адрес сервера, публи куемого в сети, защищенной брандмауэром ISA, в текстовое поле **Server IP add ress** (IP-адрес сервера). В данном примере мы введем 10.0.0.2. Вы также можете щелкнуть мышью кнопку **Browse** (Просмотр) для поиска сервера, но имейте в виду, что брандмауэр ISA должен быть способен разрешить имя сервера коррект но. Щелкните мышью кнопку **Next** (Далее).
4. На странице **Select Protocol** (Выберите протокол) (рис. 8.42) щелкните кноп кой мыши стрелку, направленную вниз, в списке **Selected protocol** (Выбран ный протокол) и щелкните мышью протокол **RDP (Terminal Services) Server.** Параметры выбранного протокола можно увидеть в диалоговом окне **Properties** (Свойства). Можно также изменить порты, используемые для приема входящих соединений, и порты, применяемые для передачи соединения с опубликован ным Web-сервером. Щелкните мышью кнопку **Ports** (Порты).

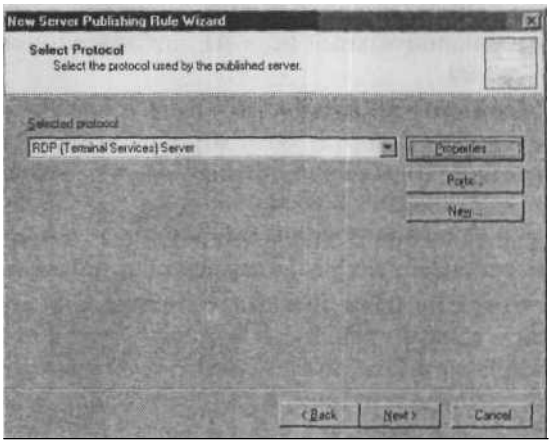


Рис. 8.42. Страница Select Protocol (Выберите протокол)

В диалоговом окне **Ports** (Порты) доступны следующие параметры.

- **Publish using the default port defined in the Protocol Definition** (Публиковать с применением порта по умолчанию, указанного в определении протокола). Этот параметр разрешает брандмауэру ISA ожидать запросы на порт по умолчанию, заданный в определении протокола для выбранного протокола. В данном примере определение протокола RDP ожидает запросы на TCP-порте 3389. Используя этот вариант, брандмауэр ISA ожидает запросы на TCP-порте 3389 к IP-адресу, который задан в приемнике для этого правила публикации сервера. Этот вариант выбран по умолчанию.
- **Publish on this port instead of the default port** (Публиковать на данном порте вместо порта по умолчанию). Можно изменить номер порта, применяемого для ожидания входящих запросов. Этот вариант позволяет переопределить номер порта в определении протокола. Например, можно задать

брандмауэру ISA ожидание RDP-соединения на TCP-порте 8989. Мы могли бы выбрать вариант **Publish on this port instead of the default port,** а затем ввести альтернативный порт **8989** в текстовое поле рядом с этим вариантом. D **Send requests to the default port on the published server** (Посылать запросы на порт **по умолчанию** на опубликованном сервере). Этот вариант конфигурирует брандмауэр ISA на пересылку соединения на тот же порт, на который брандмауэр ISA получил запрос. В этом примере правило публикации RDP-сервера принимает RDP-соединения наTCP-порт 3389. Далее соединение передается на порт 3389 на опубликованном сервере. Этот вариант выбран по умолчанию.

D Send requests to this port on the published server (Посылать запросы на данный порт на опубликованном сервере). Этот вариант позволяет выполнить переадресацию портов. Например, если брандмауэр ISA принимает входящие запросы RDP-соединений **на TCP-порт** 3389, можно перенаправить соединение на дополнительный порт на опубликованном RDP-сервере, такой как TCP-порт 89-

D Allow traffic from any allowed source port (Разрешить трафик с любого допустимого исходного порта). Этот вариант позволяет брандмауэру ISA принимать входящие соединения от клиентов, применяющих любой исходный порт в своих запросах к опубликованному серверу. Этот вариант выбран по умолчанию, и большинство приложений проектируется с возможностью принимать соединения с любого исходного порта клиента. □ **Limit access to traffic from this range of source ports** (Ограничить доступ трафиком с данного диапазона портов). Выбрав этот вариант, можно ограничить исходные порты, которые использует приложение, соединяющееся с опубликованным сервером. Если приложение разрешает настроить исходный порт, можно повысить безопасность вашего правила публикации сервера, ограничив соединения, поступающие с хостов, с помощью заданного исходного порта и вводя номер этого порта в текстовое поле, связанное с этим вариантом.

Внеся необходимые изменения, щелкните мышью кнопку ОК. В данном примере мы не будем менять приемник или передавать номер порта.

б. На странице IP **Addresses** (IP-адреса) вы можете выбрать сети, в которых по вашему мнению брандмауэр ISA должен ожидать входящие **соединения** с опубликованным Web-сайтом. Эта страница в правилах публикации серверов действует так же, как одноименная страница в правилах публикации Web-серверов. Более подробную информацию о том, как использовать параметры страницы IP **Addresses** (IP-адреса), вы найдете в разделе этой главы, посвященном этой странице в правилах публикации Web-сервера по протоколу, отличному от SSL В данном примере мы выберем внешнюю сеть, установив флажок **External** (Внешняя) и щелкнув мышью кнопку **Next** (Далее).

7. Щелкните мышью кнопку Finish (Готово) на странице Completing the New Server Publishing Rule Wizard (Завершение мастера создания нового правила публикации сервера).
8. Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.
9. Щелкните мышью кнопку OK в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

Диалоговое окно Properties правила публикации сервера

Можно точно настроить правило публикации сервера, открыв диалоговое окно Properties (Свойства) правил публикации сервера. Дважды щелкните кнопкой мыши правило публикации сервера, чтобы открыть это окно. Первой появится вкладка General (Общие). На ней можно изменить название правила публикации сервера и вставить описание правила, можно также разрешить или заблокировать правило, изменяя состояние флажка Enable (Разрешить). Вкладка General (Общие) показана на рис. 8.43.

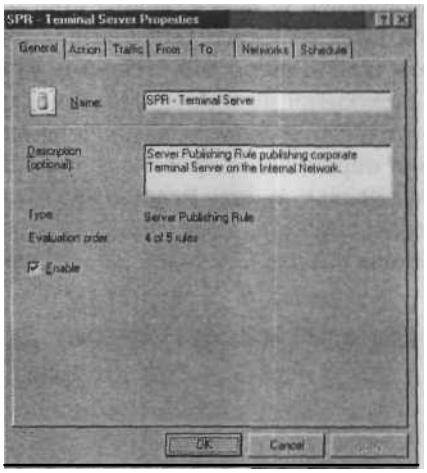


Рис. 8.43. Вкладка **General** (Общие)

На вкладке Action (Действие) (см. рис. 8.44) настройте правило на регистрацию или отказ от регистрации соединений, применяемых к этому правилу. Мы рекомендуем всегда регистрировать соединения, выполненные с помощью правила публикации сервера. Если же имеется причина для отказа от регистрации этих соединений (например, законы защиты конфиденциальности вашей страны не разрешают регистрировать данную информацию), можно заблокировать регистрацию, сбросив флажок Log requests matching this rule (Регистрация запросов, соответствующих данному правилу).

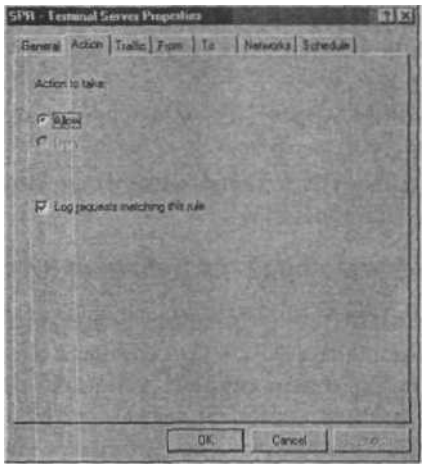


Рис. 8.44. Вкладка **Action** (Действие)

На вкладке **Traffic** (Трафик) вы можете изменить протокол, используемый в правиле публикации сервера, **щелкнув** стрелку, направленную вниз, в раскрывающемся списке **Allow network traffic using the following protocol** (Разрешить сетевой трафик, используя следующий протокол). Можно создать новое определение протокола для правила публикации сервера, щелкнув мышью кнопку **New** (Новое), и увидеть характеристики определения протокола, используемого в правиле публикации сервера, щелкнув мышью кнопку **Properties** (Свойства). Также можно настроить порты источника и адресата, разрешенные в правиле публикации сервера, с помощью кнопки **Ports** (Порты). Параметры вкладки Traffic (Трафик) показаны на рис. 8.45.

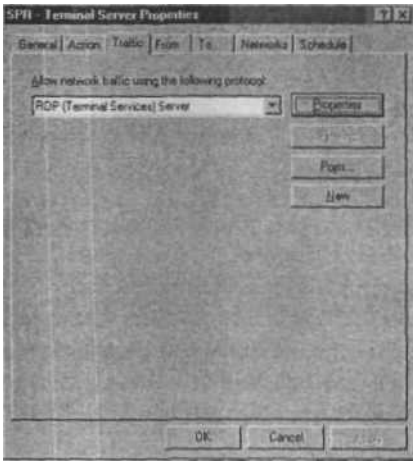


Рис. 8.45. Вкладка **Traffic** (Трафик)

Можно задать хосты, которые могут соединяться с опубликованным сервером, используя установочные параметры на вкладке From (От). По умолчанию хостам, расположенным Anywhere (Везде), разрешено соединяться с опубликованным сервером с помощью данного правила. Однако соединения могут быть разрешены только для хостов, способных соединяться через сети, заданные на вкладке Networks (Сети). Поэтому, несмотря на то, что хосты, размещенные Anywhere (Везде), могут соединяться с опубликованным сервером, возможные соединения ограничиваются теми хостами, которые могут установить соединение с интерфейсом (интерфейсами), ответственным за сети, перечисленные на вкладке Networks (Сети).

Имеется возможность более детального контроля над хостами, которым разрешен доступ к опубликованному серверу, если удален вариант Anywhere (Везде) и доступ к опубликованному серверу разрешен более ограниченной группе компьютеров. Щелкните кнопкой мыши строку Anywhere (Везде), а затем кнопку Remove (Удалить). Затем щелкните мышью кнопку Add (Добавить) и выберите сетевой объект, определяющий группу машин, которым необходимо предоставить доступ к опубликованному серверу.

Позже можно точно настроить управление доступом, задав исключения в дополнение к списку разрешенных хостов и добавив эти исключения в список Exceptions (Исключения). Щелкните мышью кнопку Add (Добавить) в области Exceptions (Исключения). Параметры вкладки From (От) показаны на рис. 8.46.

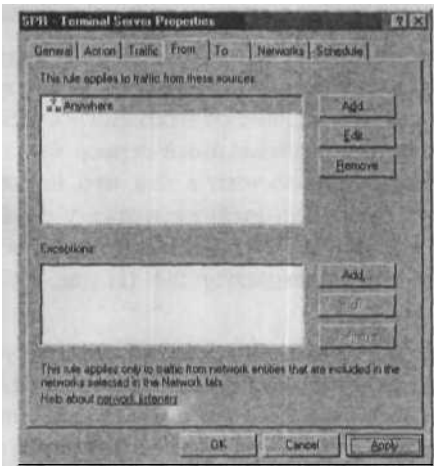


Рис. 8.46. Вкладка From (От)

На вкладке To (Кому) настройте IP-адрес сервера, опубликованного с помощью правила публикации сервера. Вы также можете указать, какой IP-адрес клиента будет виден опубликованному серверу, задав один из вариантов из области Request for the published server (Запрос к опубликованному серверу). На вкладке приведены два варианта.

- Requests appear to come from the ISA Server computer (Запросы отображаются как пришедшие с компьютера брандмауэра ISA Server).
- Requests appear to come from the original client (Запросы отображаются как при шедшие от исходного клиента).

Вариант **Requests appear to come from the ISA Server computer** (Запросы отображаются как пришедшие с компьютера брандмауэра ISA Server) позволяет опубликованному серверу видеть IP-адрес источника входящего соединения как IP-адрес сетевого интерфейса брандмауэра ISA, находящегося в той же сети, что и опубликованный сервер. Например, если опубликованный сервер находится во внутренней сети и IP-адрес интерфейса брандмауэра ISA во внутренней сети **10.0.0.1,** опубликованный сервер получит IP-адрес входящего соединения **10.0.0.1.**

Этот вариант полезен, если нежелательно делать опубликованный сервер клиентом SecureNAT. Клиент SecureNAT — это компьютер, который настроен на применение адреса шлюза по умолчанию и направляет маршруты всех соединений, связанных с Интернетом, через брандмауэр ISA. Если нет нужды менять адрес шлюза по умолчанию на опубликованном сервере, используйте вариант **Requests appear to come from the ISA Server computer** (Запросы отображаются как пришедшие с компьютера брандмауэра ISA Server). Единственное требование — если опубликованный сервер и брандмауэр ISA находятся в разных подсетях, опубликованный сервер должен уметь прокладывать маршрут через IP-адрес, который брандмауэр ISA использует для передачи соединения на опубликованный сервер.

Если нужно, чтобы на опубликованном сервере был виден действительный IP-адрес клиента, выберите вариант **Requests appear to come from the original client** (Запросы отображаются как пришедшие от исходного клиента). В этом случае необходимо сконфигурировать опубликованный сервер как клиент SecureNAT. Причина выбора такой конфигурации состоит в том, что, поскольку IP-адрес клиента находится в нелокальной сети (non-local network), у опубликованного сервера должен быть шлюз по умолчанию, который направляет маршруты соединений, связанных с Интернетом, через брандмауэр ISA. На рис. 8.47 показаны параметры вкладки To (Кому).

На вкладке **Networks** (Сети) (см. рис. 8.48) вы можете указать, из каких сетей может брандмауэр ISA ожидать и принимать входящие соединения с опубликованным сервером. В данном примере мы настраиваем правило публикации сервера для приема входящих соединений от хостов во внешней сети (внешняя сеть (External Network) по умолчанию включает все адреса, не определенные в любой другой сети, на брандмауэре ISA).

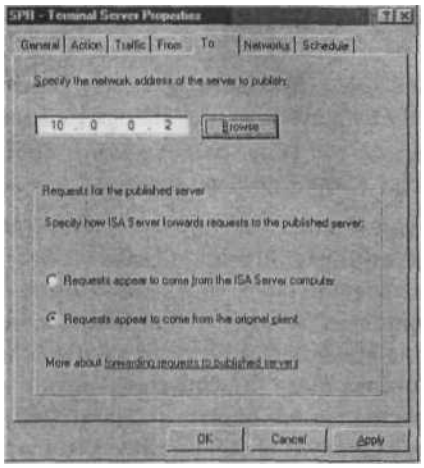


Рис. 8.47. Вкладка **To** (Кому)

Можно настроить брандмауэр ISA на ожидание запросов из любой сети. Например, можно сконфигурировать правило публикации сервера для ожидания соединений от клиентов сети VPN (Virtual Private Network, виртуальная частная сеть). Затем клиенты VPN могут соединяться с опубликованным сервером, используя данное правило публикации сервера.

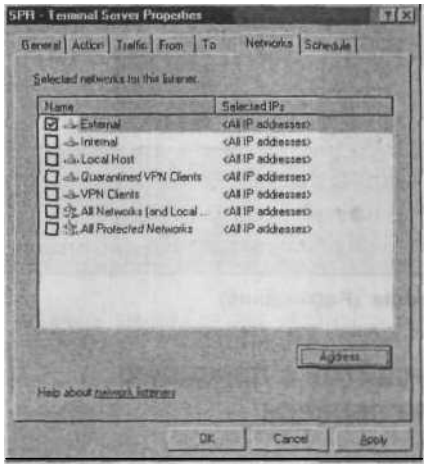


Рис. 8.48. Вкладка **Networks** (Сети)

На вкладке **Schedule** (Расписание) (см. рис. 8.49) можно определить периоды времени, в которые устанавливаются соединения с опубликованным сервером. Есть три стандартных расписания:

- **Always** (Всегда) Пользователи могут всегда соединяться с опубликованным сервером;
- **Weekends** (Выходные дни) Пользователи могут соединяться с опубликованным сервером с 12:00 дня в субботу до 12:00 дня в воскресенье;
- **Work hours** (Рабочие часы) Пользователи могут соединяться с опубликованным сервером с 9:00 до 17:00 с понедельника по пятницу.

Можно создать собственное расписание, пользуясь кнопкой New (Новое). Мы расскажем больше о создании расписаний в главе 10. Имейте в виду, что расписания управляют временем соединения с опубликованным сервером, но не удаляют уже установленные соединения. Потому что пользователи соединились с опубликованным сервером, когда соединения были разрешены, и у них может быть продолжающаяся работа, которая была бы нарушена, если бы соединение было произвольно прекращено расписанием. Можно создать сценарий прерывания соединений, остановив сервис Microsoft Firewall и запустив его повторно после разрыва всех соединений.

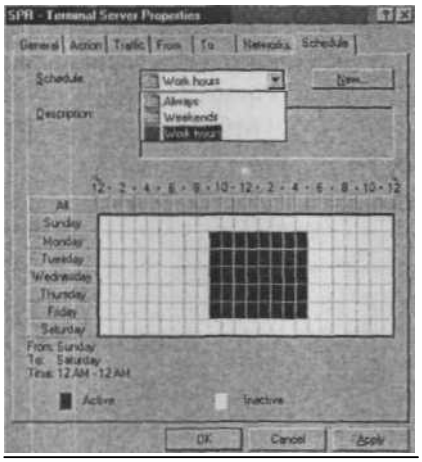


Рис. 8.49. Вкладка Schedule (Расписание)

Публикация HTTP-сайтов с помощью правил публикации сервера

Просматривая список определений протоколов, используемых в правилах публикации серверов, можно заметить, что в нем нет определения протокола для HTTP-сервера. Есть определение протокола для HTTPS-серверов (HyperText Transmission Protocol, Secure, протокол защищенной передачи гипертекстов), но не для HTTP-серверов. Если требуется создать правило публикации для HTTP-сервера, нужно создать собственное определение протокола HTTP-сервера.

Мы рекомендовали всегда использовать правила публикации Web-сервера для публикации Web-сайтов, но бывают ситуации, когда нужно опубликовать Web-сайт, не согласующийся с серверами Web-прокси. В этом случае потребуется правило публикации сервера вместо правила публикации Web-сервера.

Выполните следующие шаги для создания определения протокола для публикации HTTP-сервера.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). Щелкните кнопкой мыши вкладку **Toolbox** (Инструментальная панель) на панели **Task** (Задача) и щелкните мышью заго ловок **Protocols** (Протоколы).
2. Щелкните кнопкой **мыши** последовательность команд меню **New** / **Protocol** (Новый / Протокол).
3. На странице **Welcome to the New Protocol Definition Wizard** (Вас привет ствует мастер создания нового определения протокола) введите **HTTP Server** в текстовое поле **Protocol Definition name** (Имя определения протокола) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Primary Connection Information** (Информация первичного со единения) щелкните мышью кнопку **New** (Новое).
5. На странице **New** / **Edit Protocol Connection** (Новый / Редактировать прото кол соединения) (рис. 8.50.) задайте **Protocol type** (Тип протокола) — **TCP** и **Direction** (Направление) — **Inbound.** В области страницы **Port range** (Диапа зон портов) укажите в текстовых полях **From** (От) и **To** (Кому) значения 80. Щелкните мышью кнопку OK.

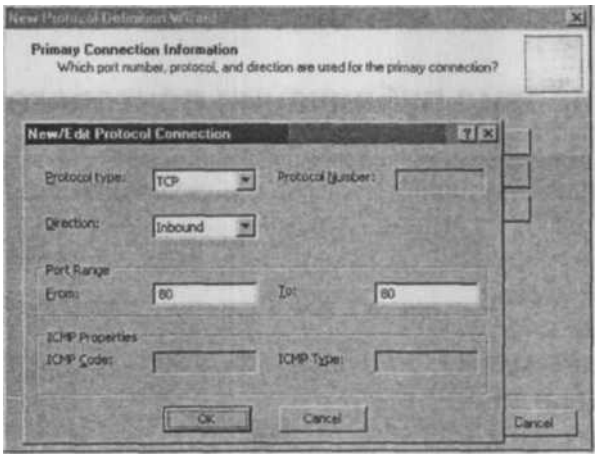


Рис. 8.50. Диалоговое окно New / Edit Protocol Connection (Новый / Редактировать протокол соединения)

6. Щелкните мышью кнопку Next (Далее) на странице **Primary Connection [nfor mation** (Информация первичного соединения).
7. На странице **Secondary Connections** (Вторичные соединения) выберите вариант No (Нет) и щелкните мышью кнопку **Next** (Далее).
8. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Protocol Definition Wizard** (Завершение мастера создания нового определе ния протокола).
9. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
10. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
11. Новое определение протокола **HTTP Server** появляется в списке определений протоколов **User-Defined** (Определенный пользователем) (рис. 8.51.).

Рис. 8.51. Новое определение протокола HTTP Server

Создание правил публикации почтового сервера

В брандмауэр ISA включен готовый мастер публикации почтового сервера (Mail Server Publishing Wizard). Его можно использовать для публикации следующих сервисов, связанных с почтой:

Outlook Web Access;
Outlook Mobile Access;
Secure Exchange RPC;
IMAP4 and Secure IMAP4;
POP3 and Secure POP3;
SMTP and Secure SMTP.

Мастер публикации почтового сервера создает соответствующие правила публикации сервера **и** Web-сервера, необходимые для разрешения доступа к опубликованному почтовому серверу через брандмауэр ISA. Получить доступ к мастеру публикации почтового сервера можно, щелкнув мышью на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и на вкладке **Tasks** (Задачи) панели **Task** (Задачи). Щелкните кнопкой мыши ссылку **Publish a Mail Server** (Опубликовать почтовый сервер).

На странице **Welcome to the New Mail Server Publishing Rule Wizard** (Вас приветствует мастер создания нового правила публикации почтового сервера) введите **название** правила в текстовое поле **Mail Server Publishing Rule name** (Название правила публикации почтового сервера). Присвойте правилу осмысленное название, чтобы по нему можно было определить назначение правила. Можно создать несколько правил публикации Web-сервера или сервера, основанных на ваших установках; имейте это в виду при выборе названия правила. Всегда можно изменить название правила после завершения мастера. Щелкните мышью кнопку **Next** (Далее).

На странице **Select Access Type** (Выберите тип доступа) (рис. 8.52) есть следующие варианты:

- Web client access (Доступ Web-клиента): Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync;
- Client access (Доступ клиента): RPC, IMAP, POP3, SMTP;
- Server-to-server communication (Связь сер вер-сервер): SMTP, NNTP.

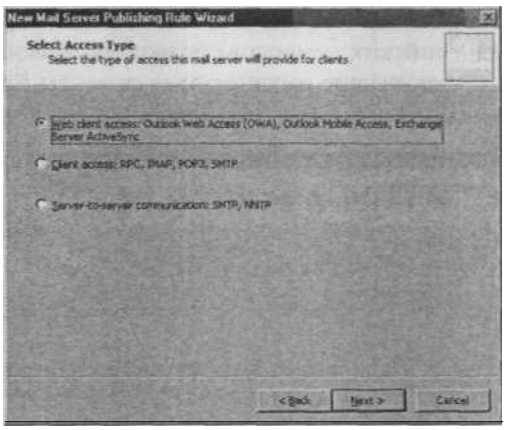


Рис. 8.52. Страница Select Access Type (Выберите тип доступа)

Вариант **Web client access** (Доступ Web-клиента): **Outlook Web** Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync публикует перечисленные сервисы с помощью правил публикации Web-сервера. Мастер конфигурирует в соответ-

ствии с вашими требованиями правила публикации Web-сервера. Можно создать SSL-соединения и соединения по протоколу, отличному от SSL.

Вариант **Client access** (Доступ клиента): **RPC, IMAP, POP3, SMTP** публикует перечисленные протоколы с помощью правил публикации сервера. Выбрав его, можно опубликовать один или несколько этих протоколов.

Вариант **Server-to-server communication** (Связь сер вер-сер в ер): **SMTP, NNTP** публикует указанные два протокола. Можно выбрать один или оба.

Поскольку параметры зависят от выбора, сделанного на этой странице, мы рассмотрим каждый из них отдельно в следующих разделах.

Вариант Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync

Выберите этот вариант и щелкните мышью кнопку **Next** (Далее). На странице **Select Services** (Выберите сервисы) выберите Web-сервисы Exchange, которые необходимо опубликовать с помощью правила публикации Web-сервера. Имеются следующие варианты:

- Outlook Web Access (Web-доступ в Outlook);
- Outlook Mobile Access (Мобильный доступ в Outlook);
- Exchange ActiveSync.

Правило публикации Web-сервера будет содержать выбранные пути доступа к сервисам сервера Exchange. Параметр **Enable high bit characters used by non-English character sets** (Разрешить символы, занимающие верхние биты и применяемые в наборах неанглийских символов) позволяет просматривать сообш.ения электронной почты, использующие расширенные символы. Если необходимо поддерживать символы английского языка, сбросьте этот флажок.

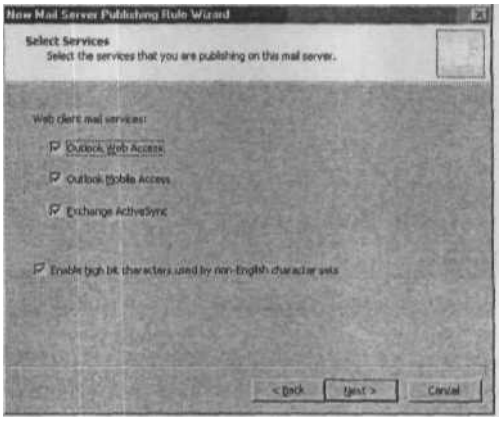


Рис. 8.53. Страница Select Services (Выберите сервисы)

Щелкните мышью кнопку **Next** (Далее) на странице **Select Services** (Выберите сервисы), показанной на рис. 8.53.

На странице **Bridging Mode** (Режим перенаправления) укажите, как вы хотите публиковать Web-сайт. Мы настоятельно рекомендуем всегда использовать перенаправление SSL-в-SSL. Это наиболее защищенный метод, минимизирующий проблемы совместимости. Более подробную информацию о настройке SSL-перенаправления можно найти в разделе, посвященном правилам публикации Web-серверов.

На странице **Specify the Web Mail Server** (Задайте почтовый Web-сервер) (см. рис. 8.54) введите имя Web-сервера в сети, защищенной брандмауэром ISA. Советуем использовать полностью определенное имя домена (FQDN) компьютера, совпадающее с общим именем в сертификате Web-сайта, используемом на Web-сайте Exchange OWA /OM A/Act iveSync. Кроме того, брандмауэр должен быть способен разрешить это имя в адрес, который действительно связан с сервером Exchange в корпоративной сети, а не с адресом внешнего интерфейса брандмауэра ISA. Посмотрите раздел, посвященный правилам публикации защищенных Web-серверов для получения более подробных сведений об этом.

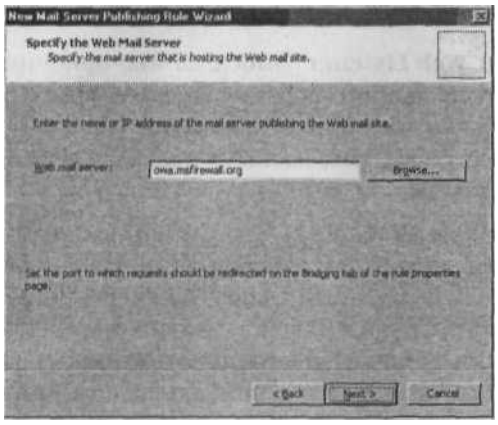


Рис. 8.54. Страница **Specify the Web Mail Server** (Задайте почтовый Web-сервер)

На странице **Public Name Details** (Параметры общедоступного имени) вы можете задать имя, которое пользователь, обращающийся к опубликованному серверу с помощью правила публикации Web-сервера, должен использовать для соединения с сайтом. Мы настоятельно рекомендуем всегда применять вариант **This domain name (type below)** (Данное имя домена, ввести ниже) в раскрывающемся списке **Accept requests for** (Принимать запросы к). Другой вариант списка менее безопасен и его следует избегать по мере возможности.

Введите в текстовое поле **Public name** (Общедоступное имя) имя, которое удаленные пользователи будут применять для доступа к сайту. Это имя должно разрешаться в IP-адрес на брандмауэре ISA, который ожидает запросы на входящие со-

единения. Этот IP-адрес определяется установками для Web-приемника, который вы сконфигурировали для использования данным правилом публикации Web-сервера. Щелкните мышью **кнопку Next** (Далее) (рис. 8.55).

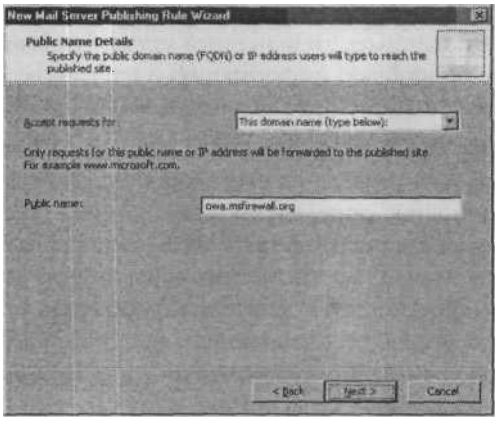


Рис. 8.55. Страница Public Name Details (Параметры общедоступного имени)

На странице **Select Web Listener** (Выберите Web-приемник) выберите или создайте Web-приемник для данного правила. Подробности создания и конфигурирования Web-приемников для правил публикации Web-серверов, пожалуйста, поищите в разделах этой главы, посвященных правилам публикации Web-серверов по HTTP- и SSL-протоколам.

На странице **User Sets** (Наборы пользователей) вы можете сконфигурировать правило, разрешающее всем пользователям соединяться с опубликованным Web-сервером, или потребовать предварительного подтверждения подлинности пользователей на брандмауэре ISA, прежде чем разрешить им доступ к опубликованному Web-сайту. Если выбрать предварительную аутентификацию на брандмауэре ISA, то необходимо сделать брандмауэр ISA членом домена пользователей или домена, которому доверяет домен пользователей. Альтернативный вариант — настроить брандмауэр ISA для RADIUS-аутентификации. Мы обсуждали, как конфигурировать брандмауэр ISA для RADIUS-аутентификации и как настроить RADIUS-группы в глаие 7, при обсуждении исходящего доступа через брандмауэр ISA. Щелкните мышью кнопку **Next** (Далее).

Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Mail Server Publishing Rule Wizard** (Завершение мастера создания нового правила публикации почтового сервера). Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра. В диалоговом окне **Apply New** Configuration (Применить новую конфигурацию) щелкните мышью кнопку ОК

Вариант Client Access: RPC, IMAP, P0P3, SMTP Option

Выберите этот вариант и щелкните мышью кнопку **Next** (Далее). На странице Select Services (Выберите сервисы) есть следующие параметры (см. рис. 8.56):

- Outlook (RPC) (Remote Procedure Call, удаленный вызов процедуры);
- POP3 (Post Office Protocol v. 3, почтовый протокол): Standard ports (Стандарт ные порты) и Secure ports (Защищенные порты);
- ШАР4 (Internet Message Access Protocol, протокол доступа к сообщениям в сети Интернет): Standard ports (Стандартные порты) и Secure ports (Защищенные порты);
- SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты): Standard ports (Стандартные порты) и Secure ports (Защищенные порты).

Вариант **Outlook (RPC)** создает правило публикации сервера, разрешающее входящий доступ к защищенным RPC-соединениям с сервером Exchange. Защищенная RPC-нубликация сервера Exchange разрешает программам Outlook 2000, 2002 и 2003 работать независимо от местоположения пользователя. Имея хорошо спроектированную разделяемую DNS-инфраструктуру, пользователи могут путешествовать между корпоративной сетью и удаленными местонахождениями, открывать программу Outlook и обращаться к своей электронной почте прозрачно (т. е. без перенастройки их приложений электронной почты). Secure Exchange RPC — очень безопасный протокол публикации, вы можете настроить правило публикации сервера по этому протоколу, которое будет требовать от клиентов Outlook шифрования их сообщений, отправляемых на сервер Exchange.

Варианты **POP3, IMAP4** и **SMTP** позволяют публиковать как защищенные, так и незащищенные версии этих протоколов. Защищенные версии используют SSL-протокол для шифрования и верительных данных пользователя и пользовательской информации. Брандмауэр ISA будет публиковать эти протоколы, используя правила **публикации** сервера, но для окончательной конфигурации вы должны задать на сервере Exchange сертификаты соответствующих Web-сайтов, если хотите применять защищенные версии этих протоколов.

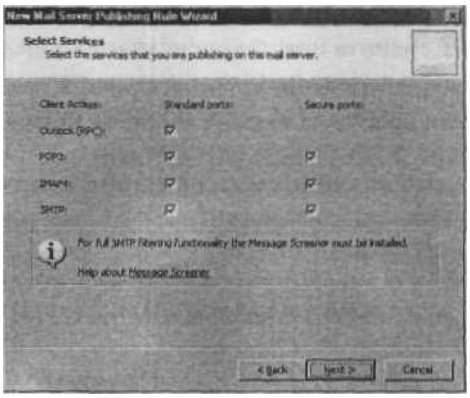


Рис. 8.56. Страница Select Services (Выберите сервисы)

Обратите внимание на информационную область на этой странице. В ней сообщается, что **For full SMTP filtering functionality the Message Screener must be installed** (Для обеспечения полных функциональных возможностей SMTP-фильтрации нужно установить **Message Screener** (программа просмотра сообщений)). Когда создается правило публикации SMTP-сервера с помощью данного мастера, включается фильтр защиты SMTP. Этот фильтр блокирует атаки на опубликованный SMTP-сервер, вызывающие переполнение буфера. Можно улучшить отслеживающий состояние соединения контроль прикладного уровня SMTP-сообщений, проходящих через правило публикации SMTP-сервера, установив и сконфигурировав программу просмотра SMTP-сообщений (SMTP Message screener) на брандмауэре ISA, специализированном SMTP-ретрансляторе (SMTP relay) или на самом сервере Exchange. Мы подробно обсудим программу SMTP Message Screener в главе К) при описании набора характеристик отслеживающей состояние соединения фильтрации прикладного уровня. Щелкните мышью кнопку **Next** (Далее) на странице **Select Services** (Выберите сервисы).

На странице **Select Server** (Выберите сервер) введите IP-адрес опубликованного сервера в корпоративной сети в текстовое поле **Select Server** (Выберите сервер). Щелкните мышью кнопку **Next** (Далее).

На странице **IP Addresses** (IP-адреса) выберите сеть, представляющую интерфейс, который должен принимать запросы на соединение с опубликованным сервером. Можно ограничить IP-адреса, используемые для доступа входящих соединений, если имеется несколько адресов, связанных с любым из данных интерфейсов, щелкнув мышью кнопку **Address** (Адрес). Для получения более подробных сведений о том, как конфигурировать установочные параметры на странице **IP Addresses** (IP-адреса) посмотрите обсуждение этого вопроса в разделе этой главы, посвященном правилам публикации сервера. Щелкните мышью кнопку **Next** (Далее).

Щелкните мышью кнопку **Finish** (Готово) на **странице Completing the New Mail Server Publishing Rule Wizard** (Завершение мастера создания правила публикации почтового сервера). Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра. В диалоговом окне **Apply New Configuration** (Применить новую конфигурацию) щелкните мышью кнопку ОК.

Вы увидите ряд новых правил на вкладке **Firewall Policy** (Политика брандмауэра) брандмауэра ISA **(рис.** 8.57). Можно переименовать эти правила, чтобы привести их в порядок и сделать их более согласованными с вашей собственной **политикой** именования правил.

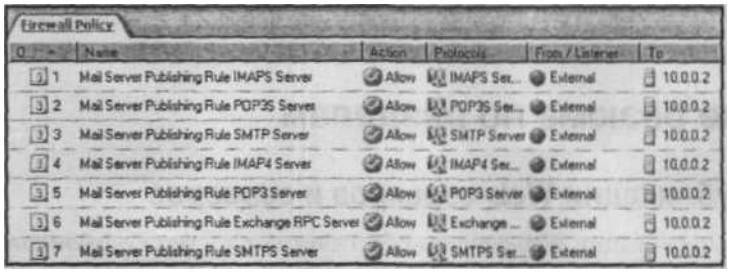


Рис. 8.57. Политика брандмауэра после выполнения **New Mail Server Publishing Rule Wizard** (Мастер создания правила публикации почтового сервера)

Можно усилить безопасность правила RPC-публикации защищенного сервера Exchange, заставив клиентов Outlook использовать защищенное соединение. Щелкните правой кнопкой мыши правило **Exchange RPC Server** и щелкните левой кнопкой мыши команду **Configure Exchange RPC** (Настроить Exchange RPC). Установите флажок **Enforce Encryption** (Требовать шифрование), щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK (рис. 8.58).

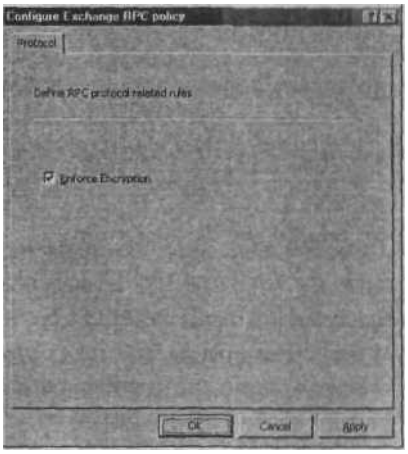


Рис. 8.58. Диалоговое окно **Configure Exchange RPC Policy** (Настроить Exchange RPC)

Резюме

В данной главе мы обсуждали методы, которые можно применять для обеспечения защищенного доступа к серверам и сервисам, защищенным брандмауэром ISA. Два первостепенных метода безопасного удаленного доступа к корпоративным сервисам — правила публикации Web-серверов и правила публикации серверов. Правила публикации Web-серверов можно применять для публикации HTTP-, HTTPS- и FTP-серверов. Правила публикации серверов могут опубликовать почти все другие про-

токолы. Мы подробно рассмотрели публикацию серверов и Web-серверов и способы конфигурирования и создания правил публикации серверов и Web-серверов.

Краткое резюме по разделам

Обзор публикации Web-серверов и серверов

0 Правила публикации Web-сервера обеспечивают доступ к опубликованным серверам через прокси; это более безопасный способ, чем реверсивные соединения с применением средств NAT.

13 Правила публикации Web-се рве ров и серверов предоставляют соединения для тщательного контроля на прикладном уровне, зависящего от протоколов публикации.

0 Фильтр защиты HTTP предоставляет HTTP- и SSL-соединения для очень глубокого контроля и позволяет контролировать доступ, основываясь на любом аспекте HTTP-коммуникаций.

0 Публикация Web-сервера разрешает выполнять перенаправление маршрутов.

0 Публикация Web-сервера предоставляет возможность предварительной аутентификации пользователя.

0 Публикация Web-сервера позволяет кэшировать содержимое опубликованных Web-сайтов.

0 Публикация Web-сервера разрешает публиковать многочисленные Web-сайты с применением одного IP-адреса, связанного с внешним интерфейсом брандмауэра ISA.

0 В правилах публикации как Web-сервера, так и сервера, вы можете замещать исходный адрес клиента адресом брандмауэра ISA или сохранять IP-адрес клиента.

0 Публикация Web-сервера поддерживает RADIUS-аутентификацию.

0 В правилах публикации как Web-сервера, так и сервера, поддерживается переадресация портов, Публикация Web-сервера обеспечивает также перенаправление протоколов.

0 Публикация сервера поддерживает публикацию всех TCP- и UDP-протоколов, включая составные протоколы.

0 Вы можете применять расписания, ограничивающие время доступности опубликованных сайтов как для правил публикации Web-серверов, так и для правил публикации серверов.

Создание и настройка правил публикации Web-серверов по протоколу, отличному от SSL

И Вы можете создать правила публикации Web-серверов по протоколу, отличному от SSL, с помощью Мастера создания правила публикации Web-сервера.

0 Используйте параметр **Forward the original host header instead of the actual one (specified above)** (Пересылать исходный заголовок хоста вместо фактического, заданного выше), когда необходимо, чтобы брандмауэр ISA пересылал имя хоста, которое клиент в Интернете посылает на брандмауэр ISA.

И Всегда применяйте конкретное общедоступное имя во всех правилах публикации Web-серверов. Не используйте параметр **Any domain name** (Любое имя домена) для приема запросов.

0 Используйте задание пути для управления доступом клиентов к определенным папкам и файлам на опубликованном Web-сервере при соединении по правилу публикации Web-сервера.

0 Параметры аутентификации, настроенные в Web-приемнике, определяют, какие протоколы аутентификации поддерживаются брандмауэром ISA для предварительного подтверждения подлинности соединений с опубликованным Web-сайтом.

0 Применяйте делегирование базовой аутентификации при публикации Web-сайтов для того, чтобы помешать представлению пользователей в многочисленных диалоговых окнах регистрационных журналов.

И Настраивайте Web-приемники для ожидания запросов с конкретного IP-адреса. Не конфигурируйте Web-приемники для ожидания запросов со всех IP-адресов, до тех пор пока вы не применяете телефонное соединение с Интернетом.

И Избегайте конфликтов сокетов и снижения защищенности брандмауэра ISA — не устанавливайте на брандмауэр ISA никаких сервисов IIS (Internet Information Server, информационный сервер Интернета) за исключением SMTP-сервиса **IIS.**

0 Выбирайте вариант **Require all users to authenticate** (Требуется аутентификация всех пользователей), если все правила публикации Web-серверов, использующие конкретный Web-приемник, будут требовать предварительной аутентификации брандмауэром ISA.

0 Конфигурируйте разные Web-приемники для HTTP- и SSL-соединений, даже когда Web-приемники ожидают запросы на одном и том же IP-адресе.

Создание и настройка правил публикации Web-серверов по протоколу SSL

В Брандмауэр ISA поддерживает как SSL-сопряжение, так и SSL-туннелирование, SSL-сопряжение — более безопасный вариант.

И Сопряжение SSL-с-SSL — наиболее защищенный метод SSL-перенаправления и предпочтительный метод SSL-публикации.

ЕЗ Общедоступное имя должно быть таким же, как общее имя в сертификате, связанном с Web-прием ником.

0 Имя на вкладке То (Кому) в правиле публикации Web-сервера должно быть таким же, как имя, связанное с сертификатом Web-сайта на опубликованном Web-сайте.

0 Если возникает несовпадение имен, пользователь увидит ошибку 500 внутреннего сервера.

И Наиболее распространенная причина отсутствия сертификата Web-сайта в списке сертификатов, доступных для связывания с Web-приемником, состоит в том, что п сертификат не включен секретный ключ.

Создание правил публикации сервера

В Правила публикации серверов предоставляют реверсивные NAT-средства для публикуемых серверов.

0 Правила публикации серверов открыты для отслеживающего состояние соединения контроля на прикладном уровне, зависящего от протокола публикации.

И Можно настроить пере адресацию порта для любого протокола, используемого и правиле публикации сервера.

И Можно управлять исходными портами, доступными для любого протокола правила публикации сервера.

0 Можно конфигурировать правила публикации серверов для сохранения IP-адреса удаленного клиента или замещения этого адреса IP-адресом брандмауэра ISA.

Создание правил публикации почтового сервера

0 Мастер публикации почтового сервера брандмауэра ISA позволяет публиковать общие почтовые протоколы сервера.

0 Можно использовать мастер публикации почтового сервера для публикации Web-сайтов OWA, OMA и ActiveSync.

0 С помощью мастера публикации почтового сервера можно создавать правила публикации серверов SMTP, NNTP, POP3(S) и IMAP4(S).

0 На опубликованном почтовом Web-сервере может потребоваться дополнительная настройка для полной поддержки конфигурации публикации.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»),** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Я могу получать входящую электронную почту с моего SMTP-сервера, опубликованного правилом публикации сервера, но исходящая почта не отправляется. Как мне справиться с этим?

О: Поступление почты с SMTP-серверов в Интернете на ваши корпоративные SMTP-серверы управляется правилом публикации сервера, пропускающим почту через брандмауэр ISA на SMTP-сервер в корпоративной сети. Внешний DNS также

был сконфигурирован для разрешения ваших MX-имен (mail exchange) в IP-адрес внешнего интерфейса брандмауэра ISA. Для исходящих SMTP-соединений вам нужно убедиться в том, что SMTP-сервер способен разрешать имена SMTP-серверов, ответственных за почту в каждом интернет-домене. Вы должны настроить брандмауэр ISA с помощью правил доступа, разрешающих исходящий доступ с SMTP-сервера в Интернет. Кроме того, следует убедиться, что SMTP-сервер сконфигурирован с DNS-сервером, у которого есть доступ к правилу доступа DNS-сервера.

В: Я получаю ошибку внутреннего сервера 500 Internal Server, когда пытаюсь соединиться с Web-сайтом OWA. В чем дело?

О: Проблема состоит в том, что общее имя в сертификате Web-сайта, связанного с опубликованным Web-сервером, не совпадает с именем на вкладке To (Кому) в правиле публикации Web-сервера. Измените имя или IP-адрес, приведенный в списке на вкладке To (Кому), так, чтобы оно было таким же, как общее имя в сертификате Web-сайта. Убедитесь также, что брандмауэр ISA способен разрешать это имя в действительный IP-адрес Web-сайта (за исключением случая, когда Web-сайт отделен от брандмауэра ISA механизмом NAT, в этой ситуации имя должно разрешаться в IP-адрес интерфейса на устройстве, выполняющем обратное NAT-преобразование).

В: Мои пользователи получают многочисленные запросы подтверждения подлинности при попытке соединиться с моим опубликованным Web-сайтом. Как мне настроить брандмауэр ISA, чтобы пользователи видели окно регистрации один раз?

О: В настройках Web-приемника задайте базовую аутентификацию (Basic authentication), а затем в правиле публикации Web-сервера выберите делегирование базовых верительных данных (delegation of Basic credentials). Затем убедитесь в том, что опубликованный Web-сайт поддерживает базовую аутентификацию. После этого пользователи не будут получать многочисленных запросов аутентификации.

В: Я хочу опубликовать почтовый сервер в сети, защищенной брандмауэром ISA, но при этом не хочу, чтобы компьютер был клиентом SecureNAT. Как я могу конфигурировать брандмауэр ISA без необходимости настройки машины как клиент SecureNAT?

О: Вы можете конфигурировать правило публикации сервера так, чтобы IP-адрес брандмауэра ISA замещал IP-адрес исходного хоста. В этом случае единственный маршрут, который должен знать SMTP-сервер, — это маршрут к сетевому идентификатору, на который интерфейс передает соединение с SMTP-сервером.

В: Мы хотим разрешить VPN-клиентам доступ только к нашему почтовому серверу Microsoft Exchange Server по протоколу Secure Exchange RPC. Это возможно?

О: Вы можете использовать Мастер публикации почтового сервера (Mail Server Publishing Wizard) для создания правила публикации Secure Exchange RPC Server с приемником для сети VPN-клиентов. Затем создайте правило публикации DNS-сервера с приемником для сети VPN-клиентов. Используя комбинацию этих двух правил публикации сервера, вы сможете опубликовать DNS- и Exchange-серверы вашей корпоративной сети для членов сети VPN-клиентов и разрешить им соединяться с вашим сервером Exchange только с помощью защищенного протокола Exchange RPC и получать доступ только к Exchange- и DNS-серверам и ни к каким другим серверам сети.

В: Для нашего опубликованного Web-сайта настроено перенаправление SSL-B-HTTP, но оно не работает. Как я могу настроить правило публикации Web-сервера для того, чтобы перенаправление SSL-B-HTTP функционировало нормально?

О: Проблемы, связанные с перенаправлением SSL-B-HTTP, заключаются в том, что Web-серверы часто динамически формируют ссылки, основанные на протоколе, применяемом для соединения. Поскольку связь между брандмауэром ISA и опубликованным Web-сервером устанавливается по HTTP- протокол у, Web-сервер генерирует HTTP-ссылку, которая и возвращается Web-клиенту в Интернете. Но для соединения Web-клиента с брандмауэром ISA требуется SSL-ссылка, и соединение заканчивается неудачей. Вы можете решить эту проблему, используя трансляцию ссылок (Link Translation) брандмауэра ISA, но гораздо лучше применить сопряжение SSL-c-SSL. Не только потому, что этот вид перенаправления решает проблему некорректной ссылки, но и потому, что он повысит общий уровень безопасности вашего опубликованного Web-сервера.

В: Мы хотим опубликовать Web-сервер по протоколу HTTP с помощью правила публикации сервера, потому что на компьютере есть Web-приложен ие, не поддерживающее CERN-совместимые Web-прокси, Как это можно сделать?

О: Вы можете опубликовать Web-сервер по протоколу HTTP, используя правило публикации сервера вместо правила публикации Web-сервера. Прежде чем применять правило публикации сервера для опубликования Web-сервера по протоколу HTTP, вы должны убедиться в том, что нет Web-приемника, использующего со кет, который вы хотите применить в этом правиле (и сервис IIS WWW не установлен на брандмауэре ISA). Если это действительно так, создайте определение протокола для TCP-порта 80 с направлением Inbound (Входящий). Затем используйте это определение протокола в правиле публикации сервера.

Глава

VPN-соединения удаленного доступа и конфигурации «узел-в-узел» в брандмауэре ISA Server 2004

Основные темы главы:

- **Обзор использования VPN брандмауэром ISA**
- **Создание VPN-сервера удаленного доступа по протоколу PPTP**
- **Создание VPN-сервера удаленного доступа по протоколу L2TP/IPSec**
- **Создание VPN-соединения « узел-в-узел» по протоколу PPTP**
- **Создание VPN-соединения «узел-в-узел» по протоколу L2TP/IPSec**
- **Туннельный режим протокола IPSec *в* VPN конфигурации «узел-в-узел» с VPN-шлюзами**
- **Использование системы RADIUS для VPN-аутентификации и политики удаленного доступа**
- **Применение аутентификации сертификатами пользователя с помощью протокола EAP для VPN-соединений удаленного доступа**
- **Поддержка исходящих VPN-соединений через брандмауэр ISA**
- **Установка и конфигурирование DHCP-сервера и агента ретрансляции DHCP на брандмауэре ISA**
- **Создание VPN конфигурации «узел-в-узел» между ISA Server 2000 и брандмауэром ISA**
- **Заметки о VPN-карантине**

Обзор использования VPN брандмауэром ISA

Постоянный рост популярности виртуальных частных сетей (VPN) превратил их в стандарт для компаний, имеющих надомных работников, администраторов и продавцов, которым необходим доступ к сети вне офиса, а также партнеров и клиентов, нуждающихся в доступе к ресурсам корпоративной сети. Задача VPN — разрешить удаленный доступ к ресурсам корпоративной сети, которые в противном случае могут быть доступными только при непосредственном подключении пользователя к локальной сети. С помощью VPN-соединения пользователь получает «виртуальное», конфигурации узел-в-узел соединение удаленного VPN-пользователя с корпоративной сетью. Пользователь может работать так, как будто он (она) находится в офисе; приложения и сервисы, выполняющиеся на компьютерах пользователей, интерпретируют VPN-линию связи как типичное соединение Ethernet. Интернет, через который клиент соединяется с корпоративной сетью, полностью скрыт от пользователей и приложений (прозрачен для них).

Одно из главных преимуществ применения VPN-соединения по сравнению с клиент-серверным Web-приложением заключается в том, что VPN-пользователи, находящиеся далеко от локальной сети, могут получить доступ ко всем протоколам и серверам корпоративной сети. Это означает, что у ваших пользователей есть возможность получить доступ к полному набору сервисов серверов Microsoft Exchange, Microsoft SharePoint Servers, Microsoft SQL Servers и Microsoft Live Communication Servers так же, как если бы эти пользователи непосредственно подключались к сети, находясь в корпоративном офисе. Программное обеспечение VPN-клиента встроено во все современные операционные системы Windows. VPN-пользователю не нужны никакие специальные программные средства для подключения к любому из этих сервисов и нет необходимости создавать специальные приложения прокси, разрешающие вашим пользователям подсоединяться к этим ресурсам.

ISA Server 2000 был первым брандмауэром корпорации Microsoft, обеспечивающим тесную интеграцию VPN и управление ими. В состав ISA Server 2000 были включены удобные мастера, упрощающие создание VPN-соединений удаленного доступа и межшлюзовых.или узел-в-узел VPN-соединений с брандмауэром ISA Server 2000/VPN-серВероМ. Но сформированную структуру все еще можно было улучшить. VPN-сервер брандмауэра ISA Server 2000 требовал от администратора брандмауэра значительных затрат времени на точную настройку конфигурации VPN-сервера с помощью консоли сервиса Routing and Remote Access (маршрутизация и удаленный доступ).

В ISA Server 2004 существенно усовершенствованы VPN-компоненты, которые включены в состав брандмауэра из сервиса Routing and Remote Access (RRAS) операционных систем Windows 2000 и Windows Server 2003. Теперь администратор имеет возможность конфигурировать VPN-сервер и шлюзовые компоненты и управлять ими непосредственно на консоли управления брандмауэра ISA Server 2004,

не переключаясь между консолью управления ISA MMC и консолью управления RRAS MMC. Вам очень редко понадобится консоль сервиса маршрутизации и удаленного доступа для конфигурирования VPN-компонентов.

К другим усовершенствованиям функциональных возможностей использования VPN в ISA Server 2004 можно отнести следующие:

- политику брандмауэра, применяемую к соединениям VPN-клиентов;
- политику брандмауэра, применяемую к VPN-соединениям конфигурации узел-в-узел;
- VPN-карантин или временную изоляцию;
- отображение пользователей для VPN-клиентов;
- поддержку клиентов SecureNAT для VPN-соединений;
- виртуальную частную сеть конфигурации «узел-в-узел» с применением туннельного режима протокола IPSec;
- публикацию VPN-серверов по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол);
- поддержку аутентификации секретным ключом Pre-shared Key для VPN-соединений по протоколу IPSec;
- улучшенная работа сервера имен для VPN-клиентов;
- мониторинг соединений VPN-клиентов.

Эти новые свойства VPN-сервера и шлюза делают ISA 2004 одной из наиболее мощных реализаций как VPN, так и брандмауэров, представленных сегодня на рынке. В следующих разделах обсуждаются эти новые характеристики и их совместное функционирование, делающее VPN-реализацию в ISA 2004, предпочтительной для всех организаций, эксплуатирующих сети Microsoft.

Политика брандмауэра, применяемая к соединениям VPN-клиентов

Когда VPN-клиент удаленного доступа устанавливает соединение с VPN-сервером, он действует как компьютер, непосредственно подключенный к корпоративной сети. Это виртуальное соединение с корпоративной сетью разрешает удаленному VPN-пользователю получить доступ почти к любому ресурсу корпоративной сети, ограниченный только конфигурированием средств управления доступом на серверах и рабочих станциях. Однако такие широкие возможности для доступа к ресурсам корпоративной сети могут стать угрозой ее безопасности. Как правило, не следует предоставлять неограниченный доступ к корпоративным ресурсам пользователям, если они соединяются с помощью VPN-соединения удаленного доступа. Такой подход объясняется тем, что эти пользователи могут подключаться с компьютеров, находящихся вне сферы вашего контроля и не удовлетворяющих требованиям корпоративной программной политики и политики безопасности, либо они

устанавливают соединения с компьютеров, находящихся в ненадежных сетях (untrusted networks), таких как широковещательные сети отелей, и нет способа проверить, не представляют ли они угрозу для вашей сети.

В VPN-политике следует особо оговорить, что только пользователям с широкими полномочиями (highly-trusted), подключающимся с известных высоконадежных машин, размещенных в известных заслуживающих доверия сетях, разрешен свободный доступ к корпоративной сети по VPN-каналу удаленного доступа. К числу таких пользователей с гарантированным полным доступом относятся администраторы сети, системы безопасности и брандмауэра и, возможно, некоторые руководители высокого ранга. Всех остальных пользователей, подключающихся по VPN-каналу, следует ограничить, предоставив им доступ только к подмножеству сетевых ресурсов, необходимых для выполнения их работы.

Например, многие администраторы брандмауэров разрешают пользователям устанавливать VPN-соединения для использования полного клиента Outlook 2000/2002/2003 MAPI (Messaging Application Programming Interface, интерфейс прикладного программирования для **электронной** почты корпорации Microsoft) и получения доступа к почтовому серверу Microsoft Exchange. Пакет Microsoft Exchange предоставляет несколько разных методов удаленного доступа к ресурсам сервера Exchange. К ним относятся сервисы SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты), POP3 (Post Office Protocol v. 3, почтовый протокол), IMAP3 (Interactive Mail Access Protocol v. 3, протокол интерактивного доступа к электронной почте) и Outlook Web Access (OWA) (Web-доступ в Outlook). Однако пользователи предпочитают иметь широкий диапазон возможных вариантов, предоставляемых полным клиентом Outlook MAPI.

В этом случае есть три основных способа удовлетворения потребностей пользователей:

- опубликовать сервер Exchange, используя в ISA Server правило публикации сервера с помощью протокола secure Exchange RPC (защищенный удаленный вызов процедуры);
- заставить ваших пользователей применять Outlook 2003/Exchange 2003 RPC по HTTP- протоколу;
- предоставить вашим пользователям VPN-доступ к корпоративной сети.

Механизм публикации сервера с помощью сервиса secure RPC позволяет удаленным клиентам Outlook MAPI из любого местонахождения устанавливать соединения с полным набором сервисов сервера Microsoft Exchange. Единственная проблема заключается в том, что по соображениям безопасности многие брандмауэры и провайдеры интернет-услуг блокируют доступ к порту редиректора (mapper port) RPC (TCP-порт 135). Этот порт требуется для создания начального защищенного подключения к серверу Exchange с применением правила публикации по протоколу secure Exchange RPC, но червь Blaster, поражающий этот порт, вынуждает боль-

шинство администраторов закрыть порт. В результате RPC-публикация утрачивает большую часть упомянутой полезности.

Эту проблему может решить применение RPC-протокола поверх протокола HTTP(S), инкапсулирующее RPC-соединение внутри HTTP- за головка, что позволяет клиенту Outlook MAPI посылать запросы серверу Exchange с помощью HTTP-протокола. Этот протокол, как правило, разрешают использовать все корпоративные брандмауэры и провайдеры интернет-услуг, поскольку он применяется для Web-соединений. Недостаток такого подхода заключается в том, что не все организации обновили свои версии до версий Outlook 2003 и Exchange Server 2003.

Предоставление пользователям VPN-доступа устраняет ограничения, присущие другим подходам, но подобный доступ может представлять собой угрозу безопасности в том случае, когда все VPN-клиенты получают доступ ко всей сети. Лучшим решением может быть формирование для VPN-клиентов политики доступа, основанной на учетных записях пользователей/групп. В этом случае пользователи смогут обращаться только к тем серверам и протоколам, которые им необходимы.

Создание VPN-сервера на базе брандмауэра ISA 2004 — это решение, дающее администраторам именно такой уровень контроля доступа. Когда VPN-клиенты соединяются с VPN-сервером, они помещаются во встроенный сетевой объект, названный *VPN Clients Network (сеть VPN-клиентов)*. Брандмауэр ISA 2004 трактует эту сеть, как любую другую, что означает возможность строгого, ориентированного на пользователей/группы контроля данных, перемещающихся между сетью VPN-клиентов и корпоративной сетью.

Все, что для этого требуется, — *создать* учетные записи пользователей и сформировать политику доступа на брандмауэре ISA 2004/VPN-серВере, ограничивающую машины и протоколы, которые поль зов а тел и/группы могут использовать, и все эти сетевые компоненты будут защищены от доступа VPN-пользователей удаленного доступа.

Эта функциональная возможность фактически исключает необходимость SSL-соединений в сетях VPN (за исключением случаев, когда удаленные пользователи находятся за крайне ограничивающими доступ брандмауэрами, которые блокируют чуть ли не исходящие HTTP- и SSL-соединения) и других патентованных методах удаленного доступа, направленных на обеспечение доступа к ресурсам корпоративной сети, ориентированного на протокол, сервер, пользователя/группу. В большинстве коммерческих широкополосных сетей отелей и конференц-центров разрешается исходящий доступ по протоколам PPTP и L2TP/IPSec с применением средств обходящего NAT (NAT Traversal). В этом случае вы можете предоставить удаленный доступ вашим VPN-пользователям без угрозы безопасности, как правило, сопровождающей соединения VPN-клиентов.

Политика брандмауэра, применяемая к VPN-соединениям конфигурации узел-в-узел

VPN-соединение с конфигурацией узел-в-узел соединяет две или несколько сетей (а не отдельный клиент и сеть) через Интернет. Использование VPN-канала конфигурации узел-в-узел может дать существенное снижение себестоимости по сравнению с выделенными соединениями (dedicated link) WAN (Wide-Area Network, глобальная сеть), использующими выделенные каналы (dedicated circuits) (например, соединение двух сайтов с помощью специализированной многоканальной телефонной линии T-1).

Для применения VPN-соединения узел-в-узел каждому сайту нужен VPN-шлюз и сравнительно недорогое интернет-соединение. Когда VPN-шлюзы **установят** соединения друг с другом, VPN-соединение типа узел-в-узел установлено. Далее пользователи на каждом конце соединения могут связываться с другими сетями через VPN-соединение типа узел-в-узел так, как они это делали бы с помощью маршругного соединения в их собственной сети. VPN-шлюзы действуют как маршрутизаторы *и* пересылают пакеты в соответствующую сеть.

В VPN-соединениях конфигурации узел-в-узел используются те же технологии, что и в VPN-соединениях (удаленного доступа) типа клиент-сервер, и обычно они сталкиваются с той же проблемой безопасности. Все пользователи получают доступ ко всей сети, с которой соединена их собственная сеть. Единственное, что может оградить пользователей от самовольного доступа к ресурсам без разрешения, — локальные средства управления доступом на серверах.

VPN-соединения конфигурации узел-в-узел обычно устанавливаются между сетями филиала и центрального офиса. Предоставление пользователям филиала доступа ко всей сети центрального офиса может создать серьезную угрозу безопасности ресурсов.

Брандмауэр ISA 2004/VPN-сереер может решить эту проблему, контролируя исходящие данные, которые передаются по каналу узел-в-узел. Доступ пользевателей филиала можно ограничить только теми ресурсами сети центрального офиса, которые нужны им для работы, и таким образом помешать доступу к другим сетевым ресурсам центрального офиса. Как и VPN-клиентам удаленного доступа, пользователям филиала следует разрешить применение только определенных протоколов, требующихся на серверах, к которым пользователи получили доступ.

VPN-соединения конфигурации узел-в-узел, обладающие средствами управления доступом, основанными на строгом контроле пользователей и групп, помогут сэкономить деньги без ущерба безопасности.

VPN-карантин

Временная изоляция, или VPN-карантин (VPN-Q), — новое свойство, позволяющее тщательно проверять машины VPN-клиентов, прежде чем разрешить им доступ к корпоративной сети. VPN-карантин, включенный в состав ISA Server 2004, подобен сетевому карантину служб маршрутизации и удаленного доступа (RRAS) в операционной системе Windows Server 2003.

Для использования VPN-Q нужно создать модуль CMAK (Connection Manager Administration Kit, комплект администрирования менеджера соединений), включающий сценарий VPN-Q клиента (VPN-Q client) и VPN-Q клиентской стороны (VPN-Q client-side). Клиент запускает сценарий и передает результаты серверному компоненту VPN-Q на брандмауэре ISA 2004/VPN-сервере. VPN-клиент перемещается из сети «VPN Quarantine» (VPN-карантин) в сеть «VPN Clients» (VPN-клиенты), если сценарий сообщает, что клиент соответствует требованиям, предъявляемым к сетевым соединениям. Вы можете задать для хостов в сети VPN-карантина политику доступа, отличающуюся от политики доступа сети VPN-клиентов.

Брандмауэр ISA Server 2004 расширяет функциональные возможности средств управления карантина службы маршрутизации и удаленного доступа Windows Server 2003, поскольку карантин в сервисе RRAS операционной системы Windows Server 2003 не позволяет установить средства управления доступом, базирующиеся на политике доступа. Карантин в RRAS использует простые средства управления, основанные на портах, но реально такой подход не обеспечивает никакого серьезного уровня защиты. Брандмауэр ISA Server 2004 применяет мощные базирующиеся на политике брандмауэра средства управления доступом к хостам в сети VPN-карантина и подвергает эти соединения обработке с помощью усовершенствованных фильтров уровня приложений брандмауэра ISA Server 2004.

> ПРИМЕЧАНИЕ Есть хорошие новости для администраторов брандмауэра ISA Server 2004, планирующих установить брандмауэр в Windows 2000: если вы устанавливаете ISA Server 2004 на машине под управлением Windows 2000, вам доступно в брандмауэре свойство VPN-Q. Другими словами, для использования VPN-карантина не нужна ОС Windows Server 2003, если ISA 2004 инсталлирован на компьютере под управлением Windows 2000. (Есть ограничение, заключающееся в том, что вы вынуждены использовать политики VPN-Q брандмауэра ISA 2004 скорее чем RADIUS-политики, но дополнительная функциональность, которую вносит ISA 2004 в VPN сервиса RRAS ОС Windows 2000, — значительна.)

Отображение пользователей для VPN-клиентов

Отображение пользователей (User mapping) — способ, позволяющий отображать клиентов виртуальной частной сети, соединяющихся с ISA Server, с помощью ме-

тода аутентификации, отличного от «Windows-аутентификации» (например, RADIUS- или EAP-аутентификация), в пространство имен Windows. Включенное и должным образом настроенное отображение пользователей дает возможность применять к пользователям, подтвердившим подлинность без применения Windows-аутентификации, политику правил доступа брандмауэра, определяющую наборы пользователей для пользователей и групп ОС Windows. По умолчанию политика правил доступа брандмауэра не распространяется на пользователей из других (не Windows) пространств имен до тех пор, пока не определено отображение пользователей.

Функциональная возможность отображения пользователей расширяет набор мощных, основанных на пользователе/группе средств управления доступом, которые можно применять к VPN-клиентам, использующим метод аутентификации, отличный от Windows-аутентификации.

Это важно, потому что Windows-аутентификация пользователей домена доступна, только если брандмауэр ISA 2004 принадлежит домену, содержащему учетные записи пользователей, или **домену,** заслуживающему доверие домена с учетными записями пользователей. Если брандмауэр ISA 2004 не включен в домен, аутентификация применяется только для пользователей, учетные записи которых хранятся непосредственно на машине с брандмауэром ISA 2004.

Благодаря отображению пользователей можно использовать RADIUS-аутентификацию пользователей домена и применять средства управления и контроля доступа, основанные на пользователе/группе, к VPN-клиентам, подтвердившим свою подлинность с помощью RADIUS-аутентификации.

Поддержка клиентов SecureNAT для VPN-соединений

Когда VPN-клиент соединяется с VPN-сервером, таблица маршрутизации VPN-клиента изменяется и текущим шлюзом становится IP-адрес VPN-сервера. Это создает потенциальные проблемы для VPN-клиентов, поскольку во время VPN-соединения у них нет доступа к ресурсам Интернета.

Проблема брандмауэра ISA Server 2000/VPN-серВероВ заключалась в следующем: для доступа VPN-клиентов к ресурсам Интернета следовало выбрать один из перечисленных далее вариантов:

- разрешить разделенное туннелирование (split tunneling) для VPN-клиента;
- установить программное обеспечение клиента брандмауэра (Firewall Client) на машинах VPN-клиентов;
- настроить установочные параметры Dial-up и виртуальной частной сети VPN-соединения с помощью параметров прокси-сервера (этот вариант разрешает просмотр в Internet Explorer, только когда клиент соединен с VPN).

Разделенное туннелирование означает конфигурацию, в которой машина VPN-клиента не использует шлюз по умолчанию в удаленной сети. Установка по умол-

чанию VPN-клиентов Microsoft предполагает применение этого шлюза. Для VPN требуется два соединения: первое — подключение **к** Интернету (благодаря широкополосной или другой всегда функционирующей (always-on) технологии это соединение не должно устанавливаться каждый раз вручную); второе — VPN-соединение, устанавливаемое поверх интернет-соединения. Когда VPN-клиенты не сконфигурированы для использования шлюза по умолчанию, они могут получать доступ к ресурсам корпоративной сети с помощью VPN-соединения, а к ресурсам Интернета с помощью интернет-соединения, установленного машиной VPN-клиента, прежде чем было создано VPN-соединение.

Возникают серьезные угрозы безопасности, если машина VPN-клиента может получать прямой доступ к Интернету в то же самое время, **когда** она способна обращаться к ресурсам корпоративной сети через VPN-соединение. Это позволяет компьютеру VPN-клиента игнорировать все правила доступа к Интернету, сконфигурированные на брандмауэре ISA Server 2000 для периода VPN-соединения. Разделенное туннелирование похоже на разрешение пользователям корпоративной сети устанавливать локально соединения через модем наряду с подключениями к локальной сети. Модемные соединения в этом случае полностью **игнорировали** бы политику брандмауэра ISA Server 2000 и давали бы возможность рабочей станции получить доступ к Интернету, который иначе был бы запрещен политикой брандмауэра ISA Server 2000. Такая ситуация создает возможность загрузки червей, вирусов и другого опасного содержимого. Злоумышленник в Интернете мог бы отправить свои вредоносные программы с внешнего компьютера через машину, выполняющую разделенное туннелирование, в корпоративную сеть.

Описанный риск делает важным выбор альтернативного метода предоставления доступа к Интернету VPN-клиентам во время их соединения с брандмауэром ISA 2004/VPN-сервером. В брандмауэре ISA Server 2000 предпочтительный вариант — установка программного обеспечения клиента брандмауэра на машину VPN-клиента. Клиент брандмауэра пересылает запросы прямо на внутренний IP-адрес брандмауэра ISA Server и не требует разделенного туннелирования для разрешения компьютеру клиента подключения к Интернету. Кроме того, клиент брандмауэра делает открытой машину VPN-клиента для применения политики доступа брандмауэра ISA Server 2000.

Брандмауэр ISA 2004/VPN-серверы решают эту проблему, не требуя установки клиента брандмауэра, с помощью предоставления доступа к Интернету клиентов SecureNAT (безопасное преобразование сетевых адресов) VPN-клиентов, VPN-клиенты являются по умолчанию клиентами SecureNAT брандмауэра ISA 2004, потому что они используют брандмауэр как шлюз по умолчанию. Брандмауэр ISA 2004/VPN-сервер может использовать верительные данные регистрации VPN-клиента для применения усиленных, основанных на пользователе/группе средств управления доступом для того, чтобы ограничить набор сайтов, типы содержимого и протоколы, разрешенные на машинах VPN-клиентов для доступа к Интернету.

ПРИМЕЧАНИЕ Несмотря на то, что не требуется установки клиента брандмауэра на компьютеры VPN-клиентов для разрешения доступа к Интернету через машину с брандмауэром ISA 2004, возможно вы все-таки захотите установить клиенты брандмауэра на машинах VPN-клиентов для поддержки сложных (complex) протоколов, необходимых для вторичных (secondary) соединений, если не применяется фильтр приложения, обеспечивающий вторичные соединения. Машины с установленными клиентами брандмауэра могут без участия фильтра приложений получить доступ по любому TCP- или UDP-протоколу, даже если они требуют вторичных соединений.

Альтернативой применения клиентов брандмауэра на машинах VPN-клиентов может быть конфигурирование параметров коммутации (Dial-up) и сетевых установочных параметров объекта соединения VPN-клиента в Internet Explorer с помощью установки параметров прокси-сервера. Если вы используете ISA Server 2000, можно конфигурировать объект VPN-соединения с помощью тех же установочных параметров Web-прокси, которые применяются внутренними клиентами. Однако такой подход позволяет VPN-клиентам использовать HTTP-, HTTP(S)- и FTP-протоколы (только для загрузки файлов) для доступа в Интернет. И эта же возможяость сохраняется при соединении с брандмауэром ISA 2004/VPN -сервера МН.

VPN конфигурации узел-в-узел с применением туннельного режима протокола IPSec

С помощью брандмауэра ISA Server 2000 VPN-клиенты удаленного доступа могли использовать протоколы PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол) или L2TP/IPSec (Layer Two Tunneling Protocol/Internet Protocol Security, протокол туннелирования второго уровня модели OSI/протокол безопасности IP) для соединения с VPN-сервером брандмауэра ISA Server 2000. И другие VPN-шлюзы могли соединиться с VPN-шлюзом брандмауэра ISA Server 2000 и установить VPN-каналы конфигурации узел-в-узел между двумя географически разделенными сетями. Однако большинство разработанных сторонними фирмами VPN-шлюзов (такие как Cisco или другие популярные реализации VPN-шлюзов) не поддерживали протоколов PPTP или L2TP/IPSec для межшлюзовых VPN-каналов. Вместо этого они требовали применения туннельного режима протокола IPSec (IPSec tunnel mode) для VPN-соединения.

Если на обоих сайтах стояли брандмауэры ISA Server 2000/VPN-серверы, было просто создать между двумя сайтами с высокой степенью защиты VPN-соединение по протоколу L2TP/IPSec или менее защищенное VPN-соединение по протоколу PPTP. Однако, если в центральном офисе был размещен VPN-шлюз сторонней фирмы, а вы хотели установить VPN-шлюз брандмауэра ISA Server 2000 в филиале, вы не могли создать VPN-со единение типа узел-в-узел с VPN-шлюзом центрального офиса, поскольку этот шлюз не поддерживал соединения по протоколам PPTP или L2TP/IPSec,

а брандмауэр ISA Server 2000 не поддерживал туннельного режима протокола IPSec для соединений по каналам с конфигурацией узел-в-узел.

Брандмауэры ISA 2004 решают эту проблему, потому что теперь можно использовать туннельный режим протокола IPSec для соединений конфигурации узел-в-узел между VPN-шлюзом брандмауэра ISA 2004 и VPN-шлюзом стороннего производителя. Кроме того, что вы можете применять протокол PPTP или протокол L2TP/IPSec с высоким уровнем защиты для создания каналов типа узел-в-узел между двумя брандмауэрами ISA Server/VPN-шлюзами, брандмауэр ISA 2004 позволяет использовать плохо защищенное соединение *с* применением туннельного режима протокола IPSec для подключения к VPN-шлюзам сторонних фирм.

> ПРИМЕЧАНИЕ Туннельный режим протокола IPSec поддерживается только для VPN-соединений конфигурации узел-в-узел. Клиент-серверные VPN-соединения удаленного доступа тем не менее используют только протоколы PPTP или L2TP/IPSec. Туннельный режим протокола IPSec уязвим для нескольких хорошо известных атак, а протокол L2TP/IPSec требует более строгой аутентификации и не подвержен этим атакам. Таким образом, если есть выбор, гораздо лучше применять набор протоколов L2TP/IPSec для VPN-соединений конфигурации узел-в-узел.

Публикация VPN-серверов по протоколу PPTP

Правила публикации сервера брандмауэра ISA Server 2000 разрешали публиковать серверы, требующие только TCP- или UDP-протоколов. Другими словами, невозможно было опубликовать серверы, которым необходимы другие протоколы, например, такие как ICMP (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет) или GRE (Generic Routing Encapsulation, протокол инкапсуляции маршрутизации). Это означало, что вы не могли опубликовать сервер по протоколу PPTP, потому что при этом использовался протокол GRE, который не относится к TCP- или UDP-протоколам. Единственной альтернативой для ISA Server 2000 было размещение таких серверов в сегменте сети периметра и применение пакетных фильтров для использования требуемых протоколов в соединениях с Интернетом и из него.

В брандмауэре ISA 2004 эта проблема решена. Теперь, используя брандмауэр ISA 2004, можно создавать правила публикации серверов для любого IP-протокола, включая правила публикации сервера для протокола GRE. Улучшенный PPTP-фильтр брандмауэра ISA 2004 разрешает входящий и исходящий доступ. Новые средства поддержки исходящего доступа означают возможность публикации по протоколу PPTP VPN -сервера, расположенного за брандмауэром ISA 2004.

Это свойство, конечно, будет очень популярно среди администраторов брандмауэра ISA Server 2000, которые раньше должны были создавать транзитные (pass-through) VPN-соединения для того, чтобы достичь внутренней сети.

Поддержка аутентификации секретным ключом в VPN-соединениях по протоколу IPSec

Public Key Infrastructure (PKI) (инфраструктура открытого ключа) необходима в среде с высокой степенью защищенности, для того чтобы на компьютерах, участвующих в VPN-соединении на базе протокола IPSec, можно было сформировать сертификаты компьютеров и пользователей. Цифровые сертификаты применяются для аутентификации компьютера при удаленном доступе по протоколу L2TP/IPSec и межШЛЮЗОВЫХ соединениях, а также соединениях с применением туннельного режима протокола IPSec. Сертификаты можно использовать также для подтверждения подлинности пользователей в соединениях по протоколам PPTP и L2TP/IPSec.

Установка PKI — не простая задача и у многих сетевых администраторов недостаточно времени и опыта для быстрой ее реализации. В этом случае можно иначе извлечь выгоду из уровня безопасности, обеспечиваемого VPN-соединениями, защищенными протоколом IPSec.

В брандмауэре ISA Server 2004, когда создаются VPN-соединения удаленного доступа и межшлюзовые VPN-соединения, можно использовать секретные ключи (pre-shared keys) вместо сертификатов. Все машины VPN-клиентов, на которых выполняется обновленн ое программное обеспечение VPN-клиента для протокола L2TP/IPSec, могут использовать секретный ключ для создания соединения удаленного доступа VPN-клиента по протоколу L2TP/IPSec с брандмауэром ISA 2004/VPN-сервером. VPN-шлюзы ОС Windows 2000 и Windows Server 2003 также можно настроить для применения секретного ключа и установки соединений узел-в-узел.

> ПРЕДУПРЕЖДЕНИЕ Секретные ключи (pre-shared key) для VPN-соединений, основанных на протоколе IPSec, следует применять с осторожностью. Сертификаты остаются более надежным методом аутентификации.

Имейте в виду, что отдельный сервер удаленного доступа может использовать только один секретный ключ (pre-shared key) для всех соединений по протоколу L2TP/IPSec, требующему секретный ключ для аутентификации. Необходимо предоставить один и тот же секретный ключ (pre-shared key) всем VPN-клиентам, соединяющимся по протоколу L2TP/IPSec с сервером удаленного доступа, который использует секретный ключ. До тех пор пока этот ключ не будет распространен в пределах профиля Менеджера соединений (Connection Manager, CMAK), каждый пользователь должен будет вручную вводить секретный ключ в набор установочных параметров программного обеспечения VPN-клиента. Это снижает безопасность применения протокола L2TP/IPSec в виртуальной частной сети и увеличивает вероятность ошибок пользователя и количество обращений за технической поддержкой, связанных с невозможностью подключений по протоколу L2TP /IPSec.

ПРЕДУПРЕЖДЕНИЕ Если секретный ключ (pre-shared key) на брандмауэре ISA 2004/VPN-сервере изменяется, клиент с введенным вручную секретным ключом не сможет установить соединение с помощью секретного ключа для протокола L2TP/IPSec до тех пор, пока не буден изменен ключ на машине клиента.

Несмотря на недостатки защиты, возможность с легкостью применять секретные ключи для создания защищенного соединения по протоколу L2TP/IPSec с брандмауэром ISA 2004/VPN-сервером наверняка станет популярной среди администраторов брандмауэра. Секретные ключи (pre-shared key) — идеальное средство «латания дыр», которое можно установить немедленно и использовать в процессе компоновки сертификатов, основанных на инфраструктуре открытого ключа (Public Key Infrastructure, PKI). Когда PKI сформирована, можно перевести клиентов с секретных ключей на аутентификацию высокого уровня защищенности с помощью сертификатов компьютера и пользователя.

Улучшенное назначение сервера имен для VPN-клиентов

VPN-сер вер/шлюз брандмауэра ISA Server 2000 был основа н на VPN- компонентах, включенных в его состав из сервиса маршрутизации и удаленного доступа (RRAS) ОС Windows 2000 и Windows Server 2003. VPN-сервисы RRAS позволяют назначить адреса сервера имен VPN-клиентам удаленного доступа. Правильное назначение сервера имен очень важно для VPN-клиентов, потому что некорректные назначения могут сделать VPN-клиент, не способным соединиться как с ресурсами внутренней сети, так и с ресурсами Интернета.

Возможен и другой вариант — конфигурирование объекта-соединения (connectoid) VPN-клиента с IP-адресами серверов WINS и DNS. Этот процесс можно автоматизировать, применяя модуль Connection Manager Administration Kit (CMAK) для распространения установочных параметров. Назначение сервера имен на клиентской стороне требует настройки вручную каждого объекта-соединения (connectoid) или распространения параметров установки с помощью CMAK.

Можно распространить установки разрешения имен с VPN-сервера. Но если вы хотите передать параметры установки VPN-клиенту с VPN-сервера брандмауэра ISA Server 2000, придется использовать одно из двух:

- адреса сервера имен, связанные с одним из сетевых интерфейсов на машине с брандмауэром ISA Server 2000;
- адреса сервера имен, предоставляемые VPN-клиенту протоколом DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) (это возможно, только если на брандмауэре ISA Server 2000/VPN-сервере установлен DHCP Relay Agent — агент ретрансляции DHCP).

Иногда может возникнуть желание назначить VPN-клиентам адреса сервера имен, не основанные на конфигурации сетевого интерфейса брандмауэра/VPN-сервера,

при этом, не устанавливая на брандмауэре DHCP Relay Agent (агент ретрансляции DHCP). К сожалению, в этом случае вы лишитесь преимуществ применения ISA Server 2000, поскольку он не поддерживает такой сценарий.

Хотим обрадовать: у брандмауэра ISA 2004/VPN-серВероВ нет этой проблемы, потому что они разрешают переопределять свои параметры установки сервера имен и предоставлять настраиваемые адреса сервера имен VPN-клиентам. Делается это с помощью консоли управления ISA Server 2004; нет необходимости переходить на консоль сервиса RRAS для создания настраиваемой конфигурации.

Мониторинг соединений VPN-клиентов

VPN-сервер ISA Server 2000 был ограничен возможностями ведения регистрационных журналов и мониторинга сетей VPN сервиса RRAS для ОС Windows 2000 и Windows Server 2003. Для определения того, кто подключился к сети с помощью VPN-соединения, требовалось просматривать текстовые файлы или записи базы данных. И это еще не все, поскольку брандмауэр не контролировал соединения VPN-клиентов удаленного доступа, не было централизованного механизма брандмауэра, позволяющего определить, к каким ресурсам обращались VPN-клиенты удаленного доступа.

В брандмауэре ISA Server 2004 эта проблема решается применением политики брандмауэра ко *всем* соединениям с брандмауэром, включая VPN-соединения. Можно воспользоваться программой просмотра журнала регистрации в режиме реального времени для проверки действующих соединений VPN-клиентов удаленного доступа и установить в ней фильтр для вывода только VPN-соединений. Если соединения регистрируются в машине базы данных MSDE (Microsoft Data Engine), можно запросить базу данных и вывести хронологический список VPN-соединений. В брандмауэре ISA 2004/VPN-серВере вы не только получаете полную информацию о том, кто подключился к брандмауэру ISA 2004/VPN, но и сведения о том, к каким ресурсам обращались эти пользователи и какие протоколы они использовали для подключения к ресурсам.

Например, можно задать критерии VPN-фильтрации в программе просмотра регистрационного журнала, если воспользоваться прямой регистрацией (live logging) и сохранить регистрации в файле. Применяя запись журналов регистрации в файл, нельзя запросить у программы просмотра регистрационных журналов брандмауэра ISA архивные данные. Но можно фильтровать и отслеживать в реальном времени VPN-соединения в программе просмотра регистрационного журнала. Кроме того, можно фильтровать VPN-соединения для отображения сеансов (Sessions view) или регистрации (Log view).

На консоли управления **Microsoft Internet** Security **and Acceleration Server** 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004) можно открыть вкладку Tasks (Задачи) панели задачи для узла **Virtual Private Networks (VPN)** (Виртуальные частные сети) и щелкнуть кнопкой мыши по ссылке, которая разре-

шает отслеживать соединения VPN-клиентов и шлюзов. Если выбран этот вариант, убедитесь, что сделана копия параметров фильтрации по умолчанию, для того чтобы можно было вернуться к базовой конфигурации фильтрации.

Эти функциональные возможности регистрации и мониторинга представляют собой существенное усовершенствование по сравнению с аналогичными функциями, включенными в ISA Server 2000 и автономными VPN сервиса маршрутизации и удаленного доступа, входящими в состав Windows 2000 и Windows Server 2003.

Создание VPN-сервера удаленного доступа по протоколу PPTP

VPN-сервер удаленного доступа принимает VPN-вызовы от компьютеров VPN-клиентов. Он разрешает *отдельным компьютерам клиента и пользователям* получать доступ к сетевым ресурсам после того, как установлено VPN-соединение. VPN-шлюз, напротив, соединяет целые сети друг с другом и разрешает многочисленным хостам в каждой сети соединяться с другими сетями с помощью VPN-канала типа узел-в-узел.

Для соединения с VPN-сервером можно использовать любое клиентское программное обеспечение, поддерживающее протоколы PPTP или L2TP/IPSec. Идеальным выбором может служить VPN-клиент Microsoft, входящий в состав всех версий ОС Windows. Но если вы хотите использовать протокол L2TP/IPSec с секретными ключами (pre-shared keys), обходящий NAT (NAT traversal), следует загрузить и установить обновленный клиент L2TP/IPSec с сайта загрузки корпорации Microsoft. Мы обсудим подробности получения этого программного обеспечения позже в этой главе.

В этом разделе мы рассмотрим процедуры, необходимые для создания на брандмауэре ISA VPN-сервера удаленного доступа по протоколу PPTP. Выполним следующие конкретные шаги:

- активизируем компонент VPN-сервера брандмауэра ISA;
- создадим правило доступа, разрешающее VPN-клиентам доступ к внутренней сети;
- разрешим удаленный доступ по телефонной линии (Dial-in) для учетных записей пользователей VPN;
- протестируем VPN-соединение по протоколу PPTP.

Включение VPN-сервера

Необходимо включить компонент VPN-сервера, так как он по умолчанию отключен. Первый шаг — активизация функции VPN-сервера и конфигурирование его компонентов. Делается это на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004), а *не* на консоли сервиса RRAS.

Большая часть проблем конфигурации VPN брандмауэра ISA, с которыми мы сталкивались, была связана с применением неопытными администраторами брандмауэра ISA консоли сервиса RRAS (Routing and Remote Access Services, сервис маршрутизации и удаленного доступа) для настройки VPN-компонентов. Несмотря на то, что возможны ситуации, в которых нам понадобится эта консоль, подавляющая часть конфигурирования VPN-сервера брандмауэра ISA и VPN-шлюза выполняется на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа *к* сети Интернет 2004).

ПРЕДУПРЕЖДЕНИЕ Лучше выполнить большую часть конфигурирования VPN-сервера и шлюза на консоли управления Microsoft Internet Security and Acceleration Server 2004, потому что установочные параметры брандмауэра ISA перезапишут большую часть установок, сделанных на консоли RRAS. Для получения дополнительной информации об этой проблеме проверьте ссылку Interoperability of Routing and Remote Access and Internet Security and Acceleration Server 2004 (Возможность взаимодействия сервиса маршрутизации и удаленного доступа и сервера защищенного быстрого доступа к сети Интернет 2004) по адресу http://support.microsoft.com/defaurt.aspx7scicb kb;en-us;838374.

Выполните следующие шаги для включения и настройки VPN-сервера ISA 2004.

1. Откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети).
2. Щелкните мышью вкладку **Tasks** (Задачи) на панели задачи. Щелкните кнопкой мыши ссылку **Enable VPN Client Access** (Разрешить доступ VPN-клиентов) (рис. 9.1).

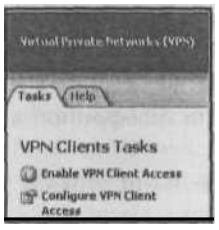


Рис. 9.1. Ссылка Enable VPN Client Access (Разрешить доступ VPN-клиентов)

3. Щелкните мышью кнопку **Apply** (Применить) для сохранения измен ени й и обновления политики брандмауэра.
4. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
5. На вкладке **Tasks** (Задачи) щелкните кнопкой мыши ссылку **Configure VPN Client Access** (Настроить доступ VPN-клиента).

6. На вкладке **General** (Общие) (рис. 9.2) в диалоговом окне **VPN Clients Properties** (Свойства VPN-клиентов) измените значение параметра **Maximum number of VPN clients allowed** (Максимальное число разрешенных VPN-клиентов) с 5 на 10. Версия Standard Edition брандмауэра ISA поддерживает до 1000 параллельных VPN-соединений. Это жестко заданный предел, и он не меняется независимо от количества VPN-соединений, поддерживаемых операционной **системой** Windows, в которой установлен брандмауэр ISA. У версии Enterprise edition брандмауэра ISA нет жестко заданного лимита и количество поддерживаемых VPN-соединений определяется базовой операционной системой. Точно число неизвестно, но если брандмауэр ISA установлен в ОС Windows Server 2003 версии Enterprise, вы можете создать к брандмауэру ISA 1б 000 VPN-подключений по протоколу PPTP и 30 000 — по протоколу L2TP/IPSec.

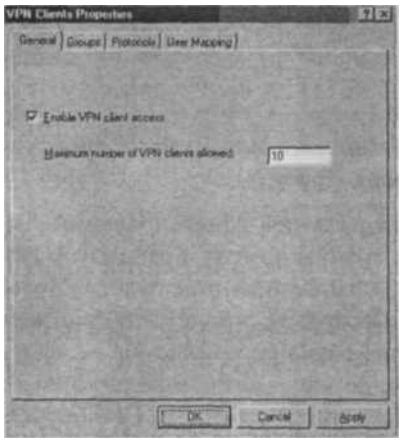


Рис. 9.2. Вкладка **General** (Общие)

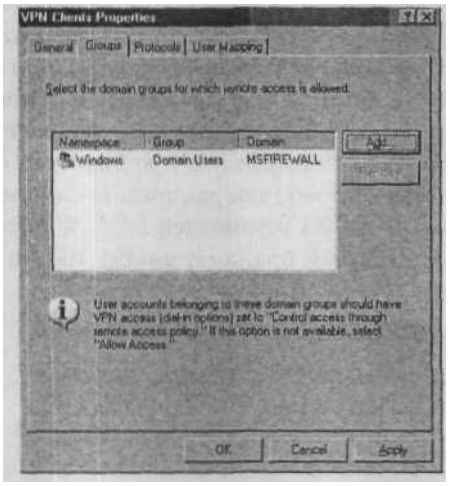
Убедитесь, что имеется количество IP-адресов для VPN-клиентов, по меньшей мере, равное числу, указанному в текстовом поле **Maximum number of VPN clients allowed** (Максимальное число разрешенных VPN-клиентов). Определите количество VPN-клиентов, которые необходимо соединить с брандмауэром ISA, а затем добавьте единицу для самого брандмауэра ISA. Это и будет число, которое нужно ввести в **данное** текстовое поле.

7. Щелкните кнопкой мыши вкладку **Groups** (Группы) (рис. 9-3). На этой вкладке щелкните мышью кнопку **Add** (Добавить).

8. В диалоговом окне **Select Groups** (Выберите группы) щелкните мышью кнопку **Locations** (Местонахождения). В диалоговом окне **Locations** (Местонахождения) щелкните кнопкой мыши адрес **msfirewall.org,** а затем кнопку ОК. В
" диалоговом окне **Select Groups** (Выберите группы) в текстовое поле **Enter the object names to select** (Введите имена выбранных объектов) введите **Domain Users** (Пользователи домена). Щелкните мышью кнопку **Check Names**

Рис. 9.3. Вкладка Groups (Группы)

(Проверить имена). Как только имя группы будет найдено в базе данных Active Directory, оно будет подчеркнуто. Щелкните мышью кнопку ОК.



Можно ввести локальные группы, сформированные на машине с брандмауэром ISA, или использовать группы домена. Брандмауэр ISA будет применять только глобальные группы (Global Groups) и не будет использовать локальные группы домена (Domain Local Groups). Настроить глобальные группы на вкладке **Groups** (Группы) можно, только если брандмауэр ISA — член домена. Если брандмауэр ISA не является членом домена, можно использовать подтверждение подлинности RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя) для разрешения глобальным группам домена обращаться к VPN-серверу брандмауэра ISA. Мы подробно обсудим настройку RADI US-аутентификации для VPN-соединен и й удаленного доступа позже в этой главе.

ВНИМАНИЕ! Домен должен быть установлен *в* ОС Windows 2000 Native или в более новых ОС для того, чтобы управлять доступом с помощью политики удаленного доступа (Control access through remote access policy) либо пользователи/группы должны быть созданы собственным диспетчером учетных записей безопасности SAM (Security Accounts Manager) брандмауэра ISA. Кроме того, следует иметь *в* виду, что когда вы управляете доступом к VPN-серверу с помощью группы домена (или локальной), у пользователей должно быть разрешение для доступа. Мы обсудим этот вопрос позже в этой главе. 10. Щелкните кнопкой мыши вкладку Protocols (Протоколы). На этой нкладке установите флажок Enable PPTP (Разрешить PPTP) (рис. 9.4).

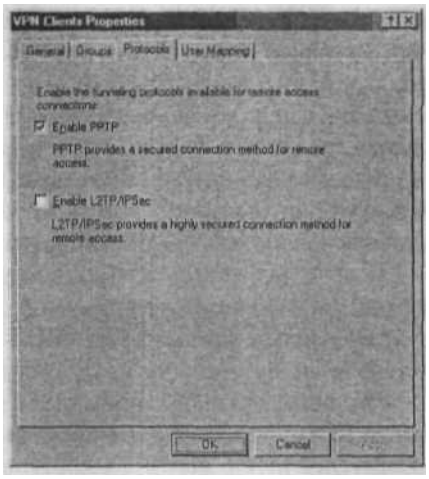


Рис. 9.4. Вкладка **Protocols** (Протоколы)

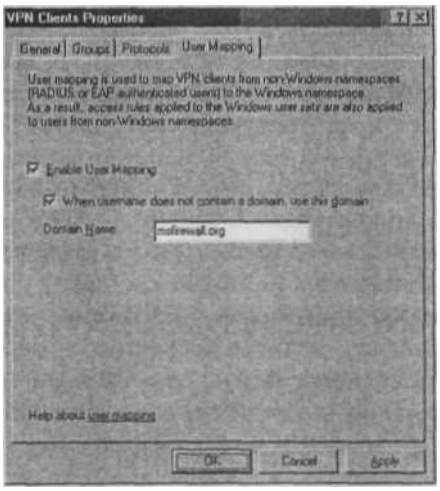


Рис. 9.5. Вкладка **User Mapping** (Отображение пользователя)

11. Щелкните кнопкой мыши вкладку **User Mapping** (Отображение пользователя) (рис. 9.5). Установите флажок **Enable** User **Mapping** (Разрешить отображение пользователей) и флажок **When username does not contain a domain, use this domain** (Если имя пользователя не содержит имя домена, использовать данный домен). Введите имя **msfirewall.org** в текстовое поле **Domain Name** (Имя домена). Имейте в виду, что эти установки будут применяться при использовании аутентификации RADIUS/EAR Они игнорируются, когда используется аутентификация Windows (например, когда машина с брандмауэром ISA 2004 принадлежит домену и пользователь явно вводит верительные данные домена). Щелк-

ните мышью кнопки **Apply** (Применить) и ОК. Вы увидите диалоговое окно **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004), информирующее вас о том, что необходимо перезапустить компьютер для ввода в действие установленных параметров. Если так, щелкните мышью кнопку ОК в диалоговом окне. Функция отображения пользователей немного непонятна, и в настоящее время нет хорошей документации о функционировании отображения пользователей с системой RADIUS. Действительно, вы можете запретить все VPN-соединения с вашим брандмауэром ISA, если разрешите отображение пользователей и *не* сделаете брандмауэр ISA членом домена. Исходя из этого можно утверждать, что отображение пользователей может применяться, когда брандмауэр ISA является членом вашего домена и вы применяете RADIUS-аутентификацию для подтверждения подлинности пользователей, принадлежащих разным доменам. В этом случае вы можете разрешить отображение пользователей для создания основанного на пользователе/группе контроля доступа пользователей, зарегистрировавшихся с помощью системы RADIUS, и отображения **учетных** записей пользователей в учетные записи домена, которому принадлежит брандмауэр) ISA, а затем формирования правил доступа с использованием этих **учетных** записей, создав **User Sets** (Наборы пользователей) на брандмауэре ISA. Информацию о **User Mapping** (Отображение пользователей) и о том, как оно работает и не работает, можно получить из статьи «Using RADIUS Authentication with the ISA Firewall's VPN Server» (Применение RADIUS-аутентификации на VPN-сервере брандмауэра ISA) по адресу http://isaserver.org/articles/2004vpnradius.html. Мы будем обсуждать эту тему более подробно позже в этой главе и рассмотрим, как применять основанный на пользователе/группе контроль доступа VPN-клиентов, зарегистрировавшихся с помощью системы RADIUS. Одна область, в которой применение отображения пользователей вполне понятно и, как мы убедились, работает корректно, — использование аутентификации **сертификатами** пользователей по протоколу EAP (Extensible Authentication Protocol, наращиваемый протокол аутентификации). Мы подробно рассмотрим, как функционирует отображение пользователей совместно с аутентификацией сертификатами пользователей по протоколу EAP позже в этой главе.

12. На вкладке **Tasks** (Задачи) щелкните кнопкой мыши строку **Select Access Networks** (Выбрать сети доступа).
13- В диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства виртуальных частных сетей) (рис. 9.6) щелкните кнопкой мыши вкладку **Access Networks** (Сети доступа). Обратите внимание на то, что установлен флажок **External** (Внешняя). Это означает, что внешний интерфейс ожидает входящие соединения от VPN-клиентов. Если вы хотите внутренних пользователей подключить к брандмауэру ISA, выберите флажок **Internal** (Внутренняя) Есть также варианты, разрешающие VPN-подключения из **All Networks (and Local Host Network)** (Все сети, и сеть локального хоста) **и All Protected Networks** (Все защищенные сети).

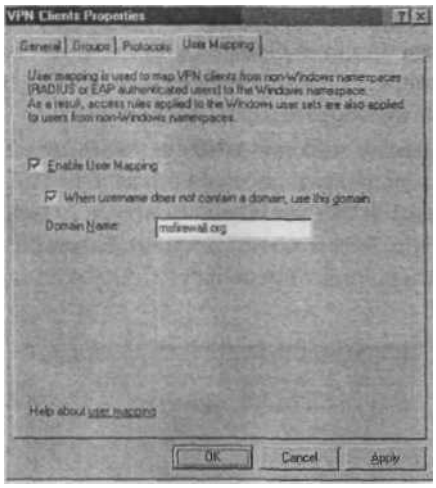


Рис. Э.6. Выбор и настройка параметров сетей доступа

Возможность выбора VPN-соединений из разных сетей может быть полезна, если у вас есть небезопасные сети, расположенные за брандмауэром ISA. Предположим, что у вас есть трехадаптерный брандмауэр ISA, имеющий внешний интерфейс, внутренний интерфейс и интерфейс WLAN (Wireless Local Area Network, беспроводная локальная сеть). Интерфейс WLAN применяется для пользователей портативных компьютеров (laptop), которые не управляются вашей организацией. Вы можете потребовать также и от пользователей управляемых компьютеров использовать сегмент WLAN, когда они приносят портативные компьютеры, которые перемещаются между корпоративной сетью и сетями, не заслуживающими доверия.

Вы настраиваете правила доступа на брандмауэре ISA, запрещающие соединения из сегмента WLAN. Но ш формируете правила доступа, разрешающие VPN-соединения с интерфейсом WLAN для подключения к ресурсам корпоративной внутренней сети. В этом случае никто из пользователей, соединяющихся с сегментом WLAN, не способен получить доступ к ресурсам в корпоративной внутренней сети, за исключением тех корпоративных пользователей, кто может установить VPN-соединение с интерфейсом WLAN на брандмауэре ISA и предоставить соответствующие верительные данные для завершения VPN-соединения. Другой сценарий, в котором вы можете разрешить VPN-соединение с брандмауэром ISA, — **функционирование** брандмауэра ISA как внешнего (front-end) брандмауэра. В этом случае вы, возможно, не захотите разрешать прямые соединения по протоколу RDP (Remote Desktop Protocol, протокол удаленного рабочего стола) или удаленные соединения MMC с брандмауэром ISA. У вас есть возможность разрешить RDP-соединения *только от VPN-клиентов* и затем разрешить VPN-клиентам доступ по протоколу RDP к сети локального хоста (Local

Host Network). В этом случае пользователь должен установить защищенное VPN-соединение с внешним брандмауэром ISA, прежде чем может быть установлено RDP-соединение. Хостам, соединяющимся с помощью любых других средств, запрещается доступ к RDP-протоколам. Отлично!

14. Щелкните кнопкой мыши вкладку **Address Assignment** (Назначение адреса) (рис. 9-7). Выберите в раскрывающемся списке **Use the following network to obtain DHCP, DNS and WINS services** (Использовать следующую сеть для получения сервисов DHCP, DNS и WINS) элемент **Internal** (Внутренняя). Это важная установка, поскольку она определяет сеть, в которой осуществляется доступ к сервису DHCP.

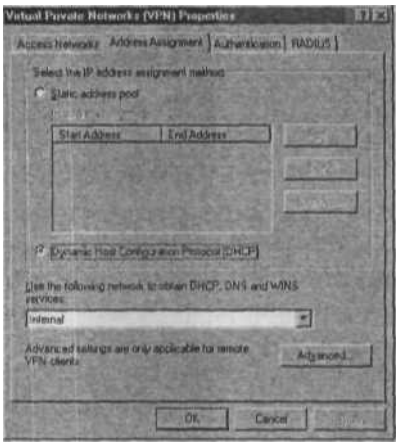


Рис. 9.7. Вкладка Address Assignment (Назначение адреса)

Заметьте, что это не единственно возможный выбор. Можно выбрать любой из адаптеров брандмауэра ISA в списке **Use the following network to obtain DHCP, DNS and WINS services** (Использовать следующую сеть для получения сервисов DHCP, DNS и WINS). Ключевой вывод заключается в том, что вы выбираете адаптер, на котором есть корректная информация сервера имен и наиболее вероятный кандидат — внутренний интерфейс брандмауэра ISA. У вас также есть возможность использовать **Static address pool** (Пул статических адресов) для назначения адресов VPN-клиентам. Проблема применения пула статических адресов заключается в том, что при назначении адресов *из подсети* (адреса в сети с тем же сетевым идентификатором (ID), что и один из интерфейсов брандмауэра ISA) необходимо удалять эти адреса из сети, к которой подсоединен брандмауэр ISA.

Предположим, что у брандмауэра ISA есть два сетевых интерфейса: внешний и внутренний. Внутренний интерфейс соединен с вашей внутренней сетью по умолчанию и ее сетевой идентификатор — 192.168.1.0/24. Если вы хотите назначить адреса VPN-клиентам из диапазона адресов внутренней сети, используя пул статических адресов, например 192.168.1.200/211 (всего 10 адресов), вам

нужно будет вручную удалить эти адреса из определения внутренней сети, прежде чем вы сможете создать из них пул статических адресов. Если вы попытаетесь создать пул статических адресов с сохранением этих адресов *в подсети (on subnet),* то увидите сообщение об ошибке, показанное на рис. 9.8.

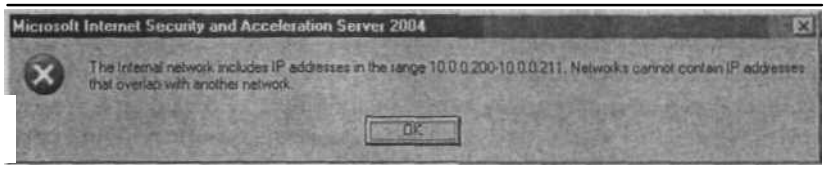


Рис. 9.8. Диалоговое окно с сетевым предупреждением

Можно назначить VPN-клиентам адреса сервера имен, не зависящие от конфигурации сервера имен и любого интерфейса брандмауэра ISA. Щелкните мышью кнопку **Advanced** (Дополнительно) и увидите диалоговое окно **Name Resolution** (Разрешение имен). По умолчанию установлены переключатели **Obtain DNS server addresses using DHCP configuration** (Получать адреса DNS-сервера с помощью DHCP-конфигурации) и **Obtain WINS server addresses using DHCP configuration** (Получать адреса сервера WINS с помощью DHCP-конфигурации). Конечно, невозможно получить параметры **DHCP** (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) для VPN-клиентов, пока на брандмауэре ISA не установлен и не настроен **DHCP Relay Agent** (агент ретрансляции DHCP). Сервис *RRAS* брандмауэра ISA будет получать только блоки IP-адресов для VPN-клиентов, а не варианты DHCP. Мы обсудим эту проблему более подробно позже в этой главе.

Если вы хотите избежать установки агента **DHCP Relay Agent,** у вас все равно есть возможность предоставить VPN-клиентам адреса серверов DNS и WINS, установив переключатели Use **the following DNS server addresses** (Использовать следующие адреса DNS-сервера) и Use **the following WINS server addresses** (Использовать следующие адреса сервера WINS) (рис. 9.9).

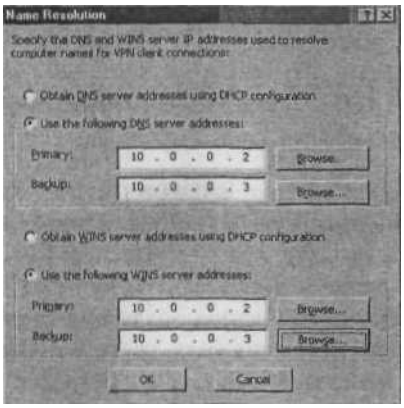


Рис. 9.9. Диалоговое окно **Name** Resolution (Разрешение имен)

15. Щелкните кнопкой **мыши** в **кл** г ад ку **Authentication (Аутентификация)** (рис. 9-Ю). Отметьте, что установлен только флажок **Microsoft encrypted authentication version 2 (MS-CHAPv2)** (Шифрованная аутентификация версии 2, Протокол проверки подлинности запроса-подтверждения Microsoft версии 2). Обратите внимание на флажок **Allow custom IPSec policy for L2TP connection** (Разрешить настраиваемую IPSec-политику для соединения по протоколу L2TP). Если вы не хотите создавать инфраструктуру открытого ключа (PKI) или вы создаете ее, но процесс не завершен, можно установить этот флажок и ввести **pre-shared** (секретный) ключ. Следует также разрешить применение секретного ключа настраиваемой IPSec-политики, если вы хотите создать VPN-соединение конфигурации узел-в-узел с помощью секретных (pre-shared) ключей. Мы подробнее обсудим эту проблему позже в этой главе. Для обеспечения самого высокого уровня безопасности аутентификации установите флажок **Extensible authentication protocol (EAP) with smart card or other certificate** (Наращиваемый протокол аутентификации, (EAP) с помощью смарт-карты или другого сертификата). Позже в этой главе мы рассмотрим, как конфигурировать брандмауэр ISA и VPN-клиенты для подтверждения подлинности на брандмауэре ISA с помощью сертификатов пользователя (User Certificates).

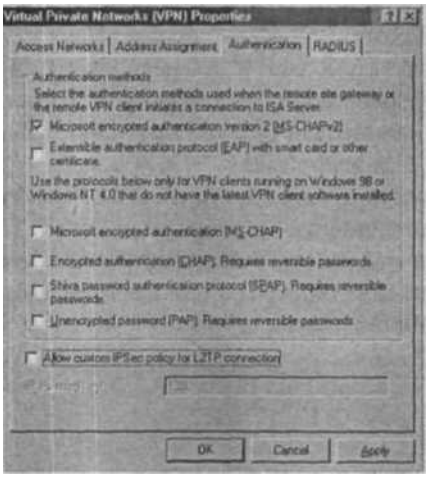
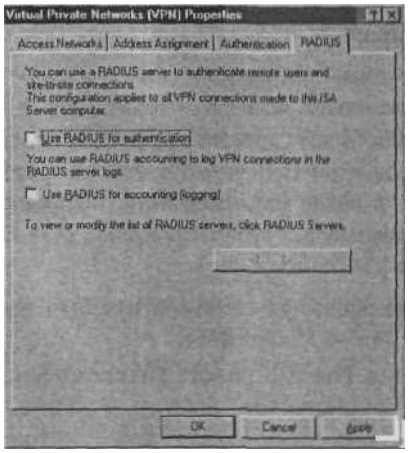


Рис. 9.10. Вкладка Authentication (Аутентификация)

16. Щелкните кнопкой мыши вкладку **RADIUS** (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя). На этой вкладке можно настроить VPN-сервер брандмауэра ISA 2004 для применения аутентификации VPN-пользователей с помощью сервиса RADIUS. Преимущество подтверждения подлинности средствами RADIUS з а к л ю **чается** в том, что можно привлечь базу данных пользователей службы Active Directory (или других каталогов) для аутентификации пользователей без обяза-

тельного членства в домене брандмауэра ISA. Мы подробно рассмотрим способы конфигурирования сервиса RADIUS для поддержки аутентификации VPN-пользователей позже в этой главе.



JJ

Рис. 9.11. Окно Virtual Private Networks (VPN) Properties (Свойства виртуальных частных сетей)

17. В диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства вир туальных частных сетей) (рис. 911) щелкните мышью кнопку **Apply** (Приме нить) и затем кнопку ОК.
18. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
19. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию). 20.

Перезапустите машину с брандмауэром ISA.

После перезагрузки брандмауэр ISA получит блок IP-адресов от DHCP-сервера во внутренней сети. Обратите внимание на то, что все промежуточные маршрутизаторы рабочей сети, в которой DHCP-сервер расположен в сетевом сегменте, удаленном от брандмауэра ISA 2004, должны иметь ретранслятор BOOTP (Bootstrap Protocol) или DHCP, включенный так, чтобы DHCP-запросы от брандмауэра могли достичь удаленных DHCP-серверов.

Создание правила доступа, предоставляющего VPN-клиентам доступ к разрешенным ресурсам

Брандмауэр ISA после перезапуска компьютера сможет принимать входящие VPN-соединения. Но VPN-клиенты не получат доступ к ресурсам, поскольку нет правил доступа, разрешающих им получать что-либо. Следует создать правила доступа,

разрешающие членам сети VPN-клиентов обращаться к ресурсам, которые вы захотите им предоставить. Этот вариант значительно отличается от других комбинированных решений брандмауэра/VPN-сервера, в которых применяются отслеживающие состояние соединений фильтрация и проверка на прикладном уровне всех соединений VPN-клиентов.

В следующем примере создается правило доступа, разрешающее любому трафику проходить из сети VPN-клиентов во внутреннюю сеть. В производственной среде вам пришлось бы создавать более строгие правила доступа, для того чтобы пользователи сети VPN-клиентов получали доступ только к тем ресурсам, которые им необходимы. Позже в этой главе мы продемонстрируем, как можно сконфигурировать более строгую политику доступа с помощью основанного на пользователе/группе контроле доступа VPN-клиентов.

Выполните следующие шаги для создания правила доступа, обеспечивающего неограниченный доступ для VPN-клиентов.

1. На консоли управления **The Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). Щелкните правой кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), укажите левой кнопкой мыши команду **New** (Новое) и затем **Access Rule** (Правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В данном примере — **VPN Client to Internal.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите вариант **All outbound protocols** (Все исходящие протоколы) в списке **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Next** (Далее).
5. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) (рис. 912) щелкните кнопкой мыши папку **Networks** (Сети) и дважды щелкните мышью узел **VPN Clients** (VPN-клиенты). Щелкните мышью кнопку **Close** (Закрыть).
6. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).
7. **На** странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети) и дважды щелкните мышью узел **Internal** (Внутренняя). Щелкните мышью кнопку **Close** (Закрыть).

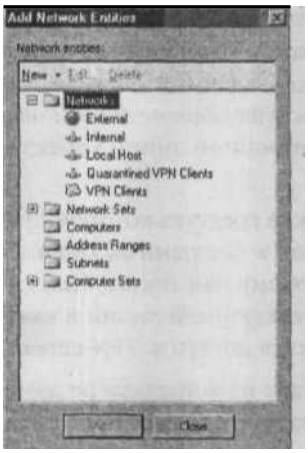


Рис. 9.12. Диалоговое окно Add Network Entities (Добавить сетевые объекты)

8. На странице User Sets (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
9 Щелкните кнопку **Finish** (Готово) на странице Completing the New Access **Rule Wizard** (Завершение мастера создания нового правила).
10. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
11. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию). Политика VPN-клиента теперь отражена в верхнем правиле доступа, приведенном в списке политики доступа (рис. 9-13).

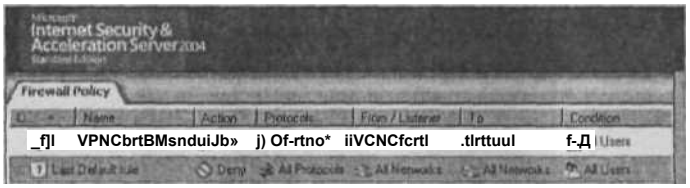


Рис. 9.13. Политика VPN-клиента

С этого момента VPN-клиенты, успешно подтвердившие свою подлинность и имеющие разрешение на соединение по телефонной линии, имеют возможность доступа ко всем ресурсам внутренней сети с помощью любого протокола.

Разрешение удаленного доступа по телефонной линии

В доменах Active Directory, находящихся в неосновном режиме (non-native mode), для всех учетных записей пользователей по умолчанию удаленный доступ по телефонной линии (dial-in) запрещен. Вы должны разрешить такой доступ, ос новы ва-

ясь на *учетных записях* для этих доменов Active Directory, находящихся в неосновном режиме. Напротив, в доменах Active Directory, находящихся в основном режиме (native mode), по умолчанию удаленный доступ по телефонной линии управляется политикой удаленного доступа *(Remote Access Policy).* В доменах ОС Windows NT 4.0 удаленный доступ по телефонной линии управляется посредством учетных записей пользователя.

В лаборатории, технические средства которой применялись для написания этой книги, служба Active Directory в смешанном режиме (mixed mode) установлена в ОС Windows Server 2003, поэтому нам понадобилось вручную изменить установки для удаленного доступа по телефонной линии в каждой учетной записи пользователя домена, которой требуется доступ к VPN-серверу.

Выполните следующие шаги на контроллере домена для разрешения удаленного доступа по телефонной линии для учетной записи **Administrator.**

1. Щелкните мышью кнопку **Start** (Пуск) и строку **Administrative Tools** (Адми нистрирование). Щелкните мышью оснастку **Active Directory Users and Compu ters** (Active Directory — пользователи и компьютеры).
2. В оснастке **Active Directory Users and Computers** (Active Directory' — пользо ватели и компьютеры) щелкните мышью узел **Users** (Пользователи) на левой панели. Дважды щелкните кнопкой мыши учетную запись **Administrator** на правой панели оснастки.
3. Щелкните кнопкой мыши вкладку **Dial-in** (Соединение по телефонной линии). В области **Remote Access Permission (Dial-in or VPN)** (Разрешение удален ного доступа, по модему или через сеть VPN) выберите переключатель **Allow access** (Разрешить доступ) **(рис.** 9-14). Щелкните мышью кнопку **Apply** (Приме нить) и затем кнопку ОК.

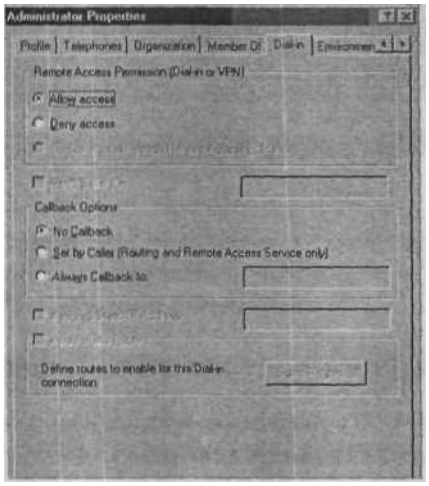


Рис. 9.14. Вкладка Dial-in (Соединение по телефонной линии) учетной записи

4. Закройте оснастку **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).

Другой вариант — создать группы на самом брандмауэре ISA и поместить их в группы. Этот метод позволит применить установочные параметры по умолчанию в учетных записях пользователей, созданных на брандмауэре, для которых по умолчанию выбран для удаленного доступа по телефонной линии **Control access via Remote Access Policy** (Контроль доступа с помощью политики удаленного доступа).

Несмотря на то, что этот вариант не слишком хорошо регулируется, он вполне жизнеспособен в тех организациях, у которых ограниченное количество VPN-пользователей и которые не хотят применять подтверждения подлинности с помощью системы RADIUS или не имеют RADIUS-сервер а для использования.

Выполните следующие шаги для создания группы пользователей, имеющих доступ к VPN-серверу брандмауэра ISA.

1. На рабочем столе брандмауэра ISA щелкните правой кнопкой пиктограмму **My Computer** (Мой компьютер) и щелкните левой кнопкой мыши команду **Manage** (Управление).
2. На консоли **Computer Management** (Управление компьютера) раскройте узел **System Tools** (Служебные программы) и затем узел **Local Users and Groups** (Ло кальные пользователи и группы). Щелкните правой кнопкой мыши папку **Groups** (Группы) и левой кнопкой мыши щелкните **команду New Group** (Новая группа).
3. В диалоговом **окне** New **Group** (Новая группа) введите имя группы в текстовое поле **Group Name** (Имя группы). В данном примере мы назовем группу **VPN Users.** Щелкните мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Select: users** (Выбор: пользователи) щелкните мышью кнопку **Advanced** (Дополнительно).
5. В диалоговом окне **Select: users** (Выбор: пользователи) выберите пользовате лей или группы, которые вы хотите сделать членами группы **VPN Users.** В этом примере мы выберем **Authenticated Users** (Аутентифицированные пользова тели). Щелкните мышью кнопку ОК.
6. Щелкните мышью кнопку ОК в диалоговом окне **Select: users** (Выбор: пользо ватели).
7. Щелкните мышью кнопку **Create** (Создать), а затем кнопку **Close** (Закрыть).

Теперь настроим компонент VPN-сервера брандмауэра ISA для разрешения доступа членам группы **VPN Users.**

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networking (VPN)** (Виртуальные частные сети). Щелкните кнопкой мыши строку **Configure VPN Client Access** (Конфигурировать доступ VPN-клиента) на вкладке **Tasks** (Задачи) на панели задачи.

2. В диалоговом окне **VPN Clients Properties** (Свойства VPN-клиентов) щелкни те мышью кнопку **Add** (Добавить).
3. В диалоговом окне **Select Groups** (Выберите группы) введите **VPN Users** в тек стовое поле **Enter the object name to select** (Введите имя выбранного объек та) и щелкните мышью кнопку **Check Names** (Проверить имена). Найденное имя группы будет подчеркнуто. Щелкните мышью кнопку OK.
   В данном примере мы ввели локальную группу VPN Users на вкладке **Groups** (Группы), потому что VPN-доступ может контролироваться с помощью режима **Control access through Remote Access Policy** (Контроль доступа с помощью политики удаленного доступа), установленного для учетных записей пользователей в локальном диспетчере SAM (Security Accounts Manager, диспетчер учетных записей безопасности) брандмауэра ISA. Вы также можете ввести пользователей и группы домена (если брандмауэр ISA является членом домена пользователей), если домен поддерживает удаленный доступ по телефонной линии с помощью политики удаленного доступа. Мы поговорим более подробно о пользователях и группах домена и политике удаленного доступа позже в этой главе. На рис. 915 показано управление разрешением политики удаленного доступа.

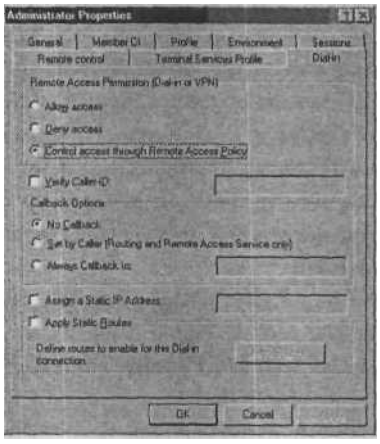


Рис. 9.15. Управление разрешением политики удаленного доступа

4. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK в диалоговом окне **VPN Client Properties** (Свойства VPN-клиентов) (рис. 916).
5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

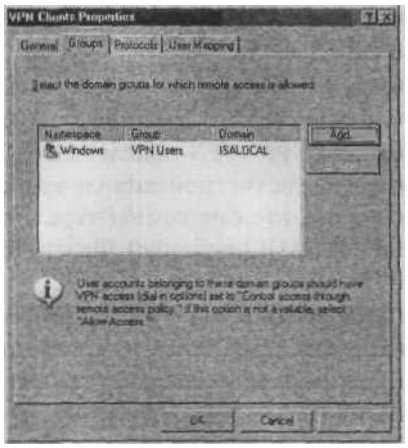


Рис. 9.16. Вкладка Groups (Группы)

Тестирование VPN-соединения по протоколу PPTP

Теперь VPN-сервер брандмауэра ISA 2004 готов для приема соединений от VPN-клиентов. Установите пиктограмму (connectoid) VPN-соеди нения на вашем VPN-клиенте и затем установите VPN-соединение с брандмауэром ISA. В тестовой лаборатории при подготовке этой книги мы использовали клиент под управлением ОС Windows XP с установленным Service Pack 1.

Выполните следующие шаги для тестирования VPN-сервера.

1. На машине внешнего клиента с ОС Windows XP щелкните правой кнопкой мыши пиктограмму **My Network Places** (Сетевое окружение) на рабочем столе и вы берите команду **Properties** (Свойства).
2. Дважды щелкните кнопкой мыши строку **New Connection Wizard** (Мастер новых подключений) в окне **Network Connections** (Сетевые под ключе ния).
3. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the New Con nection Wizard** (Вас приветствует мастер новых подключений).
4. На странице **Network Connection Type** (Тип сетевого подключения) выбери те переключатель **Connect to a private network at my workplace** (Подклю чить к сети на рабочем месте) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Network Connection** (Сетевое подключение) выберите переклю чатель **Virtual Private Network connection** (Подключение к виртуальной частной сети) и щелкните мышью кнопку **Next** (Далее).
6. На странице **Connection Name** (Имя подключения) введите **VPN** в текстовое поле **Company Name** (Организация) и щелкните мышью кнопку **Next** (Далее).
7. На странице **VPN Server Selection** (Выбор VPN-сервера) введите IP-адрес на внешнем интерфейсе брандмауэра ISA (вданном примере — 192.168.1,70) втек-

стовое поле **Host name or IP address** (Имя компьютера или IP-адрес). Щелкните мышью кнопку **Next** (Далее).

8. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Connection Wizard** (Завершение Мастера новых подключений).
9. В диалоговом окне **Connect VPN** (VPN-подключение) введите имя пользователя **Administrator** и пароль для учетной записи администратора (если брандмауэр ISA — член домена, введите имя компьютера или имя домена перед именем пользователя в формате NAME\username). Щелкните мышью кнопку **Connect** (Подключиться).
10. VPN-клиент устанавливает соединение с VPN-сервером брандмауэра ISA 2004. Щелкните мышью кнопку ОК в диалоговом окне **Connection Complete** (Соединение установлено), информирующем об установке соединения.
11. Дважды щелкните кнопкой мыши пиктограмму соединения на системной панели задач, а затем щелкните мышью вкладку **Details** (Сведения). Вы увидите шифрование **MPPE 128** (Microsoft Point-to-Point Encryption), применяемое для защиты данных, и IP-адрес, назначенный VPN-клиенту (рис. 9.17). Щелкните мышью кнопку **Close** (Закрыть).

Рис. 9.17. Параметры соединения по протоколу PPTP

12. Если вы используете лабораторную установку, описанную в этой книге, щелкните мышью кнопку **Start** (Пуск), а затем команду **Run** (Выполнить). В диалоговом окне **Run** введите **\\EXCHANGE2003BE** в текстовое поле **Open** (Открыть) *к* щелкните мышью кнопку ОК. Появятся ресурсы, совместно используемые (shares) на компьютере контроллера домена. Закройте окна, отображающие содержимое контроллера домена. Обратите внимание на то, что мы могли использовать имя без доменного суффикса (single label name) для соединения с контроллером домена, потому что брандмауэр ISA назначил VPN-клиенту адрес сервера WINS. Имя без доменного суффикса сработало бы *и* в случае DNS-запроса, если бы машина VPN-клиента была настроена на полное определение имен без доменного суффикса с помощью корректного имени домена.

13. Щелкните правой кнопкой мыши по пиктограмме соединения на панели задач и щелкните левой кнопкой мыши кнопку **Disconnect** (Отключить).

Создание VPN-сервера удаленного доступа по протоколу L2TP/IPSec

В предыдущем разделе обсуждались процедуры, необходимые для включения и конфигурирования компонента VPN-сервера брандмауэра ISA, разрешающего удаленные соединения VPN-клиентов по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол). В следующем разделе мы сформируем конфигурацию, созданную нами в предыдущем разделе, и настроим брандмауэр ISA для поддержки удаленного соединения VPN-клиента по протоколу L2TP/IPSec.

Мы выполним следующие процедуры для разрешения соединения удаленного доступа VPN-клиентов с брандмауэром ISA:

- обеспечение сертификатами брандмауэра ISA 2004 и VPN-клиентов;
- тестирование VPN-соединения по протоколу L2TP/IPSec;
- отслеживание соединений VPN-клиентов.

Обеспечение сертификатами брандмауэра ISA 2004 и VPN-клиентов

Можно существенно повысить уровень безопасности VPN-соединений, используя для них протокол L2TP/IPSec. Протокол шифрования IPSec (протокол безопасности IP) обладает рядом преимуществ в обеспечении безопасности по сравнению с протоколом Microsoft Point-to-Point Encryption (MPPE) (Сквозной протокол шифрования Microsoft), применяемым в защищенных PPTP-соед и нениях. Если брандмауэр ISA поддерживает использование секретного ключа (pre-shared key) для процесса шифрования в протоколе IPSec, этот способ имеет низкий уровень безопасности и его следует избегать.

> **СОВЕТ** Несмотря на то, что протоколы PPTP и MPPE являются защищенными протоколами, которые могут применять организации, не желающие использовать PKI (Public Key Infrastructure, инфраструктура открытого ключа) и L2TP/IPSec (Layer Two Tunneling Protocol, протокол туннелирования на втором уровне модели OS1; Internet Protocol Security, протокол безопасности IP), уровень защиты, обеспечиваемый PPTP/MPPE, напрямую зависит от сложности верительных данных пользователя и прокола аутентификации пользователя PPP (Point-to-Point Protocol, протокол передачи от точки к точке). Следует использовать сложные пароли пользователей с аутентификацией сертификатами пользователя по протоколам MS-CHAPv2 (Microsoft Challenge Handshake Protocol, протокол проверки подлинности за проса-подтверждения Microsoft) или EAP (Extensible Authentication Protocol, наращиваемый протокол аутентификации).

Однако если вы в настоящий момент не находитесь в стадии развертывания системы PKI, секретный ключ (shared key) для протокола L2TP/IPSec — по-прежнему приемлемый вариант. Только учтите, что он снижает уровень безопасности ваших соединений по протоколу L2TP/IPSec по сравнению с соединениями, устанавливаемыми с применением сертификатов компьютеров. Безопасная реализация для протокола IPSec — применение сертификатов компьютера для VPN-сервера и VPN-клиентов. Мы обсудим использование секретных ключей после знакомства С процедурами, необходимыми для подтверждения подлинности с помощью сертификатов в соединениях по протоколу L2TP/IPSec.

Первый шаг — обеспечить сертификатом компьютера брандмауэр ISA. Есть несколько методов, которые можно использовать для получения сертификата компьютера. В следующем примере мы воспользуемся автономной оснасткой Certificates (Сертификаты) консоли управления MMC. Имейте в виду, что вы можете применять эту оснастку, только когда брандмауэр ISA является членом того же домена, в котором установлен Центр сертификации предприятия. Если брандмауэр ISA не входит в этот домен, можно использовать Web-сайт регистрации (Web enrollment site) для получения сертификата компьютера.

Для того чтобы автономная оснастка MMC могла связаться с Центром сертификации, нам понадобится правило «all open» (все открыто), разрешающее всему трафику проходить из сети локального хоста (Local Host network) к сети Интернет. Мы заблокируем это правило, как только получение сертификата будет завершено.

Выполните следующие шаги на брандмауэре ISA 2004 для запроса сертификата из Центра сертификации предприятия во внутренней сети.

1. На консоли **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, на левой панели и затем щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). На панели задач щелкните кнопкой мыши вкладку **Tasks** (Задачи) и затем ссылку **Create a New Access Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В этом примере мы назовем правило **All Open from Local Host to Internal.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) согласитесь с выбором по умолчанию **All outbound traffic** (Весь исходящий трафик) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети). Дваж-

ды щелкните мышью строку **Local Host** (Локальный хост) и щелкните мышью кнопку **Close** (Закрыть).

6. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети). Дважды щелкните мышью строку **Internal** (Внутренняя) и щелкните мышью кнопку **Close** (Закрыть).
7. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умол чанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
8. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила доступа).
9. Щелкните правой кнопкой мыши правило доступа **All Open from Local Host to Internal** и щелкните левой кнопкой мыши команду **Configure RPC Protocol** (Настроить RPC-протокол).
10. В диалоговом окне **Configure RPC protocol policy** (Настроить политику RPC-протокола) сбросьте флажок **Enforce strict RPC compliance** (Требовать стро гого RPC-соответствия). Щелкните мышью кнопку **Apply** (Применить) и затем кнопку OK.
11. На консоли **Microsoft Internet Security and Acceleration Server 2004** (Сер вер защищенного быстрого доступа к сети Интернет 2004) раскройте узел **Con figuration** (Конфигурация) и щелкните кнопкой мыши узел **Add-ins** (Дополне ния). Правой кнопкой мыши щелкните строку **RPC Filter** на панели дополни тельных параметров и затем левой кнопкой команду **Disable** (Отключить).
12. В диалоговом окне **ISA Server Warning** (Предупреждение сервера ISA) выберите ссылку **Save the changes and restart the services** (Сохранить изменения и перезапустить сервисы). Щелкните мышью кнопку OK.
13. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
14. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
15. Щелкните мышью кнопку **Start** (Пуск) и команду **Run** (Выполнить). Введите mmc в текстовое поле **Open** (Открыть) и щелкните мышью кнопку OK.
16. В окне **Consolel** щелкните кнопкой мыши пункт меню **File** (Файл) и команду **Add/Remove Snap-in** (Добавить/Удалить оснастку).
17. В диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку) щелкните мышью кнопку **Add** (Добавить).
18. В диалоговом окне **Add Standalone Snap-in** (Добавить изолированную оснаст ку) выберите строку **Certificates** (Сертификаты) из списка **Available Standalone Snap-ins** (Доступные изолированные оснастки). Щелкните мышью кнопку **Add** (Добавить).

19- На странице **Certificates snap-in** (Оснастка Сертификаты) выберите вариант **Computer account** (Учетная запись компьютера).
20. На странице **Select Computer** (Выберите компьютер) выберите вариант **Local computer** (Локальный компьютер).
21. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **Add Standalone Snap-in** (Добавить изолированную оснастку).
22. Щелкните мышью кнопку ОК в диалоговом окне **Add/Remove Snap-in** (Доба вить/Удалить оснастку).
23. На левой панели консоли раскройте элемент **Certificates (Local Computer)** (Сертификаты, локальный компьютер) и щелкните мышью папку **Personal** (Лич ные). Правой кнопкой мыши щелкните папку **Personal** (Личные). Укажите мы шью на команду **All Tasks** (Все задачи) и щелкните левой кнопкой мыши ко манду **Request New Certificate** (Запросить новый сертификат).
24. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Request Wizard** (Вас приветствует мастер запроса сертификата).
25. На странице **Certificate Types** (Типы сертификатов) выберите элемент **Compu ter** (Компьютер) в списке **Certificate** Types (Типы сертификатов) и щелкните мышью кнопку **Next** (Далее).
26. На странице **Certificate Friendly Name and Description** (Дружественное имя сертификата и описание) введите имя в текстовое поле **Friendly name** (Дру жественное имя). В данном примере введите **Firewall Computer Certificate.** Щелкните мышью кнопку **Next** (Далее).
27. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certifi cate Request Wizard** (Завершение мастера запроса сертификата).
28. Щелкните мышью кнопку ОК на странице, информирующей о том, что запрос сертификата завершился успешно.
29. Вернитесь на консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте на левой панели окно, связанное с именем компьютера. Щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). Правой кнопкой мыши щелкните правило доступа **All Open from Local Host to Internal** и щелк ните левой кнопкой мыши команду **Disable** (Блокировать).
30. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те узел **Configuration** (Конфигурация) и щелкните кнопкой мыши узел **Add-ins** (Дополнения). Щелкните правой кнопкой мыши элемент **RPC Filter** на па нели дополнительных параметров и щелкните левой кнопкой мыши команду **Enable** (Включить).
31. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.

32. На странице **ISA Server Warning** (Предупреждение сервера ISA) выберите ссылку **Save the changes and restart the services** (Сохранить изменения и перезапустить сервисы). Щелкните мышью кнопку ОК.
33. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

СОВЕТ Если вы не отключите RPC-фильтр перед попыткой запросить сертификат из оснастки Certificates консоли MMC, запрос сертификата завершится неудачно. Если вы отключите RPC-фильтр после запрашивания сертификата, запрос снова закончится неудачей. Вам придется перезапустить брандмауэр ISA, для того чтобы запросить сертификат. Мораль? Отключите RPC-фильтр, прежде чем запрашивать сертификаты из оснастки Certificates консоли MMC.

Имейте в виду, что не нужно вручную копировать сертификат ЦС предприятия в хранилище сертификатов брандмауэра **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации), потому что сертификат ЦС автоматически устанавливается на членах домена. Если брандмауэр — не член домена, в котором установлен ЦС предприятия, вам придется вручную поместить сертификат ЦС в это хранилище сертификатов.

СОВЕТ Ознакомьтесь с комплектом документации по установке VPN брандмауэра ISA Server 2000 (ISA Server 2000 VPN Deployment Kit) для выяснения того, как получить сертификаты с помощью Web-сайта регистрации (Web enrollment site) и как импортировать сертификат ЦС в хранилище сертификатов брандмауэра Trusted Root Certification Authorities (Доверенные корневые центры сертификации). Комплект документации можно найти на Web-сайте ISAserver.org по адресу http://www.isaserver.org/articles/isa2000vpn-deploymentkit.html.

Следующий шаг — обеспечение сертификатом компьютера VPN-клиента. В данном примере машина VPN-клиента — не член домена. Необходимо запросить сертификат компьютера, используя Web-сайт регистрации ЦС предприятия и вручную поместить сертификат ЦС предприятия в хранилище сертификатов **Trusted Root Certification Authorities** на машине клиента. Легче всего запросить сертификат с машины VPN-клиента, установив на ней PPTP-соединение.

ПРИМЕЧАНИЕ В рабочей среде не заслуживающие доверия машины клиентов не должны обеспечиваться сертификатами компьютера. Только машинам, находящимся в сфере вашего управления, следует разрешать установку компьютерных сертификатов. Члены домена — управляемые клиенты и, следовательно, находятся под административным контролем вашей организации. Настоятельно рекомендуем запретить пользователям устанавливать их собственные сертификаты на машинах вне зоны управления. Сертификат компьютера — это средство защиты, не предназначенное для обеспечения свободного доступа всем пользователям, желающим его получить.

Выполните следующие шаги для запроса и установки сертификата ЦС.

1. Установите VPN-соединение по протоколу PPTP с брандмауэром ISA.
2. Откройте обозреватель Internet Explorer. В строке **Address:** (Адрес:) введите **http://10.0.0.2/certsrv** (где 10.0.0.2 — IP-адрес центра сертификации во внутренней сети), щелкните мышью кнопку ОК.
3. В диалоговом окне **Enter Network Password** (Введите сетевой пароль) введите **Administrator** в текстовое поле **User Name** (Имя пользователя) и пароль администратора в текстовое поле **Password** (Пароль). Щелкните мышью кнопку ОК.
4. Щелкните переключатель **Request a Certificate** (Запросить сертификат) на странице **Welcome** (Добро пожаловать).
5. На странице **Request a Certificate** (Запросить сертификат) щелкните мышью переключатель **Advanced certificate request** (Расширенный запрос сертификата).
6. На странице **Advanced Certificate Request** (Расширенный запрос сертификата) установите переключатель **Create and submit a request to this CA** (Создать и представить запрос данному ЦС).
7. На странице **Advanced Certificate Request Расширенный** запрос сертификата) выберите сертификат **Administrator** из списка **Certificate Template** (Шаблон сертификата). Установите флажок **Store certificate in the local computer certificate store** (Сохранить сертификат в хранилище сертификатов локального компьютера). Щелкните мышью кнопку **Submit** (Принять).
8. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).
9. На странице **Certificate Issued** (Выданные сертификаты) щелкните мышью кнопку **Install this certificate** (Установить данный сертификат).
10. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).
11. Закройте обозреватель после просмотра страницы **Certificate Installed** (Установленный сертификат).
12. Щелкните мышью кнопку **Start** (Пуск) и затем команду **Run** (Запустить). Введите mmc в текстовое поле **Open** (Открыть) и щелкните мышью кнопку ОК.
13. В окне консоли **Consolel** щелкните мышью пункт меню **File** (Файл), а затем команду **Add/Remove Snap-in** (Добавить/Удалить оснастку).
14. Щелкните мышью кнопку **Add** (Добавить) в диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку).
15. В диалоговом окне **Add Standalone Snap-in** (Добавить изолированную оснастку) выберите строку **Certificates** (Сертификаты) из списка **Available Standalone Snap-ins** (Доступные изолированные оснастки). Щелкните мышью кнопку **Add** (Добавить).
16. Выберите вариант **Computer account** (Учетная запись компьютера) на странице **Certificates snap-in** (Оснастка Сертификаты).

17. Выберите вариант **Local computer** (Локальный компьютер) на странице **Select Computer** (Выберите компьютер).
18. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **Add Standalone Snap-in** (Добавить изолированную оснастку).
19. Щелкните мышью кнопку ОК в диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку).
20. На левой панели консоли раскройте элемент **Certificates (Local Computer)** (Сертификаты, локальный компьютер) и папку **Personal** (Личные). Щелкните кнопкой мыши **\Personal\Certificates.** Дважды щелкните кнопкой мыши сертификат **Administrator** на правой панели консоли.
21. В диалоговом окне **Certificate** (Сертификат) щелкните мышью вкладку **Certification Path** (Путь сертификации). На вершине иерархии сертификатов, показанной в области **Certification Path** (Путь сертификации), находится сертификат корневого ЦС. Щелкните кнопкой мыши элемент EXCHANGE2003BE в начале списка и кнопку **View Certificate** (Просмотр сертификата).
22. В диалоговом окне **Certificate** (Сертификат) сертификата ЦС щелкните кнопкой мыши вкладку **Details** (Состав). Щелкните мышью кнопку **Copy to File** (Копировать в файл).
23. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Export Wizard** (Вас приветствует мастер экспорта сертификатов).
24. На странице **Export File Format** (Формат экспортируемого файла) выберите переключатель **Cryptographic Message Syntax Standard - PKCS *7 Certificates (.P7B)** (Стандарт Cryptographic Message Syntax — сертификаты PKCS *7 (.P7B)) и щелкните мышью **кнопку Next** (Далее).
25. На странице **File to Export** (Имя файла экспорта) введите **c:\cacert** в текстовое поле **File name** (Имя файла). Щелкните мышью кнопку **Next** (Далее).
26. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certificate Export Wizard** (Завершение работы мастера экспорта сертификатов).
27. Щелкните мышью кнопку ОК в диалоговом окне **Certificate Export Wizard** (Мастер экспорта сертификатов).
28. Щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат). Снова щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат).
29- На левой панели консоли раскройте папку **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации) и щелкните кнопкой мыши папку **Certificates** (Сертификаты). Щелкните правой кнопкой мыши на левой панели узел **\Trusted Root Certification Authorities\Certificates.** Укажите мышью на команду **All Tasks** (Все задачи) и щелкните левой кнопкой мыши команду **Import** (Импорт).
30. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Import** Wizard (Вас приветствует мастер импорта сертификатов).

31. На странице **File to Import** (Импортируемый файл) воспользуйтесь кнопкой **Browse** (Обзор) для указания сертификата ЦС, который вы сохранили на ло кальном жестком диске и щелкните мышью кнопку **Next** (Далее).
32. На странице **Certificate Store** (Хранилище сертификатов) согласитесь с уста новками по умолчанию и щелкните мышью кнопку **Next** (Далее).
33. На странице **Completing the Certificate Import Wizard** (Завершение работы мастера импорта сертификатов) щелкните мышью кнопку **Finish** (Готово).
34. В диалоговом окне **Certificate Import Wizard** (Мастер импорта сертификатов), информирующем вас об успешном импортировании сертификата, щелкните мышью кнопку ОК.
35. Отсоединитесь от VPN-сервера. Щелкните правой кнопкой мыши пиктограмму соединения на системной панели задач и щелкнитслевой кнопкой мыши кнопку **Disconnect** (Отключить).

Тестирование VPN-соединения по протоколу L2TP/IPSec

Теперь, когда и у брандмауэра ISA, и у машин VPN-клиентов есть сертификаты, можно тестировать защищенное клиентское VPN-соединение удаленного доступа по протоколу L2TP/IPSec с брандмауэром. Начать следует с перезапуска сервиса **Routing and Remote Access** (Сервис маршрутизации и удаленного доступа), для того чтобы он зарегистрировал новый сертификат.

Выполните следующие шаги для включения поддержки протокола L2TP/IPSec.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети). Щелкните кнопкой мыши строку **Configure VPN Client Access** (Конфигурировать доступ VPN-клиентов) на вкладке **Tasks** (Задачи) на панели задач. Щелкните мышью кнопку **Apply** (Применить) и затем кнопку ОК.
2. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
3. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
4. Перезапустите компьютер с брандмауэром ISA.

Следующий шаг — установка соединения VPN-клиента.

1. На компьютере VPN-клиента откройте пиктограмму соединения VPN-клиента (VPN client connectoid). Щелкните мышью кнопку **Properties** (Свойства). В диалоговом окне **VPN Properties** (VPN-свойства) щелкните кнопкой мыши вкладку **Networking** (Сеть). На этой вкладке замените тип подключения **Type of VPN** на тип **L2TP IPSec VPN.** Щелкните мышью кнопку ОК.

2. Инициируйте VPN-подключение к брандмауэру ISA.
3. Щелкните мышью кнопку ОК в диалоговом окне **Connection Complete** (Уста новленное соединение), информирующее об установке соединения.
4. Дважды щелкните кнопкой мыши пиктограмму соединения на системной панели задач.
5. В диалоговом окне **ISA VPN Status** (Состояние ISA VPN) (рис. 918) щелкните мышью кнопку **Details** (Состав). Вы увидите строку **IPSEC Encryption,** свиде тельствующую об успешной установке соединения по протоколу L2TP/IPSec.

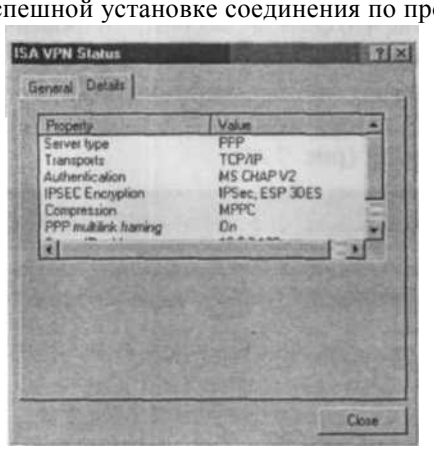


Рис. 9.18. Состав соединения по протоколу L2TP/IPSec

6. Щелкните мышью **кнопку Close** (Закрыть) в диалоговом окне **ISA VPN Status** (Состояние ISA VPN).

Мониторинг VPN-клиентов

Брандмауэр ISA позволяет следить за соединениями VPN-клиентов. Выполните следующие шаги, чтобы узнать способы отображения соединений VPN-клиентов. 1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети). Щелкните кнопкой мыши строку **Monitor VPN Clients** (Мониторинг VPN-клиентов) (рис. 9.19) на вкладке **Tasks** (Задачи) на панели задач. Имейте в виду, что этот выбор изменит характер фильтра сеансов (Sessions filter). Возможно вы захотите скопировать текущие установки фильтра сеансов, для того чтобы вернуться к ним после создания VPN-фильтра.

Related Tasks f*
Monitor VPN Clients
(?) Export VPN Clients Configuration

Рис. 9.19. Ссылка **Monitor VPN Clients** (Мониторинг VPN-клиентов)

2. Вы перемещаетесь на вкладку **Sessions** (Сеансы) в узле **Monitoring** (Мониторинг). На вкладке видно, что сеансы связи отфильтрованы и отображаются только соединения **VPN Client.**

3. Щелкните кнопкой мыши вкладку **Dashboard** (Инструментальная панель). На ее панели **Sessions** (Сеансы) можно увидеть соединения **VPN Remote Client** (Удаленный VPN-клиент) (рис. 9.20).

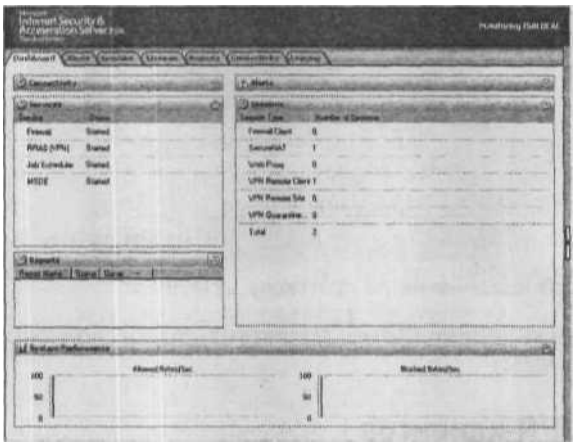


Рис. 9.20. Инструментальная панель брандмауэра ISA

4. Также можно воспользоваться журналами регистрации в режиме реального времени для слежения за соединениями VPN-клиентов. Щелкните кнопкой мыши вкладку **Logging** (Регистрация), а затем вкладку **Tasks** (Задачи) на панели задач. Щелкните мышью **Start Query** (Запустить запрос). Вы можете применять свойства фильтров для отбора конкретных VPN-клиентов или только клиентов сети VPN. На рис. 921 показаны элементы журнала регистрации.

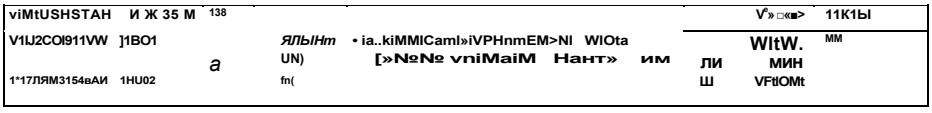


Рис. 9.21. Записи журнала регистрации для соединений VPN-клиентов

Использование секретного ключа в соединениях VPN-клиентов удаленного доступа

Как упоминалось ранее в этой главе, вы можете использовать секретные ключи (pre-shared keys) для IPSec-аутентификации, если у вас не установлена инфраструктура открытого ключа (PKI). Брандмауэр ISA можно настроить для поддержки как секретных ключей, так и сертификатов соединений удаленного доступа VPN-клиентов. VPN-клиент должен поддерживать секретные ключи для подтверждения подлинности по протоколу IPSec. Вы можете загрузить обновленную версию VPN-клиента по протоколу L2TP/IPSec для ОС Windows с адреса http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/12tpclient.asp. Эта версия VPN-клиента позволяет применять секретные ключи (pre-shared keys) для клиентских операционных систем Windows 9X, Windows NT 4.0 и Windows 2000.

Брандмауэр ISA может быть сконфигурирован для поддержки секретных ключей. Выполните следующие шаги для того, чтобы настроить брандмауэр ISA для поддержки секретных ключей при IPSec-аутентификации.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети).
2. Щелкните кнопкой мыши ссылку **Select Authentication Methods** (Выбрать методы аутентификации) на вкладке **Tasks** (Задачи) на панели задач.

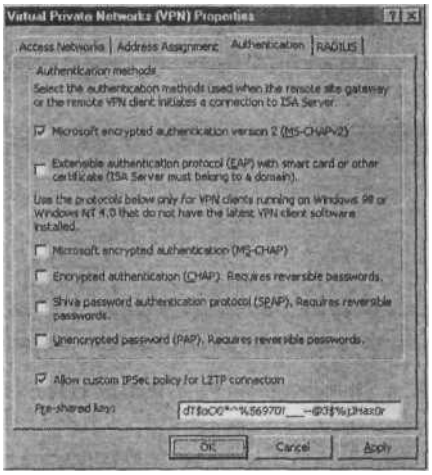


Рис. 9.22. Вкладка Authentication (Подтверждение подлинности)

3. Б диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства вир-**туальнш** чэсгных сетей) установите флажок **Allow customer IPSec policy for L2TP connection** (Разрешить настраиваемую IPSec-политику для Ь2ТР-СОЕДИНЕ-

ния). Введите секретный ключ в текстовое поле **Pre-shared key** (Секретный ключ). Убедитесь, что ключ достаточно сложен, содержит буквы, цифры и символы (рис. 9.22) и его длина не менее 17 символов.

4. Щелкните мышью кнопку **Apply** (Примен ить), а затем кнопку ОК в диалоговом окне **ISA** 2004, информирующем о том, что сервис маршрутизации и удаленного досту па нужно **перезапустить.** Щелкните мышью **кнопку ОК** в диалоговом окне **Virtual Private Networking (VPN) Properties** (Свойства виртуальных частных сетей).
5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (При менить новую конфигурацию).

Следует настроить VPN-клиент для поддержки секретного ключа. Необходимые процедуры зависят от используемого вами варианта клиента. Перечисленные далее описывают, как настроить VPN-клиента под управлением ОС Windows XP для применения секретного ключа.

1. Откройте пиктограмму VPN-соединения (VPN connectoid), которое используется для связи с брандмауэром ISA, и щелкните мышью кнопку **Properties** (Свойства).
2. В диалоговом окне **Properties** (Свойства) пиктограммы соединения щелкните кнопкой мыши вкладку **Security** (Безопасность).

Ь- На вкладке **Security** (Безопасность) щелкните мышью кнопку **IPSec Settings** (Установочные параметры IPSec). 4. В диалоговом окне **IPSec Settings**

(Установочные параметры IPSec) установите

флажок **Use** *a* **pre-shared key for authentication** (Использовать секретный ключ для аутентификации), а затем введите ключ в текстовое поле **Key** (Ключ) (рис. 9.23). Щелкните мышью кнопку ОК.

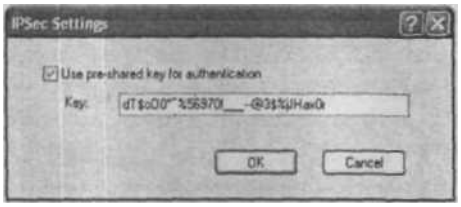


Рис. 9.23. Ввод ключа для протокола L2TP/IPSec на машине клиента

Щелкните кнопку ОК в диалоговом окне **Properties** (Свойства) пиктограммы соединения.

Соединитесь с брандмауэром ISA. Вы можете убедиться в том, что секретный ключ применяется для соединения по протоколу IPSec, просматривая характеристики соединения в оснастке консоли MMC **IPSec Security Monitor** (Монитор IP-безопасности) (рис. 9.24).

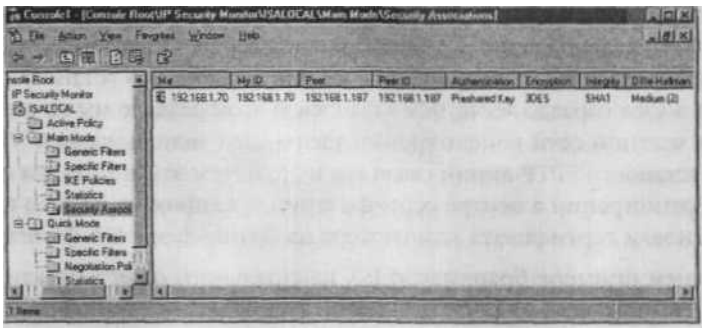


Рис. 9.24. Отображение IPSec-информации в оснастке консоли MMC для протокола IPSec

Создание VPN-соединения «узел-в-узел» по протоколу PPTP

Виртуальные частные сети конфигурации узел-в-узел соединяют друг с другом целые сети. Это может привести *к* значительной экономии средств в организациях, использующих выделенные каналы с ретрансляцией кадров (dedicated frame relay links) для соединения филиалов между собой или с центральным офисом. Для VPN-конфигурации узел-в-узел брандмауэр ISA использует следующие VPN-протоколы:

- PPTP (Point-to-Point Tunneling Protocol) (сквозной туннельный протокол);
- L2TP/IPSec (Layer Two Tunneling Protocol over IPSec) (протокол туннелирования на втором уровне модели OSI поверх протокола IP-безопасности);
- IPSec Tunnel Mode (туннельный режим протокола IPSec).

Наиболее защищенный VPN-протокол для VPN конфигурации узел-в-узел — протокол L2TP/IPSec. Этот протокол позволяет запрашивать подтверждение подлинности и машины, и пользователя. Второй наиболее защищенный протокол для VPN конфигурации узел-в-узел является предметом спора. Если у вас есть два брандмауэра ISA или вы устанавливаете соединение брандмауэра ISA с машиной, на которой установлен сервис RRAS Windows (Routing and Remote Access Services, сервис маршрутизации и удаленного доступа), рекомендуем использовать протокол PPTP и настроить аутентификацию с помощью сертификата. Туннельный режим протокола IPSec следует применять, только когда вы вынуждены подключаться к VPN-шлюзу более ранних версий (downlevel). Главная проблема, связанная с туннельным режимом протокола IPSec, заключается в том, что поставщики VPN-шлюзов более ранних версий требуют применения секретного ключа вместо подтверждения подлинности сертификатом, и существует ряд злонамеренных программ, способных извлечь выгоду из этой ситуации.

Создание виртуальной частной сети конфигурации узел-в-узел может быть непростым процессом, включающим ряд обязательных шагов. Однако, как только вы поймете их смысл и причину их выполнения, вы обнаружите, что установка VPN конфигурации узел-в-узел гораздо легче, чем казалось. В этом разделе мы начнем с создания виртуальной частной сети конфигурации узел-в-узел, использующей VPN-протокол PPTP. После установки PPTP-линии связи мы используем эту линию для соединения с Web-сайтом регистрации в центре сертификации предприятия из сети центрального офиса и установки сертификата компьютера на брандмауэре ISA филиала.

В следующем примере брандмауэр ISA центрального офиса назван ISALOCAL, а брандмауэр ISA филиала — REMOTEISA. Нами используется установка сети лаборатории, описанная в главе 4, поэтому, если вы не помните подробностей этой установки, просмотрите ее сейчас. Сведения об установке сети лаборатории помогут вам понять процедуры создания VPN конфигурации узел-в-узел, которые мы вам предложим.

ПРИМЕЧАНИЕ В следующем примере брандмауэр ISA филиала не является членом домена центрального офиса. Но есть возможность сделать брандмауэр ISA филиала членом домена и расширить домен, включив в него филиалы. Из-за ограниченности объема книги мы не можем подробно описать процедуры, необходимые для формирования этой конфигурации. Обязательно подпишитесь на рассылку RSS feed (файлы в формате RSS (Really Simple Syndication, Rich Site Summary)) с новостным контентом Web-ресурса на сайте www.isaserver.org, чтобы получить уведомление о том, что на сайт ISAserver.org поступила серия наших статей об установке машин филиала как членов домена и расширении вашего домена за счет филиалов.

Еще одно важное замечание, касающееся последующего разбора, — для назначения IP-адресов VPN-клиентам и шлюзам мы используем сервис DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста). Вы можете применить как сервис DHCP, так и пул статических адресов. Однако, если вы решите использовать пул статических адресов и назначите IP-адреса *подсети* VPN-клиентам и шлюзам, вам придется удалить эти адреса из определения внутренней сети (или любой другой сети, для которой они представляют собой перекрывающиеся адреса).

Для получения работающей по протоколу PPTP VPN конфигурации узел-в-узел следует выполнить следующие процедуры.

- **Создать удаленную сеть (Remote Network) в центральном офисе** Сеть удаленного сайта (Remote Site Network) — это использование брандмауэром ISA для VPN-соединений конфигурации узел-в-узел. Всегда, когда брандмауэр ISA соединяется с другой сетью с помощью VPN типа узел-в-узел, необходимо создать сеть удаленного сайта. Эта сеть применяется в правилах доступа для управления доступом к ней и из нее. Сеть удаленного сайта, которая создается в центральном офисе, будет представлять IP-адреса, используемые в сети филиала.

Создать сетевое правило в центральном офисе Сетевое правило контролирует маршрутную связь между сетями. Мы настроим сеть конфигурации узел-в-узел так, чтобы установилась маршрутная связь между центральным офисом и филиалом. Маршрутные связи предпочтительнее, поскольку не все протоколы поддерживают средства NAT.

Создать правила доступа в центральном офисе Эти правила позволят всему трафику из центрального офиса достигать филиала, а всему трафику из филиала достигать главного офиса. В вашей рабочей сети вы, вероятно, захотите несколько ограничить эти правила, для того чтобы пользователи филиала могли получать доступ только *к той* информации *в* центральном офисе, которая им необходима. Например, пользователям филиала нужен доступ только сайтам OWA (Outlook Web Access, Web-доступ *в* Outlook) в центральном офисе, создайте правила доступа, разрешающие пользователям обращаться только по протоколу HTTPS только к серверу OWA.

Создать в центральном офисе учетную запись VPN-шлюза для удаленного доступа по телефонной линии Мы должны создать пользовательскую учетную запись, которую брандмауэр ISA филиала будет использовать для аутентификации на брандмауэре ISA центрального офиса. Когда брандмауэр ISA филиала вызывает брандмауэр ISA главного офиса, филиал будет применять эти имя пользователя и пароль для подтверждения подлинности в центральном офисе. Интерфейс вызова по требованию (demand-dial) брандмауэра ISA филиала настраивается на использование этой учетной записи. **Создать удаленную сеть (Remote Network) в филиале** После того, как VPN-конфигурация типа узел-в-узел выполнена в центральном офисе, мы перенесем свое внимание на брандмауэр ISA филиала. На брандмауэре ISA филиала мы начнем с создания сети удаленного сайта, которая представляет IP-адреса, используемые в центральном офисе. Воспользуемся этим сетевым объектом для управления прохождением трафика филиала к главному офису и от него. **Создать сетевое правило в филиале** Так же как и в центральном офисе, в филиале нужно создать сетевое правило, контролирующее маршрутную связь для обмена сообщениями между сетью филиала и сетью центрального офиса. Мы настроим сетевое правило для осуществления маршрутной связи между филиалом и центральным офисом.

Создать правила доступа в филиале Мы создадим два правила доступа на брандмауэре ISA филиала. Первое разрешит всему трафику филиала достигать центрального офиса, а второе правило позволит всему трафику центрального офиса достигать филиала. В рабочей среде вы возможно захотите ограничить трафик, направляющийся из филиала в центральный офис. Имейте в виду, что вы можете установить такой контроль как на брандмауэре ISA филиала, так и **на** брандмауэре ISA центрального офиса. Мы предпочитаем установку средств контроля доступа на обоих узлах, **но** средства контроля в центральном офисе

важнее, потому что часто нет возможности изменения средств управления, настраиваемых в филиалах.

- **Создать в филиале учетную запись VPN-шлюза для удаленного доступа по телефонной линии** Нам нужно создать учетную запись пользователя на брандмауэре ISA филиала, чтобы брандмауэр ISA центрального офиса мог использовать ее для аутентификации, когда устанавливается соединение с брандмауэром ISA филиала. Интерфейс вызова по требованию (demand-dial) брандмауэра ISA центрального офиса применяет эту учетную запись для аутентификации на брандмауэре ISA филиала.
- **Активизировать каналы типа узел-в-узел** Мы активизируем VPN-канал конфигурации узел-в-узел, установив соединение хоста филиала с хостом в сети центрального офиса.

Создание удаленной сети в центральном офисе

Начнем с конфигурирования брандмауэра ISA в центральном офисе. Первый шаг — конфигурирование сети удаленного сайта на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004).

Выполните следующие шаги для создания сети удаленного сайта на брандмауэре ISA центрального офиса.

1. Откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети).
2. Щелкните кнопкой мыши вкладку **Remote Sites** (Удаленные сайты) на панели **Details** (Состав). Щелкните мышью вкладку **Tasks** (Задачи) на панели задач. Щелкните мышью кнопку **Add Remote Site Network** (Добавить сеть удаленного сайта).
3. На странице **Welcome to the New Network Wizard** (Вас приветствует мастер создания новой сети) введите имя удаленной сети в текстовое поле **Network name** (Имя сети). В данном примере мы назовем удаленную сеть **Branch.** Выбранное имя очень важно, поскольку оно будет именем интерфейса вызова по требованию (demand-dial), созданного на брандмауэре ISA в центральном офисе, и именем учетной записи пользователя, которое брандмауэр ISA филиала будет использовать для соединения с брандмауэром ISA центрального офиса. Щелкните мышью кнопку **Next** (Далее).
4. На странице **VPN Protocol** (VPN-протокол) есть возможность выбрать **IP Security protocol** (Протокол IP-безопасности) **(IPSec tunnel mode, Layer Two Tunneling Protocol (L2TP) over IPSec)** (Туннельный режим протокола IPSec, протокол L2TP поверх протокола IPSec) и **Point-to-Point Tunneling Protocol** (Сквозной туннельный протокол).

Если у вас нет сертификатов, установленных на машинах филиала и центрального офиса, и вы не планируете применять их в будущем, следует выбрать протокол PPTP. Если же у вас есть сертификаты, установленные на машинах филиала и центрального офиса, или вы планируете установить их в будущем, выбирайте протокол L2TP/IPSec (вы сможете применять секретный ключ до тех пор, пока не установите сертификаты). *Не* используйте вариант IPSec до тех пор, пока вы не соединяетесь с VPN-шлюзом сторонних поставщиков (из-за низкой защищенности линий связи типа узел-в-узел с применением туннельного режима протокола IPSec, которые обычно зависят от секретных ключей). В данном примере мы сконфигурируем сеть VPN конфигурации узел-в-узел по протоколу PPTP, поэтому выберем переключатель **Pdint-to-Point Tunneling Protocol (PPTP)** (рис. 9-25). Щелкните мышью кнопку **Next** (Далее).

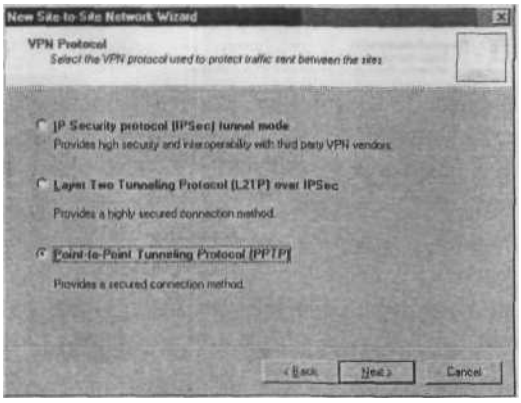


Рис. 9.25. Выбор VPN-протокола

5. На странице **Remote Site Gateway** (Шлюз удаленного сайта) введите IP-адрес во внешнем интерфейсе удаленного брандмауэра ISA, в этом примере — **192.168.1.71.** Имейте в виду, что вы можете также использовать полностью определенное имя домена в этом текстовом поле. Это полезно, если в филиале применяется дина мический адрес на внешнем интерфейсе и вы используете сервис DDNS **(Dynamic** Domain Name System, динамическая система имен доменов), такой как TZO (про грамма привязки доменных имен к динамическим IP-адресам) (www.tzo.com). Мы применяем сервис TZO в течение нескольких лет и настоятельно рекомен дуем его. Щелкните мышью **кнопку Next** (Далее).
6. На странице **Remote Authentication** (Удаленная аутентификация) установите флажок **Local site can initiate connections to remote site using these creden tials** (Локальный сайт может инициировать соединения с удаленным сайтом, используя эти верительные данные). Введите имя учетной записи, которую вы создадите на удаленном брандмауэре ISA для разрешения брандмауэру ISA цен трального офиса подтвердить свою подлинность на брандмауэре ISA филиала.

В данном примере назовем учетную запись пользователя **Main** (учетная запись пользователя вполне соответствует имени запрашивающего соединение по телефонной линии интерфейса, созданного на удаленном сайте; мы еще не создали этот интерфейс, но обязательно сделаем это, когда будем настраивать брандмауэр ISA филиала). Имя **Domain** (Домен) — это имя компьютера с брандмауэром ISA филиала, в данном примере — **REMOTEISA** (если удаленный брандмауэр ISA является контроллером домена, вы должны использовать имя домена вместо имени компьютера, поскольку на контроллере домена нет сохраненных локальных учетных записей). Введите пароль для учетной записи и подтвердите его, как показано на рис. 9.26. Убедитесь, что вы записали пароль, потому что вам придется вспомнить его, когда позже будет создаваться учетная запись на брандмауэре ISA филиала. Щелкните мышью кнопку **Next** (Далее).

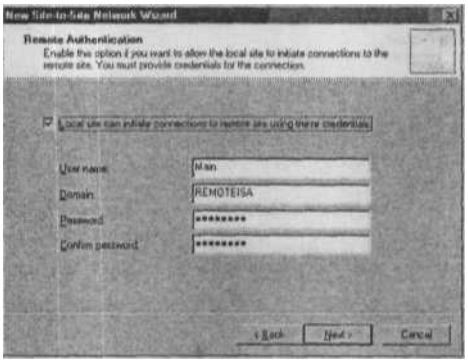


Рис. 9.26. Задание верительных данных для соединения удаленного доступа по телефонной линии

7. Познакомьтесь с информацией, представленной на странице **Local Authen tication** (Локальная аутентификация) и щелкните мышью кнопку **Next** (Далее). Эта страница напоминает вам о необходимости создания учетной записи на данном брандмауэре ISA, которую брандмауэр ISA филиала может использовать для подтверждения подлинности при инициализации VPN-соединения конфи гурации **узел-в-узел.** Если вы забудете создать учетную запись пользователя, попытка аутентификации завершится неудачно и VPN-канал типа узел-в-узел не будет установлен.
8. Щелкните мышью кнопку **Add** (Добавить) на странице **Network Addresses** (Се тевые адреса). В диалоговом окне **IP Address Range Properties** (Свойства диа пазона IP-адресов) введите **10.0.1.0** в текстовое поле **Starting address** (Началь ный адрес). Введите **10.0.1.255** в текстовое поле **Ending address** (Конечный адрес). Щелкните мышью кнопку ОК.
   Это важный шаг в создании вашей VPN конфигурации узел-в-узел. Вы должны включить все адреса сети удаленного сайта. Несмотря на то, что вы можете создать правила доступа, разрешающие доступ только к подмножеству адресов в

этой сети, следует включить все адреса, используемые в данной сети. Также не забудьте о сетевых идентификаторах (ID), достигаемых с брандмауэра ISA филиала. Например, может существовать несколько сетей, достигаемых из интерфейса LAN (локальной сети) (любой внутренний или DMZ-интерфейсы брандмауэра ISA филиала). Вставьте все эти адреса в данное диалоговое окно (рис. 9-27).

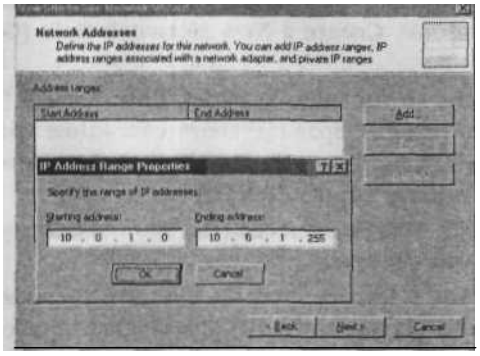


Рис. 9.27. Конфигурирование диапазона IP-адресов для сети удаленного сайта

9. Щелкните мышью кнопку **Next** (Далее) на странице **Network** Addresses (Сете вые адреса).
10. Щелкните мышью кнопку Finish (Готово) на странице **Completing the New Network Wizard** (Завершение мастера создания новой сети).

Создание сетевого правила в центральном офисе

Брандмауэр ISA должен знать, как направлять пакеты в сеть филиала. Есть две возможности: **Route** (Маршрут) и NAT (network address translation, преобразование сетевых адресов). Маршрутная связь позволяет направлять пакеты в филиал и сохранять исходный IP-адрес клиента, устанавливающего соединение по линии связи узел-в-узел. NAT-связь заменяет исходный IP-адрес клиента, устанавливающего соединение. Как правило, маршрутная связь предоставляет поддержку протоколов более высокого уровня, а средства NAT обеспечивает более высокий уровень безопасности, потому что скрывают на стороне соединения с NAT действительный IP-адрес хоста-источника.

Важным основанием для применения маршрутной связи может стать наличие членов домена в сети удаленного сайта. Аутентификация по протоколу Kerberos встраивает исходный IP-адрес в передаваемые пользовательские данные (payload) и не имеет NAT-редактора или фильтра приложения для выполнения этой работы.

В данном примере мы будем использовать маршрутную связь между центральным офисом и филиалом, для того чтобы позже иметь возможность включить машины из сети филиала в домен Active Directory центрального офиса. Выполните

следующие шаги для создания сетевого правила, контролирующего маршругную связь между сетями центрального офиса и филиала.

1. Раскройте узел **Configuration** (Конфигурация) на левой панели консоли. Щелкните кнопкой мыши узел **Networks** (Сети).
2. Щелкните кнопкой мыши вкладку **Network Rules** (Сетевые правила) на панели **Details** (Сведения). Щелкните мышью вкладку **Tasks** (Задачи) на панели задач. Щелкните мышью кнопку **Create a New Network Rule** (Создать новое сетевое правило).
3. На странице **Welcome to the New Network Rule Wizard** (Вас приветствует мастер создания нового сетевого правила) введите название правила в текстовое поле **Network rule name** (Название сетевого правила). В данном примере — **Маш to Branch.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Network Traffic Sources** (Источники сетевого трафика) щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши **папку Networks** (Сети). Дважды щелкните кнопкой мыши сеть **Internal** (Внутренняя). Щелкните мышью кнопку **Close** (Закрыть).
6. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Sources** (Источники сетевого трафика).
7. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелкните мышью кнопку **Add** (Добавить).
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) дважды щелкните кнопкой мыши сеть **Branch (Филиал).** Щелкните мышью кнопку **Close** (Закрыть).
9. Щелкните мышью кнопку **Next** (Далее) на **странице Network Traffic Destinations** (Адресаты сетевого трафика).
10. На странице **Network Relationship** (Связь сетей) (рис. 9.28) выберите вариант **Route** (Маршрут).

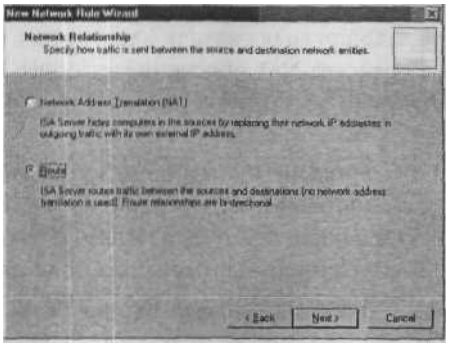


Рис. 9.28. Страница Network Relationship (Связь сетей)

11. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Network Rule Wizard** (Завершение мастера создания нового сетевого правила).

Создание правил доступа в центральном офисе

Мы хотим хостам в сетях центрального офиса и филиала предоставить полный доступ *к* ресурсам каждой сети. Необходимо создать правило доступа, разрешающее прохождение трафика из центрального офиса в филиал и *в* обратном **направлении.**

ПРИМЕЧАНИЕ В реальной обстановке вам придется несколько ограничить доступ и разрешить пользователям филиала доступ только к тем ресурсам центрального офиса, которые им необходимы. Кроме того, возможно вы не захотите предоставлять пользователям центрального офиса полный доступ к любым ресурсам филиала. Есть также возможность ограничить доступ из центрального офиса в филиал только членами группы администраторов.

Выполните следующие шаги для создания правил доступа, разрешающих движение трафика между центральным офисом и филиалом.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). На панели задач щелкните кнопкой мыши вкладку **Tasks** (Задачи). Щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас **приветствует** мастер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере — **Main to Branch.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью **кнопку Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **All outbound traffic** (Весь исходящий трафик) из списка **This rule applies to** (Это правило применяется к) (рис. 9.29). Щелкните мышью кнопку **Next** (Далее).
5. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети), дважды щелкните мышью сеть **Internal** (Внутренняя). Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).
8. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).

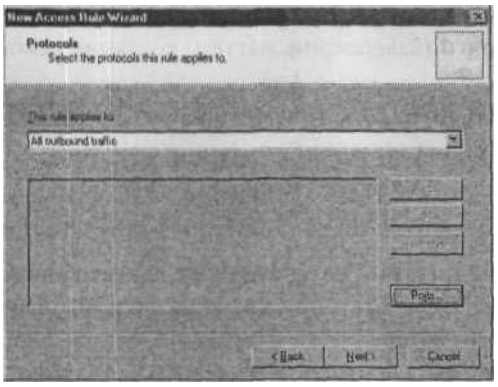


Рис. 9.29. Страница Protocols (Протоколы)

9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью сеть **Branch** (Филиал). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
11. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
12. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила **доступа).**

Второе правило доступа разрешает хостам сети филиала получать доступ к сети центрального офиса (рис. 9-30).

1. Щелкните вкладку **Tasks** (Задачи) на панели задачи. Щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** введите название правила в текстовое поле **Rule name** (Имя правила). В данном примере — **Main to Branch.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **All outbound protocols** (Все исходящие протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Next** (Далее).
5. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети), дважды щелкните мышью сеть **Branch** (Филиал). Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).

8. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью сеть **Internal** (Внут ренняя). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
11. На странице **User Sets** (Состав пользователей) согласитесь с установкой по умол чанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
12. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard.**

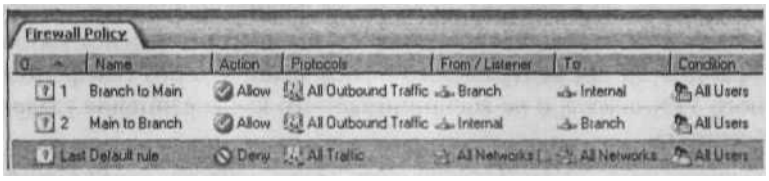


Рис. 9.30. Результирующая политика брандмауэра

Последний этап — предоставление доступа VPN-клиентам (хотя технически VPN-шлюз филиала в действительности не является VPN-клиентом удаленного доступа).

1. Щелкните кнопкой мыши узел **Virtual Private Network** (Виртуальная частная сеть) на левой панели консоли.
2. Щелкните кнопкой мыши вкладку **VPN Clients** (VPN-клиенты) на панели **Details** (Состав). Щелкните мышью вкладку **Tasks** (Задачи) на панели задач и выберите **Enable VPN Client Access** (Разрешить доступ VPN-клиентам).
3. Щелкните мышью кнопку ОК в диалоговом окне **ISA 2004,** информирующем вас о том, что сервис **Routing and Remote Access** (Маршрутизация и удаленный доступ) должен быть запущен заново.
4. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
5. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Создание в центральном офисе учетной записи VPN-шлюза для удаленного доступа по телефонной линии

Необходимо создать учетную запись пользователя на брандмауэре центрального офиса, которую брандмауэр филиала может использовать для подтверждения подлинности VPN-канала конфигурации узел-в-узел. У учетной записи пользователя *должно быть тоже имя,* что и у интерфейса вызова по требованию (demand-dial) на компьютере центрального офиса. Позже вы настроите брандмауэр ISA 2004

филиала для применения этой учетной записи при установлении связи по VPN-каналу конфигурации узел-в-узел.

Соглашения об именовании учетных записей пользователей и интерфейса вызова по требованию — источник путаницы для администраторов брандмауэра ISA. Суть заключается в том, что устанавливающий телефонную связь VPN-шлюз должен представить верительные данные, в которых имя пользователя *такое же, как имя интерфейса вызова по требованию, отвечающего на телефонный звонок.* На рис. 9-31 видно, что происходит, когда центральный офис звонит в филиал, а филиал звонит в центральный офис.

Имя интерфейса вызова по требованию в центральном офисе — **Branch.** Когда филиал **устанавливает** телефонную связь с центральным офисом, для аутентификации на брандмауэре ISA центрального офиса филиал использует учетную запись **Branch.** Поскольку имя этой записи такое же, как имя интерфейса вызова по требованию, брандмауэр ISA центрального офиса знает, что это телефонный звонок от удаленного VPN-шлюза, и *не* воспринимает его как соединение удаленного доступа VPN- клиента.

Когда центральный офис устанавливает соединение по телефонной линии с филиалом, он представляет верительные данные пользователя с именем **Маш.** таким же, как имя интерфейса вызова по требованию брандмауэра ISA филиала. Поскольку имя пользователя в учетной записи, представленное в процессе аутентификации такое же, как имя интерфейса вызова по требованию, брандмауэр ISA филиала знает, что это подключение VPN-шлюза (VPN-маршрутизатора), а не клиентское VPN-соединение удаленного доступа. На рис. 931 показана конфигурация интерфейса вызова по требованию.

Рис. 9.31. Конфигурация интерфейса вызова по требованию на локальном и удаленном сайтах

Выполните следующие шаги для создания учетной записи, которую будет применять удаленный брандмауэр ISA 2004 для подключения к VPN-шлюзу центрального офиса.

1. Щелкните правой кнопкой мыши на рабочем столе пиктограмму **My Computer** (Мой компьютер) *и* выберите команду **Manage** (Управление).
2. На консоли **Computer Management** (Управление компьютером) раскройте узел **Local Users and Groups** (Локальные пользователи и группы). Щелкните правой кнопкой мыши узел **Users** (Пользователи) и щелкните левой кнопкой мыши команду **New User** (Новый пользователь).
3. В диалоговом окне **New User** (Новый пользователь) введите имя интерфейса вызова по требованию центрального офиса. В данном примере — **Branch** (Филиал). Введите в текстовые поля пароль и его подтверждение. Запишите и сохраните этот пароль, потому что он вам понадобится, когда вы будете конфигурировать брандмауэр ISA филиала. Сбросьте флажок **User must change password at next logon** (Потребовать смену пароля при следующем входе в систему). Установите флажки **User cannot change password** (Запретить смену пароля пользователем) и **Password never expires** (Срок действия пароля не ограничен). Щелкните мышью кнопку **Create** (Создать).
4. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **New User** (Новый пользователь).
5. Дважды щелкните кнопкой мыши пользователь с именем **Branch** на правой панели консоли.
6. В диалоговом окне **Branch Properties** (Свойства: Branch) щелкните кнопкой мыши вкладку **Dial-in** (Профиль) выберите переключатель **Allow access** (Подключить).
7. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК.
8. Перезапустите компьютер с брандмауэром ISA.

СОВЕТ Следует применять очень сложный пароль для этих учетных записей, содержащий заглавные и строчные буквы, цифры и другие символы.

Создание сети удаленного сайта в филиале

Теперь обратимся к брандмауэру ISA филиала. Повторим те же шаги, которые выполнялись на брандмауэре ISA центрального офиса, но теперь начнем с создания сети удаленного сайта на брандмауэре филиала, представляющей IP-адреса, применяемые в сети центрального офиса.

Выполните следующие шаги для создания сети удаленного сайта в филиале. 1. Откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети).

2. Щелкните кнопкой мыши узел **Remote Sites** (Удаленные сайты) на панели до полнительных параметров. Щелкните мышью вкладку **Tasks** (Задачи) на пане ли задач. Выберите вариант **Add Remote Site Network** (Добавить сеть удален ного сайта).
3. На странице **Welcome to the New Network Wizard** (Вас приветствует мастер создания новой сети) введите имя удаленной сети в текстовое поле **Network name** (Имя сети). В этом примере — **Main.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **VPN Protocol** (VPN-протокол) выберите **Point-to-Point** Tunne ling **Protocol (PPTP)** (Сквозной туннельный протокол) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Remote Site Gateway** (Шлюз удаленного сайта) введите IP-адрес внешнего интерфейса брандмауэра ISA центрального офиса. В данном приме ре IP-адрес — **192.168.1.70,** поэтому введите это значение в текстовое поле. Щелкните мышью кнопку **Next** (Далее),
6. На странице **Remote Authentication** (Удаленная аутентификация) установите флажок **Local site can initiate connections to remote site using these cre dentials** (Локальный сайт может инициировать подключения к удаленному айту, используя следующие верительные данные). Введите имя учетной записи, создан ной вами на брандмауэре ISA центрального офиса, для разрешения доступа для VPN-шлюза филиала.

   В данном примере учетная запись пользователя названа **Branch** (имя учетной записи пользователя должно совпадать с именем интерфейса вызова по требованию в центральном офисе). Имя **Domain** (Домен) — это имя удаленного компьютера с брандмауэром ISA 2004, в данном случае, **ISALOCAL** (если удаленный брандмауэр ISA служит контроллером домена, следует использовать *имя домена* вместо имени компьютера). Введите пароль для учетной записи и подтвердите пароль, как показано на рис. 932. Щелкните мышью кнопку **Next** (Далее).

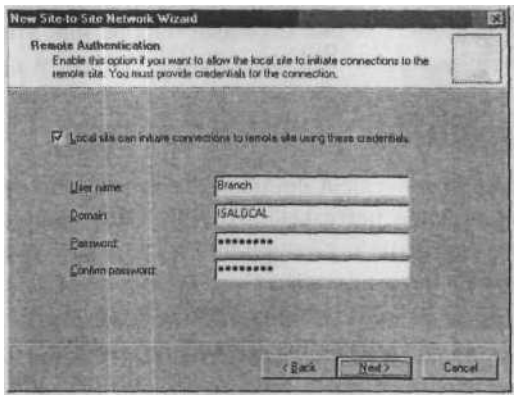


Рис. 9.32. Ввод верительных данных для доступа по телефонной линии

7. Прочтите информацию на странице Local Authentication (Локальная аутен тификация) и щелкните мышью кнопку Next (Далее).
8. Щелкните мышью кнопку Add (Добавить) в диалоговом окне Network Addresses (Сетевые адреса), введите адрес 10.0.0.0 в текстовое поле Starting address (На чальный адрес). Введите 10.0.0.255 в текстовое поле Ending address (Конеч ный адрес). Щелкните мышью кнопку ОК.
9. Щелкните мышью кнопку Next (Далее) на странице Network Addresses (Сете вые адреса).
10. Щелкните мышью кнопку Finish (Готово) на странице Completing the New Network Wizard (Завершение мастера создания новой сети).

Создание сетевого правила в филиале

Так же как в центральном офисе, мы должны создать сетевое правило, контролирующее маршрутную связь между сетями филиала и центрального офиса. Мы настроим маршрутную связь для обеспечения максимального уровня поддержки протоколов.

Выполните следующие шаги для создания сетевого правила в филиале.

1. Раскройте узел Configuration (Конфигурация) на левой панели консоли. Щелк ните кнопкой мыши узел Networks (Сети)
2. Щелкните кнопкой мыши вкладку Network Rules (Сетевые правила) на панели с дополнительной информацией. Щелкните мышью вкладку Tasks (Задачи) на панели задач. Щелкните мышью кнопку Create a New Network Rule (Создать новое сетевое правило).
3. На странице Welcome to the New Network Rule Wizard (Вас приветствует мастер создания нового сетевого правила) введите название правила в тексто вое поле Network rule name (Название сетевого правила). В данном приме ре — Branch to Main. Щелкните мышью кнопку Next (Далее).
4. На странице Network Traffic Sources (Источники сетевого трафика) щелкни те мышью кнопку Add (Добавить).
5. В диалоговом окне Add Network Enti ties (Добавить сетевые объекты) щелкните кнопкой мыши папку Networks (Сети). Дважды щелкните кнопкой мыши сеть Internal (Внутренняя). Щелкните мышью кнопку Close (Закрыть).
6. Щелкните мышью кнопку Next (Далее) на странице Network Traffic Sources (Источники сетевого трафика).
7. На странице Network Traffic Destinations (Адресаты сетевого трафика) щелк ните мышью кнопку Add (Добавить).
8. В диалоговом окне Add Network Entities (Добавить сетевые объекты) дважды щелкните кнопкой мыши сеть Main. Щелкните мышью кнопку Close.
9. Щелкните мышью кнопку Next (Далее) на странице Network Traffic Desti nations.

10. На странице **Network Relationship** (Связь сетей)выберите **Route** (Маршрутная) связь.
11. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Network Rule Wizard (Завершение** мастера создания нового сетевого прави ла). На рис. 9.33 показано новое сетевое правило.

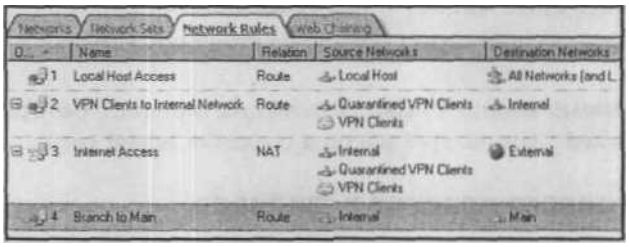


Рис. 9.33. Новое сетевое правило

Создание правил доступа в филиале

Создадим два правила доступа: разрешающее весь трафик из филиала в центральный офис и разрешающее трафик из центрального офиса в филиал.

Выполните следующие шаги для создания правил доступа, разрешающих движение всего трафика между сетями филиала и центрального офиса.

1. Щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). На па нели задач щелкните кнопкой мыши вкладку **Tasks** (Задачи). Щелкните кноп кой мыши вариант **Create New** Access **Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере — **Branch to Main.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разре шить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **All outbound traffic** (Весь исходящий трафик) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью **кнопку Next** (Далее).
5. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети), дважды щелкните мышью сеть **Internal** (Внут ренняя). Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Ис точники в правиле доступа).

8. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью сеть **Main.** Щелк ните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью **кнопку Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле **доступа).**
11. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умол чанию **All Users** (Все пользователи) и щелкните мышью **кнопку Next** (Далее).
12. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила доступа).

Второе правило доступа разрешает хостам сети центрального офиса получать доступ к сети филиала.

1. Щелкните кнопкой мыши вкладку **Tasks** (Задачи). Щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила доступа) введите название правила в текстовое поле **Rule name.** В данном примере — **Main to Branch.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **All outbound** traffic (Весь исходящий трафик) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Next** (Далее).
5. На странице **Access Rule Sources** (Источники правила доступа) щелкните мы шью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети), дважды щелкните мышью сеть **Main.** Щелкни те мышью **кнопку Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (До бавить сетевые объекты) .
8. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью сеть **Internal** (Внут- ренняя). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
11. На странице **User Sets** (Наборы пользователя) согласитесь с установкой по умол чанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).

12. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила доступа). На рис. 9-34 показана результирующая политика брандмауэра.

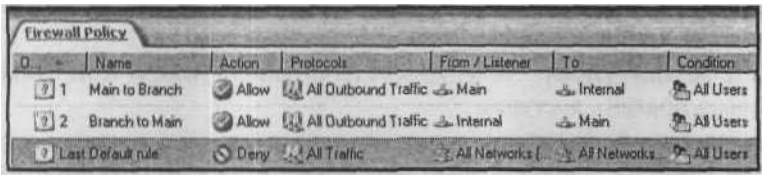


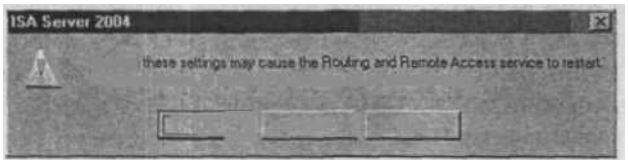
Рис. 9.34. Результирующая политика брандмауэра

Следующий шаг — разрешить доступ VPN-клиентам.

Щелкните кнопкой мыши узел **Virtual Private Network** (Виртуальная частная сеть) на левой панели консоли.

2. Щелкните кнопкой мыши вкладку **VPN Clients** (VPN-клиенты) на панели дополнительных параметров. Щелкните мышью вкладку **Tasks** (Задачи) на панели задач и выберите **Enable VPN Client Access** (Разрешить доступ VPN-клиентам).

3. Щелкните мышью кнопку ОК *в* диалоговом окне **ISA 2004,** информирующем вас о том, что сервис **Routing and Remote Access** (Маршрутизация и удаленный доступ) должен быть запущен заново (рис. 9.35).



»\ АиЛЧ
■\ If a jeddft оссигз. dl active VPN se«iom **wil be damrtnaettd**

~'jj!rj C«nc«l | Hdp

Рис. 9.35. Перезапуск сервиса **Routing and Remote Access** (Маршрутизация и удаленный доступ)

4. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
5. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Создание в филиале учетной записи VPN-шлюза для удаленного доступа по телефонной линии

Следует создать учетную запись пользователя, которую VPN-шлюз центрального офиса сможет использовать для аутентификации при установке VPN-соединения конфигурации узел-в-узел с филиалом. Имя в учетной записи пользователя должно быть таким же, как имя интерфейса вызова по требованию, созданного на машине филиала, в данном примере — **Main.**

Выполните следующие шаги для создания учетной записи, которую брандмауэр ISA 2004 будет применять для соединения с VPN-шлюзом центрального офиса. 1. Щелкните правой кнопкой мыши на рабочем столе пиктограмму **My Computer** (Мой компьютер) и выберите команду **Manage** (Управление). На консоли

2. **Computer Management** (Управление компьютером) раскройте узел **Local Users and Groups** (Локальные пользователи и группы). Щелкните правой кнопкой мыши узел **Users** (Пользователи) и щелкните левой кнопкой мыши команду **New User** (Новый пользователь).

3. В диалоговом окне **New User** (Новый пользователь) введите имя интерфейса вызова по требованию центрального офиса. В данном примере — **Main.** Введите в текстовые поля пароль и его подтверждение. Это тот же пароль, который использовался для создания сети удаленного сайта в центральном офисе. Сбросьте флажок **User must change password at next logon** (Потребовать смену пароля при следующем входе в систему). Установите флажки **User cannot change password** (Запретить смену пароля пользователем) и **Password never expires** (Срок действия пароля не ограничен). Щелкните мышью кнопку **Create** (Создать).

4. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **New User** (Но вый пользователь).

5. Дважды щелкните кнопкой мыши пользователь с именем **Main** на правой пане ли консоли.

6 В диалоговом окне **Main Properties** (Свойства: Main) щелкните кнопкой мыши вкладку **Dial-in** (Профиль) (рис. 936). Выберите переключатель **Allow access** (Подключить). Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК.

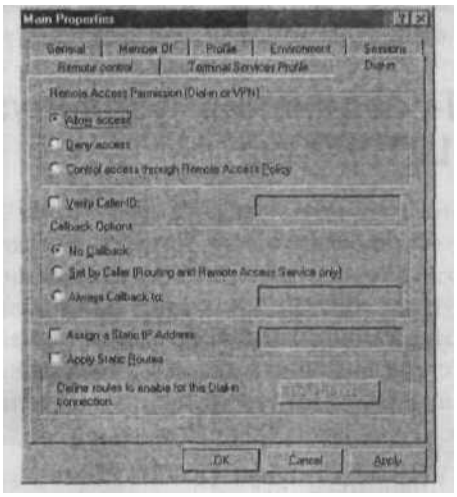


Рис. 9.36. Вкладка Dial-in (Профиль) 7.

Перезапустите компьютер о брандмауэром ISA.

Активизация каналов конфигурации узел-в-узел

Теперь, когда брандмауэры ISA центрального офиса и филиала сконфигурированы как VPN-маршрутизаторы, можно тестировать соединение конфигурации узел-в-узел, для этого выполните следующие шаги:

1. На компьютере удаленного клиента, находящегося за машиной удаленного бранд мауэра ISA 2004, щелкните мышью кнопку **Start** (Пуск), а затем команду **Run** (Выполнить).
2. В диалоговом окне **Run** (Выполнить) введите cmd в текстовое поле **Open** (Открыть) и щелкните мышью кнопку ОК.
3. Введите в окне командной строки ping -t 10.0.0.2 и нажмите клавишу <Enter>.
4. Вы увидите несколько тайм-аутов команд ping, а затем начнут возвращаться отклики на команды ping с контроллера домена в центральном офисе.
5. Выполните те же действия на контроллере домена центрального офиса, но при этом в команде ping укажите адрес **10.0.1.2.**

> СОВЕТ Если соединение конфигурации узел-в-узел заканчивается неудачей, убедитесь, что вы правильно определили назначения допустимых IP-адресов для VPN-клиентов и шлюзов. Обычная причина сбоев VPN-соединений заключается в том, что брандмауэры ISA не могут получить адрес от DHCP-сервера и нет адресов, отведенных для пула статических адресов. В этой ситуации брандмауэр ISA назначает VPN-клиентам и шлюзам IP-адреса в диапазоне автосети (autonet) (169.254.0.0/16). Если обоим шлюзам назначены адреса из этого диапазона, интерфейсы вызова по требованию обеих машин размещаются в сети с одним и тем же сетевым идентификатором, что вызывает сбой в линии связи конфигурации узел-в-узел.

Создание VPN-соединения «узел-в-узел» по протоколу L2TP/IPSec

Мы рекомендуем использовать протокол L2TP/IPSec (Layer Two Tunneling Protocol over IPSec, протокол туннелирования на втором уровне модели OSI поверх протокола IP-безопасности) как VPN-протокол для VPN-соединений конфигурации узел-в-узел. Протокол L2TP/IPSec гораздо безопаснее протокола PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол) и туннельного режима протокола IPSec. Однако для установки защищенного VPN-соединения конфигурации узел-в-узел с применением протокола L2TP/IPSec вы должны использовать сертификаты компьютера на всех VPN-шлюзах брандмауэров ISA.

Можно применить VPN-канал конфигурации узел-в-узел по протоколу PPTP, созданный нами в предыдущем разделе, разрешив брандмауэру ISA филиала доступ к Web-сайту регистрации ЦС предприятия, размещенного в сети центрального офиса.

Мы выполним следующие процедуры дл! остановки VPN-канала конфигурации узел-в-узел по протоколу L2TP/IPSec.

Разблокирование правила системна политики на брандмауэре цен-трального офиса для доступа к ЦС п] цприятия Снимем запрет с правила системной политики, разрешающего **б** индмауэру ISA соединяться из сети локального хоста (Local Host Network) со гми сетями. Несмотря на то, что это правило якобы предназначено для провер CRL (Certificate Revocation List, список аннулированных сертификатов), мы мо м использовать его для разрешения брандмауэру ISA в центральном офисе эступа к Web-сайту регистрации во внутренней сети.

Запрос и установка сертификата We сайта для брандмауэра централь-ного офиса Соединившись с Web-сай **м** регистрации, мы запросим серти-фикат Administrator, который установим хранилище сертификатов локально-го компьютера центрального офиса. Мы кже установим сертификат ЦС пред-приятия в компьютерном хранилище с тификатов Trusted Root Certification Authorities (доверенные корневые центр :ертификации) брандмауэра ISA цен-трального офиса.

Конфигурирование брандмауэра ISA ентрального офиса для использо-вания канала связи конфигурации :л-в-узел по протоколу L2TP/IPSec л >еделяющая сеть филиала, настроена Конфигурация сети удаленного сайта, с связи конфигу рации узел-в-узел. Не-на применение протокола PPTP в кана; колом L2TP/IPSec. **политики** обходимо заменить протокол PPTP про **брандмауэра филиала**

Разблокирование правила системнс как на брандмауэре ISA центрально-**для доступа к ЦС предприятия** Так: Ш системной политики, которое раз-го офиса, необходимо снять запрет с прз ила к Web-сайту регистрации в сети решит доступ сети локального хоста ф! центрального офиса. **Запрос и**

установка сертификата W **-сайта для брандмауэра филиала** Когда 1ции узел-в-узел по протоколу PPTP, будет установлен канал конфш ься к Web-сайту регистрации по этому брандмауэр ISA филиала сможет подклн вателя Administrator на брандмауэре каналу. Мы установим сертификат по сертификатов и установим сертифи-филиала в его компьютерном хранил] кат штия центрального офиса в компью-ЦС для центра сертификации пре, <oot Certification Authorities (доверен-терном хранилище сертификатов Тш? **рандмауэре** ISA филиала. ные корневые центры сертификаци .

Конфигурирование брандмауэра ISA ^л **лиала для использования канала связи конфигурации узел-в-узел по протоколу L2TP/IPSec** Сеть **удален-ного** сайта, представляющая сеть центрального офиса, должна быть настроена для применения протокола L2TP/IPSec вместо протокола PPTP в канале конфи-гурации узел-в-узел.

- **Установка соединения конфигурации узел-в-узел по протоколу IPSec** После того, как будут установлены сертификаты и внесены изменения в конфигурации брандмауэров ISA, мы инициируем канал конфигурации узел-в-узел и увидим соединение по протоколу L2TP/IPSec в узле мониторинга брандмауэра ISA.
- **Настройка секретных ключей (Prc-shared keys) для VPN-каналов конфигурации узел-в-узел по протоколу L2TP/IPSec** Это не обязательная процедура. Хотя, предпочтительней использование всех сертификатов для аутентификации компьютеров, ясно, что это не всегда возможно. Мы рассмотрим процедуры, которые вы можете применять для поддержки аутентификации секретными ключами (pre-shared key) в ваших VPN-каналах конфигурации узел-в-узел по протоколу L2TP/IPSec.

Разблокирование правила системной политики на брандмауэре центрального офиса для доступа к ЦС предприятия

Брандмауэр ISA 2004 по умолчанию почти закрыт, и очень ограниченный набор протоколов и сайтов доступен для исходящих подключений с брандмауэра ISA сразу после его установки. Что касается любых других коммуникаций, проходящих через брандмауэр ISA, для доступа к *любой* сети или хосту в сети необходимы разрешающие правила доступа. Нам потребуется конфигурировать брандмауэр ISA в центральном офисе с помощью правила доступа, разрешающего HTTP-доступ к Web-сайту регистрации. Можно создать правило доступа или снять запрет с правила системной политики. Создание правила доступа, разрешающего доступ из сети локального хоста к ЦС предприятия с помощью только HTTP-протокола, было бы более безопасным вариантом, но легче разблокировать правило системной политики. В данном примере мы снимем запрет с правила системной политики, разрешающего доступ брандмауэра к Web-сайту регистрации.

Выполните следующие шаги для разблокирования правила системной политики на брандмауэре центрального офиса.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. Щелкните правой кнопкой мыши узел **Firewall Policy** (Политика брандмауэра). Укажите команду **View** (Просмотр) и щелкните левой кнопкой мыши команду **Show** System **Policy Rules** (Показать правила системной политики).
3. В списке правил системной политики дважды щелкните кнопкой мыши строку **Allow HTTP from ISA Server to all networks (for CRL downloads)** (Разрешить HTTP с ISA Server ко всем сетям для загрузки списка аннулированных сертификатов CRL). Это правило системной политики #2б.

4. В диалоговом окне **System Policy Editor** (Редактор системной политики) на вкладке **General** (Общие) установите флажок **Enable** (Разрешить), как показа но на рис. 9-37. Щелкните мышью кнопку ОК.
5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку ОК в диалоговом окне **Apply New** Configuration (Применить новую конфигурацию).
7. Щелкните мышью кнопку **Show/Hide System Policy Rules** (Показать/скрыть правила системной политики) (крайнюю справа на инструментальной панели консоли MMC), чтобы скрыть системную политику (рис. 9.38).

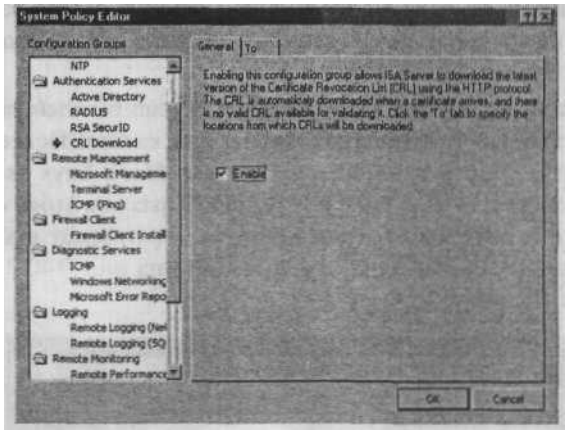


Рис. 9.37. Конфигурирование системной политики

Рис. 9.38. Кнопка Show/Hide System Policy Rules (Показать/скрыть правила системной политики)

Запрос и установка сертификата Web-сайта для брандмауэра центрального офиса

Теперь следует запросить сертификат с Web-сайта регистрации ЦС предприятия. После получения сертификата мы скопируем его в хранилище сертификатов **Trusted Root Certification Authorities** (Доверенные коневые центры сертификации) брандмауэра ISA.

Выполните следующие шаги на брандмауэре ISA центрального офиса для за-проса и инсталляции сертификатов. 1. Откройте обозреватель Internet Explorer. В строке **Address** (Адрес) введите **http://**

10.0.0.2/certsrv (где 10.0.0.2 — IP-адрес центра сертификации предприятия), щелкните мышью кнопку ОК.

В диалоговом окне **Enter Network Password** (Введите сетевой пароль) введите **Administrator** в текстовое поле **User Name** (Имя пользователя) и пароль администратора в текстовое поле **Password** (Пароль). Щелкните мышью кнопку ОК.

3. В диалоговом окне безопасности Internet Explorer щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Trusted Sites** (Доверенные сайты) щелкните мышью **Add and Close** (Добавить и закрыть).

4. Щелкните переключатель **Request a Certificate** (Запросить сертификат) на странице **Welcome** (Добро пожаловать).

На странице **Request a Certificate** (Запросить сертификат) щелкните мышью переключатель **Advanced certificate request** (Расширенный запрос сертификата).

6. На странице **Advanced Certificate Request** (Расширенный запрос сертификата) установите переключатель **Create and submit a request to this CA** (Создать и представить запрос данному ЦС).

7. На странице **Advanced Certificate Request** (Расширенный запрос сертификата) выберите сертификат **Administrator** из списка **Certificate Template** (Шаблон сертификата) (рис. 9-39). Сбросьте флажок **Mark keys as exportable** (Пометить ключи как экспортируемые). Установите флажок **Store certificate in the local computer certificate store** (Сохранить сертификат в хранилище сертификатов локального компьютера), как показано на рис. 940. Щелкните мышью кнопку **Submit (Принять).**

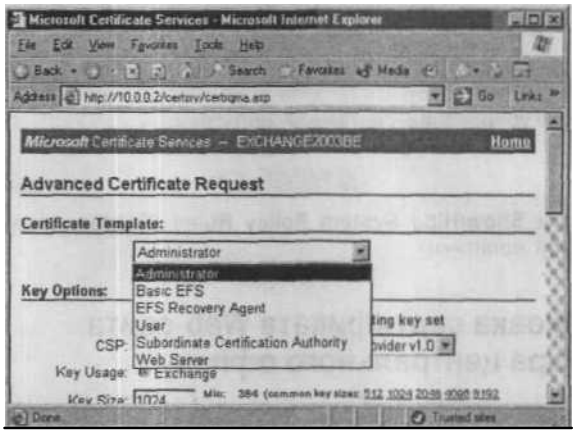


Рис. 9.39. Страница **Advanced Certificate Request** (Расширенный запрос сертификата)

8. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).

9. На странице **Certificate Issued** (Выданные сертификаты) щелкните мышью кнопку **Install this certificate** (Установить данный сертификат).

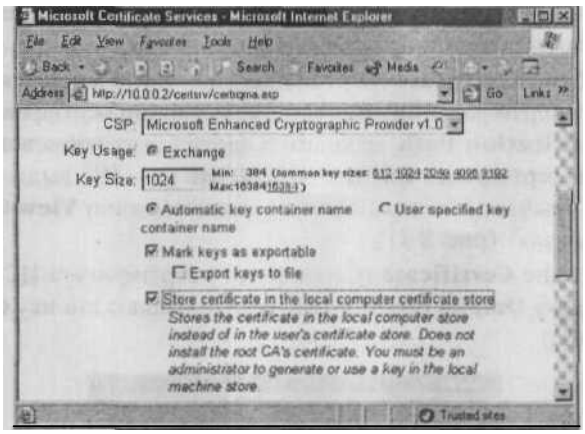


Рис. 9.40. Флажок **Store Certificate in the Local Computer Certificate Store** (Сохранить сертификат в хранилище сертификатов локального компьютера)

10. Щелкните мышью кнопку Yes (Да) в диалоговом окне Potential Scripting Viola tion (Возможное нарушение сценариев).
11. Закройте обозреватель после просмотра страницы Certificate Installed (Уста новленный сертификат).
12. Щелкните мышью кнопку Start (Пуск) и затем команду Run. Введите mmc в текстовое поле Open (Открыть) и щелкните мышью кнопку ОК.
13. В окне консоли Console! щелкните мышью пункт меню File (Файл), а затем команду Add/Remove Snap-in (Добавить/Удалить оснастку).
14. Щелкните мышью кнопку Add (Добавить) в диалоговом окне Add/Remove Snap-in (Добавить/Удалить оснастку).
15. Выберите строку Certificates (Сертификаты) из списка Available Standalone Snap-ins (Доступные изолированные оснастки) в диалоговом окне Add Standa lone Snap-in (Добавить изолированную оснастку). Щелкните мышью кнопку Add (Добавить).
16. Выберите вариант Computer account (Учетная запись компьютера) на странице Certificates snap-in (Оснастка Сертификаты).
17. Выберите вариант Local computer (Локальный компьютер) на странице Select Computer (Выберите компьютер).
18. Щелкните мышью кнопку Close (Закрыть) в диалоговом окне Add Standalone Snap-in (Добавить изолированную оснастку).
19. Щелкните мышью кнопку ОК в диалоговом окне Add/Remove Snap-in (Доба вить/Удалить оснастку).
20. На левой панели консоли раскройте элемент Certificates (Local Computer) (Сертификаты, локальный компьютер) и папку Personal (Личные). Щелкните

кнопкой мыши **\Personal\Certificates.** Дважды щелкните кнопкой мыши сертификат **Administrator** на правой панели консоли.

21. В диалоговом окне **Certificate** (Сертификат) щелкните мышью вкладку **Certification Path** (Путь сертификации). На вершине иерархии сертификатов, показанной в области **Certification Path,** находится сертификат корневого ЦС. Щелкните кнопкой мыши сертификат **EXCHANGE2003BE** (это ЦС, выдавший сертификат Administrator) в начале списка. Щелкните мышью кнопку **View Certificate** (Просмотр сертификата) (рис. 9.41).
22. В диалоговом окне **Certificate** (Сертификат) сертификата ЦС щелкните кнопкой мыши вкладку **Details** (Состав). Щелкните мышью кнопку **Copy to File** (Копировать в файл).

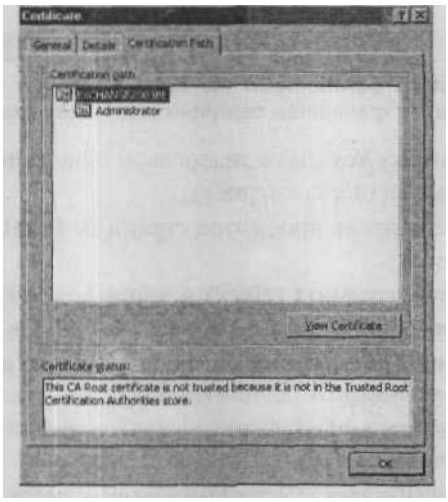


Рис. 9.41. Вкладка Certificate Path (Путь сертификации)

23. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Export Wizard** (Вас приветствует мастер экспорта сертификатов).
24. На странице **Export File Format** (Формат экспортируемого файла) выберите переключатель **Cryptographic Message Syntax Standard - PKCS *1 Certificates (.P7B)** (Стандарт Cryptographic Message Syntax — сертификаты PKCS *7 (.P7B)) и щелкните мышью кнопку **Next** (Далее).
25. На странице **File to Export** (Имя файла экспорта) введите **c:\cacert** в текстовое поле **File name** (Имя файла). Щелкните мышью кнопку **Next** (Далее).
26. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certificate Export Wizard** (Завершение работы мастера экспорта сертификатов).
27. Щелкните мышью кнопку ОК в диалоговом окне **Certificate Export Wizard** (Мастер экспорта сертификатов).

28. Щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат). Снова щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат).
29. На левой панели консоли раскройте папку **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации) и щелкните кнопкой мыши папку **Certificates** (Сертификаты). Щелкните правой кнопкой мыши на левой панели узел **\Trusted Root Certification Authorities\Certificates.** Укажите мышью на команду **All Tasks** (Все задачи) и щелкните левой кнопкой мыши команду **Import** (Импорт).
30. Щелкните мышью кнопку Next (Далее) на странице **Welcome to the Certificate Import Wizard** (Вас приветствует мастер импорта сертификатов).
31. На странице **File to Import** (Импортируемый файл) воспользуйтесь кнопкой **Browse** (Обзор) для указания сертификата ЦС, который вы сохранили на ло кальном жестком диске и щелкните мышью кнопку **Next** (Далее).
32. На странице **Certificate Store** (Хранилище сертификатов) согласитесь с уста новками по умолчанию и щелкните мышью кнопку **Next** (Далее).
33. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certifi cate Import Wizard** (Завершение работы мастера импорта сертификатов).
34. Щелкните мышью кнопку ОК в диалоговом окне **Certificate Import Wizard** (Мастер импорта сертификатов), информирующем вас об успешном импорти-ровании сертификата.

Конфигурирование брандмауэра ISA центрального офиса для использования канала связи конфигурации узел-в-узел по протоколу L2TP/IPSec

Сеть удаленного сайта в центральном офисе, представляющая сеть филиала, настроена на применение в соединении конфигурации узел-в-узел протокола PPTP. Необходимо заменить его протоколом L2TP/IPSec. Выполните следующие шаги для внесения изменений.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) рас кройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети) на левой панели консоли.
2. На панели дополнительных параметров выберите вкладку **Remote Sites** (Уда ленные сайты) узла **Virtual Private Networks (VPN).** Дважды щелкните кноп кой мыши элемент сети удаленного сайта с именем **Branch.**
3. В диалоговом окне **Branch Properties** (Свойства Branch) выберите вариант **L2TP/IPSec (provides a highly secure connection method)** (Предоставляет наибо лее защищенный способ соединения). Щелкните мышью кнопку **Apply** (При менить), а затем кнопку ОК.

4. *Не* применяйте пока новую политику брандмауэра. Она может разорвать нашу линию связи конфигурации узел-в-узел по протоколу PPTP, которая нужна до тех пор, пока мы не установим сертификат на брандмауэре ISA филиала. После конфигурирования брандмауэра ISA филиала мы сможем внести изменения в системную политику в центральном офисе.

Разблокирование правила системной политики брандмауэра филиала для доступа к ЦС предприятия

Теперь сосредоточимся на брандмауэре ISA филиала. Необходимо разблокировать правило системной политики, разрешающее брандмауэру филиала соединяться с ЦС предприятия в сети центрального офиса.

Выполните следующие шаги для активизации правила системной политики на брандмауэре филиала.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. Щелкните правой кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), укажите команду **View** (Просмотр) и щелкните левой кнопкой мыши команду **Show System Policy Rules** (Показать правила системной политики).
3. В списке правил системной политики дважды щелкните кнопкой мыши строку **Allow HTTP from ISA Server to all networks (for CRL downloads)** (Разрешить HTTP с ISA Server ко всем сетям, для загрузки списка CRL). Это правило системной политики #2б.
4. В диалоговом окне **System Policy Editor** (Редактор системной политики) (рис. 9.42), на вкладке **General** (Общие) установите флажок **Enable** (Разрешить). Щелкните мышью кнопку OK.

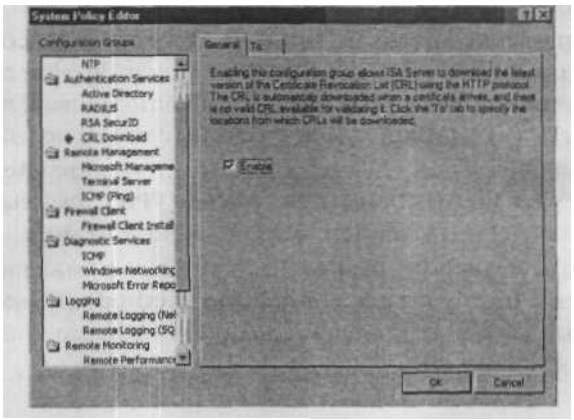


Рис. 9.42. Настройка системной политики

5. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
6. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Запрос и установка сертификата Web-сайта для брандмауэра филиала

Теперь необходимо запросить сертификат для брандмауэра филиала. После получения сертификата скопируем сертификат ЦС в компьютерное хранилище сертификатов **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации).

Выполните следующие шаги на брандмауэре ISA центрального офиса для запроса и установки сертификатов.

1. Откройте обозреватель Internet Explorer. В строке **Address** (Адрес) введите **http://10.0.0.2/certsrv** и щелкните мышью кнопку ОК.
2. В диалоговом окне **Enter Network Password** (Введите **сетевой** пароль) введите **Administrator** в текстовое поле **User Name** (Имя пользователя) и пароль администратора в текстовое поле **Password** (Пароль). Щелкните мышью кнопку ОК.
3. В диалоговом окне безопасности Internet Explorer щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Trusted Sites** (Доверенные сайты) щелкните мышью **Add and Close** (Добавить и закрыть).
4. Щелкните переключатель **Request a Certificate** (Запросить сертификат) на странице **Welcome** (Добро пожаловать).
5. На странице **Request a Certificate** (Запросить сертификат) щелкните мышью переключатель **Advanced certificate request** (Расширенный запрос сертификата).
6. На странице **Advanced Certificate Request** (Расширенный запрос сертификата) установите переключатель **Create and submit я request to this CA** (Создать и представить запрос данному ЦС).
7. На странице **Advanced Certificate Request** (Расширенный запрос сертификата) выберите сертификат **Administrator** из списка **Certificate Template** (Шаблон сертификата). Сбросьте флажок **Mark keys as exportable** (Пометить ключи как экспортируемые). Установите флажок **Store certificate in the local computer certificate store** (Сохранить сертификат в хранилище сертификатов локального компьютера) (рис. 9.40). Щелкните мышью кнопку **Submit** (Принять).
8. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).
9. На странице **Certificate Issued** (Выданные сертификаты) щелкните мышью кнопку **Install this certificate** (Установить данный сертификат).
10. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев).

11. Закройте обозреватель после просмотра страницы **Certificate Installed** (Уста новленный сертификат).
12. Щелкните мышью кнопку **Start** (Пуск) и затем команду **Run** (Запустить). Вве дите mmc в текстовое поле **Open** (Открыть) и щелкните мышью кнопку ОК.
13. В окне консоли **Consolel** щелкните мышью пункт меню **File** (Файл), а затем команду **Add/Remove Snap-in** (Добавить/Удалить оснастку).
14. Щелкните мышью кнопку **Add** (Добавить) в диалоговом окне **Add/Remove Snap-in** (Добавить/Удалить оснастку).
15. Выберите строку **Certificates** (Сертификаты) из списка **Available Standalone** Snap-ins (Доступные изолированные оснастки) в диалоговом окне **Add Standa lone Snap-in** (Добавить изолированную оснастку). Щелкните мышью кнопку **Add** (Добавить).
16. Выберите вариант **Computer account** (Учетная запись компьютера) на странице **Certificates snap-in** (Оснастка Сертификаты).
17. Выберите вариант **Local computer** (Локальный компьютер) на странице **Select Computer** (Выберите компьютер).
18. Щелкните мышью кнопку **Close** (Закрыть) в диалоговом окне **Add Standalone Snap-in** (Добавить изолированную оснастку).
19. Щелкните мышью кнопку ОК в диалоговом окне **Add/Remove Snap-in** (Доба вить изолированную оснастку).
20. На левой панели консоли раскройте элемент **Certificates (Local Computer)** (Сертификаты, локальный компьютер) и папку **Personal** (Личные). Щелкните кнопкой мыши **\Personal\Certificates.** Дважды щелкните кнопкой мыши сер тификат **Administrator** на правой панели консоли.
21. В диалоговом окне **Certificate** (Сертификат) щелкните мышью вкладку **Certifica tion Path** (Путь сертификации). На вершине иерархии сертификатов, показанной в области **Certification Path** (Путь сертификации), находится сертификат кор невого ЦС. Щелкните кнопкой мыши сертификат EXCHANGE2003BE в начале списка. Щелкните мышью кнопку **View Certificate** (Просмотр сертификата).
22. В диалоговом окне **Certificate** (Сертификат) сертификата ЦС щелкните кноп кой мыши вкладку **Details** (Состав). Щелкните мышью кнопку **Copy to File** (Ко пировать в файл).
23. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Export Wizard** (Вас приветствует мастер экспорта сертификатов).
24. На странице **Export File Format** (Формат экспортируемого файла) выберите переключатель **Cryptographic Message Syntax Standard - PKCS *7 Certificates (.P7B)** (Стандарт Cryptographic Message Syntax — сертификаты PKCS *7 (P7B)) и щелкните мышью кнопку **Next** (Далее).
25. На странице **File to Export** (Имя файла экспорта) введите **c:\cacert** в тексто вое поле **File name** (Имя файла). Щелкните мышью кнопку **Next** (Далее).

26. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certificate Export Wizard** (Завершение работы мастера экспорта сертификатов).
27. Щелкните мышью кнопку ОК в диалоговом окне **Certificate Export Wizard** (Мастер экспорта сертификатов).
28. Щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат). Снова щелкните мышью кнопку ОК в диалоговом окне **Certificate** (Сертификат).
29. На левой панели консоли раскройте папку **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации) и щелкните кнопкой мыши папку **Certificates** (Сертификаты). Щелкните правой кнопкой мыши на левой панели узел **\Trusted Root Certification Authorities\Certificates.** Укажите мышью на команду **All Tasks** (Все задачи) и щелкните левой кнопкой мыши команду **Import** (Импорт).
30. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Certificate Import Wizard** (Вас приветствует мастер импорта сертификатов).
31. На странице **File to Import** (Импортируемый файл) воспользуйтесь кнопкой **Browse** (Обзор) для указания сертификата ЦС, который вы сохранили на локальном жестком диске, и щелкните мышью кнопку **Next** (Далее).
32. На странице **Certificate Store** (Хранилище сертификатов) согласитесь с установками по умолчанию и щелкните мышью кнопку **Next** (Далее).
33. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the Certificate Import Wizard** (Завершение работы мастера импорта сертификатов).
34. Щелкните мышью кнопку ОК в диалоговом окне **Certificate Import Wizard** (Мастер импорта сертификатов), информирующем вас об успешном импортировании сертификата.

Конфигурирование брандмауэра ISA центрального офиса для использования канала связи конфигурации узел-в-узел по протоколу L2TP/IPSec

Сеть удаленного сайта на брандмауэре ISA филиала, представляющая сеть центрального офиса, настроена на применение в соединении конфигурации узел-в-узел протокола PPTP. Необходимо изменить его на протокол L2TP/IPSec. Для внесения изменений выполните следующие шаги.

1. На консоли управления **Microsoft Internet Security and Acceleration Server** 2004 (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети) на левой панели консоли.
2. На панели дополнительных параметров выберите вкладку **Remote Sites** (Удаленные сайты) узла **Virtual Private Networks (VPN).** Дважды щелкните кнопкой мыши элемент сети удаленного сайта с именем **Main.**

3. В диалоговом окне **Branch Properties** (Свойства Branch) выберите вариант **L2TP/IPSec (provides a highly secure connection method)** (Предоставляет наибо лее защищенный способ соединения). Щелк ните мышью кнопку **Apply** (При менить), а затем кнопку OK.
4. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
5. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
6. Теперь вы можете сохранить изменения в политике брандмауэра в центральном офисе.

Установка VPN-соединения конфигурации узел-в-узел по протоколу L2TP/IPSec

Проверим, **функционирует** ли VPN-соединение **конфигурации** узел-в-узел по протоколу L2TP/IPSec.

1. Сначала необходимо перезапустить **Routing and Remote Access Service** (Сер вис маршрутизации и удаленного доступа) на обоих брандмауэрах ISA, для того чтобы он распознал сертификаты.
2. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) рас кройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Moni toring** (Мониторинг).
3. В узле **Monitoring** (Мониторинг) щелкните кнопкой мыши вкладку **Services** (Сервисы). Щелкните правой кнопкой мыши сервис **Routing and Remote Access Service** (Сервис маршрутизации и удаленного доступа) и левой кнопкой мыши щелкните команду **Stop** (Остановить).
4. Когда сервис будет остановлен, снова щелкните по нему правой кнопкой мыши и выберите команду **Start** (Запустить).
5. С хоста в сети филиала с помощью команды ping свяжитесь с контроллером домена в центральном офисе.
6. Когда вы получите отклики на команду ping, перейдите на брандмауэр ISA фи лиала и откройте консоль управления **Microsoft Internet Security and Accele ration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004), раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Monitoring** (Мониторинг).
7. В узле **Monitoring** (Мониторинг) щелкните кнопкой мыши вкладку **Sessions** (Сеансы связи), щелкните правой кнопкой мыши любой из заголовков столбцов и затем левой кнопкой строку **Application Name** (Имя приложения) (рис. 9.43).

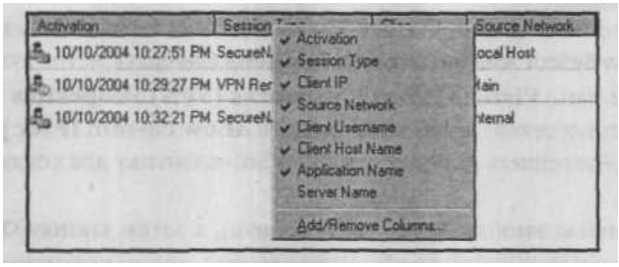


Рис. 9.43. Вставка столбца Application Name (Имя приложения)

8. В столбце **Application Name** (Имя приложения) вы увидите установленное соединение по протоколу L2TP/IPSec (рис. 9.44).

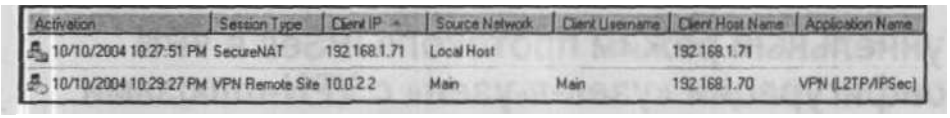


Рис. 9.44. Отображение соединения L2TP/IPSec

Настройка секретных ключей для VPN-каналов конфигурации узел-в-узел по протоколу L2TP/IPSec

В предыдущем примере мы описали процедуры, необходимые для создания канала конфигурации узел-в-узел по протоколу L2TP/IPSec с использованием сертификатов для аутентификации компьютеров. Если у вас еще не установлена инфраструктура открытого ключа (PKI) или вы не планируете реализацию инфраструктуры сертификатов, можно применить секретные ключи (pre-shared keys) для подтверждения подлинности компьютера-ком по нента установки соединения по протоколу L2TP/IPSec. Этот метод обеспечивает большую защищенность соединения по сравнению с туннельным режимом протокола IPSec в сочетании с секретными ключами, потому что для соединения по протоколу L2TP/IPSec сохраняется необходимость подтверждения подлинности пользователя.

Выполним следующие шаги на обоих брандмауэрах ISA, *в* центральном офисе и филиале, для включения применения секретных ключей (pre-shared keys) в VPN-соединение конфигурации узел-в-узел.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networking (VPN)** (Виртуальные частные сети) на левой панели консоли.
2. В узле **Virtual Private Networking (VPN)** (Виртуальные частные сети) щелк ните мышью вкладку **VPN Clients** (VPN-клиенты) на панели с дополнительны ми параметрами.

3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач. Щелкните мышью ссылку **Select Authentication Methods** (Выбрать метод аутентификации).
4. В диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства вир туальных частных сетей) установите флажок **Allow custom IPSec policy for L2TP connection** (Разрешить настраиваемую IPSec-политику для соединения по про токолу L2TP).
5. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK.
6. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
7. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Туннельный режим протокола IPSec в VPN конфигурации «узел-в-узел» с VPN-шлюзами

Одно из основных усовершенствований брандмауэра ISA Server 2004 по сравнению с ISA Server 2000 — возможность его конфигурирования для применения туннельного режима протокола IPSec в VPN-соединениях конфигурации узел-в-узел. Большинство VPN-шлюзов сторонних фирм-разработчиков требует использования туннельного режима протокола IPSec в VPN-соединениях этого типа. Было очень трудно найти VPN-шлюз сторонней организации, способный функционировать с ISA Server 2000, а в новом брандмауэре ISA можно установить связь в туннельном режиме протокола IPSec почти с любым VPN-шлюзом сторонних разработчиков.

Поскольку сегодня на рынке представлен целый ряд VPN-шлюзов сторонних фирм, невозможно подробно описать, как конфигурировать брандмауэр ISA для соединения с каждым из этих устройств. К счастью, корпорация Microsoft опубликовала полный набор документов о способах соединения брандмауэра ISA с рядом популярных VPN-шлюзов. Во время написания книги существовали документы о способах соединения брандмауэра ISA со следующими VPN-шлюзами:

- Cisco PIX;
- Astaro Linux;
- SmoothWall Express;
- непатентованные шлюзы сторонних фирм.

Вы можете найти эти документы и дополнительную информацию на сайте документации по ISA 2004 VPN корпорации Microsoft по адресу http://www.microsoft.com/isaserver/techinfo/guidance/2004/vpn.asp.

Использование системы RADIUS для VPN-аутентификации и политики удаленного доступа

Мы предпочитаем не соединять внешние (front-end) брандмауэры ISA с пользовательским доменом. Причина в том, что сегменты сети между внешним брандмауэром ISA и внутренними брандмауэрами представляют собой неаутентифицированные DMZ-сегменты (или сегменты сети периметра), и мы хотим избежать передачи информации домена через эти сегменты насколько это возможно.

Если брандмауэр ISA — не член пользовательского домена, следует использовать механизм, отличный от предлагаемого ОС Windows для подтверждения подлинности и полномочий пользователей домена. Брандмауэр ISA может аутентифицировать VPN-пользователей с помощью сервиса RADIUS (Remote Access Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя). RADIUS-протокол позволяет брандмауэру ISA 2004 пересылать верительные данные пользователя с RADIUS-сервера во внутренней сети. RADIUS-сервер отправляет запрос для подтверждения подлинности на серверы аутентификации, такие как контроллер домена службы Active Directory. Реализация системы RADIUS корпорации Microsoft — Internet Authentication Service (IAS) (сервис интернет-аутентификации).

Помимо аутентификации пользователей IAS-сервер можно использовать для централизации политики удаленного доступа. Например, если под вашим административным контролем находится шесть брандмауэров ISA/VPN-серверов, вы можете применять одну и ту же политику удаленного доступа на всех этих машинах, создав политику на IAS-сервере в вашей сети.

Брандмауэр ISA может работать не только с IAS, он поддерживает все типы RADIUS-серверов. Но IAS-сервер корпорации Microsoft включен во все программные продукты семейств Windows 2000 and Windows Server 2003, что делает очень удобным его применение в любом центре Microsoft.

В этом разделе мы обсудим процедуры, требуемые для включения RADIUS-аутентификации и политики удаленного доступа RADIUS на VPN-клиентах. Выполним следующие процедуры:

- конфигурирование IAS Server;
- создание политики удаленного доступа VPN-клиентов;
- включение VPN Server на брандмауэре ISA Server 2004 и настройка RADIUS-подДСрЖКИ;
- создание правила доступа VPN-клиента;
- установка подключения VPN-клиента по протоколу PPTP.

Конфигурирование сервера сервисов интернет-аутентификации (RADIUS)

Если на ваших машинах во внутренней сети, работающих под управлением ОС Windows 2000 или Windows Server 2003, до сих пор не установлен IAS-сервер, это можно сделать сейчас с помощью апплета панели управления **Add/Remove Programs** (Установка и удаление программ). Необходимо конфигурировать IAS-сервер для связи с Active Directory, а затем предоставить инструкции IAS-серверу по совместной работе с компьютером брандмауэра ISA 2004/VPN-серВера. В данном примере IAS-сервер установлен на контроллере домена во внутренней сети (EXCHANGE2003BE).

Выполните следующие шаги для настройки IAS-сервера.

1. Щелкните мышью кнопку **Start** (Пуск), укажите строку **Administrative Tools** (Администрирование) и щелкните кнопкой мыши оснастку **Internet Authentication Services** (Службы интернет-аутентификации).
2. На консоли **Internet Authentication Services** (Службы интернет-аутентификации) щелкните правой кнопки мыши узел **Internet Authentication Service (Local)** (Службы интернет-аутентификации, локальные) на левой панели консоли. Щелкните левой кнопкой мыши команду **Register Server in Active Directory** (Зарегистрировать сервер в Active Directory).
3. Эта установка позволяет IAS-серверу аутентифицировать пользователей в домене Active Directory. Щелкните мышью кнопку ОК в диалоговом окне **Register Internet Authentication Server in Active Directory** (Регистрация сервера интернет-аутентификации в Active Directory).
4. Щелкните мышью кнопку ОК в диалоговом окне **Server registered:** (Зарегистрированный сервер). Это окно информирует о том, что IAS-сервер был зарегистрирован в конкретном домене, и если вы захотите, чтобы этот IAS-сервер считывал пользовательские свойства вызовов по телефонной линии из других доменов, необходимо ввести этот сервер в группу **RAS/IAS Server Group** в этих доменах. Это автоматически помещает компьютер в одноименную группу службы Active Directory. Если вы хотите зарегистрировать сервер в другом домене, вы должны поместить его в группу серверов RAS (remote access service, сервис удаленного доступа) и IAS в этом домене или применить команду netsh ras add registeredserver Domain IASServer.
5. Щелкните правой кнопкой мыши узел **RADIUS Clients** (RADIUS-клиенты) на левой панели консоли и левой кнопкой мыши команду **New RADIUS Client** (Новый RADIUS-клиент).
6. В диалоговом окне New **RADIUS Client** (Новый RADIUS-клиент) наберите в текстовом поле **Friendly name** (дружественное имя) брандмауэра ISA. Можно использовать любое понравившееся имя. В данном примере мы введем имя DNS-хоста для брандмауэра ISA — **ISALOCAL.** Введите или полностью определенное

доменное имя (FQDN), или IP-адрес брандмауэра ISA 2004/VPN-сер Вера в диалоговом окне **Client address (IP or DNS)** (Адрес клиента (IP or DNS)). Не вводите FQDN, если 1Радрес внутреннего интерфейса вашего брандмауэра ISA не зарегистрирован на вашем внутреннем DNS-сервере. Можно воспользоваться кнопкой **Verify** (Проверить) для того, чтобы выяснить, может ли IAS-сервер разрешить (Преобразовать) FQDN. Щелкните мышью кнопку **Next** (Далее). 7. На странице **Additional Information** (Дополнительная информация) в раскрывающемся списке оставьте выбранным элемент **RADIUS Standard** (Стандарт RADIUS). Ваш брандмауэр ISA будет использовать эту установку. Введите сложный пароль в текстовое поле **Shared secret** (Сложный пароль) и подтвердите его в текстовом поле **Confirm shared secret** (Подтверждение пароля). Пароль должен представлять собой сложную строку, состоящую из заглавных и строчных букв, цифр и небуквенных символов. Установите флажок **Request must contain the Message Authenticator attribute** (Запрос должен содержать атрибут аутентификатора сообщения). Этот параметр повышает защищенность RADIUS-сообщений, пересылаемых между брандмауэром ISA *и* IAS-серверами. Щелкните мышью кнопку **Finish** (Готово) (рис. 9.45).

ВНИМАНИЕ! Пароль должен быть длинным и сложным. Мы советуем применять пароли не короче 20 символов, содержащие смесь заглавных и строчных букв, чисел и других символов.

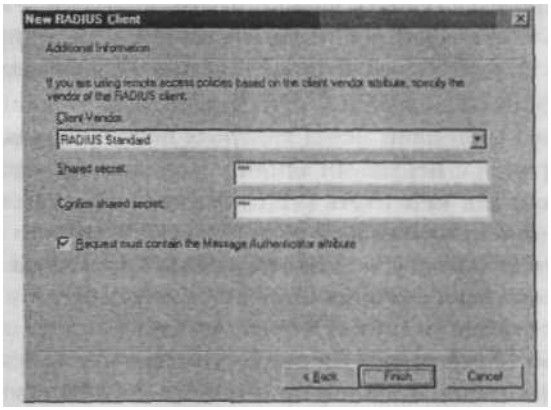


Рис 9.45. Ввод пароля

Создание политики удаленного доступа VPN-клиентов

Теперь можно сформировать политику удаленного доступа на IAS-сервере. Эти политики, настроенные на IAS-сервере, применяются к соединениям VPN-клиентов, устанавливаемым с брандмауэром ISA, когда брандмауэр сконфигурирован для использования RADIUS-аутентификации и политики и настроен как RADIUS-кли-

ент. К счастью, в ОС Windows Server 2003 у IAS-сервера есть Remote Access Policy Wizard (Мастер создания политики удаленного доступа), облегчающий создание политики удаленного доступа для VPN-клиента.

Выполните следующие шаги для создания политики удаленного доступа для VPN-клиента на IAS-сервере.

1. На консоли **Internet Authentication Service** (Сервис интернет-аутентификации) щелкните правой кнопкой мыши узел **Remote Access Policies** (Политики удаленного доступа) и затем левой кнопкой мыши команду **Access Policy** (Политика доступа).
2. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the New Remote Access Policy Wizard** (Вас приветствует мастер создания новой политики удаленного доступа).
3. На странице **Policy Configuration Method** (Метод конфигурирования политики) выберите вариант **Use the wizard to set up a typical policy for a common scenario** (Использовать мастер для установки типичной политики в общем сценарии). В текстовое поле **Policy name** (Имя политики) введите имя политики. В данном примере — **VPN Access Policy.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Access Method** (Метод доступа) выберите вариант **VPN.** Эта политика применяется во всех VPN-соединениях. Существует возможность создать отдельные политики для VPN-каналов связи по протоколам PPTP и L2TP/IPSec. Но для этого вам придется вернуться на предыдущую страницу мастера и сформировать две пользовательские политики. В этом примере мы применим одну и ту же политику ко всем VPN-соединениям. Щелкните мышью кнопку **Next** (Далее).
5. Вы можете предоставить доступ к VPN-серверу, базирующийся на пользователях или группах. Наилучший метод контроля доступа основан на группах, поскольку он сопряжен с меньшими административными затратами. Можно создать группу, такую как **VPN Users** (VPN-пользователи), и разрешить им доступ или разрешить доступ всем вашим пользователям. В данном примере мы выберем вариант **Group** (Группа) и щелкнем мышью кнопку **Add** (Добавить). На экране появится окно **Select Groups** (Выбрать группы). Введите имя группы в поле **Enter the object name to select** (Введите имя выбранного объекта) и щелкните мышью кнопку **Check names** (Проверить имена), чтобы подтвердить правильность введенного имени. В данном примере используйте группу **Domain Users** (Пользователи домена). Щелкните мышью кнопку ОК в диалоговом окне **Select Groups** (Выбрать группы) и кнопку **Next** (Далее) в диалоговом окне **User or Group Access** (Доступ пользователей или групп).
6. На странице **Authentication Methods** (Методы аутентификации) выберите методы аутентификации пользователей, которые вы хотите разрешить. Можно разрешить и **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** (Протокол проверки подлинности запроса-подтверждения Microsoft версии 2), и **Extensible Authentication Protocol (EAP)** (Наращиваемый протокол аутентификации).

Оба варианта подтверждения подлинности безопасны, поэтому мы установим оба флажка: **Extensible Authentication Protocol (EAP)** и **Microsoft Encrypted Authentication version 2 (MS-CHAPv2).** Щелкните кнопкой мыши стрелку, направленную вниз, в раскрывающемся списке **Type (based on method of access and network configuration)** (Тип, основанный на методе доступа и конфигурации сети) и выберите элемент списка **Smart Card or other certificate** (Смарт-карта или другой сертификат), затем щелкните мышью кнопку **Configure** (Настроить) (рис. 946). В диалоговом окне **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата) выберите сертификат, который сервер будет использовать для собственной идентификации в соединениях VPN-клиентов. Самоподписанный (self-signed) сертификат появляется в раскрывающемся списке **Certificate issued to** (Сертификат, выданный). Он будет применяться для подтверждения подлинности сервера, когда VPN-клиенты настроены на подтверждение законности сервера. Щелкните мышью кнопку ОК в диалоговом окне **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата) (рис. 947) и щелкните мышью **Next** (Далее).

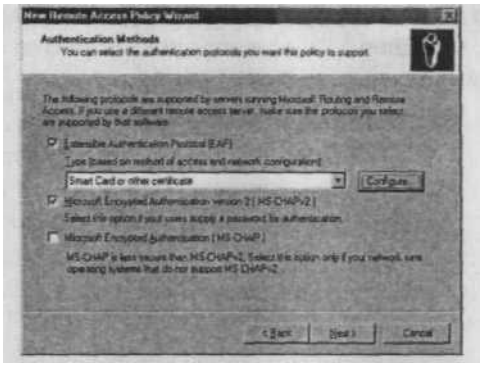


Рис. 9.46. **Страница Authentication Method** (Метод аутентификации)

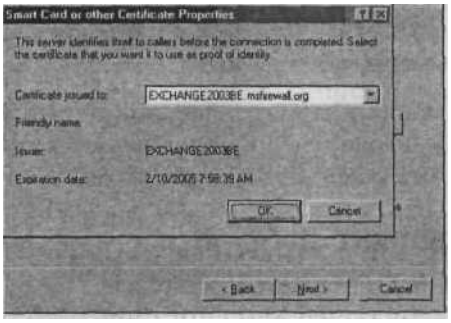


Рис. 9.47. Диалоговое окно **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата)

ПРИМЕЧАНИЕ Если вы не видите сертификата в диалоговом окне Smart Card or other Certificate Properties (Свойства смарт-карты или другого сертификата), перезапустите RADIUS-сервер и повторите заново. Сертификат появится в диалоговом окне после перезапуска. Если и после этого вы не увидите сертификат, это означает, что или на компьютере нет установленного сертификата, или у машины есть сертификат, но она не доверяет ЦС, выдавшему сертификат. Проверьте сертификат компьютера и компьютерное хранилище сертификатов Trusted Root Certification Authorities (доверенные корневые центры сертификации), чтобы убедиться в том, что оба эти сертификата установлены.

7. Выберите уровень (уровни) шифрования, который вы хотите назначить для VPN-соединений. Все клиенты Microsoft поддерживают самый высокий уровень шифрования. Если у вас есть клиенты, не поддерживающие 128-битного шифрования, выберите более низкие уровни, но имейте в виду, что вы снижаете уровень безопасности, обеспечиваемый методом шифрования, применяемым VPN-протоколом. В данном примере мы выберем три варианта (рис. 948). В среде с высокой степенью защиты следует выбирать вариант усиленного шифрования. Однако убедитесь, что ваши VPN-клиенты поддерживают этот уровень шифрования. Щелкните мышью **кнопку Next** (Далее).

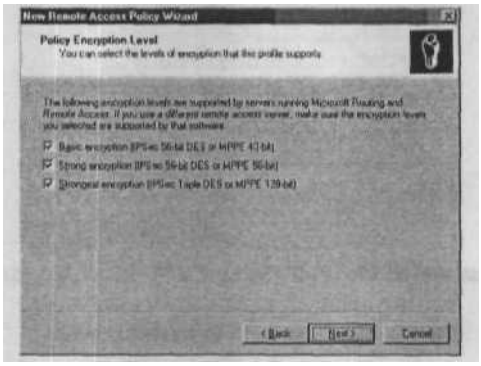


Рис. 9.48. Уровень шифрования в политике

8. Просмотрите ваши установки на странице **Completing the** New **Remote** Access **Policy Wizard** (Завершение мастера создания новой политики удаленного доступа) и щелкните мышью кнопку **Finish** (Готово).

Разрешения удаленного доступа и функциональный уровень домена

Новая политика удаленного доступа требует, чтобы соединение было VPN-соединением. VPN-протокол может быть как PPTP, так и L2TP/IPSec. VPN-клиент должен использовать протоколы CHAPv2 или EAP-TLS (Transport Layer Security, безопасность

на транспортном уровне) для подтверждения подлинности и поддерживать уровень шифрования, установленный в политике удаленного доступа. Пользователь должен принадлежать группе **Domain Users** (Пользователи домена) в домене, заданном в политике удаленного доступа.

Следующий шаг — настроить разрешения удаленного доступа. Разрешения удаленного доступа отличаются от политики удаленного доступа.

Когда VPN-пользователь устанавливает соединение по телефонной линии с брандмауэром ISA, параметры сравниваются с политикой удаленного доступа (политика удаленного доступа может находиться как на самом брандмауэре ISA, так и на LAS-сервере). Политики удаленного доступа представляются в виде иерархического списка. Политика на вершине списка оценивается первой, затем оценивается политика, указанная в списке второй, затем третья и т. д.

Параметры соединения VPN-клиента сравниваются *с условиями (conditions),* заданными в политике. В политике удаленного доступа, которую мы создали, есть два условия:

- тип соединения — виртуальное соединение;
- пользователь — член группы **Domain Users** (Пользователи домена).

Если запрос на соединение соответствует обоим этим условиям, устанавливаются разрешения удаленного доступа. Разрешения удаленного доступа определяются по-разному, в зависимости от типа домена, к которому принадлежит пользователь.

В доменах ОС Windows Server 2003 не используют понятий основного (Native Mode) и смешанного (Mixed Mode) режимов, применяемых в ОС Windows 2000. В этой операционной системе поддерживаются домены различных *функциональных уровней (functional levels).* Если на всех контроллерах вашего домена функционирует Windows Server 2003, по умолчанию уста на вливаетс я функциональный уровень *Windows 2000 mixed.* По умолчанию на этом функциональном уровне всем учетным записям пользователей запрещен коммутируемый (Dial-up) VPN-доступ. В режиме Windows 2000 Mixed Mode следует настроить учетную запись каждого пользователя для получения разрешения регистрации на VPN-сервере. Дело в том, что разрешения в учетной записи пользователя переопределяют разрешения политики удаленного доступа в доменах со смешанным режимом.

Если вы хотите управлять разрешениями для удаленного доступа через политику удаленного доступа, необходимо повысить функциональный уровень домена до уровня Windows 2000 Native или Windows Server 2003. Разрешение удаленного доступа по умолчанию в доменах этого уровня — **Control access through Remote Access Policy** (Управлять доступом через политику удаленного доступа). Поскольку вы можете использовать политику удаленного доступа для назначения разрешения удаленного доступа, появляется возможность, применяя членство в группах, разрешать или запрещать VPN-доступ к VPN-серверу.

Если VPN-соединение удовлетворяет *условиям* в политике удаленного доступа и пользователю предоставляется для соединения по телефонной линии доступ в соответствии с установками учетной записи пользователя или установками политики удаленного доступа, параметры VPN-соединения сравниваются с рядом установок, определенных в *Remote Access Profile (профиль удаленного доступа).* Если входящее соединение не соответствует установкам в профиле удаленного доступа, следующая политика удаленного доступа сравнивается с соединением. Если ни одна политика удаленного доступа не соответствует параметрам входящего соединения, запрос VPN-соединения с брандмауэром ISA отвергается.

Политика удаленного доступа в VPN, созданная вами ранее, включает все параметры, необходимые для защищенного VPN-соединения. Теперь ваша задача — решить, как вы хотите управлять разрешениями удаленного доступа: **м Enable Remote Access on a per group basis** (разрешить удаленный доступ, основанный на группах) этот вариант требует установки функционального уровня Windows 2000 Native или Windows Server 2003;

- **Enable Remote Access on a per user basis** (разрешить удаленный доступ, ос нованный на пользователях) этот вариант поддерживается функциональными уровнями: Windows 2000 Native, Windows 2000 Mixed и Windows Server 2003;
- **Enable Remote Access on both a per user and per group basis** (разрешить удаленный доступ, основанный на пользователях и группах) этот выбор тре бует функционального уровня Windows 2000 Native или уровня Windows Server 2003; выполняется детальный контроль доступа, основанный на пользователях, переопределяющий контроль доступа, основанный на группах.

Разрешение доступа, основанного на пользователе и группе, включает следующие необходимые процедуры:

- изменение разрешения для соединения по телефонной линии в учетной запи си пользователя, находящейся в Active Directory, для управления разрешением удаленного доступа, основанным на пользователе;
- изменение функционального уровня домена для поддержки разрешений для со единений по телефонной линии в соответствии с политикой удаленного доступа;
- изменение установочных параметров разрешений в политике удаленного доступа.

Изменение разрешений в учетной записи пользователя для соединения по телефонной линии

Предоставляются разрешения для соединения по телефонной линии на основе учетных записей или создаются политики удаленного доступа, которые могут быть настроены для включения разрешений соединения по телефонной линии, относящихся к целым группам.

Выполните следующие шаги, если хотите контролировать доступ отдельных пользователей или у вас нет другого выбора из-за установленного функционального уровня на вашем домене.

1. Щелкните мышью кнопку **Start** (Пуск), укажите на строку **Administrative Tools** (Администрирование) и щелкните кнопкой мыши команду **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
2. На консоли **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) раскройте окно, связанное с именем домена, и щелкните кнопкой мыши узел **User** (Пользователь).
3. Дважды щелкните кнопкой мыши учетную запись **Administrator** на правой панели консоли. В диалоговом окне учетной записи пользователя **Properties** (Свойства) щелкните кнопкой мыши вкладку **Dial-in** (Входящие звонки). Установка по умолчанию для учетной записи — **Deny access** (Запретить доступ). Вы можете разрешить доступ для учетной записи, выбрав вариант Allow **access** (Разрешить доступ). Установки в каждой учетной записи переопределяют набор разрешений, установленный в политике удаленного доступа. Обратите внимание на то, что параметр **Control access through Remote Access Policy** (Управлять доступом через политику удаленного доступа) недоступен. Этот параметр становится доступным, только когда функциональный уровень домена — Windows 2000 Native или Windows Server 2003. Сейчас не вносите никаких изменений в параметры учетной записи (рис. 949).

Рис. 9.49. Изменение разрешений для соединений по телефонной линии

4. Щелкните мышью кнопку **Cancel** (Отменить) для удаления с экрана этого диалогового окна.

Изменение функционального уровня домена

Если вы хотите управлять доступом, основываясь на группах, необходимо изменить функциональный уровень домена, установленный по умолчанию. Для этого выполните следующие шаги.

На контроллере вашего домена откройте консоль **Active Directory Domains and Trusts** (Active Directory — домены и доверие). Для этого щелкните мышью кнопку **Start** (Пуск), укажите на строку **Administrative Tools** (Администрирование) и щелкните кнопкой мыши команду **Active Directory Domains and Trusts** (Active Directory — домены и доверие).

На консоли **Active Directory Domains and Trusts** (Active Directory — домены и доверие) щелкните правой кнопкой ваш домен и левой кнопкой команду **Raise Domain Functional Level** (Повысить функциональный уровень домена). В

3. диалоговом окне **Raise Domain Functional Level** (Повысить функциональный уровень домена) щелкните кнопкой мыши стрелку, направленную вниз, в раскрывающемся списке **Select an available domain functional level** (Выбрать допустимый функциональный уровень домена) и выберите **Windows 2000 native или Windows Server 2003** в зависимости от того, какой функциональный уровень домена может поддерживать ваша сеть. В данном примере мы выберем вариант **Windows Server 2003**. После выбора нужного уровня щелкните мышью кнопку **Raise** (Повысить) (рис. 9.50).

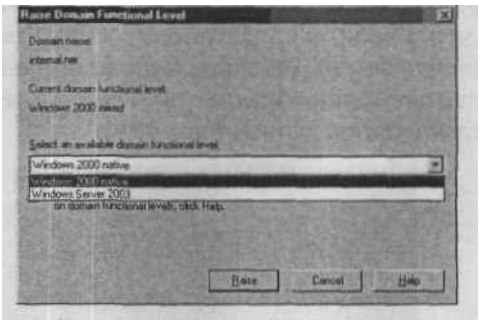


Рис. 9.50. Повышение функционального уровня домена

4. Щелкните мышью кнопку ОК в диалоговом окне **Raise Domain Functional Level** (Повысить функциональный уровень домена). В этом окне поясняется, что внесенное изменение воздействует на домен в целом и после того, как изменение сделано, нельзя вернуться к прежнему состоянию.

Щелкните мышью кнопку ОК в диалоговом окне **Raise Domain Functional Level** (Повысить функциональный уровень домена), информирующем о том, что функциональный уровень повышен. Учтите, что не нужно перезапускать компьютер для того, чтобы изменения вступили в силу. Однако текущее разрешение удаленного доступа для учетных записей пользователей не изменится до тех пор, пока не завершится репликация Active Directory. В этом примере мы перезапустим компьютер. Выполните перезагрузку машины и зарегистрируйтесь как Administrator.

6. Вернитесь на консоль **Active Directory Users and Computers** (Active Directory — домены и доверие) и дважды щелкните кнопкой мыши учетную запись пользователя. Щелкните мышью вкладку Dial-in (Входящие звонки) в диалого-

вом окне пользователя **Properties** (Свойства). Обратите внимание на то, что теперь вариант **Control access through Remote** Access **Policy** (Управлять доступом через политику удаленного доступа) доступен и выбран в качестве установки по умолчанию (рис. 9.51).

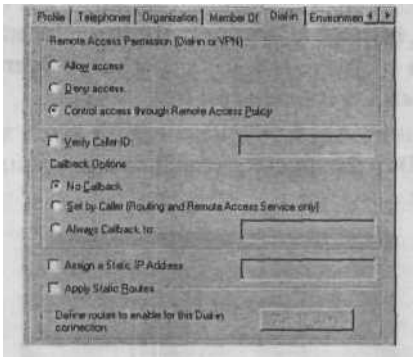


Рис. 9.51. Управление доступом с помощью политики удаленного доступа

Управление доступом с помощью политики удаленного доступа

Теперь у нас есть возможность управлять доступом с помощью политики удаленного доступа (вместо ориентации на учетные записи пользователей), рассмотрим, как выполняется такое управление VPN-доступом.

1. Щелкните мышью кнопку **Start** (Пуск), укажите на строку **Administrative Tools** (Администрирование) и щелкните кнопкой мыши команду **Internet Authenti cation Service** (Сервис интернет-аутентификации).
2. Щелкните кнопкой мыши **Remote Access Policies** (Политики удаленного до ступа) на левой панели консоли. Вы увидите **VPN Access Policy** (Политика VPN-доступа) и две другие встроенные политики удаленного доступа. Можно удалить другие политики, если вам нужны только VPN-подключен и я к брандмауэру ISA. Щелкните правой кнопкой мыши политику **Connections to other access servers** (Соединения с серверами другого доступа) и щелкните левой кнопкой команду **Delete** (Удалить). Повторите те же действия для политики **Connections to Micro soft Routing and Remote Access server** (Соединения с сервером маршрутиза ции и удаленного доступа).
3. Щелкните дважды кнопкой мыши политику **VPN Access Policy** (Политика VPN-доступа) на правой панели консоли. В диалоговом окне **VPN Access Policy Properties** (Свойства политики VPN-доступа) есть два варианта, которые управ ляют разрешениями доступа, основанными на политике удаленного доступа:
   - D разрешение, блокирующее удаленный доступ;
   - D разрешение, предоставляющее удаленный доступ.

В этом диалоговом окне сообщается, что установки в учетной записи пользователя переопределяют установки политики удаленного доступа: **Unless individual access permissions are specified in the user profile, this policy controls access to the network** (Пока в профиле пользователя не заданы индивидуальные разрешения для доступа, данная политика управляет доступом к сети). Выберите переключатель **Grant remote access permission** (Предоставить разрешение удаленного доступа) для разрешения членам группы **Domain Users** (Пользователи домена) обращаться к VPN-серверу (рис. 9.52).

4. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK в диалоговом окне **VPN Access Policy Properties** (Свойства политики VPN-доступа) для сохранения изменений.

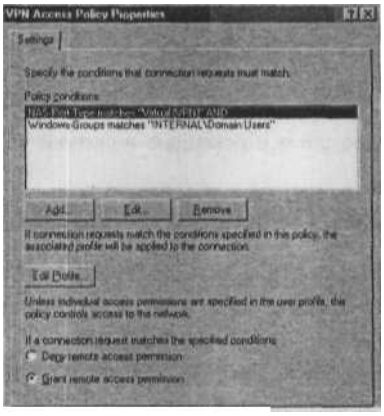


Рис. 9.52. Свойства политики удаленного доступа

Включение VPN-сервера на брандмауэре ISA и конфигурирование поддержки RADIUS

После того, как установлен и сконфигурирован RADIUS-сервер и сформированы политики удаленного доступа, можно начать настраивать брандмауэр ISA. Снимала мы включим компонент VPN-сервера, а затем сконфигурируем VPN-сервер для поддержки подтверждения подлинности с помощью сервиса RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя).

Выполните следующие шаги для включения VPN-сервера и настройки его для *RAD* I US- поддержки.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networking (VPN)** (Виртуальные частные сети).

2. Щелкните кнопкой мыши вкладку Tasks (Задачи) на панели задач. Щелкните мышью ссылку Enable VPN Client Access (Разрешить доступ VPN-клиента).
3. Щелкните кнопкой мыши Configure VPN Client Access (Настроить доступ VPN-клиента).
4. В диалоговом окне VPN Clients Properties (Свойства VPN-клиентов) установите флажок Enable VPN client access (Разрешить доступ VPN-клиента). Задайте коли чество клиентов, которым вы хотите разрешить доступ, в текстовом поле Maximum number of VPN allowed (Максимальное число разрешенных VPN-клиентов).
5. Щелкните кнопкой мыши вкладку Protocols (Протоколы). Установите флажки Enable PPTP и Enable L2TP/IPSec. Щелкните мышью кнопку Apply (Приме нить) и затем кнопку OK (рис. 9.53).

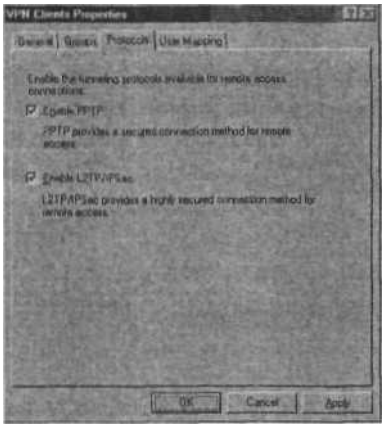


Рис. 9.53. Разрешение VPN-протоколов

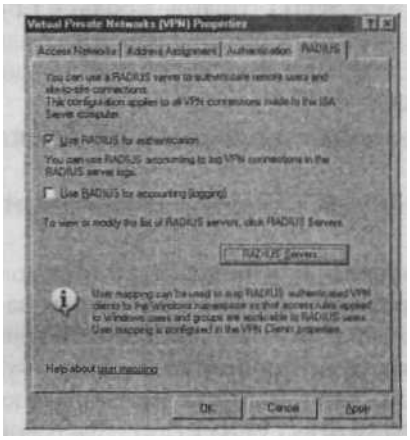


Рис. 9.54. Настройка RADIUS-аутентификации

6. Щелкните мышью ссылку **Specify RADIUS Configuration** (Задать RADIUS-конфигурацию) на вкладке Tasks (Задачи).
7. На вкладке **RADIUS** в диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства виртуальных частных сетей) (рис. 9.54) установите флажок **Use RADIUS for authentication** (Применять RADIUS-аутентификацию).
8. Щелкните мышью кнопку **RADIUS Servers** (RADIU S-серверы) в диалоговом окне **RADIUS,** щелкните мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add RADIUS Server** (Добавить RADIUS-сервер) введите имя компьютера с IAS-сервером в текстовое поле **Server name** (Имя сервера). В данном примере имя IAS-сервера — **EXCHANGE2003BE.msfirewall.org.** Введите описание сервера в текстовое поле **Server description** (Описание серве ра). В этом примере введем описание **IAS Server.** Щелкните мышью кнопку **Change** (Изменить) (рис. 9-55).

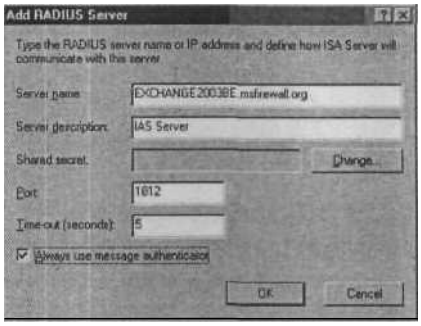


Рис. 9.55. Диалоговое окно Add RADIUS Server (Добавить RADIUS-сервер)

10. В диалоговом окне **Shared Secret** (Пароль) введите пароль и его подтвержде ние в текстовые поля **New Secret** (Новый пароль) и **Confirm new secret** (Под тверждение нового пароля). Убедитесь в том, что введен тот же пароль, кото рый вы вводили в конфигурацию RADIUS-клиента на машине IAS-сервера. Шелк ните мышью кнопку ОК.
11. Щелкните мышью кнопку ОК в диалоговом окне **Add RADIUS Server** (Добавить RADIUS-сервер).
12. Щелкните мышью кнопку ОК в диалоговом окне **RADIUS Servers** (RADIUS-сер вер) (рис. 956).
13. Щелкните мышью кнопку **Apply** (Применить) в диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства виртуальных частных сетей). Щелкните мышью кнопку ОК в диалоговом окне **ISA** 2004, информирующем о возможности перезапуска сервиса **Routing and Remote Access Service** (Сервис маршрутизации и удаленного доступа). Щелкните мышью кнопку ОК в диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства виртуальных частных сетей).

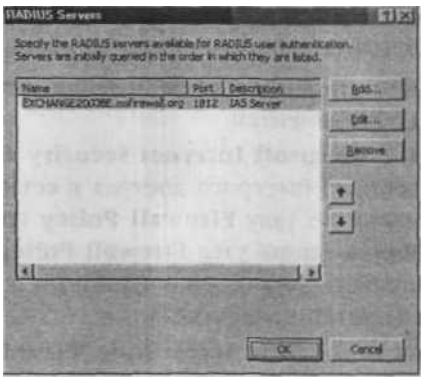


Рис. 9.56. Диалоговое окно RADIUS Server (RADIUS-сервер)

14. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
15. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).
16. Перезапустите брандмауэр ISA и зарегистрируйтесь как **Administrator.**

Создание правила доступа, разрешающего доступ VPN-клиентов к санкционированным ресурсам

После перезапуска брандмауэр ISA может принимать входящие VPN-подключения. Однако VPN-клиенты не могут получить доступ ни к одному ресурсу во внутренней сети, потому что нет правил доступа, разрешающих такой доступ. Следует создать правило доступа, разрешающее доступ к внутренней сети машинам, принадлежащим сети VPN-клиентов. В отличие от других комбинированных брандмауэр/VPN-сервер решений на брандмауэре ISA применяются средства управления доступом для сетевого доступа к VPN-клиентам.

В.данном примере мы создадим правило **доступа,** разрешающее VPN-клиентам доступ к серверу OWA (Outlook Web Access, Web-доступ в Outlook) во внутренней сети и больше ни к какому другому серверу. Кроме того, мы ограничим пользователей с помощью применения только HTTP- протокол а для установки соединения.

Этот тип конфигурации мог бы быть привлекателен для организаций, которые хотят разрешить безопасный удаленный доступ к корпоративному OWA-сайту, но не хотят использовать сопряжение SSL-в-SSL, потому что:

- могут существовать потенциальные уязвимости в реализациях шифрования SSL/TLS;
- хотят разрешить нешифрованным сообщениям проходить через корпоративную сеть для того, чтобы IDS (Intrusion-Detection System, система обнаружения вторжений) имела возможность проверить соединения.

Позже в этой главе мы покажем другие способы реализации управления доступом VPN-клиентов, использующие пользователь/группу.

Выполните следующие шаги для создания правила доступа, предоставляющего неограниченный доступ VPN-клиентам.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) щелкните кнопкой мыши по узлу **Firewall Policy** (Политика брандмауэра). Щелкните правой кнопкой мыши узел **Firewall Policy** (Политика брандмауэ ра), укажите левой кнопкой команду **New** (Новая) и щелкните кнопкой мыши команду **Access Rule** (Правило доступа).
2. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере мы назовем правило **OWA for VPN Clients.** Щелкните мышью кнопку **Next** (Далее).
3. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разре шить) и щелкните мышью кнопку **Next** (Далее).
4. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **Add Protocols** (Добавить протоколы) щелкните мышью папку **Common Protocols** (Общие протоколы) и затем дважды щелкните кнопкой мыши протоколы **HTTP** и **HTTPS.** Щелкните мышью кнопку **Close** (Закрыть).
6. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
7. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (До бавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и затем дважды щелкните кнопкой мыши сеть **VPN Clients** (VPN-клиенты). Щелкните мышью кнопку **Close** (Закрыть).
8. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources.** (Ис точники в правиле доступа).
9. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New** и команду **Computer** (Компьютер).
10. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите имя OWA-сервера в текстовое поле **Name** (Имя). В данном примере — **OWA Server.** Введите IP-адрес OWA-сервера в текстовое поле **Computer IP Address** (IP-адрес компьютера). Щелкните мышью кнопку ОК.
11. Щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните кнопкой мыши элемент **OWA Server.** Щелкните мышью кнопку **Close** (Закрыть).

12. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
13. На странице **User Sets** (Наборы пользователей) согласитесь с установкой по умолчанию **All Users** (Все пользователи) и щелкните мышью кнопку **Next** (Далее).
14. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).
15. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
16. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию). Политика **OWA for VPN Clients** теперь представлена как правило доступа в верхней строке списка политики брандмауэра (рис. 9.57).

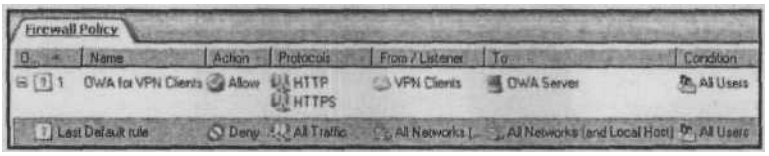


Рис. 9.57. Результирующая политика брандмауэра

Создание подключения VPN-клиента по протоколу PPTP

Сформированы все элементы, необходимые для поддержки RADIUS-аутентификации для VPN-клиентов. В следующем упражнении вы установите VPN-соединение по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол) из внешней сети VPN-клиентов.

Выполните следующие шаги для подключения к VPN-серверу с помощью RADIUS-**аутентификации.**

1. В окне **Dial-up and Network Connections** (Сетевые подключения) на компью тере клиента внешней сети создайте пиктограмму нового VPN-соединения. Настройте ее, используя IP-адрес **192.168.1.70** как адрес VPN-сервера. Зарегис трируйтесь с именем пользователя **Administrator.**
2. Щелкните мышью кнопку ОК в диалоговом окне, информирующем вас о том, что VPN-соединение установлено.
3. На машине контроллера домена щелкните мышью кнопку **Start** (Пуск) и ука жите на строку **Administrative Tools** (Администрирование). Щелкните кноп кой мыши оснастку **Event Viewer** (Просмотр событий).
4. **В Event Viewer** щелкните кнопкой мыши узел **System** (Система) на левой па нели консоли. Дважды щелкните мышью элемент **Information** (Уведомление), которому соответствует источник **IAS** (рис. 9.58).

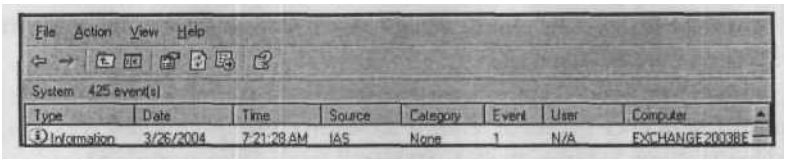


Рис. 9.58. Строка из **Event Viewer** (Просмотр событий)

5. В диалоговом окне **Event Properties** (Свойства: Событие) вы увидите **Description** (Описание) запроса регистрации. В нем сообщается, что RADIUS-сервер подтвердил подлинность запроса и в описание также включена RADIUS-информация, отправленная на контроллер домена. Просмотрите ее и закройте диалоговое окно **Event Properties** (Свойства: Событие) (рис. 9.59).

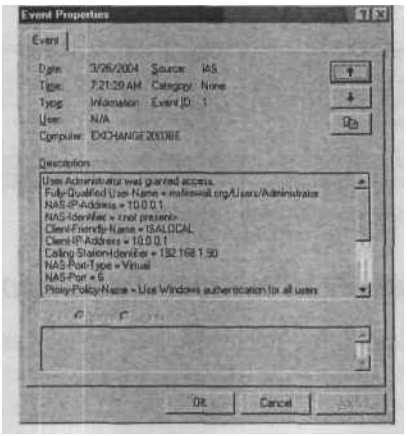


Рис. 9.59. Состав запроса регистрации

6. На брандмауэре ISA можно увидеть в журнале регистрации строки, характерны!; для этого VPN-запроса. Обратите внимание на PPTP- и RADIUS-соединения (рис. 9.60).

82.16*1*	1И.1И1Я	17ЛРРТР	I		
132.1681.30	132168170	0 PPTP	liAml tmnoamn		
taO.il	*Ш01*	*mi тент*	*ы*ЫЬтЛон*	JUt»FUC>fU5ulnieiu,l«ilUSan>ui>»«lttun»t	
ПР01Д	1[1QD106	II	WNMnMilPFTFj ImMMVPN [ддШи	_____	___ ____

Рис. 9.60. Строки журнала регистрации, относящиеся к RADIUS-аутентификации VPN-клиента

7. На сервере брандмауэра ISA можно увидеть сеанс связи VPN-клиента на вкладке **Sessions** (Сеансы) узла **Monitoring** (Мониторинг) на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) (рис. 961).

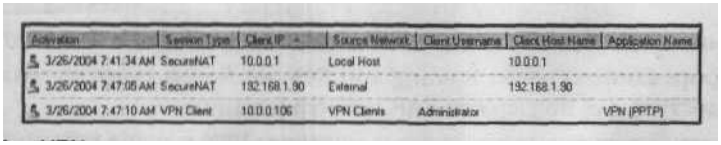


Рис. 9.61. VPN-сеанс в секции сеансов

8. На компьютере VPN-клиента отключите VPN-соединение.
9. Если вы запустите сеанс **Network Monitor** (Сетевой монитор) на RADIUS-сервере, то увидите, что один **Access Request** (Запрос доступа) сервиса RADIUS отправлен с брандмауэра ISA на RADIUS-сервер и единственное сообщение **Access Accept** (Доступ принимается) послано на брандмауэр ISA с RADIUS-сервера (рис. 9-62).

Рис. 9.62. Сообщения сервиса RADIUS в записи Network Monitor (Сетевой монитор)

Применение аутентификации сертификатами пользователя с помощью протокола EAP для VPN-соединений удаленного доступа

Можно существенно повысить безопасность соединений ваших VPN-клиентов удаленного доступа с брандмауэром ISA с помощью аутентификации сертификатами пользователя, выполняемой по протоколу EAP (Extensible Authentication Protocol, наращиваемый протокол аутентификации). Подтверждение подлинности с помощью сертификата пользователя требует, чтобы пользователь имел сертификат пользователя, выданный доверенным центром сертификации (ЦС).

Как брандмауэру ISA, так и VPN-клиенту удаленного доступа должны быть назначены соответствующие сертификаты. Брандмауэру ISA следует назначить сертификат компьютера, который брандмауэр сможет использовать для самоидентификации. Пользователям необходимо присвоить сертификаты пользователей от центра сертификации, которому доверяет брандмауэр ISA. Если и компьютер клиента удаленного доступа, предоставляющий сертификат пользователя, и брандмауэр ISA содержат сертификат общего ЦС в своих хранилищах сертификатов Trusted Root Certification Authorities (доверенные корневые центры сертификации), то и клиент, и сервер доверяют одной и той же иерархии сертификатов.

Следующие шаги необходимы для поддержки подтверждения подлинности с помощью сертификатов пользователя VPN-соединений клиентов удаленного доступа с брандмауэром:

- выдача сертификата компьютера брандмауэру ISA;
- настройка программного обеспечения брандмауэра ISA для поддержки EAP-аутентификации;

- разрешение отображения пользователей для пользователей EAP-аутентификации;
- конфигурирование сервиса Routing and Remote Access (маршрутизация и удаленный доступ) для поддержки EAP-аутентификации;
- выдача сертификата пользователя для компьютера VPN-клиента удаленного доступа.

Мы уже обсуждали процедуры получения сертификата компьютера для брандмауэра ISA в других главах этой книги и на сайте www.isaserver.org, поэтому мы не будем повторять их здесь. Начнем с конфигурирования программного обеспечения брандмауэра ISA для поддержки EAP-аутентификации, а затем обсудим, как настроить сервис RRAS и клиенты.

ПРИМЕЧАНИЕ Следующие примеры предполагают, что вы уже включили и настроили компонент VPN-сервера на брандмауэре ISA перед обеспечением поддержки EAP-аутентификации. Также имейте в виду, что этот вариант подтверждения подлинности доступен только, когда брандмауэр ISA является членом домена. Это еще один неоспоримый довод в пользу членства брандмауэра ISA в домене.

Настройка программного обеспечения брандмауэра ISA для поддержки EAP-аутентификации

Выполните следующие шаги для конфигурирования поддержки EAP-аутентификации брандмауэром ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networking (VPN)** (Виртуальные частные сети) на левой панели консоли.

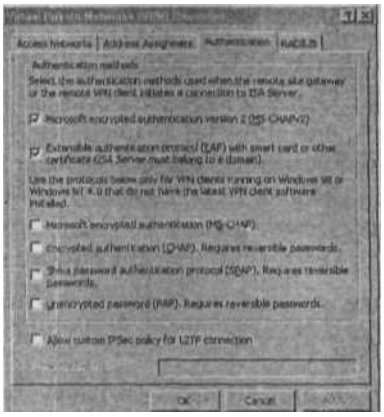


Рис. 9.63. Установка EAP-аутентификации

2. В узле **Virtual Private Networks (VPN)** (Виртуальные частные сети) щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач. На вкладке **Tasks** (Зада чи) щелкните кнопкой мыши **Authentication Methods** (Методы аутентификации).
3. В диалоговом окне **Virtual Private Networks (VPN) Properties** (Свойства: вир туальные частные сети) установите флажок **Extensible authentication protocol (EAP) with smart card or other certificate (ISA Server must belong to a domain)** (Наращиваемый протокол аутентификации со смарт-картой или дру гим сертификатом, ISA Server должен принадлежать домену) (рис. *9.63)*.
4. Прочтите информацию в диалоговом окне **Microsoft Internet Security and Ac celeration Server 2004** (Сервер защищенного быстрого доступа к сети Интер нет 2004): «EAP authenticated users belong to the RADIUS namespace and are not part of the Windows namespace. To apply user-based access rules to these users you can either define a RADIUS user set for them or you can use user mapping to map these users to the Windows namespace. If user mapping is enabled, access rules applied to the Windows users and group will be applicable to EAP authenticated users» (Поль зователи, подлинность которых подтверждена с помощью протокола EAP, при надлежат пространству имен сервиса RADIUS и не являются частью пространства имен Windows. Для того чтобы применить к ним правила доступа, ориентирован ные на пользователей, вы можете либо определить для этих пользователей на бор RADIUS-пользователей, либо использовать отображение пользователей для переноса их в пространство имен Windows. Если отображение пользователей включено, правила доступа, используемые для пользователей и групп ОС Windows, будут применимы и к пользователям, аутентифицируемым с помощью EAP). Это важная информация, демонстрирующая реальное назначение отображения пользователей, которое обсуждалось ранее в этой главе. Поскольку EAP-аутен-тификация не использует «Windowso-аутентификацию, вы не можете по умол чанию применять политику доступа, основанную на пользователе/группе к VPN-клиентам, подтверждающим подлинность с помощью EAP-сертификатов пользователя. Однако если для этих пользователей активизировать отображе ние пользователей и отобразить имена пользователей из пользователей, аутен-тифицированных с помощью EAP-сертификатов, в пользователей домена, то те же правила, которые применяются к пользователям, зарегистрировавшимся с по мощью Windows-аутентификации, будут применяться и к пользователям, под твердившим подлинность с помощью EAP-сертификатов пользователей. Мы подробно рассмотрим процедуры активизации и настройки отображения пользо вателей в следующем разделе.
5. Щелкните мышью кнопку ОК (рис. 9.64), чтобы подтвердить, что вы прочли и поняли эту информацию.
6. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК.

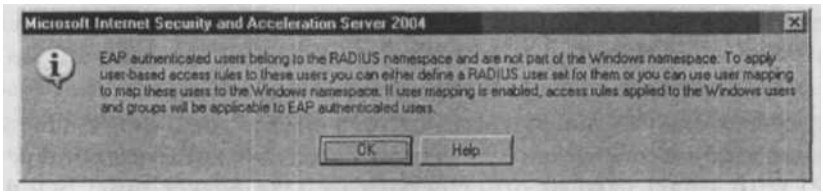


Рис. 9.64. Сообщение об отображении пользователей и EAP

Включение отображения пользователей для пользователей, подтверждающих подлинность с помощью протокола EAP

Выполните следующие шаги для включения и настройки отображения пользователей для пользователей, подтверждающих подлинность с помощью протокола EAR

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети) на левой панели консоли.
2. В узле **Virtual Private Networks (YPN)** (Виртуальные частные сети) щелкните кнопкой мыши вкладку **Tasks** (Задачи) на панели задач. Щелкните кнопкой мыши **Configure VPN Client Access** (Настроить доступ VPN-клиента) на вкладке **Tasks** (Задачи).
3. В диалоговом окне **VPN Clients Properties** (Свойства VPN-клиентов) щелкни те кнопкой мыши вкладку **User Mapping** (Отображение пользователей).
4. На вкладке **User Mapping** (Отображение пользователей) установите флажок **Enable User Mapping** (Включить отображение пользователей). Установите также флажок **When username does not contain a domain, use this domain** (Если в имя пользователя не включен домен, использовать данный домен). Поскольку сертификаты пользователей не содержат доменных имен, необходимо включить этот режим. В текстовое поле **Domain Name** (Имя домена) введите имя доме на, которому принадлежит брандмауэр ISA. Это позволит брандмауэру ISA ото бражать имена пользователей, подтверждающих подлинность с помощью EAP-сертификатов, в учетные записи данного домена, после этого правила, при меняющиеся к пользователям, будут применяться и к пользователям, аутенти фицирующимся по протоколу EAP, точно так же, как если бы они были пользо вателями, подтвердившими свою подлинность с помощью традиционной аутен тификации «Windows».
5. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК (рис. 9-65).
6. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.

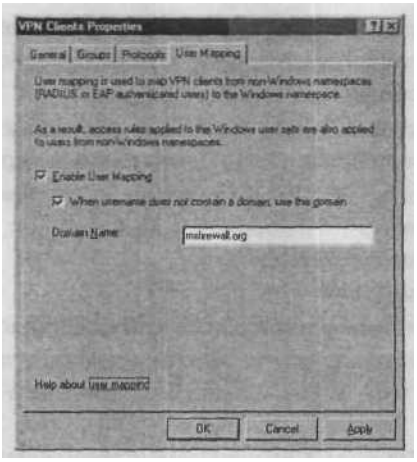


Рис. 9.65. Включение отображения пользователей для EAP-аутентификации

7. Щелкните мышью кнопку OK в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

Выдача сертификата пользователя компьютеру VPN-клиента удаленного доступа

Компьютеры VPN-клиентов удаленного доступа должны получить сертификаты пользователей и их необходимо настроить на подтверждение своей подлинности с помощью сертификатов пользователей на VPN-сервере удаленного доступа брандмауэра ISA.

Выполните следующие шаги для получения VPN-клиентом удаленного доступа сертификата пользователя.

1. Откройте обозреватель Internet Explorer. В строке **Address** (Адрес) введите URL-адрес Web-сайта регистрации вашего центра сертификации и нажмите клави шу <Enter>.
2. Введите **Administrator** (или любое другое имя, для которого нужно получить сертификат пользователя) в текстовое поле **User** Name (Имя пользователя). Введите пароль администратора в текстовое поле **Password** (Пароль). Щелкните мышью кнопку OK.
3. На странице **Welcome** (Добро пожаловать) Web-сайта регистрации ЦС щелк ните переключатель **Request a Certificate** (Запросить сертификат).
4. На странице **Request a Certificate** (Запросить сертификат) щелкните мышью переключатель **User Certificate** (Сертификат пользователя).
5. Щелкните мышью кнопку **Submit** (Принять) на странице **User Certificate — Identifying Information** (Сертификат пользователя — идентифицирующая информация).

6. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting Violation** (Возможное нарушение сценариев), информирующем, что Web-сайт запрашивает новый сертификат от вашего имени.
7. На странице **Certificate Issued** (Выданные сертификаты) щелкните мышью кнопку **Install this certificate** (Установить данный сертификат).
8. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **Potential Scripting** Violation (Возможное нарушение сценариев), сообщающем, что Web-сайт добавляет один или несколько сертификатов.
9. Закройте **Internet Explorer.**
   Теперь мы можем настроить пиктограмму VPN-соединения (VPN connectoid) для аутентификации с помощью сертификатов пользователя, поскольку у нас есть сертификат пользователя, установленный на машине VPN-клиента удаленного доступа.
10. В окне **Dial-up and Network Connections** (Сетевые подключения) на компьютере клиента внешней сети создайте пиктограмму нового VPN-соединения. Настройте его, указав IP-адрес **192.168.1.70** как адрес VPN-сервера.
11. Когда вы завершите мастер создания соединения, то увидите диалоговое окно **Connect** (Подключение). Щелкните мышью кнопку **Properties** (Свойства).
12. В диалоговом окне подключения **Properties** (Свойства) щелкните кнопкой мыши вкладку **Security** (Безопасность) (рис. 9.66) и выберите переключатель **Advanced** (custom **settings)** (Дополнительные, выборочные параметры). Щелкните мышью кнопку **Settings** (Параметры).

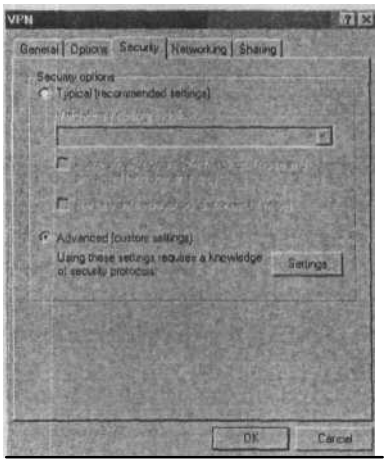


Рис. 9.66. Вкладка Security (Безопасность)

13- В диалоговом окне **Advanced Security Settings** (Дополнительные параметры безопасности) (рис. 9-67) выберите переключатель **Use Extensible Authentica-**

tion Protocol (EAP) (Протокол расширенной проверки подлинности). Щелкните мышью кнопку **Properties** (Свойства).

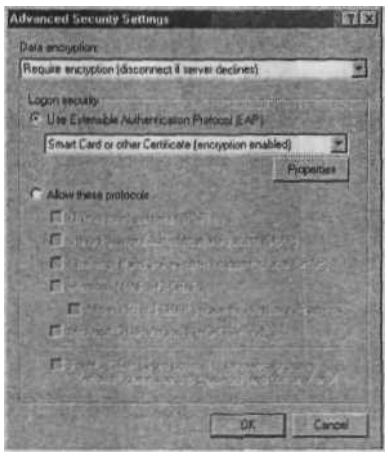


Рис. 9.67. Включение EAP-аутентификации

14. В диалоговом окне **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата) выберите переключатель **Use a** certificate **on this computer** (Использовать сертификат на этом компьютере). Установите флажок **Validate server certificate** (Проверка сертификата сервера). Установите также флажок **Connect only if server name ends with** (Подключение к серверам) и введите имя домена сервера аутентификации. В данном примере — msfirewall.org, введите это имя в текстовое поле. В списке **Trusted root certificate authority** (Доверенные корневые центры сертификации) выберите имя ЦС, выдавшего сертификаты. В данном примере имя ЦС — **EXCHANGE2003BE.** Щелкните мышью кнопку ОК в диалоговом окне **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата) (рис. 9.68).

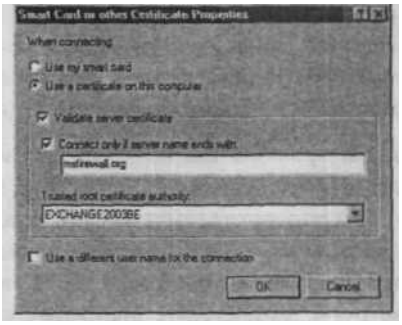


Рис. 9.68. Диалоговое окно **Smart Card or other Certificate Properties** (Свойства смарт-карты или другого сертификата)

15. Щелкните мышью кнопку ОК в диалоговом окне **Advanced Security Settings** (Дополнительные параметры безопасности).
16. Щелкните мышью кнопку ОК в диалоговом окне **Properties** (Свойства).
17. Появляется диалоговое окно **Connect** (Подключение), содержащее имя сертифи ката пользователя, полученного из ЦС (рис. 9-69). Щелкните мышью кнопку ОК.

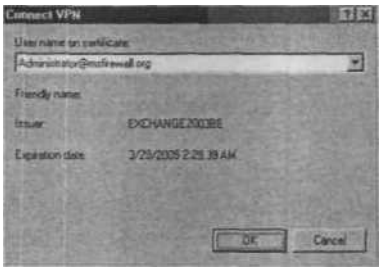


Рис. 9.69. Выбор сертификата пользователя для EAP-аутентификации пользователя

Устанавливается VPN-соединение, и ваша подлинность будет подтверждена контроллером домена в корпоративной сети.

Поддержка исходящих VPN-соединений через брандмауэр ISA

Можно конфигурировать брандмауэр ISA для разрешения исходящего доступа к VPN-серверам *в* **Интернет.** Брандмауэр ISA поддерживает все действительные (true) VPN-протоколы, включая PPTP, L2TP/IPSec и IPSec NAT Traversal (NAT-T) (обходящий NAT по протоколу IP-безопасности).

Брандмауэр ISA может пропускать VPN-подключения по протоколу PPTP из любой защищенной сети к Интернету с помощью своего PPTP-фильтра. PPTP-фильтр брандмауэра ISA перехватывает соединение от клиента защищенной сети и служит промежуточным звеном для сообщений по протоколу GRE (Generic Routing Encapsulation/IP Protocol 47, обобщенная инкапсуляция маршрутизации) и канала управления (TCP 1723) протокола PPTP. Единственное, что от вас требуется, — создать правило доступа, разрешающее исходящий **доступ** по протоколу PPTP.

Внимание! В следующем примере *мы* настраиваем исходящий доступ по протоколу PPTP только с компьютеров удаленного управления (Remote Management Computers). Мы подчеркиваем этим, что исходящий доступ к VPN-серверам следует предоставлять только заслуживающим доверие хостам. VPN-клиент соединяется с сетью, которая находится, вероятно, вне вашего административного контроля. VPN-клиент действует как потенциально безопасный мост между вашей сетью и удаленной сетью. Следовательно, вы должны быть очень осмотрительны, предоставляя исходящий удаленный VPN-

доступ. Данный пример также разрешает соединение с конкретным VPN-сервером. Всегда следует предварительно определить VPN-серверы, с которыми соединяются ваши пользователи, для того чтобы уменьшить общее негативное влияние на безопасность вашей корпоративной сети, которое могут оказать исходящие VPN-подключения.

Выполните следующие шаги для разрешения исходящего доступа по протоколу PPTP через брандмауэр ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004), раскройте окно, связанное с именем сервера, щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) на панели задач.
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере — **Outbound PPTP for Administrators.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **VPN and IPSec** и дважды щелкните по элементу **PPTP.** Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computer Sets** (Наборы компьютеров) и дважды щелкните мышью элемент **Remote Management Computers** (Компьютеры удаленного управления). Щелкните мышью кнопку **Close** (Закрыть).
9. Щелкните мышью кнопку **Next** (далее) на странице **Access Rule Sources** (Источники правила доступа).
10. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New** (Новый) и команду **Computer** (Компьютер).
12. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите имя внешнего VPN-сервера в текстовое поле **Name** (Имя). Введите IP-адрес авторизованного VPN-сервера в текстовое поле **Computer IP**

Address (IP-адрес компьютера). В данном примере — **Authorized VPN Server.** Щелкните мышью кнопку ОК. 13. Щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните

кнопкой мыши элемент **Authorized VPN Server.** Щелкните мышью кнопку **Close** (Закрыть). 14.Щелкните мышью кнопку Next (Далее) на странице **Access Rule Destinations**

(Адресаты в правиле доступа).

15. Щелкните мышью кнопку Next (Далее) на странице **User Sets** (Наборы пользо вателей).
16. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).

СОВЕТ Поскольку VPN-протоколу PPTP требуется протокол GRE (протокол IP-уровня, который не использует TCP- или UDP-протокол как транспортный), машины, конфигурированные только как клиенты брандмауэра и/иги клиенты Web-прокси, не смогут соединиться с VPN-серверами в Интернете с помощью протокола PPTP. Компьютер должен быть также настроен как клиент SecureNAT для того, чтобы успешно завершить PPTP-соединение. В результате вы не сможете использовать средства управления доступом, базирующиеся на пользователе/группе для ограничения пользователей, которым разрешены PPTP-соединения с VPN-серверами в Интернете. Альтернативой может быть применение объектов Computer Objects или Computer Address Set Objects для управления исходящим доступом по протоколу PPTP с помощью IP-адреса клиента. Это справедливо и для протоколов NAT-T по протоколу IPSec (хотя по другим причинам), в чем вы убедитесь в следующем обсуждении.

Все современные VPN-клиенты, базирующиеся на протоколе IPSec, поддерживают тот или иной тип NAT traversal (NAT-T, обходящий NAT). Клиент Microsoft no протоколу L2TP/IPSec поддерживает IETF (Internet Engineering Task Force, проблемная группа проектирования сети Интернет) рабочие документы (Internet draft) hup:// www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-08.txt для пересылки протокола IPSec через средства NAT (Network Address Translation, преобразование сетевых адресов). Несмотря на то, что ряд VPN-поставщиков, не относящихся к корпорации Microsoft, разнообразят рынок IPSec NAT-T, предлагая патентованные реализации средств NAT-T для их VPN-клиентов, большинство из них следует указаниям Mic rosoft и реализует рекомендации IETF draft для своих VPN-клиентов и серверов.

RFC-совместимый (RFC-compliant) обходящий NAT требует, чтобы были разрешены исходящие протоколы UDP 500 и UDP 1701 через брандмауэр ISA. UDP-порт 500 применяется для согласования Internet Key Exchange (IKE) (протокол обмена ключами), а UDP-порт 1701 используется для канала управления протокола L2TP. По этой причине вы могли бы ожидать, что применение RFC-совместимого обхо-

дящего NAT по протоколу IPSec позволит управлять исходящим VPN-доступом, ориентированным на пользователя/группу, так как большинство UDP- и TCP-протоколов используют интерфейс сетевого соединения Winsock. К сожалению, это не так для Microsoft L2TP/IPSec NAT-T и большинства других протоколов IPSec NAT-T, поскольку клиент NAT-T реализован как тонкая прокладка *(shim)* в Windows-стеке протокола TCP/IP и позволяет обходить интерфейс Winsock.

> ВНИМАНИЕ! Не все реализации протокола IPSec NAT-T являются RFC-совместимыми и используют собственные заголовки UDP или TCP NAT-T. Для обеспечения исходящего доступа для этих патентованных не RFC (Requests for Comments, запросы на комментарии) VPN-клиентов IPSec NAT-T необходимо выяснить, какие протоколы требуются для этих клиентов, и убедиться в том, что и клиент, и сервер настроены для поддержки одних и тех же протоколов IPSec NAT-T. Подробное обсуждение этой проблемы и возможные решения можно найти в статье Стефана Поусила (Stefaan Pouseele) «How to Pass IPSec Traffic Through ISA Server» (Как пересылать IPSec-трафик через ISA Server) по адресу http://isaserver.org/articles/IPSec_Passthrough.html.

Выполните следующие шаги для разрешения RFC-совместимых VPN-соединений по протоколу IPSec NAT-T (таких как Windows-клиент L2TP/IPSec) через брандмауэр ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера, щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вариант Create New Access **Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) на панели задач.
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере — **Outbound L2TP/IPSec NAT-T for Administrators.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **VPN and IPSec** и дважды щелкните по элементам **IKE Client** и **IPSec NAT-T Client.** Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).

8. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computer Sets** (Наборы компьютеров) и дважды щелкните мышью элемент **Remote Management Computers** (Компьютеры удаленного управления). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники правила доступа).
11. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New** (Новый) и команду **Computer** (Компьютер).
13. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите имя внешнего VPN-сервера в текстовое поле **Name** (Имя). Введите IP-адрес авторизованного VPN-сервера в текстовое поле **Computer IP Address** (IP-адрес компьютера). В данном примере — **Authorized VPN Server** Щелкните мышью кнопку ОК.
14. Щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните кнопкой мыши элемент **Authorized VPN Server.** Щелкните мышью кнопку **Close** (Закрыть).
15. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
16. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователей).
17. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).

Установка и конфигурирование DHCP-сервера и агента ретрансляции DHCP на брандмауэре ISA

У многих небольших организаций может возникнуть желание установить DHCP-сервер на брандмауэре ISA. Это позволит им автоматически назначать IP-адреса хостам в корпоративной сети без установки DHCP-сервера на отдельном сервере корпоративной сети. У многих таких компаний в сети всего один Windows-сервер, и часто он служит контроллером домена Windows. Поскольку возможны отрицательные последствия для безопасности сети при размещении DHCP-сервера на контроллере домена Windows, мы считаем его установку на брандмауэре ISA приемлемым вариантом.

У брандмауэра ISA есть системная политика, разрешающая брандмауэру быть DHCP-клиентом. Существуют два правила системной политики (см. табл. 9-1).

Табл. 9.1. Правила системной политики, разрешающие брандмауэру ISA быть DHCP-клиентом

Номе пра- вила	Rule Name (название правила)	Action (действие)	Protocols (Протоколы)	From/Listener (от/приемник)	To (К)	Condition (условие)
8	Allow DHCP requests from ISA Server ю all networks (Разрешить DHCP-запросы с ISA Server ко всем сетям)	Allow (Разрешить)	DHCP (request) DHCP-запрос	All Users (Все пользователи)	Local Host (Локальный хост)	Anywher (Везде)
9	Allow DHCP replies from DHCP servers to ISA Server (Разрешить DHCP-ответы с DHCP-серверов на ISA Server)	Allow (Разрешить)	DHCP (reply) DHCP-ОТКЛИК	Internal (Внутренняя)	Local Host (Локальный хост)	All Users (Все пользователи)

DHCP-правила системной политики разрешают DHCP-запросы с брандмауэра ISA и DHCP-отклики из внутренней сети на брандмауэр ISA. Эти правила не помогут при установке DHCP-сервера на самом брандмауэре ISA, потому что в этом случае нужно разрешить DHCP-запросы *из внутренней сети* к брандмауэру ISA и также разрешить DHCP-ответы *с брандмауэра ISA* во внутреннюю сеть. Нам придется создать правила доступа, разрешающие пересылку необходимых DHCP-сообщений на брандмауэр ISA и с него.

Выполните следующие шаги для создания правил доступа, разрешающих DHCP-запросы к брандмауэру ISA и DHCP-ответы с брандмауэра ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) рас кройте окно, связанное с именем сервера, щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши ва риант **Create New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) на панели задач.
3. На странице **welcome to the New Access Rule Wizard** (Вас приветствует мас тер создания нового правила) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере введите **DHCP Request.** Щелкни те мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выб ранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Infrastructure** (Инфраструктура) и дважды щелкните элемент **DHCP (request).** Щелкните мышью кнопку **Close** (Закрыть).

7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
9- В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью элемент **Internal** (Внутренняя). Если вы хотите разрешить клиентам из многочисленных защищенных сетей обращаться к DHCP-серверу на брандмауэре ISA, включите все эти сети тоже. Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники правила доступа).
11. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети) и дважды щелкните мышью сеть **Local Host** (Локальный хост).
13-Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
14. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователей).
15. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).

Далее создадим правило для DHCP-ответа с брандмауэра ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004} раскройте окно, связанное с именем сервера, щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) на панели задач.
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Rule name** (Название правила). В данном примере — **DHCP Reply.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).
6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Infrastructure** (Инфраструктура) и дважды щелкните элемент **DHCP (reply).** Щелкните мышью кнопку Close (Закрыть).

7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).
8. На странице **Access Rule Sources** (Источники правила доступа) щелкните мышью кнопку **Add** (Добавить).
9. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью элемент **Local Host** (Локальный хост). Щелкните мышью кнопку **Close** (Закрыть).
10. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники правила доступа).
11. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить),
12. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Networks** (Сети) и дважды щелкните мышью элемент **Internal** (Внутренний). Если вы хотите, чтобы брандмауэр ISA отвечал клиентам из многочисленных защищенных сетей при их обращении к DHCP-серверу на брандмауэре, включите все эти сети тоже. Щелкните мышью кнопку **Close** (Закрыть).
13. Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
14. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы пользователя).
15. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение работы мастера создания нового правила доступа).

Создание VPN конфигурации «узел-в-узел» между ISA Server 2000 и брандмауэром ISA

Многие администраторы брандмауэра ISA Server 2000, имеющие установленные в филиалах брандмауэры ISA Server 2000, заменяют или дополняют в центральном офисе «аппаратные» брандмауэры с пакетной фильтрацией (filter-based «hardware» firewalls) брандмауэрами ISA. Поскольку это поощряемая тенденция, мы сочли важным обсуждение объединения брандмауэра ISA Server 2000 в филиале с брандмауэром ISA в центральном офисе.

Процедура не сложна, но если у вас нет большого опыта в настройке виртуальной частной сети конфигурации узел-в-узел на брандмауэрах ISA 2000 и 2004, некоторые вещи могут показаться замысловатыми. К счастью, после знакомства с этим разделом вы увидите, как легко установить VPN-канал конфигурации узел-в-узел между этими двумя устройствами.

Прежде всего обратимся к сети лаборатории, которую мы используем как общую точку отсчета. Обычно мы настоятельно рекомендуем тестировать конфигурацию, применяя лабораторную сеть или программное обеспечение виртуализа-

ции операционной системы (operating system virtuaiization software) (им может быть Virtual Server/Virtual PC фирмы Microsoft, VMware Workstation фирмы VMware или GSX Server (и даже ESX Server))[1]. Как VPC, так и VMware отлично подходят для тестирования сценария с участием брандмауэра ISA.

На рис. 9.70 показана конфигурация сети лаборатории.

и
с филиала
10.0.2.0/24

Рис. 9.70. Конфигурация сети лаборатории

Виртуальная сеть лаборатории подобна применявшейся в других примерах книги с некоторыми пользовательскими установками для поддержания данного сценария. Сведения об IP-адресации для брандмауэров ISA приведены в табл. 9-2.

Табл. 9.2. IP-адресация и сетевая информация для VPN-шлюзов брандмауэра ISA

Параметр	ISALOCAL	REMOTEVPNISA
IP-адрес	Внешний: 192.168.1.7024 внутренний: 10.0.0.1/24	Внешний: 192.168.1.71/24 внутренний: 10.0.2.0/24
Шлюз по умолчанию	Внешний: None* внутренний: None	Внешний: None' внутренний: None
DNS	Внешний: None **внутренний:** 10.0.0.2	Внешний: None внутренний: 10.0.2.2
WINS	Внешний: None внутренний: 10.0.0,2	Внешний: None внутренний: 10.0 2.2
Диапазон IP-адресов VPN-клиентов	10.0.0.0 /24 (через DHCP)	10.0.30/24 (пул статических адресов)
ОС сервера	Windows Server 2003 ISA 2004	Windows Server 2003 ISA Server 2000
Версия брандмауэра ISA		

В вашей рабочей среде вы применяете интерфейс LAN или маршрутизатор в качестве шлюза.

Программное обеспечение, позволяющее использовать несколько операционных систем на одном сервере. — *Прим. пер.*

Мы выполним следующие процедуры для создания VPN-соединения конфигурации узел-в-узел по протоколу PPTP между брандмауэром ISA Server 2000 в филиале и брандмауэром ISA в центральном офисе:

- выполнение **Local VPN Wizard** (Мастер создания локальной VPN) на ISA Server **2000;**
- изменение **Password** (Пароль) для **Remote VPN User Account** (Учетная запись удаленного VPN-пользователя), созданной в мастере создания локальной VPN;
- изменение **Credentials** (Верительные данные), которые брандмауэр ISA Server 2000 использует для **Demand-dial Connection** (Коммутируемое соединение по требованию) с центральным офисом;
- изменение **Idle Properties** (Параметры простоя) интерфейса **Demand-dial Interface** (Интерфейс вызова по требованию) VPN-шлюза ISA Server 2000;
- создание **Static Address Pool** (Пул статических адресов) для VPN-клиентов и **шлюзов;**
- выполнение **Remote Site Wizard** (Мастер создания удаленного сайта) на бранд мауэре ISA в центральном офисе;
- создание а **Network Rule Defining the Route Relationship Between the Main and Branch Office** (Сетевое правило, определяющее маршрутную связь между центральным офисом и филиалом);
- создание **Access Rules Allowing Traffic from the Main Office to the Branch Office** (Правила доступа, разрешающие трафик из центрального офиса в филиал);
- создание учетной записи пользователя для удаленного VPN-маршрутизатора;
- тестирование соединения.

В этом разделе мы сосредоточимся на применении протокола PPTP, хотя можно использовать и протокол L2TP/IPSec, так как и ISA Server 2000, и брандмауэр ISA поддерживают протокол L2TP/IPSec для виртуальных частных сетей. Протестируем конфигурацию с помощью правила доступа «all open» (все открыто) для соединения сайтов. В вашей рабочей сети вы можете ограничить доступ некоторым пользователям из филиала в центральный офис.

Выполнение Local VPN Wizard на ISA Server 2000

Первый шаг — запуск Local VPN Wizard (мастер создания локальной VPN) на служащем VPN-шлюзом брандмауэре ISA Server 2000 филиала. Local VPN Wizard не представлял особых сложностей для нас, надеемся, что он сохранился и в новом брандмауэре ISA.

Выполните следующие шаги для запуска **Local VPN Wizard** на служащем VPN-шлюзом ISA Server 2000 филиала.

1. На консоли **ISA Management** (Управление ISA) раскройте узел **Servers and Arrays** (Серверы и массивы), а затем узел **server** (сервер). Щелкните кнопкой мыши узел **Network Configuration** (Сетевая конфигурация).

2. Щелкните правой кнопкой мыши узел **Network Configuration** (Сетевая конфигурация), а затем элемент **Set Up Local ISA VPN Server** (Установить локальный VPN-сервер ISA).
3. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Local ISA Server VPN Configuration** (Добро пожаловать в VPN-конфигурацию локального сервера ISA).
4. Щелкните мышью кнопку **Yes** (Да) в диалоговом окне **ISA Virtual Private Network (VPN) Wizard** (Мастер создания виртуальной частной сети ISA).
5. На **странице ISA Virtual Private Network (VPN) Identification** (Идентификация виртуальной частной сети ISA) (рис. 9-71) введите **Branch** в текстовое поле **Type a short name to describe the local network** (Введите короткое имя, описывающее локальную сеть). Введите **Main** в текстовое поле **Type a short name to describe the remote network** (Введите короткое имя, описывающее удаленную сеть). Щелкните мышью кнопку **Next** (Далее).

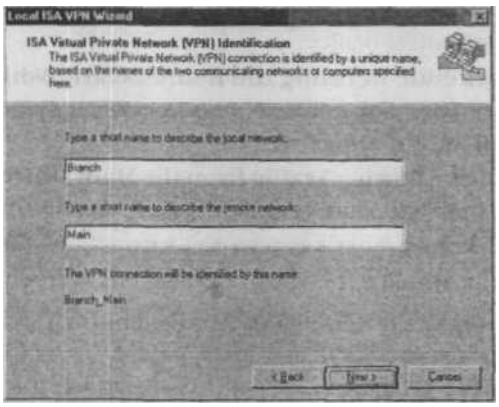


Рис. 9.71. Страница ISA Virtual Private Network (VPN) Identification (Идентификация виртуальной частной сети ISA)

6. На странице **ISA Virtual Private Network (VPN) Protocol** (Протокол виртуальной частной сети ISA) выберите переключатель **Use** PPTP (Использовать PPTP) и щелкните мышью кнопку **Next** (Далее).
7. На странице **Two-way Communication** (Двусторонний обмен сообщениями) установите флажок **Both the local and remote ISA VPN computer can initiate the connection** (Оба компьютера ISA, из локальной и удаленной VPN, могут инициировать соединение). В текстовое поле **Type the fully qualified domain name or IP address of the remote VPN computer** (Введите полностью определенное имя домена или IP-адрес компьютера удаленной VPN) введите IP-адрес брандмауэра ISA центрального офиса. В данном примере (рис. 972) — **ISA-**LOCAL. Имя домена придется вводить, только если VPN-шлюз является контрол-

лером домена, но мы уверены в том, что вы никогда бы не сделали ваш брандмауэр ISA контроллером домена. Щелкните мышью кнопку **Next** (Далее).

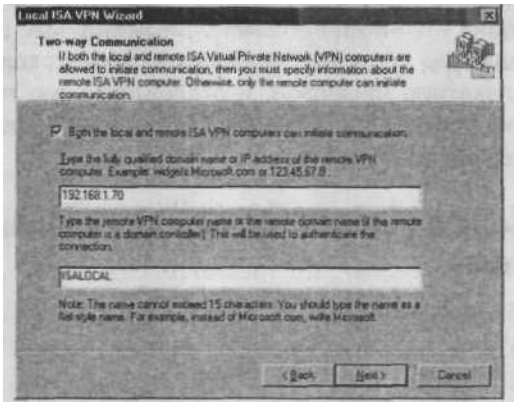


Рис. 9.72. Страница Two-way Communication (Двусторонний обмен сообщениями)

8. На странице **Remote Virtual Private Network (VPN) Network** (Сеть удаленной виртуальной частной сети) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **ISA Virtual Private Network (VPN) Wizard** (Мастер создания виртуальной частной сети ISA) введите начальный и конечный IP-адреса для сети центрального офиса. Поскольку мы используем целиком сетевой ID центрального офиса — 10.0.0.0/24, введем **10.0.0.0** в текстовое поле **From (От)** и **10.0.0.255** в текстовое поле To (До). Щелкните мышью кнопку OK, а затем кнопку **Next** (Далее).
9. На страницу **Local Virtual Private Network (VPN) Network** (Сеть локальной виртуальной частной сети) будут автоматически добавлены IP-адреса филиала. Можно щелкнуть мышью кнопку **Add** (Добавить), если нужно добавить больше адресов для представления сети филиала. Однако, поскольку эти адреса автоматически добавлены из таблицы маршрутизации Windows, убедитесь в корректности таблицы маршрутизации брандмауэра ISA Server 2000 филиала, прежде чем вставлять дополнительные адреса. Щелкните мышью кнопку **Next** (Далее).
10. На странице **ISA VPN Computer Configuration File** (Файл конфигурации VPN компьютера ISA) введите имя файла в текстовое поле **File name** (Имя файла). В данном примере введите **C:\main.** Введите пароль и его подтверждение. Имейте в виду, несмотря на то, что мы опишем процесс создания этого файла, мы не будем его использовать, потому что брандмауэр ISA его не поддерживает. Щелкните мышью кнопку **Next** (Далее).
11. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the ISA VPN Setup Wizard** (Завершение работы мастера установки виртуальной частной сети ISA).

ПРИМЕЧАНИЕ Брандмауэр ISA Server 2000 не выполняет отслеживающей состояние соединений фильтрации или проверки на прикладном уровне на VPN-клиенте удаленного доступа или VPN-интерфейсах вызова по требованию конфигурации узел-в-узел. Новый брандмауэр ISA, напротив, выполняет и отслеживающую состояние соединений фильтрацию (отслеживающую состояние пакетную проверку), и отслеживающую состояние соединений проверку на прикладном уровне на всех VPN-интерфейсах, включая интерфейс вызова по требованию.

Изменение пароля в учетной записи для удаленного VPN-пользователя

Теперь мы готовы настроить учетную запись пользователя, созданную мастером создания локальной VPN. Этот мастер создал учетную запись пользователя, которую брандмауэр ISA центрального офиса будет использовать для подтверждения подлинности VPN-шлюза филиала. Но мы не знаем, какой пароль назначил этой учетной записи мастер. Следовательно, поскольку мы будем пользоваться этой учетной записью, надо изменить ее пароль.

Выполните следующие шаги для переустановки пароля в учетной записи пользователя VPN-шлюза.

1. Щелкните правой кнопкой мыши пиктограмму **My Computer** (Мой компьютер) на рабочем столе и щелкните левой кнопкой мыши команду **Manage** (Управление).
2. На консоли **Computer Management** (Управление компьютером) раскройте узел **System Tools** (Служебные программы), а затем узел **Local Users and Groups** (Локальные пользователи и группы).
3. На правой панели щелкните правой кнопкой мыши учетную запись пользова теля **Branch_Main** и щелкните левой кнопкой мыши команду **Set Password** (Задать пароль). В диалоговом окне **Set Password for BranchMain** (Установка пароля для BranchMain) щелкните мышью кнопку **Proceed** (Продолжить).
4. Введите новый пароль и подтвердите его в диалоговом окне **Set Password for** Branch_Main. Щелкните мышью кнопку ОК.
5. Щелкните мышью кнопку ОК в диалоговом окне, информирующем о том, что пароль установлен.

Помните, что эту учетную запись пользователя вы настроили для использования брандмауэром ISA центрального офиса при вызове VPN-шлюза ISA Server 2000 филиала.

Изменение верительных данных, используемых брандмауэром ISA Server 2000 для соединения с центральным офисом по телефонной линии

Local VPN Wizard (мастер локальной VPN) создал интерфейс вызова по требованию для вызова по телефонной линии VPN-шлюза центрального офиса. В нем также сделаны предположения о правиле именования, которое использовалось бы вами для интерфейса вызова по требованию, создаваемого в центральном офисе. Нам не нравятся предложения мастера, поэтому мы собираемся изменить верительные данные, которые применяет интерфейс вызова по требованию VPN-шлюза брандмауэра ISA Server 2000, соединяясь с брандмауэром ISA центрального офиса.

Выполните следующие шаги для изменения верительных данных, используемых интерфейсом вызова по требованию VPN-шлюза брандмауэра ISA Server 2000 при подключении к брандмауэру ISA центрального офиса.

1. Откройте консоль **Routing and Remote Access** (Маршрутизация и удаленный доступ) и раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел **Interfaces** (Интерфейсы).
2. Щелкните правой кнопкой мыши интерфейс по требованию **Branch_Main,** который появляется на правой панели консоли, и щелкните мышью команду **Set Credentials** (Установить верительные данные).
3. В диалоговом окне **Interface Credentials** (Верительные данные интерфейса) измените **User name** (Имя пользователя) на **Branch.** Введите и подтвердите пароль. Интерфейс вызова по требованию, создаваемый нами в центральном офисе, будет назван **Branch.** Мы также создадим учетную запись пользователя с именем **Branch** на брандмауэре ISA центрального офиса. Запомните введен ный пароль, поскольку он понадобится при создании учетной записи **Branch** на брандмауэре ISA центрального офиса. Щелкните мышью кнопку ОК.
4. Перезапустите сервис **Routing and Remote Access Service** (Маршрутизация и удаленный доступ).

ПРИМЕЧАНИЕ Имя Branch будет именем интерфейса вызова по требованию, создаваемого нами на брандмауэре ISA центрального офиса. Вы увидите, как оно функционирует, чуть позже в этой главе.

Изменение параметров простоя интерфейса по требованию VPN-шлюза ISA Server 2000

Установка по умолчанию для интерфейса вызова по требованию на VPN-шлюзе брандмауэра ISA Server 2000 филиала — прекращение вызова после пяти минут простоя. Чтобы интерфейс никогда не разрывал соединение, надо выполнить следующие действия в диалоговом окне **Properties** (Свойства) интерфейса вызова по требованию.

1. На консоли **Routing and Remote Access** (Маршрутизация и удаленный доступ) щелкните кнопкой мыши узел **Network Interfaces** (Сетевые интерфейсы).
2. Щелкните правой кнопкой мыши интерфейс вызова по требованию **Branchy-Main** и щелкните левой кнопкой мыши строку **Properties** (Свойства).
3. В диалоговом окне **Branch_Main Properties** (Branch_Main — свойства) щелкните кнопкой мыши вкладку **Options** (Параметры), измените значение в поле **Idle time before hanging up** (Время простоя до разъединения) на **never** (никогда).
4. Измените значение в поле **Redial attempts** (Число повторений набора номера) на 99 и установите интервал между повторениями равным **10 seconds** (10 сек) (рис. 9-73). Щелкните мышью кнопку OK.

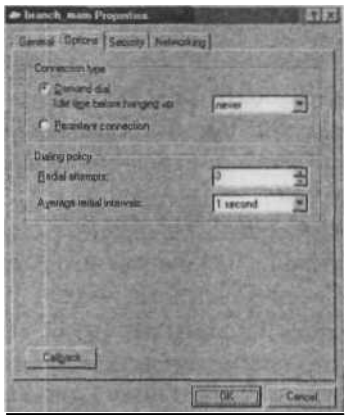


Рис. 9.73. Вкладка Options (Параметры) в диалоговом окне Properties (Свойства) интерфейса вызова по требованию

Создание пула статических адресов для VPN-клиентов и шлюзов

В данном примере у нас нет DHCP-сервера в филиале. Мы можем создать *пул* статических адресов на VPN-шлюзе филиала. Этот пул содержит адреса, которые VPN-шлюз ISA Server может назначить соединяющимся по телефонной линии VPN-клиентам и VPN-шлюзам. Мы создадим пул статических адресов, включающий целиком диапазон адресов 10.0.3.0/24.

Выполните следующие шаги для создания пула статических адресов на VPN-шлюзе ISA Server 2000 в филиале.

1. На машине брандмауэра ISA Server 2000 филиала откройте консоль **Routing and Remote Access** (Маршрутизация и удаленный доступ).
2. На консоли **Routing and Remote Access** (Маршрутизация и удаленный доступ) щелкните правой кнопкой мыши по имени сервера и левой кнопкой мыши щелкните команду **Properties** (Свойства).

3. В диалоговом окне **REMOTEVPNISA (local) Properties** (REMOTEVPNISA (локаль ный) — свойства) щелкните кнопкой мыши вкладку **IP.**
4. На вкладке **IP** выберите вариант **Static address pool** (Пул статических адресов). Щелкните мышью кнопку **Add** (Добавить).
5. В диалоговом окне **New Address Range** (Новый диапазон адресов) введите зна чения в поля **Start IP address** (Начальный IP-адрес) и **End IP address** (Конеч ный IP-адрес). В данном примере начальный IP-адрес — 10.0.3.1, а конечный — 10.0.3.254. Щелкните мышью кнопку ОК.
6. Щелкните мышью **кнопку Apply** (Применить), а затем кнопку ОК в диалоговом окне **REMOTEVPNISA (local) Properties** (REMOTEVPNISA (локальный) — свойства).
7. Перезапустите сервис **Routing and Remote Access Service** (Маршрутизация и удаленный доступ).

Выполнение Remote Site Wizard на брандмауэре ISA в центральном офисе

Теперь сосредоточим наше внимание на брандмауэре ISA в центральном офисе. У брандмауэра нет такого наглядного мастера, как Local VPN Wizard (мастер локальной VPN) брандмауэра ISA Server 2000. Но у него существует, хотя и не столь всеобъемлющий мастер, который поможет нам в создании сети удаленного сайта, представляющей используемые в филиале адреса.

Выполните следующие шаги на брандмауэре ISA центрального офиса для создания удаленной сети.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) рас кройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Virtual Private Networks (VPN)** (Виртуальные частные сети).
2. Щелкните кнопкой мыши на панели дополнительных параметров вкладку **Remo te Sites** (Удаленные сайты). Щелкните мышью вкладку **Tasks** (Задачи) на пане ли задач и затем кнопку **Add Remote Site Network** (Добавить сеть удаленного сайта).
3. На странице **Welcome to the New Network Wizard** (Вас приветствует мастер создания новой сети) введите **Branch** в текстовое поле Network **name** (Имя сети). Это имя **интерфейса** вызова по требованию брандмауэра ISA централь ного офиса. Щелкните мышью кнопку **Next** (Далее).
4. На странице **VPN Protocol** (VPN-протокол) выберите **Point-to-Point Tunneling Protocol** (PPTP) (Сквозной туннельный протокол) и щелкните мышью кнопку **Next** (Далее).
5. На странице **Remote Site Gateway** (Шлюз удаленного сайта) введите IP-адрес или полностью определенное имя домена (FQDN) внешнего интерфейса бранд мауэра ISA Server 2000 филиала. Если используется FQDN, убедитесь, что оно

преобразуется в корректный IP-адрес. В данном примере введите 192.168.1.71. Щелкните мышью кнопку Next (Далее).

6. На странице **Remote Authentication** (Удаленная аутентификация) установите флажок **Local site can initiate connections to remote site using these credentials** (Локальный сайт может инициировать подключения к удаленному сайту, используя следующие верительные данные). **Введите** имя учетной записи, которую брандмауэр ISA центрального офиса будет использовать для подтверждения подлинности VPN-шлюза ISA Server 2000 филиала. Это имя, используемое для интерфейса вызова по требованию, созданного на брандмауэре ISA филиала. В данном примере — **Branch_Main.** Введите имя компьютера VPN-шлюза ISA Server 2000 филиала в текстовое поле **Domain** (Домен). В этом примере введите **REMOTEVPNISA.** Введите пароль и его подтверждение учетной записи пользователя **Branch_Main,** созданной на брандмауэре Server 2000 в филиале. Ш,елкните мышью кнопку **Next** (Далее) (рис. 9.74).

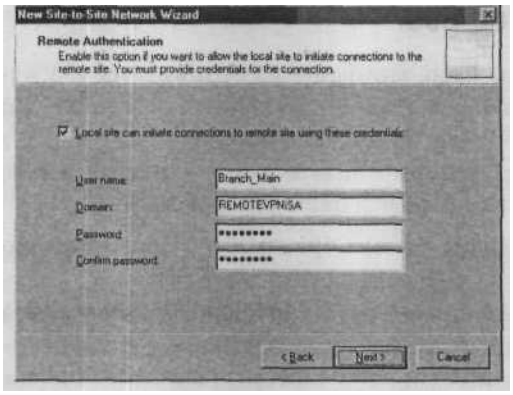


Рис. 9.74. Страница Remote Authentication (Удаленная аутентификация)

7. На странице **Local Authentication** (Локальная аутентификация) вы найдете напоминание о том, что необходимо создать учетную запись пользователя на брандмауэре ISA центрального офиса, которую VPN-шлюз ISA Server 2000 фи лиала будет использовать для аутентификации. Мы создадим эту запись позже. У нее должно быть то же имя, что и у интерфейса вызова по требованию, соз данного на брандмауэре ISA центрального офиса, в данном примере **Branch.** Щелкните мышью кнопку **Next** (Далее).
8. На странице **Network Addresses** (Сетевые адреса) введите IP-адреса, использу емые в сети филиала. В данном примере в филиале используется целиком сеть с сетевым идентификатором 10.0.2.0/24. Щелкните мышью кнопку **Add.** Введи те начальный адрес **10.0.2.0** и конечный адрес **10.0.2.255-** Щелкните мышью кнопку ОК, а затем кнопку **Next** (Далее).
9. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Network Wizard** (Завершение мастера создания новой сети).

Создание сетевого правила, определяющего маршрутную связь между центральным офисом и филиалом

Как любой брандмауэр с отслеживающей состояние соединений фильтрацией (пакетной проверкой, отслеживающей состояние соединений), брандмауэр ISA позволяет управлять маршрутной связью между сетью-источником и сетью-адресатом. Мы предпочитаем использовать маршрутную связь между сетями, соединенными виртуальной частной сетью конфигурации узел-в-узел. Но вы можете применить средства NAT (network address translation, преобразование сетевых адресов). Однако имейте в виду, что не все приложения функционируют при наличии NAT.

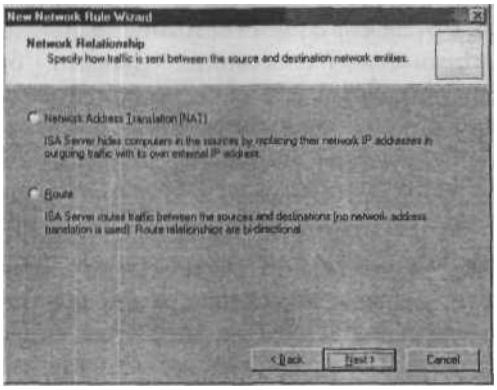
> ПРЕДУПРЕЖДЕНИЕ Несмотря на то, что вы можете выбрать вариант применения NAT, мы не тестировали эту конфигурацию, поэтому она может и не работать. Используйте средства NAT на свой страх и риск. Можно уменьшить риск, протестировав этот вариант сначала в вашей лаборатории.

В данном примере мы создадим маршрутную связь между центральным офисом и филиалом. Выполните следующие шаги для формирования сетевого правила, управляющего данной маршрутной связью.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищен ного быстрого доступа к сети Интернет Server 2004) рас кройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Con figuration** (Конфигурация). Щелкните мышью узел **Networks** (Сети).
2. В узле **Networks** (Сети) щелкните кнопкой мыши вкладку **Network Rules** (Сетевые правила). Щелкните мышью вкладку **Tasks** (Задачи) на панели задач и щелкните мышью ссылку **Create a New Network Rule** (Создать новое сетевое правило).
3. На странице **Welcome to the New Network Rule Wizard** (Вас приветствует мас тер создания нового сетевого правила) введите название правила в текстовое поле **Network rule name** (Название сетевого правила). В данном примере — **Main to Branch.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Network Traffic Sources** (Источники сетевого трафика) щелкни те мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети). Дважды щелкните кнопкой мыши сеть **Internal** (Внутренняя). Щелкните мышью кнопку **Close** (Закрыть).
5. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Sources** (Источники сетевого трафика).
6. На странице **Network Traffic Destinations** (Адресаты сетевого трафика) щелк ните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) дважды щелкните кнопкой мыши сеть **Branch** (Фи лиал). Щелкните мышью кнопку **Close** (Закрыть).
7. Щелкните мышью кнопку **Next** (Далее) на странице **Network Traffic Destina tions** (Адресаты сетевого трафика).

Рис. 9.75. Страница Network Relationship (Связь сетей)

8. На странице **Network Relationship** (Связь сетей) (рис. 9.75) выберите вариант **Route** (Маршрут) и щелкните мышью кнопку Next (Далее).



9. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Network Rule Wizard** (Завершение мастера создания нового сетевого правила).

Создание правил доступа, разрешающих трафик из центрального офиса в филиал

В то время как VPN-шлюз ISA Server 2000 филиала не выполняет отслеживающую состояние соединений фильтрацию или проверку прикладного уровня его VPN-интерфейсов, брандмауэр ISA центрального офиса делает это. Следовательно, необходимо создать правила доступа, управляющие трафиком из филиала к центральному офису и из центрального офиса к филиалу.

Выполните следующие шаги для создания правил доступа.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. Щелкните мышью вкладку Tasks (Задачи) на панели задач и ссылку **Create New Access Rule** (Создать новое правило доступа).
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле **Access Rule name** (Название правила доступа). В данном примере введите **All Open Main-Branch.** Щелкните мышью кнопку **Next** (Далее).
4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).

5. На странице **Protocols** (Протоколы) согласитесь с вариантом по умолчанию в списке **This rule applies to** (Это правило применяется к) и щелкните мышью кнопку **Next** (Далее).
6. На странице **Access Rule Sources** (Источники в правиле доступа) щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (До бавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети). Дваж ды щелкните мышью узел **Internal** (Внутренняя) и щелкните мышью кнопку **Close** (Закрыть). Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Sources** (Источники в правиле доступа).
7. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкни те мышью кнопку **Add** (Добавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети). Дважды щелкните мышью узел **Branch** (Филиал) и щелкните мышью кнопку **Close (Закрыть).** Щелкните мышью кнопку **Next** (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).
8. Щелкните мышью кнопку **Next** (Далее) на странице **User Sets** (Наборы поль зователей).
9. Щелкните кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).
10. Щелкните правой кнопкой мыши правило **All Open Main-Branch** и выберите левой кнопкой мыши команду **Copy** (Копировать).
11. Щелкните правой кнопкой мыши правило **All Open Main-Branch** и выберите левой кнопкой мыши команду **Paste** (Вставить).
12. Дважды щелкните кнопкой мыши правило **All Open Main-Branch(l).**
13- В диалоговом окне АН **Open Main-Branch(l) Properties** (All Open Main-Branch(l) — свойства) щелкните кнопкой мыши вкладку **General** (Общие). Из-мените название правила на **All Open Branch-Main.**
14. Щелкните мышью вкладку **From** (От). Щелкните кнопкой мыши элемент **Internal** (Внутренняя) и кнопку **Remove** (Удалить). Щелкните мышью кнопку **Add** (До бавить). В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши папку **Networks** (Сети) и дважды щелкните мышью элемент **Branch.** Щелкните мышью кнопку **Close** (Закрыть).
15. Щелкните кнопкой мыши вкладку То (К). Щелкните мышью элемент **Branch** и кнопку **Remove** (Удалить). Щелкните мышью кнопку **Add** (Добавить). Щелкни те кнопкой мыши папку **Networks** (Сети) и дважды щелкните мышью элемент **Internal** (Внутренняя). Щелкните мышью кнопку **Close** (Закрыть).
16. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК.
17. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
18. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

19. Ваша политика брандмауэра будет выглядеть так, как показано на рис. 9.76 (у вас могут быть и другие правила, однако данные правила разместите над другими правилами).

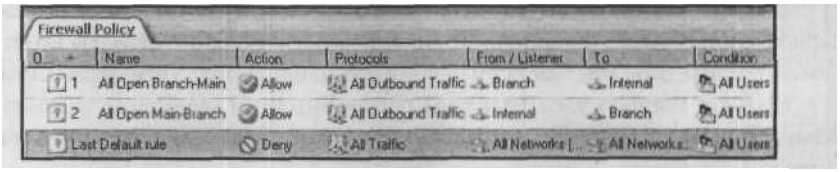


Рис. 9.76. Результирующая политика брандмауэра 20. Перезапустите

компьютер с брандмауэром ISA в центральном офисе.

Создание учетной записи пользователя для удаленного VPN-маршрутизатора

Remote site Wizard (Мастер удаленного сайта) не создает учетную запись пользователя для брандмауэра ISA Server 2000 в филиале, подтверждающую его подлинность на брандмауэре ISA центрального офиса. Мы создадим эту учетную запись самостоятельно.

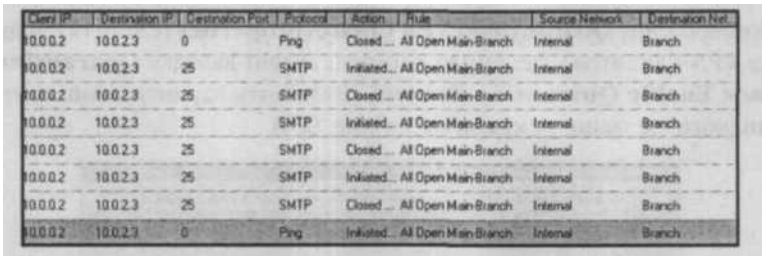
Выполните следующие шаги для создания учетной записи пользователя.

1. Щелкните правой кнопкой мыши пиктограмму **My Computer** (Мой компьютер) и левой кнопкой мыши команду **Manage** (У правление).
2. На консоли **Computer Management** (Управление компьютера) раскройте узел **System Tools** (Служебные программы) и затем узел **Local Users and Groups** (Локальные пользователи и группы).
3. Щелкните правой кнопкой мыши папку **Users** (Пользователи) и левой кнопкой мыши щелкните команду **New User** (Новый пользователь).
4. В диалоговом окне **New User** (Новый пользователь) введите имя интерфейса вызова по требованию на брандмауэре ISA в центральном офисе. В данном при мере имя этого интерфейса — **Branch.** Введите пароль и его подтверждение. Сбросьте флажок **User must change password at next logon** (Потребовать смену пароля при следующем входе в систему). Установите флажки **User cannot change password** (Запретить смену пароля пользователем) и **Password never expires** (Срок действия пароля неограничен). Щелкните мышью кнопку **Create** (Создать).
5. Дважды щелкните кнопкой мыши учетную запись пользователя с именем **Branch.** В диалоговом окне **Branch Properties** (Свойства: Branch) щелкните кнопкой мыши вкладку **Dial-in** (Профиль). На этой вкладке выберите переключатель **Allow access** (Подключить) в области окна **Remote Access Permission (Dial-in or VPN)** (Разрешение удаленного доступа, удаленный доступ по телефонной линии или виртуальная частная сеть).

Тестирование соединения

Теперь протестируем соединение. С хоста в сети центрального офиса выполните команду ping для хоста в сети филиала. Вы должны увидеть отклик на команду ping после нескольких сообщений об отсутствии отклика, так как интерфейс вызова по требованию инициализируется. Если вы не получите ответа после четырехкратного выполнения команды ping, попробуйте еще раз. После того, как соединение установлено, попробуйте воспользоваться Telnet для соединения с SMTP-сервером в сети удаленного хоста.

На рис. 977 показаны записи журнала регистрации, относящиеся к этим двум тестам.



Client IP	Destination IP	Destination Port	Protocol	Action	Rule	Source Network	Destination Net
10.0.0.2	10.0.2.3	0	Ping	Closed ...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Initiated...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Closed ...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Initiated...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Closed ...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Initiated...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	25	SMTP	Closed ...	All Open Main-Branch	Internal	Branch
10.0.0.2	10.0.2.3	0	Ping	Initiated...	All Open Main-Branch	Internal	Branch

Рис. 9.77. Записи журнала регистрации о соединениях команды Ping и подключении к SMTP-серверу

Заметки о VPN-карантине

Как упоминалось во введении к этой главе, у брандмауэра ISA есть функциональная возможность предварительной «проверки правомочности» VPN-клиентов, прежде чем разрешить им соединение с корпоративной сетью. Это свойство брандмауэра ISA, именуемое *VPN Quarantine (VPN-карантин)*. Соответствующим образом реализованный VPN-карантин можно использовать для помещения всех VPN-клиентов в специальную сеть VPN-карантина и содержания их в этой сети до тех пор, пока они не пройдут ряд тестов безопасности. После того как VPN-клиент успешно пройдет эти тесты безопасности, он автоматически удаляется из сети VPN-карантина и перемещается в сеть VPN-клиентов.

Проблема выполнения VPN-карантина на брандмауэре ISA заключается в том, что он совершенно бесполезен для типичного администратора брандмауэра ISA, не имеющего серьезных навыков создания сценариев или программирования. Поставляемый в составе брандмауэра ISA VPN-карантин предоставляет только *платформу разработки (development platform)* для реализации VPN-карантина. В действительности без коллектива разработчиков, способных помочь воплотить реализацию VPN-карантина (VPN-Q), вы можете полностью заблокировать для всехVPN-клиентов доступ к ресурсам, для которых вы создали правила доступа, разрешающие доступ к ним.

К сожалению, пользовательский интерфейс брандмауэра может создать впечатление, что включение VPN-карантина — это установка соответствующего флажка. Для того чтобы понять, что мы имеем в виду, откройте панель управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004), раскройте окно, связанное с именем сервера, затем раскройте узел **Configuration** (К он фи гу рация) и щелкните кнопкой мыши узел **Networks** (Сети).

В узле **Networks** (Сети) щелкните правой кнопкой мыши сеть **Quarantined VPN Clients** (Подвергнутые карантину VPN-клиенты) на вкладке **Networks** (Сети) панели дополнительных параметров и щелкните левой кнопкой мыши команду **Properties** (Свойства).

В диалоговом окне **Quarantined VPN Clients Properties** (Свойства подвергнутых карантину VPN-клиентов) щелкните кнопкой мыши вкладку **Quarantine.** Установите флажок **Enable Quarantine Control** (Включить карантинный контроль). Вы увидите диалоговое окно, показанное на рис. 9.78.

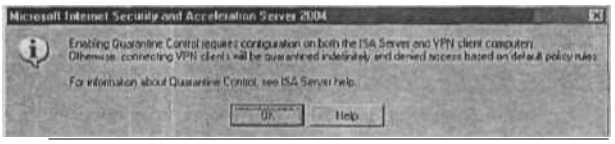


Рис. 9.78. Предупреждение, относящееся *к* VPN-карантину и доступу VPN-клиентов

Это диалоговое окно утверждает, что включение контроля с помощью VPN-карантина требует конфигурирования как компьютера сервера ISA, так и компьютера VPN-клиента. В противном случае, подключающиеся VPN-клиенты будут подвергаться карантину неопределенно долго и доступ, базирующийся на правилах политики по умолчанию, будет запрещен. Это означает, что пока вы не выполните обеспечивающие корректный VPN-карантин процедуры конфигурирования и разработки, *все* VPN-клиенты останутся в сети VPN-клиентов, подвергнутых карантину, и смогут получить доступ только к тем ресурсам, которые доступны членам этой сети. Конечно, вы могли бы создать правила доступа, разрешающие членам сети VPN-клиентов, подвергнутых карантину, доступ к любому ресурсу в корпоративной сети, но это прежде всего уничтожит смысл применения VPN-Q.

После включения VPN-карантина вы увидите, что у вас появляются следующие возможности.

- **Quarantine according to RADIUS server policies** (Карантин в соответствии с политиками RADIUS-сервера) Этот вариант доступен только, если брандмауэр ISA установлен на машинах под управлением ОС Windows Server 2003. Он позволяет реализовать политику VPN-карантина RADIUS-сер вера.

Quarantine according to ISA Server policies (Карантин в соответствии с политиками сервера ISA) Это вариант может применяться на компьютерах под управлением Windows 2000 для включения VPN-Q.

Disconnect quarantined users after (seconds) (Отсоединение пользователей, подвергнутых карантину через, секунд) Этот вариант позволяет ограничить время пребывания VPN-клиентов в сети Quarantined VPN Clients. Если VPN-клиент не может выполнить процедуры, требуемые для его удаления из карантина, за данный промежуток времени, он отсоединяется.

Exempt these users from Quarantine Control (Освободить данных пользователей от карантинного контроля) Можно избавить пользователей или группы от помещения в сеть Quarantined VPN Clients (VPN-клиентов, подвергнутых карантину), включив их в данный список. Возможные варианты на вкладке **Quarantine** (Карантин) показаны на рис. 9.79.

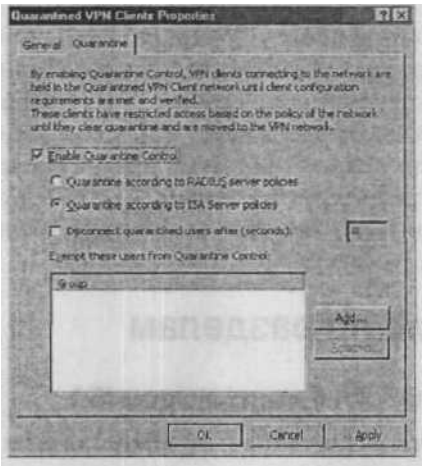


Рис. 9.79. Вкладка **Quarantine** (Карантин) на странице **Quarantined VPN Client Properties** (Свойства подвергнутых карантину VPN-клиентов)

Если в вашем распоряжении есть разработчики или вы умеете программировать и писать сценарии, посмотрите документацию фирмы Microsoft о VPN-Q по адресу http://www.microsoft.com/isaserver/techinfo/guidance/2004/vpn.asp.

Есть хорошие новости и для тех администраторов брандмауэра ISA, у которых нет доступа к расширенным ресурсам по разработке и написанию сценариев. Фредерик Исноуф (Frederic Esnouf), обладающий званием MVP (Microsoft Most Valuable Professional — An annual award given by Microsoft to members of the computing community), разработал полнофункциональную законченную реализацию VPN-карантина, названную Quarantine Security Suite (QSS) (комплект защиты с помощью карантина). Мы настоятельно рекомендуем предложенное Фредериком решение; более подробную информацию о нем можно найти по адресу http://fesnoufonline.fr/programs/QSS/QSS.htm.

В разработку фирмы Avanade также включена помощь в решении головоломки VPN-Q. По адресу http://www.avanade.com/solutions/section.aspx?id=8&parentID=2 можно найти экспериментальные программные средства (prototype software), которые помогут создать действующий вариант VPN-Q.

СОВЕТ Если вы считаете себя специалистом по написанию сценариев в ОС Windows, корпорация Microsoft выпустила недавно несколько образцов сценариев, которые вы можете настроить для своей производственной среды. Прочитать о них можно на странице **VPN Quarantine Sample Scripts for Verifying Client Health Configurations** (примеры сценариев VPN-карантина для проверки конфигураций состояний клиентов) (www.microsoft.com/downloads/details.aspx?FamilyID=a290f2ee-0b55-491e-bc4c-8161671b2462&displaylang=en).

Резюме

В этой главе мы обсудили свойства VPN-сервера удаленного доступа брандмауэра ISA и VPN-шлюза. VPN-сервер удаленного доступа поддерживает подключения VPN-клиентов удаленного доступа как по протоколу PPTP, так и по протоколу L2TP/lPSec. VPN-шлюз брандмауэра ISA поддерживает поступающие от других VPN-шлюзов соединения в туннельном режиме протокола IPSec, а также по протоколам PPTP и L2TP/IPSec. Мы рассмотрели и другие темы, связанные с поддержкой брандмауэром ISA VPN-клиентов и шлюзов, включая аутентификацию по протоколу EAP и конфигурирование DHCP-сервера.

Краткое резюме по разделам

Обзор использования VPN брандмауэром ISA

0 Политика брандмауэра в сочетании с отслеживающими состояние соединений фильтрацией и проверкой на прикладном уровне применяется к VPN-клиентам удаленного доступа брандмауэра ISA и интерфейсам VPN-шлюзов.

И В состав брандмауэра ISA включен VPN-карантин, позволяющий проверить правомочность VPN-клиентов, прежде чем разрешить им доступ к сети. Предварительная проверка включает в себя подтверждение того, что на клиенте установлены самые свежие оперативные коррекции (hotfixes), сервисы, антивирусные и антишпионские (anti-spyware) определения.

S3 Свойство отображения пользователей брандмауэра ISA позволяет преобразовать пользователей, подтвердивших подлинность с помощью сервиса RADIUS или по протоколу EAP, в действующие учетные записи пользователей и использовать эту информацию для строгого, базирующегося на пользователе/группе контроля доступа для соединений удаленного доступа VPN и VPN-шлюзов с брандмауэром ISA.

0 Теперь поддержка клиента SecureNAT предоставляет VPN-клиентам удаленного доступа возможность выхода в Интернет через брандмауэр ISA без установки клиента брандмауэра на машине VPN-клиента удаленного доступа.

0 Поддержка туннельного режима протокола IPSec позволяет брандмауэру ISA устанавливать VPN-соединения конфигурации узел-в-узел с низкоуровневыми VPN-устройствами сторонних разработчиков, такими как VPN-концентраторы фирмы Cisco.

0 Новый PPTP-фильтр предоставляет возможность публикации VPN-серверов по протоколу PPTP.

0 Брандмауэр ISA поддерживает сертификаты и секретные ключи (pre-shared keys) для туннельного режима протокола IPSec и VPN-соединений по протоколу L2TP/IPSec. В случае протокола L2TP/IPSec такая поддержка обеспечивается для клиентов удаленного доступа и соединений VPN-шлюзов.

0 Новый брандмауэр ISA позволяет назначать настраиваемые серверы имен VPN-клиентам, для того чтобы вы не зависели от адресов интерфейса сервера имен при назначении сервера имен VPN-клиенту.

S Можно отслеживать соединения VPN-клиента и VPN-шлюза, проходящие через брандмауэр ISA. Появилась возможность определения имени пользователя, приложения, протоколов и IP-адреса источника и адресата, а также дополнительной информации, просматривая консоль регистрационных журналов брандмауэра ISA.

Создание VPN-сервера удаленного доступа по протоколу PPTP

И Используйте консоль управления Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004), а не консоль сервиса RRAS (Routing and Remote Access Services, сервис маршрутизации и удаленного доступа).

0 Если для назначения адресов VPN-клиентам и шлюзам применяется DHCP-сервер, убедитесь в том, что у вас есть в запасе достаточно IP-адресов для поддержки нужного вам числа соединений VPN-клиентов.

И Версия ISA 2004 Standard Edition поддерживает до 1000 одновременных VPN-соединений независимо от операционной системы, в которой установлено программное обеспечение брандмауэра.

ЕЯ Можно создать разрешение для удаленного доступа по сети VPN с помощью настройки учетной записи пользователя или политики удаленного доступа.

0 Отображение пользователей особенно полезно при применении аутентификации сертификатом пользователя по протоколу EAP (Extensible Authentication Protocol, наращиваемый протокол аутентификации). Оно позволяет выполнить основанный на пользователе/группе контроль пользователей, подтверждающих подлинность с помощью аутентификации сертификатом пользователя по протоколу EAR

0 Применяйте DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) для назначения IP-адресов вашим VPN-клиентам, если

хотите использовать адреса из подсети *(cm-subnet* addresses) для ваших VPN-клиентов. Если вы применяете пул статических адресов, необходимо удалить эти адреса из определения сети, уже определенной на брандмауэре ISA с использованием адресов.

Создание VPN-сервера удаленного доступа по протоколу L2TP/IPSec

0 Можно применять как сертификаты компьютера, так и секретные ключи (pre-shared keys) для соединений VPN-клиентов удаленного доступа по протоколу L2TP/IPSec.

0 Следует временно отключить RPC-фильтр для получения с помощью изолированной оснастки Certificates сертификата брандмауэра ISA от оператиного центра сертификации.

Е Новый VPN-клиент для протокола L2TP/IPSec допускает использование почти всех версий ОС Windows для установки VPN-соединения удаленного доступа с брандмауэром ISA по протоколу L2TP/IPSec. Кроме того, новое программное обеспечение поддерживает секретные ключи (pre-shared key) и средства обходящего NAT (NAT traversal).

И Секретные ключи снижают масштабируемость и безопасность аутентификации с помощью сертификатов, но служат приемлемой заменой до тех пор, пока вы не установили инфраструктуру открытого ключа (public key infrastructure).

Создание VPN-соединения «узел-в-узел» по протоколу PPTP

И Виртуальная частная сеть конфигурации узел-в-узел соединяет целые сети друг с другом.

И Мастер сети удаленного сайта нужно выполнить на обеих сторонах VPN-соединения конфигурации узел-в-узел.

Я На каждом брандмауэре ISA следует создать учетную запись пользователя, которую вызывающий брандмауэр ISA может использовать для аутентификации на отвечающем брандмауэре ISA.

0 Необходимо создать правила доступа, разрешающие трафик к/от каждой сети, соединенной VPN-каналом конфигурации узел-в-узел.

И На каждом брандмауэре ISA, участвующем в VPN-связи конфигурации узел-в-узел, необходимо создать сетевое правило, определяющее маршрутную связь между локальной и удаленной сетями.

0 Можно использовать IP-адрес или FQDN (полностью определенное доменное имя) при определении адреса шлюза удаленного сайта. Это полезно, если в филиалах на внешних интерфейсах применяются динамические адреса.

0 Интерфейс вызова по требованию, созданный мастером создания сети удаленного сайта, определяет имя учетной записи пользователя, которую вызывающий брандмауэр ISA должен использовать для аутентификации на этом интерфейсе. Если вызывающий VPN-шлюз не применяет учетную запись с именем вызывае-

мого интерфейса, соединение трактуется как соединение VPN-клиента удаленного доступа и маршрутизация между сетями не выполняется.

Создание VPN-соединения «узел-в-узел» по протоколу L2TP/IPSec

0 Протокол L2TP/IPSec — более защищенный VPN-протокол, чем PPTP.

0 Аутентификация для VPN-соединений конфигурации узел-в-узел с помощью сертификатов компьютеров более безопасна, чем подтверждение подлинности с помощью секретных ключей (pre-shared key). 0 Протокол L2TP/IPSec использует транспортный UDP-протокол для своего канала управления, что может обеспечить большую степень стабильности VPN-соединений конфигурации узел-в-узел по протоколу L2TP/IPSec.

Использование системы RADIUS для VPN-аутентификации и политики удаленного доступа

0 На внешнем и внутреннем брандмауэрах ISA можно отказаться от членства брандмауэра в домене, а применять RADIUS-аутентификацию для соединений VPN-клиентов удаленного доступа.

0 Сервис RADIUS может использоваться для централизации политики удаленного доступа в пределах организации. Это избавляет от необходимости копирования политики удаленного доступа на многочисленные VPN-серверы удаленного доступа брандмауэра ISA и его VPN-шлюзы.

И RADIUS-аутентификация для VPN-клиентов удаленного доступа поддерживает как подтверждение подлинности ОС Windows, так и EAP-аутентификацию сертификатами пользователя.

0 Разрешения для соединений по телефонной линии можно настроить, основываясь на учетных записях или группах, с помощью политики удаленного доступа. Только локальные учетные записи в SAM (Security Accounts Manager, диспетчер учетных записей безопасности) или учетные записи доменов, находящихся в режимах Native Mode или Windows Server 2003 Mode, поддерживают установку разрешений соединений по телефонной линии через политику удаленного доступа.

Применение аутентификации сертификатами пользователя с помощью протокола EAP для VPN-соединений удаленного доступа

0 EAP-аутентификация сертификатами пользователя обеспечивает более высокий уровень защиты по сравнению с традиционным подтверждением подлинности с помощью имени пользователя/пароля.

Я Можно использовать свойство отображения пользователей брандмауэра ISA для поддержки ориентированных на пользователя/группу средств управления пользователями, подтверждающими подлинность с помощью протокола EAR Но при этом брандмауэр ISA должен быть членом домена.

Создание VPN конфигурации «узел-в-узел» между ISA Server 2000 и брандмауэром ISA

0 Можно создать виртуальные частные сети конфигурации узел-в-узел между брандмауэрами ISA и ISA Server 2000. На компьютере с ISA Server 2000 можно воспользоваться мастером создания локальной VPN (Local VPN Wizard), а на компьютере с брандмауэром ISA — мастером создания сети удаленного сайта (Remote Site Network Wizard).

И Мастер создания локальной сети на машине с ISA Server 2000 автоматически создает учетную запись для использования вызывающим VPN-шлюзом. Но вам придется изменить пароль этой учетной записи, потому что вы не знаете пароля, назначенного ей мастером создания локальной VPN.

Заметки о VPN-карантине

И VPN-карантин позволяет проверить правомочность VPN-клиентов, прежде чем разрешить им доступ к корпоративной сети. Процесс предварительной проверки правомочности включает проверку того, что у VPN-клиента установлены последние обновления системы безопасности, оперативные корректировки (hot-fixes), антивирусные сигнатуры (anti-virus signatures), сигнатуры антишпионского ПО (anti-spyware signatures) и т. д.

S3 Реализация VPN-Q брандмауэра ISA — скорее платформа для разработки чем свойство, которое может использоваться типичным новоиспеченным администратором брандмауэра ISA.

И Quarantine Security Suite (комплект защиты с помощью карантина) Фредерика Исноуфа (Frederic Esnouf) — эффективное решение проблемы VPN-Q.

И Фирма Avanade предоставляет среду разработки, которую можно применять для создания функционирующего варианта VPN-Q, использующего брандмауэр ISA.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»),** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Я хочу создать VPN конфигурации узел-в-узел между сетями филиалов и центрального офиса. Должен ли я менять схему IP-адресации в какой-либо из этих сетей?

О: Это зависит от текущей схемы IP-адресации. Брандмауэры ISA, соединяющие центральный офис с филиалами, действуют как VPN-маршрутизаторы. Маршрутизаторы прокладывают маршруты между сетями с различными сетевыми

идентификаторами. Следовательно, если любой из ваших филиалов использует адреса с тем же сетевым ID, что и центральный офис или любой другой филиал, необходимо изменить схему IP-адресации в этом офисе, для того чтобы все сети, объединяемые VPN-каналами конфигурации узел-в-узел, имели разные сетевые идентификаторы.

В: Я хочу использовать систему Voice over IP system (VoIP) (передача голоса по IP-протоколу) для вызовов внутри организации в нашем центральном офисе и филиалах. Я планирую применить сети VPN конфигурации узел-в-узел брандмауэра ISA для соединения офисов. Я должен использовать маршрутную связь или средства NAT между сетями, соединяемыми с помощью VPN-каналов конфигурации узел-в-узел?

О: Известно, что системы VoIP плохо сосуществуют со средствами NAT, поскольку они часто встраивают IP-адрес клиента в данные прикладного уровня. Если вы планируете реализацию VoIP, то, конечно, используйте сетевые правила маршрутизации между всеми вашими сетями, соединяемыми с помощью VPN-каналов конфигурации узел-в-узел.

В: Я использую EAP-аутентификацию сертификатами пользователя на моем VPN-сервере удаленного доступа брандмауэра ISA. Однако, когда пользователи пытаются соединиться с VPN-сервером, их соединения немедленно разрываются. Как исправить это?

О: Вероятнее всего проблема заключается в том, что ваш брандмауэр ISA — не член домена. При использовании EAP-аутентификации сертификатами пользователя брандмауэр ISA должен быть членом домена. Другая ситуация, в которой возникает эта проблема, — применение RADIUS-аутентификации VPN-клиентов и активизация отображения пользователей. Если брандмауэр ISA — не член домена, то не существует базы данных пользователей Windows, в которую выполняется отображение и поэтому VPN-соединение разрывается сразу после запроса на соединение.

В: Мои VPN-соединения конфигурации узел-в-узел часто разрываются, и зачастую я должен выполнять перезагрузку сервера для их восстановления. Могу ли я сделать что-нибудь для устранения этой проблемы?

О: Если вы используете протокол PPTP для сети VPN конфигурации узел-в-узел, подумайте о применении протокола L2TP/IPSec. Есть сведения о большей стабильности VPN-соединений по протоколу L2TP/IPSec. Еще один вариант, заслуживающий внимания, — убедиться в том, что только одна сторона VPN-канала конфигурации узел-в-узел сконфигурирована как вызывающий VPN-шлюз и один узел служит отвечающим VPN-шлюзом. Если обе стороны настроены как вызывающие VPN-шлюзы, есть возможность возникновения «конфликта», когда они оба попытаются обратиться друг к другу в одно и то же время. Если вы применяете DSL-соединение (Digital Subscriber Line, цифровая абонентская линия), проверьте, нет ли на пути маршрутизаторов-черных дыр (black hole routers), тести-

руя и регулируя MTU (Maximum Transmission Unit, максимальный блок данных) на брандмауэре ISA и клиентах. Эта проблема связана прежде всего с любительскими учетными записями протокола PPPoE (PPP over Ethernet). Стоит получить DSL-канал бизнес-класса, чтобы преодолеть проблему размера MTU.

В: Я установил сертификат машины на моем брандмауэре ISA, для того чтобы использовать протокол L2TP/IPSec в соединениях моих VPN-клиентов удаленного доступа. Однако соединения всегда дают сбой. При этом нет никаких проблем, когда я пытаюсь установить соединение с помощью протокола PPTP. Что можно сделать, чтобы заставить протокол L2TP/IPSec работать?

О: Одна из обычных причин сбоев соединений по протоколу L2TP/IPSec заключается в том, что при наличии компьютерного сертификата на брандмауэре ISA или на VPN-клиентах на этих машинах отсутствует сертификат ЦС корневого центра сертификации, выдающего сертификаты, в хранилище сертификатов Trusted Root Certification Authorities (доверенные корневые центры сертификации). Другая возможная причина сбоев протокола L2TP/IPSec состоит в том, что машинам назначаются сертификаты пользователей вместо сертификатов компьютеров. Сертификаты компьютеров хранятся в хранилище компьютерных сертификатов, а сертификаты пользователей — в хранилище сертификатов пользователей.

В: Я хочу создать виртуальную частную сеть конфигурации узел-в-узел между моим главным офисом и филиалами с помощью брандмауэров ISA. Сейчас у нас есть брандмауэры/^РИ-шлюзы сторонних организаций, как в главном офисе, так и в филиале, и для канала конфигурации узел-в-узел на них используется по большей части туннельный режим протокола IPSec и секретные ключи (shared keys). Следует ли использовать те же методы при замене описанных устройств брандмауэрами ISA?

О: Нет. Наивысшего уровня защиты можно достичь, используя протокол L2TP/IPSec с EAP-аутентификацией сертификатами пользователя для последовательности PPP-аутентификации (PPP authentication sequence). Мы рекомендуем применять туннельный режим протокола IPSec только для VPN-каналов конфигурации узел-в-узел, поддерживающих соединения между брандмауэром ISA и низкоуровневыми (downlevel) VPN-шлюзами.

Глава 10

Динамическая фильтрация и фильтрация на уровне приложений в брандмауэре ISA Server 2004

Основные темы главы:

- **Фильтры приложений**
- **Web-фильтры**

Введение

Брандмауэр ISA способен выполнять как динамическую фильтрацию[1] пакетов, так и их динамическую проверку на уровне приложений. Набор параметров динамической фильтрации брандмауэра ISA позволяет причислить его к классу брандмауэров с динамической фильтрацией на сетевом уровне, а также к классу аппаратного брандмауэра, выполняющего подобную фильтрацию на сетевом и транспортном уровнях. Динамическую фильтрацию часто называют пакетной проверкой с отслеживанием состояния соединения *(stateful packet inspection),* что не совсем правильно, поскольку пакеты — это объекты 3-го уровня OSI (layer 3), а для того чтобы оценить состояние соединения, необходимо определить информацию на 4-м уровне.

В отличие от традиционных пакетных фильтров базовых брандмауэров с динамической фильтрацией брандмауэр ISA способен выполнять динамическую проверку (фильтрацию) на уровне приложений. Такая проверка позволяет брандмауэру ISA полностью обследовать коммуникационные потоки, проходящие через него из одной сети в другую. Истинная проверка с отслеживанием состояния соединения в отличие от динамической фильтрации, проверяющей информацию только на сетевом и транспортном уровнях, требует, чтобы брандмауэр мог анализировать и принимать решения на всех коммуникационных уровнях, включая наиболее важный прикладной уровень или уровень приложений.

В этой главе мы обсудим фильтры приложений и web-фильтры.

Web-фильтры выполняют динамическую фильтрацию информации, передаваемой компонентами Web-прокси брандмауэра ISA, на уровне приложений. Web-прокси поддерживает соединения для протоколов HTTP, HTTPS (SSL) и HTTP tunneled FTP. Web-фильтры разделяют на составляющие HTTP-сообщения и предоставляют их средствам проверки на уровне приложений брандмауэра ISA, примерами которых служат фильтр защиты HTTP (HTTP Security filter) и OWA-фильтр аутентификации, основанной на формах (OWA forms-based authentication filter).

Фильтры приложений отвечают за выполнение динамической фильтрации на прикладном уровне протоколов, отличных от HTTP, таких как SMTP, POP3 и DNS. Эти фильтры также расчленяют сообщения на составляющие и предоставляют их для глубокой динамической фильтрации на брандмауэре ISA.

Web-фильтры и фильтры приложений могут обеспечивать две функции:

- доступ протокола;
- защиту протокола.

[1] Динамическая фильтрация (stateful inspection) изобретена и запатентована компанией Check Point Software Technologies. — *Прим. пер.*

Доступ протокола обеспечивает доступ для протоколов, требующих вторичных соединений. Сложные протоколы (complex protocol) могут запросить более одного соединения через брандмауэр ISA, как входящего, так и исходящего. Клиенты SecureNAT нуждаются в этих фильтрах при использовании сложных протоколов, поскольку у клиентов SecureNAT нет функциональных возможностей клиентов брандмауэра. В отличие от клиента брандмауэра, который умеет согласовывать сложные протоколы при совместной работе с брандмауэром ISA, клиент SecureNAT — это простой NAT-клиент брандмауэра ISA, нуждающийся в помощи фильтров приложений для соединения с применением сложных протоколов (таких как FTP или MMS).

Защита протоколов — это защита соединений, проходящих через брандмауэр ISA. Фильтры защиты протоколов, такие как SMTP- и DNS-фильтры, проверяют соединения, применяющие эти фильтры, и блокируют те из них, которые считают не соответствующими параметрам безопасности. Некоторые из этих фильтров (такие как DNS- и SMTP-фильтры) запрещают соединения, которые могут создавать переполнения буфера, а некоторые (такие как средство просмотра сообщений SMTP Message Screener) выполняют более глубокую проверку и блокируют соединения или содержимое, основываясь на политике.

Фильтры приложений

Брандмауэр ISA включает ряд фильтров приложений. В этом разделе мы обсудим следующие:

- фильтр SMTP и средство просмотра сообщений Message Screener;
- фильтр DNS;
- фильтр обнаружения атак (Intrusion Detection) по протоколу POP;
- В фильтр SOCKS V4;
- фильтр FTP-доступа;
- фильтр H.323;
- фИЛЬТр MMS;
- фИЛЬТр PNM;
- фИЛЬТр PPTP;
- фИЛЬТр RPC;
- фильтр RTSP.

Фильтр SMTP и Message Screener

Фильтр SMTP и средство просмотра сообщений *SMTP Message Screener* применяются для защиты опубликованных SMTP-серверов. Фильтр SMTP защищает опубликованные SMTP-серверы от атак переполнения буфера, а средство просмотра сообщений оберегает вашу компанию от нежелательных сообщений электронной почты.

SMTP Message Screener можно поместить в разных местах:

- на брандмауэре ISA;
- на выделенном SMTP-ретрансляторе *в* сегменте защищенной сети;
- на сервере Exchange.

Мы советуем размещать средство просмотра сообщений SMTP Message Screener на брандмауэре ISA или на выделенном SMTP-ретрансляторе в корпоративной сети или в DMZ-сегменте. Причина, по которой мы не рекомендуем размещать его на сервере Exchange, заключается в том, что просмотр сообщений потребляет много циклов процессора и оказывает негативное влияние на общую производительность сервера Exchange.

В данном разделе сосредоточимся на предпочитаемой нами конфигурации, т. е. размещении средства просмотра сообщений SMTP Message Screener на машине с выделенным SMTP-ретранслятором. Этот вариант наиболее безопасен, обеспечивает наилучшую производительность и включает утилиту SMTPcred, необходимую, если SMTP Message Screener используется на компьютере без установки SMTP Message Screener на самом брандмауэре ISA.

Установка SMTP Message Screener на выделенном SMTP-ретрансляторе

Установка и настройка средства блокировки сообщений SMTP Message Screener на выделенном SMTP-ретрансляторе в сегменте защищенной сети (корпоративная сеть или сеть DMZ) относительно просты. Однако для получения законченной действующей реализации придется выполнить дополнительные настройки и установочные задачи.

- Exchange-сер вер должен уметь разрешать доменные MX-имена (mail exchange, имя в DNS-ресурсе для обработки почтовых сообщений) исходящей электрон ной почты, или SMTP-ретранслятор должен быть способен разрешать доменные MX-имена) исходящей электронной почты, если машина со средством блоки ровки сообщений SMTP Message Screener действует так же, как исходящий SMTP-ретранслятор.
- Необходимо создать правило доступа для компьютера, выполняющего разреше ние имен для Exchange-сервера. Лучше всего, если это будет DNS-сервер в кор поративной сети, способный разрешать имена интернет-хостов.

а Потребуется настройка правила доступа, разрешающего исходящий доступ по протоколу SMTP для каждой машины, нуждающейся в отправке исходящей электронной почты по этому протоколу.

а Следует создать правило публикации сервера, разрешающее внешним SMTP-серверам посылать электронную почту на SMTP-ретранслятор, на котором выполняется средство блокировки сообщений SMTP Message Screener.

В этом разделе обсуждается установка и конфигурирование средства блокировки сообщений SMTP Message Screener со ссылками на соответствующие главы книги

для получения подробной информации о требуемых правилах доступа и публикации сервера.

Средство блокировки сообщений SMTP — Message Screener — необязательный компонент ISA Server 2004. Он интегрируется с SMTP-сервисом IIS 6.0 (Internet Information Server, информационный сервер Интернета) и блокирует электронную почту по протоколу SMTP в соответствии с заданными в нем параметрами.

Установка SMTP Message Screener на SMTP-ретрансляторе

На компьютере с брандмауэром ISA Server 2004 выполните следующие шаги для установки средства блокировки сообщений SMTP Message Screener.

1. Поместите в нужное место файлы, необходимые для установки ISA Server 2004, и дважды щелкните кнопкой мыши файл ISAautorun.exe.
2. В меню автозапуска щелкните кнопкой мыши пиктограмму **Install ISA Server** 2004 (Установить ISA Server 2004).
3. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the Installation Wizard for Microsoft ISA Server 2004** (Вас приветствует мастер установки Microsoft ISA Server 2004).
4. На странице **Program Maintenance** (Сопровождение программ) щелкните кнопкой мыши вариант **Modify** (Модифицировать) и кнопку **Next** (Далее).
5. На странице **Custom Setup** (Настраиваемая установка) щелкните кнопкой мыши вариант **Message Screener** (Средство просмотра сообщений) и щелкните кнопкой мыши строку **This feature, and all subfeatures will be installed on local hard drive** (Этот компонент и в с е входящие в его состав компоненты будут установлены на локальном жестком диске). Щелкните мышью кнопку **Next** (Далее) (рис. 10.1).

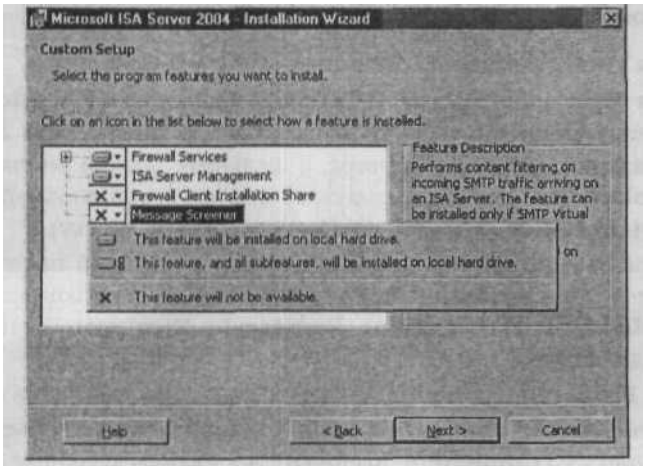


Рис. 10.1. Диалоговое окно Custom Setup (Настраиваемая установка)

6. Щелкните мышью кнопку **Next** (Далее) на странице **Services** (Службы), ин формирующей о том, что службы **SNMP** и **IIS Admin Service** (Служба админи стрирования IIS) будут остановлены во время установки.
7. Щелкните мышью кнопку **Install** (Установить) на странице **Ready to** Modify **the Program** (Все готово для модификации программы).
8. Установите флажок **Invoke ISA Server Management** (Запустить управление ISA Server) перед закрытием мастера, затем щелкните мышью кнопку **Finish** (Гото во) на странице **Installation Wizard Completed** (Мастер установки завершил работу).
9. Закройте меню автозапуска.

SMTP Message Screener должен связаться с брандмауэром ISA Server 2004 для получения установочной информации, включая домены, ключевые слова и прикрепляемые файлы (attachments), которые вы хотите заблокировать. Настраивать установочные параметры SMTP Message Screener следует на компьютере с брандмауэром ISA Server 2004 с помощью интерфейса фильтра SMTP, а *не* на машине с SMTP-ретранслятором, на которой установлено средство блокировки сообщений SMTP Message Screener.

Утилита smtpcred.exe применяется для облегчения обмена информацией между компьютером с SMTP Message Screener и брандмауэром ISA Server 2004. Для установки этого соединения придется ввести сведения о пользователе, компьютере и домене в утилиту smtpcred.exe.

ПРЕДУПРЕЖДЕНИЕ На брандмауэре ISA Server 2000 для связи между ним и Message Screener использовались вызовы DCOM (модель распределенных объектов). В новом брандмауэре ISA отпала необходимость применения DCOM. Такой подход повышает безопасность соединения между компьютером с SMTP Message Screener и брандмауэром ISA.

Для запуска утилиты smtpcred.exe выполните следующие шаги.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскрой те окно, связанное с именем сервера, и щелкните правой кнопкой мыши узел **Firewall Policy** (Политика брандмауэра), а затем левой кнопкой мыши коман ду **Edit System Policy** (Редактировать системную политику).
2. На странице **System Policy Editor** (Редактор системной политики) найдите группу **Remote Management** (Удаленное управление) и щелкните кнопкой мыши подпапку **Microsoft Management** (Управление Microsoft). Щелкните кнопкой мыши вкладку **From** (От).
3. На вкладке **From** (От) щелкните мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши узел **Computers** (Компьютеры). Дважды щелкните кнопкой мыши

элемент **SMTP Relay** (SMTP-ретранслятор) и щелкните мышью кнопку **Close** (Закрыть).

5. На странице **System Policy Editor** (Редактор системной политики) щелкните мышью кнопку ОК (рис. 10.2).

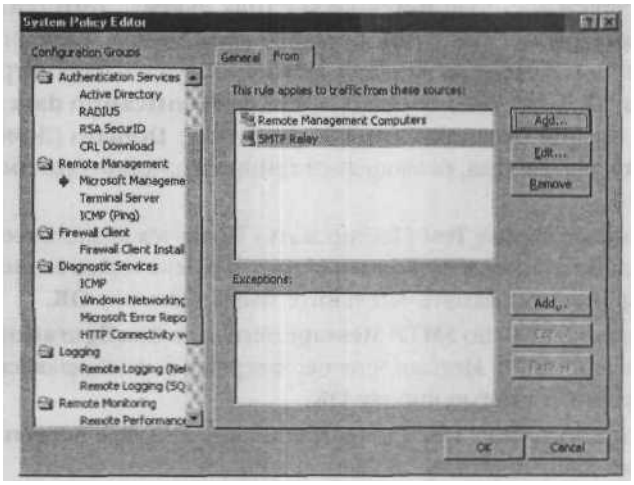


Рис. 10.2. Страница System Policy Editor (Редактор системной политики)

6. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
7. Щелкните мышью кнопку ОК в диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

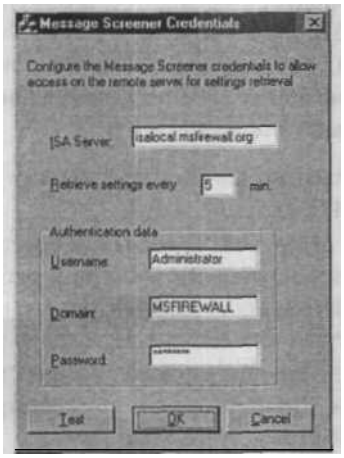


Рис. 10.3. Диалоговое окно Message Screener Credentials (Верительные данные Message Screener)

8. На компьютере **SMTPRELAY** перейдите в папку C:\Program Files\Microsoft ISA Server и дважды щелкните кнопкой мыши утилиту smtpcredexe.
   В диалоговом окне **Message Screener Credentials** (Верительные данные Message Screener) введите имя брандмауэра ISA Server 2004 в текстовое поле **ISA Server** (Сервер). В текстовое поле **Retrieve settings every** ... **min** (Получать установочные параметры каждые ... мин.) введите промежуток времени в минутах, через который SMTP Message Screener должен получать параметры установки с брандмауэра ISA Server 2004. В области окна **Authentication data** (Данные аутентификации) введите **Username** (Имя пользователя), **Domain** (Домен) и **Password** (Пароль) для пользователя, являющегося администратором брандмауэра ISA Server 2004 (рис. 10.3).
9. Щелкните мышью кнопку **Test** (Тестировать). Появится диалоговое окно **Warning** (Предупреждение), информирующее о том, что некоторые значения не записаны в долговременную память. Щелкните мышью кнопку OK.
10. Появится диалоговое окно **SMTP Message Screener Configuration Test Completed** (Тестирование SMTP Message Screener завершено), сообщающее об отсутствии ошибок. Щелкните мышью кнопку OK.
11. Щелкните мышью кнопку OK в диалоговом окне **Message Screener Credentials** (Верительные данные Message Screener).

Настройка SMTP Message Screener

Теперь можно настраивать средство просмотра сообщений SMTP Message Screener — фильтр приложений, проверяющий все входящие соединения, проходящие через брандмауэр ISA Server 2004 под управлением правила публикации SMTP-сервера.

> **ПРЕДУПРЕЖДЕНИЕ** Следует соблюдать благоразумие при настройке SMTP Message Screener. Необходимо убедиться в том, что сделанные установки не задают ограничений, блокирующих нужную почту. У всех приложений фильтрации электронной почты есть потенциальная возможность блокирования почты, необходимой пользователям.

Выполните следующие шаги для настройки правила публикации сервера **Inbound SMTP Relay** (Входящий SMTP-ретранслятор).

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните правой кнопкой мыши узел **Configuration** (Конфигурация). Щелкните мышью узел **Add-ins** (Дополнения).
2. В узле **Add-ins** щелкните правой кнопкой мыши строку **SMTP Filter** (Фильтр SMTP) на панели **Details** (Дополнительные параметры) и левой кнопкой мыши команду **Properties** (Свойства) (рис. 10.4).
3. Щелкните кнопкой мыши вкладку **General** (Общие) в диалоговом окне **SMTP Filter Properties** (Свойства фильтра SMTP). Убедитесь в том, что установлен флажок **Enable this filter** (Включить данный фильтр).

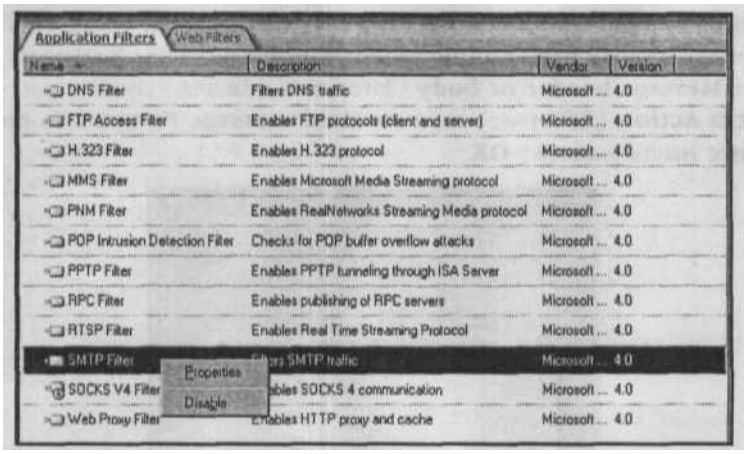


Рис. 10.4. SMTP Filter (Фильтр SMTP)

4. Щелкните кнопкой мыши вкладку **Keywords** (Ключевые слова) (рис. 10.5). Щелкните мышью кнопку **Add** (Добавить). В диалоговом окне **Mail Keyword Rule** (Правило для ключевых слов электронной почты) убедитесь, что установлен флажок **Enable keyword rule** (Разрешить применение правила ключевого слова). В области вкладки **Apply action if keyword is found in** (Выполнить действие, если ключевое слово найдено в) можно выбрать один из следующих вариантов.
   - □ **Message header or body** (Заголовок или тело сообщения) Действие, задан ное для правила, будет выполняться, если ключевое слово найдено в заголовке *или* в теле сообщения.
   - D **Message header** (Заголовок сообщения) Действие, заданное для правила, будет выполняться, если ключевое слово найдено в заголовке сообщения.
   - П **Message body** (Тело сообщения) Действие, заданное для правила, будет выполняться, если ключевое слово найдено в теле сообщения, Щелкните кнопкой мыши стрелку, направленную вниз, в области раскрывающегося списка **Action** (Действия). Имеются следующие варианты.
   - □ **Delete message** (Удалить сообщение) SMTP-сообщение удаляется без уве домления кого-либо об этом.
   - **Q Hold message** (Сохранить сообщение) SMTP-сообщение сохраняется в каталоге BADMAIL, принадлежащем иерархии папок SMTP-сервиса. Компоненты этого сообщения можно просмотреть, но формат его хранения не позволяет легко отправить данное сообщение адресату.
   - □ **Forward message to** (Переслать сообщение) SMTP-сообщение пересыла ется по адресу электронной почты, заданному в данном правиле. В каждом правиле можно указать свой адрес для пересылки сообщений.

5. В диалоговом окне **Mail Keyword Rule** (Правило для ключевых слов электронной почты) введите **mail enhancement** в текстовое поле **Keyword.** Выберите вариант **Message header or body** (Заголовок или тело сообщения). Выберите из списка **Action** (Действие) вариант **Hold message** (Сохранить сообщение). Щелкните мышью кнопку ОК.

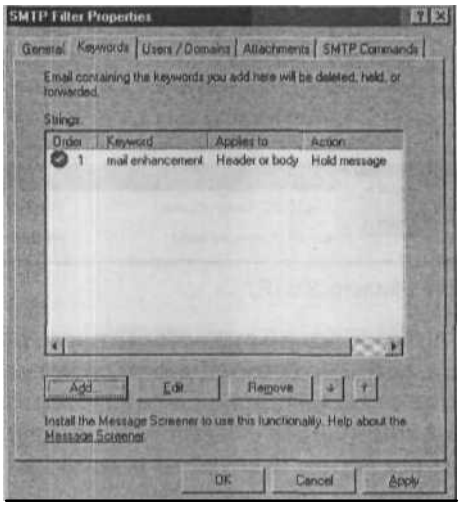


Рис. 10.5. Диалоговое окно SMTP Filter Properties (Свойства фильтра SMTP)

6. Щелкните кнопкой мыши вкладку **Users/Domains** (Пользователи/Домены). На этой вкладке можно настроить блокирование сообщений в SMTP Message Screener, основываясь на учетной записи отправителя или домене электронной почты. Введите адрес электронной почты отправителя в текстовое поле **Sender's email address** (Адрес отправителя) и щелкните мышью кнопку **Add** (Добавить). Адрес электронной почты отправителя появится в списке **Blocked Senders** (Заблокированные отправители). Введите имя почтового домена в текстовое поле **Domain name** (Имя домена) и щелкните мышью кнопку **Add** (Добавить). Имя домена электронной почты появится *в* списке **Blocked domains** (Заблокированные домены). Обрабатываемые SMTP Message Screener сообщения электронной почты, соответствующие адресам или доменам электронной почты, указанным в упомянутых списках, удаляются. Эти сообщения не сохраняются на сервере и не пересылаются ни пользователю, ни администратору. Если сообщение от отвергаемого отправителя или из отвергаемого почтового домена также содержит ключевое слово, соответствующее правилу обработки ключевых слов, а в этом правиле задано сохранение подобных сообщений, указанное сообщение не будет сохранено, потому что оно отвергается прежде, чем начинается поиск ключевого слова.
7. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК (рис. 10.6).

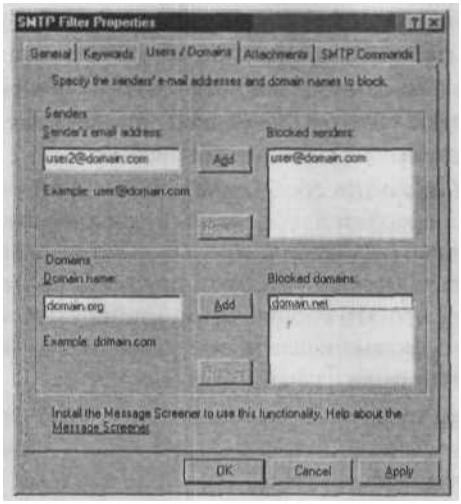


Рис. 10.6. Вкладка User/Domains (Пользователи/Домены)

8. Щелкните кнопкой мыши вкладку **Attachments** (Прикрепленные файлы) и кнопку **Add** (Добавить). Убедитесь в том, что установлен флажок **Enable attachment rule** (Включить правило для прикрепленных файлов) в диалоговом окне **Mail Attachment Rule** (Правило для прикрепленных файлов электронной почты). В области окна **Apply action to messages containing attachments with one of these properties** (Выполнять действие с сообщениями, содержащими прикрепленные файлы с одной из следующих характеристик) есть три варианта для выбора.

   П **Attachment name** (Имя прикрепленного файла) Выберите этот вариант и введите имя прикрепленного файла. Используйте этот вариант, если нет нужды блокировать все прикрепленные файлы с определенным расширением, но вы действительно хотите заблокировать файл с конкретным именем. Например, не нужно блокировать все файлы с расширением zip, но необходимо заблокировать пересылку файла с именем exploit.zip.

   - **Attachment extension** (Расширение прикрепленного файла) Более распространенный случай — блокирование всех файлов с определенным расширением. Например, если необходимо заблокировать все файлы с расширением exe, введите **exe** или **.exe** в текстовое поле, расположенное справа от данного варианта переключателя.
   - **Attachment size limit (in bytes)** (Ограничение размера прикрепленного файла, в байтах) Можно блокировать прикрепленные файлы, основываясь на их размерах. Выберите этот вариант и введите минимальный размер для прикрепленных файлов, которые нужно блокировать.

9. Щелкните кнопкой мыши стрелку, направленную вниз, в области раскрывающегося списка **Action** (Действие). В нем приведены следующие варианты действий. D
   Delete message (Удалить сообщение) SMTP-сообщение удаляется без уведомления кого-либо об этом. Выбирайте это действие, если вы уверены, что никому не понадобится удаленное сообщение.
   - □ **Hold message** (Сохранить сообщение) SMTP-сообщение сохраняется в каталоге BAD MAIL иерархии папок SMTP-сервиса. Можно просмотреть компоненты сохраненного сообщения, но его формат не позволяет легко переслать сообщение адресату. Используйте этот вариант, если считаете, что существует вероятность того, что это сообщение кому-нибудь понадобится. Если сообщение сохранено, можно извлечь его позже, когда пользователь обеспокоится тем, что почта была случайно удалена.
   - О **Forward message to** (Переслать сообщение) SMTP-сообщение пересылается по адресу электронной почты, который задан в данном правиле. В каждом правиле могут указываться разные адреса, по которым пересылается сообщение. Применяйте этот вариант, если существует администратор электронной почты, просматривающий сообщения для выявления спама и устранения нежелательных последствий. Этот вариант подходит также для сохранения спама и его последующего использования при обучении других приложений, борющихся со спамом с помощью фильтрации по методу Байеса (Bayesian filtering), и других самообучающихся средств фильтрации (рис. 10.7).

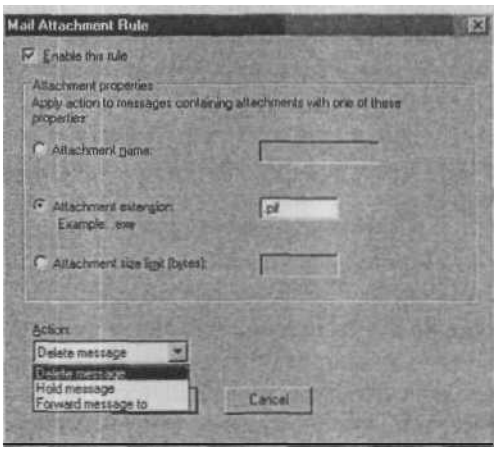


Рис. 10.7. Диалоговое окно Mail Attachment Rule (Правило для прикрепленных файлов электронной почты)

В данном примере выберем вариант **Forward message to** (Переслать сообщение), чтобы показать, как вводить адрес пересылки.

10. После выбора варианта **Forward message to** (Переслать сообщение) появляется текстовое поле, в которое можно ввести адрес электронной почты, на ко-

торый будет пересылаться сообщение. При этом сервер должен уметь разрешить адрес почтового домена этого пользователя.

Например, на рис. 10.8 мы ввели электронный адрес smtpsecurityadmin@msfirewall.org. Брандмауэр ISA Server должен иметь доступ к MX-записи (записи обмена сообщениями) для домена внутренней сети internal.net. Брандмауэр ISA Server пересылает сообщение на SMTP-сервер, отвечающий за почту домена internal.net, основываясь на информации в MX-записи.

В данном примере брандмауэр настроен на адрес DNS-сервера во внутренней сети, который может разрешать имена как внутренней, так и внешней сети. Сообщение перенаправляется на внутренний адрес сервера Exchange. Следует конфигурировать *инфраструктуру разделенных доменных имен (split DNS infrastructure),* если домен internal.net доступен внутренним и внешним пользователям.

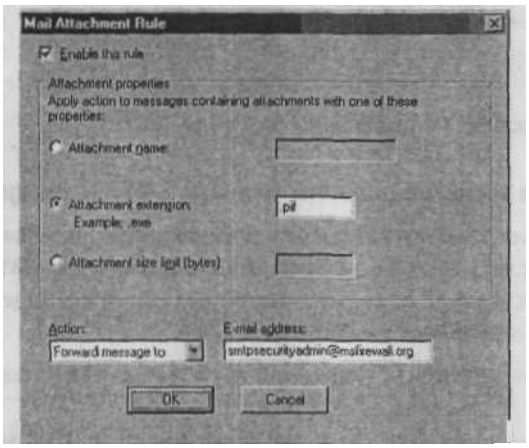


Рис. 10.8. Диалоговое окно **Mail Attachment Rule** (Правило для прикрепленных файлов электронной почты)

11. Установочные параметры на вкладке **SMTP Commands** (Команды SMTP) служат посредниками для компонентов фильтра SMTP. Средство просмотра сообщений SMTP Message Screener не оценивает команды SMTP и не защищает от переполнений буфера. Команды в списке ограничены заранее определенной длиной. Если входящее SMTP-соединен ие посылает команду, превышающую разрешенную длину, соединение отвергается. Кроме того, если команда, посылаемая по SMTP-каналу, не указана в данном списке, она отвергается (рис. 10.9).
12. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK в диалоговом окне **Configure SMTP Protocol Policy** (Настроить политику SMTP-протокола).
13. Щелкните мышью кнопку **Apply** (Применить) для сохранения изменений и обновления политики брандмауэра.
14. Щелкните мышью кнопку OK *в* диалоговом окне **Apply New Configuration** (Применить новую конфигурацию).

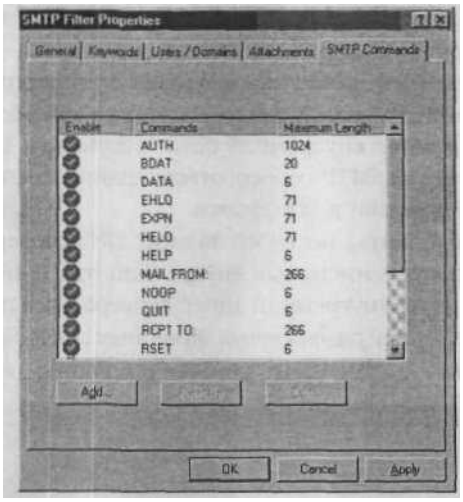


Рис. 10.9. Вкладка SMTP Commands (Команды SMTP)

Конфигурирование регистрационного журнала SMTP Message Screener

Брандмауэр ISA Server 2004 хранит отдельный регистрационный журнал для сообщений, обрабатываемых средством блокировки сообщений SMTP Message Screener. Этот журнал предоставляет значимую информацию о сообщениях, отвергнутых Message Screener, и о причине их блокирования.

Выполните следующие шаги для конфигурирования регистрации в SMTP Message Screener.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) щелкните кнопкой мыши узел **Monitoring** (Наблюдение) на левой панели консоли.
2. В узле **Monitoring** (Наблюдение) щелкните мышью вкладку **Logging** (Регистрация) на панели дополнительных параметров.
3. Щелкните мышью вкладку **Tasks** (Задачи) на панели задач. На вкладке щелкните кнопкой мыши ссылку **Configure SMTP Message Screener Logging** (Конфигурировать создание регистрационного журнала SMTP Message Screener).
4. В диалоговом окне **SMTP Message Screener Logging Properties** (Свойства регистрационного журнала SMTP Message Screener) щелкните кнопкой мыши вкладку **Log** (Регистрационный журнал). Обратите внимание на то, что доступен единственный метод регистрации сообщений — **File** (Файл). В этом случае создается текстовый файл регистрации. Из списка **Format** (Формат) выберите вариант **ISA Server file** format (Формат файла ISA Server). Данный выбор позволяет при регистрации использовать местное время в регистрационных журналах. Убедитесь, что установлен флажок **Enable logging for this service** (Разрешить создание регистрационного журнала для данного сервиса) (рис. 10.10).

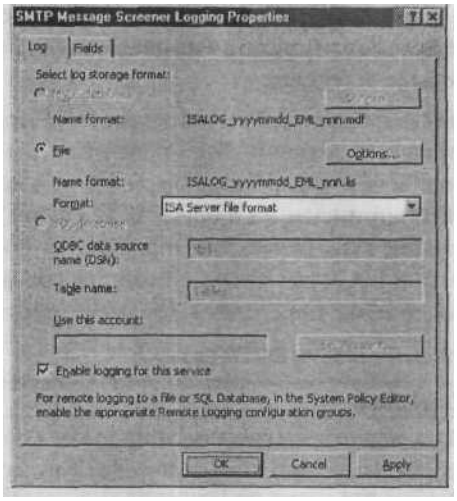


Рис. 10.10. Вкладка **Log** (Регистрационный журнал)

5. Щелкните мышью кнопку **Options** (Параметры). По умолчанию место хранения журналов регистрации — папка **ISALogs** на локальном жестком диске. Обратите внимание на параметры в области окна **Log file storage** limits (Ограничения для хранения регистрационных файлов). Отметьте, что текстовые файлы регистрации по умолчанию сжаты с помощью функции сжатия файловой системы NTFS. Согласитесь с установками, принятыми по умолчанию, и щелкните мышью кнопку **Cancel** (Отмена) (рис. 10.11).

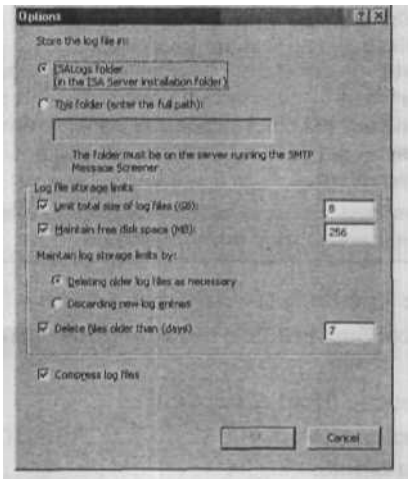


Рис. 10.11. Диалоговое окно **Options** (Параметры)

6. Щелкните мышью кнопку **Apply** (Применить), а затем **кнопку ОК** в диалоговом окне **SMTP Message Screener Logging Properties** (Свойства регистрационного журнала SMTP Message Screener).

В табл. 10.1 приведены поля журнала регистрации SMTP-сервиса и характеристики хранящихся в каждом из них сведений. Если поле не активно в журнале регистрации SMTP Message Screener, в нем появится прочерк «-» при использовании формата регистрации ISA Server. Если применяется формат W3C (World Wide Web Consortium), поле не выводится. В столбце *Field* (поле) указана позиция поля при использовании формата файла регистрации ISA Server (знание позиции очень важно, поскольку нет «указания» или заголовка столбца, определяющего регистрируемое поле).

Табл. 10.1. Поля журнала регистрации SMTP-сервиса

Поле	W3C	Описание
1.	Date	Дата возникновения регистрируемого события Время
2.	Time	возникновения регистрируемого события. В формате W3C — это время по Гринвичу (Universal Time Coordinated, UTC) Имя
3.	cs-sender	отправителя, как задано в поле «MAIL FROM:» SMTP-заголовка. Не более 72 символов
4.	cs-recipient	Список адресатов, как задано в поле «RCPT TO> SMTP-заголовка. Не более 72 символов
5.	cs-subject	Тема сообщения. Не более 72 символов
6.	cs-messageid	Идентификатор (ID) сообщения. Идентификатор — это либо уникальный ID, генерируемый отправителем, либо ID, автоматически назначаемый SMTP-сер в и сом ОС Windows при получении. Не более 72 символов
7.	x-action	Действие, предпринимаемое ISA Server. Одно из следующих: **Delete** — сообщение удаляется; **Hold** — сообщение сохраняется в очереди BADMAIL; **Forward** — сообщение пересылается другому адресату (не тому, который указан в исходном сообщении); **Pass** — сообщение посылается заданным адресатам (в поле cs-recipient)
8.	x-reason	Причины, по которым ISA Server выполняет действие (x-action), приведены сразу после таблицы

Возможны следующие причины выполнения действия брандмауэром ISA Server.

Свойства некоторых сообщений невозможно прочитать. Выполняется действие по умолчанию.

Действие по умолчанию — Hold (Сохранить).

Штамп правила политики (policy rule stamp) не найден в сообщении. Выполняется действие по умолчанию.

Действие по умолчанию — Hold (Сохранить). Штамп правила политики — отметка, помещаемая брандмауэром ISA Server в сообщение для того, чтобы дать

знать Message Screener, какое правило следует применить к сообщению. Он создается, если сообщение не проходит через прикладной фильтр SMTP прежде чем пройти через средство блокировки сообщений SMTP Message Screener.

- Программа регистрации (logger) до сих пор не инициализирована. Выполняет ся действие по умолчанию.
- Действие по умолчанию — Hold (Сохранить).
- Правило политики невозможно прочесть. Выполняется действие по умолчанию.
- Действие по умолчанию — Hold (Сохранить).
- Возник сбой при попытке переслать сообщение по другому адресу.
- Далее приведены конкретные коды ошибок:

  П *правило* политики SMTP Message Screener отвергает сообщения от *отправителя;*

  О *правило* политики SMTP Message Screener отвергает *прикрепленный файл; о правило* политики SMTP Message Screener отвергает *расширение прикрепленного файла;*

  - □ *правило* политики SMTP Message Screener отвергает *прикрепленные файлы указанного размера;*
  - □ *правило* политики SMTP Message Screener отвергает сообщения с указанной *темой;*

  D *правило* политики SMTP Message Screener отвергает сообщения с заданным *телом сообщения.*

Фильтр DNS

Фильтр DNS брандмауэра ISA защищает DNS-сервер, опубликованный брандмауэром ISA с помощью правил публикации сервера. Получить доступ к интерфейсу конфигурации для страницы настройки защиты фильтра DNS от атак можно в диалоговом окне **Intrusion Detection** (Обнаружение вторжения). Раскройте окно, связанное с именем сервера, а затем узел **Configuration** (Конфигурация). Щелкните кнопкой мыши вкладку **General** (Общие).

На панели дополнительных параметров щелкните кнопкой мыши ссылку **Enable Intrusion Detection and DNS Attack Detection** (Включить обнаружение вторжения и DNS-атак). В диалоговом окне **Intrusion Detection** (Обнаружение вторжения) щелкните кнопкой мыши **DNS Attacks** (DNS-атаки) и установите флажок **Enable detection and filtering of DNS attacks** (Включить обнаружение и фильтрацию DNS-атак) (рис. 10.12).

После включения функции обнаружения можно активизировать защиту. Есть возможность обезопасить себя от трех видов атак:

- DNS host name overflow (переполнение буфера имен узлов в DNS);
- DNS length overflow (переполнение буфера номера узла в DNS);
- DNS zone transfer (зонная передача в DNS).

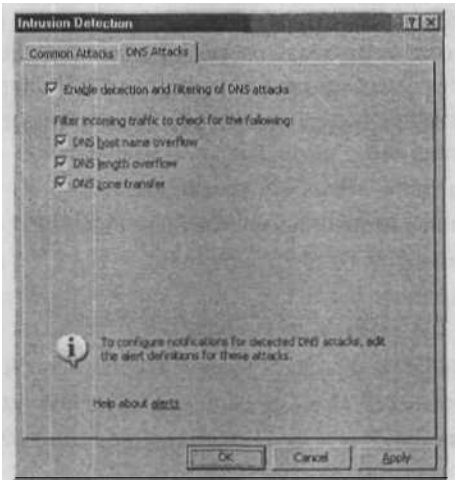


Рис. 10.12. Вкладка DNS Attacks (DNS-атаки)

Атаки **DNS host name overflow** и **DNS length overflow** относятся к DNS-атакам отказов от обслуживания (denial-of-service, DoS-атаки). Подобная DNS-атака использует разницу размеров DNS-запроса и DNS-отклика, заполняя всю полосу пропускания сети фиктивными DNS-запросами. Атакующие используют DNS-серверы как «усилители», увеличивающие DNS-трафик.

Сначала злоумышленник посылает небольшие DNS-запросы на каждый DNS-сервер, содержащий ложный IP-адрес подтверждения (spoofed IP address) намеченной жертвы. Размер ответов, возвращаемых на эти запросы, гораздо больше, поэтому, если большое количество ответов вернется в одно и то же время, линия связи будет перегружена и возникнет отказ от обслуживания.

Администраторы могут решить эту проблему, настроив DNS-серверы при получении DNS-запросов от подозрительных или неожиданных источников на отклик с помощью «отвергающего» ответа («refused» response), который гораздо меньше, чем ответ с разрешением имени.

Подробную информацию о конфигурировании DNS-серверов для решения этой проблемы можно найти в информационном бюллетене департамента США по энергетике (Computer Incident Advisory Capability information, Консультационная служба компьютерных сбоев) bulletin J-063, который доступен по адресу www.ciac.org/ciac/bulletins/j-063.shtml.

Фильтр обнаружения атак на протокол POP

Фильтр обнаружения атак (Intrusion Detection) на протокол POP защищает серверы POP3, опубликованные с помощью правил публикации серверов брандмауэра ISA, от атак переполнения буферов POP-сервисов. У этого фильтра нет интерфейса настройки.

Фильтр SOCKS V4

Фильтр SOCKS v4 используется для приема запросов на соединения SOCKS версии *4* от приложений, разработанных в соответствии со спецификацией SOCKS версии 4. В операционных системах семейства Windows нет необходимости применять фильтр SOCKS, поскольку можно установить клиент брандмауэра на этих машинах для прозрачной аутентификации на брандмауэре ISA и поддержки взаимодействия сложных протоколов.

На хостах, которые нельзя конфигурировать как клиенты брандмауэра, таких как Linux- и Mac-хосты, можно использовать для поддержки фильтр SOCKS v4. По умолчанию этот фильтр отключен. Для его включения откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004), раскройте окно, связанное с именем сервера, а затем узел **Configuration** (Конфигурация). Щелкните кнопкой мыши узел **Add-ins** (Дополнения). На панели дополнительных параметров щелкните правой кнопкой мыши элемент SOCKS V4 и левой кнопкой мыши команду **Enable** (Включить).

Необходимо настроить фильтр SOCKS V4 для ожидания запросов приема соединений от конкретных сетей, в которых предполагается использовать фильтр. Дважды щелкните кнопкой мыши элемент SOCKS V4. В диалоговом окне **SOCKS V4 Filter Properties** (Свойства фильтра SOCKS V4) щелкните кнопкой мыши вкладку **Networks** (Сети). **На** этой вкладке можно настроить порт, на котором фильтр ожидает соединения от клиентов SOCKS. Затем установите флажок, расположенный рядом с сетью, из которой фильтр SOCKS будет принимать соединения. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК (рис. 10.13).

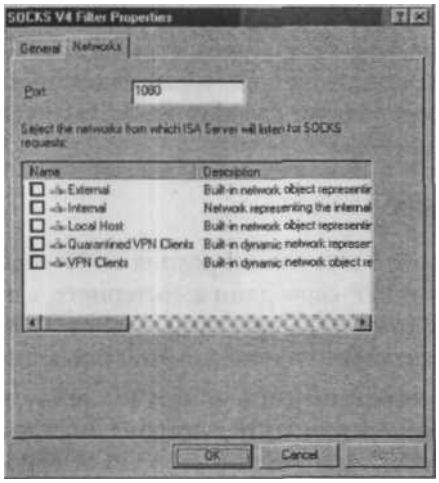


Рис. 10.13. Диалоговое окно **SOCKS V4 Filter** Properties (Свойства фильтра SOCKS V4)

Фильтр SOCKS v4 поддерживает приложения клиентов SOCKS v4.3. Это универсальный фильтр сокетов, поддерживающий все клиентские приложения, разработанные в соответствии со спецификацией SOCKS v4.3. Этот фильтр выполняет функции, аналогичные функциям клиента брандмауэра. Однако в работе клиента SOCKS и клиента брандмауэра есть существенные отличия.

- Клиент брандмауэра — это типовое Winsock-приложение прокси-клиента (Winsock Proxy client application). Все приложения, разработанные для спецификации Windows Sockets, будут автоматически использовать клиент брандмауэра.
- Фильтр SOCKS поддерживает приложения, написанные в соответствии со спецификацией SOCKS v4.3.
- Если на клиентской машине установлен клиент брандмауэра, все Winsock-приложения автоматически используют клиент брандмауэра и верительные данные пользователя автоматически пересылаются брандмауэру ISA. Кроме того, клиент брандмауэра будет работать с сервисом брандмауэра ISA для управления сложными протоколами, требующими вторичных соединений (такими как FTP, MMS и многими другими).
- Клиент SOCKS должен конфигурироваться с учетом приложения. Каждое приложение следует настроить явно на применение брандмауэра ISA как его сервера SOCKS. В этом случае фильтр SOCKS будет управлять сложными протоколами клиентского приложения SOCKS.
- Фильтр SOCKS 4.3a, включенный в состав брандмауэра ISA, не поддерживает аутентификацию. В протоколе SOCKS 5 введена возможность подтверждения подлинности клиентского приложения, пытающегося получить доступ к содержимому через прокси протокола SOCKS.

Мы всегда рекомендуем применять клиент брандмауэра, потому что он обладает впечатляющими преимуществами, предоставляя возможность подтверждения подлинности всех Winsock-соединений, устанавливаемых через брандмауэр ISA. Однако SOCKS — это подходящий, лучший из оставшихся, вариант, если нельзя установить клиент брандмауэра.

Фильтр FTP-доступа

Фильтр FTP-доступа применяется как посредник в FTP-соединениях между клиентами защищенной сети и FTP-серверами в Интернете, а также между внешними хостами и опубликованными FTP-серверами. Фильтр FTP-доступа поддерживает режимы PASV и PORT (пассивный и стандартный, или активный) FTP-соединений.

Фильтр FTP-доступа необходим для клиентов SecureNAT, поскольку протокол FTP использует вторичные соединения для FTP-соединений в режиме PORT. FTP — сложный протокол, требующий исходящих соединений от FTP-клиента в режиме PORT и новых вторичных входящих соединений от FTP-сервера. **Клиенту** брандмауэра не нужна поддержка фильтра приложений для вторичных соединений, клиенты

SecureNAT нуждаются в такой поддержке, вот почему разработчики брандмауэра ISA включили в него фильтр приложений FTP-доступа.

> ПРИМЕЧАНИЕ Если планируется устанавливать клиентские FTP-соединения в режиме PORT, убедитесь в том, что на брандмауэре ISA включена IP-маршрутизация (установка по умолчанию). Если IP-маршрутизация включена, вторичные соединения поддерживаются в режиме ядра (kernel mode), а не в режиме пользователя. Этот режим обработки вторичных соединений (которые содержат данные, передаваемые от FTP-сервера FTP-клиенту) существенно повышает производительность.

Стефан Поусил (Stefaan Pouseele), специалист высшего класса по брандмауэру ISA Server (Microsoft Valuable Professional, MVP), написал отличную статью о протоколе FTP и о том, как с его помощью можно влиять на безопасность брандмауэра, *How the FTP Protocol Challenges Firewall Security,* хранящуюся по адресу: http://isaserver.org/articles/How_the_FTP_protocol_Challenges_Firewall_Security.html.

У фильтра FTP-доступа нет интерфейса конфигурирования.

Фильтр H.323

Фильтр H.323[1] применяется для поддержки соединений H.323 брандмауэра ISA. Для его настройки откройте консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте окно, связанное с именем сервера. Далее раскройте узел **Configuration** (Конфигурация) и щелкните кнопкой мыши узел **Add-ins** (Дополнения). Дважды щелкните кнопкой мыши элемент **H.323 Filter** на панели дополнительных параметров (Details Pane).

В диалоговом окне **H.323 Filter Properties** (Свойства фильтра H.323) щелкните кнопкой мыши вкладку **Call Control** (Контроль вызова) (рис. 10.14). Появится возможность установки следующих параметров:

- **Use this Gatekeeper** (Использовать данный привратник);
- **Use DNS gateway lookup and LRQs for alias resolution** (Использовать поиск в DNS-шлюзе и запросы определения местоположения для разрешения имен);
- **Allow audio** (Разрешить передачу аудиозапросов);
- **Allow video** (Разрешить передачу видеозапросов);
- **Allow** T120 **and application sharing** (Разрешить совместное использование приложений и удаленное управление).

[1] H.323 — стандарт Международного телекоммуникационного союза для передачи мультимедиа в сетях с коммуникацией пакетов и организации конференц-связи. — *Прим. пер.*

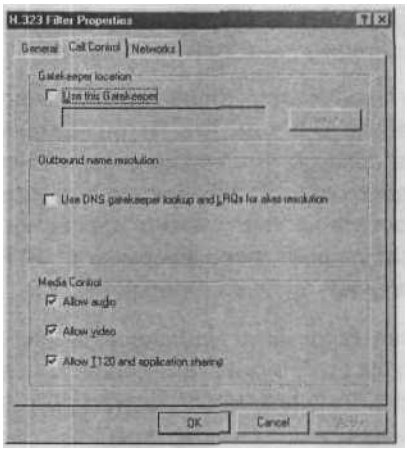


Рис. 10.14. Вкладка Call Control (Контроль вызова)

Щелкните кнопкой мыши вкладку **Networks** (Сети) и установите флажок, расположенный слева от сети, из которой фильтр H.323 должен принимать запросы на соединение (рис. 10.15).

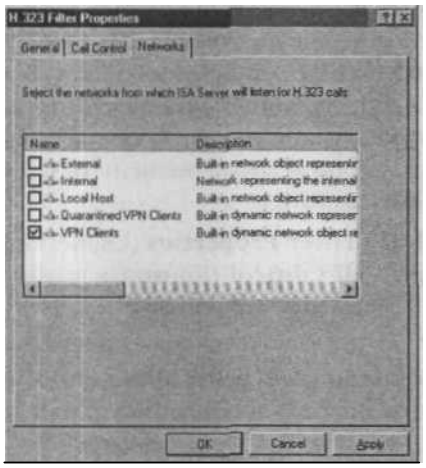


Рис. 10.15. Вкладка Networks (Сети)

Фильтр MMS

Фильтр MMS поддерживает соединения сервисов передачи мультимедийных данных (Microsoft Media Services) через брандмауэр ISA с применением правил доступа и правил публикации сервера. Фильтр MMS — это фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичным соединениям,

необходимым для подключения к содержимому, хранящемуся на сервере Microsoft Media Services. Клиентам брандмауэра не нужна помощь фильтра MMS для соединения с MMS-серверами. У фильтра MMS нет конфигурационного интерфейса.

Фильтр PNM

Фильтр PNM поддерживает соединения по протоколу Progressive Networks Media Protocol (протокол потоковой передачи мультимедийных данных фирмы Progressive Networks). Это фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичному соединению, необходимым для подключения к серверам Progressive Networks Media. У фильтра PNM нет конфигурационного интерфейса.

Фильтр PPTP

Фильтр PPTP поддерживает соединения по протоколу PPTP (Point-to-Point Tunneling Protocol, сквозной туннельный протокол) через брандмауэр ISA для исходящих соединений, устанавливаемых с помощью правил доступа, и входящих соединений, выполняемых с применением правил публикации сервера. Фильтр PPTP брандмауэра ISA отличается от одноименного фильтра ISA Server 2000 поддержкой и входящих, и исходящих PPTP-соединений. Фильтр PPTP брандмауэра ISA Server 2000 обрабатывает только исходящие PPTP-соединения.

Фильтр PPTP необходим как клиентам SecureNAT, так и клиентам брандмауэра. В действительности машина, расположенная в сети, защищенной брандмауэром ISA, должна быть сконфигурирована как клиент SecureNAT для того, чтобы использовать фильтр PPTP для соединения через брандмауэр ISA с VPN-серверами по протоколу PPTP. Причина такого подхода заключается в том, что клиент брандмауэра не может быть связующим звеном для протоколов, отличных от TCP/UDP. Протокол PPTP, используемый в виртуальной частной сети, требует применения протокола GRE (Generic Routing Encapsulation, обобщенная инкапсуляция маршрутизации) (IP-протокол 47) и TCP-протокола 1723. TCP-сеанс используется протоколом PPTP для управления туннелем.

Когда разрешен исходящий доступ по протоколу PPTP, фильтр PPTP автоматически перехватывает GRE- и TCP-соединения, выполненные VPN-клиентом по протоколу PPTP. Не нужно создавать правило доступа, разрешающее VPN-клиентам исходящий доступ к TCP-протоколу 1723.

Фильтр RPC

Фильтр RPC (Remote Procedure Call, удаленный вызов процедуры) применяется как промежуточное звено в RPC-подключениях к серверам, требующим удаленных вызовов процедур, как для исходящих соединений, использующих правила доступа, так и для входящих соединений, применяющих правила публикации серверов.

Сюда же относится защищенная RPC-публикация сервера Exchange (secure Exchange RPC publishing).

У этого фильтра нет конфигурационного интерфейса.

Фильтр RTSP

Фильтр RTSP (Real Time Streaming Protocol, протокол непрерывной передачи и контроля данных в режиме реального времени) поддерживает соединения по протоколу RTSP через брандмауэр ISA для правил доступа и публикации серверов. Фильтр RTSP — это фильтр доступа, позволяющий клиенту SecureNAT получить доступ к сложным протоколам и вторичным соединениям, необходимым для подключения к содержимому, хранящемуся на сервере Microsoft Real Time Streaming Protocol (таком как мультимедийные MMS-серверы в ОС Windows Server 2003). Клиентам брандмауэра не нужна помощь фильтра RTSP для соединения с MMS-серверами.

У фильтра RTSP нет конфигурационного интерфейса.

Web-фильтры

Web-фильтры используются как промежуточное звено в соединениях через брандмауэр ISA по протоколам HTTP, HTTPS и туннелированному FTP (с применением Web-прокси). В этом разделе будут рассмотрены следующие Web-фильтры:

- HTTP Security filter (HTTP-фильтр защиты);
- ISA Server Link Translator (транслятор ссылок брандмауэра ISA Server);
- Web Proxy filter (фильтр Web-прокси);
- SecurlD filter (фильтр SecurlD);
- OWA Forms-based Authentication filter (OWA-фильтр аутентификации, основан ной на формах).

HTTP-фильтр

HTTP-фильтр (HTTPS-фильтр) брандмауэра ISA — одно из ключевых средств фильтрации и проверки на прикладном уровне, включенных в состав брандмауэра ISA. Этот фильтр позволяет брандмауэру ISA выполнять проверку на уровне приложений всех HTTP-коммуникаций, проходящих через брандмауэр ISA, и блокировать соединения, не отвечающие требованиям вашей защиты протокола HTTP.

HTTP-фильтр тесно связан с фильтром Web-прокси. Если фильтр Web-прокси привязан к HTTP-протоколу, все сообщения, исходящие от брандмауэра ISA с TCP-портом назначения 80, подвергаются глубокой проверке на уровне приложений, выполняемой HTTP-фильтром. Позже мы покажем, как отсоединить фильтр Web-прокси от HTTP-протокола, если не требуется, чтобы все сообщения чистились HTTP-фильтром защиты.

ПРИМЕЧАНИЕ Несмотря на то, что есть возможность отсоединить фильтр Web-прокси от исходящего HTTP-протокола, его нельзя отсоединить от правил публикации Web-сервера. Соединения, проходящие обработку правилами публикации Web-сервера, всегда будут обрабатываться и с помощью прокси. Более подробную информацию об отсоединении в правилах доступа HTTP-фильтра от HTTP-протокола можно найти в главе 6.

Применение HTTP-фильтра основано на правилах, можно использовать различные параметры HTTP-фильтрации в каждом правиле, разрешающем исходящие HTTP-коммуникации. Такой подход обеспечивает тщательный, хорошо настраиваемый контроль над типами соединений, которые могут проходить по HTTP-каналу. Кроме того, можно связать фильтр Web-прокси с другими портами и ужесточить политику HTTP-фильтра защиты для соединений, проходящих через альтернативные порты. Эта возможность дает в руки мощное оружие против пользователей и приложений, пытающихся нарушить сетевую политику и политику защиты брандмауэра, туннелируя Web-соединения на альтернативные порты.

В текущий раздел включены следующие темы:

- обзор установочных параметров HTTP-фильтра защиты;
- создание регистрационных журналов HTTP-фильтра защиты;
- отключение HTTP-фильтра защиты для Web-запросов;
- экспортирование и импортирование установочных параметров HTTP-фильтра защиты;
- исследование HTTP-заголовков для выявления потенциально опасных приложений (Potentially Dangerous Applications);
- пример политик HTTP-фильтра защиты;
- сигнатуры, как правило, отвергаемых приложений;
- опасности SSL-тун нелирова ни я.

Обзор установочных параметров HTTP-фильтра защиты

HTTP-фильтр защиты содержит ряд вкладок, позволяющих, основываясь на правилах, установить строгий контроль над типами HTTP-сообщений, которым разрешен проход через брандмауэр ISA. Конфигурирование HTTP-фильтра защиты выполняется на следующих вкладках:

- General (Общие);
- Methods (Методы);
- Extensions (Расширения);
- Headers (Заголовки);
- Signatures (Сигнатуры).

Вкладка General

На вкладке **General** (Общие) можно настроить следующие параметры (рис. 10.16):

максимальную длину заголовков;
размер полезных данных;
максимальную длину URL-адреса;
проверку нормализации;
удаление символов, использующих старшие биты;
блокирование ответов, содержащих исполняемые файлы ОС Windows.

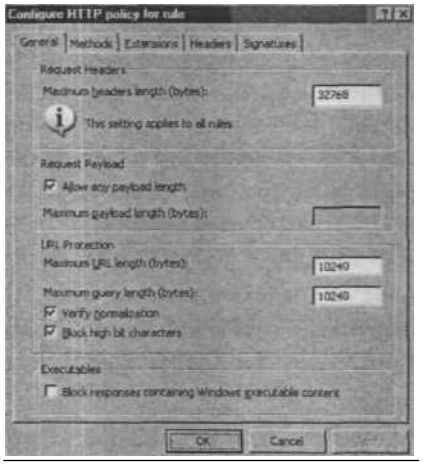


Рис. 10.16. Вкладка General (Общие)

Параметр **Maximum headers length (bytes)** (Максимальная длина заголовков, в байтах) позволяет задать максимальную длину всех заголовков, включенных в запрос соединения по HTTP-протоколу. Он применяется ко *всем* правилам, использующим HTTP-фильтр защиты. Этот установочный параметр защищает от атак, пытающихся создать переполнение буферов Web-сайта за счет отправки на Web-сервер избыточно длинных заголовков. Если задать слишком маленькую величину, некоторые приложения на сайте могут работать некорректно. Если же установить слишком большое значение, злоумышленники смогут сформировать специальный HTTP-запрос, способный породить на Web-сайте или Web-сервере известные и неизвестные проблемы, связанные с переполнением буферов. Можно начать с 10 000 байтов и при необходимости увеличивать это значение. Администратор Web-сайта вероятно сможет помочь определить максимальную длину заголовка, для сайтов, защищенных брандмауэром ISA.

В области **Request Pay load** (Полезные данные запроса) можно разрешить любой размер полезных данных или задать конкретную максимальную длину для них. Полезные данные — это часть HTTP-сообщения, не относящаяся к HTTP-заголовку или структуре команды. Например, если разрешить пользователям посылать данные на Web-сайт (бланк заказа или обсуждение для форума), то можно установить предельную длину для этих отправлений, сбросив флажок **Allow any payload length** (Разрешена любая

длина полезных данных) и введя настраиваемое значение в текстовое поле **Maximum** payload **length** (bytes) (Максимальная длина полезных данных, в байтах). Как и в предыдущем случае, можно обсудить требования с администратором Web-сайта или Web-программистом и получить подробные рекомендации для определения максимальной длины полезных данных, требуемой защищенными Web-сайтами.

В области **URL Protection** (Защита URL) есть несколько параметров. Вариант **Maximum URL length (bytes)** (Максимальная длина URL, в байтах) позволяет задать максимальную длину URL-адреса, который пользователь может переслать через брандмауэр, выполняя запрос к Web-сайту через брандмауэр. Злонамеренные программы могут посылать избыточно длинные URL-адреса, пытаясь создать переполнение буфера или другой тип атаки на Web-сервере. Значение по умолчанию — **10240,** но его можно изменить в соответствии с требованиями сайтов. Параметр **Maximum query length (bytes)** (Максимальная длина запроса, в байтах) позволяет задать максимальную длину доли запроса в URL-адресе. Эта часть URL-адреса появляется после вопросительного знака (?) *в* URL-запросе. Значение, установленное по умолчанию, — **10240,** но его можно изменить в соответствии с определенными требованиями. Имейте в виду, что **Maximum URL length** (Максимальная длина URL-адреса) должна быть больше **Maximum query length** (Максимальная длина запроса), поскольку запрос — это только часть URL-адреса.

Параметр **Verify normalization** (Проверка нормализации) также включен в область URL Protection. *Нормализация* — процесс декодирования так называемых «управляющих» («escaped») символов. Web-серверы могут получать запросы, закодированные с помощью таких символов. Один из наиболее распространенных примеров — наличие пробела в URL-адресе, таком как **http://msfirewall.org/Dir% 20One/default%20file.htm.** Символьная комбинация **%20** — это escape-символ, представляющий пробел. Проблема заключается в том, что злоумышленники могут закодировать символ «%* и выполнить так называемые дважды кодированные (double encoded) запросы. Двойное кодирование может применяться в атаках на Web-серверы. Когда выбран параметр **Verify normalization,** HTTP-фильтр защиты нормализует или декодирует запрос дважды. Если запрос после первого и второго декодирования не один и тот же, HTTP-фильтр защиты отбросит его. Это действие защищает от атак «двойного кодирования». Следует активизировать этот параметр, но помнить о том, что плохо написанные Web-сайты и Web-приложения не всегда учитывают проблемы безопасности и могут на самом деле принимать и требовать запросы с двойным кодированием. Если это касается сайтов в Интернете, к которым вы хотите получить доступ, или сайтов, публикуемых вами с помощью брандмауэра ISA, необходимо сбросить данный флажок.

Вариант **Block high bit characters** (Удалять символы с использованием старших битов) позволяет удалять HTTP-запросы, включающие URL-адреса с символами, использующими старшие биты. Символы, для представления которых используются старшие биты, применяются во многих языках, использующих расширенные наборы символов, поэтому, если выяснится, что невозможно получить доступ

к Web-сайтам, применяющим такие расширенные наборы символов в своих URL-адресах, следует сбросить этот флажок.

Параметр **Block responses containing Windows executable content** (Блокировать ответы, содержащие исполняемые файлы Windows) позволяет помешать пользователям пересылать исполняемые файлы Windows (такие как файлы с расширением exe, но для обозначения исполняемых файлов Windows может быть использовано любое расширение файла). HTTP-фильтр защиты способен определить, является ли файл исполняемым файлом Windows, поскольку ответ будет начинаться с комбинации MZ. Это свойство может оказаться очень полезным, если необходимо помешать пользователям загружать исполняемые файлы через брандмауэр ISA.

СОВЕТ Помните, что HTTP-политика настраивается для каждого правила. Поскольку можно конфигурировать ее, основываясь на отдельном правиле, перечисленные установочные параметры можно задать для одних правил и отказаться от них в других правилах. Такая возможность настройки HTTP-политики отдельно для каждого правила обеспечивает существенную гибкость в выборе содержания, доступного с конкретных сайтов, для определенных пользователей и в заданное время.

Вкладка Methods

Используя установочные параметры на вкладке **Methods** (Методы) (рис. 10.17), можно управлять HTTP-методами, применяемыми в правиле доступа или правиле публикации Web-сервера. Предлагаются три варианта: а разрешить все методы;

- разрешить только заданные методы;
- запретить заданные методы (разрешить все остальные).

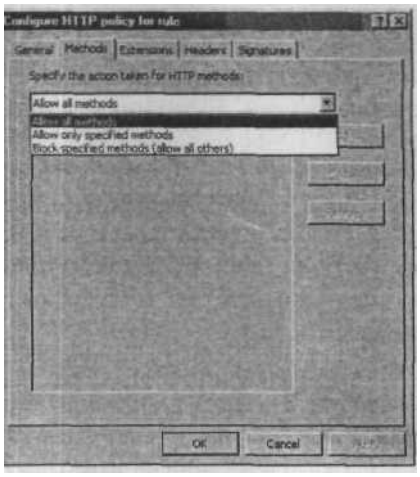


Рис. 10.17. Вкладка **Methods** (Методы)

HTTP-методы — это HTTP-команды, которые хосты могут посылать на Web-сервер для выполнения определенных действий, такие как GET, PUT и POST. Существуют и другие команды, с которыми вы можете быть незнакомы как администратор сети и брандмауэра, к ним можно отнести HEAD, SEARCH и CHECKOUT. Есть и узкоспециализированные методы, применяемые конкретными Web-приложениями, такие как Outlook Web Access. Вариант **Allow all methods** (Разрешить все методы) позволит разрешить использование HTTP-методов в HTTP-соединении, устанавливаемом через брандмауэр ISA.

ПРИМЕЧАНИЕ Если разрешить доступ к приложениям Microsoft, то обнаружатся и другие HTTP-методы, в том числе RPC_IN_DATA и RPC_OUT_DATA, которые применяются для клиентов Outlook 2003 при защищенной публикации по протоколу RPC поверх HTTP-протокола. Но помните, что фильтр *блокирует* только коммуникации, заданные в политике HTTP-фильтра, поэтому будьте осторожны и не блокируйте методы, которые могут понадобиться, особенно если точно не известно, какие именно методы могут потребоваться. Мы советуем тщательно протестировать установленные параметры фильтра и выяснить у администраторов и разработчиков Web-приложений, какие методы необходимы.

Вариант **Allow only specified methods** (Разрешить только заданные методы) позволяет указать, какие именно методы разрешается пересылать через брандмауэр ISA. Если есть возможность выяснить, какие методы требуются вашим Web-сайту и Web-приложению, то можно разрешить только их и заблокировать любые другие методы. Некоторые методы могли бы поставить под угрозу Web-сайт, поэтому, если они не нужны, блокируйте их.

Параметр **Block specified methods (allow all others)** (Запретить заданные методы, разрешить все остальные) позволяет разрешить применение всех методов за исключением заданных, которые следует запретить. Этот вариант наделяет пользователя несколько большими возможностями, даже если он не знает всех методов, которые могут потребоваться сайту, но может знать некоторые из тех, что определенно не нужны. Одним из примеров может быть метод POST. Если пользователям не разрешается посылать данные на Web-сайт, нет смысла разрешать метод POST, и его можно блокировать явным образом.

Если выбран параметр **Allow only specified methods** (Разрешить только заданные методы) или вариант **Block specified methods (allow all others)** (Запретить заданные методы, разрешить все остальные), необходимо щелкнуть мышью кнопку **Add** (Добавить) и ввести метод, который нужно разрешить или запретить. После нажатия кнопки **Add** (Добавить) на экране появляется диалоговое окно **Method** (Метод).

В диалоговом окне **Method** (Метод) вводится имя метода в одноименное текстовое поле (рис. 10.18). Можно также добавить описание метода в текстовое поле **Description** (Описание). Оно поможет запомнить, что делает метод, а также окажет помощь пришедшему вам на смену **специалисту,** столкнувшемуся с необходи-

мостью управления брандмауэром ISA и не знающему внутренней структуры набора команд HTTP-протокола.

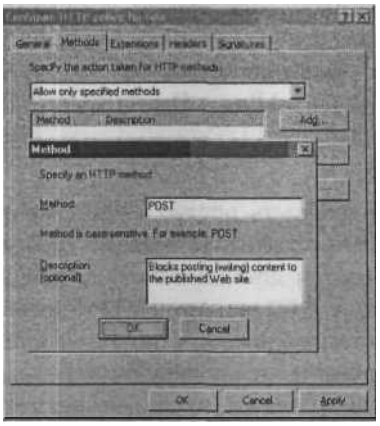


Рис. 10.18. Диалоговое окно **Method** (Метод)

Вкладка Extensions

На вкладке **Extensions** (Расширения) представлены следующие варианты (рис. 10.19):

- Allow all extensions (Разрешить все расширения);
- Allow only specified extensions (Разрешить только указанные расширения);
- Block specified extensions (allow all others) (Запретить указанные расширения, разрешить все остальные);
- Block requests containing ambiguous extensions (Запретить запросы, содержащие подозрительные расширения).

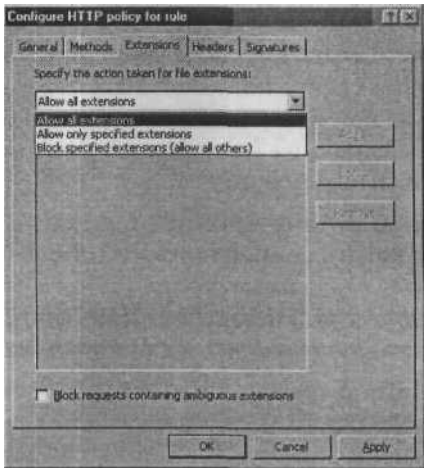


Рис. 10.19. Вкладка Extensions (Расширения)

Предоставляется возможность управлять расширениями файлов, которые можно запрашивать через брандмауэр ISA. Это крайне полезно, если нужно запретить пользователям запросы файлов определенных типов через брандмауэр. Например, можно запретить пользователям доступ через брандмауэр ISA к файлам с расширениями exe, com, zip и любыми другими.

Вариант **Allow all extensions** (Разрешить все расширения) позволяет настроить правило доступа или правило публикации Web-сервера для разрешения доступа пользователей, основанного на расширении файла, к файлам любого типа через брандмауэр ISA. Выбрав вариант **Allow only specified extensions** (Разрешить только указанные расширения), можно задать определенные расширения файлов, к которым возможен доступ пользователей через брандмауэр ISA. Вариант **Block specified extensions (allow all others)** (Запретить указанные расширения, разрешить все остальные) предоставляет возможность запретить заданные расширения файлов, которые вы считаете опасными.

Если выбран вариант **Allow only specified extensions** (Запретить указанные расширения, разрешить все остальные) или **Block specified extensions (allow all others)** (Запретить указанные расширения, разрешить все остальные), необходимо щелкнуть мышью кнопку **Add** (Добавить) и ввести расширения, которые вы хотите разрешить или запретить.

После нажатия мышью кнопки **Add** (Добавить) на экране появится диалоговое **окно Extension** (Расширение). Введите расширение в текстовое поле **Extension** (Расширение). Например, если следует запретить доступ к файлам с расширением exe, введите **exe.** Есть возможность ввести описание в необязательное текстовое поле **Description (optional)** (Описание, необязательно). Щелкните мышью кнопку ОК для сохранения добавленного расширения (рис. 10.20).

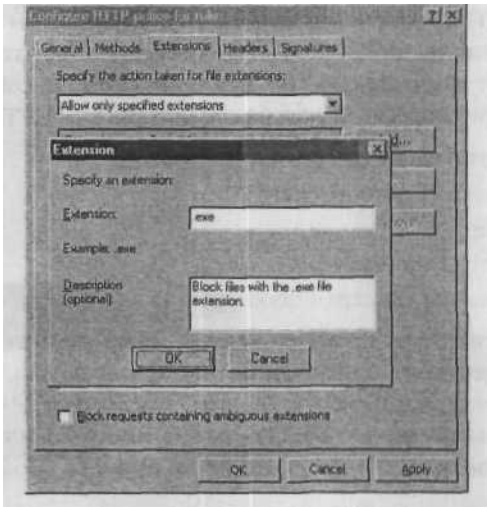


Рис. 10.20. Диалоговое окно **Extension** (Расширение)

Вкладка Headers

На вкладке **Headers** (Заголовки) представлены следующие параметры (рис. 10.21):

- Allow all headers except the following (Разрешить все заголовки за исключением следующих);
- Server header (Заголовок сервера);
- Via header (Маршрутный заголовок).

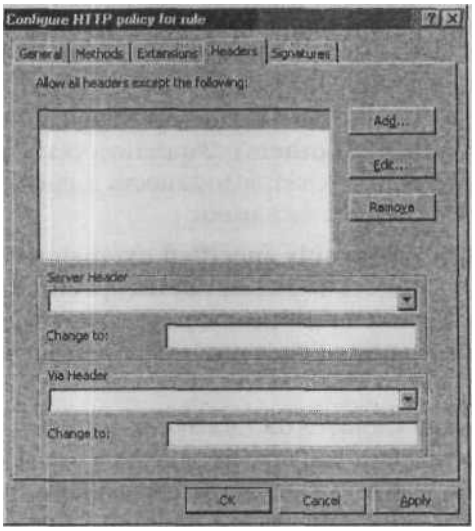


Рис. 10.21. Вкладка Headers (Заголовки)

HTTP-заголовок содержит характерную для HTTP-сообщения информацию, которая включается в HTTP-запросы, сделанные Web-клиентом (таким как Web-обозреватель), и HTTP-ответы, посылаемые Web-сервером обратно Web-клиенту. Эти заголовки выполняют многочисленные функции, такие как определение статуса и состояния HTTP-коммуникаций и других характеристик HTTP-сеанса связи

К общим HTTP-заголовкам относятся следующие:

- размер содержимого (Content-length);
- директива (Pragma);
- пользователь-агент (User-Agent);
- принятое кодирование (Accept-Encoding).

Можно принимать все HTTP-за головки или запретить конкретные, заданные HTTP-заголовки. Существуют определенные HTTP-заголовки, которые рекомендуется блокировать всегда, например такие, как заголовок P2P-Agent, используемый многими одноранговыми (peer-to-peer) приложениями. Если нужно запретить конкретный HTTP-заголовок, щелкните мышью кнопку **Add** (Добавить).

В диалоговом окне **Header** (Заголовок) выберите вариант **Request headers** (Заголовки запросов) или вариант **Response headers** (Заголовки ответов) в раскрывающемся списке **Search in** (Искать в). Введите HTTP-за головок, который вы хотите запретить, в текстовое поле **HTTP header** (HTTP-заголовок). Щелкните мышью кнопку OK (рис. 10.22).

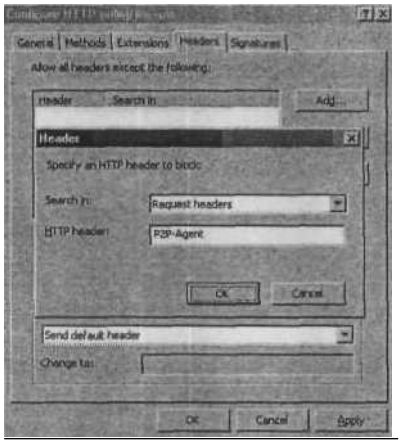


Рис. 10.22. Диалоговое окно Header (Заголовок)

Можно настроить заголовок сервера, возвращаемый в HTTP-ответах, выбрав вариант **Server Header** (Заголовок сервера) в раскрывающемся списке. Заголовок сервера — это HTTP-заголовок, посылаемый Web-сервером обратно Web-клиенту и информирующий последнего о типе Web-сервера, с которым соединяется клиент. Злоумышленники могут использовать эту информацию для атаки Web-сервера. Имеются следующие возможности:

- послать исходный заголовок;
- удалить заголовок из ответа;
- изменить заголовок в ответе.

Вариант **Send original header** (Послать исходный заголовок) позволяет передать неизмененным заголовок, посланный Web-сервером. Вариант **Strip header from response** (Удалить заголовок из ответа) разрешает брандмауэру ISA убрать заголовок сервера, а вариант **Modify header in response** (Изменить заголовок в ответе) позволяет изменить заголовок. Следует изменять заголовок, чтобы запутать злоумышленников. Поскольку Web-клиенты не требуют этот заголовок, можно изменить его на **Private,** CompanyName или другое понравившееся вам имя.

Перечисленные варианты помогут помешать злоумышленникам (или, по крайней мере, задержать их). Им придется потратить больше усилий и использовать альтернативные методы для просмотра идентификационной информации («fingerprint») вашего Web-сервера (рис. 10.23).

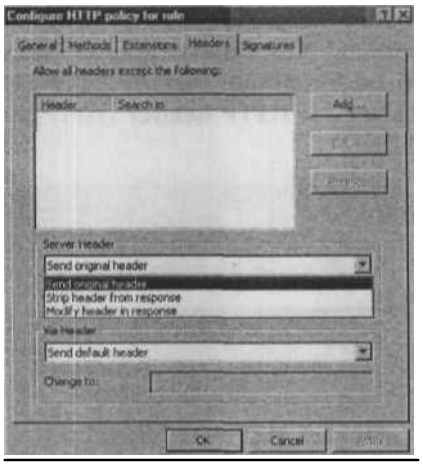


Рис. 10.23. Параметр Server Header (Заголовок сервера)

Параметр Via Header (Маршрутный заголовок) позволяет управлять маршрутным заголовком, посылаемым Web-клиенту. Если между клиентом и Web-сервером располагаются серверы Web-прокси, то сервер Web-прокси вставляет маршрутный заголовок в HTTP-сообщение, информирующий клиента о том, что запрос был обработан сервером Web-прокси в процессе передачи. Каждый сервер Web-прокси на пути запроса может добавить свой собственный маршрутный заголовок, и каждый отправитель на пути следования ответа удаляет свой маршрутный заголовок и пересылает ответ на сервер, заданный в следующем маршрутном заголовке, хранящемся в «стеке» маршрутных заголовков. Параметры маршрутного заголовка позволяют изменить имя брандмауэра ISA, включенное в его собственный маршрутный заголовок, или скрыть это имя. Установка по умолчанию на брандмауэре ISA — включать имя компьютера, на котором размещен брандмауэр, в маршрутный заголовок.

Имеются два возможных варианта:

- послать заголовок, установленный по умолчанию;
- изменить заголовок в запросе и ответе.

Вариант Send default header (Послать заголовок, установленный по умолчанию) оставляет маршрутный заголовок без изменений. Вариант Modify header in request and response (Изменить заголовок в запросе и ответе) позволяет изменить имя, включенное в маршрутный заголовок, вставляемый вашим брандмауэром ISA. Мы советуем изменять его, чтобы скрыть действительное имя вашего брандмауэра ISA и тем самым помешать злоумышленникам определить настоящее имя компьютера вашего брандмауэра ISA (рис.10.24).

Введите другой маршрутный заголовок в текстовое поле Change To (Заменить на).

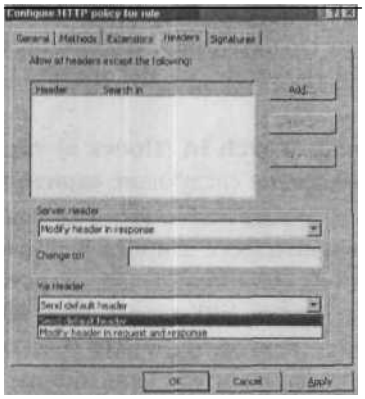


Рис. 10.24. Параметр Via **Header** (Маршрутный заголовок)

Вкладка Signatures

На вкладке Signatures (Сигнатуры) можно управлять доступом через брандмауэр ISA с помощью HTTP-сигнатур или подписей, созданных вами. Эти сигнатуры представляют собой строки, содержащиеся в следующих компонентах HTTP-сообщения:

- U RL-адресе запроса;
- заголовках запроса;
- теле запроса;
- заголовках ответа;
- теле ответа.

Получить доступ к диалоговому окну Signatures (Сигнатуры) (рис. 10.25) можно, щелкнув мышью кнопку Add (Добавить).

Рис. 10.25. Вкладка Signatures (Сигнатуры) **30**

За», *л т*

В диалоговом окне **Signature** (Сигнатура) введите имя сигнатуры в текстовое поле **Name** (Имя) и описание сигнатуры в текстовое поле **Description** (Описание). Последнее особенно полезно для того, чтобы знать о назначении и смысле этой сигнатуры.

В раскрывающемся списке **Search** in (Поиск в) укажите, где брандмауэру ISA искать заданную строку. Возможны следующие варианты.

- **Request URL** (URL-адрес запроса). Выбор этого варианта позволяет ввести строку, обнаружение которой в URL-адресе запроса Web-клиента вызовет блокирова ние соединения. Например, если нужно предотвратить любые запросы к сай там, содержащим строку *Kazaa* в URL-адресе, включенном в запрос Web-клиен та, введите *Kazaa* в текстовое поле **Signature** (Сигнатура).
- **Request headers** (Заголовки запроса). При выборе этого варианта введите в текстовое поле **HTTP header** конкретный HTTP-заголовок, который должен проверять брандмауэр ISA, и в текстовое поле **Signature** — строку в заголовке, которую необходимо блокировать. Например, если необходимо блокировать приложения P2P (одноранговые) файлообменной сети eDonkey, можно выбрать этот вариант, а затем **User-Agent** (Пользователь-агент) в текстовом поле **HTTP header.** Далее в текстовое поле **Signature** введите *ed2k.* Обратите внимание на то, что этот вариант предоставляет более тонкое управление, чем на вкладке **Headers** (Заголовки), — простая блокировка заголовков. Если запретить кон кретный заголовок на вкладке **Headers** (Заголовки), то будут блокироваться все HTTP-сообщения, использующие заданный заголовок. Создав сигнатуру, встро енную в указанный заголовок, можно разрешить этот заголовок во всех сооб щениях, не содержащих строку, которая введена как сигнатура.
- **Request body** (Тело запроса). Можно блокировать HTTP-сообщения, основыва ясь на теле Web-запроса, информации, не входящей ни в HTTP-команды, ни в заголовки. Несмотря на то, что это очень мощная функциональная возможность, она может потреблять большой объем ресурсов на компьютере брандмауэра ISA. По этой причине следует определить диапазон проверяемых брандмауэром ISA байтов в текстовых полях **From** (От) и **To** (До) в области вкладки **Byte range** (Диапазон, в байтах). У нас нет точных рекомендаций, касающихся конкретных значений, которые следует вводить в этой области, но мы предоставим дополни тельные сведения об этом на сайте **www.isaserver.org,** как только они появятся.
- **Response headers** (Заголовки ответов). Если выбран этот вариант, то вводится конкретный HTTP-заголовок, который следует блокировать, основываясь на HTTP-ответе, возвращенном Web-сервером. Введите этот заголовок в текстовое поле **HTTP header,** а строку, включенную в HTTP-заголовок, — в текстовое поле **Signature.**
- **Response body** (Тело ответа). Этот вариант функционирует так же, как вариант **Request body** (Тело запроса), за исключением того, что он применяется к со держимому, возвращаемому Web-клиенту с Web-сервера. Например, если нуж-

но блокировать Web-страницы, содержащие конкретные строки, которые определяются как опасные или неподходящие, можно создать сигнатуру для блокирования этих строк. Вспомните об этом, узнав о новейшей Web-ориентированной атаке, и создайте сигнатуру, блокирующую соединения, организующие подобные атаки.

На рис. 10.26 показано несколько примеров сигнатур, блокирующих некоторые часто встречающиеся приложения, которые могут считаться ощутимой угрозой безопасности для корпоративных сетей.

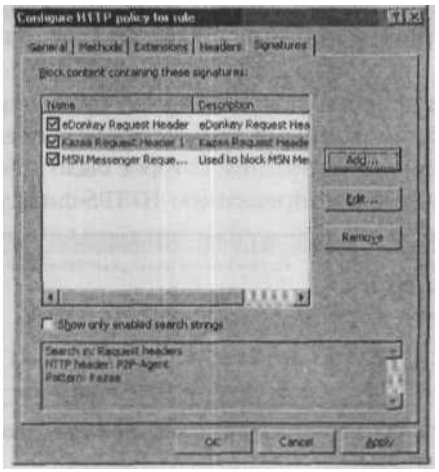


Рис. 10.26. Примеры сигнатур

СОВЕТ Еще одна сигнатура, которую, возможно, потребуется создать, блокирует строку <iframe src="?"/> в теле ответа. Эта строка потенциально может опознать процессор на машине-жертве и вызвать зависание операционной системы.

Ведение журнала регистрации HTTPS-фильтра

Как узнать, работают ли ваши фильтры защиты? Один из способов определения эффективности параметров, установленных вами в HTTPS-фильтре, — применение встроенного в брандмауэр ISA средства просмотра журналов регистрации (built-in log viewer). Выполните следующие шаги для конфигурирования встроенного в брандмауэр ISA средства просмотра журналов регистрации и проверки действий HTTPS-фильтра. 1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел **Monitoring** (Наблюдение) на левой панели консоли.

2. В узле **Monitoring** (Наблюдение) щелкните кнопкой мыши вкладку **Logging** (Ведение журнала регистрации). На вкладке **Tasks** (Задачи) панели задач щелкните мышью ссылку **Start Query** (Начать запрос).
3. Щелкните правой кнопкой мыши на заголовках столбцов и левой кнопкой мыши команду **Add/Remove Columns** (Добавить/Удалить столбцы). В диалоговом
4. окне **Add/Remove Columns** (Добавить/Удалить столбцы) щелкните кнопкой мыши элемент **Filter Information** (Информация фильтра) в списке **Available Columns (Доступные** столбцы) и щелкните мышью кнопку **Add** (Добавить). После этого элемент **Filter Information** (Информация фильтра) появится в списке **Displayed columns** (Отображаемые столбцы). Щелкните мышью кнопку ОК.
5. Выводится запрос от клиента, находящегося за брандмауэром ISA, который был бы заблокирован установочными параметрами вашего HTTPS-фильтра. На рис. 10.27 показан пример соединения, которое было заблокировано, потому что URL-адрес содержал строку, запрещенную HTTPS-фильтром.

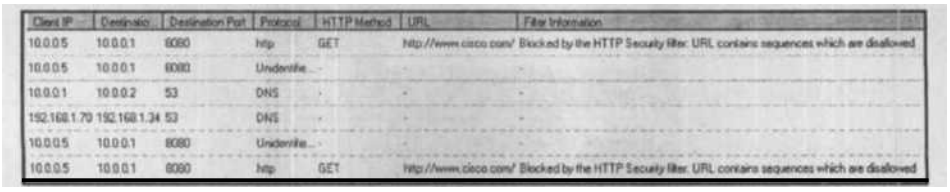


Рис. 10.27. Записи файла регистрации, показывающие блокирование соединения HTTP-фильтром защиты

Экспортирование и импортирование установочных параметров HTTPS-фильтра

HTTP-политика может быть экспортирована из правила доступа, использующего HTTP-протокол, или из правила публикации Web-сервера либо импортирована в подобные правила. Для экспорта существующей HTTP-политики, которая ухе настроена в правиле доступа или правиле публикации Web-сервера, может применяться сценарий HttpFilterConfig.vbs, хранящийся в папке \sdk\samples\admin. HTTP-политика, уже экспортированная в файл, может импортироваться в существующее правило доступа или правило публикации Web-сервера.

Сценарий HttpFilterConfig.vbs значительно упрощает конфигурирование сложных HTTP-политик, включающих многочисленные входные параметры, такие как сигнатуры, расширения файлов и заголовки. Мы советуем вам экспортировать HTTP-политики после создания их на консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004).

В этом разделе мы обсудим, как можно экспортировать HTTP-политику из правила публикации Web-сервера и импортировать ее в такое правило.

СОВЕТ У Джима Харрисона (Jim Harrison), разработчика сценариев брандмауэра ISA, на сайте есть несколько предотвращающих атаки средств и сценариев, которые автоматически настраивают HTTP-политику как часть конфигурации, предотвращающей и ослабляющей атаки. Познакомьтесь с фантастическими средствами брандмауэра ISA, разработанными Джимом, на Web-сайте www.isatools.org.

Экспортирование HTTP-политики из правила публикации Web-сервера

HTTP политики можно экспортировать из правила доступа или правила публикации Web-сервера, используя файл HttpFilterConfig.vbs, расположенный на CD-диске ISA 2004. Выполните следующие шаги для экспорта HTTP-политики из существующего правила публикации Web-сервера.

1. Скопируйте файл HttpFilterConfig.vbs с CD-диска ISA 2004 в корневой каталог диска C:.
2. Откройте окно командной строки и перейдите в корневой каталог диска C:. Введите следующую команду и нажмите клавишу <Enter> (имейте в виду, что, если в названии правила есть пробел, название следует заключить в кавычки):

```
C:\Httpfilterconfig.vbs export "Publish OWA Site" C:\webpol.xml
```

3. На экране появится диалоговое окно, подтверждающее, что информация из правила была успешно экспортирована (рис. 10.28).

Рис. 10.28. Диалоговое окно, информирующее об успешном экспорте

Импортирование HTTP-политики в правило публикации Web-сервера

HTTP-политики можно импортировать в **правила** доступа, включающие HTTP-протокол, и правила публикации Web-сервера. Мы используем тот же сценарий, который применялся при экспортировании HTTP-политики, — HttpFilterConfig.vbs. Для импортирования политики, сохраненной в файле с расширением *xml,* в правило публикации Web-сервера с именем **Publish OWA Site** выполните следующие шаги.

1. Скопируйте файл с расширением xml и сценарий HttpFilterConfig.vbs, хранящийся на CD-диске ISA 2004, в корневой каталог диска C:. В нашем примере xml-файл назван webpol.xml.
2. Откройте окно командной строки и перейдите в корневой каталог диска C:. Введите следующую команду и нажмите клавишу <Enter> (имейте в виду, что, если в названии правила есть пробел, название следует заключить в кавычки):

   C:\Httpfilterconfig.vbs import "Publish OWA Site" C:\webpol.xml

3. На экране появится диалоговое окно, подтверждающее, что информация была успешно импортирована в правило (рис. 10.29).

Рис. 10.29. Диалоговое окно, информирующее об успешном импорте

Исследование HTTP-заголовков для поиска потенциально опасных приложений

Одна из первоочередных задач администратора брандмауэра ISA — исследование характеристик сетевого трафика с целью блокирования новых и всегда более опасных приложений. Это могут быть одноранговые (peer-to-peer) приложения, приложения диалогового обмена сообщениями (instant messaging) или другие приложения, прячущиеся в HTTP-заголовке. Многие разработчики скрывают свои приложения внутри HTTP-заголовка, пытаясь разрушить вашу политику брандмауэра. Задача администратора брандмауэра ISA — расстроить попытки разработчиков, направленные на разрушение политики использования сети.

Как можно догадаться, разработчики подобных приложений неохотно делятся информацией о том, как помешать их приложениям нарушать защиту брандмауэра. Зачастую следует самостоятельно добывать эти сведения, особенно относящиеся к новым и скрытым приложениям.

Главное средство в борьбе с мусорным программным обеспечением в сети (scumware) — анализатор протоколов (protocol analyzer). Два наиболее популярных анализатора протоколов — Microsoft Network Monitor (сетевой монитор фирмы

Microsoft) и бесплатное программное средство Ethereal. Оба варианта превосходны, единственный недостаток Ethereal — необходимость установки сетевого драйвера для корректной работы этого средства. Поскольку взаимодействие драйвера WinPcaP, требуемого Ethereal, с программным обеспечением брандмауэра ISA не подвергалось регрессионному тестированию, сложно выяснить, не ухудшит ли оно стабильность или производительность брандмауэра. По этой причине в следующих примерах мы будем использовать версию Network Monitor, включенную в состав операционной системы Windows Server 2003.

Рассмотрим несколько примеров, описывающих способы блокирования некоторых угрожающих приложений. Одно из таких приложений — одноранговое приложение совместного использования файлов (peer-to-peer file-sharing application) файлообменной сети eDonkey. Первый шаг — запуск сетевого монитора Network Monitor и выполнение трассировки сетевого монитора во время работы приложения eDonkey на машине клиента, получающего доступ к Интернету через брандмауэр ISA. Лучше всего начать с конфигурирования Network Monitor для ожидания обращений к интерфейсу внутренней сети брандмауэра ISA или какому-либо интерфейсу, используемому приложением eDonkey или другими вызывающими сбои в работе приложениями для доступа к Интернету через брандмауэр ISA.

Остановите трассировку на время после выполнения нарушающего работу приложения. Поскольку нас интересуют только Web-соединения, устанавливаемые через TCP-порт 80, можно исключить из трассировки все остальные коммуникации. Сделать это можно с помощью фильтров отображения (Display filter).

Щелкните кнопкой мыши пункт меню **Display** (Отображение) и команду **Filter** (Фильтр). В диалоговом окне **Display Filter** (Фильтр отображения) дважды щелкните кнопкой мыши строку **Protocol** = **Any** (Протокол = Любой) **(рис.** 10.30).

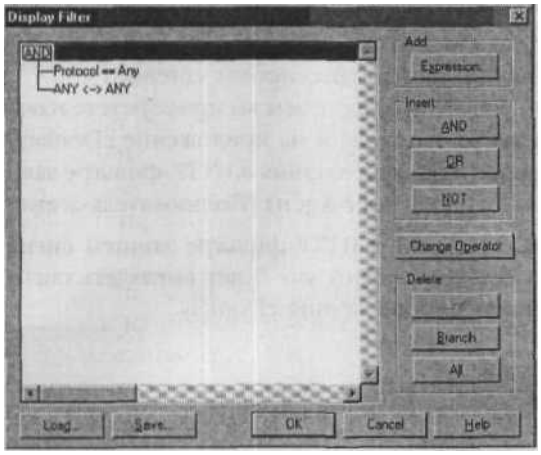


Рис. 10.30. Диалоговое окно **Display Filter** (Фильтр отображения)

В диалоговом окне **Expression** (Представление) щелкните кнопкой мыши вкчадку **Protocol** (Протокол) *и* затем кнопку **Disable All** (Скрыть все). В списке **Disabled Protocols** (Скрытые протоколы) щелкните кнопкой мыши протокол HTTP, а затем кнопку **Enable** (Разрешить отображение) и далее кнопку OK (рис. 10.31).

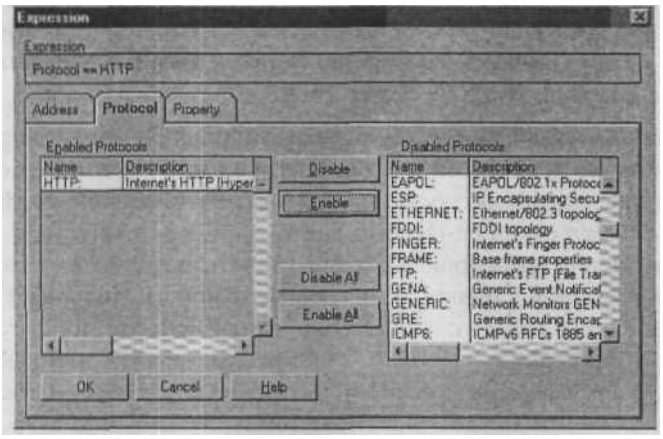


Рис. 10.31. Диалоговое окно Expression (Представление)

Щелкните мышью кнопку OK в диалоговом окне **Display Filter** (Фильтр отображения). Теперь на верхней панели консоли **Network Monitor** (Сетевой монитор) отображаются только HTTP-соединения. Стоит начать с просмотра запросов **GET,** которые появляются как **GET Request from Client** (Запрос GET от клиента) в столбце **Description** (Описание). Дважды щелкните кнопкой мыши запросы **GET** и раскройте строку **HTTP: Get Request from Client** в форме, расположенной в средней части консоли. В ней отображается список заголовков запросов.

На рис. 10.32 показано, что появился один необычный заголовок (вы поймете это, только имея опыт просмотра трассировок сетевого монитора; не отчаивайтесь, пройдет достаточно времени, прежде чем вы приобретете навык). Заголовок **HTTP: User-Agent = ed2k** кажется похожим на приложение eDonkey2000. Мы можем использовать эту информацию для создания в HTTP-фильтре защиты параметра блокирующего заголовок запроса **User-Agent** (Пользователь-агент) со значением ed2k.

Сделать это можно, создав в HTTP-фильтре защиты сигнатуру с указанными значениями. На рис. 10.33 показано, как будет выглядеть сигнатура HTTP-фильтра защиты для блокирования приложения e Don key.

Рис. 10.32. Окно отображения Network Monitor (Сетевой монитор)

Рис. 10.33. Диалоговое окно Signature (Сигнатура)

Еще один пример опасного приложения — приложение файлообменной сети *Kazaa.* На рис. 10.34 показана область отображения запроса GET, посылаемого клиентом через брандмауэр ISA. В списке HTTP-заголовков есть один, который может помочь блокированию клиента сети *Kazaa.* Можно полностью блокировать HTTP-заголовок запроса P2P-Agent или создать сигнатуру и блокировать этот заголовок, только если он содержит значение *Kazaa.* Вы также можете блокировать заголовок Host (Хост) в HTTP-заголовке запроса, если в нем установлено значение desktop.kazaa.com.

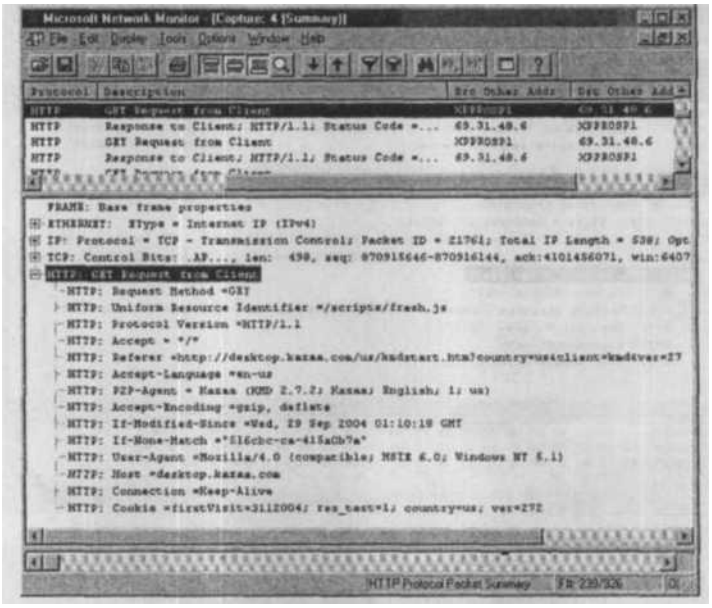


Рис. 10.34. Представление Network Monitor (Сетевой монитор), показывающее заголовки запроса *Kazaa*

Примеры политик HTTPS-фильтра

Создание политик HTTPS-фильтра может занять некоторое время. Придется выполнить требуемые приложения и затем определить необходимые методы, расширения, заголовки и сигнатуры, характерные для данного приложения. Безусловно, это время не будет потрачено зря, но иногда нужно быстро подготовить и выполнить критические приложения.

По этой причине мы включаем несколько примеров политик HTTPS-фильтра, которые сразу можно применить для защиты Web-сайтов IIS (Internet Information Server, информационный сервер Интернета) и сайтов Outlook Web Access (Web-доступ посредством Outlook).

В табл. 10.2 приведены задаваемые по умолчанию установочные параметры хорошей политики HTTPS-фильтра гипотетического Web-сайта, которую можно использовать. Эта политика разрешает большую часть широко распространенных методов, требуемых для простых Web-сайтов, и ограничивает расширения файлов, способных позволить злоумышленник^' повредить сайт. В нее включено также несколько HTTP-сигнатур, блокирующих часто встречающиеся строки, которые интернет-преступники могут использовать для нарушения работы Web-сайта или сервера.

Табл. 10.2. Пример политики HTTPS-фильтра для типичных Web-сайтов

Вкладка	**П а р а м е т р .**
General (Общие)	Максимальная длина заголовка — 32768 Установлен флажок **Allow** any **payload length** Максимальная длина URL-адреса — 260 Максимальная длина запроса — 4096 Установлен флажок **Verify normalization** Сброшен флажок **Block high bit characters**
Methods (Методы)	**Allow only specified methods:** GET HEAD POST
Extensions (Расширения)	**Block specified extensions (allow all others):** .exe, **.bat,** .cmd, .com, litw, .ida, .idq, .htr, .idc.shtm, .shtml, stm, printer, .ini, .log, ,pol, .dat
Headers (Заголовки)	Никаких изменений по сравнению с установками по умолчанию
Signatures (Сигнатуры)	**Block content containing these signatures:**
(Request URL) (URL запроса)	./ \ % &

В табл. 10.3 приведены установочные параметры, с помощью которых можно конфигурировать политику HTTPS-фильтра для OWA-публикации. Обратите внимание на методы, требуемые OWA (Outlook Web Access, Web-доступ посредством Outlook). Увидеть их в действии можно с помощью встроенного в брандмауэр ISA фильтра регистрации, в столбце **HTTP Methods** (HTTP-методы).

СОВЕТ Иногда не следует включать в список сигнатур символ & и в список блокируемых расширений — расширение **.exe.** Вам придется разрешить это расширение для загрузки элемента управления S/MIME. Однако, поскольку политика HTTPS-фильтра применяется к каждому правилу поочередно, мы надеемся, что вы создадите отдельное правило, разрешающее доступ для специфических нужд Outlook Web Access, и поместите его перед правилом, блокирующим доступ в соответствии с установками из табл. 10.3. Разрешающее правило разрешит доступ только к каталогу OWA, содержащему упомянутые элементы управления. Если запретить символ & в запросах, определенные функции, такие как Calendaring (Ведение календарей), не будут выполняться корректно.

Табл. 10.3. Установочные параметры HTTPS-фильтра для правил публикации Web-сервера OWA

Вкладка	Параметр
General (Общие)	Максимальная длина заголовка — 32768 **Установлен** флажок **Allow any payload length** Максимальная длина URL-адреса — 260 Максимальная длина запроса — 4096 Установлен флажок **Verify normalization** брошен флажок **Block high bit characters**
Methods (Методы)	**Allow only specified methods:**
GET, POST, PROPFIND, PROPPATCH, BPROPPATCH, MKCOL **DELETE,** BDELETE, BCOPY, MOVE, SUBSCRIBE, BMOVE, POLL, SEARCH **Extensions** (Расширения) **Block specified extensions (allow all others):**	
	.exe, .bat, .cmd, .com, **.htw,** ,ida, .idq, .htr, .idc, .slum, .shtml, .stm, .printer, .ini, Jog, pol, .dat
Headers (Заголовки)	**Никаких** изменений по сравнению с установками по умолчанию
Signatures (Сигнатуры)	**Block content containing these signatures**
(Request URL)	./
(URL запроса)	\
	&

В табл. 10.4 приведены входные параметры политики HTTPS-фильтра, которые можно использовать для правила публикации Web-сервера по протоколу RPC поверх HTTP. Обратите внимание на то, что в протоколе RPC поверх HTTP программ Outlook 2003 применяются необычные методы.

Табл. 10.4. Установочные параметры HTTPS-фильтра для правил публикации Web-сервера по протоколу RPC поверх HTTP

Вкладка	Параметр
General (Общие)	Максимальная длина заголовка — 32768 Максимальный размер полезных данных — 2000000000 Максимальная длина URL-адреса — 16384 Максимальная длина запроса — 4096 Установлен флажок **Verify normalization** Сброшен **флажок Block high bit characters**
Methods (Методы)	**Allow only specified methods:** RPC IN_DATA RPC_OUT_DATA
Extensions (Расширения)	Никаких изменений по сравнению с установками по умолчанию
Headers (Заголовки)	Никаких изменений по сравнению с установками по умолчанию

Табл. 10.4. (окончание)

Вкладка	Параметр
Signatures (Сигнатуры) (Request URL) (URL запроса)	Никаких изменений по сравнению с установками по умолчанию

Обычно блокируемые заголовки и сигнатуры приложений

Несмотря на то, что мы считаем увлекательным времяпрепровождением просиживание долгими вечерами за сетевым монитором и выяснение способов блокирования угрожающих приложений, не все администраторы брандмауэра ISA разделяют эту точку зрения. Для тех, кому необходимо как можно быстрее сконфигурировать свой брандмауэр ISA для защиты сети от опасных приложений, мы предлагаем необходимую информацию в табл. 10,5, Ш,б.

В табл. 10.5 приведены данные, которые нужно включить в сигнатуры для блокирования часто встречающихся опасных приложений. Указанную информацию следует использовать для создания образцов сигнатур в HTTPS-фильтре.

Табл. 10.5. Образцы сигнатур для блокирования часто встречающихся опасных приложений

Приложение	Ме стона хожден ие	HTTP-за головок	Сигнатура
MSN Messenger	Request headers (Заголовки запроса)	User-Agent: (Пользователь-агент)	MSN Messenger
Windoivs Messenger	Request headers (Заголовки запроса)	User-A gent: (П о л ьзова те л ь - а ген т)	MSMSGS
Netscar)e 7	Request headers (Заголовки запроса)	User-A gent: (П о л ь зо вате ль- а ге нт)	Netscape/7
Netscap>e 6	Request headers (Заголовки запроса)	User-A gent: (Пол ьзователь- агент)	Netscape/6
AOL Misssenger (and all Gecko browsers) (и все обозреватели Gecko)	Request headers (Заголовки запроса)	User-Agent: (Пользователь-агент)	Gecko/
Yahoo Messenger	Request headers (Заголовки запроса)	Host (Хост)	msg yah oo. com
Kazaa	Request headers (Заголовки запроса)	P2P-Agent	Kazaa
KazaaCilient: Kazaa	Request headers (Заголовки запроса)	Use r-Agent:	KazaaClient
Kazaa	Request headers (Заголовки запроса)	X-Kazaa-Network: (сеть X- Kazaa)	KaZaA

(см. след. стр.)

Табл. 10.5. (окончание)

Приложение	Местонахождение	HTTP-заголовок	Сигнатура
Gnutella	Request headers (Заголовки запроса)	User-Agent: (Пользователь-агент)	Gnutella Gnucleus
eDonkey	Request headers (Заголовки запроса)	User-Agent: (Пользователь-агент)	e2dk
Internet Explorer 6.0	Request headers (Заголовки запроса)	User-Agent: (Пользователь-агент)	MSIE 6.0
Morpheus	Response header (Заголовок ответа)	Server (Сервер)	Morpheus
BearShare	Response header (Заголовок ответа)	Server (Сервер)	Bearshare
BitTorrent	Request headers (Заголовок ответа)	User-Agent; (Пользователь-агент)	BitTorrent
SOAP over HTTP	Request headers (Заголовок ответа)	User-Agent: (Пользователь-агент)	SOAPAction

Табл. 10.6 содержит некоторые значения HTTP-заголовков, которые можно использовать для блокирования угрожающих приложений. В отличие от сигнатур, которые требуют значения и имени HTTP-заголовка, параметры, приведенные в табл. 10.6, могут быть настроены на вкладке Headers (Заголовки) HTTP-фильтра защиты. Эти заголовки специфичны для перечисленных опасных приложений и не применяются для законных HTTP-сообщений, поэтому не нужно задавать конкретные значения для блокированных HTTP-заголовков.

Табл. 10.6. HTTP-заголовки, применяемые для блокирования опасных приложений

Приложение	**Местонахождение**	**Тип**	Значение
Жахая	Заголовки	Заголовок запроса (Request Header)	X-Kazaa-Username: X-Kazaa-IP: X-Kazaa-SupernodeIP:
BitTorrent	Расширения	Нет	.torrent
Многие одноранговые клиенты (peer-to-peer clients)	Заголовки	Заголовок запроса (Request Header)	P2P-Agent

Опасности SSL-туннелирования

Главная забота администратора брандмауэра ISA — определение внешних пользователей, которые могут получить доступ к вашей корпоративной сети, и пользователей корпоративной сети, которые могут получить доступ к Интернету и другим сетям в пределах корпоративной сети. Много времени затрачивается на конфигурирование политики брандмауэра таким образом, чтобы пользователи имели доступ только к тем протоколам, которые могут применяться, к тем серверам, с кото-

рыми разрешено соединение, загружать только содержимое (контент), одобренное корпоративной политикой безопасности, и обращаться к ресурсам только в определенное время дня.

Должна быть предусмотрена возможность разрешать или запрещать VPN-соединения, подключения удаленного управления рабочим столом, доступ к Web-серверам и передачу файлов с помощью Web-соединений или соединений Instant Messenger (обмен диалоговыми сообщениями). Истина заключается в том, что необходима возможность явного разрешения или запрещения всех коммуникаций, устанавливаемых через брандмауэр ISA.

Главные проблемы возникают, когда брандмауэр сталкивается с зашифрованными сообщениями. Например, что произойдет, если пользователи применяют шифрованное SSL-соединение с Web-сайтом OWA (Outlook Web Access, Web-доступ посредством Outlook). Традиционные аппаратные брандмауэры (такие как PIX или Sonicwall) обнаружат входящее соединение с TCP-портом 443. Список контроля доступа (Access Control List, ACL) на аппаратном брандмауэре дает рекомендацию — разрешить входящее соединение и переслать его на сайт OWA в корпоративной сети.

OWA-клиент удаленного доступа устанавливает зашифрованное SSL-соединение с сайтом OWA. Все сообщения, проходящие через аппаратный брандмауэр, теперь зашифрованы, и брандмауэр не имеет сведений о содержимом зашифрованного «туннеля» SSL. Аппаратный брандмауэр ничего не может сделать, если злоумышленник или червь на машине клиента инициирует атаку на сервер с помощью зашифрованного SSL-сеанса связи. Простые аппаратные брандмауэры с отслеживающей состояние соединений фильтрацией просто сообщат: «Это SSL-соединение, а мой список ACL разрешает SSL-подключения к серверу OWA. Всего доброго».

Это серьезная проблема безопасности, одна из тех, которым аппаратные брандмауэры противостоять не могут. Тот факт, что злоумышленники способны выгодно использовать зашифрованный канал связи, который *разрешено установить* через брандмауэр, означает, что теряется контроль доступа, поскольку не может быть приведена в действие корпоративная политика брандмауэра для контроля содержимого зашифрованного канала.

Ситуация может стать еще *хуже*. Многие разработчики приложений проникают в процесс HTTP-туннелирования. Делается это очевидно для того, чтобы обойти «ограничительные брандмауэры», которые разрешают исходящие и входящие соединения только по HTTP- и/или HTTPS-протоколу. Подобные разработчики «заворачивают» свой протокол приложения в HTTP-заголовок для того, чтобы брандмауэры, настроенные на разрешение HTTP/HTTPS-коммуникаций, пропустили их приложение.

Примерами этого типа HTTP-туннелирования приложений, отличных от Web-приложений, могут быть RPC поверх HTTP(S), приложение GoToMyPC и большое число приложений HTTP-туннелирования, явно разработанных для разрушения политики брандмауэра (http://www.google.com/search?hl=en&ie=UTF-8&q=HTTP+ tunnel).

Так называемые «SSL VPNs» (VPN-соединения по протоколу SSL) также принадлежат к этой группе. VPN-соединения по протоколу SSL применяются для обхода защиты брандмауэра массивом протоколов приложений, спрятанных в зашифрованном SSL-канале. У всех этих приложений, разработанных либо для повышения производительности (таких как использующие протокол RPC поверх HTTP), либо явно для нарушения политики сетевого использования, одна цель: скрыть базовый протокол приложения внутри зашифрованного SSL-туннеля.

ПРИМЕЧАНИЕ Большинство «SSL VPNs» — вовсе не VPN-соединения. Многие поставщики рекламируют соединение как «SSL VPN», хотя в действительности оно не является VPN-соединением IP-уровня. Напротив, разработчики предоставляют специфичные для приложения шлюзы, туннелирующие их протоколы в заголовки SSL (HTTPS). Затем шлюз приложения пересылает соединения на сервер корпоративной сети. Примерами таких «SSL VPNs» могут служить соединения OWA и RPC поверх HTTP, хотя корпорация Microsoft не объявляет эти сервисы как «SSL VPNs». С другой стороны, существуют сетевые VPN-соедиенения по протоколу SSL, которые туннелируют PPP-протокол поверх SSL-протокола (PPP over SSL). Этим реализациям также присущи проблемы, но об этом в другое время и в другом месте.

Аппаратные брандмауэры не имеют возможности проверять содержимое SSL-туннеля и блокировать доступ к протоколам приложений, скрытым внутри туннеля, а брандмауэр ISA лишен ограничений, присущих архитектуре аппаратных брандмауэров. Он обладает функциональными возможностями, большими, чем простая отслеживающая состояние соединений фильтрация; брандмауэр ISA способен разорвать открытый зашифрованный SSL-туннель, выполнить глубокую, отслеживающую состояние соединений на уровне приложений проверку содержимого, а затем заново зашифровать сообщение и переслать его на сайт в корпоративной сети.

Таким образом, брандмауэр ISA обеспечивает более высокий уровень безопасности, чем традиционный аппаратный брандмауэр с отслеживающей состояние соединений фильтрацией. Сегодня атаки ведутся на уровне приложений и направлены против серверов и сервисов корпоративной сети, управляющих бизнесом.

Нельзя сказать, что у администратора брандмауэра ISA — легкая жизнь. В то время как функциональная возможность брандмауэра ISA, именуемая SSL-сопряжением, позволяет ему обеспечивать для *входящих* SSL-соединений уровень безопасности на порядок выше, чем у аппаратных брандмауэров, нам все еще приходится беспокоиться о SSL-туннелированных приложениях, посылаемых из корпоративной сети на интернет-сайты.

Брандмауэр ISA выполняет входящее SSL-сопряжение и отслеживающую состояние соединений проверку на уровне приложений, но не обеспечивает исходящее SSL-сопряжение, необходимое для борьбы со злонамеренными программами, содержащимися в исходящих SSL-туннелях. Как только исходящее SSL-сопряжение

станет доступно, мы сможем помешать внутренним пользователям прятать HTTP-туннелированные приложения в зашифрованных SSL-каналах.

Наш совет — будьте очень осторожны с VPN-соединениями по протоколу SSL и любым другим приложением, прячущим природу соединения внутри зашифрованного SSL-канала. Брандмауэр ISA может запретить или разрешить эти приложения, если их необходимо обработать с помощью правила публикации Web-сервера, но бессилен при их обработке правилом доступа. Жизненно важно помнить об этом при создании политик брандмауэра.

Убедитесь, действительно ли пользователям необходим исходящий доступ к SSL-сайтам. Если да, то следует строго ограничить количество сайтов, с которыми они могут устанавливать SSL-соединение. В противном случае пользователи смогли бы распространить полученное разрешение на туннелирование любого протокола внутри SSL-канала, а вы *совсем не хотите* этого.

ПРЕДУПРЕЖДЕНИЕ Убедитесь, что все пользователи сети и те, кто подключается к ресурсам через брандмауэр ISA, осведомлены о том, что коммуникации через зашифрованный туннель отслеживаются (в настоящее время только входящие соединения, использующие SSL-сопряжения). Пользователи должны подтвердить согласие с этой политикой, а эта политика должна быть проверена и одобрена корпоративными юридическими отделами. Наконец, необходимо делать все возможное для предотвращения применения пользователями зашифрованных SSL-туннелей. Оказывается, подавляющее большинство зашифрованных SSL-соединений, выполняемых через брандмауэр **ISA,** предназначены вовсе не для деловых целей.

Транслятор ссылок ISA Server

Трансляция ссылок решает ряд проблем, которые могут возникнуть у внешних пользователей, соединяющихся через брандмауэр ISA с внутренним Web-сайтом.

Транслятор ссылок (Link Translator) брандмауэра ISA реализован как Web-фильтр брандмауэра ISA. Функциональные возможности встроенного транслятора ссылок, а также наличие встроенного установленного по умолчанию словаря позволяют использовать его сразу после установки брандмауэра для решения общих проблем, встречающихся в сценариях публикации Web-серверов, основанных на средствах прокси.

Например, если страницы внутреннего Web-сайта содержат абсолютные URL-адреса, указывающие сами на себя, транслятор ссылок вернет внешнему пользователю подходящие ссылки, даже если в этих URL-адресах содержатся префиксы http://, а внешний пользователь соединялся с Web-сайтом с помощью префикса https://.

Установленный по умолчанию словарь транслятора ссылок может также должным образом преобразовывать запросы к нестандартным портам. Например, если пользователи подключаются к Web-сайту, опубликованному на нестандартном порте,

такому как **http://www.msfirewall.org:8181,** трансляция ссылок включит номер порта в URL-адреса, посылаемые обратно внешнему клиенту.

Словарь трансляции ссылок создается автоматически, когда включается трансляция ссылок в правиле публикации Web-сервера. В большинстве случаев не придется включать дополнения в словарь, установленный по умолчанию.

Этот словарь содержит следующие компоненты.

- Любое появление на Web-сайте имени компьютера, заданного на вкладке To (К) в свойствах правила публикации Web-сервера, заменяется именем Web-сайта (или IP-адресом). Например, если правило перенаправляет все запросы *к* http://www.microsoft.com на внутренний компьютерс именем SERVER 1 (или 192.168.1.1), все вхождения http://SERVERl на странице ответа, возвращаемой клиенту, заменяются адресом http://www. microsoft .com.
- Если на Web-приемнике задан нестандартный порт, он используется при замене ссылок на странице ответа. Если задан стандартный порт, он удаляется при замене ссылок на странице ответа. Например, если Web-приемник ожидает ответ на TCP-порт 88, ответы, возвращаемые клиенту, будут содержать ссылку на TCP-порт 88.
- Если клиент задает протокол HTTPS (HyperText Transmission Protocol, Secure, протокол защищенной передачи гипертекстов) в запросе к брандмауэру ISA, брандмауэр заменит все вхождения HTTP-протокола на HTTPS.

Предположим, что брандмауэр ISA публикует сайт, размещенный на машине с внутренним именем SERVER1. Брандмауэр ISA публикует сайт, используя общедоступное имя www.msfirewall.orgdocs. Затем внешний Web-клиент делает следующий запрос

```
GET /docs HTTP/1.1 Host:
www.insfirewall.org
```

Обратите внимание, что имя каталога не завершается слэшем (/). Когда сервер, на котором запущен Internet Information Services (IIS, информационный сервис Интернета), получает этот запрос, он автоматически возвращает ответ 302 с заголовком местонахождения http: //SERVERl /docs/, в котором за именем сервера следует имя каталога и затем завершающий слэш.

Затем транслятор ссылок преобразует заголовок ответа в значение http://www.msfirewall.org/docs/.

В данном примере следующие элементы автоматически добавляются в словарь трансляции ссылок:

- http://SERVERl отображается в http://www.msfirewall.org;
- http://SERVERl:80 отображается в http://www.msfirewall.org;
- https://SERVER l отображается в https://www.msfirewall.org;
- https://SERVERl:443 отображается в https://www.msfirewall.org.

Из соображений безопасности, если начальный запрос послан по SSL-протоколу, все ссылки на один и тот же Web-сервер преобразуются в SSL. Следующие элементы автоматически включаются в словарь трансляции ссылок:

- http://SERVERl отображается в https://www. msfirewall.org;
- http://SERVERl:80 отображается в https://www.msfirewall.org;
- https://SERVERl отображается в https://www. msfirewall.org;
- https://SERVER l:443 отображается в https://www.msfirewall.org.

Если опубликованный Web-сайт использует нестандартные HTTP- и SSL-порты (например, для HTTP-протокола 88, а для SSL-протокола 488), ссылки, содержащие эти номера портов, также будут транслироваться. Например,

- http://SERVERl:88 отображается в http://www.msfirewall.org;
- https://SERVERl:488 отображается в https://www.msfirewall.org.

Аналогично, если брандмауэр ISA публикует сайт, использующий Web-приемник, настроенный на нестандартные порты (например, 85 для HTTP-протокола и 885 для SSL-протокола), ссылки будут транслироваться на опубликованные порты:

- http://SERVERl отображается в http://www.msfirewall.org:85;
- http://SERVERl:80 отображается в http://www.msfirewall.org:85;
- https://SERVERl отображается в https://www.msfirewall.org:885;
- https://SERVERl:443 отображается в https://www.msfirewall.org:885.

ПРИМЕЧАНИЕ Не заканчивайте строку в словаре трансляции ссылок завершающим символом. Например, используйте http://SERVER1, а не http://SERVER1/.

Включая элемент с именем сайта, также включайте элемент с именем сайта и портом. Например, если вы добавляете в словарь трансляции ссылок строку поиска http://SERVER1, также добавьте строку поиска http://SERVER1:80. Применяйте и http://, и https://.

С осторожностью меняйте структуры словаря, поскольку это повлияет на установочные параметры словаря трансляции ссылок. Словари с большим числом элементов, применяемые к Web-сайтам с многочисленными ссылками, требующими трансляции, могут ощутимо повлиять на производительность ISA Server.

Несмотря на то, что установленный по умолчанию словарь эффективен для большинства простых сценариев публикации Web-сервера, появляются некоторые трудности, когда публикуются более сложные Web-сайты. В случае более сложных сценариев публикации Web-сервера или при включении кода ASP (Active Server pages, активные серверные страницы, например, в сервисах SharePoint — система управления и совместного использования документов) необходимо конфигурировать элементы словаря, отображающие имена, возвращаемые внутренним Web-сайтом.

Транслятор ссылок проверяет заголовок Content-type (тип содержимого) ответа для того, чтобы определить, не нужна ли трансляция ссылок в теле сообщения. Установки по умолчанию позволяют выполнять трансляцию ссылок только в МШЕ-типах (многоцелевые расширения электронной почты), принадлежащих группе содержимого или контента HTML-документов. Транслятор ссылок брандмауэра ISA сначала ищет заголовок Content-type для определения необходимости трансляции. Если этот заголовок отсутствует, фильтр будет искать заголовок Content-location (местонахождение содержимого) для того, чтобы выполнить трансляцию. Если такого заголовка нет, фильтр будет просматривать расширения файлов.

Транслятор ссылок отображает текстовые строки в соответствии со следующими правилами.

- Транслятор ссылок ищет самые длинные строки, затем более короткие и, в конце, строки по умолчанию.
- Если транслятор ссылок находит совпадающую текстовую строку, он проверяет следующий символ справа от нее, чтобы выяснить, *завершающий* ли это символ. Завершающими символами считаются следующие символы:

  \t *V* \n ; " < ! " & ') $) *
  + , - / > = ? [\ ] " < | }

- Если транслятор ссылок находит завершающий символ непосредственно сле дом за строкой, он выполняет трансляцию этой строки.

Например, рассмотрим сценарий, в котором словарь трансляции ссылок настроен на замену строки «sps» строкой «extranet.external.net» и страница ответа, возвращаемая Web-сервером, включает жестко закодированную ссылку на http://Sps/SpsE)ocs/. Транслятор ссылок преобразует эту строку в строку http://extranet.externai.net/SpsDocs/. Однако, если страница ответа содержит ссылку на http://sps/sps-isa/, *оба* вхождения строки «sps» должны транслироваться, поскольку за каждым из них следует завершающий символ, в результате внешнему клиенту посылается ссылка на http://extranet.external.net/extranet.external.net-isa/.

Из-за описанных возможных проблем трансляции очень важно понимать, как отображаются ссылки при трансляции, чтобы избежать подобных ситуаций в пользовательских словарях транслятора ссылок.

Определение собственных элементов словаря

Следует протестировать поведение транслятора ссылок, чтобы выяснить, не нужны ли свои собственные элементы словаря. Сервер SharePoint Portal Services предоставляет разнообразную тестовую нагрузку для проверки транслятора ссылок. Начните тест с соединения с опубликованным сайтом SharePoint, используя внешний клиент и тестируя функциональные возможности опубликованного сайта. Следует искать ссылки, указывающие на имена внутреннего сервера, и ссылки, использующие неверный префикс (например, http вместо https).

Учтите, что некоторые ссылки будут включены в сценарии на стороне клиента, возвращаемые обозревателю для обработки. Следовательно, необходимо просмотреть исходный HTML-код, а не визуализированный в Web-обозревателе HTML-документ.

В случае опубликованного сайта SharePoint, возможно, понадобится включение в словарь собственных элементов. Например, несмотря на то, что включен транслятор ссылок, функция поиска на сайте SharePoint может вернуть результаты, содержащие и неверный префикс (http вместо https), и имена внутренних серверов.

Кроме того, после вставки собственных элементов словаря для устранения указанных проблем, исходный код страницы с результатами поиска содержит код на языке JavaScript, включающий ссылки на неверный префикс, вызывающие ошибки, которые возвращаются обозревателю при попытке выполнения дополнительного поиска со страницы с результатами поиска.

Например, после вставки двух элементов словаря для замены строки «http://» на строку «https://» и строки «sps» на строку “extranet.external.net>> возвращенный исходный код на клиентской стороне содержит следующие строки на языке JavaScript:

```
f.action='http: \/\/extranet.external.net\/Search¡aspx',     and
http:\\\/\\\/extranet. external. net\\\/Search.aspx
```

Для устранения этой проблемы необходимо явно отобразить более короткую строку. Важно включить двоеточие (:) в элемен т словаря. Просто отображение «http» в «https» вызовет полную недоступность сайта.

Теперь должно быть ясно, что выявление корректных собственных элементов словаря должно включать разнообразное и многократное тестирование. Некорректные отображения ссылок трансляции могут сделать Web-сайт недоступным для внешних клиентов, поэтому мы настоятельно рекомендуем тестировать конфигурации в вашей тестовой лаборатории, прежде чем применять трансляцию ссылок в рабочей среде.

Конфигурирование собственных элементов словаря трансляции ссылок

Собственные словари трансляции ссылок конфигурируются для отдельного правила. Помните о том, что трансляция ссылок выполняется только для ссылок, возвращаемых Web-серверами, опубликованными с помощью правил публикации Web-серверов: не следует настраивать трансляцию ссылок для исходящих запросов к Web-серверам в Интернете.

Для конфигурирования трансляции ссылок выполните следующие шаги.

1. Щелкните правой кнопкой мыши правило публикации Web-сервера и левой кнопкой мыши команду **Properties** (Свойства).
2. В диалоговом окне **Properties** (Свойства) правила публикации Web-сервера щелкните кнопкой мыши вкладку **Link Translation** (Трансляция ссылок).

3. На вкладке **Link Translation** (Трансляция ссылок) установите флажок **Replace absolute links in Web pages** (Заменить абсолютные ссылки на Web-страницах). Щелкните мышью кнопку **Add** (Добавить).
4. В диалоговом окне **Add/Edit Dictionary Item** (Добавить/Отредактировать элемент словаря) введите в текстовое поле **Replace this text** (Заменять данный текст) строку, которую вы хотите заменять в возвращаемых ссылках. Введите замещающую строку в текстовое поле **With this text** (Указанным текстом). Щелкните мышью кнопку OK (рис. 10.35).

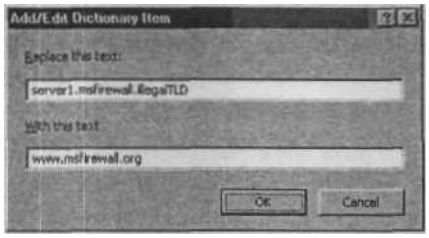


Рис. 10.35. Диалоговое окно **Add/Edit Dictionary Item** (Добавить/отредактировать элемент словаря)

5. Элемент словаря появится в списке элементов словаря. Щелкните мышью кнопку **Content Types** (Типы содержимого) (рис. 10.36).

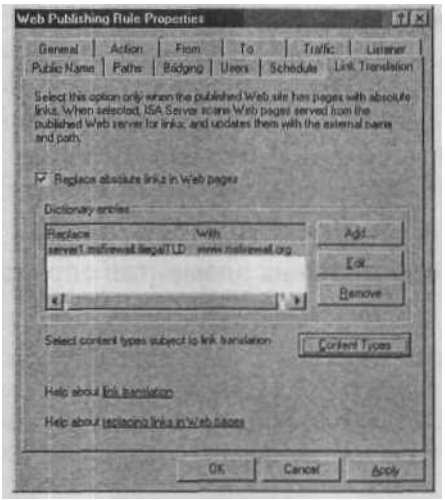


Рис. 10.36. Вкладка Link Translation (Трансляция ссылок) в окне **Web Publishing Rule Properties** (Свойства правила публикации Web-сервера)

6. В диалоговом окне **Link Translation** (Трансляция ссылок) выберите типы содержимого, к которым вы хотите применить трансляцию ссылок. По умолчанию выбран только тип **HTML Documents** (HTML-документы). Выбор будет глобальным, т. е. применяться ко всем правилам публикации Web-серверов.

Несмотря на это, можно создать собственные словари для каждого правила публикации Web-сервера, а типы содержимого будут общими для всех словарей.

ПРЕДУПРЕЖДЕНИЕ В правиле публикации Web-сервера должно быть явно приведено полностью определенное имя домена (fully qualified domain name, FQDN) или IP-адрес для того, чтобы выполнить трансляцию ссылок. Если конфигурируется правило публикации Web-сервера для перенаправления всех входящих соединений на приемник, то появится диалоговое окно ошибки, информирующее о том, что на вкладке Public (Общедоступные) диалогового окна **Properties** (Свойства) правила публикации Web-сервера необходимо использовать явное, полностью определенное имя домена или IP-адрес.

Фильтр Web-прокси

Фильтр Web-прокси позволяет перенаправлять в кэш брандмауэра ISA или на компоненты Web-прокси соединения от хостов, не конфигурированных как клиенты Web-прокси. Если требуется, чтобы только хосты, настроенные явно как клиенты Web-прокси, использовали функциональные возможности Web-прокси брандмауэра ISA, можно отсоединить фильтр Web-прокси, сбросив флажок **Web Proxy Filter** (Фильтр Web-прокси).

ПРЕДУПРЕЖДЕНИЕ Имейте в виду, что отключение HTTP-фильтра для HTTP-протокола — глобальная установка, действующая на все правила, использующие HTTP-фильтр. Несмотря на то, что он остается активным для клиентов Web-прокси, конфигурационный интерфейс HTTP-фильтра удаляется и невозможно настроить HTTP-политику для клиентов Web-прокси. Эта проблема может быть решена в будущем, и мы опубликуем необходимую информацию на сайте www.isaserver.org, как только найдем решение этой проблемы (рис. 10.37).

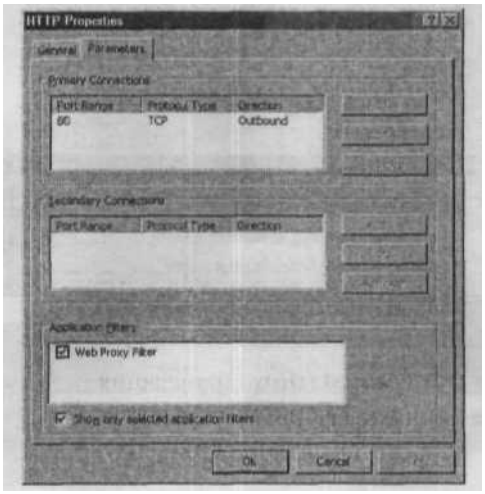


Рис. 10.37. Диалоговое окно HTTP Properties

Фильтр SecurID

Фильтр SecurID служит связующим звеном для аутентификации SecurID (система двухфакторной аутентификации) на брандмауэре ISA. Интерфейс конфигурации фильтра SecurID доступен в диалоговом окне свойств аутентификации Web-приемника. На рис. 10.38 и 10.39 показаны конфигурационные интерфейсы.

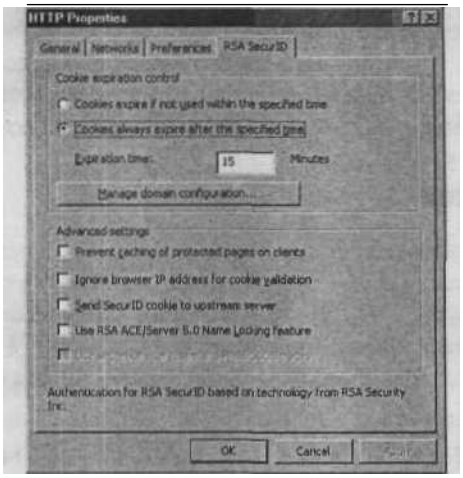


Рис. 10.38. Диалоговое окно **HTTP Properties** и вкладка **RSA SecurID**

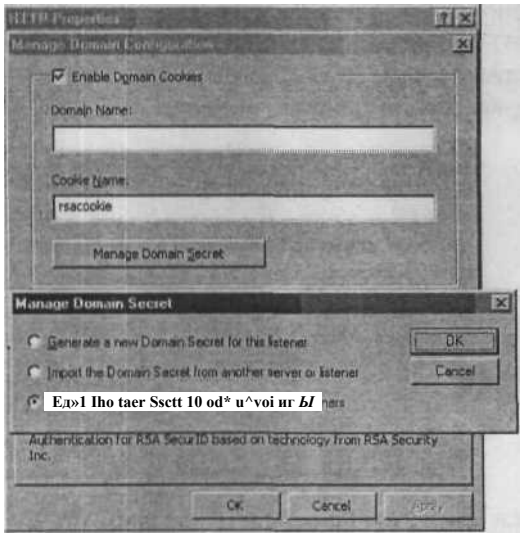


Рис. 10.39. Диалоговое окно **Manage Domain Configuration**

OWA-фильтр аутентификации, основанной на формах

OWA-фильтр аутентификации, основанной на формах, служит связующим звеном для подтверждения подлинности с помощью форм на Web-сайтах OWA (Outlook Web Access, Web-доступ посредством Outlook), доступность которых задается в правилах публикации Web-сервера брандмауэра ISA. На рис. 10.40 показан интерфейс конфигурации для OWA-фильтра, основанной на формах аутентификации, доступный в диалоговом окне аутентификации для Web-приемника.

Более подробную информацию об OWA-фильтре аутентификации, основанной на формах, можно найти в главе 8.

ПРЕДУПРЕЖДЕНИЕ По умолчанию вы не можете использовать аутентификацию брандмауэра ISA, основанную на формах, совместно с RADIUS-аутентификацией. Однако во время написания книги появилось обновление, позволяющее это делать. Посмотрите статью «You cannot use the RADIUS authentication protocol when you use the Outlook Web Access (OWA) Forms-Based Authentication on a Web publishing rule to publish an internal Web site such as OWA in ISA Server 2004» (Вы не можете использовать протокол RADIUS-аутентификации при применении аутентификации Web-доступа посредством Outlook, основанной на формах в правиле публикации Web-сервера для публикации внутреннего Web-сайта, такого как OWA на ISA Server 2004), http://support. microsoft, com/default. aspx?scid=kb;en-us;884560.

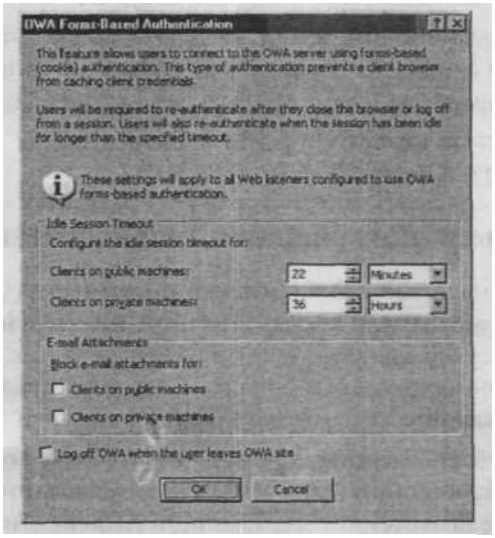


Рис. 10.40. Диалоговое окно OWA Forms-Based Authentication (OWA аутентификация, основанная на формах)

Фильтр RADIUS-аутентификации

Фильтр RADIUS-аутентификации (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя) служит связующим звеном для RADIUS-аутентификации клиентов Web-прокси и внешних хостов, соединяющихся с Web-сайтами, опубликованными с помощью правил публикации Web-серверов.

Фильтр RADIUS применяется Web-приемниками, если приемники настроены на использование RADIUS-аутентификации. Несмотря на то, что фильтр RADIUS предоставляет возможность подтверждения подлинности в любом RADIUS-совместимом каталоге (включая Active Directory), придется применять только RADIUS-аутентификацию на приемнике, настроенном на этот метод подтверждения подлинности. Используя другие методы аутентификации, такие как базовая или интегрированная аутентификация, можно поддерживать многочисленные протоколы аутентификации на одном Web-приемнике.

Для получения более подробной информации об использовании фильтра RADIUS и его конфигурировании для прямых и обратных сценариев Web-прокси обратитесь к главам 6 и 8.

IP-фильтрация и обнаружение/предупреждение вторжения

Брандмауэр ISA выполняет обнаружение и предотвращение вторжений. В этом разделе мы рассмотрим следующие типы обнаружения и предотвращения вторжений:

- обнаружение и предотвращение типовых атак (Common Attacks);
- обнаружение и предотвращение DNS-атак;
- IP-параметры и фильтрация IP-фрагментов.

Обнаружение и предотвращение типовых атак

Получить доступ к диалоговому окну **Intrusion Detection** (Обнаружение вторжения) можно, открыв консоль управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет 2004), раскрыв окно, связанное с именем сервера, а затем раскрыв узел **Configuration** (Конфигурация). Щелкните кнопкой узел **General** (Общие).

В узле **General** (Общие) щелкните кнопкой мыши ссылку Enable **Intrusion Detection and DNS Attack Detection** (Включить обнаружение вторжения и обнаружение DNS-атак). На экране появится вкладка **Common Attacks** (Типовые атаки).

На вкладке **Common Attacks** (Типовые атаки) установите флажок **Enable intrusion detection** (Включить обнаружение вторжения). Установите флажки, расположенные слева от тех типов атак, которые необходимо предотвращать. Если вклю-

чается атака типа **Port scan** (Сканирование портов), введите значения в поля **Detect after attacks ... well-known ports** (Обнаруживать после атак на ... популярных портов) и **Detect after attacks on ... ports** (Обнаруживать после атак на ... портов) (рис. 10.41).

Можно отключить регистрацию пакетов, отвергнутых фильтром обнаружения вторжения, сбросив флажок **Log dropped packets** (Регистрировать отвергнутые пакеты).

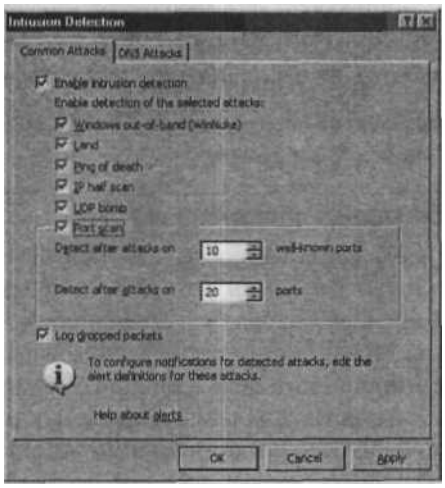


Рис. 10.41. Вкладка Common Attacks (Типовые атаки)

Атаки отказов от обслуживания

Атаки отказов от обслуживания (Denial-of-service, DoS-атака) особенно популярны у интернет-хакеров, стремящихся нарушить сетевые операции. Хотя эти атаки не разрушают и не крадут данные, как делают некоторые атаки других типов, цель злоумышленника, запускающего атаку DoS, вывести сеть из строя и вызвать отказ от обслуживания ее законных пользователей. Атаки отказов от обслуживания легко инициировать, программное обеспечение готово и доступно на Web-сайтах хакеров и в группах новостей краденого программного обеспечения (warez newsgroups), что позволяет любому человеку, имеющему небольшой технический навык или вообще не имеющему таковых, запустить DoS-атаку.

ПРИМЕЧАНИЕ *Warez* — термин, применяемый хакерами и «взломщиками» (crackers) для описания контрабандного (bootlegged) программного обеспечения, которое было «взломано», т. е. в котором была удалена защита от копирования, и стало доступным в Интернете, или в более широком смысле для обозначения любого незаконно распространяемого программного обеспечения.

В феврале 2000 г. массовые DoS-атаки парализовали работу самых крупных сайтов, включая Yahoo.com и Buy.com.

Цель DoS-атаки — сделать сеть недоступной за счет типа или объема сетевого трафика, который приведет к аварийному сбою серверов, переполнению маршрутизаторов или в противном случае нарушит нормальную работу сетевых устройств. Отказ от обслуживания достигается связыванием сетевых ресурсов, например за счет переполнения CPU (центрального процессора) или объема памяти. В других случаях определенный пользователь/компьютер может стать объектом DoS-атак, «подвешивающих» компьютер и требующих его перезагрузки.

ПРИМЕЧАНИЕ В сообществе компьютерной безопасности DoS-атаки иногда называют атаками «nuke» (ядерными).

Распределенная атака отказа от обслуживания

Распределенные атаки отказов от обслуживания (DDoS) используют промежуточные компьютеры, называемые *агентами,* на которых предварительно тайно установлены программы, именуемые *зомби.* Злоумышленник удаленно активизирует программы-зомби, вызывая на промежуточных компьютерах (которых может быть сотни и даже тысячи) одновременный запуск действительной атаки. Поскольку атака приходит с компьютеров, выполняющих программы-зомби и расположенных в сетях по всему миру, хакер способен скрыть истинный источник атаки.

К средствам распределенных атак отказов от обслуживания относятся TFN (Tribe FloodNet), TFN2K, Trinoo и Stacheldraht (German for «barbed wire» — «колючая проволока»). В то время как ранние версии этих средств поражали операционные системы UNIX и Solaris, программа TFN2K уже может выполняться как в ОС UNIX, так н в Windows.

Поскольку распределенные DoS-атаки очень популярны, разрабатывается множество средств, помогающих обнаруживать, удалять и анализировать программное обеспечение для распределенных атак отказов от обслуживания, которые можно установить в вашей сети. Национальный центр защиты инфраструктуры (National Infrastructure Protection Center) недавно анонсировал одно такое средство для обнаружения некоторых типов программ распределенных DoS-атак в некоторых системах. Более подробную информацию о нем можно найти по адресу www.fbi.gov/nipc/trinoo.htm.

ПРИМЕЧАНИЕ Отличная статья, описывающая подробности работы программ TFN, TFN2K, Trinoo и Stacheldraht и озаглавленная «Distributed Denial of Service Attacks» (Распределенные атаки отказов от обслуживания), доступна на Web-сайте NetworkMagazine.com по адресу www.networkmagazine.com/article/NMG20000512S0041.

Важно отметить, что распределенные атаки отказов от обслуживания можно трактовать двояко. Сеть может быть целью DoS-атаки, вызывающей сбои в работе

серверов и нарушающей входящий и исходящий трафик, и компьютеры сети могут использоваться как «невинные посредники» (innocent middlemen) для запуска DoS-атаки, направленной против другой сети или сайта.

SYN-aTaKa/LAND-атака

SYN-атаки используют «трехстороннее квитирование» («three-way handshake») по TCP-протоколу — процесс, с помощью которого сеанс связи устанавливается между двумя компьютерами. Поскольку TCP-протокол (в отличие от UDP-протокола) ориентирован на соединение, сеанс или прямой канал связи один-к-одному устанавливается прежде, чем посылаются данные. Компьютер клиента инициирует соединение с сервером (компьютер, к ресурсам которого он хочет получить доступ).

Квитирование включает следующие шаги.

1. Компьютер клиента посылает сегмент SYN (запрос синхронизации).
2. Сервер отправляет сообщение ACK (acknowledge, подтверждение), подтверждающее получение запроса с машины клиента, отправленного на шаге 1, и SYN, свой собственный запрос синхронизации. Компьютеры клиента и сервера должны синхронизировать номера последовательности друг друга.
3. Клиент отправляет сообщение ACK обратно серверу, подтверждая получение запроса сервера на синхронизацию. Когда оба компьютера подтвердили запросы друг друга, рукопожатие успешно завершается и между ними устанавливается соединение.

На рис. 10.42 показан этот процесс.

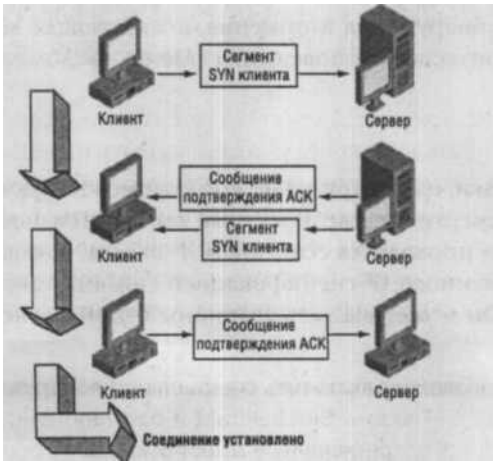


Рис. 10.42. Использование TC P-протоколом трехстороннего квитирования для установки соединения между клиентом и сервером

Было приведено описание нормального течения процесса. SYN-атака использует его для лавинной загрузки выбранной в качестве жертвы атаки системы многочисленными пакетами синхронизации, имеющими неверные IP-адреса источников, которые заставляют систему отвечать с помощью сообщений SYN/ACK. Проблема возникает, когда система, ожидающая сообщение ACK от клиента, обычно приходящее в ответ на ее сообщение SYN/ACK, помещает ожидаемые сообщения SYN/ACK в очередь. Дело в том, что очередь может хранить ограниченное число таких сообщений. Когда она заполнена, все последующие приходящие пакеты SYN будут игнорироваться. Для удаления сообщения SYN/ACK из очереди необходимо, чтобы вернулось сообщение ACK от клиента или было превышено допустимое время ожидания и завершился процесс трехстороннего квитирования.

Поскольку исходные IP-адреса пакетов SYN, посланных злоумышленником, неверны, сообщения ACK, ожидаемые сервером, никогда не придут. Очередь остается заполненной, и нет места для обработки корректных запросов синхронизации. Таким образом, законным пользователям, пытающимся установить соединения с сервером, будет отказано в обслуживании.

LAND-атака (атака с обратной адресацией) — это разновидность SYN-атаки. В LAND-атаке вместо отправки пакетов синхронизации с несуществующими IP-адресами вся лавина пакетов посылается на один ложный IP-адрес подтверждения (spoof IP address), совпадающий с адресом атакуемого компьютера.

LAND-атака может быть предотвращена за счет отфильтровывания входящих пакетов, в которых IP-адреса источника совпадают с адресами компьютеров внутренней сети. У брандмауэра ISA Server есть заранее установленная функциональная возможность обнаружения вторжения, позволяющая выявить попытки LAND-атак и настроить сигнальные оповещения (Alerts), уведомляющие об обнаружении такой атаки.

Ping of Death

Другой тип DoS-атаки, на обнаружение которой можно настроить ISA Server, — так называемый «Ping смерти» (также известный как «пингование большими пакетами»). Атака «Ping смерти» проводится созданием IP-пакета, большего чем 65 536 байтов, максимума, разрешенного IP-спецификацией (иногда такой пакет называют «пакетом-убийцей»). Он может вызвать аварийный сбой, зависание или перезагрузку системы.

Брандмауэр ISA позволяет включить специальное обнаружение атак «Ping смерти».

Teardrop

Атака Teardrop действует несколько иначе, чем «Ping смерти», но с теми же результатами. Программа Teardrop создает IP-фрагменты, части IP-пакета, на которые он может делиться, путешествуя по Интернету. Проблема заключается в том, что поля смещения (offset fields) в этих фрагментах, которые должны отображать величину

порции исходного пакета (в байтах), содержащейся в фрагменте, накладываются друг на друга.

Например, поля смещения двух фрагментов могут быть следующими:

```
Fragment 1: (offset) 100 - 300
Fragment 2: (offset) 301 - 600
```

Это означает, что в первом фрагменте содержатся байты исходного пакета с 100-го по ЗОО-й, а во втором фрагменте — с 301-го по 600-й.

Наложение полей смещения приведет к событию, подобному приведенным далее строкам:

```
Fragment 1:  (offset) 100 - 300
Fragment 2:  (offset) 200 - 400
```

Когда компьютер-адресат попытается повторно собрать эти пакеты, он не сможет этого сделать и аварийно завершит работу, зависнет или выполнит перезагрузку.

У этого типа атаки есть следующие варианты:

- NewTear;
- Teardrop2;
- SynDrop;
- Boink.

Все эти программы создают тот или иной сорт наложения фрагментов.

Ping-лавина (ЮМР-лавина)

Ping-лавина (ping flood), или ЮМР-лавина (ICMP flood) (Internet Control Message Protocol, протокол управляющих сообщений в сети Интернет), — средство «связывания» определенной машины клиента. Оно создается за счет отправки злоумышленником большого количества ping-пакетов (ICMP-пакетов эхо-запросов) программному обеспечению интерфейса Winsock или набора телефонного номера. Эти действия мешают компьютеру-клиенту отвечать серверу на запросы ping-активности и в конечном итоге приводят к разрыву соединения по истечении допустимого времени ожидания ответа. Симптомом Ping-переполнения может служить невероятная активность модема, о чем свидетельствуют его сигнальные лампочки. Иногда этот тип атаки называют *ping storm* (ping-шторм).

К ping-шторму относится и *fr'aggie-атака* («осколочная граната»). Используя ложный IP-адрес подтверждения (spoofed IP address), адрес компьютера-жертвы, злоумышленник посылает ping-пакеты в подсеть, заставляя все компьютеры подсети отвечать по ложному адресу подтверждения, и заваливает его сообщениями эхо-ответов.

ПРИМЕЧАНИЕ Во время кризиса в Косово fraggle-атака часто использовалась про-сербски настроенными хакерами против сайтов Соединенных штатов и НАТО для переполнения их и вызова аварийных ситуаций.

Можно применять программы, такие как NetXray, или другое программное обеспечение IP-трассировки для записи и отображения журналов регистрации лавинных пакетов. Брандмауэры могут быть конфигурированы для блокирования ping-пакетов и предотвращения подобных атак.

Smurf-атака

Smurf-атака — это разновидность атаки «brute force» (атаки грубой силой), использующая тот же метод, что и ping-лавина, но направляющая лавину ICMP-пакетов эхо-запросов на маршрутизатор сети. Адресом назначения ping-пакетов в этом случае служит широковещательный адрес сети, вынуждающий маршрутизатор рассылать пакет всем компьютерам сети или ее сегмента. Это может привести к большому объему сетевого трафика, если имеется много компьютеров-хостов, способных создать перегрузку, вызывающую отказ от обслуживания законных пользователей.

ПРИМЕЧАНИЕ Широковещательный адрес обычно в идентификаторе хоста представляется всеми единицами. Это означает, что, например, в сети класса C 192.168.1.0 широковещательный адрес будет 192.168.1.255 (255 в десятичной системе счисления и 1111111 — в двоичной), а идентификатор хоста в сети класса C представляется последним или z-октетом. Сообщение, посланное на широковещательный адрес, немедленно отправляется на все хосты сети.

Самая коварная форма — применение Smurf-атакующим ложного IP-адреса подтверждения получения ping-пакетов. В этом случае и сеть, в которую посланы пакеты, и сеть, которой принадлежит IP-адрес ложного источника будут перегружены трафиком. Сеть, к которой относится адрес ложного источника, будет наводнена ответами на команду ping, когда все хосты, которым послана эта команда, ответят на эхо-запрос эхо-ответом.

Smurf-атаки могут нанести гораздо больший ущерб, чем некоторые другие разновидности DoS-атак, такие как SYN-лавины. Последние воздействуют только на способность других компьютеров устанавливать соединения по TCP-протоколу с атакованным сервером, а Smurf-атака может полностью нарушить работу ISP (провайдер интернет-услуг) на несколько минут или часов. Это объясняется тем, что один злоумышленник может легко отправить 40 или 50 ping-пакетов в секунду даже с помощью медленного модемного соединения. Поскольку каждый запрос пересылается каждому компьютеру в сети-адресате, число ответов в секунду равно от 40 до 50, помноженным на число компьютеров в сети, т. е. может достигать сотен или тысяч. Этих данных достаточно, чтобы перегрузить даже канал T-1.

Один из способов предотвращения Smurf-атаки на сеть как цель широковещательной рассылки — отключение возможности передачи широковещательного трафика на маршрутизатор. Большинство маршрутизаторов позволяют сделать это. Для того чтобы помешать сети стать жертвой, IP-адрес который используется для ложного подтверждения, необходимо конфигурировать брандмауэр для отфильтровывания входящих ping-пакетов.

UDP-бомба, или UDP-шторм

Злоумышленник может применить протокол пользовательских дейтаграмм (User Datagram Protocol, UDP) и один из нескольких сервисов, формирующих эхо-пакеты на адресатах, для создания сетевой перегрузки и отказов от обслуживания за счет генерации лавины UDP-пакетов между двумя системами назначения. Например, генерирующий символы (chargen) UDP-сервис на первом компьютере, служащий тестирующим средством, которое создает последовательность символов для каждого полученного им пакета, посылает пакеты на эхо-сервис UDP другой системы, который формирует эхо-ответ на каждый полученный символ. С помощью этих тестирующих средств бесконечный поток эхо-символов пересылается в обоих направлениях между двумя системами, создавая перегрузку сети. Иногда этот тип атаки называют *штормом UDP-пакетов (UDP packet storm).*

Помимо эхо-порта 7 злоумышленник может использовать порт 17 сервиса quote of the day (quotd) или порт 13 сервиса daytime. Эти сервисы также создают эхо-ответы на получаемые ими пакеты. Символы, сгенерированные UDP-сервисом, поступают на порт 19-

Отключение ненужных UDP-сервисов на каждом компьютере (особенно упомянутых ранее) или применение брандмауэра для отфильтровывания этих портов/сервисов защитит от атаки этого типа.

UDP-атака Snork

Snork-атака подобна UDP-бомбе. В ней применяется UDP-блок, содержащий порт источника 7 (эхо) или 19 (генерация символов) и порт адресата 135 (средства адресации (location service) фирмы Microsoft). Результат аналогичный — лавина ненужных передач, способных снизить производительность или вызвать аварийный сбой вовлеченных систем.

Атака WinNuke (атака Windows Out-of-Band)

Атака передачи срочных данных (out-of-band, OOB), иногда называемая *Windows OOB bug,* использует в своих интересах уязвимость сетей Microsoft. Программа WinNuke (и ее разновидности, такие как Sinnerz и Muerte) выполняет передачу экстренных данных, вызывающих аварийный сбой на компьютере-адресате. Работает она следующим образом: устанавливается соединение TCP/IP с IP-адресом адресата, использующее порт 139 (порт NetBIOS). Затем программа посылает дан-

ные, содержащие в заголовке пакета флаг MSG_OOB (или Urgent). Этот флаг заставляет интерфейс Win sock компьютера посылать данные, называемые экстренными или срочными (out-of-band data, OOB). На приеме Windows-сервер, адресат, ожидает указатель в пакете, ссылающийся на позицию завершения экстренных данных, за которой следуют обычные данные. Однако OOB-указатель в пакете, созданном программой WinNuke, ссылается на блок, за которым нет последующих данных.

Компьютер под управлением ОС Windows не знает, как обработать такую ситуацию и прерывает коммуникации в сети, и все последующие попытки пользователей связаться с ним закончатся отказом от их обслуживания. Атака WinNuke обычно требует перезагрузки атакованной системы для восстановления сетевых коммуникаций.

ОС Windows 95 и NT версий 3.5 1 и 4.0 уязвимы для атаки WinNuke, несмотря на установку исправлений, предоставленных фирмой Microsoft. Операционные системы Windows 98/ME и Windows 2000/2003 не подвержены атакам WinNuke, брандмауэр ISA Server позволяет включить обнаружение попыток атак передачи срочных данных.

Атака Mall Bomb

Атака «почтовая бомба» (mail bomb) — средство переполнения почтового сервера, вызывающее остановку его функционирования и тем самым отказ от обслуживания пользователей. Это относительно простая разновидность атаки, выполняемая с помощью отправки большого массива сообщений электронной почты конкретному пользователю или системе. На хакерских сайтах *в* Интернете есть программы, позволяющие легко запустить почтовую бомбу, автоматически отправляя лавину сообщений электронной почты на заданный адрес и скрывая при этом авторство злоумышленника.

Разновидностью почтовой бомбы может служить программа, автоматически подписывающая компьютер-адресат на сотни и тысячи рассылок интернет-списков огромного объема, которые заполняют почтовый ящик пользователя и/или почтовый сервер. Бомбисты называют этот вид атаки *загрузкой списков рассылки {list linking).* К примерам таких программ относятся почтовые бомбы Unabomber, extreme Mail, Avalanche и Kaboom.

Справиться с повторяющимися почтовыми бомбами поможет блокирование с помощью пакетных фильтров трафика из сети, порождающей атаку. К сожалению, этот способ не годится для загрузки списков рассылки, поскольку адрес-источник скрыт, поток трафика приходит от почтовых рассылок списков, на которые жертва была подписана.

Сканирование и подмена адреса подтверждения

Термин *сканер {scanner)* в контексте сетевой безопасности означает программу, которая используется хакерами для удаленного определения открытых на данной

системе и, следовательно, уязвимых для атаки TCP/UDP-портов. Сканеры также применяются администраторами для выявления слабых мест в их собственных системах и устранения их, прежде чем эти уязвимости обнаружит злоумышленник. Сетевые диагностические средства, такие как известное Security Administrator's Tool for Analyzing Networks (SATAN, Средство автоматизированного контроля безопасности), утилита UNIX, включают развитые функциональные возможности сканирования портов.

Хорошая сканирующая программа может определить местонахождение компьютера-цели в Интернете (одного из уязвимых для атаки), определить, какие TCP/IP-сервисы выполняются на машине, и исследовать слабые места в защите этих сервисов.

ПРИМЕЧАНИЕ Среди хакеров бытует мнение: «Хороший сканер портов стоит тысячи паролей».

Многие сканирующие программы можно найти в Интернете как свободно распространяемое программное обеспечение. Замечательный источник информации об истории сканирования, о методах работы сканеров и некоторых популярных сканирующих программах находится по адресу www.ladysharrow.ndirect.co.uk/Maximum%20Securi ty /scanners.htm.

Сканирование портов

Сканирование портов — это процесс поиска «слушающих» TCP- или UDP-портов на компьютере или маршрутизаторе и получение от слушающих портов максимума сведений об устройстве. TCP- и UDP-сервисы применяют ряд *популярных портов (well-known ports),* которые широко опубликованы. Хакер использует эти сведения о широко используемых портах для экстраполяции информации.

Например, протокол Telnet обычно использует порт 23. Если хакер обнаружит, что этот порт открыт и ожидает запрос, он догадывается, что на машине, возможно, разрешен Telnet. Затем злоумышленник может попытаться проникнуть в систему, например, подобрав подходящий пароль в ходе атаки грубой силой (brute-force).

Обнаружение и предотвращение DNS-атак

DNS-фильтр брандмауэра ISA защищает DNS-серверы, опубликованные брандмауэром ISA с помощью правил публикования сервера (Server Publishing Rules). К странице конфигурирования предотвращения DNS-атак можно получить доступ в диалоговом окне **Intrusion Detection** (Обнаружение вторжения). Раскройте имя сервера, а затем раскройте узел Configuration (Конфигурирование). Щелкните мышью узел **General** (Общие).

На панели **Details** (Дополнительная настройка) щелкните мышью ссылку **Enable Intrusion Detection and DNS Attack Detection** (Включить обнаружение проник-

новения и выявление DNS-атак). В диалоговом окне **Intrusion Detection** (Обнаружение проникновения) щелкните вкладку **DNS Attacks** (DNS-атаки). На вкладке **DNS Attacks** (DNS-атаки) установите флажок **Enable detection and filtering of DNS attacks** (Включить выявление и фильтрацию DNS-атак). Эти действия представлены на рис. 10.43-

После того, как выявление атак включено, можно включить предотвращение и защиту от трех типов атак

- переполнение имен хостов DNS;
- переполнение длины имени DNS;
- подмена зоны DNS.

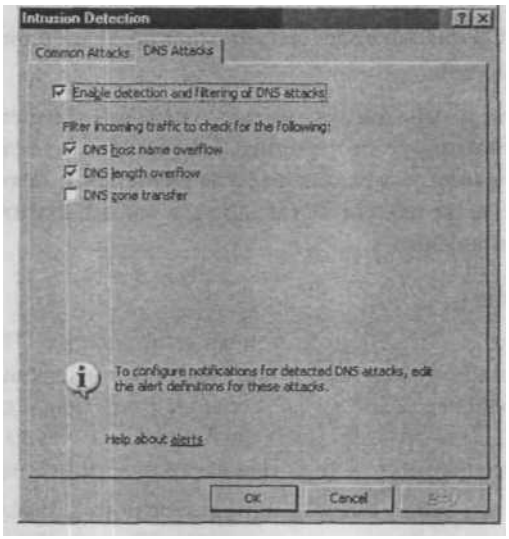


Рис. 10.43. Вкладка **DNS Attacks** (DNS-атаки)

Атаки типа переполнения имен хостов DNS и переполнения имен DNS представляют собой DoS-атаки. DoS-атаки DNS отличаются по размеру от DNS-запроса и от DNS-ответа, в которых вся пропускная способность сети занимается поддельными DNS-запросами. Для увеличения DNS-трафика атакующий использует DNS-серверы в качестве «усилителей».

Атакующий начинает посылать на каждый DNS-сервер небольшие DNS-запросы, которые содержат поддельный IP-адрес потенциальной «жертвы». Ответы, возвращаемые на небольшие запросы, довольно большие, поэтому, если одновременно имеется много возвращаемых ответов, канал связи перегружается и имеет место отказ от обслуживания (DoS-атака).

Одно из решений этой проблемы состоит в том, что администратор должен конфигурировать DNS-серверы так, чтобы они при получении DNS-запроса от подозрительного или неожиданного источника отвечали отрицательным ответом (refused response), который намного меньше, чем ответ утвердительный.

Подробная информация о конфигурировании DNS-серверов, позволяющая разрешить эту проблему, содержится в информационном бюллетене департамента энергетики США Energy Computer Incident Advisory Capability (консультативная служба компьютерных сбоев) за номером J-Об3, который доступен по адресу http://www/ciac.org/ciac/bulletins/j-063.shtml.

Фильтрация IP-параметров и IP-фрагментов

Можно определить IP-параметры, которые может пропускать брандмауэр ISA, и указать, разрешено ли IP-фрагментам проходить через брандмауэр. На рис. 10.44 и 10.45 показаны конфигурационные интерфейсы для фильтрации IP-параметров и фильтрации IP-фрагментов. На рис. 10.46 приведено диалоговое окно, предупреждающее о том, что включение фильтрации фрагментов может создавать помехи для протокола L2TP/IPSec и сервисов потоковых мультимедиа данных.

Более подробную информацию о фильтрации фрагментов можно найти в этой главе при обсуждении типовых атак сетевого уровня.

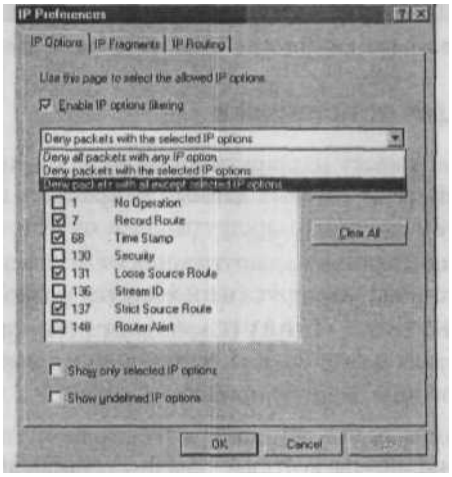


Рис. 10.44. Вкладка **IP Options** (IP-параметры)

Рис. 10.45. Вкладка IP Fragments (IP-фрагменты)

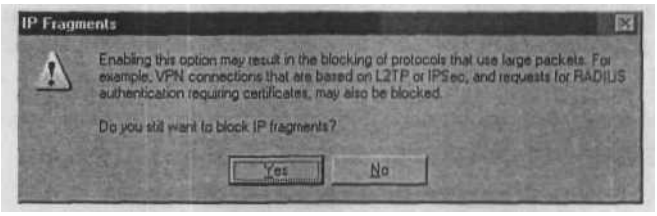


Рис. 10.46. Предупреждающее диалоговое окно фильтра IP-фрагментов

Атака маршрутизации от источника

Протокол TCP/IP поддерживает маршрутизацию от источника *(source routing),* которая позволяет отправителю сетевых данных направлять пакеты через заданную точку в сети. Существуют два типа маршрутизации от источника.

- **Strict source routing** (Строгая маршрутизация от источника) Отправитель дан ных может задать точный маршрут (используется редко).
- **Loose source record route (LSRR)** (Свободная регистрация маршрута от ис точника) Отправитель может указать определенные маршрутизаторы (сетевые сегменты), через которые должен проходить пакет.

Маршрут от источника — это параметр в IP-заголовке, позволяющий отправителю переопределить маршруты, которые обычно устанавливаются маршрутизаторами между отправляющим и принимающим компьютерами. Маршрутизация от источника применяется сетевыми администраторами для отображения сети, диагностической маршрутизации или решения коммуникационных проблем. Она также используется для увеличения трафика по маршруту, обеспечивающему наивысшую производительность. К сожалению, маршрутизацией от источника могут воспользоваться хакеры.

Если в системе разрешена маршрутизация от источника, злоумышленник может использовать ее для того, чтобы узнать внутренние частные адреса в локальной сети (LAN), которые обычно не видны из Интернета, из-за направления трафика через другую машину, которая достижима как из Интернета, так и с компьютера внутренней сети.

Маршрутизацию от источника можно отключить на большинстве маршрутизаторов для предотвращения атаки этого типа. Брандмауэр ISA по умолчанию также блокирует маршрутизацию от источника.

Резюме

В данной главе обсуждался набор параметров фильтрации уровня приложений брандмауэра ISA. Описаны два типа фильтров приложений, используемых брандмауэром ISA: фильтры доступа и фильтры защиты. Несмотря на то, что мы разделили фильтры на указанные два основных типа, нельзя сказать, что фильтры доступа лишены защиты. Оба типа фильтров выставляют требования, в которых указана необходимость соответствия соединений спецификациям законных соединений, использующих соответствующие протоколы.

Заканчивается глава обсуждением механизмов брандмауэра ISA, направленных на обнаружение и предотвращение вторжения. Рассказано о типовых атаках сетевого уровня, которые могут быть запущены против брандмауэра ISA, и применяемых брандмауэром способах защиты от подобных атак.

Краткое резюме по разделам

Фильтры уровня приложений

И Фильтры уровня приложений выполняют динамическую проверку протоколов, отличных от Web.

Ш Для наиболее распространенных протоколов уровня приложений, используемых для выхода в Интернет, существуют фильтры приложений.

Web-фильтры

И Web-фильтры применяются для соединений через брандмауэр ISA no HTTP-, HTTPS- и туннелированному FTP-протоколу. *Ш* В правилах публикации Web-серверов нельзя отключить фильтр Web-прокси.

Обнаружение и предотвращение вторжений

И Брандмауэр ISA автоматически защищает от типовых атак сетевого уровня, используя свои функциональные возможности защиты от вторжения.

И Брандмауэр ISA можно настроить на обнаружение типовых атак **и** оповещение о них. Для этого используется функция обнаружения вторжения.

И Даже если брандмауэр ISA не настроен на обнаружение вторжения, он защищает от проникновения в систему.

И Фильтр DNS защищает опубликованные Web-серверы от типовых злоумышленных переполнений и препятствует выполнению удаленными пользователями зонной передачи с опубликованных DNS-серверов.

И Можно конфигурировать брандмауэр ISA для разрешения определенных IP-параметров, необходимых для диагностики сети, и запрета их в дальнейшем, после завершения диагностики.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Могу ли я использовать аутентификацию, основанную на формах (Forms-based Authentication, FBA), для не OWA-сайтов?

О: Вы можете использовать FBA на любом сайте, опубликованном с помощью правила публикации Web-сервера. Однако некоторые пользователи сообщили о неожиданных результатах, поэтому следует тщательно протестировать эту функциональную возможность прежде, чем использовать ее в рабочей среде для не OWA-сайтов.

В: Могу ли я установить SMTP Message Screener на компьютере с брандмауэром ISA?

Os Да. Компьютер с брандмауэром ISA может быть сконфигурирован как входящий и исходящий SMTP-ретранслятор вашей компании. Кроме того, можно установить SMTP Message Screener на сервере Exchange. Однако мы не рекомендуем устанавливать SMTP Message Screener на машине с сервером Exchange.

В: Удаленные **клиенты** не могут достичь с помощью правила публикации Web-сервера некоторых URL-адресов, возвращаемых моим сайтом SharePoint. Я конфигурировал транслятор ссылок для изменения ссылок, но он, похоже, не делает этого никогда. Как быть с этим?

О: Транслятор ссылок способен надежно изменять ссылки, возвращаемые Web-клиенту сайтом SharePoint, но некоторые ссылки создаются на клиентской машине с помощью сценария клиентской стороны. Поскольку транслятор ссылок брандмауэра ISA предварительно не обрабатывает сценарий клиентской стороны во время трансляции, эти ссылки нарушаются. Мы надеемся на пакет исправле-

ний или новые версии брандмауэра ISA, в которые будет включена улучшенная поддержка публикаций серверов SharePoint и будет решена эта проблема.

В: Наш сотрудник, ответственный за безопасность, не разрешает нам присоединить брандмауэр ISA к домену, хотя и не может привести убедительных доводов в пользу отказа от членства брандмауэра ISA в домене. К сожалению, мы вынуждены подчиняться его политике. Мы предпочли бы использовать аутентификацию, основанную на формах, для публикации OWA, но нам придется применять RADIUS-аутентификацию. Есть ли способ сделать это?

О: Да. Во время написания книги эта дилемма стала частью очередного обновления. Мы надеемся, что это обновление будет включено в состав первого пакета исправлений функций брандмауэра ISA. Для получения более подробной информации посмотрите статью «You cannot use the RADIUS authentication protocol when you use the Outlook Web Access (OWA) Forms-Based Authentication on a Web publishing rule to publish an internal Web site such as OWA in ISA Server 2004» (Вы не можете использовать протокол RADIUS-аутентификации, когда применяете аутентификацию Web-доступа посредством Outlook, основанную на формах, в правиле публикации Web-сервера для публикации внутреннего Web-сайта, такого как OWA на ISA Server 2004), размещенную по адресу http://support.microsoft.com/default.aspx?scid=kb;en-us;884560.

В: Вы не включили в эту главу достаточно информации о фильтре SecurlD и способах его применения. Почему, и как мне получить дополнительные сведения о SecurlD?

О: Мы хотели включить в эту книгу подробную информацию о SecurlD, но, к сожалению, не смогли связаться ни с кем из фирмы RSA для ответов на наши запросы. Как только нам удастся заполучить консультанта в фирме RSA и выяснить все вопросы, мы опубликуем подробную информацию об аутентификации SecurlD на сайте www.isaserver.org.

Bi Фильтр MMS работает как с входящими, так и с исходящими соединениями? Я пытался опубликовать Microsoft Media Server на компьютере под управлением Windows Server 2003 с помощью правила публикации MMS-сервера, но он не работал. Есть ли способ конфигурировать фильтр для поддержки правил публикации MMS-серверов?

О: Фильтр MMS действительно работает, как с входящими, так и с исходящими соединениями. Но ваш сайт, возможно, использует RTSP-протокол вместо MMS-протокола. Попробуйте создать правило публикации, применяющее RTSP-протокол, и посмотрите, решит ли оно вашу проблему.

Глава 11

Повышение скорости доступа в Интернет с помощью функции кэширования ISA Server 2004

Основные темы главы:

Базовые понятия кэширования

Основные возможности Web-кэширования ISA Server 2004

Конфигурирование ISA Server 2004 как сервера кэширования

Уделяя большое внимание безопасности и возможностям брандмауэра или се"евого экрана, легко забыть о второй важной функции ISA Server 2004 — повышении производительности Web-пользователей внутренней и внешней сетей благодаря кэшированию — функции, которую большинство конкурентов на рынке брандмауэров не включает в свои продукты.

«Всемирная паутина» (Web) — жизненно важный компонент современного бизнеса. Сотрудники вашей организации могут обращаться к Web-сайтам в Интернете каждый день для сбора информации по конкретной теме, поиска людей и товаров, знакомства с новостями и т.д. В то же время корпоративный Web-сайт (сайты) может стать одним из лучших способов рекламирования и продвижения на рынке бизнеса и предоставления информации партнерам и клиентам.

В большинстве организаций, подсоединенных к Интернету, Web-трафик постоянно растет. Пользователь зачастую посещает одни и те же сайты регулярно, или многочисленные пользователи в пределах организации посещают одни и те же сайты и просматривают одинаковые страницы. Кроме того, общий сетевой и интернет-трафик устойчиво увеличивается, приближаясь к точке насыщения допустимой пропускной способности Интернета. В этой ситуации кэширование может стать хорошим решением.

> ПРИМЕЧАНИЕ В этой главе мы используем снимки экрана (screenshots), относящиеся к брандмауэру ISA Server 2004 Enterprise Edition. Существуют различия между интерфейсами брандмауэра редакций EE (Enterprise Edition) и SE (Standard Edition) (в основном это касается вкладок и вариантов выбора, существующих в редакции EE, но отсутствующих в редакции SE). Мы будем указывать на эти различия, если интерфейс редакции SE отличается от снимков экрана, относящихся к редакции EE.

Базовые понятия кэширования

Хорошо было бы увеличить пропускную способность Интернета. Некоторые провайдеры интернет-услуг предоставляют пользователям каналы T-1 и T-3 в зависимости от частоты пользования, таким образом, снижая нагрузку и в результате сохраняя ее на нижнем уровне. Даже если организация покупает полосу частот по безлимитному плану, снижение загрузки может повысить производительность работы сетевых пользователей. Существуют два типа кэширования — прямое (forward) и обратное (reverse) — способные принести пользу вашей организации, и в этом разделе мы обсудим их. Серверы кэширования можно развернуть в группах, которые могут быть организованы как структуры двух разных видов, в зависимости от нужд вашей сети.

ПРИМЕЧАНИЕ Если вам знакомы два типа кэширования: *активное* и *пассивное,* пожалуйста, учтите, что, как говорилось в главе 2, ISA Server 2004 больше не поддерживает активное кэширование, хотя в интерфейсе есть параметр для установки этого типа.

В следующих разделах мы рассмотрим различия двух типов Web-кэширования, структуры, используемые для развертывания множественных серверов кэширования и протоколы, применяемые серверами кэширования для взаимодействия друг с другом.

Типы Web-кэширования

Как уже упоминалось, существуют два основных типа Web-кэширования:

- прямое кэширование;
- обратное кэширование.

Брандмауэр ISA Server 2004 поддерживает оба типа, поэтому рассмотрим каждый из них немного подробнее.

Прямое кэширование

Один из способов снижения загрузки полосы пропускания Интернета — сохранение часто запрашиваемых Web-объектов в локальной сети, откуда пользователи внутренней сети могут получить их без выхода на сервер в Интернете. Он называется прямым кэшированием и обладает дополнительным преимуществом, делая доступ для внутренних пользователей более быстрым, поскольку они получают Web-объекты (такие как страницы, графика и звуковые файлы) с помощью быстрого соединения локальной сети, обычно 100 Мбит/сек и больше, взамен более медленного интернет-соединения, возможно, со скоростью 1,5 Мбит/сек.

Прямое кэширование поддерживается всеми серверами Web-кэширования. Этот тип кэширования ускоряет ответ на исходящие запросы при запросе пользователями внутренней сети Web-объекта с сервера в Интернете. Эти часто запрашиваемые объекты хранятся на сервере кэширования, т. е. они могут быть получены с помощью быстрого соединения локальной сети вместо более медленного интернет-соединения.

Прямое кэширование применяется, когда пользователь в сети, защищенной брандмауэром ISA Server 2004, выполняет запрос Web-содержимого (Web-контента). Запрашиваемое содержимое помещается в Web-кэш после того, как первый пользователь выполнил запрос. Следующий (и все остальные) пользователь, запросивший то же содержимое из Интернета, получает его из Web-кэша на машине с брандмауэром ISA Server 2004, а не с Web-сервера из Интернета. Это уменьшает объем трафика интернет-соединений и снижает общие сетевые издержки. Кроме того, содержимое доставляется пользователю из кэша гораздо быстрее, чем с ре-

ального Web-сервера. Это повышает удовлетворенность пользователя и эффективность его работы.

Основное преимущество прямого кэширования, обеспечиваемого ISA Server 2004, — уменьшение расходов за счет снижения потребления полосы пропускания при интернет-соединении.

Обратное кэширование

Обратное кэширование в отличие от прямого уменьшает трафик во внутренней сети и ускоряет доступ внешних пользователей к собственным сайтам компании. Часто запрашиваемые объекты на внутренних Web-серверах кэшируются на границе сети, на прокси-сервере, таким образом, снижая нагрузку на Web-серверы.

> ПРИМЕЧАНИЕ В типовой документации по кэшированию обратные кэши иногда называют «шлюзовыми кэшами» (gateway caches) или «суррогатными кэшами» (surrogate caches).

Обратное кэширование подходит для случая, если ваша организация создает собственные внутренние Web-сайты, доступные внешним интернет- и интранет-пользователям. Сервер кэширования хранит объекты, часто запрашиваемые с серверов внутренней сети (Internal) и обеспечивает обслуживание внешних пользователей. Это ускоряет доступ для внешних пользователей, снижает нагрузку на внутренние Web-серверы и уменьшает трафик во внутренней сети.

Обратное кэширование применяется, когда пользователь Интернета запрашивает Web-содержимое, размещенное на Web-сервере, опубликованном брандмауэром ISA Server 2004 с помощью правила публикации Web-сервера. Брандмауэр ISA извлекает содержимое с Web-сервера во внутренней сети или другой сети, защищенной брандмауэром, и возвращает содержимое интернет-пользователю, запросившему его. Компьютер с брандмауэром ISA Server 2004 кэширует полученное с Web-сервера содержимое во внутренней сети. Когда другие пользователи запрашивают ту же самую информацию, содержимое предоставляется из кэша сервера ISA, а не с исходного Web-сайта.

Сценарий обратного кэширования обладает двумя принципиальными достоинствами:

- обратное кэширование снижает нагрузку на полосу пропускания внутренней сети;
- обратное кэширование сохраняет доступность Web-содержимого при отключенном от сети Web-сервере.

Снижает нагрузки на полосу пропускания обратным кэшированием

Обратное кэширование предоставляет информацию непосредственно с компьютера брандмауэра ISA Server 2004. Полоса частот во внутренней сети не расходуется и таким образом, становится доступной для пользователей внутренней сети.

Корпоративные сети, страдающие от недостаточной пропускной способности, получают выигрыш от данной конфигурации.

Увеличение доступности Web-содержимого обратным кэшированием

У обратного кэширования есть и более привлекательное достоинство: его способность сохранять доступность содержимого Web-сайта при отключенном от сети Web-сервере. Эта способность может стать частью плана обеспечения бесперебойной работы ваших Web-сервисов.

Web-серверы могут перейти в автономный режим по разным причинам, например, если требуется выполнение процедур сопровождения или проверка после сбоев аппаратного или программного обеспечения сервера. Время простоя Web-сервера может иметь вредные последствия, начиная от мелких неудобств и заканчивая серьезными проблемами, для интернет-польз о вате лей, пытающихся получить доступ к информации на сайте. Важное преимущество обратного кэширования сервера ISA Server 2004 — его способность при отключенном от сети Web-сервере сохранять содержимое Web-сайта, доступным для интернет-пользователей, благодаря предоставлению контента из кэша сервера ISA.

Структуры Web-кэширования

Для обеспечения более эффективного кэширования можно использовать несколько серверов Web-кэширования. Существуют две базовые структуры, применяющие несколько совместно работающих серверов кэширования:

- распределенное кэширование (distributed caching);
- иерархическое кэширование (hierarchical caching).

Как следует из названия, распределенное кэширование распределяет, или распространяет, кэшированные Web-объекты между двумя или несколькими серверами кэширования, находящимися на одном уровне в сети. На рис. 11.1 показано функционирование распределенного кэширования.

Иерархическое кэширование действует несколько иначе: серверы кэширования находятся на разных уровнях сети, вышестоящие серверы кэширования взаимодействуют с нижестоящими прокси-серверами. Например, серверы кэширования расположены в каждом филиале. Эти серверы связываются с массивом кэширования в центральном офисе. Запросы обслуживаются сначала из локального кэша, а затем из централизованного кэша, прежде чем отправиться на сервер в Интернете.

Иерархическое кэширование показано на рис. 11.2.

ПРИМЕЧАНИЕ Иерархическое кэширование более эффективно с точки зрения потребления полосы пропускания, а распределенное — с точки зрения затраченного дискового пространства.

Рис. 11.1. Функционирование распределенного кэширования

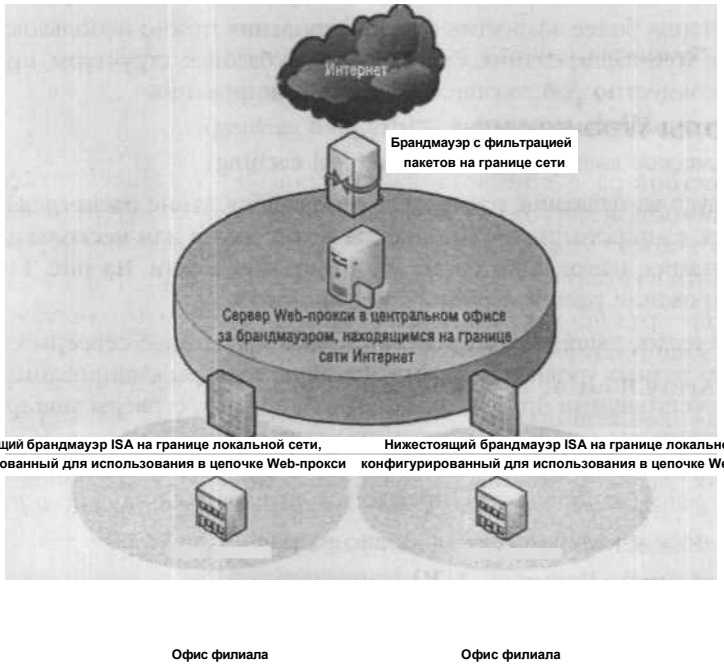


Рис. 11.2. Функционирование иерархического кэширования

И, наконец, можно комбинировать оба метода для создания гибридной структуры кэширования. Подобная комбинация обеспечит наилучший вариант, повысив

производительность и эффективность. Гибридная структура кэширования показана на рис. **11.3.**

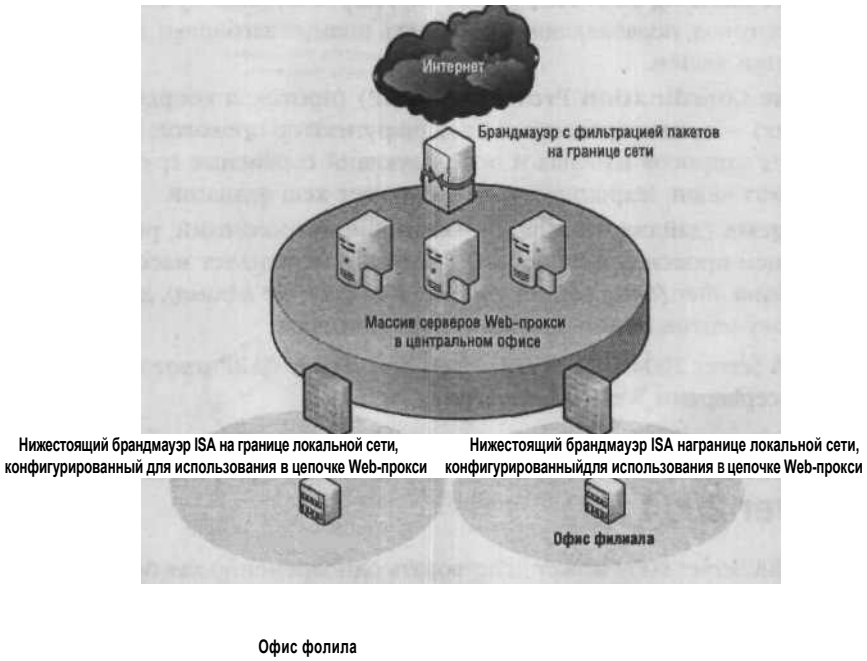


Рис. 11.3. Функционирование гибридной структуры кэширования

Протоколы Web-кэширования

При совместной работе нескольких серверов Web-кэширования им необходим способ взаимосвязи для того, чтобы запрошенный клиентом и ненайденный в кэше сервера Web-объект можно было запросить с других серверов кэширования, прежде чем выходить в Интернет и получать документ оттуда.

Существует ряд протоколов, которые можно применять для связи между серверами Web-кэширования. Наиболее популярны следующие.

- **Cache Array Routing Protocol (CARP)** (протокол маршрутизации между кэш-серверами) — хеш-ориентированный протокол, позволяющий рассматривать прокси-серверы кэширования как единый логический кэш и применять хеш-функцию для определения кэша, на который следует направить запрос. Хеш-функция также может использоваться клиентом Web-прокси для определения местонахождения содержимого в распределенном кэше.
- **Internet Cache Protocol (ICP)** (интернет-протокол кэширования) — ориен тированный на сообщения протокол, определенный в RFC 2186 (Requests for Comments, запросы на комментарии и предложения), который базируется на протоколах UDP/IP и первоначально применялся для иерархического кэширо-

вания в проекте Харвест (Harvest). Этот проект стал основой для Squid, кэширующего прокси для Web-клиентов с открытым исходным кодом.

- **HyperText Caching Protocol (HTCP)** (гипертекстовый протокол кэширования) — протокол, позволяющий применять полные заголовки запроса и ответа в управлении кэшем.
- **Web Cache Coordination Protocol (WCCP)** (протокол координации Web-кэширования) — ориентированный на маршрутизатор протокол, удаляющий распределение запросов из кэша и использующий сервисные группы, к которым принадлежат кэши. Маршрутизатор вычисляет хеш-функции.
- **Cache digests** (дайджесты кэша) — хеш-ориентированный, реализованный в кэширующем прокси Squid протокол, который использует массив битов, называемый *Bloom filter (блюмовский фильтр или фильтр Блюма),* для кодирования резюме документов, хранящихся на каждом прокси.

Сервер ISA Server 2004 Enterprise Edition применяет CARP-протокол для взаимосвязи между серверами Web-кэширования.

Основные возможности Web-кэширования ISA Server 2004

Брандмауэр ISA Server 2004 может действовать одновременно как брандмауэр и как сервер Web-кэширования или как выделенный сервер Web-кэширования. Можно установить ISA Server 2004 как сервер прямого кэширования или как сервер обратного кэширования. Для реализации функциональной возможности кэширования брандмауэр ISA использует фильтр Web-прокси.

> ПРЕДУПРЕЖДЕНИЕ Если настроить ISA Server 2004 только как сервер кэширования, то потеряется большинство функций брандмауэра и придется установить другой брандмауэр для защиты сети.

ISA Server 2004 поддерживает как прямое (для исходящих запросов), так и обратное (для входящих запросов) кэширование. Один и тот же ISA Server может выполнять одновременно оба типа кэширования.

При прямом кэшировании ISA Server располагается между внутренними клиентами и Web-серверами в Интернете. Когда внутренний клиент посылает запрос Web-объекта (Web-страницы, графического или другого Web-файла), он должен пройти через ISA Server. Прежде чем послать запрос за пределы внутренней сети, на Web-сервер в Интернете, ISA Server проверяет свой кэш для того, чтобы выяснить, не размещена ли уже в нем копия запрашиваемого объекта (поскольку кто-то во внутренней сети запросил ранее этот объект с Web-сервера в Интернете).

Если объект находится в кэше, ISA Server посылает его из кэша и нет необходимости отправлять поток данных через Интернет. Извлечение объекта из кэша ISA Server

в локальной сети пройдет гораздо быстрее, чем загрузка его *с* Web-сервера в Интернете, поэтому внутренние пользователи заметят повышение производительности.

Если объекта нет в кэше сервера ISA, он запросит объект с Web-сервера в Интернете. Когда запрос вернется, сервер ISA сохранит объект в кэше для того, чтобы в следующий раз, когда этот объект будет запрашиваться, можно было выполнить этот запрос из кэша.

В случае обратного кэширования ISA Server действует как посредник между внешними пользователями и Web-серверами компании. Когда на Web-сервер компании приходит запрос объекта от пользователя из Интернета, сервер проверяет свой кэш в поисках данного объекта. Если объект найден, ISA Server заменяет собой внутренний Web-сервер и выполняет запрос внешнего клиента, не обращаясь к Web-серверу. Подобные действия снижают трафик во внутренней сети.

В любом случае кэш — это область жесткого диска сервера ISA, которая используется для хранения запрошенных Web-объектов. Можно управлять объемом дискового пространства, отведенного под кэш (и таким образом максимальным размером кэша). Существует возможность управления максимальным размером кэшируемых объектов, для того чтобы несколько очень больших объектов не захватили весь кэш.

Кэширование использует также системную память. Объекты кэшируются в оперативной памяти (RAM) так же, как и на диске. Из оперативной памяти объекты можно извлечь гораздо быстрее, чем с диска. ISA Server 2004 позволяет определить, какой процент памяти с произвольным доступом может быть использован под кэш (по умолчанию ISA Server 2004 использует 10% RAM, а остальные объекты кэширует только на диске). Можно задать любой объем оперативной памяти от 1 до 100%. Эта величина задается при старте сервиса брандмауэра. Если нужно изменить объем используемой оперативной памяти, следует остановить и повторно запустить сервис брандмауэра.

Возможность управления объемом оперативной памяти, отведенной под кэш, гарантирует, что кэширование не исчерпает все ресурсы компьютера с сервером ISA.

> ПРИМЕЧАНИЕ Из соображений безопасности и усиления функций брандмауэра кэширование не активизируется по умолчанию после установки ISA Server 2004. Следует активизировать эту функциональную возможность перед применением.

Применение функции кэширования

Настройка *устройства кэша (cache drive)* делает возможным и прямое, и обратное кэширование на компьютере с ISA Server 2004. Позже в этой главе мы покажем, как включить функцию кэширования.

Существует несколько требований и рекомендаций, относящихся к устройству, используемому как устройство кэша.

- Устройство кэша должно быть локальным диском. Нельзя конфигурировать сетевой диск для хранения кэша.
- Устройство кэша должно быть разделом файловой системы NTFS. Нельзя использовать разделы файловых систем FAT или FAT32 для устройства кэша.
- Лучше (но не обязательно) не использовать диск, на котором установлены операционная система и/или приложение ISA Server. Производительность будет выше, если кэш поместить на отдельном диске. В действительности для наивысшей производительности недостаточно поместить кэш на отдельном диске, у устройства кэша должен быть отдельный канал ввода/вывода (т. е. устройство кэша не должно располагаться на диске, ведомом (slaved with) диском, содержащим файлы страниц, ОС или файлы программы ISA). Более того, если уделяется внимание производительности ISA Server, следует учесть, что ведение журналов регистрации MSDE (Microsoft Data Engine, машина баз данных корпорации Microsoft) потребляет больше дискового пространства, чем запись регистрации в текстовом формате. Следовательно, если используется ведение журналов регистрации в формате MSDE, устройство кэша должно находиться на дисководе, отделенном от баз данных MSDE.

СОВЕТ Для преобразования без потери данных разделов файловых систем FAT или FAT32 в раздел NTFS можно при необходимости воспользоваться утилитой convert.exe.

Файл, в котором хранятся объекты кэша, называется dirl.cdat. Он находится в папке urlcache на диске, который конфигурирован для кэширования. Этот файл называют ***файлом*** *содержимого кэша (cache content file).* Если этот файл достигает максимального размера, более старые объекты удаляются, чтобы освободить место для новых объектов.

Размер файла содержимого кэша не может быть больше 64 Гб (конечно, можно использовать файл с меньшим максимальным размером). Если необходимо ствести под кэш более 64 Гб, необходимо конфигурировать несколько дисков для кэширования и разделить кэш на несколько файлов.

ПРЕДУПРЕЖДЕНИЕ Никогда не пытайтесь редактировать или удалять файл содержимого кэша.

Описание правил кэширования

ISA Server 2004 позволяет настроить типы содержимого, сохраняемого в кэше, и точные методы обработки содержимого при выполнении запроса объекта, хранящегося в кэше.

Можно создать правила для управления промежутком времени, в течение которого объект кэша считается достоверным (как гарантия того, что объекты кэша не

смогут безнадежно устареть) и задать способ обработки объектов по истечении срока хранения в *кэше.*

Сервер ISA позволяет гибко применять правила кэширования ко всем сайтам или только к заданным. В дальнейшем можно конфигурировать правило для использования со всеми типами содержимого или только с указанными явно.

Использование правил кэширования для задания типов содержимого, которое может кэшироваться

Правило кэширования позволяет указать, какие из следующих типов содержимого должны кэшироваться.

- **Dynamic content** (Динамическое содержимое) Это содержимое, которое часто меняется и поэтому помечено как не подлежащее кэшированию. Наш выбрать кэширование динамического содержимого, то полученные объекты будут кэшироваться, даже если они помечены как некэшируемые.
- **Content for offline browsing** (Содержимое для просмотра в автономном режиме) Для того чтобы пользователи могли просматривать содержимое в автономном режиме (когда они отключены от Интернета), необходимо все содержимое сохранять в кэше. Таким образом, если выбрать этот вариант, ISA Server 2004 сохранит в кэше все содержимое, включая «не подлежащий кэшированию» контент.
- **Content requiring user authentication for retrieval** (Содержимое, требующее для извлечения аутентификации пользователя) Некоторые сайты требуют подтверждения подлинности пользователя для получения доступа к содержимому. Если выбран этот вариант, ISA Server 2004 будет кэшировать содержимое, требующее аутентификации пользователя.

Можно также задать параметр Maximum **object size** (Максимальный размер объекта). Он позволяет установить ограничение размера Web-объектов, которые будут кэшироваться по определенному правилу кэширования.

Применение правил кэширования для задания способа извлечения и обслуживания объектов из кэша

Кроме контроля над типом содержимого и размером объекта правило кэширования может управлять способом, с помощью которого сервер ISA будет выполнять извлечение и обслуживание объектов из кэша. Это относится к достоверности объекта. Достоверность объекта (object's validity) определяется тем, истекла или нет его продолжительность жизни (Time to Live, TTL). Время истечения этого срока определяется свойствами HTTP- или FTP-кэширования либо свойствами объекта. Возможны следующие варианты.

- **Setting ISA Server 2004 to retrieve only valid objects from cache (those that have not expired)** (Настройка ISA Server 2004 на извлечение из кэша только достоверных объектов (тех, чье время функционирования не закончилось)

Если срок жизни объекта истек, сервер ISA пошлет запрос на Web-сервер, содержащий данный объект, и получит его оттуда.

- **Setting ISA Server 2004 to retrieve requested objects from the cache even if they aren't valid** (Настройка ISA Server 2004 на извлечение из кэша затребованных объектов, даже если они недостоверны) Другими словами, если объект находится в кэше, сервер ISA извлечет его оттуда и обработает, даже если продолжительность жизни объекта истекла. Если в кэше нет версии объекта, сервер ISA пошлет запрос на Web-сервер и получит объект с сервера.
- **Setting ISA Server to never route the request** (Настройка ISA Server на отсутствие маршрутизации запроса) В этом случае сервер ISA полагается только на кэш при извлечении объекта. Объекты будут возвращены из кэша независимо от их достоверности. Если в кэше нет версии объекта, сервер ISA вернет сообщение об ошибке. Он *не будет* посылать запрос на Web-сервер.
- **Setting ISA Server to never save the object to cache** (Настройка ISA Server на отказ от сохранения объекта в кэше) Если конфигурировать правило таким образом, запрашиваемый объект никогда не будет сохраняться в кэше.

ПРИМЕЧАНИЕ По умолчанию продолжительность жизни FTP-объектов один день. Продолжительность жизни HTTP-объектов (определенных в правиле кэширования) представляет собой определенный процент от возраста содержимого в зависимости от времени создания и последнего изменения объекта.

Можно также управлять кэшированием содержимого, предназначенного для заданных адресатов, и установить политики для HTTP- и FTP-объектов с истекшим сроком жизни. Есть возможность активизировать кэширование SSL-содержимого.

СОВЕТ Поскольку SSL-содержимое часто содержит конфиденциальную информацию (именно поэтому защищенную SSL-протоколом), можно не разрешать кэширование этого типа содержимого для усиления безопасности.

Если существует несколько правил кэширования, они обрабатываются по порядку, от первого до последнего; правило, установленное по умолчанию, обрабатывается после всех правил, заданных пользователем. Правило по умолчанию создается автоматически при установке ISA Server 2004, сконфигурированного для извлечения из кэша только достоверных объектов и получения объекта из Интернета, если в кэше нет его достоверной версии.

Позже в этой главе мы покажем, как конфигурировать правила кэширования.

Описание функции загрузки содержимого

Функция загрузки содержимого применяется для планирования сервером ISA загрузки из Интернета нового содержимого в заранее определенное время, для того чтобы клиентам Web-прокси, запросившим данные объекты, предоставлялись обновленные версии из кэша. Это повышает производительность и гарантирует клиентам более быстрое получение новейшего содержимого.

Можно отслеживать доступ в Интернет и его использование (см. главу 12), чтобы определить, к каким сайтам пользователи обращаются чаще всего, и предсказать, какое содержимое может понадобиться в будущем. Затем можно планировать соответственно задания на загрузку содержимого из Интернета. Задание на загрузку содержимого может быть настроено на периодическую загрузку из Интернета одной страницы (URL-адреса), многих страниц или всего сайта. Есть возможность задать количество ссылок, которое должно быть пройдено при загрузке сайта. Можно также настроить ISA Server 2004 для кэширования даже тех объектов, которые помечены как не подлежащие кэшированию в заголовках управления кэшем (cache control headers). Однако планируемое задание на загрузку содержимого не завершится, если Web-сервер, на котором хранится объект, требует подтверждения подлинности клиента.

Для получения выигрыша от применения этой функции следует активизировать группу конфигурирования системной политики для заданий загрузки содержимого из Интернета по расписанию, а затем конфигурировать задание на загрузку содержимого. Мы покажем, как это делается, в одном из последующих разделов данной главы.

СОВЕТ Когда активизируется группа конфигурирования системной политики **Schedule Content Download Jobs** (Задания на загрузку из Интернета по расписанию) сервер ISA блокирует неаутентифицированный HTTP-трафик с локального хоста (сервер ISA), даже если есть правило другой политики, настроенное на разрешение такого трафика. Существует прием, делающий возможным разрешение подобного трафика и сохранение использования заданий на загрузку содержимого из Интернета. Он включает создание правила, разрешающего HTTP-доступ к All Networks (Все сети), и наличие предшествующего в списке правила, настроенного на разрешение HTTP-доступа с локального хоста.

Как Web-мастера управляют кэшированием с помощью HTTP-заголовков

Есть два различных фактора, влияющих на способ кэширования HTTP (Web)-содержимого. Один из них — конфигурация сервера кэширования, но Web-мастера также могут поместить в содержимое и заголовки информацию, указывающую на способ кэширования их сайтов и объектов.

Мета-теги — это команды в HTML-коде документа, задающие HTTP-окончание жизненного срока объекта или статус некэшируемости, но они обрабатываются только кэшами обозревателя, а не прокси-кэшами. HTTP-заголовки обрабатываются как прокси-кэшами, так и кэшами обозревателей. Они не включены в HTML-код, настраиваются на Web-сервере и отправляются Web-сервером до отправки HTML-содержимого.

(см. след. стр.)

Протокол HTTP 1.1 поддерживает категорию заголовков, называемую заголовками управляющих ответов кэша (cache control response headers). Используя эти заголовки, Web-мастер может управлять следующими характеристиками:

- максимальным возрастом (базирующимся на времени запроса, максимальным промежутком времени, в течение которого объект считается достоверным);
- кэшируемостью;
- требованиями к повторному подтверждению достоверности.

Теги Etags и заголовки Last-Modified (последний раз модифицированный) генерируются Web-сервером и используются для проверки «свежести» объекга.

В Microsoft Internet Information Services (IIS, информационный сервис Интернета фирмы Microsoft) заголовки управляющих ответов кэша конфигурируются на вкладке HTTP Headers (HTTP-заголовки) страницы свойств Web-сайта или Web-страницы.

ISA Server 2004 не кэширует ответы на запросы, содержащие определенные HTTP-заголовки, включая следующие:

- cache-control[1]: no-cache response header;
- cache-control: private response header;
- pragma: no-cache response header;
- www-authenticate response header;
- set-cookie response header;
- cache-control: no-store request header;
- authorization request header (за исключением случая, когда Web-сервер тоже посылает cache-control: public response header).

Для получения более подробной информации о том, как Web-мастер может управлять кэшированием с помощью HTTP-заголовков, посмотрите статью, расположенную по адресу www.mnot.net/cache_docs/#IMP-SERVER.

Cache-control — мета-те г.

Конфигурирование ISA Server 2004 как сервера кэширования

Несмотря на то, что по умолчанию кэширование не разрешено, очень легко конфигурировать ISA Server 2004 для выполнения прямого и/или обратного кэширования. В этом разделе мы приведем пошаговые процедуры для следующих настроек:

- активизация кэширования;
- конфигурирование размера кэша и объема памяти, отведенной под кэш;
- создание правил кэширования;
- конфигурирование заданий на загрузку содержимого из Интернета.

Активизация и конфигурирование кэширования

В этом разделе мы рассмотрим, как включить, отключить и конфигурировать основные свойства кэширования. Первый шаг в применении ISA Server 2004 как сервера кэширования — активизация или включение режима кэширования.

> ПРИМЕЧАНИЕ Инструкции по включению и отключению кэширования на ISA Server 2004 Enterprise Edition соответствуют бета-версии EE. Финальный выпуск еще не был доступен во время написания книги. Интерфейс может измениться перед выходом финального выпуска продукта, для того чтобы соответствовать интерфейсу, обеспечивающему включение и отключение кэширования *в* редакции Standard Edition.

Как активизировать кэширование в Enterprise Edition

На консоли управления сервера ISA в узле **Configuration** (Конфигурация) / **Cache** (Кэш) выполните следующее.

1. На левой панели консоли управления (MMC) ISA Server 2004 раскройте окно, свя занное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется Enterprise Edition), и раскройте узел **Configuration** (Конфигурация).
2. Щелкните кнопкой мыши вкладку **Cache Drives** (Устройства кэша) на средней панели.
3. На вкладке **Tasks** (Задачи) правой панели, если кэширование не включено, вы увидите выбор, обозначенный как **Define Cache Drives** (Определить устрой ства кэша).
4. На вкладке **Cache Drives** (Устройства кэша) окна свойств (рис. 11.4) выберите диск с файловой системой NTFS и введите нужное число в текстовое поле **Maxi mum cache size** (Максимальный размер кэша), затем щелкните мышью кнопку **Set** (Установить).
5. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK.

Рис. 11.4. Установка максимального размера кэша

Как включить кэширование в версии Standard Edition

На консоли управления сервера ISA в узле **Configuration** (Конфигурация) / **Cache** (Кэш) выполните следующее.

1. На левой панели консоли управления (MMC) ISA Server 2004 раскройте окно, свя занное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется Enterprise Edition), и раскройте узел **Configuration** (Конфигурация).
2. Щелкните правой кнопкой мыши узел **Cache** (Кэш) на левой панели и выбери те команду **Define Cache Drives** (Определить устройства кэша) или щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на средней пане ли и выберите строку **Define Cache Drives (enable caching)** (Определить ус тройства кэша, (включить кэширование)) на правой панели **Tasks** (Задачи).
3. В диалоговом окне **Define Cache Drives** (Определение устройств кэша) выбе рите диск с файловой системой NTFS и введите нужное число в текстовое поле **Maximum cache size** (Максимальный размер кэша), а затем щелкните мышью кнопку **Set** (Установить).
4. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку OK.

Как отключить кэширование в версии Enterprise Edition

После того, как кэширование включено, в разделе **Cache Drive Tasks** (Задачи уст ройства кэша) на вкладке **Tasks** (Задачи) правой панели появится новый выбор **Disable Caching** (Отключить кэширование).

Если вы щелкнете кнопкой мыши **Disable Caching** (Отключить кэширование), на экране появится диалоговое окно, советующее установить размер кэша на всех устройствах кэша равным нулю, после чего кэширование будет отключено. Для повторного включения режима кэширования придется снова конфигурировать устройства кэша. Подтвердите ваше желание отключить кэширование, щелкнув мышью кнопку **Yes** (Да), и размер кэша будет автоматически уставлен на всех устройствах кэша равным нулю.

Как отключить кэширование в версии Standard Edition

На ISA Server 2004 Standard Edition можно отключить кэширование, выполнив следующие шаги.

1. На левой панели консоли управления MMC ISA Server 2004 раскройте окно, свя занное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если ис пользуется Enterprise Edition), и затем раскройте узел **Configuration** (Конфи гурация).
2. Щелкните правой кнопкой мыши узел **Cache** (Кэш) и выберите команду **Disable Caching** (Отключить кэширование) или щелкните кнопкой мыши вкладку **Cache** Rules (Правила кэширования) на средней панели и выберите **Disable Caching** (Отключить кэширование) на правой панели **Tasks** (Задачи).

ПРИМЕЧАНИЕ Другой способ установки размера кэша равным нулю — использование кнопки **Reset** (Сбросить) на вкладке **Cache Drives** в диалоговом окне свойств (в Enterprise Edition) или в диалоговом окне **Define Cache Drives** (в Standard Edition).

ПРИМЕЧАНИЕ До тех пор, пока хотя бы у одного устройства кэша размер больше нуля, кэширование включено.

Конфигурирование свойств кэширования

В этом разделе рассматривается способ настройки общих свойств кэширования, включая следующие:

- выбор содержимого для кэширования;
- задание максимального размера объектов *в* кэше;
- настройка негативного кэширования (negative caching), называемого также кэ шированием отрицательных ответов;
- выбор способа обработки объектов кэша с истекшим жизненным сроком;
- выделение памяти для кэширования.

Рассмотрим по очереди каждое из перечисленных свойств.

Выбор содержимого для кэширования

Для выбора содержимого, которое следует кэшировать, выполните следующие шаги.

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется версия Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на средней панели.
3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на правой панели.
4. Щелкните мышью **Configure Cache Settings** (Конфигурировать установочные параметры кэша) в разделе **Related Tasks** (Связанные задачи).
5. Щелкните кнопкой мыши вкладку **Advanced** (Дополнительно) в диалоговом окне **Cache Settings** (Установочные параметры кэша).
6. На этой вкладке (рис. 11.5) можно выбрать, кэшировать ли объекты, у которых не задано время последней модификации, и объекты, у которых нет кода HTTP-состояния, равного 200 (успешное завершение), устанавливая или сбрасывая соответствующий флажок. По умолчанию оба флажка установлены (таким образом, кэширование этих объектов разрешено).

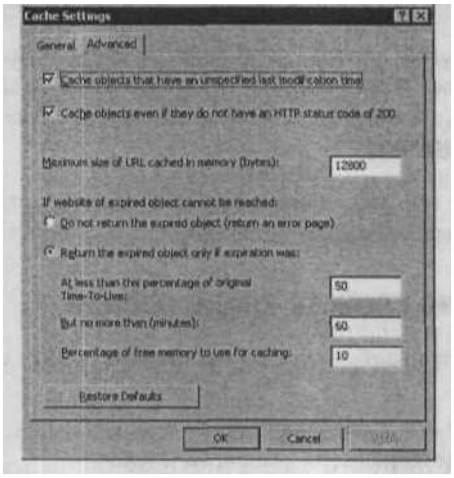


Рис. 11.5. Выбор кэшируемого содержимого

СОВЕТ У сервера ISA Server 2004 Standard Edition есть три вкладки в диалоговом окне **Cache Settings** (Установочные параметры кэша): **General** (Общие), **Advanced** (Дополнительно) and **Active Caching** (Активное кэширование). Вкладка **Active Caching** (Активное кэширование) исчезла в Enterprise Edition, она и в Standard Edition представлена как артифакт, оставшийся от ранних бета-версий, которые еще поддерживали активное кэширование. Настройки, сделанные на этой вкладке, не влияют на конфигурацию ISA Server 2004, даже если он примет эти установки.

ПРИМЕЧАНИЕ Код HTTP-состояния, равный 200, означает «ОК», т. е. запрос, посланный клиентом, успешно выполнен. Объекты кэширования, не имеющие кода состояния 200, относятся к «негативному кэшированию».

Настройка максимального размера объектов в кэше

Этот параметр устанавливается в том же диалоговом окне **Cache Settings** (Установочные параметры кэша), что и предыдущий.

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на средней панели.
3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на правой панели.
4. Щелкните мышью **Configure Cache Settings** (Конфигурировать установочные параметры кэша) в разделе **Related Tasks** (Связанные задачи).
5. Щелкните кнопкой мыши вкладку **Advanced** (Дополнительно) в диалоговом окне **Cache Settings** (Установочные параметры кэша).
6. В текстовое поле **Maximum size of URL cached in memory (bytes)** (Максимальный размер URL, кэшируемого в памяти, в байтах) введите нужное число байтов. Оно ограничит размер объектов, которые могут кэшироваться, и сохранит место на вашем устройстве кэша.

Настройка способа обработки объектов с истекшим жизненным сроком

Эта установка также делается в диалоговом окне **Cache Settings** (Установки кэша).

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется версия Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэша) на средней панели.
3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на правой панели.
4. Щелкните мышью **Configure Cache Settings** (Конфигурирование установок кэша) в разделе **Related Tasks** (Связанные задачи).
5. Щелкните кнопкой мыши вкладку **Advanced** (Дополнительно) в диалоговом окне **Cache Settings** (Установки кэша).
6. Если нежелательно, чтобы возвращался объект с истекшим жизненным сроком, если Web-сайт не доступен, выберите вариант Do **not return the expired object** (Не возвращать объект с истекшим жизненным сроком). В этом случае будет возвращаться страница с информацией об ошибке.

7. В противном случае можно выбрать возвращение объекта с истекшим жизненным сроком, если превышение его продолжительности жизни меньше заданного количества процентов от исходной продолжительности жизни (TTL), но не превышает указанного числа минут со времени истечения жизненного срока. Если выбран этот вариант, необходимо ввести конкретные значения в соответствующие поля.

По умолчанию ISA Server 2004 сконфигурирован на возвращение объекта с истекшим жизненным сроком, только если превышение продолжительности жизни объекта меньше 50% от его первоначального значения и не больше 60 мин.

Выделение объема памяти для кэширования

Этот установочный параметр задается в диалоговом окне **Cache Settings** (Установки кэша).

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связан ное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется версия Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правило кэша) на средней па нели.
3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на правой панели.
4. Щелкните мышью **Configure Cache Settings** (Конфигурирование установок кэша) в разделе **Related Tasks** (Связанные задачи).
5. Щелкните кнопкой мыши вкладку **Advanced** (Дополнительно) вдиалоговом окне **Cache Settings** (Установки кэша).
6. В текстовое поле, названное **Percentage of free memory to use for caching** (Объем свободной памяти в процентах, предназначенный для кэширования), введите нужное количество процентов.

По умолчанию под кэширование выделяется 10% объема памяти. При превышении заданного объема дополнительные объекты кэшируются только на диске (не в оперативной памяти).

Создание и настройка правил кэширования

В этом разделе рассматривается, как создавать и настраивать правила кэширования для различных ситуаций, как модифицировать существующее правило кэширования и как отключить или удалить правило кэширования, созданное ранее, а также как изменить порядок применения правил. Кроме того, в данном разделе обсуждаются способы копирования, экспортирования и импортирования правил кэширования.

Как создать правило кэширования

С помощью мастера, встроенного в ISA Server 2004, очень легко создать правило кэширования. Просто выполните следующие шаги.

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связан ное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется версия Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на сред ней панели.
3. Щелкните мышью вкладку **Tasks** (Задачи) на правой панели.
4. В разделе **Cache Rule Tasks** (Задачи правила кэширования) щелкните мышью **Create a Cache Rule** (Создать правило кэширования). Запустится мастер **New Cache Rule Wizard** (Мастер создания нового правила кэширования), показан ный на рис. 11.6.

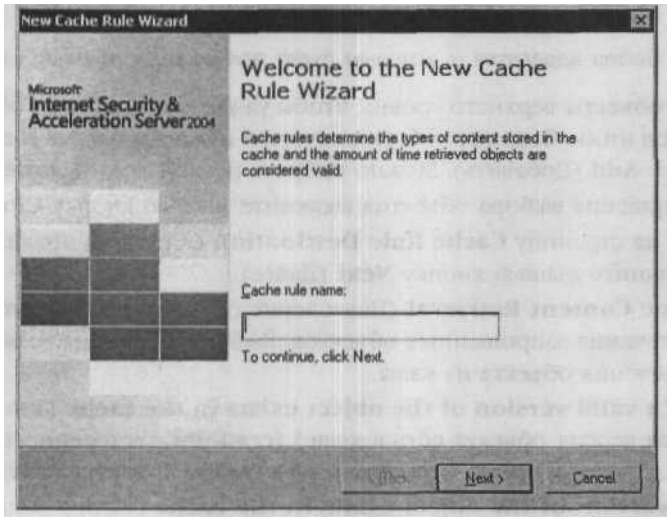


Рис. 11.6. Создание нового правила кэширования с помощью мастера

5. Введите название нового правила кэширования и нажмите мышью кнопку **Next** (Далее).
6. На следующей странице необходимо выбрать сетевые объекты-адресаты. Пра вило будет применяться к запросам, посылаемым этими адресатами. Щелкните мышью кнопку **Add** (Добавить) и выберите объекты из перечисленных в диа логовом окне **Add Network Entities** (Добавить сетевые объекты) (рис. 11.7).

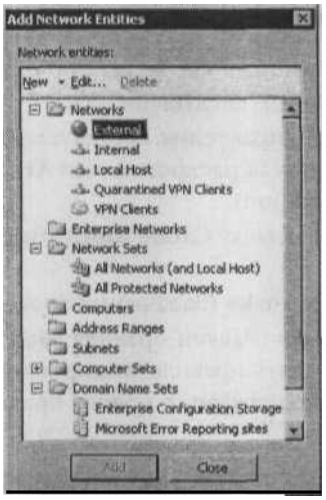


Рис. 11.7. Выбор адресатов, к которым будет применяться правило кэширования

7. Раскройте объекты верхнего уровня, чтобы увидеть конкретные объекты нахо дящиеся под ними. Выделите объект, который нужно добавить и щелкните мы шью кнопку Add (Добавить). Можно выбрать несколько объектов.
8. После завершения выбора объектов щелкните мышью кнопку Close (Закрыть).
9. Вернитесь на страницу Cache Rule Destination (Адресаты правила кэширова ния) и щелкните мышью кнопку Next (Далее).
10. На странице Content Retrieval (Извлечение объектов) можно управлять способом извлечения запрошенных объектов. Выберите один из возможных вариантов извлечения объекта из кэша.

    □ Only if a valid version of the object exists in the cache (Только если достоверная версия объекта есть в кэше) (если нет достоверного объекта, запрос будет направлен на Web-сервер, на котором хранится исходный объект). D If any version of the object exists in the cache (ЕСЛИ В кэше есть какая-нибудь версия объекта) (если в кэше есть недостоверная версия объекта, она будет возвращена из кэша. Если в кэше нет никакой версии объекта, запрос будет направлен на Web-сервер).

    D If any version of the object exists in cache (Если в кэше есть какая-нибудь версия объекта) (если в кэше нет никакой версии, запрос отвергается и не направляется на Web-сервер).

Выберите подходящий вариант и щелкните мышью кнопку Next (Далее). 11. На странице Cache Content (Содержимое кэша) можно управлять конкретными типами содержимого, или контента, которые следует кэшировать. По умолчанию объект не сохраняется в кэше до тех пор, пока в заголовках запроса и ответа нет команды кэшировать его. Но на этой странице можно изменить та-

кое поведение, выбрав один из предлагаемых вариантов: **Never, no objects will ever be cached** (Никогда никакие объекты не будут кэшироваться) и **If source and request headers indicate to cache** (Если в заголовках источника и адресата указано кэширование). Этот вариант установлен по умолчанию. Если выбрано кэширование объектов, можно также определить, какой тип содержимого, из приведенных далее, следует кэшировать: **a Dynamic content** (Динамическое содержимое); D **Content for offline browsing** (Содержимое для просмотра в автономном режиме);

D **Content requiring user authentication for retrieval** (Содержимое, требующее для извлечения аутентификации пользователя).

По умолчанию ни один из перечисленных типов не кэшируется. Можно установить любое количество флажков, определяющих тип сохраняемого содержимого (рис. 11.8).

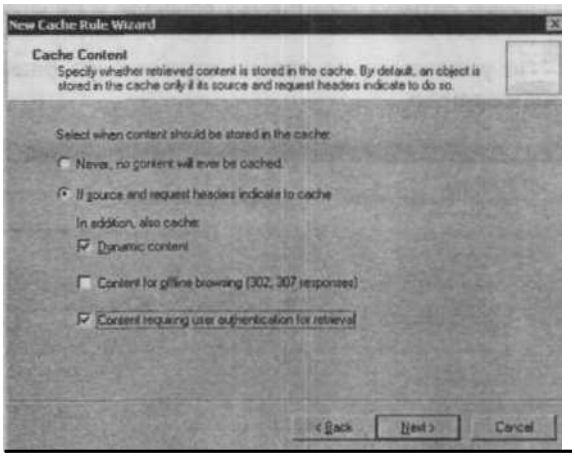


Рис. 11.8. Настройка вариантов сохранения содержимого в кэше

12. После выбора нужных переключателей щелкните мышью кнопку **Next** (Далее).
13. На странице **Cache Advanced Configuration** (Расширенная конфигурация кэша) можно задать ограничение размера кэшируемых объектов, установив флажок **Do not cache objects larger than:** (Не кэшировать объекты, размер которых больше:) и указав размер в килобайтах, мегабайтах или гигабайтах (рис. 11.9).
14. На этой странице **также** можно выбрать вариант кэширования ответов по SSL-протоколу. По умолчанию SSL-ответы кэшируются, но можно сбросить соответствующий флажок из соображений безопасности, поскольку SSL-содержимое может быть конфиденциальным, и вы не захотите хранить его копию на сервере кэширования.

3 5. После завершения выбора щелкните мышью кнопку **Next** (Далее).

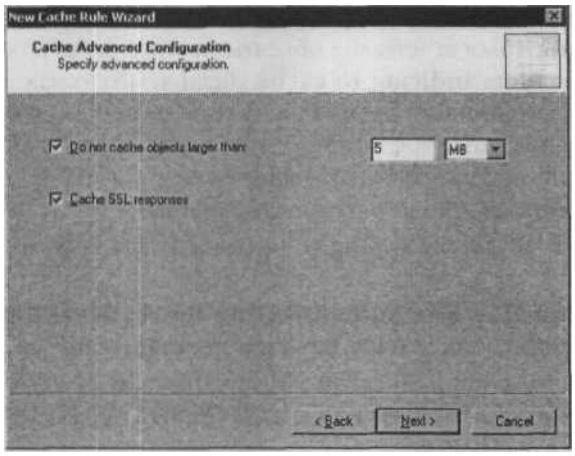


Рис. 11.9. Ограничение размера кэшируемых объектов и кэширование SSL-ответов

ПРИМЕЧАНИЕ По умолчанию не задано ограничение размера объектов, подлежащих кэшированию.

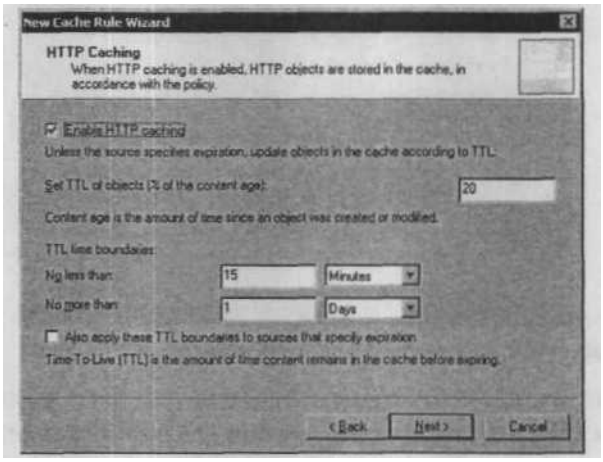


Рис. 11.10. Разрешение HTTP-кэширования и установка конфигурации TTL

16. На странице **HTTP Caching** (HTTP-кэширование) можно разрешить или запретить HTTP-кэширование (по умолчанию оно разрешено) и установить TTL (продолжительность жизни) объектов как определенный процент от возраста содержимого, основанного на времени его создания или последней модификации. Можно также задать временные границы продолжительности жизни объекта и применить их к источникам, для которых задано превышение жизненного срока (expiration) (рис. 11.10). По умолчанию продолжительность жизни объекта равна

20% от возраста содержимого и временные границы заданы не менее 15 минут и не более одного дня.

ПРИМЕЧАНИЕ Даты создания («created») и последней модификации («last modified») содержатся в HTTP-заголовках, которые возвращаются Web-сервером.

17. После того, как выбор сделан, щелкните мышью кнопку **Next** (Далее).
18. На странице **FTP Caching** (FTP-кэширование) можно разрешить или запретить FTP-кэширование (по умолчанию оно разрешено). Также можно установить продол жительность жизни (TTL) FTP-объектов (рис. 11.11). По умолчанию — один день.

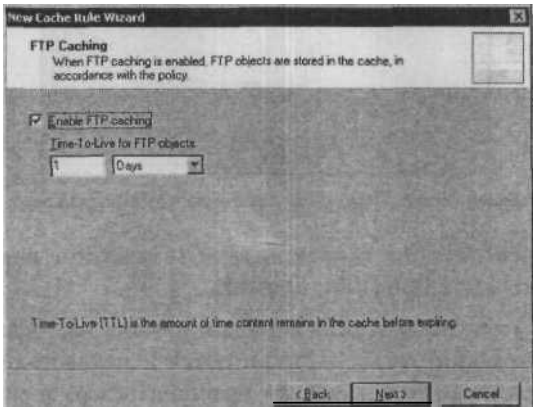


Рис. 11.11. Разрешение FTP-кэширования и задание продолжительности жизни объектов

19. После установки параметров щелкните мышью кнопку **Next** (Далее).
20. На последней странице мастера показаны все сделанные вами установки. Если необходимо внести изменения, щелкните мышью кнопку **Back** (Назад), для того чтобы вернуться на соответствующую страницу и изменить установленные ра нее параметры. В противном случае щелкните мышью кнопку **Finish** (Готово) для создания правила.

Как изменить существующее правило кэширования

Если необходимо внести изменения в уже созданное правило кэширования, выделите его цветом на вкладке **Cache Rules** (Правила кэширования) на средней панели консоли управления ISA Server 2004 и щелкните левой кнопкой мыши команду **Edit Selected Rule** (Редактировать выбранное правило) на правой панели **Tasks** (Задачи) или щелкните правой кнопкой мыши правило, которое хотите изменить, и выберите левой кнопкой мыши команду **Properties** (Свойства). В любом случае откроется диалоговое окно **Properties <Rule name>** (Свойства <название правила^, показанное на рис. 11.12.

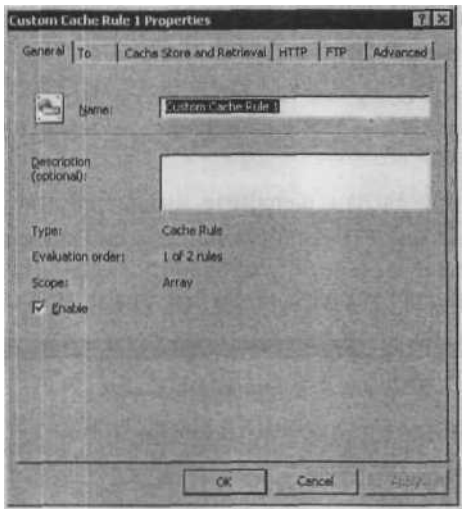


Рис. 11.12. Модификация существующего правила кэширования

На вкладке **General** (Общие) можно изменить название правила кэширования и вставить необязательное описание правила.

На вкладке To (К) можно добавить, отредактировать или удалить объекты сети-адресата. На этой странице также настраиваются исключения (рис. 11.13). В данном примере правило кэширования будет применяться ко всему содержимому, запрошенному из внешних объектов за исключением объекта shinder.net.

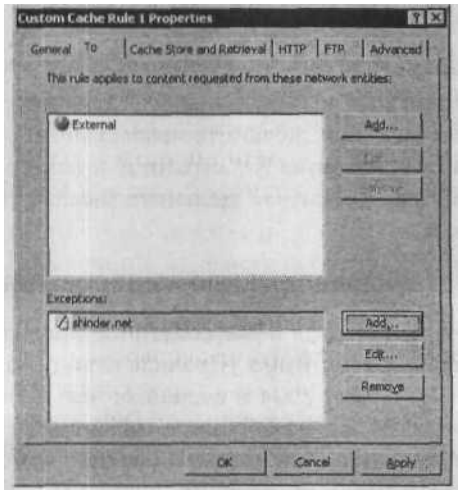


Рис. 11.13. Настройка исключений для объектов сети адресата

На вкладке **Cache Store and Retrieval** (Сохранение в кэше и извлечение из него) можно изменить выбранные установки, сделанные вами в мастере создания правила кэширования и определяющие, когда извлекать содержимое из кэша и когда сохранять его в кэше.

На вкладке **HTTP** есть возможность разрешить или запретить HTTP-кэширование и изменить ваши настройки, относящиеся к продолжительности жизни объектов. Можно также восстановить установки по умолчанию, щелкнув мышью соответствующую кнопку.

На вкладке **FTP** разрешается или запрещается FTP-кэширование, а также меняются установки продолжительности жизни объектов или восстанавливаются установки, принимаемые по умолчанию.

На вкладке **Advanced** (Дополнительно) можно задать или модифицировать ограничение размера кэшируемых объектов и изменить установки, касающиеся SSL-ответов.

Как блокировать или удалить правило кэширования

Если нужно блокировать созданное правило кэширования (но сохранить его для возможного использования в будущем), следует выполнить следующие шаги.

1. На средней панели консоли управления ISA Server 2004 выделите правило, которое необходимо блокировать, и щелкните кнопкой мыши задачу **Edit Selected Rule** (Редактировать выбранное правило) на правой панели задач или щелкните правой кнопкой мыши нужное правило и выберите левой кнопкой мыши команду **Properties** (Свойства).
2. На вкладке **General** (Общие) сбросьте флажок **Enable** (Включить).
3. Щелкните мышью кнопку **Apply** (Применить), а затем кнопку ОК.

Правило будет по-прежнему выводиться в списке **Cache Rules** (Правила кэширования), но с пиктограммой, содержащей направленную вниз красную стрелку и обозначающей, что правило блокировано или отключено. Для того, чтобы снова включить правило, нужно просто установить флажок **Enable** (Включить).

Если есть желание расстаться с правилом окончательно (не предполагается повторное использование) можно его удалить. Просто выделите на средней панели правило, которое хотите удалить, и щелкните кнопкой мыши строку **Delete Selected Rules** (Удалить выбранные правила) на правой панели **Tasks** (Задачи). Можно выделить несколько правил и удалить их одновременно. Кроме того, можно щелкнуть правой кнопкой мыши правило(а), которое следует удалить, и выбрать левой кнопкой мыши из контекстного меню команду **Delete** (Удалить). От вас потребуется подтверждение намерения удалить правило. Щелкните мышью кнопку **Yes** (Да), если правило следует удалить.

Как изменить порядок применения правил кэширования

Помните о том, что правила кэширования обрабатываются в порядке их следования от первого до последнего (с верхней до нижней строки списка вкладки **Cache Rules** (Правила кэширования) на средней панели) с обязательным выполнением правила по умолчанию в последнюю очередь.

Можно изменить порядок следования правил, выделив правило, расположенное в списке выше, и выбрав на правой панели **Tasks** (Задачи) команду **Move Selected Rules Down** (Переместить выбранные правила ниже) или щелкнув правой кнопкой мыши правило, которое необходимо передвинуть, и выбрав левой кнопкой мыши из контекстного меню команду **Move Down** (Переместить ниже).

Как копировать правило кэширования

Существует возможность копировать и вставлять созданные правила кэшироиания. Когда возникает необходимость в этом? Например, если правило уже создано, и теперь нужно создать еще одно правило, отличающееся от первого одним или двумя параметрами, вместо того, чтобы полностью повторять процесс с помощью мастера, можно щелкнуть правой кнопкой мыши первое правило и выбрать и:) контекстного меню команду **Copy** (Копировать).

Затем следует еще раз щелкнуть правой кнопкой мыши первое правило (а не свободную область списка правил кэширования, как интуитивно можно было бы предположить) и выбрать из контекстного меню команду **Paste** (Вставить). Далее следует открыть диалоговое окно **Properties** (Свойства) копии правила и изменить его название, а также другие параметры, если необходимо.

> СОВЕТ Обратите внимание на то, что команды копирования и вставки не выводятся на правой панели задач консоли управления. В отличие от большинства задач, их придется выбирать из контекстного меню, вызываемого щелчком правой кнопки мыши.

Как экспортировать и импортировать правила кэширования

Можно экспортировать правила кэширования в файл с расширением xml, который затем может быть использован для импорта данных на другой компьютер с ISA Server 2004 или повторно на этот же компьютер. Далее приведены шаги, необходимые для экспорта правил кэширования.

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связан ное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется Enterprise Edition).
2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на сред ней панели.
3. Щелкните кнопкой мыши вкладку **Tasks** (Задачи) на правой панели.

4. В разделе **Related Tasks** (Связанные задачи) щелкните кнопкой мыши команду **Export Cache Rules** (Экспортировать правила кэширования). При этом запус кается мастер экспорта. Щелкните мышью кнопку **Next** (Далее) на первой стра нице мастера.
5. На странице **Export Preferences** (Экспорт предпочтений) можно включить необязательную конфиденциальную информацию (содержащую пароли пользо вателей, секретные ключи (shared secrets) RADIUS и другие конфиденциальные сведения) вместе с правилами как таковыми. По умолчанию секретные данные не экспортируются. Если принято решение об их экспортировании с помощью установки соответствующего флажка, придется ввести и подтвердить пароль. Этот пароль будет применяться для шифрования конфиденциальных сведений. Щелк ните мышью кнопку **Next** (Далее).
6. На странице **Export File Location** (Местоположение файла экспорта) введите или укажите с помощью средств просмотра путь к файлу, в котором сохранятся экспортируемые данные. Это должен быть файл с расширением xml. Если он еще не создан, можно ввести нужный путь к файлу и его имя (например, c:\files\ cacherules.xml).

   СОВЕТ Хотя вы можете создать новый файл, набрав путь и имя файла на странице Export File Location (Местоположение файла экспорта), вы должны указать при этом существующий путь (т. е. нельзя создать новую папку на этом пути; при попытке сделать это, появится сообщение об ошибке, констатирующее, что заданный путь не существует).

7. На последней странице мастера сведены воедино все сделанные установки. Если нужно что-либо изменить, используйте кнопку **Back** (Назад) для возврата на соответствующую страницу и внесения изменений. При отсутствии подобной необходимости щелкните мышью кнопку **Finish** (Готово) для экспорта данных *з* заданный файл. Когда конфигурация будет успешно экспортирована, появит ся информирующее об этом диалоговое окно (рис. 11.14).

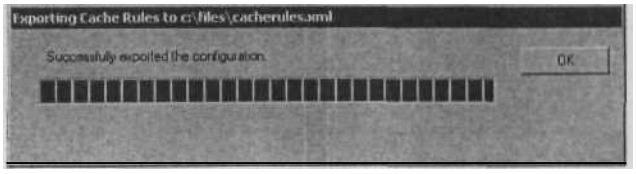


Рис. 11.14. Успешное экспортирование правил кэширования в xml-файл

Теперь для импортирования правил кэширования, сохраненных в xml-файлах, просто выполните следующие шаги.

1. На левой панели консоли управления ISA Server 2004 раскройте окно, связан ное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется версия Enterprise Edition).

2. Щелкните кнопкой мыши вкладку **Cache Rules** (Правила кэширования) на сред ней панели.
3. Щелкните мышью вкладку **Tasks** (Задачи) на правой панели.
4. В разделе **Related Tasks** (Связанные задачи) щелкните кнопкой мыши строку **Import Cache Rules** (Импортировать правила кэширования). Это действие за пустит мастер импорта **Import.** Щелкните мышью кнопку **Next** (Далее) на пер вой странице мастера.

   СОВЕТ Если в конфигурацию внесены и еще не сохранены изменения, появится сообщение, предупреждающее о возможности потери этих изме нений при возникновении ошибки в процессе импорта. На вопрос о продол жении импорта ответьте Yes (Да) для дальнейшего импортирования или No (Нет) для остановки процесса импортирования и возврата для сохранения внесенных изменений. Для того чтобы сохранить изменения, щелкните мы шью кнопку Apply (Применить) в верхней части средней панели консоли управления.

5. На странице **Select the Import File** (Выберите файл импорта) необходимо цвести или указать с помощью средств просмотра xml-файл, из которого следует им портировать правила кэширования, как показано на рис. 11.15. Щелкните мы шью кнопку **Next** (Далее).

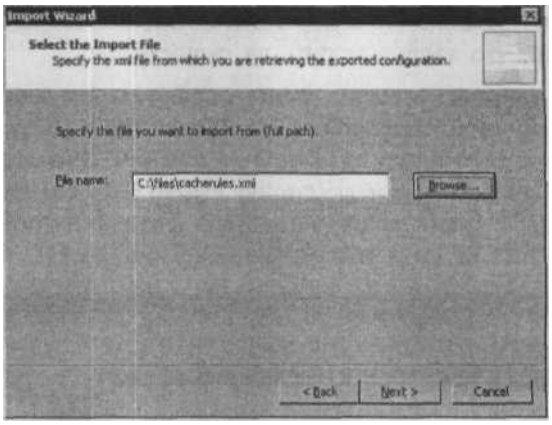


Рис. 11.15. Выбор файла импорта

6. На странице **Import Preferences** (Привилегированные параметры импорта) можно выбрать импортирование информации, зависящей от сервера (такой как устройства кэша и SSL-сертификаты), установив соответствующий флажок. По умолчанию информация, относящаяся к конкретному серверу, не импортируется. Эту информацию следует импортировать, если импортирование выполняется на тот же компьютер, с которого проводилось экспортирование. Если же подобную информацию импортировать на другую **машину,** может не запуститься

сервис брандмауэра, поскольку у этой машины нет импортированных на нее сертификатов.

7. На последней странице мастера приведена сводка введенной ранее информации. Если необходимо внести какие-либо изменения, используйте кнопку **Back** (Назад) для возврата на соответствующую страницу. При отсутствии такой необходимости щелкните мышью кнопку **Finish** (Готово) для завершения процесса импорта. Диалоговое окно проинформирует об успешном импортировании правил кэширования.

Только что описанный процесс экспортирует или импортирует все правила кэширования. Есть возможность экспорта или импорта только выбранных правил кэширования. Для этого выделите нужное правило кэширования и щелкните по нему правой кнопкой мыши, а затем из контекстного меню выберите левой кнопкой мыши команду **Export Selected** (Экспортировать выбранное) или **Import to Selected** (Импортировать в выбранное).

Конфигурирование загрузок содержимого из Интернета

Задания на загрузку содержимого из Интернета — удобное для администраторов средство, позволяющее автоматизировать процесс обновления кэшированного содержимого. В этом разделе показано, как выполнить следующие задачи:

- убедиться в том, что задание на загрузку из Интернета может быть выполнено;
- создать и настроить задание на загрузку из Интернета по расписанию;
- внести изменения в существующее задание на загрузку содержимого из Интернета;
- блокировать или удалить задание на загрузку содержимого;
- экспортировать или импортировать конфигурации заданий на загрузку содержимого из Интернета;
- немедленно запустить задание на загрузку содержимого из Интернета.

Рассмотрим каждую из перечисленных задач в следующих разделах.

Как убедиться в том, что задание на загрузку из Интернета может быть выполнено

Прежде чем задание на загрузку содержимого из Интернета будет выполнено, необходимо обеспечить следующее:

- настроить сеть Local Host (локальный хост) на ожидание запросов от клиентов Web-прокси;
- включить правила системной политики, разрешающие загрузку содержимого из Интернета;
- убедиться, что запущен сервис Job Scheduler (планировщик заданий).

Есть два способа удовлетворения перечисленных требований. Первый, самый легкий, автоматизирует процесс. Если попытаться создать задание на загрузку содержимого из Интернета до внесения изменений в конфигурацию, появится сообщение, извещающее о том, что следует внести эти изменения, и спрашивающее, согласны ли вы настроить установочные параметры (рис. 11.16).

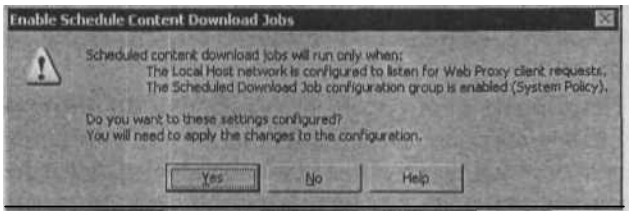


Рис. 11.16. Автоматическое внесение изменений в конфигурацию

Щелкните мышью кнопку **Yes** (Да) для внесения изменений в автоматическом режиме (необходимо также щелкнуть мышью кнопку **Apply** (Применить) в верхней части средней панели консоли управления, для того чтобы внесенные изменения подействовали).

Второй способ — выполнить изменения конфигурации вручную. В следующих разделах показано, как внести в конфигурацию каждое из этих изменений.

Настройка сети локального хоста

Для конфигурирования сети локального хоста на ожидание запросов от клиентов Web-прокси выполните следующие шаги.

1. На левой панели консоли управления (MMC) ISA Server 2004 раскройте окно, свя занное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если исполь зуется Enterprise Edition), и раскройте узел **Configuration** (конфигурация).
2. Щелкните кнопкой мыши узел **Networks** (Сети).
3. На средней панели консоли управления щелкните кнопкой мыши вкладку **Net works** (Сети).
4. Дважды щелкните кнопкой мыши элемент **Local Host** (Локальный хост) в списке **Networks** (Сети) или щелкните его правой кнопкой мыши и выберите команду **Properties** (Свойства). Эти действия вызовут появление на экране диалогового окна свойств локального хоста.
5. Щелкните кнопкой мыши вкладку **Web Proxy** (Web-прокси).
6. Установите флажок **Enable Web Proxy clients** (Разрешить клиенты Web-прокси) (по умолчанию он сброшен), как показано на рис. 11.17.

По умолчанию при разрешении клиентов Web-прокси HTTP-запросы будут разрешены, а SSL-запросы нет. Можно разрешить и SSL-сапросы, установив соответствующий флажок, а также задать, если необходимо, HTTP- и SSL-порты, отличные от применяемых по умолчанию (8080 и 8443).

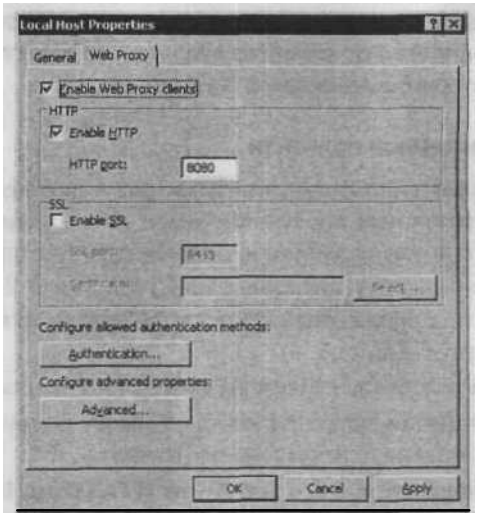


Рис. 11.17. Разрешение клиентов Web-прокси

ПРИМЕЧАНИЕ Вкладка CARP, показанная на рис. 11.17, появляется только в установке ISA Server 2004 Enterprise Edition; вариант установки Standard Edition (SE) не поддерживает протокол CARP (Cache Array Routing Protocol, протокол маршрутизации между кэш-серверами), поэтому на компьютерах с установкой SE будут видны только две вкладки General (Общие) и Web Proxy (Web-прокси).

Если разрешить SSL-запросы, то необходимо выбрать сертификат сервера, щелкнув мышью кнопку **Server Certificates** (Сертификаты сервера), выделив цветом имя сервера и щелкнув кнопкой мыши **Select** (Выбрать) для выбора из перечня сертификатов, установленных на сервере.

Необходимо также настроить следующие методы аутентификации:

- Digest (на основе хеша);
- Integrated (интегрированная, по умолчанию);
- Basic (базовая);
- SSL certificate (на основе SSL-сертификатов);
- RADIUS.

Для этого щелкните мышью кнопку **Authentication** (Аутентификация) и установите флажки методов аутентификации, которые предполагается использовать. На этой странице можно также установить флажок, требующий от всех пользователей подтверждения подлинности.

Можно выбрать домен аутентификации, используемый по умолчанию, RADIUS-серверы и настроить OWA-аутентификацию, основанную на формах.

ПРИМЕЧАНИЕ Более подробная информация о конфигурировании ISA Server для ожидания запросов от клиентов Web-прокси **и** настройке аутентификации для таких клиентов приведена в главе 4.

Включение правил системной политики

Для активизации правила системной политики, разрешающего загрузку содержимого из Интернета, выполните следующие шаги после конфигурирования сети локального хоста для ожидания запросов от клиентов Web-прокси.

1. На левой панели консоли управления (MMC) ISA Server 2004 раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется Enterprise Edition).
2. Щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
3. На правой панели консоли щелкните кнопкой мыши задачу **Show System Policy Rules** (Показывать правила системной политики).
4. На средней панели перейдите к правилу **Allow HTTP from ISA Server computers for Content Download Jobs** (Разрешить HTTP для заданий загрузки содержимого из Интернета с компьютеров ISA Server). На экране появится пиктограмма с направленной вниз стрелкой красного цвета, **означающая,** что правило заблокировано.
5. Для снятия блокировки или включения правила выполните следующие шаги: на правой панели **Tasks** (Задачи), в секции **System Policy Tasks** (Задачи системной политики) щелкните кнопкой мыши задачу **Edit System Policy** (Редактировать системную политику) или щелкните правой кнопкой мыши правило и выберите из контекстного меню команду **Edit System Policy** (Редактировать системную политику).
6. В разделе **Configuration Groups** (Группы конфигурации) перейдите к вложенной папке **Various** (Разные) и выберите строку **Scheduled Download** (Загрузка из Интернета по расписанию).

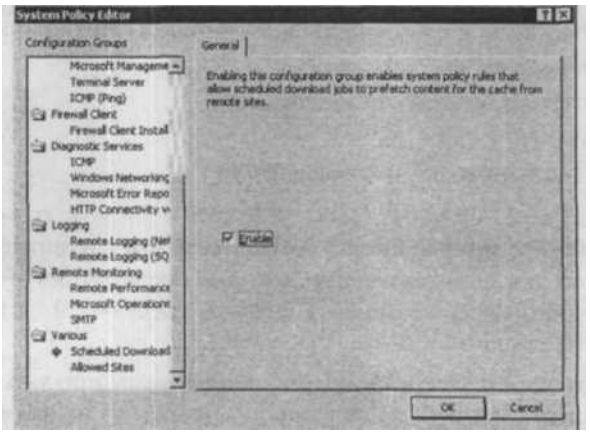


Рис. 11.18. Включение группы конфигурации системной политики

7. На вкладке **General** (Общие) установите флажок **Enable** (Включить), как показано на рис. 11.18.
8. Щелкните мышью кнопку OK.
9. Щелкните мышью кнопку **Apply** (Применить) в верхней части средней панели.

Запуск сервиса Job Scheduler

Для останова или запуска сервиса **Job Scheduler** (Планировщик заданий) с консоли управления Microsoft ISA Server 2004 выполните следующие шаги.

1. На левой панели консоли управления (MMC) **ISA Server 2004** раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется Enterprise Edition).
2. Щелкните кнопкой мыши узел **Monitoring** (Мониторинг).
3. Если на вкладке **Services** (Сервисы) средней панели состояние сервиса **Job Scheduler** (Планировщик заданий) обозначено **Stopped** (Остановлен), щелкните по нему правой кнопкой мыши и выберите из контекстного меню команду **Start** (Запустить) или выделите цветом этот сервис и щелкните левой кнопкой мыши задачу **Start Selected Service** (Запустить выбранный сервис) в области **Services Tasks** (Сервисные задачи) панели задач (рис. 11.19).

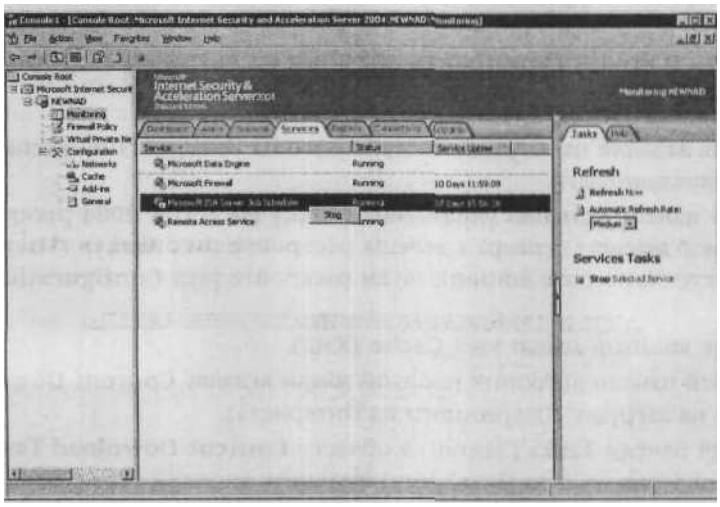


Рис. 11.19. Запуск и останов сервиса Job Scheduler (Планировщик заданий) с консоли управления сервера ISA

Запустить и остановить сервис можно также с консоли управления компьютером (Computer Management Console) в ОС Windows 2000/Server 2003, из узла **Services** (Службы), как это делается для других сервисов Windows. Щелкните мышью кнопку **Start** (Пуск), а затем щелкните правой кнопкой мыши строку **My Computer** (Мой компьютер) (или щелкните правой кнопкой мыши пиктограмму **My Computer** (Мой

компьютер) на рабочем столе) и щелкните левой кнопкой мыши команду **Manage** (Управление), затем раскройте узел **Services and Applications** (Службы и приложения) на левой панели и щелкните мышью подузел **Services** (рис. 11.20).

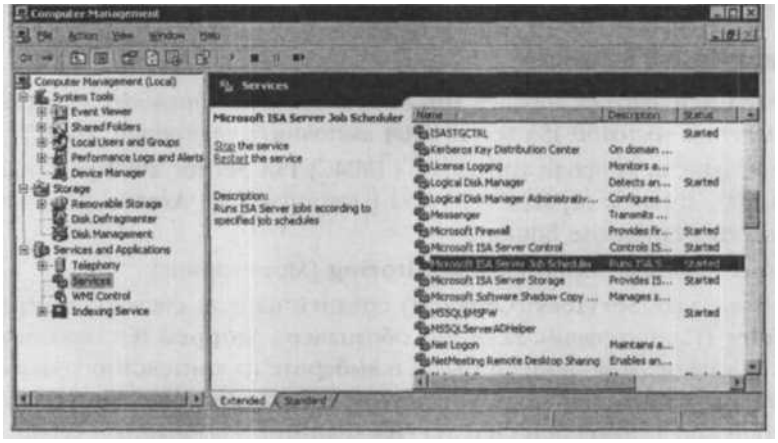


Рис. 11.20. Запуск или останов сервиса Job Scheduler (Планировщик заданий) с консоли Computer Management Console

Как создать и конфигурировать задания на загрузку содержимого из Интернета по расписанию

Для создания задания на загрузку содержимого из Интернета по расписанию выполните следующие шаги.

1. На левой панели консоли управления (MMC) ISA Server 2004 раскройте окно, связанное с именем сервера (сначала раскройте узел **Arrays** (Массивы), если используется Enterprise Edition), затем раскройте узел **Configuration** (Конфи гурация).
2. Щелкните кнопкой мыши узел **Cache** (Кэш).
3. На средней панели щелкните кнопкой мыши вкладку **Content Download Jobs** (Задания на загрузку содержимого из Интернета).
4. На правой панели **Tasks** (Задачи) в области **Content Download Tasks** (Задачи загрузки содержимого из Интернета) щелкните кнопкой мыши задачу **Schedule a Content Download Job** (Планировать задание на загрузку содержимого из Интернета). Запустится **New Content Download Job Wizard** (Мастер создания нового задания на загрузку содержимого).
5. На первой странице мастера дайте имя заданию на загрузку содержимого и щелкните мышью кнопку **Next** (Далее).
6. На странице **Download Frequency** (Частота загрузки) выберите частоту выпол нения задания. Можно выбрать из следующих вариантов: только один раз, по

завершении мастера; один раз по расписанию; ежедневно, еженедельно. Выберите подходящий вариант и щелкните мышью кнопку Next (Далее). 7. На странице Content Download (Загрузка содержимого) введите URL-адрес страницы интернет-сервера, с которой нужно загрузить содержимое. Можно также задать ограничения для задания (рис. 11.21), например отказаться от следования по ссылкам за пределы доменного имени URL-адреса, установить максимальную глубину ссылок на странице, задать максимальное число извлекаемых объектов и указать максимальное количество одновременных или параллельных TCP-со-единений, создаваемых для выполнения задания. По умолчанию флажок Do not follow link outside the specified URL domain name (Не следовать по ссылке за пределы доменного имени URL-адреса) сброшен, поэтому возможен переход по внешним ссылкам. По умолчанию также не задана максимальная глубина ссылок. Ограничение числа извлекаемых объектов по умолчанию равно 60 000, а максимальное количество параллельных соединений — 4. После установки необходимых параметров щелкните мышью кнопку Next (Далее).

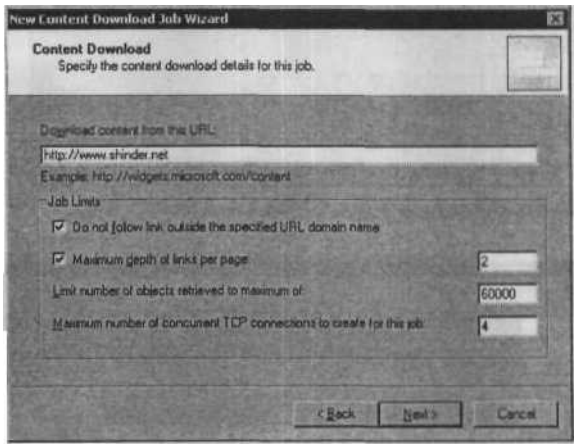


Рис. 11.21. Задание дополнительных параметров загрузки содержимого из Интернета

8. На странице Content Caching (Кэширование содержимого) можно определить, какое содержимое будет кэшироваться и время хранения объектов *в* кэше до того, как они превысят продолжительность жизни (TTL). Сначала укажите, что надо кэшировать: все содержимое; содержимое, в заголовках источника и запроса которого указано на необходимость кэширования, либо динамический контент; содержимое, в заголовках источника и запроса которого указано на необходи мость кэширования (этот вариант установлен по умолчанию).
9. Как видно из рис. 11.22, можно задать продолжительность жизни в соответствии с одним из трех вариантов: expire content according to the cache rule (ис течение жизненного срока контента в соответствии с правилом кэширования),

set the TTL if it's not defined in the response (установка продолжительности жизни, если она не задана в ответе) или override the object's TTL (переопределить продолжительность жизни объекта). По умолчанию срок жизни содержимого истекает в соответствии с правилом кэширования. Если выбран вариант переопределения продолжительности жизни объекта, можно задать новую продолжительность жизни (в минутах), которой будут помечаться загружаемые из Интернета объекты. По умолчанию она равна 60 мин. После задания параметров щелкните мышью кнопку Next (Далее).

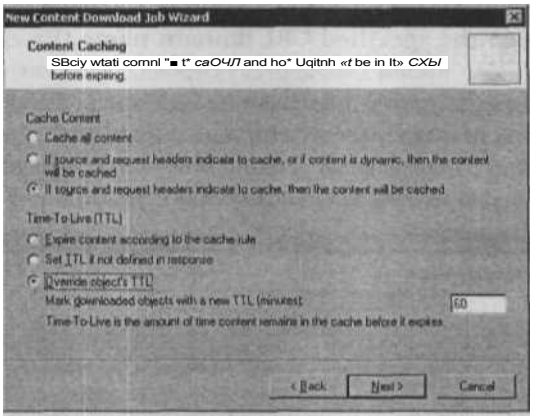


Рис. 11.22. Конфигурирование кэширования контента

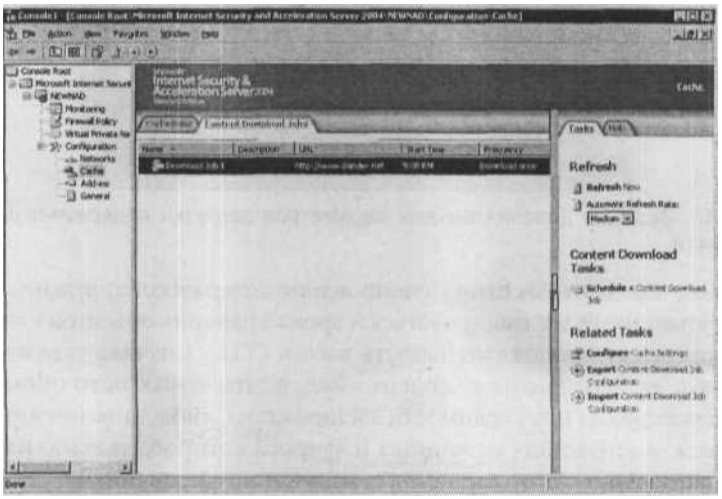


Рис. 11.23. Появление нового задания в списке заданий на загрузку содержимого из Интернета

10. На последней странице мастера приведена сводка сделанных вами установок. Если необходимо внести какие-либо изменения, используйте кнопку **Back** (Назад) для возврата на соответствующую страницу. В противном случае щелкните мышью кнопку **Finish** (Готово) для создания нового задания на загрузку содержимого из Интернета.

    Теперь созданное вами новое задание появится на вкладке **Content Download Jobs** (Задания на **загрузку** содержимого из Интернета) узла **Cache** (Кэш), на средней панели консоли управления, как показано на рис. 11.23.

Внесение изменений в существующее задание на загрузку содержимого из Интернета

Если необходимо модифицировать созданное прежде задание на загрузку содержимого, выделите его цветом на средней панели и щелкните кнопкой мыши задачу **Edit the selected job** (Редактировать выбранное задание) на правой панели **Tasks** (Задачи) или щелкните правой кнопкой мыши задание и выберите из контекстного меню команду **Properties** (Свойства).

На вкладке **General** (Общие) можно изменить имя задания и добавить необязательное описание.

На вкладке **Schedule** (Расписание) задаются дата и время начала загрузки из Интернета, а также при необходимости изменяется частота загрузки (один раз, ежедневно или еженедельно, в определенный день недели). Можно настроить частоту ежедневной загрузки, если выбран режим ежедневный. Как показано на рис. 11.24, задание может выполняться один раз в день или повторяться через заданные интервалы (часы или минуты). Есть возможность указать время дня, после

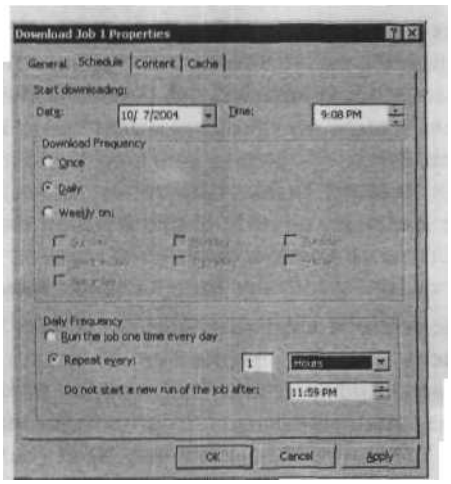


Рис. 11.24. Изменение расписания выполнения задания

которого не следует выполнять новый запуск задания.

На вкладке **Content** (Содержимое) можно изменить URL-адрес, с которого содержимое должно загружаться, и ограничения, заданные при создании этого задания с помощью мастера.

На вкладке **Cache** (Кэш) возможно изменение параметров, определяющих кэширование содержимого, и параметров продолжительности жизни, установленных во время создания задания с помощью мастера.

Блокирование или удаление задания на загрузку содержимого из Интернета

Если возникло желание отказаться от выполнения задания по расписанию, но остается вероятность его выполнения в будущем, можно заблокировать или отключить задание. Для этого выделите задание на средней панели и щелкните кнспкой мыши задачу **Disable the Selected Jobs** (Заблокировать выбранные задания) на правой панели **Tasks** (Задачи). Есть возможность выделить несколько заданий и заблокировать их одновременно. Другой вариант — щелкнуть правой кнопкой мыши задание и выбрать из контекстного меню команду **Disable** (Блокировать).

Чтобы убрать задание целиком, если оно не будет применяться в будущем, можно удалить его, выделив на средней панели и щелкнув кнопкой мыши задачу **Delete the Selected Jobs** (Удалить выбранные задания) на правой панели **Tasks** (Задачи). Есть возможность выделить несколько заданий и удалить их все одновременно. Другой вариант — щелкнуть правой кнопкой мыши задание и выбрать из контекстного меню команду **Delete** (Удалить).

Экспорт и импорт конфигурации задания на загрузку содержимого из Интернета

Конфигурацию задания на загрузку содержимого из Интернета можно экспортировать, сохранив ее в файле с расширением xml, так же, как экспортировались установочные параметры других конфигураций ISA Server 2004. Для этого выделите задание на правой панели и щелкните кнопкой мыши задачу **Export Content Download Job Configuration** (Экспортировать конфигурацию задания на загрузку содержимого) из области **Related Tasks** (Связанные задачи) правой панели **Tasks** (Задачи). Можно также щелкнуть правой кнопкой мыши выбранное задание и левой кнопкой мыши щелкнуть в контекстном меню команду **Export Selected** (Экспортировать выбранное). При этом запускается **Export Wizard** (Мастер экспорта).

На первой странице мастера щелкните мышью кнопку **Next** (Далее). На странице **Export Preferences** (Экспорт предпочтений) укажите, нужно ли экспортировать конфиденциальную информацию. Если выбран этот вариант, необходимо ввести и подтвердить пароль, с помощью которого будет шифроваться конфиденциальная информация. Щелкните мышью кнопку **Next** (Далее).

Введите или задайте с помощью средств просмотра путь для сохранения xml-файла. На этой странице можно ввести путь к файлу и его имя, но нельзя создать новую папку.

На последней странице мастера приведены все сделанные вами установки. Если нужно что-то изменить, воспользуйтесь кнопкой **Back** (Назад) для возврата на соответствующую страницу. В противном случае щелкните мышью кнопку **Finish** (Готово) для завершения процесса экспорта. Об успешном экспортировании конфигурации сообщит диалоговое окно.

Сохраненное задание на загрузку содержимого из Интернета можно импортировать с данного или другого компьютера с установленным сервером ISA Server 2004 во многом аналогичным способом. Щелкните кнопкой мыши задачу **Import Content Download Job Configuration** (Импортировать конфигурацию задания для загрузки содержимого из Интернета) в разделе **Related Tasks** (Связанные задачи) правой панели **Tasks** (Задачи). Запустится **Import Wizard** (Мастер импорта). На его первой странице щелкните мышью кнопку **Next** (Далее).

Введите или укажите с помощью средств просмотра путь к файлу, из которого необходимо импортировать конфигурацию и щелкните мышью кнопку **Next** (Далее). Выберите, нужно ли импортировать информацию, относящуюся к конкретному серверу (такую как устройства кэша и сертификаты). По умолчанию такая информация не импортируется. Ее следует импортировать, если импорт выполняется на тот компьютер, с которого эта информация была ранее экспортирована. Если же импортировать относящиеся к конкретному серверу сведения на другой компьютер и выбрать режим их импорта, сервис брандмауэра может не запуститься, если на новом компьютере не установлены те же самые сертификаты. После сделанных вами установок щелкните мышью кнопку **Next** (Далее).

На последней странице мастера приведены все сделанные вами установки. Если нужно что-то изменить, воспользуйтесь кнопкой **Back** (Назад) для возврата на соответствующую страницу. В противном случае щелкните мышью кнопку **Finish** (Готово) для завершения процесса импорта. Об успешном импортировании конфигурации сообщит диалоговое окно.

Немедленное выполнение задания на загрузку содержимого из Интернета

Помимо выполнения заданий на загрузку содержимого из Интернета по расписанию, настроенному вами, можно выполнить любое существующее подобное задание вручную, в любое время. Для этого выделите нужное задание на средней панели и щелкните кнопкой мыши задачу **Start Selected Jobs** *Now* (Запустить выбранные задания сейчас) в разделе **Content Download Tasks** (Задачи загрузки содержимого из Интернета) правой панели **Tasks** (Задачи). Есть возможность выделить несколько заданий и запустить их одним щелчком кнопки мыши.

Кроме того, можно щелкнуть правой кнопкой мыши задание, которое нужно выполнить, и выбрать из контекстного меню команду **Start** (Запустить).

Резюме

Корпорация Microsoft, продвигая на рынке ISA Server 2004, делает особый акцент на его функциональных возможностях как брандмауэра и VPN-шлюза, но этот продукт также предоставляет компаниям приемлемую реализацию Web-кэширования, позволяющую сэкономить на **покупке** отдельного сервера кэширования при покупке брандмауэров, в состав которых эта функция не включена (а таких большинство).

Функциональная возможность кэширования ISA Server 2004 повышает эффективность сети, обеспечивая ускорение доступа **внутренних** пользователей к внешним Web-сайтам с помощью прямого кэширования, а также доступа внешних пользователей, соединяющихся с внутренними Web-сайтами, с помощью обратного кэширования.

В более сложных сетевых средах может использоваться несколько компьютеров с ISA Server 2004 в системах распределенного или иерархического кэширования, обеспечивающих максимально возможную производительность. Распределенное кэширование распределяет или распространяет кэшированные Web-объекты на два или несколько серверов кэширования. Все эти серверы находятся на одном сетевом уровне. В системе иерархического кэширования серверы располагаются на разных уровнях сети. Вышестоящие (upstream) серверы кэширования взаимодействуют с нижестоящими прокси-серверами. Например, в каждом филиале установлен сервер кэширования. Эти серверы связываются с массивом кэширования в центральном офисе. Запросы обслуживаются сначала из локального кэша, затем из централизованного кэша и только после этого отправляются на сервер в Интернете.

ISA Server 2004 применяет для взаимодействия с серверами Web-кэширования протокол маршрутизации между кэш-серверами (Cache Array Routing Protocol, CARP) — это хеш-ориентированный протокол, позволяющий объединять многочисленные прокси кэширования в единый логический кэш и использовать хеш-функцию для определения кэша, на который должен быть отправлен запрос. ISA Server 2004 применяет правила кэширования для определения сохраняемых типов содержимого и конкретных способов обработки содержимого при запросе объектов из кэша.

ISA Server 2004 помимо его конфигурации, устанавливаемой по умолчанию (только в качестве брандмауэра), может функционировать в смешанном режиме: как брандмауэр и сервер кэширования или как изолированный сервер Web-кэширования. В этой главе рассматривались принципы Web-кэширования и способы конфигурирования компьютера с ISA Server 2004 для выполнения кэширования в вашей организации.

Краткое резюме по разделам

а Существуют два основных типа Web-кэширования: прямое и обратное. ISA Server 2004 может выполнять оба.

Е Прямое кэширование обладает важным достоинством, делая доступ для внутренних пользователей более быстрым, поскольку они получают Web-объекты (такие как страницы, графику и звуковые файлы) с помощью быстрого соединения локальной сети, обычно 100 Мбит/сек и больше, взамен более медленного интернет-соединения, возможно, со скоростью 1,5 Мбит/сек.

И Главное базовое преимущество прямого кэширования, обеспечиваемого ISA Server 2004, — уменьшение расходов за счет снижения потребления полосы пропускания при интернет-соединении.

И Обратное кэширование уменьшает трафик во внутренней сети и ускоряет доступ внешних пользователей к собственным сайтам компании. Часто запрашиваемые объекты на внутренних Web-серверах кэшируются на границе сети, на прокси-сервере, таким образом, снижая нагрузку на Web-серверы.

И Сценарий обратного кэширования обладает двумя принципиальными достоинствами: обратное кэширование снижает нагрузку на полосу пропускания внутренней сети и сохраняет доступность Web-содержим ого при отключенном от сети Web-сервере.

В Несколько серверов Web-кэширования могут использоваться вместе для обеспечения более эффективного кэширования. Существуют две основные структуры кэширования, использующие множественные совместно работающие серверы кэширования: распределенная и иерархическая.

В Можно комбинировать методы распределенного *и* иерархического кэширования для создания гибридной структуры кэширования. Подобная комбинация позволяет достичь наилучших результатов, повышая производительность и эффективность.

а Существует ряд различных протоколов, которые могут применяться для взаимодействия серверов Web-кэширования. Самые популярные из них — CARP, ICP, HTCP, WCCP и Cache digests.

0 ISA Server 2004 использует CARP-протокол для взаимодействия серверов распределенного Web-кэширования.

В При включенном распределенном кэшировании клиенты Web-прокси могут использовать CARP-протокол для определения местонахождения сервера ISA, содержащего объекты.

m Фильтр Web-прокси — это средство, применяемое ISA Server 2004 для реализации функции кэширования.

В Кэш — это область на жестком диске сервера ISA, используемая для хранения запрашиваемых Web-объектов. Можно управлять размером области на диске,

отведенной под кэш (и следовательно, максимальным размером кэша). Кроме того, можно задать максимальный размер объектов, которые могут кэшироваться, для того чтобы несколько очень больших объектов не «съели» все пространство, отведенное под кэш.

И Кэширование использует оперативную память. Объекты кэшируются как в RAM, так и на диск. Из оперативной памяти их можно извлечь быстрее, чем с диска. ISA Server 2004 позволяет определить, какая часть (в процентах) оперативной памяти (random access memory, RAM) может отводиться под кэш (по умолчанию сервер ISA использует 10% RAM, а остальные объекты кэшируются только на диск).

и Активизация режима кэширования на компьютере с ISA Server 2004 выполняется конфигурированием устройства кэша (cache drive). Настройка устройства кэша включает прямое и обратное кэширование.

И Файл, в котором хранятся объекты кэша, называется dirl.cdat. Он находится в папке urlcache, на отведенном под кэш диске. Этот файл также называют файлом содержимого кэша.

0 ISA Server 2004 применяет правила кэширования, позволяющие задать типы содержимого, которое будет сохраняться в кэше, и точные способы обработки этого содержимого при выполнении запроса объектов, содержащихся в кэше.

И Помимо управления типом содержимого и размером объектов правило кэширования позволяет управлять способом извлечения объектов из кэша и их обслуживания сервером ISA. Он определяется достоверностью объекта (validity of the object).

И При наличии множественных правил кэширования они обрабатываются по порядку, от первого до последнего, последним обрабатывается правило кэширования, установленное по умолчанию.

И Функция загрузки содержимого из Интернета применяется для планирования загрузки сервером ISA Server 2004 содержимого из Интернета в заранее определенное время, для того чтобы клиентам Web-прокси, запросившим объекты, предоставлялись из кэша их обновленные версии.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»),** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Что такое негативное кэширование?

О: Негативное кэширование — термин, используемый для описания функциональной возможности сервера ISA продолжать обслуживание Web-страниц и Web-

объектов из кэша сервера ISA даже по истечении продолжительности жизни (Time To Live, TTL) этих объектов. Обычно объекты сохраняются в кэше определенный период времени, прежде чем последует их обновление с Web-сервера, на котором они были созданы. При отсутствии негативного кэширования кэшированный объект становится недоступным по истечении его продолжительности жизни (до тех пор, пока не будет повторного обновления объекта с исходного Web-сервера). Применяя негативное кэширование, сервер ISA способен продолжать обслуживать объект, срок жизни которого истек.

В: Почему корпорация Microsoft использует CARP-протокол для взаимодействия серверов кэширования на базе ISA Server 2004, а не один из популярных протоколов?

О: Коротко — для эффективности. CARP-протокол позволяет серверам кэширования и клиентам Web-прокси определять местонахождение кэшированных объектов с помощью хеш-функции. Такой подход устраняет ненужный трафик и дублирование кэшируемых объектов на серверах кэширования.

В: Что обозначает событие с регистрационным номером 14193 «Cache was initialized with less memory cache than configured» (Кэш инициализирован с объемом памяти, меньшим, чем задано в конфигурации)?

О: Это событие фиксируется, когда на компьютере с сервером ISA Server 2004 нет достаточного объема свободной памяти для выделения под кэш той доли в процентах, которая была задана в конфигурации. Если свободной памяти не хватает, для кэширования выделяется меньший объем, но это событие регистрируется в журнале событий.

Bs Что происходит, когда кэш заполнен? Препятствует ли это кэшированию новых объектов?

О: Нет. Новые объекты все равно будут кэшироваться. Если кэш заполнен, ISA Server 2004 уничтожит некоторые объекты в кэше, освобождая место для новых объектов. URL-объекты в кэше стираются в соответствии со встроенной логикой, обеспечивающей удаление недавно использованных объектов в последнюю очередь.

В: Что означает появляющееся при старте компьютера с ISA Server 2004 сообщение о том, что кэш не инициализирован должным образом?

О: Это сообщение, как правило, означает, что работа на компьютере с ISA Server 2004 не была завершена корректно. Например, если из-за скачка напряжения компьютер с сервером ISA выключился, не пройдя нормальный процесс завершения сеанса работы, может появиться такое сообщение, так как сервис ISA Server был остановлен аварийно.

В: Если одна маршрутная конфигурация указана в задании на загрузку содержимого из Интернета, а другая — в правилах цепочек для маршрутизации Web-запросов, какая из них будет применяться?

О: Маршрутная конфигурация, заданная в правилах цепочек для маршрутизации Web-запросов, обладает более высоким приоритетом по сравнению с любой конфигурацией, указанной в задании на загрузку содержимого из Интернета. Таким образом, если есть правило цепочек серверов, определяющее, что запрос следует маршрутизировать, он будет маршрутизироваться, даже если в задании на загрузку содержимого из Интернета задан отказ от маршрутизации. Правила цепочек для определения маршрутизации Web-запросов позволяют определять маршруты Web-запросов в соответствии с пунктом назначения или адресатом. С помощью этих правил можно направить запрос от клиента Web-прокси на конкретный вышестоящий (upstream) сервер ISA, перенаправить его на определенный Web-сайт или получить запрошенный объект непосредственно от заданного адресата.

В: Выполняет ли ISA Server 2004 активное кэширование? Если нет, то почему?

О: Активное кэширование поддерживалось ISA Server 2000. Задачей этого типа кэширования было разрешение серверу ISA автоматически выходить в Интернет и получать обновленные версии популярных Web-объектов до того, как они будут запрошены клиентами. Сервер ISA отслеживал продолжительность жизни наиболее часто запрашиваемых объектов и, когда она была на исходе, обновлял эти объекты из Интернета, препятствуя истечению их жизненного срока. Этот превентивный подход предназначался для сохранения свежих копий популярных объектов в кэше и сокращения времени обновления объектов с истекающей продолжительностью жизни, в момент обращения к ним клиента. Однако корпорация Microsoft проверила реальное применения активного кэширования и установила, что очень часто оно не улучшало общую сетевую обстановку из-за потребления большей части пропускной способности на автоматическое обновление объектов. Таким образом, эта функция отключена в ISA Server 2004.

В: Каковы возможности кэширования ISA Server 2004 по сравнению с аналогичными функциями, предоставляемыми его конкурентами, разработанными сторонними организациями?

О: Одно из главных преимуществ ISA Server 2004 — сочетание функций брандмауэра и возможности кэширования. Большинство популярных брандмауэров предлагают кэширование только как дополнительный модуль или в виде отдельного продукта (за дополнительную плату). Единственный основной конкурент, предлагающий обе названные функции, — устройства SG (SG appliances) компании Blue Coat Systems.

Существует ряд реализаций сторонних фирм, включающих только кэширование. Одни реализации, такие как Cisco's Content Engines (которые рекламируются как маршрутно-интегрированные системы доставки содержимого, включающие кэширование), обладают и другими функциями, их разные модели имеют очень широкий диапазон цен: меньше тысячи — свыше 70 000 долларов. Другие, такие как Squid со свободно распространяемым исходным кодом, бесплат-

ны, но очень сложны в конфигурировании, требуют опыта работы в ОС Linux/UNIX и используют интерфейс командной строки и файлы конфигурации, похожие на старые ini-файлы в ОС Windows. Еще одна популярная реализация кэширования — Volera Excelerator фирмы Novell, работающая под управлением Linux и Windows. Она также относительно дорога, цена колеблется от 3 595 долларов до 44 995 со среднего класса лицензией масштаба предприятия (Enterprise license) (1 Гб), стоившей 12 945 долларов во время написания этой книги. Предлагаемые приложения кэширования отличаются поддерживаемыми функциями и используемыми протоколами кэширования. Например, разработки компании Blue Coat (раньше CacheFlow) поддерживают прямое, обратное, иерархическое и распределенное кэширование, как и сервер ISA. В них также реализованы активное кэширование и кэширование потокового мультимедиа. Обозреватели клиентов конфигурируются с помощью файла автоконфигурации прокси (Proxy Autoconfiguration, PAC), а обратное кэширование выполняется с использованием коммутатора уровня 4/7 (layer 4/7 switch) или маршрутизатора, поддерживающего протокол WCCP. Фирма Blue Coat Systems поддерживает протоколы ICP, HTCP и WCCP. Программное средство управления контентом Novell Excelerator может использовать протоколы ICP, специализированный HTTP и WCCP и также поддерживает иерархическое, распределенное, прямое и обратное кэширование. Кэширование потокового мультимедиа обеспечивается дополнительным модулем Media Excelerator (за отдельную плату). ПО Squid функционирует в ОС Linux/UNIX и поддерживает набор разнообразных протоколов: ICP, HTCP, CARP, Cache digests и WCCP. Оно обеспечивает прямое, обратное, иерархическое и распределенное кэширование, но не поддерживает активного кэширования потокового мультимедиа. В кэширующий прокси Squid не включены средства высокой готов ност и/балансировки нагрузки сети, имеющиеся у сервера ISA и программных средств фирм Blue Coat и Novell. ISA Server в противовес разработкам сторонних фирм содержит собственную реализацию кэширования, выгодно отличающуюся соотношением цены и качества.

Глава 12

Применение ISA Server 2004 для наблюдения, ведения журналов и создания отчетов

Основные темы главы:

- **Иструментальная панель ISA Server 2004**
- **Создание и конфигурирование оповещений в ISA Server 2004**
- **Наблюдение за связями, сеансами и службами в ISA Server 2004**
- **Работа с журналами и отчетами в ISA Server 2004**
- **Использование монитора производительности в ISA Server 2004**

Введение

Одно из самых распространенных нареканий к брандмауэрам практически всех производителей — недостаток средств наблюдения и ведения журналов. От брандмауэра требуется не только защита от различных интернет-атак и управление исходящим и входящим трафиком, но и возможность документирования наружных вторжений и атак, а также отслеживание использования Интернета своими пользователями.

Журналы и отчеты преследуют несколько важных целей:

- исследование неудавшихся и успешных вторжений и атак, позволяющее пред принять дополнительные профилактические меры;
- доказательная документация при судебных расследованиях гражданских или уголовных деяний злоумышленников, хакеров или содействующих им лиц, не законно использующих вычислительные сети;
- отслеживание использования канала передачи данных при планировании рас ширения сети;
- установка средств наблюдения за производительностью для планирования бу дущих требований к пропускной способности канала передачи данных;
- обоснование перед руководством резервирования необходимых бюджетных средств;
- документы для руководства и внешних управляющих структур, подтверждающие соответствие всех действий общей политике и инструкциям.

В ISA Server 2004 включено множество средств, которые могут использоваться для наблюдения за действиями ISA Server, создания и настройки *оповещений* (alerts) о происходящих изменениях, создания отчетов для обобщения информации в удобочитаемом виде и документирования производительности ISA Server. Все эти инструменты размещены в узле **Monitoring** (Наблюдение), доступном через дерево консоли в левой панели консоли управления ISA Server 2004.

> **СОВЕТ** Чтобы получить доступ к узлу **Monitoring** (Наблюдение) в ISA Server 2004 нужно раскрыть название ISA Server в левой части дерева консоли и выбрать пункт **Monitoring** (Наблюдение). В версии Enterprise Edition необходимо раскрыть узел **Arrays** (Массивы) в левой части дерева консоли, затем название ISA Server, за которым необходимо установить наблюдение и, наконец, выбрать пункт **Monitoring** (Наблюдение).

В этой главе будут исследованы инструментальные средства, встроенные в ISA Server 2004 и представлены пошаговые инструкции по их использованию. Особое внимание будет уделено следующим вопросам:

- **использование** инструментальной панели ISA Server 2004 (в каждом разделе главы):

- создание и настройка оповещений;
- сеансы и службы наблюдения в ISA Server 2004;
- конфигурирование журналов и создание отчетов;
- использование монитора производительности в ISA Server — специально настро енного экземпляра системного монитора Windows Server, установленного с ISA Server.

Инструментальная панель ISA Server 2004

Инструментальная панель (Dashboard) — совершенно новая возможность в ISA Server 2004, предоставляющая администратору ISA Server удобный способ наблюдения за происходящим в различных наблюдаемых подузлах. Для более подробных сведений можно щелкнуть мышью на отдельных вкладках **Alerts** (Оповещения), Sessions (Сеансы), **Services** (Службы), **Reports** (Отчеты), **Connectivity** (Связи) и **Logging** (Ведение журналов), для получения только самых общих сведений об инструментальной панели имеется простой интерфейс. Конфигурация инструментальной панели «по умолчанию» ISA Server 2004 Enterprise Edition представлена на рис. 12.1.

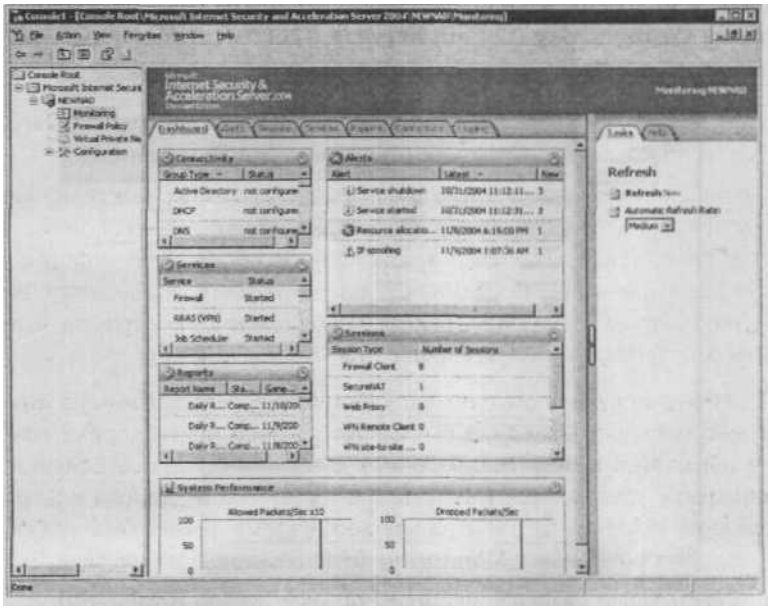


РИС. **12.1.** Инструментальная панель (Dashboard) на компьютере с установленным ISA Server 2004 Enterprise Edition

ПРИМЕЧАНИЕ В интерфейсе **Monitoring** (Наблюдение) для ISA Server 2004 Enterprise Edition существует дополнительная вкладка с названием **Configuration Status** (Статус конфигурации).

Инструментальная панель также предоставляет информацию о производительности системы. Например, можно наблюдать в графической форме количество корректно отправленных пакетов в секунду (кратно 10) и число отбракованных пакетов в секунду.

Каждый раздел инструментальной панели содержит значок, обозначающий статус данной области:

- **галочка внутри зеленого кружка** указывает, что все в порядке.
- **восклицательный знак внутри желтого треугольника** обозначает предупреждение.
- **крестик в красном кружке** указывает на проблему или возможную проблему.

Можно считать инструментальную панель началом выявления проблем или неисправностей ISA Server. Некоторые задачи, например отмену оповещений, можно выполнять непосредственно в инструментальной панели.

Можно «свернуть» различные разделы инструментальной панели, если они в данный момент не нужны. Достаточно щелкнуть значок в правом верхнем углу раздела, который должен быть «свернут» (кружок **с** двумя маленькими стрелками вверх) и раздел будет «свернут», открывая больше места для других разделов. На рис. 12.2 «свернуты» разделы **Connectivity** (Связи), **Reports** (Отчеты) и **Alerts** (Оповещения).

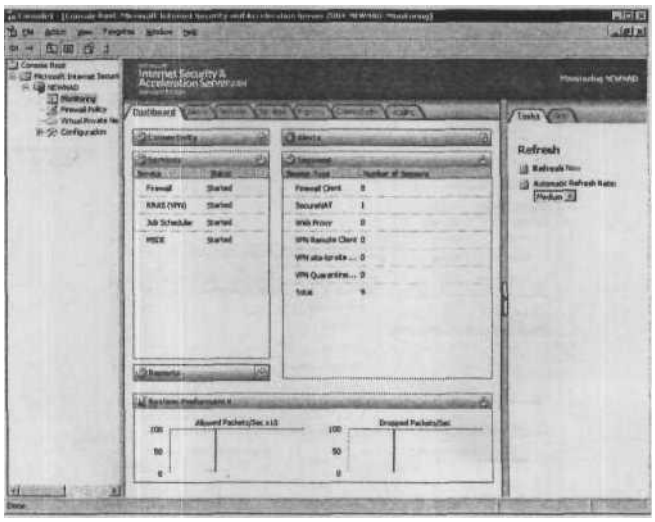


Рис. 12.2. Свертывание разделов инструментальной панели (Dashboard)

Разделы инструментальной панели

По умолчанию панель инструментов разделена на шесть разделов: ■ **Connectivity** (Связи);

- **Services** (Службы);
- **Reports** (Отчеты);
- **Alerts** (Оповещения);
- **Sessions** (Сеансы);
- **System Performance** (Производительность системы).

Раздел Connectivity

Раздел инструментальной панели **Connectivity** (Связи) позволяет наблюдать связи между машиной ISA Server и другими компьютерами. Можно следить за определенными компьютерами в сети или даже связываться с определенным Web-сервером по заданному значению URL

Однако перед тем как получить возможность отслеживания определенных компьютеров необходимо создать *верификатор связи* (connectivity verifier) и присвоить его группе. До этого в разделе **Connectivity** (Связи) все типы групп будут помечены как **«Not configured»** (Ненастроенные) (рис. 12.3).

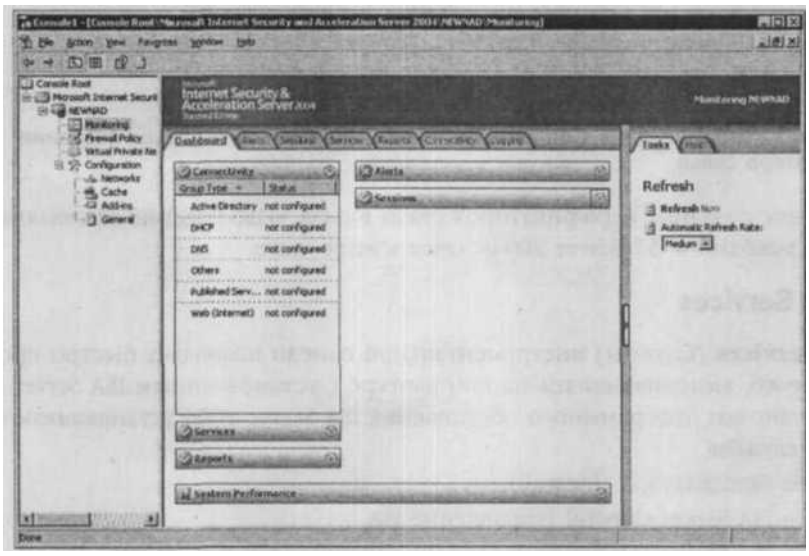


Рис. 12.3. Статус раздела Connectivity (Связи) по умолчанию до создания верификатора связи

Компьютеры могут быть причислены к следующим группам:

- Active Directory;
- DHCP;
- DNS;
- Опубликованные серверы (Published Servers);

- Web (Интернет).

После того как верификаторы связи созданы и присвоены группе (или группам), статус настроенных типов групп будет выглядеть, как показано на рис. 12.4

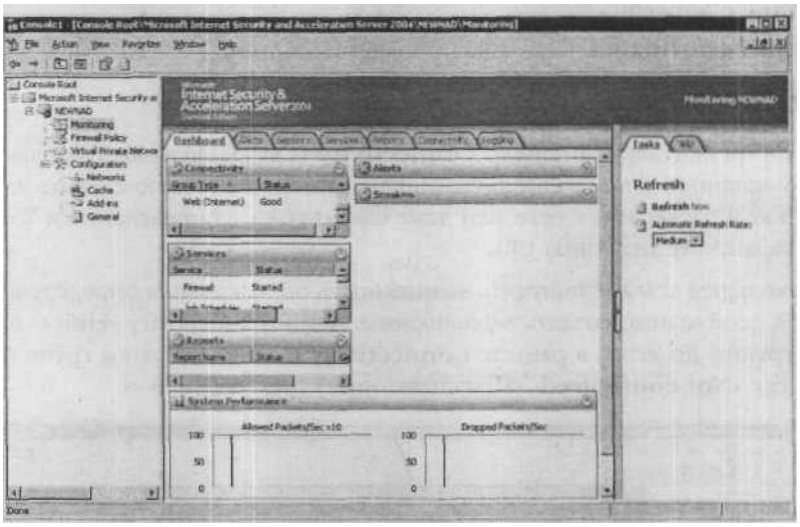


Рис. 12.4. Статус раздела Connectivity (Связи) по умолчанию после создания верификатора связи

Процесс создания верификаторов связи в разд. «Наблюдение за связями, сеансами и службами в ISA Server 2004» далее в этой главе.

Раздел Services

Раздел **Services** (Службы) инструментальной панели позволяет быстро проверить статус служб, выполняющихся на компьютере с установленным ISA Server. В процессе установки программного обеспечения ISA Server 2004 устанавливаются следующие службы:

- служба брандмауэра (firewall);
- служба ISA Server Control (управление ISA Server);
- служба ISA Server Job Scheduler (планировщик задач ISA Server);
- Microsoft Data Engine, MSDE (машина баз данных корпорации Microsoft).

Каждая из этих служб будет обсуждаться подробно в разделе «Наблюдение за связями, сеансами и службами в ISA Server 2004» далее в этой главе.

В разделе **Services** (Службы) инструментальной панели можно увидеть статус каждой службы (независимо от того, выполняются они или остановлены). В брандмауэрах ISA Server 2004 Enterprise Edition отображается третий столбец, содержащий информацию о том, сколько служб выполняется из общего количества (рис. 12.5).

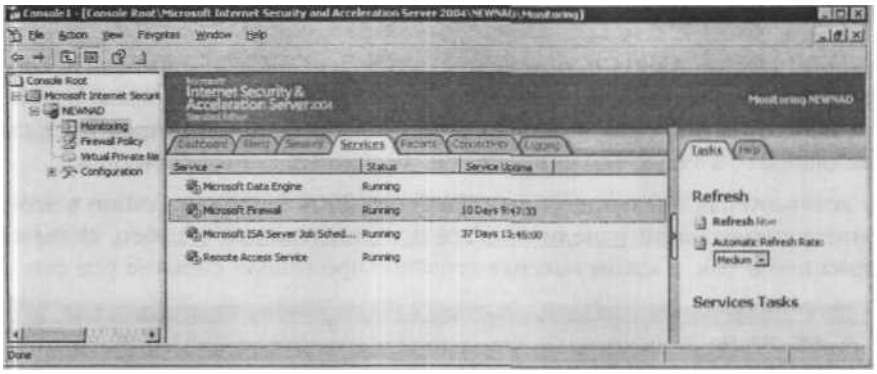


Рис. 12.5. Раздел Services (Службы) инструментальной панели ISA Server 2004

Раздел Reports

В разделе **Reports** (Отчеты) инструментальной панели представлены названия созданных отчетов, их статус (создаются или завершены), а также дата создания (рис 12.6).

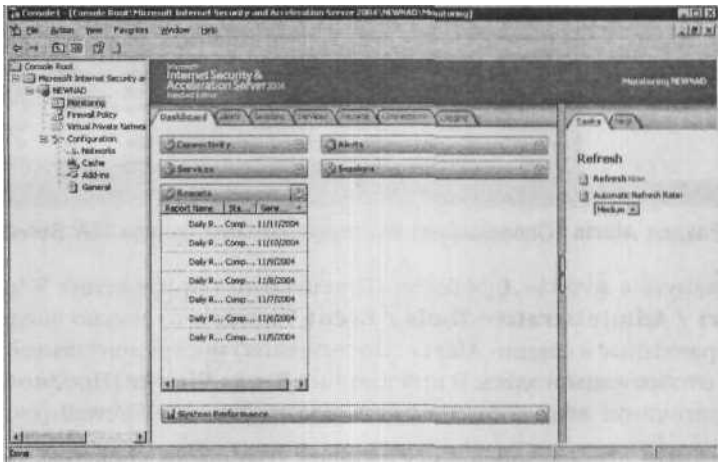


Рис. 12.6. Раздел **Reports** (Отчеты) инструментальной панели ISA Server 2004

В этом разделе можно определить, закончено или нет создание отчетов, начатое вручную или по расписанию. Можно открыть любой отчет из списка (если его создание завершено) непосредственно в интерфейсе инструментальной панели, дважды щелкнув мышью на названии отчета в столбце *Report Name* (Название отчета).

Планирование автоматического и ручного создания отчетов, а также настройка содержимого отчетов будет обсуждаться далее в этой главе.

Раздел Alerts

Интерфейс раздела **Alerts** (Оповещения) позволяет быстро определить события, которые были занесены в журнал компьютера ISA Server, время, когда произошло то или иное событие, серьезность события (информационное, предупреждающее или же ошибка), а также число процессов, связанных с этим событием.

На компьютерах с установленным ISA Server 2004 Enterprise Edition в этом разделе инструментальной панели имеется дополнительный столбец, содержащий информацию о том, в каком массиве серверов произошло событие (см. рис. 12.7).

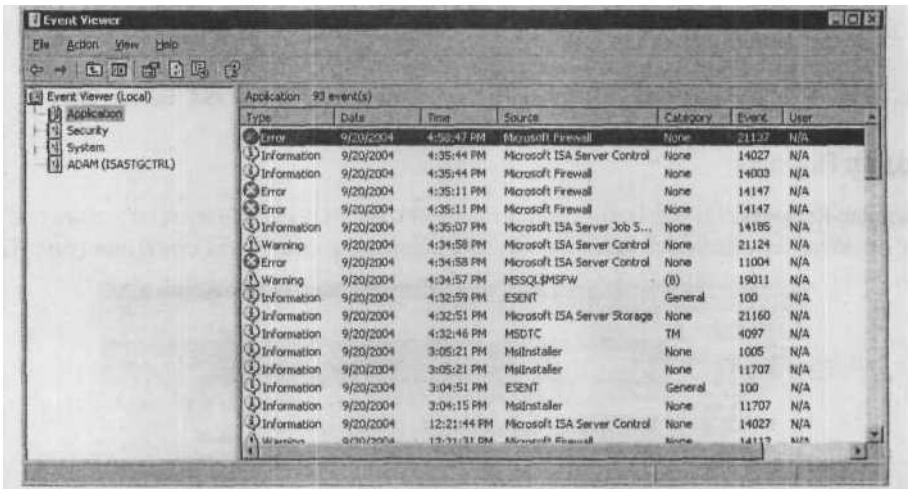


Рис. 12.7. Раздел Alerts (Оповещения) инструментальной панели ISA Server 2004

Если заглянуть в журнал *Application* (Приложения) приложения Windows Event Viewer **(Start / Administrative Tools / Event Viewer),** то можно увидеть, что события, отображенные в секции **Alerts** (Оповещения) **инструментальной** панели ISA Server 2004, отображены и здесь. В приложении **Event Viewer** (Просмотр событий) в качестве источника этих событий будет указан Microsoft Firewall (см. рис. 12.8).

> **ПРИМЕЧАНИЕ** Приложение **Event Viewer** (Просмотр событий) также показывает события, связанные со службой Microsoft ISA Server Control, службой Microsoft Server Job Scheduler и другими службами ISA Server, которые не отображаются в инструментальной панели ISA Server или во вкладке **Alerts** (Оповещения). Таким образом, всегда необходимо обращаться к приложению Event Viewer для получения более полного списка событий, происшедших на компьютере ISA Server.

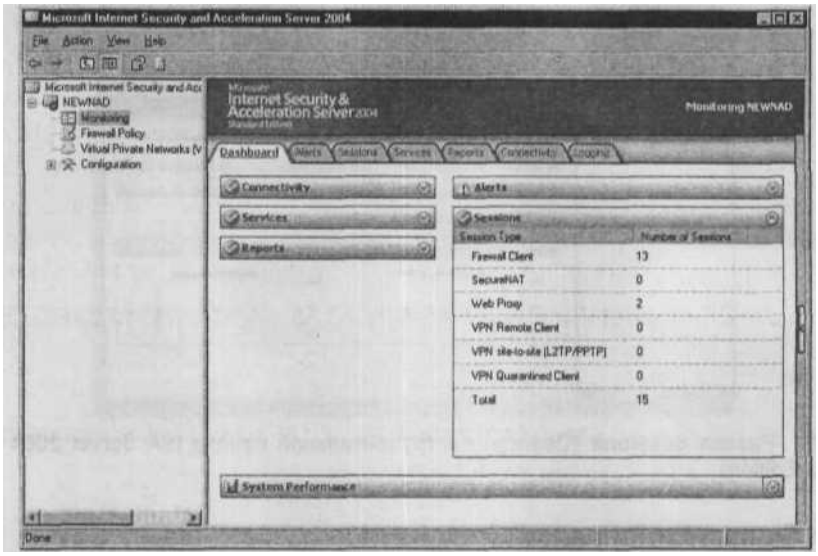


Рис. 12.8. В журналах приложения Event Viewer (Просмотр событий) показаны события службы брандмауэра, отображаемые в инструментальной панели

Раздел Sessions

Раздел Sessions (Сеансы) инструментальной панели ISA Server 2004 упрощает просмотр наблюдаемых типов сеансов и число сеансов, активированных брандмауэром ISA Server 2004. Имеются следующие типы сеансов:

- клиенты брандмауэра (firewall clients);
- клиенты SecureNAT;
- клиенты Web-прокси;
- клиенты удаленного доступа VPN;
- соединения VPN узел-в-узел;
- клиенты VPN-карантина.

Показывается и общее число сеансов, как это представлено на рис. 12.9.

Открыть вкладку **Sessions** (Сеансы) в интерфейсе инструментальной панели для просмотра подробных сведений о каждом отдельном сеансе можно, дважды щелкнув мышью заголовок раздела **Sessions** (Сеансы). Как использовать информацию вкладки **Sessions** (Сеансы), будет рассказано далее в этой главе.

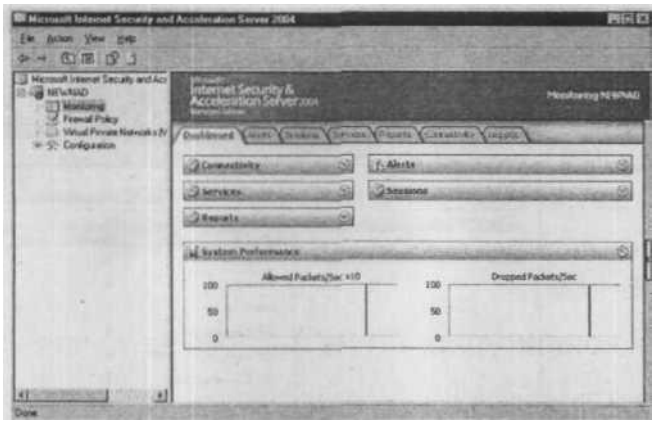


Рис. 12.9. Раздел Sessions (Сеансы) инструментальной панели ISA Server 2004 (Standard Edition)

Раздел System Performance

Интерфейс раздела **System Performance** (Производительность системы) инструментальной панели ISA Server 2004 позволяет «на скорую руку» проверить два наиболее важных счетчика производительности ISA Server:

- число разрешенных пакетов в секунду (кратное 10);
- число отброшенных пакетов в секунду.

Эти счетчики отображаются на инструментальной панели в графической форме (рис. **12.10).**

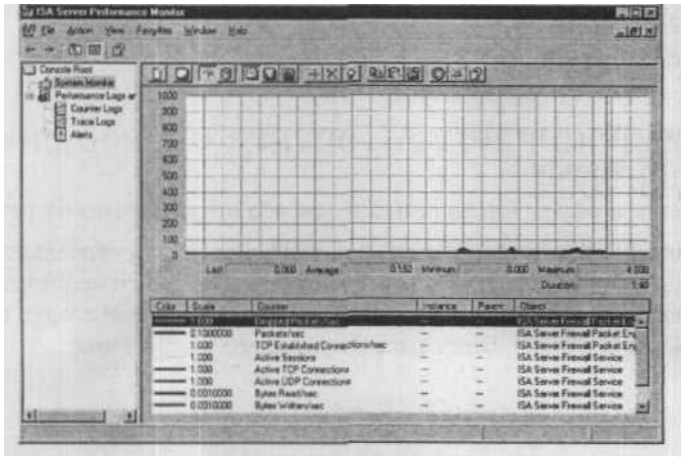


Рис. 12.10. Раздел **System Performance** (Производительность системы) инструментальной панели ISA Server 2004

Те же самые счетчики вместе с другими, специфичными для ISA Server 2004 отображаются по умолчанию в консоли ISA Server Performance Monitor, которая устанавливается во время инсталляции программного обеспечения ISA Server 2004.

ПРИМЕЧАНИЕ Экранные снимки инструментальной панели ISA Server и монитора производительности ISA Server показывают действия, которые происходят при доступе к Web-сайтам через ISA Server.

Использование ISA Server Performance Monitor (Монитор производительности ISA) будет обсуждаться в позже в этой главе.

Настройка и конфигурирование инструментальной панели

Инструментальную панель можно настроить по своему усмотрению, свернув или развернув любой раздел щелчком мыши на стрелках-указателях в правом верхнем углу раздела.

Также можно настроить отображаемые столбцы каждого раздела, щелкнув правой кнопкой мыши на заголовке столбца (например, *Status* — статус) и выбрав или отказавшись от выбора наименований столбцов.

Чтобы освободить больше места в инструментальной панели, можно закрыть консольное дерево слева, щелкнув его значок на панели, и/или закрыть панель задач справа, щелкнув мышью направленную вправо стрелку между инструментальной панелью и панелью задач.

После настройки инструментальной панели по своему усмотрению, можно использовать ее в качестве «титульного листа» обзора состояния ISA Server. Затем, чтобы получить более полную информацию, можно перейти на конкретную вкладку раздела. В последующих разделах будет показано, как использовать инструментарий конкретных вкладок для создания *и* конфигурирования наблюдения, ведения журналов, создания отчетов и оповещения в ISA Server 2004.

Создание и конфигурирование оповещений ISA Server 2004

Создание оповещений в ISA Server 2004 позволяет информировать пользователя о важнейших событиях, связанных с **работой** ISA Server, по мере их возникновения. Вместо того, чтобы тратить многие часы на выявление попытки проникновения в систему, ее можно обнаружить мгновенно: в случае неожиданной остановки одной из служб ISA Server будет создано уведомление и будут предприняты соответствующие действия для минимизации потерь.

События, вызывающие оповещения

Оповещения можно сконфигурировать для информирования о любом из нижеперечисленных событий (официальное название события приведено в скобках):

- действие, связанное с оповещением, выполнить невозможно (alert action failure);
- невозможно инициализировать контейнер кэша (cache container initialization error);
- контейнер кэша восстановлен (cache container recovery complete);
- попытка изменить размер файлового кэша потерпела неудачу (cache file resize failure);
- невозможно инициализировать кэш (cache initialization failure);
- содержимое кэша восстановлено (cache restoration complete);
- возникла ошибка при записи содержимого кэша (cache write error);
- кэшируемый объект отвергнут (cached object discarded);
- компонент расширения невозможно загрузить (component load failure);
- возникла ошибка при чтении данных конфигурации (configuration error);
- превышен лимит соединения пользователем или IP-адресом (connection limit exceeded);
- ограничение соединения для правила (число соединений в секунду) превышено (connection limit for rule exceeded);
- функция выявления попытки вторжения через искажение DHCP отключена (DHCP anti-poisoning intrusion detection disabled);
- занятость линии или ошибочный ответ вызвал срыв соединения по требованию (dial on demand failure);
- атака переноса DNS зоны (DNS zone transfer intrusion);
- информация не может быть записана в системный журнал (event log failure);
- ошибка взаимодействия клиента брандмауэра и службы ISA Server (firewall communication failure);
- сбой фильтра FTP при разборе допустимых FTP-команд (FTP filter initialization warning);
- обнаружена попытка атаки/проникновения со стороны внешнего пользователя (intrusion detected);
- CRL (Certificate Revocation List, список аннулированных сертификатов) неправильный, устарел или отсутствует (invalid CRL found);
- DHCP выдал некорректный IP-адрес (invalid DHCP offer);
- ISA Server выявил ошибку в запрошенных верительных данных (invalid dial-on-demand credential);
- верительные данные для базы данных ODBC ошибочны (invalid ODBC log credentials);
- адрес источника IP-пакета недопустим (IP spoofing);

- сделанные изменения в конфигурации требуют перезагрузки компьютера с ус тановленным ISA Server (ISA Server computer restart is required);
- сбой в журнале (log failure);
- размер журнала превысил ограничение (log storage limits);
- конфигурация сети изменена способом, который влияет на ISA Server (network configuration changed);
- в результате ошибки установки сетевого сокета отсутствуют доступные порты (no available ports);
- ISA Server не может подключиться к запрошенному серверу (no connectivity);

ш один из компонентов операционной системы (Network Address Translation, NAT, преобразование сетевых адресов; Internet Connection Sharing, ICS, общий доступ в Интернет или Routing and Remote Access, удаленный доступ) вызывает конфликт с ISA Server (OS component conflict);

- размер пакета UDP превышает максимальное значение, определенное в реест ре, что заставляет ISA Server отвергнуть данный пакет (oversized UDP packet);
- обнаружено переполнение буфера протокола POP (POP intrusion);
- пользователь удален из клиентов VPN-карантина (Quarantined VPN Clients network changes);
- возникла ошибка в процессе создания сводного отчета (report summary generation failure);
- возникла ошибка распределения ресурсов, например недостаточно системной памяти (resource allocation failure);
- возникла ошибка маршрутизации (создания цепочки) (routing/chaining failure);
- восстановление маршрутизации (создание цепочки) (routing/chaining failure);
- фильтр RPC (Remote Procedure Call, удаленный вызов процедуры) не может ис пользовать определенный порт, который уже использовался (bind failure);
- связь RPC-фильтра изменена (RPC filter — connectivity changed);
- опубликованное правило сервера сконфигурировано некорректно (server publi shing failure);
- опубликованное правило сервера неприменимо (server publishing not applicable);

м службу невозможно запустить (service initialization failure);

- неожиданная остановка службы (service not responding);
- нормальная остановка службы (service shutdown);
- нормальный запуск службы (service started);
- соединение ISA Server с затребованным сервером слишком медленное (slow connectivity);
- нарушено правило SMTP (SMTP filter event);
- конфигурация протокола SOCKS (протокол работы через брандмауэр) ошибочна, поскольку порт используется другим протоколом (SOCKS configuration failure);

- выявлена атака SYN (SYN attack);
- я возникла незарегистрированная ошибка (unregistered event);
- верительные данные для цепочек вверх по п отоку некорректны (upstream chaining credential);
- VPN-клиент безуспешно пытается установить связь (VPN connection failure).

Служба оповещения определяет время возникновения события, а также выясняет, сконфигурировано ли оповещение для уведомления или же для выполнения других действий. Затем служба инициирует специальное уведомление или иное действие.

Просмотр предопределенных оповещений

Предопределенные сообщения и определения можно посмотреть, щелкнув мышью вкладку **Alerts** (Оповещения) и открыв панель задач, если она еще не открыта. Щелкните **Configure Alert Definition** (Конфигурирование определений для оповещений) под заголовком **Alerts Tasks** (Задачи оповещений) на панели задач вкладки **Tasks** (Задачи). При этом откроется диалоговое окно **Alerts Properties** (Свойства оповещений), как показано на рис. **12.11.**

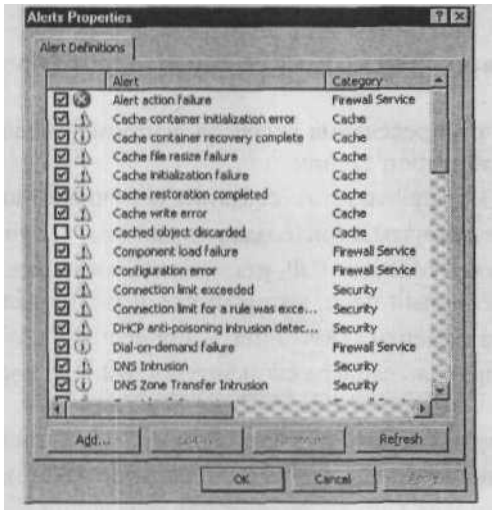


Рис. 12.11. Диалоговое окно Alerts Properties (Свойства оповещений)

Диалоговое окно **Alerts Properties** (Свойства оповещений) дает графическое представление об уровне данного оповещения, т. е. представляет ли это оповещение тип ***Error*** (Ошибка), ***Warning*** (Предупреждение) или ***Information*** (Информационное). В этом диалоговом окне можно изменить уровень оповещения или другие его свойства. Можно также присвоить уровень любому новому созданному оповещению.

Создание нового оповещения

Для определения нового оповещения нужно нажать мышью кнопку **Add** (Добавить). При этом будет вызван мастер **New Alert Configuration Wizard** (Мастер конфигурирования нового оповещения), как показано на рис. 12.12.

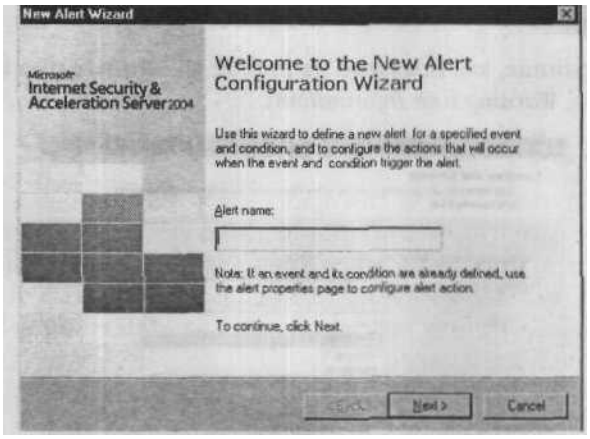


Рис. 12.12. Мастер конфигурирования нового оповещения

Необходимо задать имя нового оповещения. Затем щелкнуть мышкой кнопку **Next** (Далее). На следующей странице мастера необходимо выбрать событие и любые дополнительные условия, которые будут инициировать оповещение. Список событий, из которых необходимо сделать выбор соответствующих сообщений, описан в этой главе ранее.

Например, как показано на рис. 12.13. можно выбрать событие *Log Failure* (Сбой в журнале), а затем выбрать оповещение, которое будет инициироваться при сбое в журнале для любой службы ISA Server, ISA Server Firewall или ISA Server Web-фильтра.

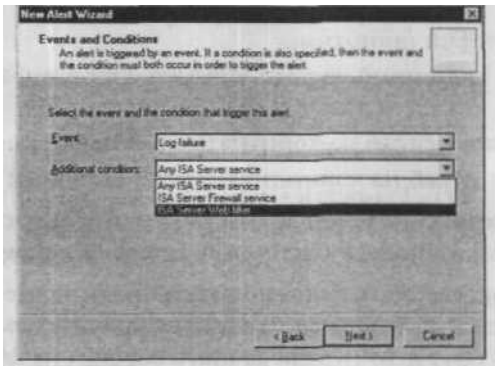


Рис. 12.13. Выбор событий и условий инициирования оповещений

Затем можно присвоить оповещению категорию из следующего списка:

- Security (Безопасность);
- Cache (Кэш);
- Routing (Маршрутизация);
- Firewall Service (Служба брандмауэра);
- Other (Другое).

На этой же странице, как показано на рис. 12.14. необходимо выбрать уровень оповещения *(Error, Warning* или *Information).*

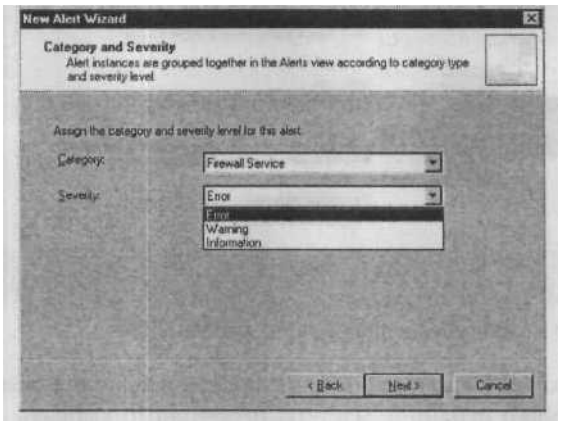


Рис. 12.14. Присвоение категории и выбор уровня нового оповещения

На следующей **странице** можно определить (если это необходимо) действие, которое нужно предпринять при возникновении заданного события и условий. ISA Server можно сконфигурировать так, чтобы при выполнении условий для оповещения выполнялось одно или все нижеперечисленные действия:

- отправка уведомления администратору (администраторам) по электронной почте;
- выполнение некоторой программы;
- запись события в системный журнал Windows (эта возможность включена по умолчанию);
- остановка выбранных служб на компьютере с установленным ISA Server;
- запуск выбранных служб на компьютере с установленным ISA Server.

Можно выбрать несколько действий, например отправку сообщения по электронной почте *и* запись события в системный журнал Windows (рис. 12.15).

Если выбрана отправка сообщения по электронной почте, то придется задать имя SMTP-сервера, который будет использоваться при отправке, и ввести значения адресов в поля **From** (От) и To (К) для данного сообщения. Можно отправить сообщение нескольким адресатам с помощью поля CC (Копия) (рис. 12.16).

СОВЕТ Может появиться диалог ввода имени и пароля для учетной записи для получения доступа к серверу SMTP. Кроме того, если уведомление по электронной почте сконфигурировано с использованием внешнего SMTP-сервера, то потребуется создать правило доступа для получения доступа локального хоста к внешней сети с помощью протокола SMTP. Более того, если отправка SMTP-сообщений к серверу внутренней сети потерпела неудачу, то возможная причина этого — запрет на правило «Allow SMTP from ISA to Trusted Servers system policy» (разрешить отправку SMTP-сообщений от ISA Server к доверенным серверам системной политики). Обратите внимание, что файл помощи (Help) подсказывает, что необходимо включить правило системной политики, позволяющее ЛВС связываться с внутренней сетью по протоколу SMTP. Однако по умолчанию это правило уже включено, поэтому не надо беспокоиться, если раньше это правило не было закрыто.

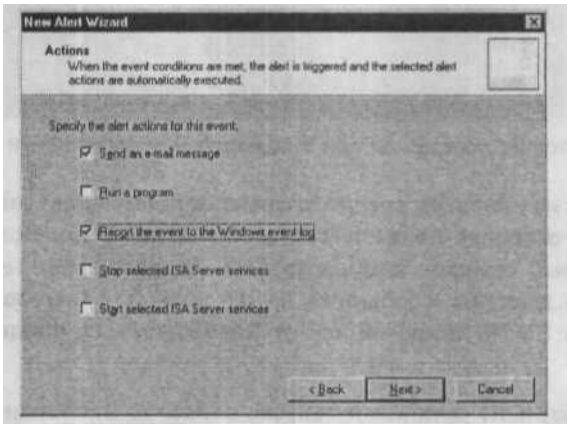


Рис. 12.15. Задание необходимых действий при инициировании оповещения

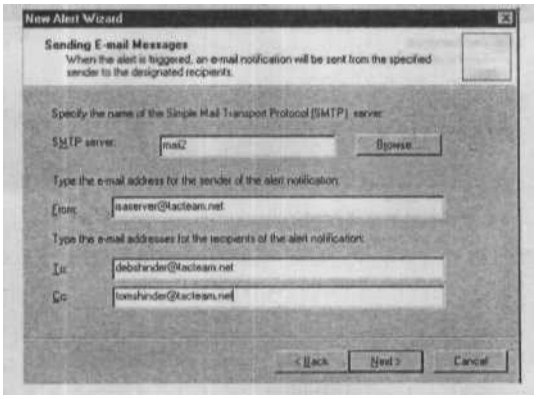


Рис. 12.16. Отправка уведомления по электронной почте

Точно так же, если выбран запуск определенной программы, то будет предложено ввести путь к исполняемому файлу этой программы и учетную запись, под которой будет выполняться данная программа (рис. 12.17).

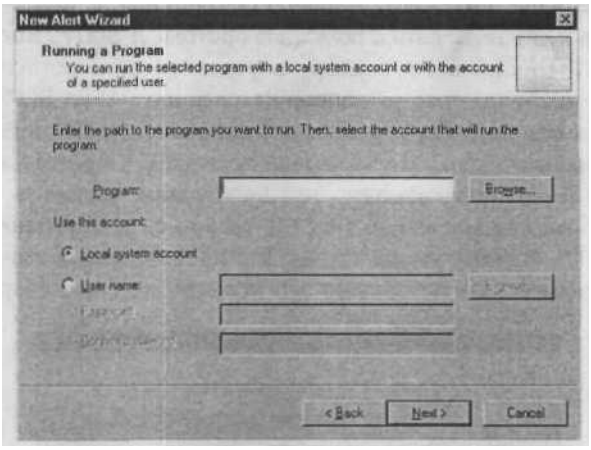


Рис. 12.17. Выполнение программы при инициировании оповещения

СОВЕТ Одно из наиболее распространенных применений запуска программы состоит в отправке пейджингового сообщения администратору. Однако, если сотовый телефон администратора поддерживает текстовые сообщения, то для доставки сообщения на сотовый телефон можно использовать протокол SMTP, отказавшись от необходимости поддержки средств пейджинга.

Если выбран вариант остановки/запуска служб, то необходимо будет выбрать службу (службы), которую необходимо запустить или остановить (рис. 12.18).

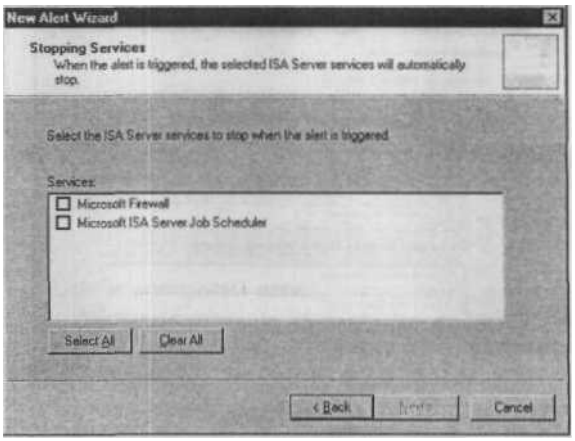


Рис. 12.18. Остановка и запуск службы при инициировании оповещения

Когда для нового оповещения все свойства сконфигурированы, на последней странице мастера выводится вся введенная информация (рис. 12.19). Необходимо проверить все введенные данные, для внесения изменений использовать кнопку **Back** (Возврат), нажать кнопку **Finish** (Готово).

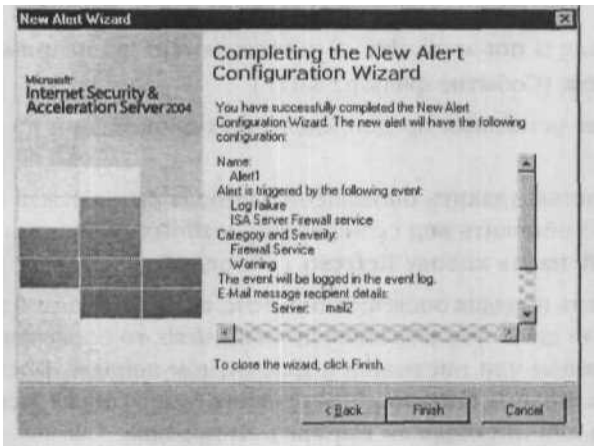


Рис. 12.19. Завершение работы мастера создания нового оповещения

Теперь новое оповещение будет представлено в диалоговом окне **Alerts Properties** (Свойства оповещений) в окне Alerts Definitions (Определения оповещений), как показано на рис. 12.20.

Рис. 12.20. Новые оповещения в окне Alerts Definitions (Определения оповещений)

В этом окне можно запретить использование оповещения, сняв пометку с флаговой кнопки. Будет выведено напоминание о том, что некоторые оповещения предопределены, но использование их по умолчанию запрещено. К таким оповещениям ОТНОСЯТСЯ:

- Cached object discarded (Отмена кэширования объекта);
- Event log failure (Ошибка журнала событий);
- Network configuration changed (Сетевая конфигурация изменена);
- Quarantined VPN Clients network changed (Сеть клиентов VPN-карантина изменена);
- Server publishing is not applicable (Публикация сервера неприменима);
- SMTP filter event (Событие фильтра SMTP).

Использование остальных предопределенных оповещений по умолчанию разрешено.

Можно полностью удалить оповещение, выбрав его и нажав кнопку **Remove** (Удалить). Можно обновить вид сконфигурированных оповещений после выполнения изменений, нажав кнопку **Refresh** (Обновить).

Можно изменить порядок оповещений в окне, щелкнув мышкой заголовок столбца. Например, если щелкнуть заголовок столбца *Alerts,* то оповещения будут упорядочены в восходящем или нисходящем алфавитном порядке. После щелчка мышкой на заголовке столбца *Categories* оповещения будут упорядочены по категориям в восходящем или нисходящем алфавитном порядке.

Изменение оповещений

Свойства нового оповещения или любого предопределенного оповещения можно изменить, выделив такое оповещение и нажав кнопку **Edit** (Редактировать) Это позволит изменить категорию и/или уровень оповещения и включить или выключить оповещение на вкладке **General** (Общие). На вкладке **Events** (События) можно изменить событие и дополнительные условия.

РИС. 12.21. Изменение пороговых значений вызова оповещения

При изменении оповещения можно определить число возникновений события до того, как оповещение должно быть инициировано, и/или можно определить число событий в секунду до момента инициирования оповещения. Также можно определить, должно ли оповещение инициироваться сразу же после заданного порогового числа или определить количество минут, которое должно пройти после последнего выполнения оповещения. Все это показано на рис. 12.21.

На вкладке **Actions** (Действия) можно изменить, удалить или добавить действия, которые должны быть выполнены при инициировании оповещения, точно так же, как это делается при создании оповещения.

Просмотр инициированных оповещений

Если щелкнуть вкладку **Alerts** (Оповещения) в узле **Monitoring** (Наблюдение), то на центральной панели будут отображены инициированные оповещения (см. рис. 12.22).

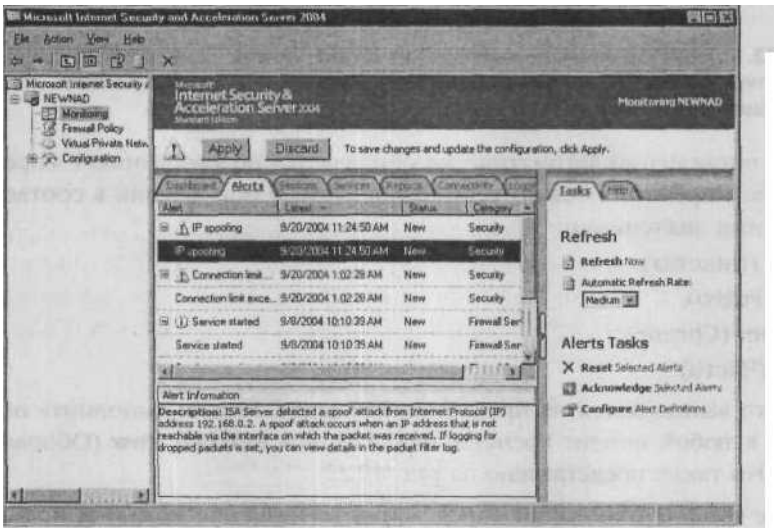


Рис. 12.22. Просмотр инициированных оповещений

Здесь отображается название оповещения, дата и время его возникновения, статус и категория, присвоенные оповещению. Оповещения группируются по типу (например, «Services started», выполняющиеся службы). Необходимо щелкнуть мышью маленький квадратик со знаком + (плюс) для того, чтобы раскрыть группу.

Если щелкнуть мышью отдельное оповещение, то в окне **Alert** Information (Информация оповещения) под списком последних оповещений будет отображено подробное описание. Точно такая же информация появится в журнале приложения **Event Viewer** (Просмотр события), как показано на рис. 12.23-

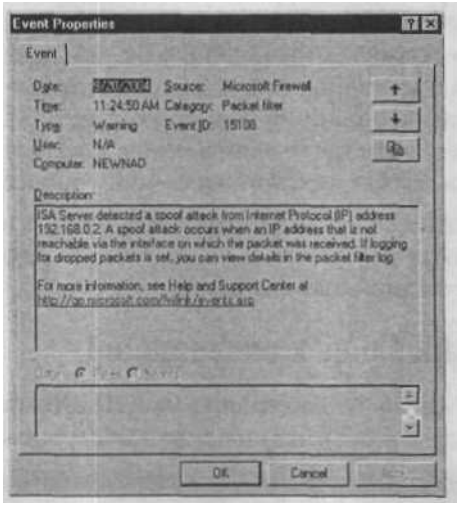


Рис. 12.23. Запись в журнале приложения Event Viewer (Просмотр события), представляющая информацию, отображаемую в окне Alerts Information (Информация оповещения)

Окно оповещений автоматически обновляется по умолчанию с определенным интервалом времени. Можно установить частоту обновления в соответствии со следующими значениями:

- None (Никогда);
- Low (Редко);
- Medium (Средне);
- High (Часто).

Все это выполняется на правой панели задач. Можно выполнить обновление вручную в любой момент времени, нажав значок **Refresh Now** (Обновить немедленно). Это также представлено на рис. 12.22.

Кроме конфигурирования определений оповещения можно выполнить следующие задачи:

- **Reset selected alerts** (Отменить выбранные оповещения) Можно отменить оповещения с тем, чтобы удалить их из окна **Alerts** (Оповещения). На средней панели нужно выделить оповещение, которое необходимо отменить, и щелкнуть мышью **Reset selected alerts** (Отменить выбранные оповещения) на правой панели задач. Будет запрошено подтверждение на отмену оповещения. Для подтверждения нужно нажать кнопку **Yes** (Да). Оповещение исчезнет из средней панели. Можно отменить целую группу оповещений, выбрав заголовок нужной группы.
- **Acknowledge selected alerts** (Квитировать выбранные оповещения) Можно квитировать (утвердить) сообщение, которое необходимо удалить из инструментальной панели. Оповещение останется в окне **Alerts** (Оповещения) во вкладке

Alerts (Оповещения), но его статус будет представлен как *«Acknowledged»* (Квитированное). Это можно использовать для указания на то, что оповещение принято и обрабатывается. В средней панели нужно выделить оповещение (оповещения), которое необходимо пометить как квитированное, и щелкнуть мышью **Acknowledged selected alerts** (Квитировать выбранные оповещения) в правой панели задач.

ПРИМЕЧАНИЕ После перезагрузки компьютера ISA Server все оповещения будут восстановлены.

Наблюдение за связями, сеансами и службами в ISA Server 2004

Можно наблюдать за связями между ISA Server и другими компьютерами на вкладке **Connectivity** (Связи). На вкладке **Sessions** (Сеансы) можно наблюдать за текущими сеансами для клиентов брандмауэра, Web-прокси и **SecureNAT.** На вкладке **Services** (Службы) можно наблюдать статус служб ISA Server. В последующих разделах эти возможности будут рассмотрены подробно.

Конфигурирование связей и наблюдение за ними

Для отслеживания связи между ISA Server и определенными серверами в любой сети (по имени сервера или IP-адресу) или между ISA Server и определенным Web-сервером (по URL) можно использовать один из трех методов проверки связи:

- **Ping** (Packet InterNet Groper, отправитель пакетов Internet[1]) ISA Server посы лает пинг-сообщение (ICMP ECHO_REQUEST) на сервер. Если сервер возвраща ет сообщение ECHOREPLY, то этим подтверждается, что данный сервер досту пен для ISA Server.
- **TCP Connect** (TCP-соединение) ISA Server пытается установить TCP-соедине ние к определенному порту на сервере. Это можно использовать для подтверж дения того, что отдельная служба выполняется на данном сервере.
- **HTTP Request** (Запрос HTTP) ISA Server отправляет команду HTTP GET на оп ределенный Web-сервер. Ответ указывает на то, что Web-сервер «поднят», рабо тает и достижим от ISA Server.

Чтобы наблюдать за связью с сервером с помощью любого из этих методов, необходимо создать верификатор связи и поместить его в *одну* из предопределенных групп:

- Active Directory;
- DHCP;

[1] Программа, используемая для проверки доступности адресата путем передачи ему специального сигнала (ICMP echo request, запрос отклика ICMP) и ожидания ответа. — *Прим. пер.*

- DNS;
- Published servers (опубликованные серверы);
- Web (Интернет);
- Others (другие).

Статус каждой группы представлен в инструментальной панели. Это позволяет быстро определить, в каком из серверов группы возникают проблемы. Затем можно щелкнуть мышкой вкладку **Connectivity** (Связи) для получения подробных сведений о проблемном сервере группы.

В последующих разделах будет показано, как создавать верификаторы связи, как присваивать их группам и как отслеживать связи с помощью созданных верификаторов.

Создание верификаторов связи

Первый шаг в наблюдении за связями между ISA Server и другими компьютерами состоит в создании верификатора связи. Чтобы выполнить это, необходимо щелкнуть мышкой на вкладке **Connectivity** (Связи) в узле **Monitoring** (Наблюдение), а затем щелкнуть мышкой кнопку **Create New Connectivity Verifier** (Создать новый верификатор связи) на правой панели задач. При этом начнет выполняться мастер создания нового верификатора связи New Connectivity Verifier Wizard. На первой странице мастера необходимо ввести название верификатора (например, если есть намерение наблюдать подключение к Web-сайту, необходимо присвоить ему имя URL данного сайта).

Затем мастер попросит ввести подробные сведения о верификаторе связи: имя сервера, IP-адрес или URL в поле ***Connection Details*** (Сведения о соединении) как показано на рис. 12.24 (местоположение сервера можно выбрать, нажав кнопку **Browse** (Обзор)).

Необходимо выбрать тип группы в выпадающем меню.

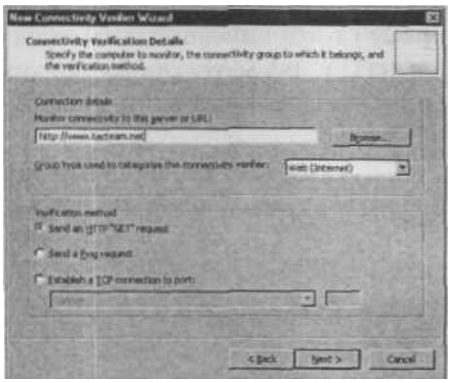


Рис. 12.24. Ввод сведений о верификаторе связи

Можно также выбрать метод верификации. Если наблюдается связь с Web-сервером (по URL), необходимо выбрать в качестве типа группы **Web** (Internet), а в качестве метода верификации (проверки) **Send HTTP «GET» request** (Отправка HTTP-запроса «GET»), Если нужно проверить выполнение определенной службы на наблюдаемом сервере, то выбирается вариант **Establish a TCP connection to port** (Установить TCP-подключение к порту) и сделать выбор в выпадающем списке. Номер порта будет указан автоматически, или его можно задать вручную, выбрав вариант **Custom** (Настройка).

В выпадающем списке можно выбрать приложения:

- AOL Instant Messenger — служба обмена сообщениями сети American On-Line;
- Chargen (TCP) — служба UNIX машин — генератор бесконечной последовательности СИМВОЛОВ;
- Daytime (TCP) — служба времени;
- Discard (TCP) — служба отмены пакетов;
- DNS — служба доменных имен;
- Echo (TCP) — отклик;
- Finger — поисковая служба;
- FTP — протокол передачи файлов;
- Gopher — поисковая система;
- Протокол H.323;
- HTTP;
- HTTPS — защищенный HTTP;
- ICA — архитектура межпрограммных связей;
- ICQ — интернет-пейджер;
- Went — служба идентификации;
- IMAP4 — Internet Mail Access Protocol, протокол доступа к электронной почте версии 4;
- IMAP5 — Internet Mail Access Protocol, протокол доступа к электронной почте версии 5;
- IRC — Internet Relay Chat, служба обмена информацией в сети Интернет;
- Kerberos-Adm (TCP) — служба защиты;
- LDAP — Lightweight Directory Access Protocol, упрощенный протокол доступа к сетевым каталогам;
- LDAP GC (глобальный каталог);
- LDAPS (безопасный LDAP);
- LDAPS GC (глобальный каталог);
- Microsoft CIFS (^{TCP}) — Common Internet File System, общая межсетевая файловая система;
- Microsoft Operations Manager Agent — агент управления операциями;

- Microsoft SQL (TCP) — структурированный язык запросов;
- MMS — Microsoft Media Server, медиа-сервер корпорации Microsoft;
- MS Firewall Control — управление брандмауэром;
- MSN — служба новостей;
- MSN Messenger — **интернет-пейджер;**
- Net2Phone Registration (NetBIOS Session) — интернет телефон;
- News — новости;
- NNTP — Network News Transfer Protocol, протокол передачи сетевых новостей;
- NNTPS — защищенный NNTP;
- PNM — Progressive Networks Media, протокол передачи данных мультимедиа;
- POP2 — почтовый протокол версии 2;
- POP3 — почтовый протокол версии 3;
- POP3S - защищенный POP3;

м PPTP — протокол «точка-точка»;

- Quote (TCP) — котировки;
- RDP (терминальная служба) — Remote Desktop Protocol, протокол доступа к удаленному рабочему столу;
- Rlogin — удаленная регистрация;
- RPC (все интерфейсы) — Remote Procedure Call, удаленный вызов процедур;
- TRSP — протокол потока реального времени;
- SMTPS — защищенный SMTP;
- SSH — Secure Shell, протокол безопасного удаленного доступа в среде UNIX;
- Telnet — протокол удаленного доступа к терминалу;
- Time — служба времени;
- Whols — поисковая служба.

На последней странице мастера обобщается вся введенная информация. Для внесения изменений нужно нажать кнопку **Back** (Вернуться). Если все в пэрядке — нажать кнопку **Finish** (Готово).

Если выбран вариант наблюдения за HTTP-соединением, **то откроется** диалоговое окно, информирующее о необходимости сконфигурировать правило, позволяющее получить доступ к адресату по протоколам HTTP или HTTPS, также необходимо будет ответить на вопрос, необходимо ли инициировать правило системной политики **«Allow HTTP/HTTPS requests from ISA Server to the selected servers for connectivity verifiers»** (Разрешить запросы H^{T}TP/HTTPS от ISA Server к выбранным серверам от верификатора связи) (рис. 12.25). Чтобы это правило задействовать, нажмите кнопку **Yes** (Да).

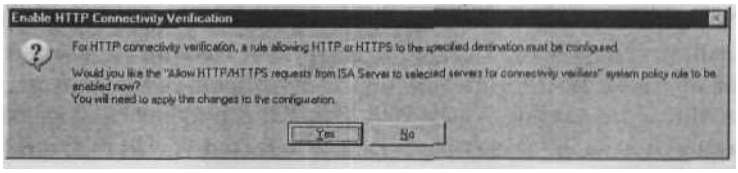


Рис. 12.25. Включение правила разрешения запросов HTTP/HTTPS

ПРИМЕЧАНИЕ Если удалить или выключить все верификаторы, использующие метод HTTP, то правило системной политики автоматически отключит правило HTTP/HTTPS запросов для верификаторов связи по соображениям безопасности. Его придется активировать вновь, если позже будет создан или включен верификатор, сконфигурированный для использования HTTP.

Если выбрать вкладку Connectivity (Связи), то на центральной панели можно увидеть новый верификатор связи (см. рис. 12.26).

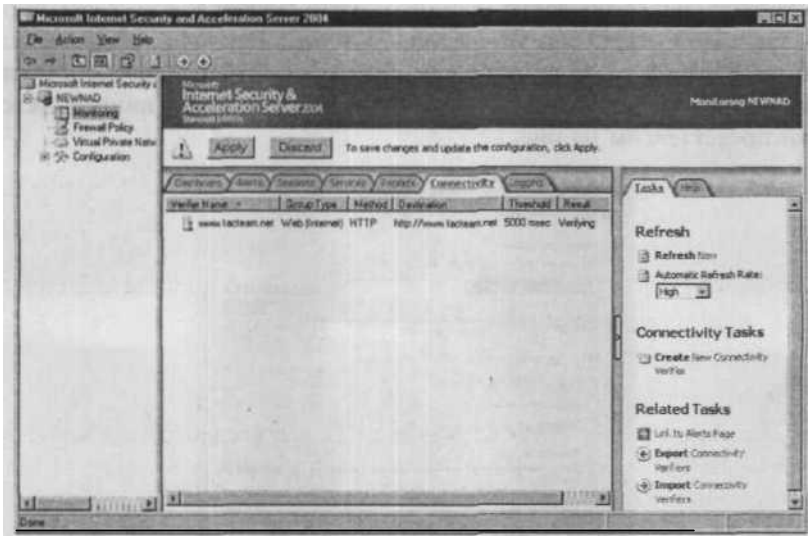


Рис. 12.26. Новый **верификатор связи**

После включения правила необходимо щелкнуть мышью Apply (Применить) в верхней части консоли. При этом все изменения и обновления будут сохранены. Появится индикатор выполнения всех сделанных изменений, затем в диалоговом окне будет выведено сообщение о том, что все изменения в конфигурации успешно применены. После этого следует нажать кнопку OK.

Теперь в колонке *Result* (Результаты) запись «Verifying» (Проверка) будет заменена на результирующее время проверки (в миллисекундах).

Можно удалить или выключить верификатор, щелкнув на нем правой кнопкой и выбрав в контекстном меню Delete (Удалить) или Disable (Выключить). Из этого меню можно также экспортировать или импортировать верификаторы. Другой способ выполнить эти задачи — выделить нужный верификатор и щелкнуть необходимую задачу на панели задач справа (Delete Selected Verifiers, Disable Selected Verifiers, Export или Import Connectivity Verifiers).

Чтобы изменить какие-либо свойства верификатора связи, нужно щелкнуть на нем правой кнопкой мыши и выбрать в контекстном меню пункт Properties (Свойства) или выбрать верификатор и щелкнуть Edit Selected Verifier (Редактировать выбранный верификатор) на панели задач справа.

На вкладке General (Общие) окна свойств можно изменить имя верификатора, включить или выключить его, изменить тип и ввести необязательное описание. На вкладке Properties (Свойства) можно изменить URL, название сервера или IP-адрес соединения, за которым необходимо установить наблюдение, изменить тип группы или изменить метод проверки (верификации). Можно также задать пороговое значение тайм-аута ответа (по умолчанию 5000 мс). Наконец, можно указать, необходимо ли инициировать оповещение, если время ответа сервера не укладывается в заданное значение тайм-аута (по умолчанию оповещение инициируется). Эти настройки представлены на рис. 12.27.

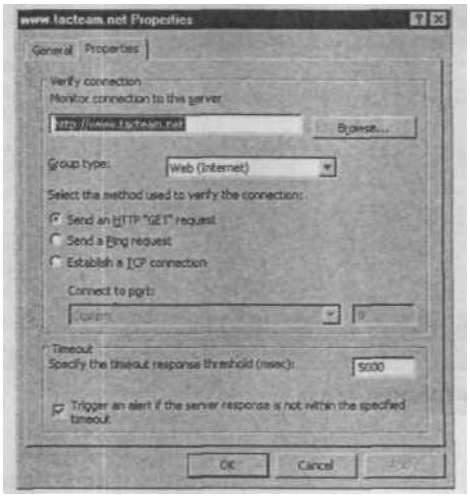


Рис. 12.27. Изменение свойств верификатора связи

Наблюдение за связями

После конфигурирования верификаторов можно с одного взгляда понять, имеются ли проблемы с серверами отдельной группы, просто посмотрев в раздел Connectivity (Связи) инструментальной панели. Как видно из рис. 12.28, для типов групп,

у которых сконфигурированы верификаторы, показан статус «Good» (Все в порядке), а связи в этой группе проверены.

Если с каким-нибудь из серверов группы возникает проблема, то статус группы укажет на нее (даже если другие серверы в группе подключены корректно). Например, если один из серверов группы Others (Прочие) оказывается подключенным с низкой скоростью, это отразится в столбце *Status* (Статус) панели инструментов (рис. 12.29).

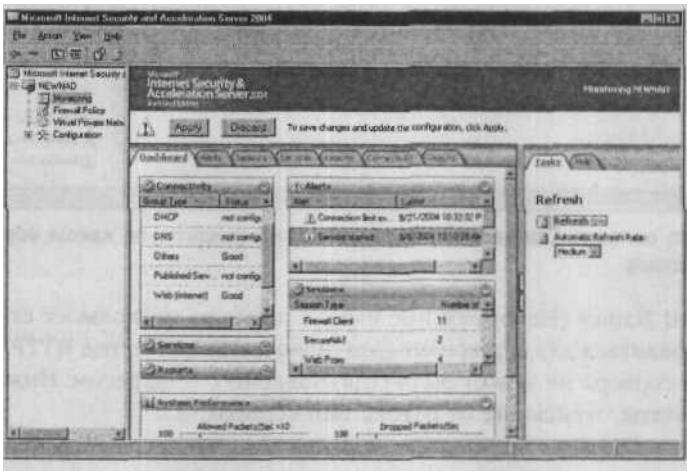


Рис. 12.28. Наблюдение за связями на пане ли инструментов

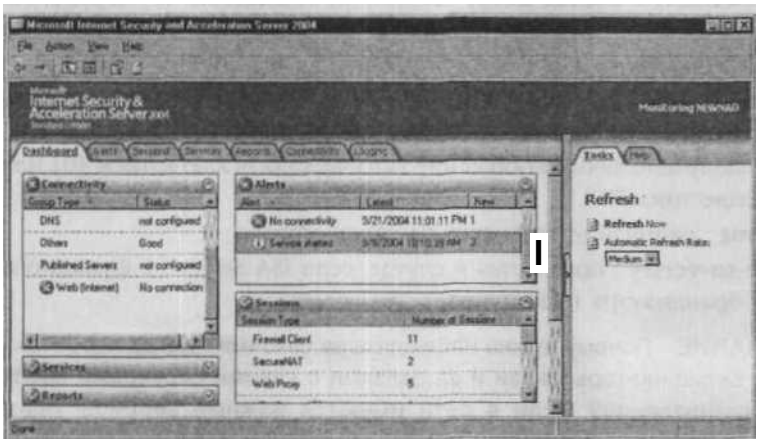


Рис. 12.29. Проблемы связи, отображаемые на панели инструментов

Для того чтобы определить, на каком из серверов возникла данная проблема, необходимо перейти на вкладку Connectivity (Связи). Здесь можно точно посмотреть, какой верификатор указывает на проблему (рис. 12.30).

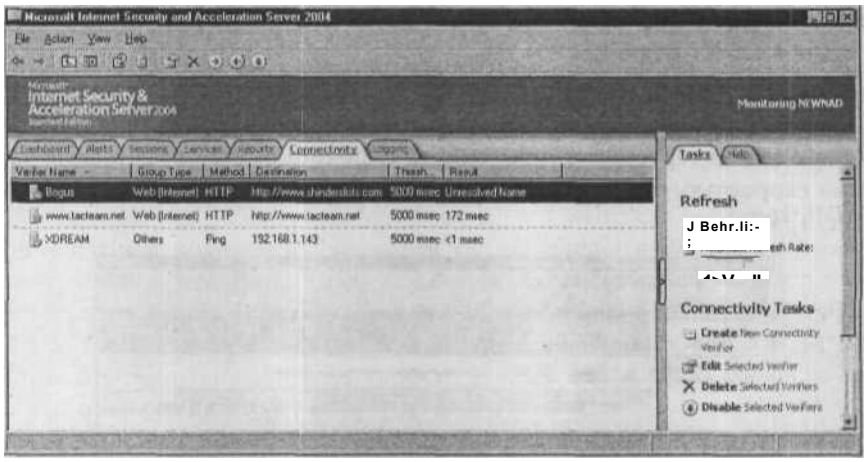


Рис. 12.30. На вкладке Connectivity (Связи) можно увидеть, на каком сервере возникла проблема

«Unresolved Name» (Некорректное имя) — один из нескольких статусов, который может появиться для верификаторов, использующих метод HTTP. Он возникает, когда имя сервера не может быть сопоставлено с IP-адресом. Ниже приведены другие результаты, зависящие от ответа web-сервера.

- OK от сервера получено сообщение 401 (Web-сервер требует аутентификации).
- **Error (Windows Server 2003)** получено сообщение 407 (требуется аутентификация прокси), поскольку ISA Server не может проверить связь с действующим Web-сервером.
- **Authentication required (Windows 2000 Server)** получено сообщение 407, если на сервере выполняется операционная система Windows 2000.
- **Error** получено любое сообщение типа 4XX (за исключением 401 или 407) или сообщение типа 5XX.
- **Time-out** окончание тайм-аута на ответ сервера.
- **Unable-to-verify** появляется в случае, если ISA Server не функционирует или служба брандмауэра недоступна.

ЗАМЕЧАНИЕ Почему нужно наблюдать за связями? Когда необходимо создавать верификаторы связи и за связями с какими серверами необходимо вести наблюдение? Если в сети имеются важные серверы (например, Exchange-сервер электронной почты), настроенные на работу с внешними клиентами, то желательно создавать верификатор связи, чтобы легко было проверять корректность их работы. Также может потребоваться создать верификатор связи для некоторых популярных Web-сайтов, которые считаются надежными в смысле продолжительности работы, чтобы можно было видеть подключение ISA Server к этим внешним сайтам.

Наблюдение за сеансами

Одно из удобств ISA Server — возможность наблюдения за сеансами связи в реальном режиме времени, т. е. за действиями отдельного клиентского компьютера (IP-адрес) и отдельного пользователя (имя учетной записи). Можно наблюдать за сеансами связи со всеми тремя типами клиентов брандмауэра, Web-прокси и SecureNAT.

> ПРИМЕЧАНИЕ Поскольку ISA Server рассматривает сеанс связи как уникальную комбинацию пользователя и IP-адреса, в счетчиках производительности службы брандмауэра можно увидеть больше текущих пользователей, чем число сеансов, видимых в окне Sessions (Сеансы). Это происходит из-за того, что при установлении нового соединения от одного и того же IP-адреса и того же пользователя, оно рассматривается как часть того же самого сеанса связи. Системный монитор (System Monitor) обозначает каждое соединение как текущий пользователь.

Просмотр, остановка и приостановка наблюдения за сеансами

Для просмотра текущих сеансов связи, проходящих через ISA Server, нужно щелкнуть мышью вкладку Sessions (Сеансы), после чего появится список сеансов, как показано на рис. 12.31.

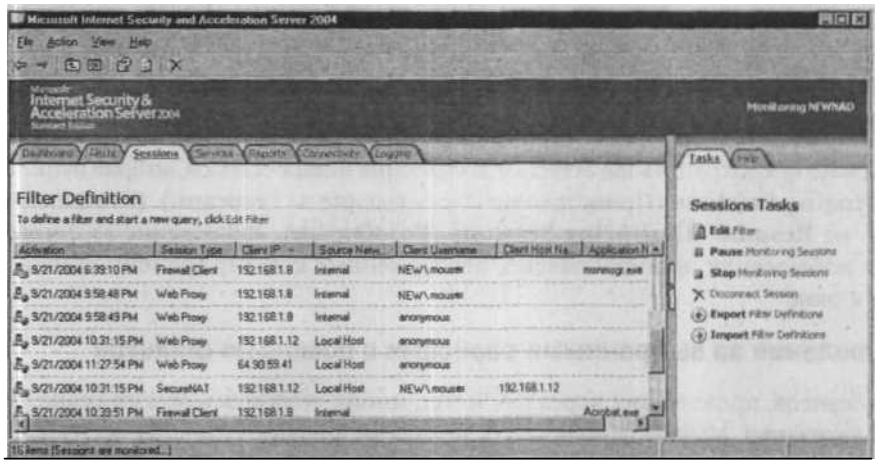


РИС. 12.31. Просмотр текущих сеансов связи

На этой вкладке отображается следующая информация о каждом сеансе:

- дата и время активации сеанса;
- тип сеанса (брандмауэр, Web-прокси, клиент SecureNAT, VPN-клиент или удаленный VPN-сайт);
- IP-адрес клиента;

- сеть-источник;
- имя пользователя клиента (если требуется аутентификация);
- имя клиентского хоста (для сеансов клиентов брандмауэра);
- имя приложения (для сеансов клиентов брандмауэра);
- имя сервера (имя ISA Server).

В версии ISA Server Standard Edition столбцы ***Server name*** (Имя сервера) *и* ***Application*** *name* (Имя приложения) по умолчанию не отображаются. Для их отображения нужно щелкнуть правой кнопкой мыши на заголовках столбцов и выбрать в контекстном меню пункт **Server name** (Имя сервера) или **Application name** (Имя приложения).

ПРИМЕЧАНИЕ Даже если анонимное соединение заблокировано, можно увидеть анонимные сеансы, поскольку по соображениям производительности клиент Web-прокси отправляет первое сообщение анонимно, затем сервер возвращает сообщение 407, требуя аутентификации, а последующие соединения включают верительные данные клиента.

Если необходимо остановить наблюдение за сеансами, просто выберите: **Stop Monitoring Sessions** (Остановить наблюдение за сеансами) на панели задач справа. Вся информация о сеансах на вкладке **Sessions** (Сеансы) исчезнет. Чтобы вновь начать наблюдение, щелкните **Start Monitoring Sessions** (Начать наблюдение за сеансами) (этот пункт появится только после остановки наблюдения).

ПРЕДУПРЕЖДЕНИЕ Если наблюдение за сессиями остановлено, вся собранная к этому времени ISA Server информация будет утеряна.

Можно предохранить ISA Server от добавления новых сеансов, выбрав пункт **Pause Monitoring Sessions** (Приостановить наблюдение за сеансами). (Этот пункт сменится на **Resume Monitoring Sessions** (Возобновить наблюдение за сеансами).) Когда наблюдение приостановлено, отображенные к этому времени сеансы остаются в окне.

Наблюдение за выбранными сеансами с помощью фильтра

Если сеансов, проходящих через ISA Server, много, то поиск нужного сеанса может быть затруднен. Можно использовать механизм фильтрования ISA Server 20D4 для сортировки сеансов по дате, чтобы отображать данные только сеансов, соответствующих определенным критериям. Если задать несколько критериев, то отображаться будут только сеансы, отвечающие *всем* критериям.

Для определения фильтра необходимо выполнить следующие действия: 1. На панели задач справа щелкнуть пункт **Edit Filter** (Редактировать фильтр) или щелкнуть правой кнопкой мыши в средней панели и выбрать в контекстном меню пункт **Edit Filter** (Редактировать фильтр).

2. В диалоговом окне **Edit Filter** (Редактировать фильтр) выбрать из выпадающего меню критерий фильтра для поля **Filter by** (Фильтр по) (см. рис. 12.32).

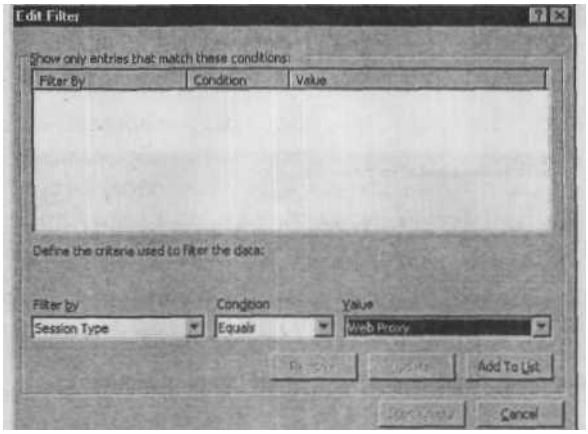


Рис. 12.32. Установка критериев фильтра

Критерии можно установить по следующим параметрам:

D активация (activation);

□ имя приложения (application name);

D имя клиентского хоста (client host name);

□ клиентский IP-адрес (client IP address);

□ имя пользователя (client user name);

□ имя сервера (server name);

D тип сеанса (session type);

□ сеть-источник (source network).

3. Затем необходимо выбрать условие («equal» (равно) или «not equal» (не равно)).
4. Выбор в поле *Value* (Значение) зависит от критерия фильтрования. В нашем примере выбран фильтр по типу сеанса, поэтому выбираемые значения — Firewall, Client, SecureNAT, VPN Client, VPN Remote Site или Web Proxy. Мы выбираем просмотр всех сеансов Web-прокси.
5. Чтобы добавить фильтр к списку, щелкните пункт **Add to list** (Добавить к списку).

Если впоследствии необходимо будет ограничить возможности сеансов, можно добавить больше критериев фильтрования, пройдя весь процесс заново. В данном примере (см. рис. 12.33) необходимо просматривать только сеансы Web-прокси для клиента с IP-адресом 192.168.1.121 (локальный хост).

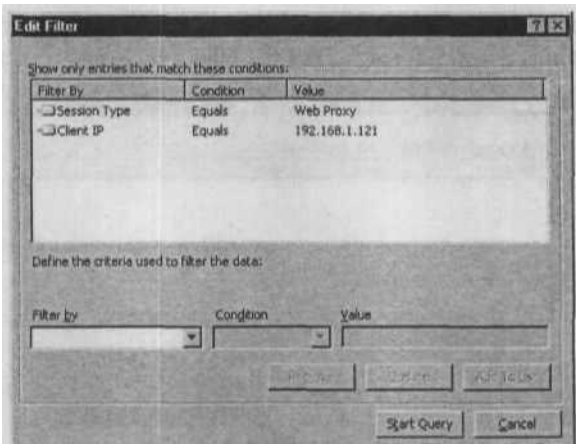


Рис. 12.33. Определение нескольких критериев фильтрования

После добавления всех необходимых критериев, щелкните пункт **Start Query** (Начать запрос), процесс фильтрования будет начат. Сеанс или сеансы, удовлетворяющие всем критериям, **будут** отображаться, как представлено на рис. 12.34.

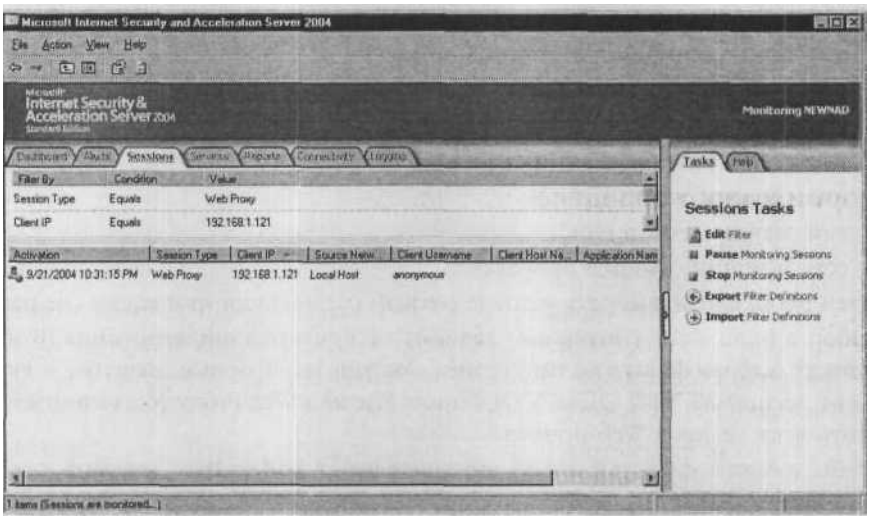


Рис. 12.34. Результат применения фильтра

Все определения фильтра можно сохранить для дальнейшего использования, экспортировав их *в* xml-файл. Подробности описаны далее в этой главе.

СОВЕТ Недостающие функции панели задач (Task Pane) В файле помощи (Help) ISA Server можно найти инструкцию по сохранению определений фильтра и «загрузки» определений фильтра, в которой говорится, что необходимо выбрать пункты **Save Filter Definitions** (Сохранить определения фильтра) или **Load Filter Definitions** (Загрузить определения фильтра) на вкладке **Tasks** (Задачи). Проблема в том, что таких пунктов на вкладке просто нет (они были в некоторых бета-версиях). В окончательном варианте продукта для этих целей используются функции **Export** (Экспорт) и **Import** (Импорт).

СОВЕТ Перед редактированием фильтра по умолчанию экспортируйте (сохраните) определения фильтра. Если придется вернуться к варианту просмотра сеанса по умолчанию, можно просто импортировать определения фильтра, а затем остановить и вновь запустить процесс наблюдения. В ISA Server отсутствует кнопка отмены, позволяющая вернуться к установкам фильтра по умолчанию (для всех сеансов). Возможно, эта функциональная возможность появится в последующих версиях ISA Server.

Прерывание сеансов связи

Можно быстро прервать сеанс, щелкнув правой кнопкой мыши в окне **Sessions** (Сеансы) и выбрав в контекстном меню пункт **Disconnect Session** (Прервать сеанс). При этом будет выведен запрос на подтверждение прерывания сеанса. Для утвердительного ответа необходимо нажать кнопку **Yes** (Да) или выделить сеанс, а затем нажать кнопку **Disconnect Session** (Прервать сеанс) на панели задач справа.

Экспорт и импорт определений фильтра

Можно сохранить установки фильтра, экспортируя его в xml-файл, а затем загружая сохраненные **установки** с помощью импорта. Если создается несколько фильтров, то, возможно, будет удобно создать несколько предопределенных фильтров, например позволяющих быстро просматривать сеансы Web-прокси с помощью одного фильтра, а сеансы брандмауэра с помощью другого. Еще один фильтр можно использовать для просмотра всех сеансов определенного клиента и т. д.

После того, как параметры фильтра определены, их желательно сохранить для дальнейшего использования, щелкнув мышью кнопку **Export Filter Definitions** (Экспортировать определения фильтра) на панели задач справа. Выберите местоположение для хранения определений фильтра (лучше всего создать для этого отдельную папку) и задать подходящее имя (например, FirewallSessionFilter). Затем следует нажать кнопку **Save** (Сохранить).

Когда этот фильтр потребуется использовать вновь, нужно просто щелкнуть на панели задач справа кнопку **Import Filter Definition** (Импорт определений фильтра), найти местоположение сохраненных определений фильтра и выбрать его. Затем

щелкнуть кнопку **Load** (Загрузить). Можно щелкнуть кнопку **Refresh** (Обновить) в верхней части панели инструментов для просмотра новых результатов фильтрования после загрузки фильтра.

Наблюдение за службами

С помощью вкладки **Services** (Службы) узла **Monitoring** (Наблюдение) можно установить наблюдение за службами ISA Server, выполняемыми на брандмауэре. По умолчанию в окне **Services** (Службы) на средней панели представлены названия служб, статус каждой из них (выполняется или остановлена) и в некоторых случаях рабочее время службы (как долго данная служба выполняется в днях, часах, минутах и секундах).

> ПРИМЕЧАНИЕ Столбец *Service Uptime* (Время работы службы) не обновляется в реальном масштабе времени. Для обновления параметров необходимо щелкнуть мышью кнопку Refresh (Обновить) на панели задач справа.

На этой вкладке можно останавливать или запускать службы. Необходимо просто щелкнуть правой кнопкой мыши на выполняющейся службе и в контекстном меню выбрать пункт **Stop** (Остановить) или выделить службу и щелкнуть мышью кнопку **Stop Selected Service** (Остановить выбранную службу) на панели задач справа. Статус службы измениться на ***Stopped*** (Остановлена) (рис. 12.35). Затем службу можно запустить вновь, щелкнув на ней правой кнопкой мыши и выбрав пункт **Start** (Запуск) или нажав кнопку **Start Selected Service** (Запуск выбранных служб) на панели задач справа.

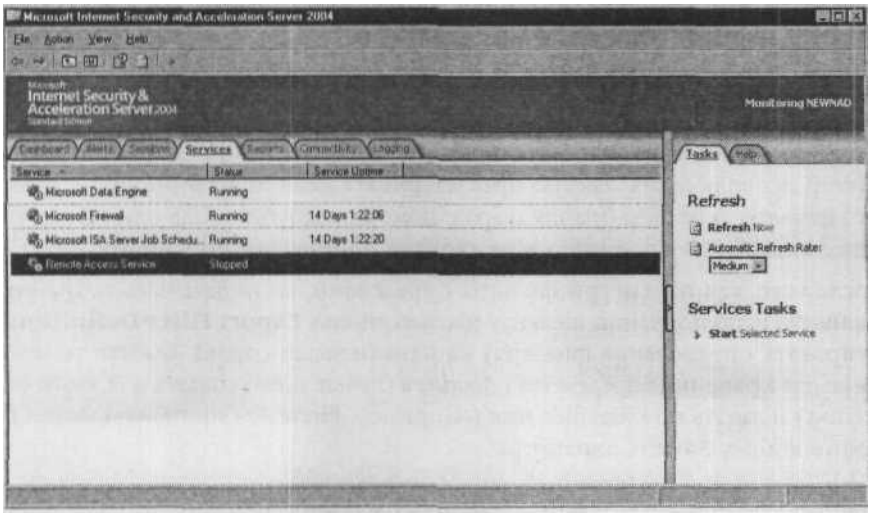


Рис. 12.35. Остановка и запуск служб

Работа с журналами и отчетами в ISA Server 2004

Возможность ведения журналов и создания отчетов в ISA Server — это значительный шаг вперед, предоставляющий пользователю документацию и рекомендующий действия, касающиеся ISA Server. В следующих разделах будут рассмотрены способы занесения данных в журналы ISA Server, конфигурирование журналов, а также методы создания отчетов на основе информации журналов.

Журналы ISA Server 2004

По умолчанию в журналах ISA Server 2004 фиксируются все компоненты. К ним относятся:

- Web-прокси;
- служба брандмауэра;
- SMTP Message Screener (отображение сообщений службы SMTP).

Способы организации журналов

По умолчанию журналы сохраняются с помощью машины баз данных MSDE (Microsoft Data Engine, машина базы данных корпорации Microsoft). Служба MSDE устанавливается вместе с установкой ISA Server 2004. Если в сети имеется SQL Server, то можно журналы хранить в базе данных SQL Server или же можно сохранять всю информацию в файле (формат Word Wide Web Consortium, W3C, или формат ISA Server). Каждый из этих способов имеет свои преимущества и недостатки.

> **ПРИМЕЧАНИЕ** Журнал SMTP Message Screener нельзя сохранять в базах данных MSDE или SQL. Его можно сохранить только в файле.

Сохранение журнала в базе данных MSDE

Для отображения информации, сохраненной с помощью MSDE, можно использовать средство просмотра журналов ISA Server 2004. При этом можно создавать запросы к БД и отыскивать нужную информацию. Это одна из основных причин, по которой авторам нравится формат MSDE. Объем одного журнала ограничен 2 Гб, но средство просмотра позволяет отображать информацию из нескольких журналов как поступающую из одного файла. Когда объем журнала достигает 2 Гб, ISA Server автоматически начинает новый журнал.

С помощью средства просмотра журнала можно также экспортировать информацию в текстовый файл, который удобно анализировать с помощью различных программных средств.

По умолчанию информация журнала в MSDE сохраняется в папке ISALogs, находящейся внутри папки, в которую установлен ISA Server.

Сохранение журнала в базе данных SQL Server

Сохранение информации в SQL Server **позволяет** использовать стандартный инструментарий запросов к БД. Существует определенная отказоустойчивость при хранении журналов на удаленном SQL-сервере. Однако если связь с SQL-сервером утеряна, то служба брандмауэра будет остановлена.

Кроме того, при хранении журналов на удаленном SQL-сервере существует ряд проблем, связанных с безопасностью. Если выбор сделан в пользу SQL Server, то корпорация Microsoft рекомендует использовать Windows-аутентификацию вместо SQL-аутентификации, кроме того, рекомендуется применять шифрование информации журналов, а также использовать протокол IPSec для шифрования пакетов, передаваемых от ISA Server на SQL-Server.

СОВЕТ При хранении журналов в БД SQL Server необходимо убедиться, что правило системной политики допускает удаленное ведение журнала с помощью транспорта NetBIOS на доверенных серверах ISA Server.

Сохранение журнала в файле

Если выбрано использование файла формата W3C, то данные сохранятся вместе с информацией о версии, дате ведения журнала и хранимых полях. В соответствии с форматом W3C поля в файле разделяются знаком табуляции.

Если выбрано использование файла формата ISA Server, то сохраняются непосредственно сами данные ISA Server и все поля, независимо от того, выбраны ли они, но невыбранные поля показываются пустыми (помечаются прочерком). В этом формате в качестве разделителя полей используется запятая.

Еще одно различие между этими двумя форматами состоит в том, что в файле формата W3C дата и время задаются в виде всеобщего скоординированного времени (Coordinated Universal Time, UTC), а в файле формата ISA Server используется локальное время, заданное на компьютере.

Файлы по умолчанию хранятся в папке ISALogs. По желанию местоположение можно изменить. Если раздел, на котором хранятся файлы, отформатирован под файловую систему NTFS (что рекомендуется), то для экономии места файлы журнала можно сжимать. Однако это может привести к уменьшению производительности (уменьшению времени доступа).

Размер файлов журналов формата W3C и ISA Server так же, как и в файлах MSDE, не должны превышать размер 2 Гб, но в этом случае новый файл открывается автоматически, когда достигается предельного размера. В ISA Server размер журнала отслеживается с десятиминутным интервалом.

ПРИМЕЧАНИЕ Независимо от способа ведения журналы должны всегда храниться в безопасном месте. Доступ к журналам должен строго контролироваться для предотвращения умышленного или случайного изменения.

Конфигурирование журнала

Можно сконфигурировать журнал отдельно для каждой службы (брандмауэра, Web-прокси и SMTP Message Screener). Нажмите вкладку **Logging** (Ведение журнала) в узле **Monitoring** (Наблюдение) и выберите один из вариантов **Configure Firewall Logging (Конфигурирование** журнала брандмауэра), **Configure Web Proxy Logging** (Конфигурирование журнала Web-прокси) или **Configure SMTP Message Screener Logging** (Конфигурирование журнала SMTP сообщений) на панели задач справа, как показано на рис. 12.36.

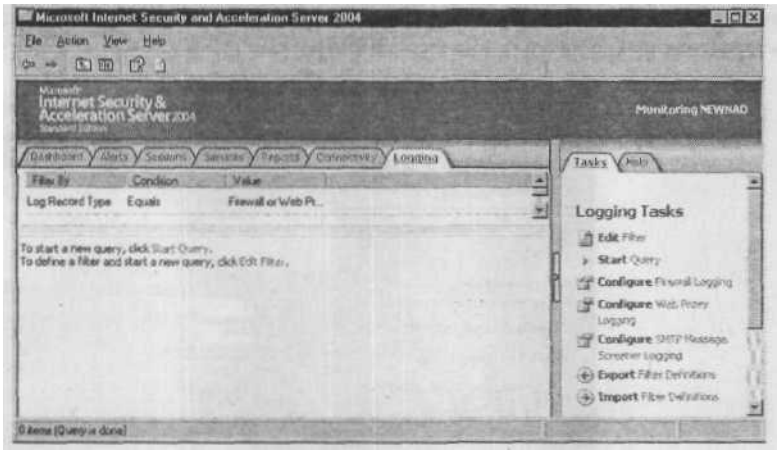


Рис. 12.36. Раздельное конфигурирование журналов

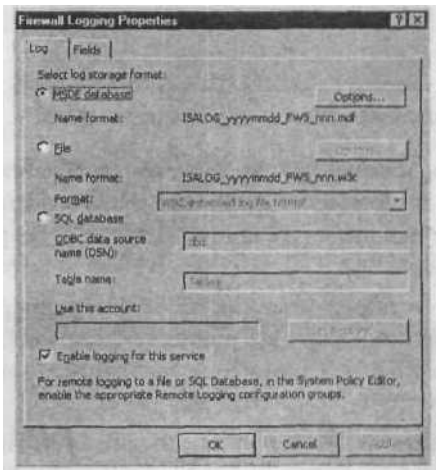


Рис. 12.37. Конфигурирование формата хранения журнала

Конфигурирование в основном для всех служб одинаково, за исключением некоторых отличий. В нашем примере будет сконфигурирован журнал для наблюдения за брандмауэром. Во-первых, необходимо убедиться, что активирован флаг **Enable logging for this service** (Разрешить ведение журнала для данной службы) в нижней части вкладки **Log** (Журнал) (по умолчанию помечен). Затем необходимо конфигурировать формат хранения журнала, как показано на рис. 12.37.

Конфигурирование записи журнала в MSDE

По умолчанию выбран именно формат MSDE. Для настройки формата необходимо щелкнуть мышью кнопку **Options** (Параметры), после чего появится диалоговое окно **Options** (Параметры), как показано на рис. 12.38.

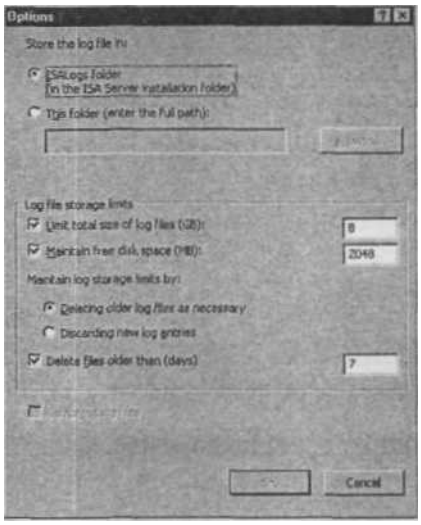


Рис. 12.38. Конфигурирование журнала для хранения в MSDE

Здесь можно выбрать, хранить файлы MSDE в установленном по умолчанию месте (в папке ISALogs) или в другом месте. Для смены местоположения необходимо ввести путь к нужной папке или щелкнуть кнопку **Browse** (Обзор), чтобы выбрать папку для хранения журналов.

Затем можно установить ограничение на общий размер файлов журнала в Гб. По умолчанию — 8 Гб. Можно также установить размер свободного дискового пространства, необходимого для обслуживания операций мониторинга в мегабайтах. Значение по умолчанию 2048 Мб (2 Гб).

Можно выбрать действие ISA Server по достижении максимального размера журнала: или удалить старые файлы для высвобождения места для новых, или запретить создание новых. Наконец, можно выбрать автоматическое удаление фай-

лов, которые были созданы заданное число дней назад (по умолчанию выбран именно этот вариант, а период времени по умолчанию равен 7 дням).

> **ПРИМЕЧАНИЕ** Вариант **Compress log files** (Сжатие журналов) выделен серым цветом, поскольку файлы MSDE сжимать невозможно. Сжимать можно только фалы формата W3C или собственного формата ISA Server.

На вкладке **Fields** (Поля) можно пометить поля, которые необходимо фиксировать в журнале, или снять пометку с тех полей, наблюдение за которыми не нужно. Если необходимо отслеживать все поля, можно щелкнуть мышью кнопку **Select All** (Выбрать все) или очистить все поля, нажав кнопку **Clear All** (Очистить все). По умолчанию выбраны все поля за исключением следующих:

- двунаправленность (bidirectional);
- прокси-источник (source proxy);
- прокси-адресат (destination proxy);
- имя хоста клиента (client host name);
- имя хоста-адресата (destination host name);
- сетевой интерфейс (network interface);
- IP-заголовок (raw IP Header);
- полезная нагрузка (raw payload).

Можно записывать в журнал только заданные по умолчанию поля, нажав кнопку **Restore Defaults** (Выбрать по умолчанию).

Конфигурирование записи журнала в файл

Если выбран вариант записи журнала в файл, необходимо из выпадающего списка выбрать формат файла: или собственный формат файла ISA Server, или расширенный формат W3C. Если нажать кнопку **Options** (Параметры), то появятся те же варианты, что и в случае с конфигурированием MSDE (место хранения файлов журнала, ограничение на размер, действия по достижению предельных размеров), но флаговая кнопка **Compress log files** (Сжимать файлы журнала) теперь будет доступна.

Конфигурирование записи журнала в базу данных SQL Server

Если выбран вариант записи журнала в БД SQL Server, то прежде всего необходимо настроить SQL Server для записи журналов ISA Server. Сюда относится настройка SQL Server для получения доступа к ODBC (Open Database Connectivity, открытый интерфейс доступа к базам данных) от ISA Server. Необходимо создать учетную запись SQL Server, если ISA Server и SQL Server находятся в одном домене Windows. При этом можно использовать Windows-аутентификацию. Если серверы находятся в разных доменах, не имеющих доверенной связи, необходимо использовать SQL-аутентифи каци ю.

Инструменты и ловушки

Настройка SQL Server для хранения журналов ISA Server

Для настройки SQL Server прежде всего необходимо подготовить базу данных SQL и таблицы. К счастью, на установочном диске ISA Server находятся два SQL-сценария fwsrv.sql и w3proxy.sql, которые создают таблицы, использующиеся для записи служебных данных Web-прокси и брандмауэра. Необходимо модифицировать эти сценарии, добавив SQL-операторы для использования существующей БД или создания новой для хранения таблиц. Для выполнения этих сценариев создания таблиц можно использовать средство SQL Query Analyzer (анализатор запросов SQL), входящее в состав SQL Server. После настройки SQL-таблиц необходимо сконфигурировать нужные права доступа для учетной записи Windows или SQL, которая используется в ISA Server, чтобы получить возможность запрашивать данные и записывать их в журнал.

После установки SQL Server на вкладке **Log** (Журнал) диалогового окна **Firewall Logging Properties** (Свойства ведения журнала брандмауэра) нужно ввести имя источника данных ODBC и имя таблицы. Затем необходимо создать пользовательскую учетную запись. Для этого в диалоговом окне щелкните мышью **Set Account** (Ввести учетную запись) и введите имя пользователя и пароль (дважды). Пользователь можно выбрать, нажав кнопку **Browse** (Обзор).

В редакторе системной политики (System Policy Editor) необходимо разрешить необходимость конфигурации групп удаленного ведения журнала (Remote Logging).

ПРИМЕЧАНИЕ Существует множество проблем, связанных с конфигурированием аутентификации SQL-сервера и созданием баз данных SQL Server, которые выходят за рамки данной главы. В любом случае необходимо обратиться к документации по SQL Server 2000 или загрузить SQL Server Bocks Online (обновлена в 2004 году) с Web-сайта корпорации Microsoft www.microsoft.com/sql/techinfo/productdoc/2000/books.asp.

Процедуры конфигурирования журналов Web-прокси или SMTP Message Screener аналогичны. Одно из главных отличий состоит в доступных полях. Кроме того, в диалоговом окне свойств SMTP Message Screener все форматы хранения (за исключением формата **File)** недоступны.

Использование средств просмотра журнала

Средство просмотра журналов показывает все сделанные записи в реальном масштабе времени. Событие отображается в программе просмотра сразу же после его фиксации в журнале. Для использования средства просмотра следует открыть вкладку **Logging** (Ведение журнала). Фильтр по умолчанию отображает все записи для журналов брандмауэра *и* Web-прокси. Для отображения этих записей нужно щелкнуть пункт **Start Query** (Начать запрос) на панели задач. Записи будут добавляться к

имеющимся в реальном **масштабе** времени до тех пор, пока не будет нажата кнопка **Stop Query** (Остановить запрос).

Поскольку средство просмотра журнала (рис. 12.39) содержит множество столбцов, можно закрыть дерево консоли и/или панель задач, для предоставления большего места. Но даже в этом случае, возможно, потребуются полосы прокрутки для того, чтобы просмотреть все столбцы.

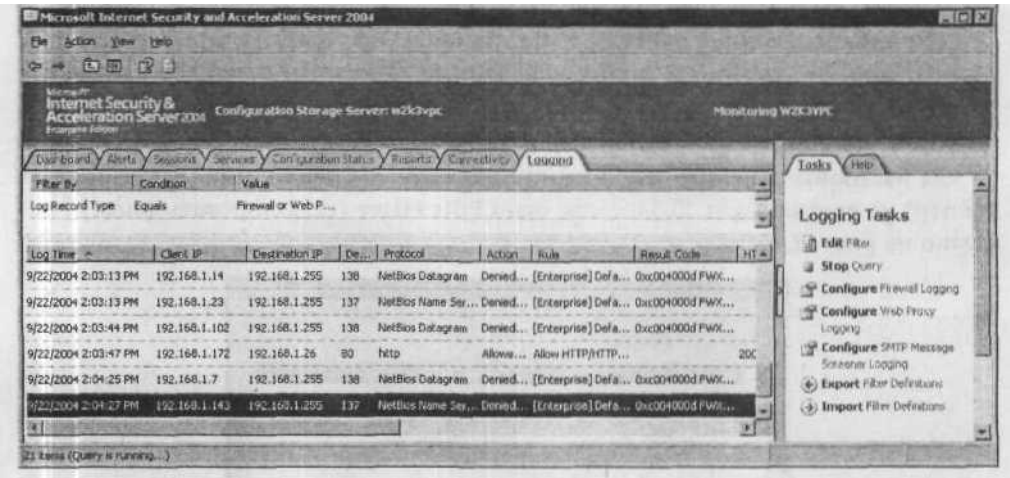


Рис. 12.39. Средство просмотра журнала с фильтром по умолчанию

По умолчанию будут показаны следующие столбцы:

- *Log Time* (Время события);
- *Destination IP* (IP адресата):
- *Destination port* (Порт адресата);
- *Protocol* (ПрОТОКОЛ);
- *Action* (Действие);
- *Rule* (Правило);
- *Client IP* (IP клиента);
- *Client user name* (Имя пользователя на клиенте);
- *Source network* (Сеть-источник);
- *Destination network* (Сеть-адресат);
- *HTTP method* (Метод HTTP);
- *URL* (Унифицированный локатор ресурса).

Можно добавить дополнительные столбцы, например ***MIME type*** (Тип MIME, Multipurpose Internet Mail Extensions, многоцелевые расширения электронной почты в сети), прокси-адресат или прокси-источник, сервер ссылок и многие другие. Для этого или просто для просмотра списка доступных столбцов нужно щелкнуть пра-

вой кнопкой мыши на заголовке любого столбца и выбрать в контекстном меню пункт **Add/Remove Columns** (Добавить/Удалить столбцы).

Фильтрование данных в журнале

Информацию журнала можно фильтровать так же, как информацию о сеансе связи. Как и в случае с фильтрами сеанса связи отображаться будут только записи, отвечающие всем заданным критериям.

Если журнал хранится в БД MSDE, можно проводить фильтрование по времени регистрации. Это позволяет отображать данные, заносимые за определенный период времени (в отличие от текущих данных). Время регистрации можно задать отличным от текущего. Такой просмотр называется автономным (offline).

Для настройки фильтра необходимо нажать кнопку **Edit Filter** (Редактировать фильтр) на панели задач. Диалоговое окно **Edit Filter** (Редактировать фильтр) показано на рис. 12.40.

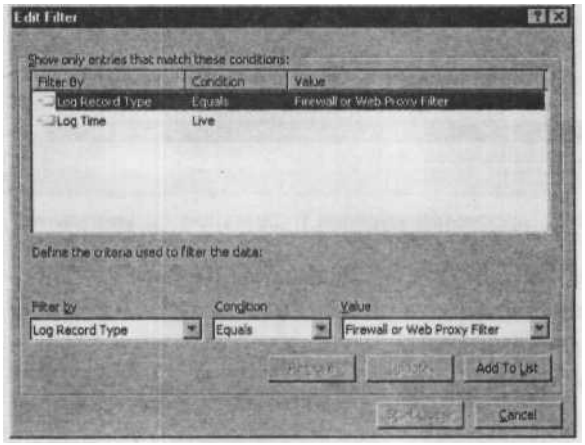


Рис. 12.40. Редактирование фильтра журнала

В поле Filter by (Фильтр по) нужно выбрать необходимый критерий.

ISA Server секреты

Невозможно удалить критерий по умолчанию

Обратите внимание, что критерий по умолчанию удалить невозможно. Если щелкнуть запись *Log Record Type* или *Log Time,* то кнопка **Remove** (Удалить) остается недоступной. Если попытаться создать новую запись для *Log Record Type* или *Log Time,* то при нажатии на кнопку **Add to List** (Добавить в список) будет выдано сообщение, что в запросе допустимо только одно выражение Log Record Type (или Log Time).

Итак, как же изменить эти параметры? Секрет прост: щелкните нужную запись или выделите ее, выполните изменения в поле **Value** (Значение), а затем нажмите кнопку **Update** (Обновить).

Для фильтра можно выбрать следующие критерии:
Action (Действие);
Authenticated client (Аутентифицированный клиент);
Bidirectional (Двунаправленность);
Bytes received (Полученные байты);
Bytes sent (Отправленные байты);
Cache information (Информация кэша);
Client agent (Агент клиента);
Client host name (Имя хоста клиента);
Client IP (IP клиента);
Client user name (Имя пользователя на клиенте);
Destination host name (Имя хоста-адресата);
Destination IP (IP адресата);
Destination network (Сеть-адресат);
Destination port (Порт адресата);
Destination proxy (Прокси адресата);
Error information (Ошибочная информация);
Filter information (Информация фильтра);
HTTP method (Метод HTTP);
HTTP status code, Log Record Type (Код статуса HTTP, тип записи журнала);
Log time (Время регистрации);
MIME type (Тип MIME);
Network interface (Интерфейс сети);
Object source (Объект-источник);
Original client IP (Исходный клиент IP);
Processing time (Время обработки);
Protocol (Протокол);
Raw IP header (Необработанный заголовок IP);
Raw payload (Необработанная полезная нагрузка);
Referring server (Сервер ссылок);
Result code (Результирующий код);
Rule (Правило);
Server name (Имя сервера);
Service (Служба);

- *Source network* (Сеть-источник);
- *Source port* (Порт-источник);
- *Source proxy* (Прокси источника);
- *Transport* (Транспорт);
- ШЛ (Унифицированный локатор ресурса).

Некоторые из этих критериев применимы только к одному или двум типам журналов (брандмауэр или Web-прокси).

После конфигурирования типа записи журнала можно выбрать отображаемые записи из фильтра брандмауэра или Web-прокси, только из фильтра брандмауэра или только из фильтра Web-прокси. Обратите внимание, что нельзя отображать записи из журналов SMTP Message Screener.

> **СОВЕТ** Записи в журнале SMTP Message Screener не появятся до тех пор, пока не будет сконфигурирован Message Screener на компьютере ISA Server.

После конфигурирования времени регистрации в поле ***Condition*** (Условие) значение по умолчанию будет **Live** (Текущее) — и это единственное значение, если записи производятся не в БД MSDE. Если же запись ведется в БД MSDE, то можно выбрать следующие варианты:

- *Last 24 hours* (Последние 24 часа);
- *Last 30 days* (Последние 30 дней);
- *Last 7 days* (Последние 7 дней);
- *Last hour* (Последний час);
- *Live* (Текущее время);
- *On or after* (В заданное время или после него);
- *On or before* (В заданное время или до него).

> **ПРИМЕЧАНИЕ** Если служба брандмауэра остановлена вручную или автоматически, средство просмотра журнала прекратит обновление информации, а ISA Server перейдет в режим изоляции. Служба брандмауэра может быть остановлена автоматически из-за возникновения некоторого события, настроенного на остановку этой службы, например при попытке проникновения. В режиме изоляции недопустим никакой другой трафик кроме **DHCP,** за исключением трафика, специально разрешенного в системной политике. Чтобы вывести ISA Server из режима изоляции, необходимо перезапустить службу брандмауэра.

Сохранение данных средства просмотра журнала в файле

Можно сохранить данные просмотра журнала в файле, копируя все результаты или же определенные данные в буфер обмена Windows. Для копирования выбранных результатов выделите записи, которые вы хотите скопировать (можно выбрать

несколько записей, удерживая клавиши <CTRL> или <SHIFT>). Щелкните пункт **Copy Selected Results to the Clipboard** (Скопировать выбранное в буфер обмена). Чтобы скопировать все результаты, щелкните пункт **Copy All Results *to* the Clipboard** (Скопировать все в буфер обмена).

Затем можно вставить скопированные результаты в текстовом редакторе, например в NotePad (Блокнот) (рис. 12.41).

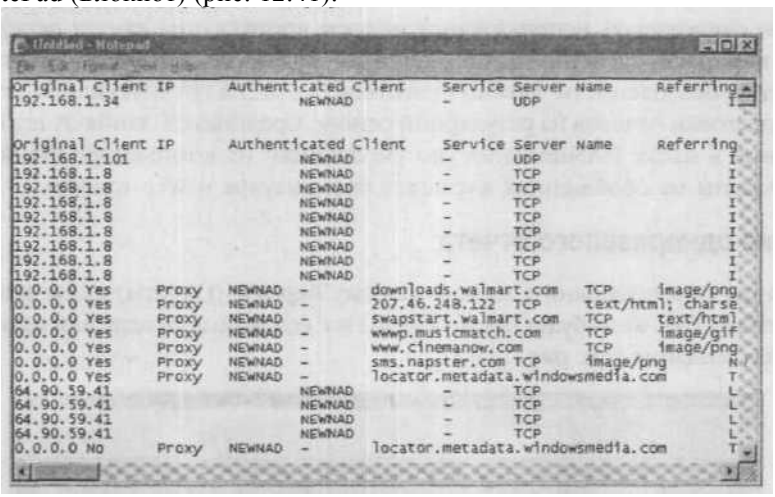


Рис. 12.41. Сохранение данных просмотра журнала с помощью копирования в буфер обмена

После того, как данные появились в текстовом редакторе, их можно сохранить в текстовом файле. Однако следует обратить внимание, что в программе просмотра журнала можно отобразить не более десяти тысяч записей, поэтому, если даже будут скопированы все результаты, в результирующем файле могут быть представлены не все записи.

Экспорт и импорт определений фильтра

Определения фильтра просмотра журнала можно сохранить точно так же, как и определения фильтра сеансов. Для этого нужно выбрать пункт **Export Filter Definitions** (Экспортировать определения фильтра) на панели задач и задать местоположение и имя файла. Определения фильтров сохраняются в xml-файлах. Их впоследствии можно будет загрузить, выбрав пункт **Import Filter Definitions** (Импорт определений фильтра) на панели задач.

Поскольку имеется очень много различных критериев фильтрования данных журнала, хорошо было бы иметь возможность сохранения множества различных фильтров и импортировать их по мере необходимости.

Создание, просмотр и публикация отчетов с помощью ISA Server 2004

Создание отчетов — это объединение всех отчетов, создание отчетов, обобщающих или детализирующих информацию журнала способом, который позволяет легко анализировать данные и их отдельные фрагменты, тенденции и аномалии.

Можно отслеживать использование полосы пропускания канала передачи данных для перераспределения потоков или же можно отслеживать доступ в целях обеспечения безопасности. Можно подготовить отчеты вручную или задать расписание подготовки отчетов на регулярной основе. Средство создания отчетов создает базу данных в папке ISASummaries (по умолчанию) на компьютере ISA Server. Отчеты основаны на обобщениях журналов брандмауэра и Web-прокси.

Создание одноразового отчета

Для создания отчета щелкните мышью вкладку **Reports** (Отчеты) в узле Monitoring (Наблюдение). При этом будут представлены все созданные отчеты или находящиеся в процессе создания (см. рис. 12.42).

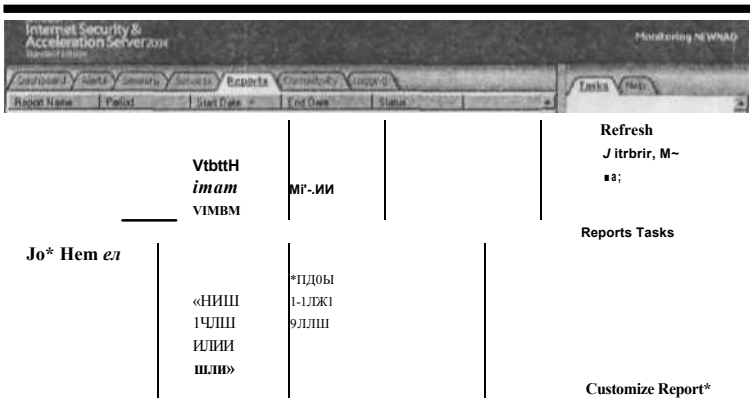


Рис. 12.42. Отображение отчетов

Для создания нового отчета щелкните пункт **Generate a New Report** (Создание нового отчета). При этом начнет выполняться мастер **New Report Wizard** (Мастер нового отчета). Этот мастер поможет вручную создать один одноразовый отчет. На первой странице необходимо задать название отчета.

На следующей странице мастера нужно выбрать тип содержимого, которое должно быть включено в отчет. Можно выбрать следующее:

- *Summary* (Сводная информация);
- *Web Usage* (Использование Web);
- *Application Usage* (Использование приложения);
- *Traffic and Utilization* (Трафик и использование канала передачи);
- *Security* (Безопасность).

В нашем примере (см. рис. 12.43) выбрано только использование Web.

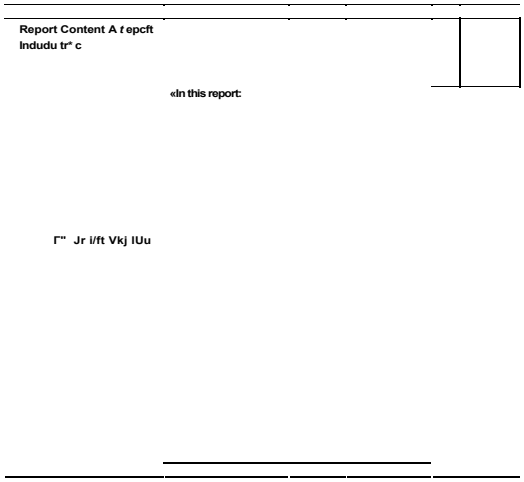


Рис. 12.43. Конфигурирование содержимого отчета

Нажмите кнопку **Next** (Далее), после чего вас попросят задать отчетный период (дату начала и конечную дату). Поскольку отчеты основаны на обобщении информации за день, текущую дату нельзя задавать в качестве конечной.

На следующей странице имеется возможность публикации отчета в каталог. Можно набрать путь к каталогу или выбрать папку для сохранения отчета. После нажатия кнопки **Browse** (Обзор) можно использовать кнопку **Make New Folder** (Создать новую папку) для создания новой папки, в которой будет храниться отчет. По умолчанию имя папки New **Folder** (Новая папка), но щелкнув правой кнопкой мыши на этом названии, можно переименовать папку прямо внутри диалогового окна **Browse for Folder** (Поиск новой папки).

Возможно, потребуется ввести имя учетной записи и пароль для учетной записи, чтобы получить возможность записи в определенный каталог. Для этого установите флаговый переключатель **Publish using this account** (Публиковать с использованием данной учетной записи), как показано на рис. 12.44, и нажмите кнопку **Set Account** (Установить учетную запись) для ввода имени учетной записи и верительных данных.

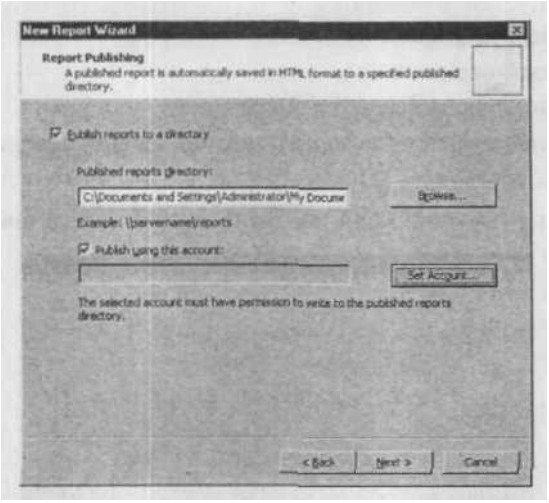


Рис. 12.44. Настройка публикации отчета

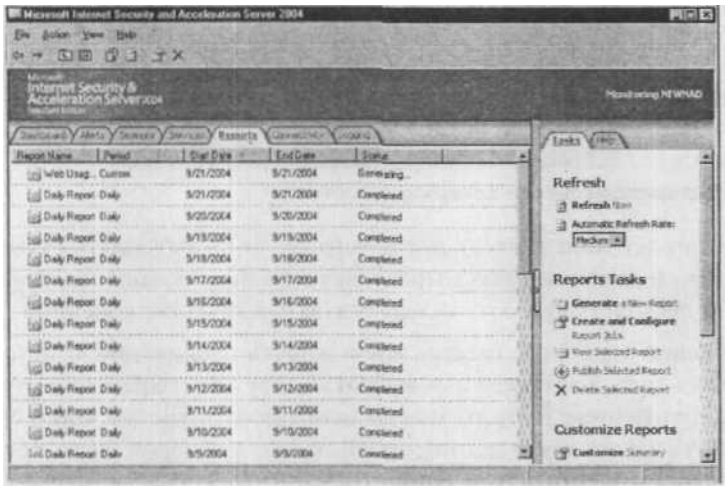


Рис. 12.45. Завершение создания отчета с помощью мастера

Отчет автоматически сохраняется в формате HTML.

На следующей странице мастера можно задать отправку уведомления по электронной почте после создания отчета. Необходимо ввести следующую информацию:

- имя SMTP-сервера или его IP-адрес;
- адрес, с которого будет отправлено уведомление;
- адрес, на который должно быть отправлено уведомление;

- CC: (копия) — адреса дополнительных получателей (если это нужно);
- содержимое уведомления.

Можно также установить флаговый переключатель для ввода ссылки на отчет внутри тела уведомления.

Последняя страница мастера обобщает все сделанные изменения. Для возврата к предыдущим страницам используйте кнопку **Back** (Возврат). Для начала создания отчета нажмите кнопку **Finish** (Готово). Отчет незамедлительно появится в списке отчетов со статусом ***Generating*** (Создается), как показано на рис. 12.45.

Поскольку это одноразовый отчет, в столбце ***Period*** (Период) будет указано ***Custom*** (Определено пользователем).

Автоматизация создания отчета

Можно настроить автоматическое создание ежедневных, еженедельных, ежемесячных или ежегодных отчетов. Это удобно при сопоставлении результатов. Например, можно создать ежедневный или еженедельный отчет об использовании Web.

ПРИМЕЧАНИЕ Для автоматического создания отчетов должна выполняться служба планировщика задач ISA Server Job Scheduler.

Для создания задания на отчет щелкните пункт **Create and Configure Report Jobs** (Создание и конфигурирование заданий на отчет) на панели задач справа. При этом откроется диалоговое окно Report **Jobs Properties** (Свойства задания на отчет), как это показано на рис. 12.46.

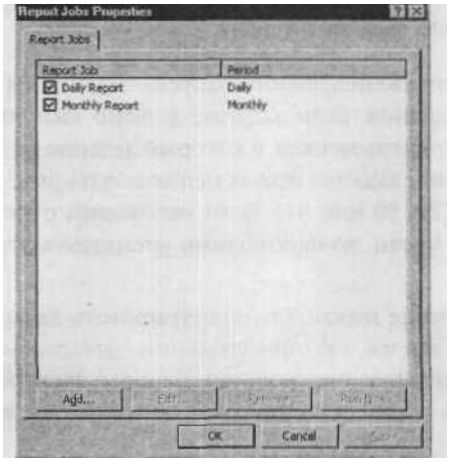


Рис. 12.46. Создание задания на отчет

Здесь будет представлен список *всех* запланированных заданий на отчеты. Чтобы добавить новое задание на отчет, нажмите кнопку **Add** (Добавить). При этом запу-

стится мастер создания нового задания на отчет — **New Report Job Wizard** (Мастер задания на новый отчет). На первой странице мастера необходимо задать имя отчета (например, Weekly Web Usage Report, еженедельный отчет об использовании Интернета).

На следующей странице можно настроить содержимое отчета точно так же, как для одноразового отчета.

На третьей странице (рис. 12.47) можно выбрать интервал времени для запуска задания на отчет: ежедневный, еженедельный или ежемесячный.

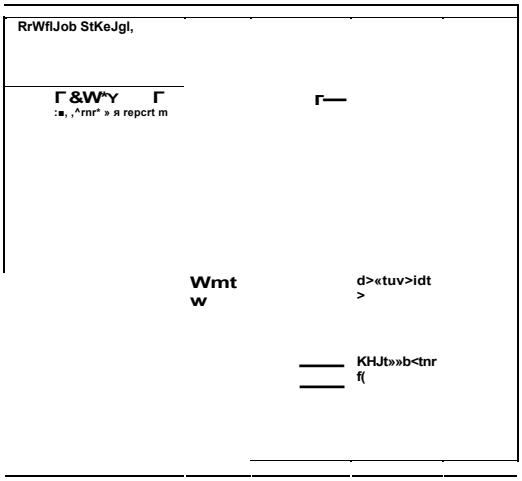


Рис. 12.47. Планирование задания на отчет

Если выбран вариант еженедельного запуска задания на отчет, можно выбрать день недели запуска задания. Если задание должно выполняться ежемесячно, то необходимо будет задать день месяца, в который задание должно выполняться. При ежемесячном выполнении задания нельзя использовать дни, которые не содержатся в некоторых месяцах (29, 30 или 31). Если необходим отчет, который охватывает весь предшествующий месяц, то необходимо установить это значение в 1 (первое число месяца).

На следующей странице можно сконфигурировать задание на публикацию отчетов в каталог точно так же, как при создании одноразового отчета. Следующая страница позволяет сконфигурировать сообщение электронной почты, которое необходимо отправить по завершении отчета, точно так же, как и при создании одноразового отчета.

Наконец, на последней странице мастера представлены все выполненные действия. При нажатии кнопки **Finish** (Готово), задание будет поставлено в расписание для выполнения в заданный день. По умолчанию отчет будет создаваться в 1 час ночи в заданный день. Это время можно изменить, выбрав задание на отчет в

диалоговом окне Report Job Properties (Свойства задания на отчет) и нажав кнопку Edit (Редактировать). Нужно щелкнуть вкладку Scheduler (Расписание), после чего можно изменить время создания отчета, как показано на рис. 12.48.

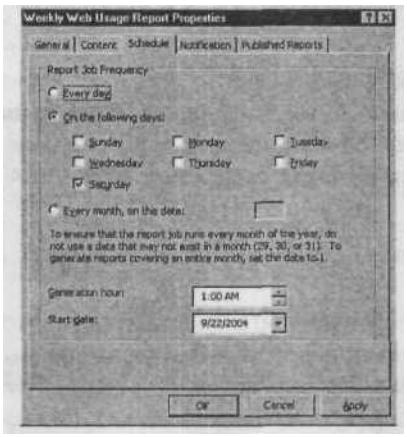


Рис. 12.48. Редактирование свойств задания на отчет

Другие задачи отчетов

Имеется множество других задач, связанных с отчетами, которые можно выполнять на панели задач. Можно сконфигурировать сводный журнал, щелкнув мышью пункт Configure Log Summary (Конфигурирование сводного журнала). При этом откроется диалоговое окно Log Summary Properties (Свойства сводного журнала) в котором можно разрешить или запретить ежедневные или ежемесячные сводки, установив флаговую кнопку, как показано на рис. 12.49.

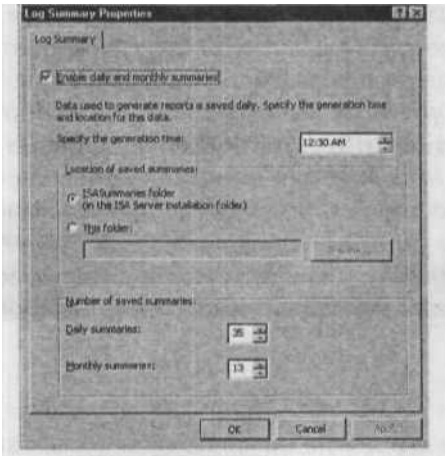


Рис. 12.49. Конфигурирование сводного журнала

Здесь можно также изменить время создания отчета по умолчанию **и** определить место хранения сводного **журнала** (по умолчанию он хранится в папке ISA-Summaries). Можно также **сконфигурировать** множество ежедневных или ежемесячных сводок для сохранения (от 35 до 999 ежедневных сводок и от 13 до 999 ежемесячных сводок).

ПРИМЕЧАНИЕ Необходимо помнить: сводные журналы — основа отчетов. Если использование базы данных сводного журнала невозможно, то ISA Server создаст ошибочную сводку при создании отчета. Однако при удалении сводок, которые были созданы до этого, ISA Server не будет создавать их вновь.

Можно настроить каждый тип содержимого отчета с помощью следующих средств панели задач:

- **Customize Summary Content** (Настройка содержимого сводки) Можно оп ределить количество протоколов, определить число **пользователей** в отчете, за дать способ сортировки для определения самых нагруженных сайтов, а также определить порядок сортировки по использованию кэша по запросам или по байтам;
- **Customize Web Usage Content** (Настройка **использования** Web-содержим ого) Можно определить число протоколов и определить порядок сортировки для определения важнейших протоколов (запросы, пользователи, входящие байты, исходящие байты или общее число байтов), определить число важнейших Web-сайтов и порядок сортировки, определить число важнейших пользователей и порядок их сортировки, определить число типов объектов и порядок их сорти ровки, определить число Web-браузеров и порядок их сортировки, а также оп ределить число операционных систем и порядок их сортировки;
- **Customize Application Usage Content** (Настройка содержимого использова ния приложения) Можно определить число важнейших протоколов и порядок их сортировки, число важнейших пользователей и порядок их сортировки, число **клиентских** приложений и порядок их сортировки, число адресатов и порядок их сортировки, а также число операционных систем и порядок их сортировки;

я Customize Traffic and Utilization Content (Настройка содержимого трафика и использования канала передачи данных) Можно определить число важнейших протоколов **и** порядок сортировки по использованию кэша;

- **Customize Security Content** (настройка содержимого безопасности) Можно определить число клиентов, которые создают наибольшее число отброшенных пакетов, *и* число пользователей, которые создают наибольшее число проблем с авторизацией.

Просмотр отчетов

После создания отчета его можно просматривать во вкладке **Reports** (Отчеты) в узле **Monitoring** (Наблюдение) консоли **ISA Server Management** (Управление ISA

Server). Дважды щелкните мышью название отчета, и он откроется в Web-браузере (рис. 12.50).

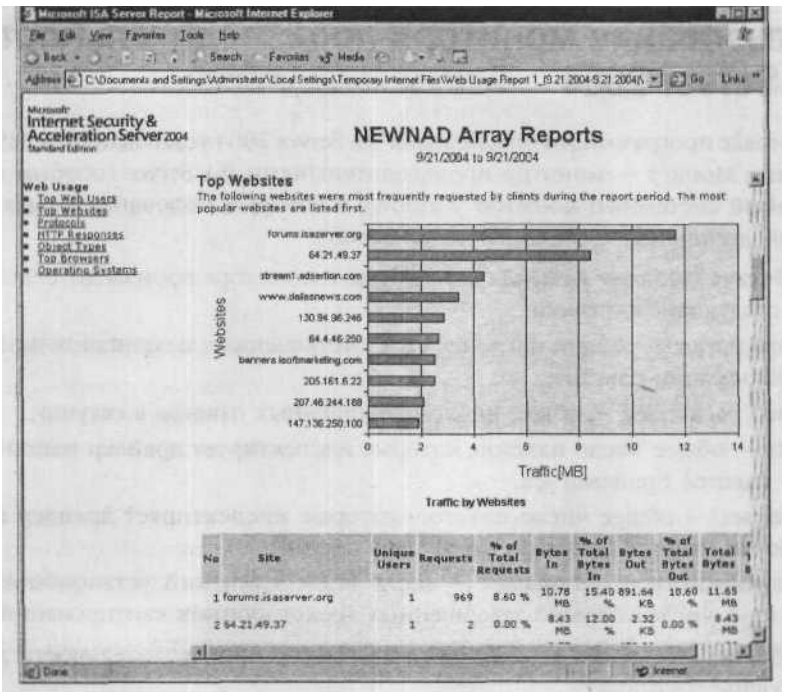


Рис. 12.50. Просмотр отчетов

Как видно, в отчетах используются графики и таблицы для облегчения восприятия информации, ее анализа и доступа к ней. Можно быстро перемещаться в различные разделы отчета, щелкая гиперссылки в левой части страницы.

Публикация отчетов

Если не выбрана автоматическая публикация отчета в каталог при конфигурировании задания на отчет, то можно опубликовать отчет после его создания. Необходимо просто выделить отчет, который необходимо опубликовать, и щелкнуть пункт **Publish Selected Report** (Опубликовать выбранный отчет) на панели задач.

Будет предложено выбрать местоположение файлов отчета. Щелкните ОК, и отчет будет опубликован (записан) в соответствующую папку. Будет создана новая подпапка внутри выбранной папки (имя папки будет состоять *из* имени отчета плюс дата). Здесь будут храниться все HTML-файлы и графические файлы отчета. Чтобы открыть отчет в данной папке, необходимо дважды щелкнуть файл с названием Report.html.

Отчеты необходимо публиковать, если они будут просматриваться на других компьютерах, а не только на компьютере с установленным ISA Server.

Использование монитора производительности в ISA Server 2004

При установке программного обеспечения ISA Server 2004 устанавливается ISA Server Performance Monitor — монитор производительности ISA Server (особым образом настроенный системный монитор Windows, в который включены только счетчики производительности, связанные с ISA Server).

Для *объекта ISA Server Firewall Packet Engine* в мониторе производительнос[т]и добавлены следующие счетчики:

- Dropped packets — общее число пакетов, отброшенных механизмом динамичес кой фильтрации пакетов;
- Dropped packet/sec — общее число отброшенных пакетов в секунду,
- Packets — общее число пакетов, которые инспектирует драйвер машины обра ботки пакетов брандмауэра;
- Packets/sec — общее число пакетов, которые инспектирует драйвер машины обработки пакетов брандмауэра за одну секунду,
- TCP established connections/sec — число TCP-соединений, установленных в се кунду (т. е. число успешно завершенных трехсторонних квитирований).

Для объекта *ISA Server Firewall Service* в монитор производительности добавлены следующие счетчики:

- Accepting TCP connections — число объектов-подключений, ожидающих TCP-подключения от клиентов брандмауэра;
- Active sessions — число активных сеансов брандмауэра;
- Active TCP connections — общее число активных TCP-соединений;
- Active UDP connections — общее число активных подключений по протоколу UDP;
- Available UDP mappings — число сопоставлений, **доступных** для UDP-соединений;
- Available worker threads — число рабочих потоков службы брандмауэра, ожида ющих завершения в очереди порта;
- Bytes read/sec — количество байт в секунду, считываемых механизмом переда чи данных;
- м Bytes written/sec — количество байт в секунду, записываемых механизмом передачи данных;
- DNS cache entries — текущее число записей доменных имен службы DNS. раз мещенных в кэше в процессе работы брандм-ауэра;
- DNS cache flushes — число сбросов, или очистки, кэша доменных имен DNS службой брандмауэра;

- DNS cache — число доменных *имен,* полученных службой брандмауэра из кэша DNS;
- DNS cache hits — доля (в процентах) доменных имен, полученных из кэша DNS, в общем числе разрешенных доменных имен;
- DNS retrievals — общее число доменных имен, полученных службой брандмауэра;
- Failed DNS resolutions — число неудачных API-запросов gethostbyname и gethostbyaddr. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра;
- Kernel mode data pumps — число созданных службой брандмауэра каналов передачи данных;
- Listening TCP — число объектов, ожидающих подключений по протоколу TCP от удаленных компьютеров Интернета;
- Pending DNS resolutions — число API-запросов gethostbyname и gethostbyaddr, ожидающих ответа. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра;
- Pending TCP connections — число TCP-соединений, ожидающих ответа;
- SecureNAT mappings — число сопоставлений, созданных по протоколу SecureNAT.
- Successful DNS resolutions — число полученных ответов на API-запросы gethostbyname и gethostbyaddr. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра;
- TCP bytes transferred/sec — количество байтов, передаваемых по протоколу TCP за секунду;
- TCP Connections Awaiting Inbound Connect Call — соединения от клиента службы брандмауэра после того, как соединение с Интернетом принято службой брандмауэра на прослушиваемом сокете;
- UDP bytes transferred/sec — количество байтов, передаваемых по протоколу UDP за секунду;
- Worker threads — число активных рабочих потоков службы брандмауэра.

Для объекта *ISA Server Web Proxy* в монитор производительности добавлены следующие счетчики"

- Active Web sessions — активные сеансы Web;
- Array bytes received/sec — скорость (байтов в секунду) входящих данных от других серверов массива;
- *ш* Array bytes sent/sec — скорость (байтов в секунду) исходящих данных, направленных другим серверам массива;
- Array bytes total/sec — сумма показаний двух предыдущих счетчиков. Отображает общую скорость обмена информацией между данным компьютером и другими серверами массива;
- Average milliseconds/request — среднее количество миллисекунд на запрос;
- Cache hit ratio *(%)* — доля (в процентах) клиентских запросов, обслуженных с использованием данных из кэша (счетчик Total Cache Fetches) в общем числе

клиентских запросов (счетчик Total Successful Requests). Наглядно представляет эффективнос[т]и работы кэша. Высокое показание счетчика указывает на большую долю запросов, обслуживаемых из кэша, то есть на снижение среднего времени отклика. Низкое значение часто обусловлено неоптимальной конфигурацией кэша — недостаточным его размером или большим числом запросов, не подлежащих кэшированию. Нулевое показание счетчика свидетельствует об отключенном кэшировании;

Cache hit ratio for last 10K requests — процент удачных обращений к кэшу для последних 10 000 запросов;

Client bytes received/sec — скорость (байтов в секунду) получения данных клиентам Web-прокси;

Client bytes sent/sec — скорость (байтов в секунду) передачи данных клиентам Web-прокси. Значение счетчика изменяется в зависимости от объема клиентских запросов, но неизменно низкие показания обычно указывают на задержки при обслуживании запросов;

Client bytes total/sec — сумма показаний двух предыдущих счетчиков. Отображает общую скорость обмена между ISA Server и клиентами Web-прокси;

Connect errors — число **ошибок** связи;

Connect errors/total errors *(96)* — отношение числа ошибок связи к общему числу ОШИбОК;

Current array fetches average milliseconds/request — среднее время обработки запросов (в миллисекундах), обслуживаемых с обращением к другому серверу массива. Запросы, обслуживающиеся по SSL-туннелям, не учитываются; Current cache fetches average milliseconds/request — среднее время обработки клиентского запроса (в миллисекундах) с использованием кэша. Не учитываются запросы, обслуживаемые по SSL-туннелям;

Current direct fetches average milliseconds/request — среднее время (в миллисекундах) обработки запросов клиента, при которой требуется обращение к Web-серверу или вышестоящему прокси. Не учитываются запросы, обслуживаемые по SSL-туннелям;

DNS cache entries — текущее число доменных имен, содержащихся в кэше Высокие значения счетчика говорят о существе нн ом приросте производительности, так как при разрешении доменных имен из кэша без обращения к серверу DNS снижается потребление системных ресурсов;

DNS cache flushes — число сбросов или очистки кэша доменных имен DNS службой Web-прокси. Кэш DNS сбрасывается при переполнении, то есть если не хватает места для размещения новых имен;

DNS cache hits — число доменных имен, полученных службой Web-прокси из кэша DNS. Сравнение показаний этого счетчика с показаниями двух предыдущих позволяет оценить эффективность работы кэша доменных имен. Низкое число попаданий кэша DNS снижает производительность, поскольку каждое

обращение к серверу DNS замедляет работу, особенно если при поиске возникают затруднения;

- DNS cache hits — доля (в процентах) доменных имен, полученных службой Web-прокси из кэша DNS, в общем количестве разрешенных доменных имен. Высо кие значения счетчика информируют о высокой производительности, поскольку большинство доменных имен получено из кэша, без обращения *к* серверу DNS;
- DNS retrievals — общее число доменных имен, полученных службой Web-про-**кси;**
- Failing requests/sec — число ошибок обращения к службе Web-прокси в секунду. Сравнение показаний этого счетчика с показаниями счетчика Requests/Sec дает представление о качестве обслуживания входящих запросов. Если большая часть входящих запросов завершается с **ошибкой,** ISA Server не справляется с обра боткой запросов. Возможные причины: некорректная конфигурация входящих подключений или низкая пропускная способность;
- Failing requests/total requests {%) — доля (в процентах) числа ошибок обраще ний к службе Web-прокси в общем числе запросов;
- FTP requests — число запросов FTP к службе Web-прокси. Постоянно низкие показания этого счетчика дают основания пересмотреть политику кэширова ния объектов FTP;
- HTTP requests — число запросов к службе Web-прокси по протоколу HTTP;
- HTTPS requests — число запросов к службе Web-прокси по протоколу HTTPS;
- Incoming connections/sec — число входящих соединений в сек;
- Ю errors to array member — ошибки ввода/вывода на сервере массива;
- Ю errors to array members/total {%) — отношение ошибок ввода/вывода сервера массива к общему числу ошибок в процентах;
- Ю errors to client — число ошибок ввода/вывода для клиента;
- Ю errors to client/total errors (%) — доля (в процентах) ошибок ввода/вывода для клиента в общем числе ошибок;
- Ю errors to server — число ошибок ввода/вывода на сервере;
- Ю error to server/total errors *{%)* — доля (в процентах) ошибок ввода/вывода на сервере в общем числе ошибок;
- Maximum users — максимальное число пользователей;
- Outgoing connections/sec — число исходящих соединений в сек;
- Requests from array member — количество запросов от элемента массива;
- Requests from array member/total errors *(%)* — доля (в процентах) числа запро сов от элемента массива в общем числе ошибок;
- Requests to array member — число запросов к элементу массива;
- Requests to array member/total errors (%) — доля (в процентах) числа запросов к серверу массива в общем числе ошибок;

- Requests with Keep Alive to array member — подтверждающие запросы к серверу массива;
- Requests with Keep Alive to array member/total errors (%) — доля (в процентах) числа подтверждающих запросов к элементу массива в общем числе ошибок;
- Requests with Keep Alive to client — число подтверждающих запросов к клиенту;
- Requests with Keep Alive to client/total errors (%) — доля (в процентах) числа подтверждающих запросов к клиенту в общем числе ошибок;
- Requests with Keep Alive to server — подтверждающие запросы к серверу;
- Requests with Keep Alive to server/total errors (%) — доля (в процентах) числа подтверждающих запросов к серверу в общем числе ошибок;
- Requests/sec — число запросов в сек;
- Reverse bytes received/sec — скорость (байтов в секунду), с которой служба Web-прокси принимает данные от опубликованных Web-серверов в ответ на запро сы извне. Показания этого счетчика помогают оценить уровень обслуживания ISA Server входящих запросов;
- Reverse bytes sent/sec. Скорость, с которой служба Web-прокси отправляет дан ные опубликованных Web-серверов в ответ на запросы внешних клиентов По казания этого счетчика помогают оценить уровень обслуживания ISA Server входящих запросов;
- Reverse bytes total/sec — сумма показаний двух предыдущих счетчиков. Представ ляет собой общую скорость обмена данными между службой Web-прокси и опубликованными Web-серверами;
- Sites allowed — общее число узлов Интернет, доступ к которым разрешен служ бой Web-прокси;
- Sites denied — общее число узлов Интернет, доступ к которым запрещен служ бой Web-прокси. Сравнение показаний этого и предыдущего счетчиков позво ляет оценить корректность конфигурации политики доступа;
- SNEWS sessions — общее число SNEWS-сеансов, обслуживающихся по SSL-туннелю.
- SSL client bytes received/sec — скорость приема данных службой Web-прокси от защищенных клиентов Web-прокси. Аналогичен счетчику Client Bytes Recicved/ Sec, но учитывает лишь данные, пересылаемые по SSL-туннелям;
- SSL client bytes sent/sec — скорость передачи данных службой Web-прокси за щищенным клиентам. Аналогичен счетчику Client Bytes Send/Sec, но учитывает только данные, пересылаемые по SSL-туннелям;
- SSL client bytes total/sec — сумма показаний двух предыдущих счетчиков. Пред ставляет собой общую скорость обмена данными по SSL-туннелям;
- Thread pool active sessions — число активных сеансов, обслуживаемых пулом потоков;
- Thread pool failures — число запросов, отклоненных из-за переполнения пула потоков;

- Thread pool size — число потоков в пуле потоков. Пул потоков представляет собой ресурсы, доступные для обслуживания клиентских запросов;
- Total array fetches — общее число клиентских запросов Web-прокси, обслужен ных с обращением к другим серверам массива, то есть запросов, выполняемых с применением протокола Cache Array Routing Protocol (CARP, протокол марш рутизации кэширования массива серверов), случайным образом размещающе го объекты в кэшах разных серверов массива. На показания этого счетчика влияет размер кэша отдельных серверов массива, поскольку сервер с кэшем большего размера обычно хранит больше объектов. Существует возможность настраивать коэффициент нагрузки отдельных серверов для распределения рабочей нагрузки между серверами массива;
- Total cache fetches — общее число клиентских запросов, выполненных с исполь зованием данных кэша. Высокие показатели этого счетчика свидетельствуют о высокой эффективности работы кэша;
- Total failing requests — общее количество запросов, которые служба Web-прокси не обслужила из-за ошибок, обусловленных невозможностью для службы Web-прокси обнаружить запрошенный URL-адрес или отсутствием у клиента прав на доступ к запрошенному адресу. Показания этого счетчика должны быть значи тельно ниже показаний счетчика Total Successful Requests. Если это не так, ве роятно, ISA Server не справляется с обслуживанием запросов. Причина может заключаться в ошибочной конфигурации, слишком низкой скорости подклю чения или слишком жестких ограничениях политики доступа;
- Total pending connects — общее число подключений к службе Web-прокси, на ходящихся в режиме ожидания прокси;
- Total requests — общее число успешно обработанных запросов к службе Web-прокси ;
- Total reverse fetches — общее число входящих запросов, выполненных с обра щением к опубликованным Web-серверам;
- Total SSL sessions — общее число SSL-сеансов, выполненных по SSL-туннелям.
- Total successful requests — общее число успешно обработанных запросов к службе Web-прокси. Сравнение показаний этого счетчика с показаниями счетчиков Total Failed Requests и Total Requests позволяет сделать вывод об уровне эффективно сти обслуживания запросов ISA Server;
- Total upstream fetches — общее число запросов, данные для которых запраши вались в Интернете или у вышестоящих прокси-серверов. Сравнение показаний этого счетчика с показаниями счетчика Total Cache Fetches позволяет опреде лить соотношение запросов, обслуживавшихся с использованием данных из Интернета или от вышестоящих прокси-серверов, и запросов, выполненных с использованием данных из кэша;
- Total users — общее чЛло пользователей, подключавшихся к службе Web-про кси. Применяется для сбора статистики использования сервера;

ш Unknown SSL sessions — общее число неопознанных SSL-сеансов, обслуженных по SSL-туннелям;

- Upstream bytes received/sec — скорость (байтов в секунду), с которой служба Web-прокси получает данные от удаленных серверов Интернета или вышестоящих прокси-серверов в ответ на свои запросы. Значение данного счетчика зависит от пропускной способности. Стабильно низкие показания счетчика свидетель ствуют о низкой скорости подключения. Это означает, что подключение стало «узким местом». Чтобы исправить положение, следует изменить приоритеты пропускной способности или увеличить скорость подключения;
- Upstream bytes sent/sec — скорость (байтов в секунду), с которой служба Web-прокси передает данные удаленным серверам Интернет или вышестоящим про кси-серверам. Значение данного счетчика зависит от пропускной способнос ти. Стабильно низкие показания счетчика свидетельствуют о низкой скорости подключения. Это означает, что подключение стало **«узким** местом». Чтобы ис править положение, следует изменить приоритеты пропускной способности или увеличить скорость подключения;
- Upstream bytes total/sec — сумма показаний двух предыдущих счетчиков. Пред ставляет собой общую скорость обмена данными между службой Web-прокси и удаленными серверами Интернета или вышестоящими прокси-серверами.

Можно добавлять или удалять счетчики, щелкая правой кнопкой мыши на заголовке любого столбца в нижней панели окна **System Monitor** (Системный монитор) и выбирая в контекстном меню пункт **Properties** (Свойства). На вкладке **Data** (Данные) выберите счетчики, которые необходимо удалить, и нажмите кнопку **Remove** (Удалить). Для добавления счетчика нажмите кнопку **Add** (Добавить) и выберите компьютер (локальный или компьютер из выпадающего списка), объект измерения производительности и счетчик (счетчики), которые необходимо добавить. Можно добавить счетчики для любого объекта, относящиеся не только к ISA Server.

Монитор производительности ISA Server конфигурируется тем же способом, что и монитор производительности Windows, при этом можно создавать журналы счетчика, журналы трассировок и предупреждения точно так же, как при наблюдении за другими показателями операционной системы Windows.

Краткое резюме по разделам

Инструментальная панель ISA Server 2004

И Инструментальная панель (Dashboard) — это новая функциональная возможность ISA Server 2004, облегчающая администраторам ISA Server оценку происходящего в различных наблюдаемых узлах.

0 Каждый раздел инструментальной панели содержит значок, указывающий на статус данной области.

0 Можно свертывать различные разделы инструментальной панели, если их не нужно просматривать.

И Раздел **Connectivity** (Связи) инструментальной панели позволяет наблюдать за связями между машиной ISA Server и другими компьютерами. Можно отслеживать работу отдельных компьютеров сети или даже подключаться к отдельному Web-серверу по URL

0 Раздел **Services** (Службы) инструментальной панели обеспечивает быструю проверку статуса служб, выполняющихся на компьютере ISA Server.

0 В разделе **Reports** (Отчеты) инструментальной панели можно увидеть имена созданных отчетов, их статус (создается или создан) и дату их создания.

0 Раздел **Alerts** (Оповещения) инструментальной панели позволяет быстро просмотреть события, занесенные в журнал событий компьютера ISA Server, время события, уровень события *(Information* — информационное, *Warning* — предупреждение или *Error* — ошибка) и число новых экземпляров данного события.

0 Раздел **Sessions** (Сеансы) инструментальной панели ISA Server упрощает просмотр типов сеансов связи и число активных сеансов, проходящих через наблюдаемый брандмауэр ISA Server 2004.

И Интерфейс раздела **System Performance** (Производительность системы) инструментальной панели ISA Server обеспечивает быстрый просмотр двух наиболее важных счетчиков ISA Server.

0 Вид инструментальной панели можно настроить по своему усмотрению.

Создание и конфигурирование оповещений в ISA Server 2004

0 Функция оповещений ISA Server 2004 позволяет **информировать** пользователя о важнейших событиях, происходящих в ISA Server, по мере их возникновения.

И Служба оповещений определяет время события и необходимость отправки оповещения об этом событии или выполнения других действий, в зависимости от конфигурации уведомления.

И Чтобы определить новое оповещения, нажмите кнопку **Add** (Добавить). После чего начнется работа мастера **New Alert Configuration** (Конфигурирование нового оповещения).

0 Можно назначить категорию для каждого оповещения и выбрать его уровень.

0 ISA Server можно настроить на определенные действия при возникновении событий, заданных для каждого оповещения.

0 Некоторые оповещения предопределены, но по умолчанию отключены.

0 Можно изменить свойства нового оповещения или свойства предопределенных оповещений.

0 Если щелкнуть мышью вкладку **Alerts** (Оповещение) в узле **Monitoring** (Наблюдение), то в средней панели будут отображены активные оповещения.

0 Окно оповещений автоматически обновляется по умолчанию с некоторым периодом времени.

Наблюдение за связями, сеансами и службами в ISA Server 2004

0 На вкладке **Connectivity** (Связи) можно наблюдать за связями между ISA Server и другими компьютерами.

И На вкладке **Sessions** (Сеансы) можно отслеживать текущие сеансы клиентов брандмауэра, Web-прокси и SecureNAT.

0 На вкладке **Services** (Службы) можно наблюдать статус служб ISA Server.

0 Для проверки связей можно использовать один из трех методов: ping, TCP-связь или HTTP-запрос.

И Для отслеживания связей с сервером по одному из этих трех методов необходимо создать верификатор связи (connectivity verifier) и поместить его в предопределенные группы.

И Если выбрать отслеживание HTTP-связи, то появится диалоговое окно, информирующее о том, что для этого необходимо сконфигурировать определенный адресат HTTP или HTTPS.

И Верификатор связи можно отключить или удалить, щелкнув правой кнопкой мыши и выбрав в контекстном меню пункт **Delete** (Удалить) или **Disable** (Отключить).

И После конфигурирования верификатора можно сразу увидеть наличие каких-либо проблем на серверах в определенной группе, просматривая раздел **Connectivity** (Связи) инструментальной панели.

Ш Удобное средство в ISA Server 2004 — возможность наблюдать сеансы связи в реальном масштабе времени, т. е. активность определенного клиентского компьютера (IP-адреса) с определенным пользователем (учетной записью).

В Можно отслеживать сеансы всех трех типов клиентов: брандмауэр, Web-прокси и SecureNAT.

И Для просмотра текущих сеансов, проходящих через ISA Server, нужно щелкнуть мышью вкладку **Sessions** (Сеансы). При этом будет выведен список сеансов.

0 Если сеансов связи, проходящих через ISA Server много, то будет трудно найти нужный. Для этого можно использовать механизмы фильтрования ISA Server 2004, которые позволяют сортировать данные сеансов и отображать только сеансы, отвечающие определенным критериям.

И Экспортируя фильтр в xml-файл, можно сохранять определения фильтра, чтобы использовать его впоследствии.

И Можно быстро отключить сеанс, щелкнув правой кнопкой мыши в окне **Sessions** (Сеансы) и выбрав в контекстном меню пункт **Disconnect Session** (Отключить сеанс).

Е По умолчанию в окне **Services** (Службы) средней панели показаны имена служб, статус каждой из служб (выполняется или остановлена) и в некоторых случаях срок работы службы (как долго служба выполняется в днях, часах и секундах).

Работа с журналами и отчетами в ISA Server 2004

В Возможность ведения журналов в ISA Server 2004 и создания отчетов значительно улучшена. Эти функциональные возможности обеспечивают постоянное документирование действий, связанных с ISA Server.

53 В журналах ISA Server по умолчанию регистрируются все компоненты, а именно: Web-прокси, служба брандмауэра и SMTP Message Screener (Построитель сообщений SMTP).

И Для просмотра информации, хранящейся в БД MSDE, можно использовать средство просмотра журналов ISA Server 2004.

И Хранение информации в БД SQL Server позволяет использовать для просмотра базы данных стандартный инструментарий языка SQL Кроме того, при хранении информации на удаленном SQL-сервере повышается отказоустойчивость и безопасность. Однако при потере связи с SQL-сервером служба брандмауэра останавливается.

Ш Безопасность — важная сторона реализации любого типа журналов.

0 Настройка журналов для хранения информации в БД SQL Server требует должного понимания проблем, связанных с безопасностью.

И Если выбран вариант хранения информации журналов в файле, то необходимо выбрать формат файла из выпадающего списка: либо собственный формат ISA Server, либо расширенный формат W3X.

И Журналы форматов W3C и ISA Server, так же как и файлы БД MSDE, ограничены размером 2 Гб, но новый файл открывается автоматически, при достижении предельного размера.

И Ведение журнала можно сконфигурировать отдельно для каждой из трех служб (брандмауэр, Web-прокси и SMTP Message Screener).

В Если выбран вариант сохранения журналов в БД SQL Serve, то прежде всего придется настроить SQL Server. Нужно сконфигурировать SQL Server для связи ODBC от ISA Server.

И На установочном диске ISA Server имеются файлы сценариев fwsrv.sql и w3proxy.sql для автоматического создания таблиц SQL.

И Средство просмотра журналов (log viewer) покажет записи в реальном масштабе времени, по мере их занесения в журнал.

0 Информацию журналов при просмотре можно фильтровать точно так же, как информацию о сеансах.

И После конфигурирования способа записи журнала, можно выбрать отображение записей от фильтра брандмауэра или Web-прокси, только от фильтра брандмауэра или только от Web-прокси. Обратите внимание, что невозможно отображать записи журнала SMTP Message Screener.

0 Отображаемые записи можно сохранить в файле, копируя в буфер обмена все результаты или только избранную информацию.

0 Можно сохранить определения фильтра точно так же, как и в случае с фильтрами сеансов, выбрав на панели задач пункт **Export Filter Definitions** (Экспорт определений фильтра), а также местоположение и имя файла.

0 Функция создания отчетов позволяет объединять отчеты, создавать отчеты или детализировать информацию, имеющуюся в файлах журналов, упрощая тем самым анализ данных, выявление тенденций и аномалий.

И Для создания нового отчета нужно на панели задач щелкнуть мышью пункт **Generate a New Report** (Создать новый отчет). После чего будет запущен мастер **New Report Wizard** (Мастер создания нового отчета).

0 Можно сконфигурировать задание на создание ежедневного, еженедельного или ежегодного отчета. Для этого нужно щелкнуть мышью на панели задач справа пункт **Create and Configure Report Jobs** (Создание и конфигурирование заданий на отчет).

0 После создания отчета можно просмотреть его на вкладке **Reports** (Отчеты) в узле **Monitoring** (Наблюдение) консоли управления ISA Server.

0 Если при конфигурации задания на отчет не выбран вариант автоматической публикации отчета в каталог, можно опубликовать отчет после его создания вручную.

И Отчеты необходимо публиковать, если они должны просматриваться на других компьютерах.

Использование монитора производительности в ISA Server 2004

Е При установке программного обеспечения ISA Server устанавливается монитор производительности (ISA Server Performance Monitor) — специальный вид системного монитора операционной системы Windows, в который включены только счетчики, имеющие отношение к ISA Server.

0 В монитор производительности добавлено большое количество счетчиков для объекта *ISA Server Firewall Packet Engine,* объекта *ISA Server Firewall Service* и объекта *ISA Server Web Proxy.*

0 Можно добавить или удалить счетчик, щелкнув правой кнопкой мыши на заголовке столбца в нижней части панели окна **System Monitor** (Системный монитор) и выбрав в контекстном меню пункт **Properties** (Свойства).

И Монитор производительности ISA Server конфигурируется точно так же, как и **системный** монитор Windows. Можно создавать журналы счетчиков, отслеживать журналы и оповещения, точно так же, как и в случае наблюдения за другими параметрами Windows.

Часто задаваемые вопросы

Приведенные ниже ответы авторов книги на наиболее часто задаваемые вопросы рассчитаны как на проверку понимания читателями описанных в главе концепций, так и на помощь при их практической реализации. Для регистрации вопросов по данной главе и получения ответов на них воспользуйтесь сайтом www.syngress.com/solutions (форма **«Ask the Author»).** Ответы на множество других вопросов см. на сайте ITFAQnet.com.

В: Мой ISA Server настроен на блокировку анонимных пользователей, но при просмотре журнала я вижу анонимные запросы. Что я сделал неправильно?

О: Даже если вы потребуете аутентификацию всех пользователей, первичный запрос пользователя отправляется анонимно и регистрируется, как анонимный. Если требуется аутентификация, ISA Server автоматически возвращает на анонимный запрос сообщение 407 (authentication required, требуется аутентификация). Затем пользователь отправляет точно такой же запрос вновь с верительными данными аутентификации NTLM. ISA Server отвечает еще одним сообщением 407 и отправляет запрос на аутентификацию. Далее пользователь отправляет тот же запрос с ответом на запрос аутентификации. Однако первые два обмена данными будут зарегистрированы как анонимные.

В: Я сконфигурировал уведомление, при выполнении условий которого запускается определенная программа. Событие отображается в обоих окнах **Alert** (Оповещение): узла ISA Server Monitoring и средства просмотра событий Windows, но программа не выполняется, как я того ожидал. Что случилось?

О: Скорее всего, учетная запись пользователя, от имени которой выполняется программа, не имеет на это соответствующих прав. Для того чтобы выполнить действие по уведомлению, учетная запись должна иметь привилегию **Logon as batch job** (Регистрация для пакетного задания). Если это не так, действие выполняться не будет. Для решения проблемы или определите другую учетную запись для выполнения нужной программы (которая имеет привилегию **Logon as batch job),** или дайте учетной записи пользователя эту привилегию.

В: Я сконфигурировал уведомление и выбрал вариант отправки сообщения по электронной почте на свой адрес при активации уведомления. Событие отображается в окне **Alerts** (Оповещение) узла ISA Server Monitoring и средства просмотра событий Windows. Но сообщения по почте я не получил. Что случилось?

О: Необходимо проверить конфигурацию SMTP-сервера, заданного для отправки почтовых сообщений. Если это внешний SMTP-сервер, сообщение по электронной почте не может быть отправлено до тех пор, пока не будет определено правило, позволяющее локальному хосту получать доступ к внешнему SMTP-серверу. Если это внутренний SMTP-сервер сети, необходимо определить правило системной политики, позволяющее локальному хосту сети получать доступ к внутренней сети с помощью SMTP-протокол а.

В: На инструментальной панели я вижу «No connectivity» (нет связи) для всей группы **Web** (Интернет), но когда я проверяю вкладку **Connectivity** (Связь), только на одном из пяти Web-серверов группы имеются проблемы. Почему инструментальная панель указывает на обрыв связи?

О: Инструментальная панель указывает на наихудший вариант, поэтому вы должны понимать, что проблема случилась с одним или более серверов в группе. Если на каком-либо сервере группы существует проблема, статус группы отображает ее. Помните, что инструментальная панель предназначена только для предварительной информации. Для подробных сведений необходимо перейти на соответствующую вкладку (в данном случае на вкладку **Connectivity** (Связь)).

В: Я знаю, что могу установить диапазон обновления для различных вкладок, выбрав **None** (Никогда), **Low** (Редко), **Medium** (Средне) или **High** (Часто) на панели задач справа. Что означают эти диапазоны в действительности? Как часто обновляются окна в каждом случае?

О: Если частота обновления выбрана **None** (Никогда), то окно не будет обновляться никогда (его можно обновить вручную, нажав кнопку **Refresh** в верхней части панели инструментов или щелкнув мышью значок **Refresh Now** в правой части панели задач). Если частота обновления установлена как **Low** (Редко), окно обновляется каждые 120 сек. Вариант **Medium** (Средне) предполагает обновление каждые 60 сек. В случае значения **High** (Часто) — каждые 30 сек.

В: Я сконфигурировал уведомление, инициирующееся в случае, когда происходит пятикратное проникновение в DNS, установив на вкладке **Events** (События) значение **Number of occurrences** (Число возникновений) равным 5. Однако я вижу в журнале, что событие проникновения в DNS происходило точно пять раз, но уведомление не было инициировано. Почему?

О: Когда задано значение поля Number **of occurrences** (Число возникновений), уведомление будет инициироваться при следующей попытке после заданного значения. Поэтому, если установлено значение 5, уведомление не будет инициировано до появления события в 6-й раз.

В: Я установил ежемесячное создание отчета по использованию Web, который должен создаваться в последний день каждого месяца (31-го числа), чтобы я мог получить данные за весь месяц. Однако за последний месяц (сентябрь) отчет не был создан. Могу ли я вручную запускать создание отчета каждый месяц для того, чтобы получить данные за весь предыдущий месяц? Если задать значение 28 (поскольку в каждом месяце есть, по крайней мере, 28-е число) у меня не будет данных по последним дням тех месяцев, где есть числа после 28-го.

О: Если день месяца создания отчета не существует (например, в сентябре только 30 дней) отчет не будет создан. Решение простое: создавайте отчет 1-го числа каждого месяца. Поскольку отчеты создаются на основе обобщенных данных, то 1-е число не будет учитываться в отчете (этот день еще не закончился). Поэтому вы получите данные за весь предыдущий месяц, независимо от количества дней в нем.