Джерри Ли Форд

Персональная ЗАЩИТА от ХАКЕРОВ

руководство для начинающих

ЮНИТИ

ЮДИЦ-ОБРАЗ

Jerry Lee Ford

Absolute Beginner's Guide to Personal Firewalls

que

201 West 103rd street,
Indianapolis, Indiana 46290

Джерри Ли Форд

Персональная защита от хакеров

Руководство для начинающих

перевод с английского

КУДИЦ-ОБРАЗ
Москва • 2002

Джерри Ли Форд.
Персональная защита от хакеров. Руководство для начинающих. Пер. с англ. - М.: КУДИЦ-ОБРАЗ, 2002. - 272 с.

ISBN 0-7897-2625-4
ISBN 5-93378-041-3

Эта книга начинает с основ безопасности вашего компьютера, таких, как определение необходимости в средствах защиты и его текущего уровня защищенности. Далее в ней показывается и достаточно подробно объясняется, как усилить защищенность, выбрать высокоскоростное подключение к Интернету, установить средства защиты персонального компьютера и оценить новый уровень защищенности.

Книга дополнена материалами, отражающими специфику Интернета в России и в странах СНГ.

Джерри Ли Форд.
Персональная защита от хакеров. Руководство для начинающих

Учебно-справочное издание

Корректор М. Матёкин
Перевела с англ. Ю. Алабина
Научный редактор Д. Миронов, IBM Certified Advanced Technical Expert - RS/6000 AIX

Лицензия ЛР № 071806 от 2.03.99, НОУ "ОЦ КУДИЦ-ОБРАЗ"
119034, Москва, Гагаринский пер., д. 21, стр. 1. Тел.: 333-82-11, ok@kudits.ru

Подписано в печать 26.04.2002.
Формат 70x100/16. Бум. офсетная. Печать офс.
Усл. печ. л. 21,9. Тираж 3000. Заказ 301

Отпечатано с готовых диапозитивов в ООО "Типография ИПО профсоюзов Профиздат", 109044. Москва, Крутицкий вал, 18.

ISBN 0-7897-2625-4 © QUE, 2002
ISBN 5-93378-041-3 © НОУ "ОЦ КУДИЦ-ОБРАЗ", 2002

Об авторе

Джерри Ли Форд-младший - писатель, преподаватель и аналитик компьютерной безопасности с 13-летним опытом в области информационных технологий. Он имеет степень магистра в бизнес-администрировании Университета штата Вирджиния "Virginia Commonwealth University", город Ричмонд, штат Вирджиния, и более чем пятилетний преподавательский опыт в области информационных технологий. Джерри - дипломированный инженер, системный программист компании "Microsoft" и является автором еще шести книг, включая "Практическое руководство по одноранговым сетям Microsoft Windows". Он живет в городе Ричмонд, штат Вирджиния со своей женой Мэри, и сыновьями Александром и. Уильямом.

Посвящение

Мэри, Александру и Уильяму.

Благодарность

Эта книга является результатом объединенных усилий ряда людей. Я хочу поблагодарить Говарда Джонса за его работу в качестве литературного редактора книги, Джоаниз Ульрич за приложение сил в качестве технического редактора и Шерри Грегори, редактора по продажам. Я также хочу поблагодарить всех работников издательства "Que" за то, что так напряженно работали, чтобы помочь мне сделать эту книгу реальностью. И в заключение хочу сказать спасибо моей жене Мэри за то, что переложила на себя большую часть домашних забот, чтобы я мог найти время написать эту книгу.

Скажите нам, что вы думаете!

Как читатель этой книги, вы для нас наиболее важный критик и комментатор. Мы ценим ваше мнение и хотим знать, что мы делаем правильно, что мы можем делать лучше и в каких областях деятельности вы хотели бы увидеть наши публикации, а также услышать другие разумные пожелания, посланные в наш адрес.

Как один из издателей издательства "Que", я буду рад вашим замечаниям. Вы можете послать их по факсу, электронной почте или написать лично мне, чтобы уведомить меня о том, что вам понравилось в данной книге, а что нет, а также что мы можем сделать, чтобы улучшить наши книги.

Пожалуйста, примите во внимание, что я не могу помочь вам с техническими проблемами, относящимися к теме данной книги, и что в связи с большим объемом получаемой мной почты я могу быть не в состоянии ответить на каждое послание.

Пожалуйста, убедитесь, что в письме вы указали название книги и имя автора, а также ваше имя и номер телефона или факса. Я внимательно просмотрю ваши замечания и поделюсь ими с автором и редакторами, работавшими над книгой.

Факс: 317-581-4666

E-mail: *feedback@quepublishing. com*

Почтовый адрес: США, 46290 Индиана, Индианаполис, Уэст 103 Роуд Стрит, 201, издательство "Que", Грег Уиганд.

Введение

Для чего вам нужна эта книга?

Прошло не так много лет с тех пор, как был выпущен первый персональный компьютер. Преимущества персональных компьютеров были очевидны, но ограничены, поскольку каждый компьютер был замкнутым миром. Через несколько лет основные усилия стали вкладываться в выяснение того, как объединить компьютерные системы. Со времени первых локальных сетей мы в настоящее время доросли до Интернета, где миллионы компьютеров со всего мира совместно используют обширную и открытую сеть ресурсов и информации.

Возможность соединения больше не является главной проблемой. Центральным вопросом стала скорость соединения. Это привело к появлению модемов со скоростью передачи 56 Кб/с, а в последнее время - к развитию кабельных и цифровых соединений, Поскольку кабельные и цифровые соединения всегда подключены к Интернету, ждать не приходится. Доступ мгновенен. Однако все эти прекрасные соединения имеют одно слабое место: безопасность.

Получается, что те же инструменты, которые обеспечивают пользователей доступом ко всей информации и ресурсам Интернета, могут обернуться против них. Появились хакеры, новое поколение людей, которые преуспевают на взломе компьютерных сетей.

Большинство людей хранит в своих персональных компьютерах большое количество ценной информации, такой, как личные финансовые записи и электронные записные книжки, которой они не хотят делиться с другими людьми. Однако многие люди не понимают, что когда они соединяются на своем персональном компьютере с Интернетом, они также соединяют с собственным компьютером Интернет, в котором любой человек с небольшим знанием технологии взлома может попытаться проникнуть в ваш компьютер и просмотреть его содержимое.

Чтобы защититься от этого воздействия, вам необходимо установить барьер, который предостережет нежелательных посетителей от проникновения в ваши домашние компьютеры, не уменьшая при этом вашей способности путешествовать по Интернету. Здесь и начинают действовать средства межсетевой защиты. В данной книге вы узнаете о рисках, связанных с безопасностью, которые возникают, когда вы соединяетесь с Интернетом, и как вы можете использовать персональный брандмауэр для защиты от внешних угроз. Вы узнаете, как работают персональные брандмауэры, как их установить и как они защищают ваш компьютер. Вне зависимости от того, используете ли вы коммутируемое или высокоскоростное кабельное или цифровое соединение с Интернетом, вы убедитесь, что книга "Персональные средства межсетевой защиты. Руководство для начинающих" может помочь вам путешествовать по сети быстрее и безопаснее.

Что вам необходимо для того, чтобы начать

Чтобы эффективно использовать эту книгу, все, что вам необходимо, это персональный компьютер, соединение с Интернетом и персональный брандмауэр. Ваше соединение с Интернетом может быть коммутируемым, через кабельный модем или цифровую абонентскую линию. Если вы не уверены, какой персональный брандмауэр вы хотите использовать, прочтите сначала эту книгу: она поможет вам принять решение. В этой книге описывается большое количество персональных средств межсетевой защиты, как на программной, так и на аппаратной основе. Вы узнаете о преимуществах и недостатках программных и аппаратных брандмауэров и о том, как определить, какой из них вам подойдет. Вы также найдете информацию о том, где можно скачать несколько действительно хороших и бесплатных брандмауэров.

Как устроена эта книга

Эта книга состоит из 11 глав и трех приложений. В главах 1–4 изложена основная информация, требуемая для понимания остальной части книги. Остальные главы описывают отдельные темы.

Глава 1 "Зачем вам нужен персональный брандмауэр?" познакомит вас с высокоскоростным доступом в Интернет и расскажет о необходимости защитить ваш домашний компьютер с помощью персонального брандмауэра. Вы также познакомитесь с хакерами и сообществом хакеров.

В главе 2 "Высокоскоростные соединения с Интернетом означают повышенную уязвимость" представлена дополнительная информация о соединениях с помощью кабеля или цифровой абонентской линии и объясняется, как установить и сконфигурировать ваше кабельное или цифровое соединение с максимальной производительностью. В этой главе также объясняется, почему высокоскоростные соединения менее безопасны и почему вам необходимо защитить их с помощью персональных брандмауэров.

В главе 3 "Описание брандмауэров" описываются различия между аппаратными и программными персональными брандмауэрами и дается более глубокое представление о том, как работают персональные брандмауэры. Эта глава также дает общее представление о протоколе TCP/IP и сущности процесса передачи данных по сети.

В главе 4 "Защита сетей в Windows" раскрывается информация о дырах в безопасности сетей Microsoft и описываются пути по защите некоторых из них. Кроме того, в главе говорится о преимуществах модернизации Windows на более безопасную версию.

Глава 5 "Аппаратные средства межсетевой защиты" знакомит с кабельно-цифровыми маршрутизаторами и объясняет, как они могут быть использованы в качестве персональных брандмауэров. В данной главе показано, как установить и сконфигурировать эти устройства. Разделы главы включают описание таких свойств, как блокировка IP-адреса и просмотр лог-файлов брандмауэра.

В главе 6 "Персональный брандмауэр McAfee" показывается, как устанавливать, конфигурировать и работать с этим персональным брандмауэром. Вы узнаете, как конфигурировать доверяемые приложения и настройки сетевой безопасности. Описаны все основные свойства этого брандмауэра, включая работу с предупреждениями и лог-файлами.

Глава 7 "BlackICE Defender" содержит полное описание этого персонального брандмауэра. Вы узнаете, как установить и сконфигурировать его, а также как установить параметры безопасности. В главе описаны все основные свойства этого брандмауэра, включая то, как анализировать события безопасности и информацию, собранную о нападающих.

Глава 8 "ZoneAlarm" предоставляет исчерпывающее описание данного персонального брандмауэра. В главе показано, как установить и сконфигурировать этот персональный брандмауэр, и описано каждое основное свойство приложения. Вы узнаете, как использовать параметры настройки безопасности программы ZoneAlarm и конфигурировать доверяемые приложения. Вы также узнаете, как анализировать лог-файлы программы ZoneAlarm и активировать ее свойство автоматического обновления.

В главе 9 "Насколько защищен ваш компьютер?" показано, как запустить бесплатное Интернет-сканирование безопасности вашего домашнего компьютера для того, чтобы вы могли проверить эффективность вашего персонального брандмауэра. Кроме того, в главе рассматриваются результаты типового сканирования, чтобы помочь вам при анализе его результатов.

Глава 10 "Навыки путешественников по сети, осознающих важность безопасности" представляет собой набор дополнительных задач, которые вы можете выполнить, чтобы еще больше повысить уровень вашей безопасности при соединении с Интернетом. Кроме того, в ней вы найдете описание рекомендуемых положительных навыков сетевых путешественников и советы по поддержанию вашего компьютера и его приложений на уровне современных требований.

В главе 11 "Домашние сети и общее подключение к Интернету" показано, как наладить вашу собственную домашнюю сеть и обезопасить ее с использованием комбинации аппаратных и программных персональных брандмауэров. В главе представлены несколько вариантов защиты вашей домашней сети и объяснены отличия каждого варианта.

В приложении А "Другие средства межсетевой защиты" представлен список дополнительных брандмауэров и дано краткое описание каждого из них.

В приложении Б "Другие web-сайты, которые проверят вашу безопасность" дополнен материал, представленный в главе 9, в нем перечислен ряд дополнительных web-сайтов, которые предоставляют бесплатные сканирующие программы, проверяющие уровень защищенности, которые вы можете запустить для проверки средств защиты вашего компьютера.

Глоссарий содержит список терминов и определений, к которому вы можете обращаться по мере чтения книги.

Как пользоваться книгой

Эта книга предназначена для прочтения от начала до конца. Однако, в зависимости от вашего опыта и интересов, вы, возможно, нуждаетесь в прочтении только отдельных частей. Главы 1–4 предоставляют необходимые сведения для чтения остальной книги. Главы 5-8 описывают отдельные персональные брандмауэры. Вы можете прочитать по крайней мере одну из этих глав. Если вы заинтересованы в максимальном повышении уровня безопасности вашего компьютера, вы можете прочитать главу *5* "Аппаратные брандмауэры", а затем одну из трех глав, описывающих программные брандмауэры.

Важнейшим предметом изучения является запуск сканирующей программы для проверки уровня безопасности вашего брандмауэра, описанный в главе 9. В главе 10 представлены дополнительные советы по обеспечению безопасности вашего компьютера, которые вы можете найти полезными. Главу 11 необходимо прочитать, если у вас есть домашняя сеть, иначе вы можете пропустить ее. Наконец, приложения могут быть использованы как дополнения к материалу, изложенному в главах.

Соглашения, принятые в этой книге

Команды, указания и пояснения в данной книге представлены в наиболее четкой и понятной форме. Следующие пункты являются характерными деталями текста, облегчающими пользование этой книгой:

- *команды, которые вы должны ввести* - команды, которые вы должны ввести, легко определяются по специальному формату: жирный моноширинный шрифт. Например, чтобы просмотреть информацию по конфигурации IP (IP-адрес, маска подсети и шлюз по умолчанию), я напечатаю такую команду: **ipconfig**. Выделение говорит о том, что вы должны ввести данную команду точно так, как она показана.
- *другие команды* - команды, которые, по моему мнению, вам необязательно печатать, указаны как простой моноширинный текст.

я *термины глоссария* - первое появление всех терминов, которые встречаются в глоссарии, вы можете найти в тексте вместе с определениями, выделенными *курсивом*.

замечания - информация, относящаяся к данной теме, или "внутренние" данные выносятся за основной текст для облегчения поиска этой ценной информации.

советы - информация, не являющаяся необходимой частью данной темы, но предлагающая вам советы или помощь для экономии времени.

предостережение - предупреждение о необходимости осторожного выполнения практической операции или задачи.

Часть I
Знакомство с персональными брандмауэрами

1

Зачем вам нужен персональный брандмауэр?

Поскольку вы читаете введение этой главы, велика вероятность того, что вы уже немного знакомы с Интернетом и знаете, почему это потрясающее и в то же время опасное место для посещений. Интернет - это золотая жила информации и возможностей. К сожалению, Интернет стал местом охоты для не очень честных людей, у которых есть как инструменты, так и знания для проникновения в ваш компьютер и кражи вашей личной и финансовой информации, или для людей, которым просто нравится применять на практике различные трюки или сознательно причинять вред компьютерным системам других людей.

Появление широко распространившегося высокоскоростного доступа в Интернет делает ваш компьютер более легкой и привлекательной целью для этих людей. Задача данной книги - познакомить вас с персональными средствами межсетевой защиты и помочь вам защитить ваши данные и вашу личную информацию во время путешествия по сети World Wide Web.

В этой главе вы:

- узнаете о сообществе хакеров и опасности путешествий по Интернету на незащищенном компьютере;
- я изучите опасности высокоскоростного кабельного и цифрового доступа;
- откроете, как легко защитить себя с помощью установки вашего собственного персонального брандмауэра;
- оцените различия между аппаратными и программными брандмауэрами и решите, какой из них лучше для вас;
- выясните, какие свойства брандмауэра необходимо искать при совершении покупки.

Новое поколение высокоскоростного доступа в Интернет

Во время путешествия по сети World Wide Web вы электронно соединяете ваш компьютер с обширной сетью, которую, пока у вас не установлен персональный брандмауэр, вы практически не можете контролировать и от которой вы защищены очень слабо. До недавнего времени, если вы не работали в компании, предоставляющей высокоскоростной доступ в Интернет, путешествие по сети означало дозвон до поставщиков услуг Интернета (провайдеров) с помощью соединения на скорости 56 Кб/с по вашей местной телефонной линии. Это относительно медленные соединения и никогда на самом деле не достигают скорости соединения 56 Кб/с. Вам повезет, если вы соединитесь на скорости приблизительно 44-49 Кб/с*.

Традиционный доступ в Интернет на скорости 56 Кб/с

До недавнего времени опыт работы в Интернете означал использование медленной и иногда неудовлетворительной коммутируемой связи, которая имела тенденцию постоянно разъединяться, таким образом принуждая вас повторно набирать телефонный номер и устанавливать связь снова и снова. Ситуация становится еще хуже, если вы неспособны соединиться с Интернетом, потому что ваш компьютер получает сигнал "занято" каждый раз, когда пытается дозвониться до вашего провайдера.

После того, как вы зарегистрировались у своего провайдера, вашему компьютеру автоматически присваивается временный адрес, называемый IP-адрес. Этот IP-адрес уникален и позволяет опознавать вас в Интернете. Присвоение IP-адреса - это, как правило, динамический процесс, что означает, что вам присваиваются различные IP-адреса каждый раз, когда вы входите в сеть.

Все коммуникации, которые ваш компьютер осуществляет с другими компьютерами в Интернете, основаны на посылке и принятии данных с или на ваш IP-адрес. Поэтому ваш IP-адрес раскрывает ваш компьютер в Интернете и, однажды обнаруженный взломщиком, представляет собой точку доступа к вашему компьютеру. К счастью, временные коммутируемые соединения, связанные с постоянно изменяющимися IP-адресами, способствуют тому, что ваш компьютер является более трудной мишенью для потенциальных захватчиков.

IP-адрес имеет почти то же назначение, что и ваш домашний адрес. Он представляет собой средство идентификации компьютера в Интернете и позволяет другим компьютерам связываться с вашим путем посылки сообщений на присвоенный ему IP-адрес. Чтобы узнать больше об адресах TCP/IP, просмотрите "Использование TCP/IP. Специальное издание" Дж, Рэя, издательство "Que", ISBN: 0-7897-1897-9.

---

* К сожалению, в России качество телефонных линий оставляет желать лучшего, и скорости выше 30 Кб/с редко достижимы. (Здесь и далее, кроме оговоренных случаев - Прим, научного редактора),

Подводя итоги, перечислим характеристики традиционного соединения с Интернетом:

- медленная связь на скорости 56 Кб/с;
- временно устанавливаемое коммутируемое соединение;
- постоянно изменяющийся IP-адрес;
- тенденция прерывания сеанса связи.

Новая эра высокоскоростного доступа в Интернет

Появление высокоскоростного доступа в Интернет является решением проблем, возникающих при использовании коммутируемых соединений со скоростью 56 Кб/с. Высокоскоростные соединения с Интернетом могут быть определены как постоянно активные сетевые соединения и бывают двух видов:

- **Кабельные** – совместно используемое соединение с Интернетом, устанавливаемое с помощью того же коаксиального кабеля, который предоставляет ваше местное кабельное телевизионное соединение.
- **Цифровая абонентская линия** - выделенное подключение к сети Интернет, устанавливаемое с помощью телефонных проводов, предоставленных вашей местной телефонной компанией (оно, тем не менее, не мешает работе ваших телефонных линий).

Обе технологии обеспечивают соединение, скорость которого превышает 56 Кб/с почти в 20 раз. Они постоянно подключены, так что вам никогда не придется терять время на дозвон или опасаться невозможности соединения из-за занятости линии, и вас не разъединят после пребывания в сети в течение длительного периода времени. Наконец, поскольку соединение всегда активно, IP-адрес, присвоенный вашему компьютеру, почти никогда не меняется.

Высокоскоростные соединения - это прекрасно. Но, как и все остальное, высокоскоростные соединения имеют отрицательные стороны. Забавно, что многие свойства, которые делают высокоскоростные соединения привлекательными, также являются причиной их уязвимости. Во многих случаях соединение с Интернетом с помощью высокоскоростного соединения подобно оставлению вашей входной двери открытой и незапертой. Это происходит потому, что у высокоскоростных соединений с Интернетом имеются следующие характеристики:

- **Постоянный IP-адрес** – позволяет взломщику, обнаружившему ваш компьютер в Интернете, с легкостью находить его снова и снова.
- **Высокоскоростной доступ** - означает, что взломщик может работать намного быстрее, пытаясь проникнуть в ваш компьютер.
- **Всегда подключенное соединение** – означает, что ваш компьютер уязвим все время, пока он соединен с сетью.

Поскольку высокоскоростное соединение с Интернетом - это просто разновидность сетевого соединения, оно активно все время, пока включен компьютер,

и остается активным до тех пор, пока его не отключат. Из-за способа, которым поставщики высокоскоростного доступа в Интернет конфигурируют свои серверы DHCP, ваш IP-адрес изменяется очень редко. В действительности, если вы входите в сеть, по крайней мере, один раз в течение нескольких недель или около того, присвоенный вашему компьютеру IP-адрес может никогда не меняться, потому что ваш компьютер будет постоянно возобновлять присвоенный ему IP-адрес. Однако, если вы не используете ваше соединение с Интернетом в течение длительного периода времени, вы можете обнаружить, что ваш IP-адрес был изменен.

Провайдеры создают общий пул IP-адресов, которые они динамически присваивают или отдают во временное пользование компьютерам-абонентам. Продолжительность пользования варьируется в зависимости от того, как работает провайдер. Когда вы впервые войдете в сеть, вашему компьютеру присвоят IP-адрес из этого фонда. До тех пор, пока ваш компьютер входит в сеть часто, он будет продолжать возобновлять предоставленный ему IP-адрес. Однако, если вы не выходили в Интернет в течение длительного периода времени, срок пользования IP-адресом может истечь, ваш провайдер потребует его обратно и вновь разместит его в фонде доступных IP-адресов. Этот процесс абсолютно незаметен для конечного пользователя.

Термин DHCP (Dynamic Host Configuration Protocol) обозначает протокол динамической конфигурации компьютера. Поставщики услуг Интернета используют серверы DHCP для управления процессом присвоения IP-адресов.

Поскольку IP-адрес является для вас разновидностью домашнего адреса при работе в Интернете и может никогда не меняться, он делает вас легкой добычей для тех людей, обитающих в Интернете, которые любят проникать в компьютеры (их называют кракерами и/или хакерами). Как-никак, после того, как они определят ваш компьютер как возможную цель, им будет легко возвращаться к нему снова и снова и пытаться взломать, поскольку его IP-адрес остается постоянным.

Высокая скорость соединения также является обоюдоострым мечом, и, хотя она обеспечивает вас удивительно высокой скоростью работы в Интернете, эта же самая скорость может быть использована против вас, позволяя вашим потенциальным противникам, пытающимся получить доступ к вашему компьютеру, работать с той же высокой скоростью.

Наконец, постоянно подключенные соединения делают ваш компьютер или сеть значительно более привлекательной целью, поскольку это означает, что если однажды ваш компьютер будет взломан, его будет несложно обнаружить и получить к нему доступ в любое время, когда он включен.

Если вы принадлежите к большинству современных людей, вы используете одну из множества операционных систем Microsoft. К сожалению, как вы узнаете в главе 9 "Насколько защищен ваш компьютер?", хотя операционные системы Microsoft могут быть наглядными и простыми в использовании, они не всегда безопасны*. Этот факт в сочетании с опасностью высокоскоростного доступа может сделать Интернет очень опасным местом для посещения.

Защитите себя с помощью персонального брандмауэра

Итак, теперь вы имеете представление о том, каким образом постоянное соединение с Интернетом делает вас более уязвимым, чем обычное соединение на скорости 56 Кб/с. Теперь вам необходимо узнать, как вы можете защитить себя от угроз, исходящих от этого типа соединения.

Я надеюсь, что не заставил вас поверить, что подключение к Интернету на скорости 56 Кб/с полностью защищено от хакерских атак, поскольку это не так. Просто хакерам немного сложнее взломать его благодаря ограниченному времени работы онлайн и постоянному изменению IP-адресов.

Как показано в этой книге, существуют простые меры предосторожности, которые вы можете предпринять, чтобы сделать ваш компьютер или сеть намного более безопасными. Если у вас установлена операционная система Microsoft, вы, возможно, захотите изменить конфигурацию некоторых параметров настройки сети, которые оставляют ненужные дыры в вашей защите. Вы узнаете, как внести эти изменения в конфигурацию, в главе 4 "Защита сетей в Windows". Вы также должны регулярно посещать Web-сайт Microsoft и использовать все доступные поправки и изменения, касающиеся безопасности. Кроме того, вы должны убедиться, что у вас установлена антивирусная программа, и что она соответствует современным требованиям. Если у вас нет антивирусной программы вы должны приобрести ее при покупке персонального брандмауэра.

Компьютерный вирус - это программа, созданная для проникновения в компьютерную систему или сеть. Многие вирусы относительно безвредны и просто показывают смешные сообщения. Другие вирусы созданы для удаления файлов или даже для форматирования жестких дисков.

Пару лет назад никто еще даже не слышал о термине "персональный брандмауэр". Брандмауэры были дорогим оборудованием или программным обеспечением, которое требовалось только большим компаниям для защиты их много-

---

* Уменьшить опасность можно, используя ПК-версии ОС UNIX, однако они более сложны для освоения.

миллионных банков данных. Однако все меняется. Персональные брандмауэры стали необходимой вещью для любого человека, у которого есть высокоскоростной доступ в Интернет. Их цель - не допустить того, чтобы хакеры могли проникнуть в ваш компьютер или даже просто увидеть его, когда вы путешествуете по Интернету. Хороший брандмауэр не только предотвращает настоящие и будущие атаки, но также предупреждает вас о присутствии и деятельности программы "Троянский конь", которая могла проникнуть на ваш компьютер до того, как вы установили персональный брандмауэр.

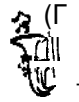
"Троянский конь" - это программа, которая, будучи однажды установленной, соединяется с компьютером хакера и выполняет то, что ей указали делать, включая нападение на другие компьютеры. Так случилось в феврале 2000 года, когда две атаки "распределенный отказ от обслуживания" остановили работу Web-сайтов Yahoo и Ebay. Вы узнаете больше о программах "Троянский конь" далее в этой главе.

Атака "распределенный отказ от обслуживания" происходит, когда хакер внедряет программу "Троянский конь" в тысячи компьютеров и затем приказывает этим компьютерам постоянно подключаться к сети компании или Web-сайту. Тем самым сайт переполняется сетевым трафиком. Цель атаки "распределенный отказ от обслуживания" - переполнение указанной компьютерной системы **бо́льшим** потоком информации, чем она может обработать, что не дает ей возможности работать с запросами реальных клиентов.

Существует ряд компаний, создающих средства межсетевой защиты. Некоторые из этих брандмауэров реализованы аппаратно, другие выполнены как программное обеспечение. В этой книге описываются четыре наиболее популярных брандмауэра:

- Кабельно-цифровой маршрутизатор Linksys EtherFast - *www.linksys.com*;
- Персональный брандмауэр McAfee - *www.mcafee.com*;
- BlackICE Defender - *www.networkice.com*;
- Персональный брандмауэр ZoneAlarm - *www.zonelabs.com.*

В дополнение к этим персональным брандмауэрам вы можете найти информацию о ряде других персональных средств межсетевой защиты в приложении *А,*



Создатели брандмауэров иногда также продают антивирусные программы. Ищите комбинированные программные пакеты, которые включают как антивирусную программу, так и программу-брандмауэр. В большинстве случаев вы сэкономите деньги при покупке подобного пакета.

Типовое соединение с Интернетом

Сегодня высокоскоростное подключение к Интернету происходит с помощью кабельного модема или цифровой абонентской линии. Кабельный модем - это способ подключения, при котором ваш поставщик услуг кабельного телевидения также предоставляет вам доступ в Интернет с помощью кабельного модема. Ваша телефонная компания, со своей стороны, предоставляет подключение с помощью цифровой абонентской линии. Модемы с высокоскоростным доступом, как правило, оснащены также для работы с более медленным соединением и не требуют конфигурирования с вашей стороны, за исключением подсоединения модема к кабелю или цифровой абонентской линии, а затем подключения его к вашему компьютеру.

На рисунке 1.1 изображено типовое высокоскоростное соединение. Компьютер соединяется с кабельным/цифровым модемом при помощи подключения к плате Ethernet или шине USB. Затем компьютер подключается к поставщику услуг Интернета.

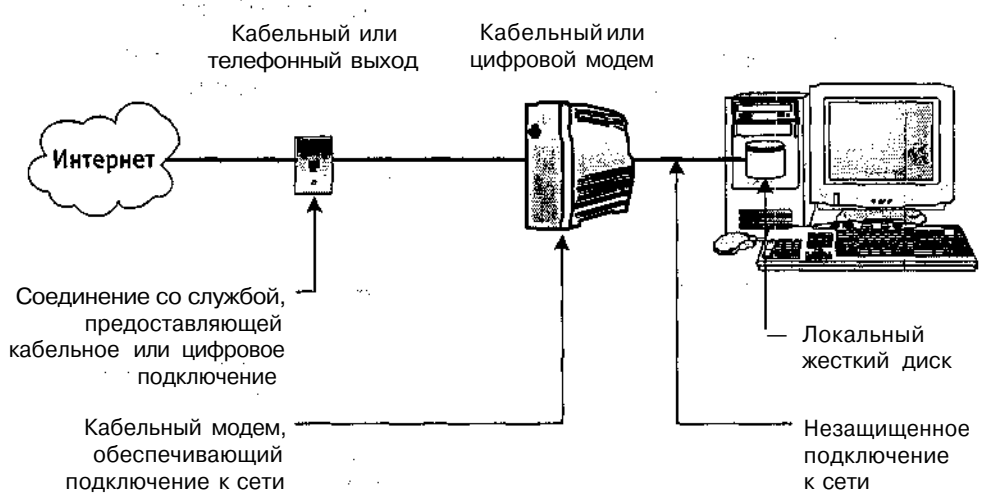


Рисунок 1.1. Кабельные и цифровые высокоскоростные соединения с Интернетом обеспечивают великолепную скорость подключения, однако оставляют вашу систему уязвимой перед атакой практически любого человека через Интернет

Данное соединение похоже на любое другое сетевое соединение, с помощью которого ваш компьютер может посылать или получать сообщения от других компьютеров сети. Только вместо безопасной корпоративной сети с доверенными сотрудниками, преданным персоналом отделов безопасности и профессионалами, работающими с сетями, - лишь вы и целый Интернет. Вот почему персональные брандмауэры столь важны.

На рисунке 1.2 показано значение программного брандмауэра. В этом случае на вашем компьютере установлена такая программа, как персональный брандмауэр McAfee. После того, как вам будет задано несколько простых вопросов,

она сама сконфигурирует себя и приступит к работе, действуя как фильтр для всего входящего и исходящего сетевого трафика вашего компьютера и убеждаясь, что Ничто не прошло через нее до тех пор, пока вы не определили, что это можно пропустить.

Программные брандмауэры позволяют вам определять, какой трафик разрешить, а какой заблокировать, с помощью служб безопасности, которые были созданы, когда вы впервые установили брандмауэр. В общем, мастер задаст вам серию простых вопросов, на которые вы ответите. Затем мастер создаст службы безопасности в соответствии с предоставленной вами информацией.

Причина того, что фильтры брандмауэра ограничивают IP-трафик - это защита от "Троянского коня". Если "Троянский конь" проникнет на ваш компьютер или уже был там до установки брандмауэра, он будет пойман в первый же раз, когда он попытается соединиться с Интернетом.

Персональные брандмауэры комплектуются в двух формах:

- **автономный** - программный брандмауэр, устанавливаемый на компьютер;
- **аппаратный** - внешнее аппаратное оборудование, которое находится между кабелем и вашим компьютером и обеспечивает сетевую защиту.

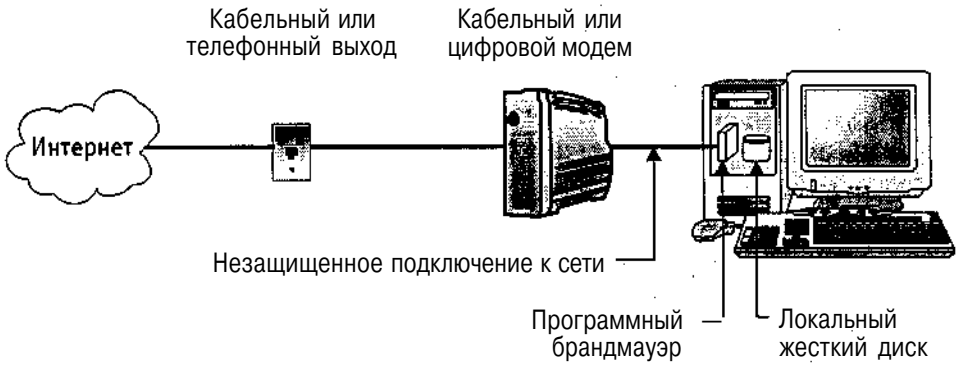


Рисунок 1.2. Программный брандмауэр действует как барьер, запрещающий прохождение любого несанкционированного потока информации в сеть или из сети

В отличие от программных брандмауэров, аппаратный брандмауэр не требует конфигурирования. Кроме того, аппаратный брандмауэр имеет дополнительные функциональные возможности для работы в сети, не предоставляемые программными брандмауэрами, включая:

- **Концентратор (hub)** - сетевое устройство, использующееся для объединения различных компьютеров в одну локальную сеть.
- **Коммутация (switching)** - способ создания динамического выделенного сеанса связи между двумя компьютерами в сети.

- **Маршрутизация (routing)** - правило, указывающее устройству направлять данные, предназначенные для Интернета, в Интернет, в то же время оставляя данные локальной сети локальными.

Дополнительные функциональные возможности для работы в сети, предоставляемые аппаратным брандмауэром, имеют значение только в том случае, если у вас есть или вы планируете создать локальную сеть. В противном случае это ненужные свойства, которые, в дополнение к стоимости оборудования, помогают объяснить, почему стоимость аппаратных брандмауэров выше, чем программных. Дополнительная информация о работе с локальными сетями представлена в главе 11 "Домашние сети и общее подключение к Интернету",

Способ, которым брандмауэр фильтрует IP-пакеты, зависит от типа вашего брандмауэра. Ниже перечислены несколько типов брандмауэров:

- Шлюз **приложений (Application gateway)** - также известен как прокси-сервер. Он фильтрует, опираясь на IP-адреса и операцию, которую приложение пытается выполнить.
- **Уровня соединений (Circuit-level)** - проверяет пакеты предварительно одобренных услуг Интернета и IP-адресов. После установки соединения с сайтом он позволяет трафику проходить без дополнительной проверки.
- **Проверки состояния (Stateful Inspection) -** исследует содержание пакетов и пропускает или блокирует их, основываясь на сопоставлении их характеристик с характеристиками одобренных типов пакетов.
- **Пакетный фильтр (Packet filter)** - фильтрует пакеты, основываясь на предварительно одобренных IP-адресах. Этот вариант включает большой объем конфигурирования и постоянную поддержку в рабочем состоянии.

Персональные брандмауэры предназначены только для личного, домашнего пользования и лишены сложности и маневренности, требуемой для управления процессами передачи данных в больших масштабах. Чтобы узнать больше о брандмауэрах индустриального уровня, используемых корпорациями, смотри *"Практическое руководство по работе с брандмауэрами",* Терри Оглетри, издательство "Que"; ISBN: 0-7897-2416-2.

Аппаратные брандмауэры представляют собой альтернативное решение, в соответствии с которым брандмауэр выносится из корпуса компьютера, который он защищает, во внешнее устройство, как изображено на рисунке 1.3. Этот вариант, в сущности, переносит поединок из внутренней части компьютера наружу. Это также освобождает ценные ресурсы вашего компьютера для целей, не связанных с работой вашего персонального брандмауэра. Аппаратные персо-

нальные брандмауэры обычно бывают немного менее маневренными, чем программные. Основной недостаток аппаратного брандмауэра - это его стоимость, которая в 3-5 раз выше стоимости стандартного программного брандмауэра.

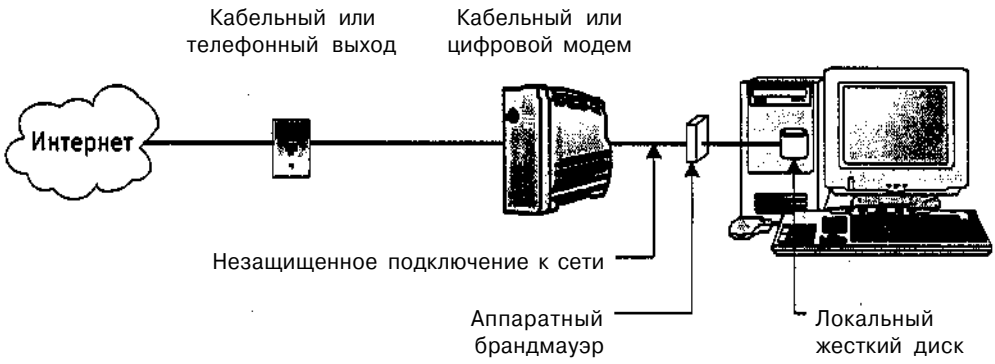


Рисунок **1.3.** Аппаратный брандмауэр выполняет ту же работу, что и его программный аналог, не требуя затрат ресурсов компьютера или сети, которые он зашишает

Кто такие хакеры?

До настоящего момента в этой главе рассказывалось, почему каждый раз, когда вы выходите в Интернет, вы рискуете, раскрывая свой компьютер перед опасностями сети. Вы также узнали, что опасность возрастает, когда вы улучшаете соединение с 56 Кб/с до высокоскоростного. Персональный брандмауэр представляет собой барьер между вашим компьютером и потенциальными захватчиками в Интернете. Но вам, должно быть, интересно, почему кто-то в этом мире хочет прилагать усилия, пытаясь взломать ваш компьютер или домашнюю сеть. Чтобы это понять, вы должны взглянуть на особую группу людей в Интернете, иногда называемую хакерами, и понять, кто они такие, или что они представляют из себя по их собственному мнению, и что они могут найти интересного в вашем компьютере и его содержимом.

Для большинства людей термин "хакер" означает человека, который проникает в компьютеры или сети с намерением причинить вред. Это общее и излишне упрощенное определение.

В действительности, существует множество различных уровней "хакеров", каждый из которых имеет различный набор навыков и различные устремления. Цель данного раздела - познакомить вас с сообществом хакеров и помочь вам лучше понять, почему они делают то, что делают.

Сообщество хакеров

Хакеры - это больше, чем просто изолированные личности, блуждающие по Интернету в поисках возможностей причинения вреда. В действительности, вы можете быть удивлены, узнав, что в Интернете процветает активное сообщество хакеров. История этого сообщества зародилась в 1960-х годах, и она может про-

следить свои корни до первых хакеров, которые взламывали телефонные компании, чтобы воспользоваться услугой удаленного телефонного звонка. Эти люди со временем назвали себя телефонными фрикерами (phone freaks). Как вы увидите, красочные имена процветают в хакерском сообществе.

Возможно, лучший способ побольше узнать о сообществе хакеров и разобраться в нем - это изучить различные виды его членов. Их классификация включает:

- хакеров (hacker);
- кракеров (cracker);
- вокеров (whacker);
- самураев (samurai);
- личинок (larva);
- полубогов (demigod).

Вы можете узнать больше об этой уникальной группе людей, посетив сетевую конференцию alt. 2600. Однако не привлекайте к себе внимания и постарайтесь не разозлить никого, пока будете там (на всякий случай).

Хакер

Хакер - это человек, в совершенстве владеющий техническими навыками в компьютерной области и преуспевающий в нахождении и решении технических задач. У этого человека обычно установлена очень мощная ОС UNIX, и он хорошо подготовлен для работы в сетях. Его знания сетей включают многолетний опыт работы в Интернете и способность взламывать и проникать в чужие сети. Хакер умеет программировать, используя различные языки программирования. В действительности, этот человек может изучить новый язык в считанные дни. Звание "хакер" - не то, о котором вы можете сожалеть. Наоборот, ваши друзья в сети должны пожаловать его вам. Эти люди (хакеры) вызывают восхищение своих сетевых знакомых. Для того чтобы завоевать подобное уважение, человек должен делиться своими знаниями. Совместное пользование знаниями является основным принципом сообщества хакеров.

UNIX - одна из старейших и наиболее мощных операционных систем в мире. Она также является одной из наиболее отлаженных. Операционная система UNIX снабжена большинством из компьютерных компонентов, которые используются в Интернете на сегодняшний день, и всестороннее понимание внутренней работы ОС UNIX является необходимым условием для настоящего хакера.

Один из основных принципов этого сообщества состоит в том, что никто не должен дважды решать одну и ту же проблему. Время слишком ценно, чтобы

тратить его на повторное изобретение колеса. Поэтому хакеры делятся своим опытом и открытиями, и в результате их статус в сообществе хакеров растет, так же как и статус самого сообщества.

Хакеры верят, что информация должна быть общедоступна и что их обязанность состоит в том, чтобы сделать ее таковой. Хакеры не причиняют вреда. Их задача, по их мнению, состоит в том, чтобы искать форму личного образования, постоянно изучать, исследовать и делиться. Конечно, это ужасно самоуверенный взгляд на вещи, но так хакеры смотрят друг на друга. Они считают свое поведение благородным и достойным уважения.

Однако, в итоге, хакеры используют свои компьютерные навыки для взлома компьютеров и сетей. Даже несмотря на то, что они могут не причинять вреда, это все равно неэтичные и незаконные действия. Проникновение в чей-либо компьютер практически то же самое, что и проникновение в его дом. Независимо от того, делает ли это их более просвещенными или нет, это недостаточное оправдание для преступлений, которые они совершают*.

Кракер

Другая группа в сообществе хакеров - это группа, из-за которой хакеры получили свое плохое имя. Люди в этой группе известны как **кракеры.** Кракеры - это люди, которые проникают в компьютеры и сети с намерением причинить вред. Кракеры стараются привлечь как можно больше внимания средств массовой информации и всегда называются хакерами в телевизионных новостях и прессе. Это, конечно, причиняет хакерам много неудобств. Хакеры не уважают кракеров и очень хотят, чтобы их различали. По мнению хакеров, кракеры являются низшей формой жизни, не заслуживающей внимания. Конечно, кракеры всегда называют себя хакерами.

Обычно навыки кракера даже близко не равны умениям настоящего хакера, хотя они и владеют квалификацией определенного уровня. Обычно они используют атаки грубой силой и некоторое количество трюков вместо изобретательности и мастерства, которыми обладают хакеры.

Вокер

Вокер - еще один термин, который вы могли **слышать.** Вокер - это, по существу, человек, который разделяет философию хакера, но не его умения. **Вокеры** менее опытны в своих методах и способности проникать в системы. В отличие от хакера, вокер - это человек, который никогда не достигал цели в виде идеального взлома. Хотя **вокеры** не так искушены технически, они, тем не менее, владеют обширными навыками и, хотя чаще всего не делают новых открытий, они способны идти по следам хакеров и часто могут воспроизводить их трюки, пытаясь научиться от них.

---

* Необходимо подчеркнуть, что хакеры (в изначальном понимании этого термина) действительно борются на бесплатность и общедоступность **информации,** однако делают это только законными методами.

Самурай

Самурай - это хакер, который решил предоставить свои превосходно отточенные умения для того, чтобы выполнять законную работу для корпораций и других организаций. Самураям часто платят компании, в чьи сети они пытаются проникнуть. Самурай подражает древнему японскому самураю и живет по жесткому кодексу чести, который запрещает ему злоупотребление своими умениями в незаконных целях.

Личинка

Личинки - это начинающие хакеры. Они новички в сообществе хакеров, у них мало мастерства и недостает многолетнего опыта, требуемого, чтобы стать настоящим хакером, Они боготворят настоящих хакеров и надеются со временем получить статус истинного хакера.

Итак, что же хакеры, кракеры, вокеры, самураи или личинки хотят от вас или вашего компьютера? Ведь в мире существует множество корпоративных и правительственных компьютеров и сетей, которые могут стать гораздо более привлекательной целью. Что ж, хотя хакеры, вокеры и самураи, возможно, не заинтересованы во взломе домашних компьютеров, эти самые компьютеры в качестве легкой добычи часто попадают в поле зрения кракеров, которых интересует легкий доступ к финансовой информации. Они таюке являются плодотворной почвой для тренировок личинок, для их игр и экспериментирования.

Но наибольшая угроза исходит от группы людей, не связанных с сообществом хакеров. Эта группа состоит из тинэйджеров и рассерженных взрослых с большим количеством свободного времени. Эти люди обычно имеют небольшие, если вообще имеют, навыки взлома. И если бы не принцип обмена информацией сообщества хакеров, эти люди никогда бы не причинили никому вреда. Однако, имея даже очень небольшие знания, эти люди все равно могут скачивать и выполнять сценарии и программы, созданные настоящими хакерами. В плохих руках эти программы ищут и обнаруживают уязвимые компьютеры и сети и наносят все виды разрушений.

Другие термины хакеров

Помимо более общих названий, представленных выше, здесь даны несколько других хакерских терминов, которые вы должны знать. Например, ванаби (wannabee) - это человек, который находится на начальной стадии личинки в своей карьере хакера. Ванаби похожи на очень активных учеников и могут быть опасны из-за своей неопытности, даже если у них хорошие намерения. *Черный хакер* (dark-side hacker) – человек, который по той или иной причине потерял веру в философию хакеров и теперь использует свои знания во зло. *Полубог* - это хакер с десятилетиями опыта и всемирной репутацией.

Запомните, что в Интернете нет ничего личного, что кто-нибудь всегда следит за **вами,** и это не всегда плохие парни, из-за которых вы должны **волноваться.** В начале 2000 года ФБР установило устройство под **названием "Carnivore"*** у каждого основного поставщика услуг Интернета, что позволило им вылавливать и просматривать каждый IP-пакет, **который** идет по проводу. Затем оно получило менее устрашающее название "**CDS1000**". ФБР установило аппаратное и программное наблюдение, говорят, что так они могут собирать информацию по приказу суда относительно специально указанных **людей****. Это ужасно, но это правда. Просто будьте осторожны с тем, что посылаете по электронной почте, потому что вы никогда не **знаете, кто** ее прочтет.

Где они берут свои игрушки?

Инструменты хакерского ремесла бесплатны и легко доступны для любого человека с выходом в Интернет. Поскольку хакеры верят, что информация должна быть общей и что их обязанность сделать ее таковой, за долгие годы они создали невероятную коллекцию хакерских инструментов. Многие из этих инструментов соперничают и даже превосходят качеством программирования коммерческие приложения. Эти инструменты были созданы **высококвалифицированными** людьми. Их исходный код общедоступен и в отличие от программ, созданных корпорациями-гигантами, их код подвергается внимательному исследованию программистов-экспертов по всему миру.

Цель данной книги - предоставить вам всю **информацию,** в которой вы нуждаетесь для выбора вашего персонального брандмауэра и обеспечения его функционирования, а не восхвалять роль хакеров и помогать продвижению их ремесла. Поэтому вы не найдете хакерских трюков или ссылок на определенные программы взлома в данной книге. Они все абсолютно доступны и легко находятся с помощью любой поисковой системы. В действительности существует даже несколько книг, изданных и легко доступных в книжных магазинах, в которых представлена эта самая информация.

Хотя существуют индивидуальные различия между хакерами, кракерами, вокерами и другими членами сообщества хакеров, суть данной книги **заключается** в том, что вы не хотите, чтобы кто-либо из этих людей получил доступ к вашему компьютеру или домашней сети, независимо от их намерений, мотивов или уровня технических знаний. Кроме того, цель данной книги - помочь вам предотвратить повреждение вашей компьютерной системы, данных или **конфиденциальности.** Некоторые из инструментов хакеров, которые вы должны знать, - это сканеры портов и программы взлома паролей. Сканеры портов исследуют Интернет в поисках компьютеров, находящихся в сети с открытыми портами

---

* Плотоядное **животное.** *Прим. перев.*

** В РФ подобная система называется **СОРМ-2** (Система Оперативно-Розыскных Мероприятий-2).

TCP/IP. Порты TCP/IP - это программные коммуникационные порты, которые установлены в сетевых приложениях. Сетевые приложения сообщаются с другими сетевыми приложениями, посылая и получая данные на соответствующий порт TCP/IP. У хакеров есть много инструментов и трюков, которые они могут использовать, чтобы попытаться получить доступ к вашему компьютеру через открытые порты. Один из самых основных способов вашей защиты - закрыть все лишние порты. Вы узнаете больше об этих портах и о том, как их закрыть, в главе 9. Вы также увидите, как персональные брандмауэры могут спрятать ваши порты так, что они не будут видны, в главе 3 "Описание брандмауэров".

TCP/IP - это язык Интернета и наиболее крупных сетей. TCP/IP состоит из набора стандартов и протоколов, которые ваш компьютер использует, когда общается в Интернете с помощью основанных на TCP/IP приложений, таких, как Web-браузеры или программы электронной почты.

Операционные системы Microsoft обеспечивают дополнительную безопасность, позволяя вам завести учетную запись пользователя и пароль. Однако в большинство операционных систем Microsoft не встроено абсолютно ничего, что позволило бы им защититься от хакерской атаки на пароли с применением грубой силы. Атака на пароли с применением грубой силы - это нападение на ваш компьютер с помощью программы, которая пытается получить доступ к компьютерным ресурсам путем локализации учетных записей пользователя и угадывания их паролей, используя список часто используемых паролей. Microsoft Windows NT, 2000 и XP могут быть сконфигурированы для блокирования учетных записей при большом количестве попыток, предпринятых против них. Это обеспечивает защиту против атак на пароли с применением грубой силы. Однако у большинства людей на домашнем компьютере эти операционные системы не установлены, и поэтому они практически беззащитны против этого типа атаки. В действительности, без хорошего брандмауэра вы никогда не узнаете, что подвергаетесь нападению.

Хакеры могут запустить атаку на пароли с применением грубой силы после получения доступа к компьютерам с Windows NT 4 и Windows 2000. Другие операционные системы Windows, такие, как Windows 98 и Windows Me, не включают такую модель безопасности, как в Windows NT 4 и 2000, и поэтому не выполняют схему доступа, основанную на паролях. Это, конечно, делает работу хакеров по взлому этих операционных систем намного легче. Кажется очевидным, что вам необходимо быть очень осторожным при создании паролей и убедиться, что они уникальны. Уникальный пароль имеет, по крайней мере, восемь знаков, содержит комбинацию чисел, строчных и заглавных букв, и, по крайней мере, один специальный знак (такой, как !@#$%^&()*).

Что они хотят от вас?

Итак, вопрос остается: что может кто-либо найти в вашем компьютере или домашней сети, что будет ценно для него или нее? Ответ может вас удивить. Например, им может понадобиться:

- Украсть ваши Microsoft Money и файлы Quicken, где вы храните личную финансовую информацию.
- Наложить руки на номера ваших личных сберегательных и текущих счетов.
- Найти ваши персональные pin-номера.
- Украсть электронные копии ваших налоговых деклараций, которые вы подготовили с помощью приложений по созданию налоговых отчетов.
- Украсть номера ваших кредитных карт или любую иную финансовую информацию, которая представляет ценность.*
- Украсть важную рабочую информацию, находящуюся на вашем компьютере, которая может быть ценной для конкурента.
- Запустить атаки "распределенный отказ от обслуживания" против других компьютеров в Интернете и Web-сайтов.

Все эти виды информации могут быть легко захвачены и посланы хакеру с использованием *программы-червя,* как изображено на рисунке 1.4. Червь может быть первоначально внедрен в ваш компьютер, спрятавшись внутри приложения электронной почты, которое после двойного нажатия незаметно установит червя на ваш жесткий диск. Затем червь начинает работать, исследуя ваш жесткий диск в поисках ценной информации, которую он может передать обратно своему создателю.

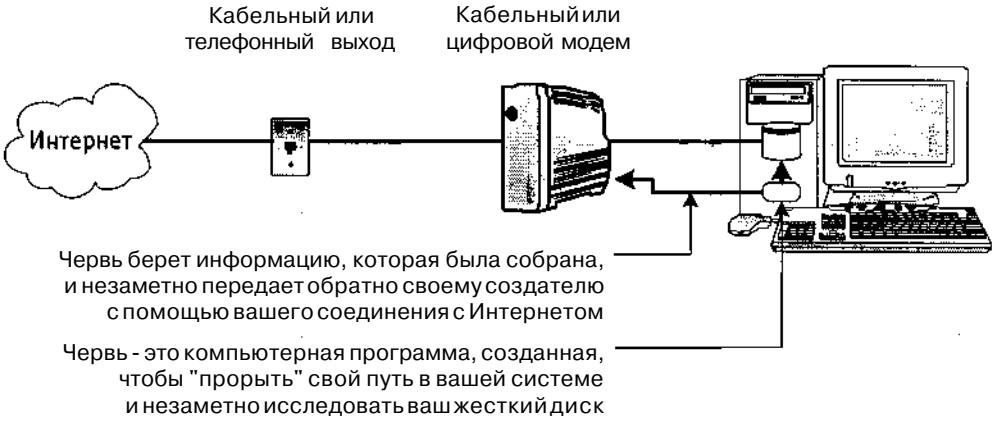


Рисунок 1.4. Программы-черви позволяют хакерам работать негласно, используя ресурсы вашего компьютера для сбора и кражи вашей личной информации

* В России самое популярное - украсть информацию об учетной записи (логин и пароль доступа) Интернет.

Деньги и личные секреты не являются единственными ценностями, которые ваш компьютер может предоставить хакерам. Некоторые люди просто наслаждаются, причиняя неприятности или практикуясь с помощью различных трюков. Вам будет не смешно, когда вы обнаружите, что кто-то проник на ваш компьютер и удалил важные файлы или переполнил ваш жесткий диск бесполезным мусором, но для некоторых кракеров это является способом проведения досуга.

Кракер также может контролировать ваш компьютер без вашего ведома и использовать его и тысячи других компьютеров для запуска атак на коммерческие Web-сайты и другие корпоративные системы связи. Кракеры достигают этого, проникая в личные компьютерные системы и внедряя "Троянских коней", которые после установки связываются с компьютером кракера и выполняют любые инструкции, которые были им выданы. Чтобы не допустить подобного бесшумного враждебного захвата, вам необходимо установить персональный брандмауэр и сконфигурировать его на блокировку всего не одобренного исходящего трафика вашего компьютера. Как вы увидите в главе 3, вы можете сконфигурировать ваш брандмауэр с помощью списка одобренных Интернет-приложений, таких, как Internet Explorer и Outlook Express. Ваш персональный брандмауэр после этого откажет в доступе в Интернет любому приложению, которого нет в этом списке, включая программы "Троянский конь".

Термин *"Троянский конь"* произошел от названия уловки, которую греческие захватчики использовали для проникновения сквозь ряды защитников города Троя. Он означает программу, которая незаметно проникает на ваш компьютер, спрятавшись в части нужной на вид программы. Затем "Конь" начинает неистовствовать. Программа Back Orifice сделала атаку такого типа знаменитой. Back Orifice - это программа класса "Троянский конь", название которой подражает названию серии сетевых приложений Microsoft Back Office. Однажды внедренная, программа Back Orifice предоставляет хакеру полный контроль над зараженным компьютером.

2

Высокоскоростные соединения с Интернетом означают повышенную уязвимость

Эта глава предоставит вам информацию, которая необходима для принятия решения о том, какой тип высокоскоростного доступа покупать. Вы также узнаете о том, что вам необходимо при покупке, установке и выходе в режим онлайн вашего кабельного или цифрового модема. Вы узнаете, как отладить ваше соединение и улучшить его производительность, а также как проверить и подтвердить его скорость.

В ней объясняется, как:

- сравнить сильные и слабые стороны кабельного и цифрового доступа в Интернет;
- установить требуемое программное и аппаратное обеспечение;
- установить ваш модем и настроить ваш высокоскоростной доступ в Интернет;
- проверить скорость вашего соединения.

Выбор высокоскоростного соединения: кабельное или цифровое

Когда дело касается выбора высокоскоростного соединения с Интернетом, у вас обычно немного вариантов. Как кабельное, так и цифровое соединение активно используется на большей части Северной Америки. Однако это не означает, что обе эти технологии доступны повсюду. В действительности во многих местах доступен только один из этих вариантов. Тем не менее, если вы проживаете на территории, где доступны оба варианта, вы должны быть достаточно осведомлены о сильных и слабых сторонах этих двух технологий, чтобы суметь принять решение о выборе одной из них на основе полученной информации.

Кабельное соединение, например, не имеет дистанционных ограничений, в то время как, чтобы установить цифровое соединение, вы обычно должны проживать в районе трех миль от главного офиса одной из телефонных компаний. В отличие от кабельного, чем дальше ваше цифровое соединение от центрального офиса, тем слабее оно будет. Конечно, единственный способ, с помощью которого вы можете выяснить, имеете ли вы ограничения в приеме цифровой связи, это связаться с местным провайдером, предоставляющим услуги цифровой связи.

Хотя как кабельное, так и цифровое соединение обеспечивает высокоскоростной доступ в Интернет, кабельное представляет собой соединение, используемое совместно с вашими соседями, тогда как цифровое использует выделенные линии связи между вашим домом и телефонной компанией. Это означает, что скорость вашего кабельного соединения может значительно снижаться в зависимости от того, сколько ваших соседей вышли в Интернет. Следующие два раздела посвящены детальному рассмотрению сильных и слабых сторон кабельного и цифрового соединения.

Высокоскоростной кабельный доступ в Интернет

Высокоскоростной кабельный доступ в Интернет предоставляется по тому же телевизионному кабелю, который, возможно, уже есть в вашем доме. Поэтому, за исключением случая, когда вы хотите установить ваш компьютер в комнате, в которой еще нет кабельного выхода, вам не нужно прокладывать новый кабель.

Кабельный доступ способен обеспечить скорость соединения до 1 Мб, но скорость от 300 до 500 Кб/с более реальна. Хотя загрузка может осуществляться на этих скоростях, передача данных на удаленный компьютер, как правило, более медленная. Это происходит потому, что кабельный доступ обычно несимметричный. Это означает, что получать данные вы можете намного быстрее, чем посылать. В действительности один из провайдеров, предоставляющих услуги кабельной связи, компания **"@Home",** ограничивает максимальную скорость посылки данных 128 Кб/с. Тем не менее, это намного лучше, чем ваше старое коммутируемое соединение, которое было способно на скорость, не превышающую 33,6 Кб/с. К счастью, за исключением Интернет-игр, большинство требований пользователей к доступу несимметрично по природе. Например, щелчок мышью на Web-сайте выводит очень небольшое количество данных, тогда как загрузка картинок и мультимедийного содержимого требует значительно большей пропускной способности или полосы пропускания для обработки всех дополнительных данных.

Проблема общего доступа

Кабельный доступ представляет собой общее подключение. Ваш поставщик услуг кабельного соединения, в сущности, устанавливает локальную сеть в вашем районе, к которой подключены вы и ваши соседи. Поскольку вы должны пользоваться сетью совместно, не вся полоса пропускания доступна вам все время. В действительности, если многие из ваших соседей выйдут в Интернет, вы можете ожидать небольшого снижения скорости. В самые напряженные часы дня скорость вашего соединения может превышать скорость вашего старого коммутируемого соединения не более чем в два-три раза. Тем не менее, это намного лучше, чем обычный модем со скоростью соединения 56 Кб/с.

Доступ с помощью кабельного модема - это незащищенное соединение, поскольку любой пользователь вашей локальной сети имеет возможность просмотреть входящие и исходящие данные, которые проходят через ваше соедине-

ние с Интернетом. Это означает, что один из ваших соседей теоретически имеет возможность наблюдать за всей вашей деятельностью в Интернете, в том числе узнавая, какого рода Web-сайты вы посещали. К сожалению, это одна из проблем, с которой вы ничего не можете сделать. Это просто характерная черта этого типа соединения. Однако вашим соседям потребуются некоторые довольно специализированные знания и большой опыт, чтобы сделать это. Также нужно отметить, что большинство современных систем кабельной связи используют зашифрованный обмен данными. Это означает, что данные, посланные и принятые вашим компьютером, автоматически кодируются таким образом, чтобы только ваш компьютер и компьютер, с которым вы общаетесь, могли расшифровать или декодировать их. Итак, хотя Web-сайты, которые вы посещаете, когда работаете в Интернете, потенциально видимы, фактические данные, которые вы посылаете или принимаете, надежно закодированы.

Компании "RoadRunner" и "@HOME"

Когда дело коснется выбора поставщика услуг кабельного доступа в Интернет, вы поймете, что у вас действительно нет выбора. Независимо от того, предлагает ли эту услугу ваш поставщик кабельного телевидения или нет. Кабельные компании обслуживают свои ограниченные территории, так что у вас нет возможности выбора того или иного поставщика.

Два крупнейших поставщика услуг кабельного доступа в Северной Америке - это компании "@HOME" и "Road Runner". Вместе они осуществляют 80% всех кабельных установок. Два других, более мелких, поставщика, компании "Softnet Systems" и "High Speed Access Corp", обслуживают большую часть остальных территорий. Эти поставщики сотрудничают с местными кабельными компаниями, предоставляя кабельный доступ в Интернет и продавая свои услуги под объединенным именем. Например, в моем районе кабельный доступ в Интернет предоставляет компания "MediaOne Road Runner".*

В обязанности местной кабельной компании входит помощь в установке вашего кабельного соединения и обеспечение его правильной работы. Затем поставщики услуг Интернета предоставляют основные услуги, входящие в область их деятельности. На сегодняшний день одиночное кабельное соединение обычно стоит в пределах 30-50 долларов в месяц и включает следующие услуги:

- неограниченный доступ;
- арендную плату за кабельный модем;
- техническую поддержку;
- бесплатное программное обеспечение, включая браузеры и диагностические утилиты.

---

* О российских компаниях рассказывается в приложении В "Домашние сети в России".

Высокоскоростной DSL доступ в Интернет

Термин DSL означает цифровая абонентская линия. Цифровой доступ предоставляет высокоскоростное соединение с Интернетом по существующим телефонным проводам, проложенным в вашем доме. Цифровая абонентская линия способна обеспечивать скорость соединения от 144 Кб/с до 1,5 Мб/с. Радиус действия цифровой абонентской линии ограничивается примерно тремя милями* от главного офиса телефонной компании**. Чем дальше ваш дом от главного офиса, тем медленнее будет ваше соединение.

Главный офис телефонной компании является узловым пунктом для телефонных соединений и передачи данных. Тысячи таких офисов расположены по всей Северной Америке. Если вам повезло, ваш дом расположен в пределах трех миль от одного из главных офисов***.

Расположение поставщиков услуг цифровой связи

Существует несколько способов определения, можете ли вы получить услугу цифровой телефонной связи в своем доме. Вы можете позвонить в свою местную телефонную компанию и спросить их, предоставляют ли они эту услугу, а затем попытаться найти поставщика услуг Интернета, который договорится с вашей компанией предоставлять эту услугу. Либо вы можете пойти прямо к местному поставщику Интернет-услуг, который рекламирует услуги цифровой связи, и попросить его наладить все совместно с телефонной компанией. В конце концов, существует ряд Web-сайтов, на которых перечислены районы, где доступны услуги цифровой связи, включая:

1 *www.thelist.com*;

m *getconnected.com*;

■ *www.dslreports.com*.

Даже если цифровая абонентская линия доступна в вашем районе, перед вами встает еще одно препятствие, которое вы должны преодолеть. Местной телефонной компании, возможно, потребуется посетить ваш дом и осуществить проверку вашей внутренней проводки для того, чтобы убедиться, что она будет поддерживать обмен данными. Дом с плохими или старыми телефонными проводами может не справиться с поддержкой цифрового соединения. В этом случае вам необходимо заменить или добавить новые провода или выяснить, предлагает ли ваш поставщик кабельного телевидения кабельный доступ в Интернет.

В зависимости от вашей местной телефонной компании вы, возможно, можете получить полный комплект, который позволит вам выполнить установку самостоятельно,

---

* Примерно 4,8 км. *Прим. перев.*

** От АТС

*** См. приложение В "Домашние сети в России".

Вилы цифровых абонентских линий

Существует большое количество видов цифровых абонентских линий. Три наиболее распространенных приведены ниже:

- **ADSL (Асинхронная цифровая абонентская линия)** - предназначена для домашних пользователей и малого бизнеса. Предоставляет меньшую пропускную способность для передачи на удаленный компьютер, чем для загрузки на свой. Это означает, что вы сможете получать данные быстрее, чем посылать.
- **SDSL (Синхронная цифровая абонентская линия)** - предназначена для организаций с большими требованиями к доступу в Интернет. Обеспечивает одинаковую пропускную способность для загрузки и передачи данных. Этот вид доступа более дорогой и предназначен для пользователей-организаций.
- **IDSL (Объединенная цифровая абонентская линия) -** предоставляет самый низкий уровень обслуживания. Этот вид доступа предназначен для клиентов, находящихся более чем в трех милях от главного офиса.

Как и кабельные соединения, ADSL - это асимметричное соединение, что означает, что оно поддерживает более быстрый прием данных, чем передачу. Сигналы данных в ASDL вынесены наверх того же соединения, которое несет и голосовые сигналы. Сигналы затем разделяются в главном офисе, где голосовой трафик направляется в общественную абонентскую телефонную сеть, а информационный трафик направляется в Интернет.

Цифровое соединение - это выделенное соединение между вашим домом и главным офисом телефонной компании. Это означает, что ваше соединение является более защищенным, чем кабельное, поскольку ваши соседи его не используют. Это также означает, что ваше соединение будет меньше подвержено перегрузке, поскольку вы не делите свое соединение со своими соседями. Однако, по мере возвращения трафика в главный офис, вам придется разделить Интернет-соединение телефонной компании с остальными пользователями цифровой абонентской линии, обслуживаемыми данным офисом, так что вы все равно можете ощутить снижение скорости в пиковые периоды пользования Интернетом.

Кабельные и цифровые модемы

Для кабельного и цифрового соединения с Интернетом требуются свои собственные специальные типы модемов. Эти модемы дороги, обычно они стоят более 200 долларов. Пользователям цифровой абонентской линии и большому количеству абонентов кабельной связи не приходится выбирать, они вынуждены арендовать свои кабельные модемы в качестве составной части пакета высокоскоростного доступа в Интернет. Обычно это добавляет лишние 10 долларов к месячному счету. Часто провайдеры, предоставляющие эту услугу, имеют системы, созданные для работы с модемами, разработанными определенными производителями. Поэтому вы не можете спокойно заменить один модем на другой.

Стандарт кабельных модемов, известный как DOCSIS, был разработан в 1998 году и постепенно установлен в индустрии кабельной связи. Организация под

названием "CableLabs" несет ответственность за определение соответствия кабельных модемов этому стандарту. Те модемы, которые соответствуют стандарту, маркируются "CableLabs Certified". Если ваша кабельная компания поддерживает аттестованные компанией "CableLabs" модемы, тогда есть шансы, что она также позволит вам купить ваш собственный модем и сэкономить 10 долларов в месяц за аренду модема. Обычно вы можете найти аттестованные компанией "CableLabs" модемы в своем местном компьютерном магазине.

Свойства

Как кабельные, так и цифровые модемы имеют одинаковый набор основных свойств. Их главное различие в том, что кабельные модемы подключаются с помощью коаксиального кабеля, тогда как цифровые модемы используют стандартное телефонное соединение.

На рисунке 2.1 изображен кабельный модем Toshiba PCX1100.

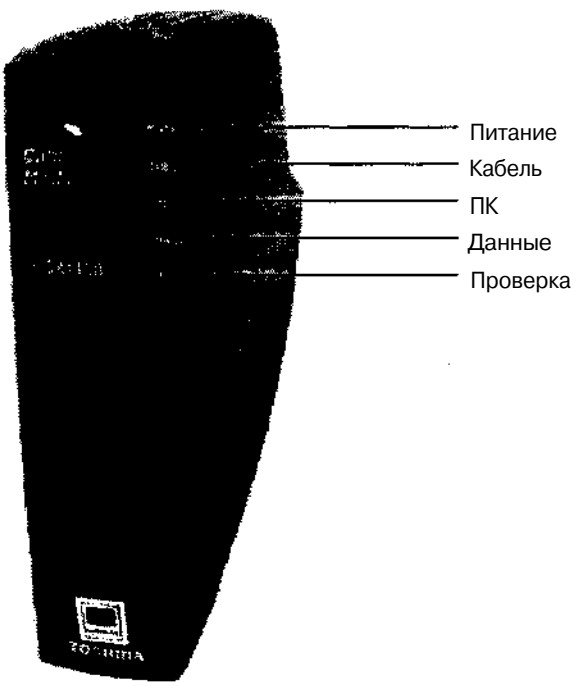


Рисунок 2.1. Кабельный модем Toshiba PCX1100. Вид спереди

Это конкретное устройство является образцом типичного модема для высокоскоростного соединения. Оно снабжено рядом светодиодных индикаторов, которые указывают на состояние модема и его состояние в сети. Эти светодиодные индикаторы включают:

- **Power (Питание)** - светится, когда модем включен в электросеть.
- **Cable (Кабель)** - светится, когда установлено надежное соединение.

- **PC (ПК)** - светится, когда компьютер включен в электросеть и его соединение с сетью активно.
- **Data (Данные)** - мигает при передаче данных.
- **Test (Проверка)** - мигает, когда модем выполняет самотестирование, и горит, если проверка не удалась.

На рисунке 2.2 показан вид сзади кабельного модема Toshiba PCX1100.

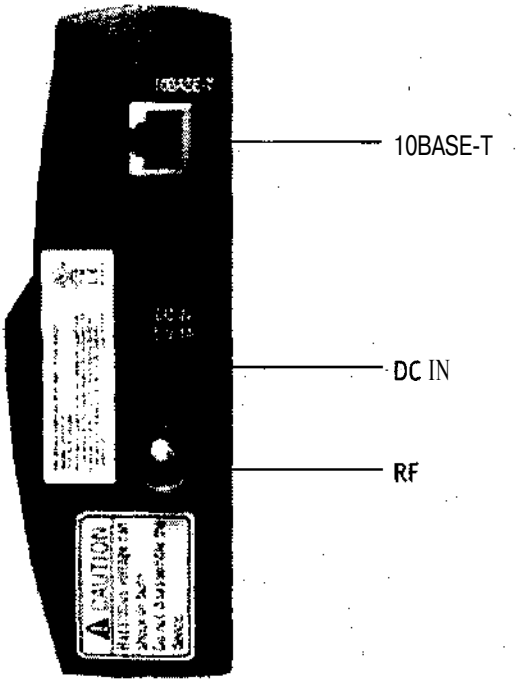


Рисунок 2.2. Кабельный модем Toshiba PCX1100. Вид сзади

Присутствуют следующие порты связи:

- **10BASE-T** - соединяет компьютер и модем с помощью сетевого кабеля, поставляемого вместе с модемом;
- DC IN - подсоединяется адаптер источника питания модема;
- RF - подсоединяется коаксиальный кабель, поставляемый местной компанией, предоставляющей услуги кабельной связи.

ДОУ Во многие современные кабельные и цифровые модемы была добавлена поддержка технологии USB (универсальной последовательной шины). USB предоставляет вариант замены традиционного сетевого соединения простым внешним plug-and-play USB соединением.

Наладка вашего кабельного или цифрового соединения

Для подготовки и запуска вашего кабельного или цифрового соединения необходимо выполнить несколько операций, включая:

- выполнение предустановочных подготовительных работ;
- установка сетевой интерфейсной платы (NIC);
- установка программного драйвера сетевой платы;
- соединение вашего модема с вашим компьютером, высокоскоростным доступом в Интернет и электросетью;
- запуск мастера установки, который поставляется вместе с модемом;
- предоставление вашему поставщику услуг Интернета MAC-адреса вашего модема и MAC-адреса сетевой интерфейсной платы вашего компьютера.

MAC-адреса - это уникальные числа, присвоенные сетевым устройствам, которые определяют эти устройства в сети, MAC-адрес - это 48-битное число, Как ваш кабельный модем, так и ваша сетевая интерфейсная плата имеют MAC-адреса, Ваш провайдер пропускает только разрешенные соединения с Интернетом. Он контролирует эти соединения, запрещая неразрешенным MAC-адресам (таким, как адреса модема и сетевой платы) соединение с сетью. Поэтому, когда вы предоставляете ваши MAC-адреса вашему провайдеру, он использует эту информацию для блокировки сетевого трафика из вашего дома, который не исходит из этих адресов,

Каждый из этих шагов описан далее в этой главе,

Действия, выполняемые перед установкой

Несколько действий вы должны выполнить до того, как вы начнете установку вашего кабельного или цифрового модема. Эти действия необходимы для того, чтобы улучшить работу вашего соединения и сделать ее более надежной во время ваших путешествий по World Wide Web.

Обновление вашей операционной системы

Одна из умнейших вещей, которые вы можете сделать прежде, чем выйти в Интернет, это убедиться, что вы используете самые последние обновления и настройки программного обеспечения своей операционной системы. Microsoft объявляет о выходе этих обновлений на домашних страничках своих операционных систем, которые во время написания этой книги были расположены по адресу: *www.microsoft.com/windows/default.asp*.

Windows 98, Me, 2000 и XP также могут помочь вам в обеспечении операционной системы текущими обновлениями с помощью утилиты Windows Update. При запуске эта утилита автоматически соединяется с сайтом обновления вашей операционной системы. Сайт проанализирует текущее состояние программного обеспечения на вашем компьютере и создаст список рекомендуемых программ для загрузки. С этого момента вы можете автоматически загружать и устанавливать любое обновление.

Обновления, которые вы должны поискать, включают:

- обновления и настройки, относящиеся к сетям Windows;
- обновления и настройки, имеющие отношение к безопасности;
- обновления и настройки, относящиеся к основным функциональным возможностям и устойчивости операционной системы.

Кроме того, вы должны убедиться, что ваше антивирусное программное обеспечение работает правильно и что оно отвечает современным требованиям. Если у вас нет антивирусной программы, вы должны серьезно подумать о ее покупке.

Ускорение вашего доступа в Интернет

Как отмечалось в главе 1 "Зачем вам нужен персональный брандмауэр?", протокол TCP/IP посылает и принимает информацию в пакетах. Протокол TCP/IP удостоверяет, что каждый пакет доставлен, требуя подтверждение от принимающего компьютера. Однако, чтобы максимально повысить свою эффективность, TCP/IP не требует подтверждения каждого отдельного пакета. Вместо этого он позволяет принимающему компьютеру собрать так много пакетов данных, сколько его окно приема протокола TCP/IP может удержать, до посылки одного подтверждения для всех пакетов в текущем окне приема. Окно приема TCP/IP - это контейнер, в котором хранятся пакеты TCP/IP при первом получении.

Увеличивая размер окна приема TCP/IP, вы увеличиваете объем данных, которые ваш компьютер может получить без необходимости посылать подтверждение. Это может привести в результате к большому росту эффективности работы в Интернете. Однако вам нужно быть осторожным, чтобы не сделать окно приема TCP/IP слишком большим, поскольку если пакет потеряется по дороге к вашему компьютеру, подтверждение не будет получено. Фактически, ни один из пакетов данных, в тот момент времени находящихся в окне приема, не будет подтвержден. В конечном счете посылающий компьютер повторно отправит все неподтвержденные пакеты.

Windows 95, Windows 98 и Windows Me автоматически устанавливают свои окна приема TCP/IP на 8 Кб. Операционные системы Windows NT и Windows 2000 устанавливают свои окна приема TCP/IP на 16 Кб. Эти размеры оптимальны для низкоскоростных модемных соединений от 28,8 Кб/с до 56 Кб/с. К сожалению, Microsoft только разрабатывает способ автоматической регулировки окна приема TCP/IP для высокоскоростных соединений.

Подходящие настройки окна приема TCP/IP зависят от величины времени ожидания, представленного в вашем соединении с Интернетом. *Время ожида-*

ния (latency) - это время, требуемое пакету для перехода от вашего компьютера до Интернета, и наоборот. Длительное время ожидания часто возникает из-за перегруженности вашего провайдера или из-за медленного отклика сервера, на котором расположен Web-сайт, который вы хотите посетить.

Вы можете проверить ваше время ожидания с помощью команды Microsoft TRACERT. TRACERT определяет количество пересылок (например, количество компьютеров в Интернете, через которые пришлось пройти вашим данным), с которыми ваш компьютер столкнется на своем пути к удаленному компьютеру, и показывает время, необходимое для каждой пересылки. Вы можете проверить время ожидания, имеющее отношение к вашему поставщику услуг Интернета, напечатав следующую команду:

```
!racert www.yourisp.com
```

В следующем примере показаны частичные результаты такой проверки и указано, что максимальное время ожидания составило 30 мс (миллионных секунды) для одной пересылки. Вы должны протестировать вашего провайдера и любые другие сайты, где вы проводите много времени. Когда определите ваше время ожидания, используйте максимальное значение для каждой пересылки.

```
C:\>tracert www.mediaone.rr.com

Трассировка маршрута к www.mediaone.rr.com [24.30.203.14]
Максимум 30 пересылок:

  1   <10 ms    10 ms    10 ms  va-24-168-254-1.va.mediaone.net [24.168.254.1]
  2    10 ms    10 ms    10 ms  va-24-30-224-53.va.mediaone.net [24.30.224.53]
  3   <10 ms   <10 ms   <10 ms  va-24-30-224-49.va.mediaone.net [24.30.224.49]
  4    10 ms    10 ms    11 ms  va-24-30-224-9.va.mediaone.net [24.30.224.9]
  5    10 ms    10 ms    10 ms  24.93.64.41
  6    10 ms    20 ms    10 ms  24.93.64.129
  7    30 ms    20 ms    30 ms  24.93.64.45
  8    20 ms    30 ms    20 ms  pos0-1.hrndva1-brt1.rr.com [24.128.6.2]
  9    20 ms    20 ms    30 ms  24.218.188.169
```

Низким временем ожидания обычно считается 100 мс или менее. Высокое время ожидания - время свыше 200 мс. Нормальный уровень находится между ними.

Если у вас нормальное время ожидания, вы должны отрегулировать окно приема TCP/IP вашего компьютера до приема 32 Кб. Если у вас высокое время ожидания, вы должны установить окно приема TCP/IP на 64 Кб.

Вы можете изменить размер вашего окна приема TCP/IP, редактируя ваш системный реестр Windows (Windows Registry). Системный реестр - это база данных Windows, в которой хранятся настройки операционной системы, пользователя и приложений. Это делается с помощью запуска программы Regedit, показанной на рисунке 2.3. Regedit - это утилита редактирования системного реестра, поставляемая вместе с операционной системой Microsoft.

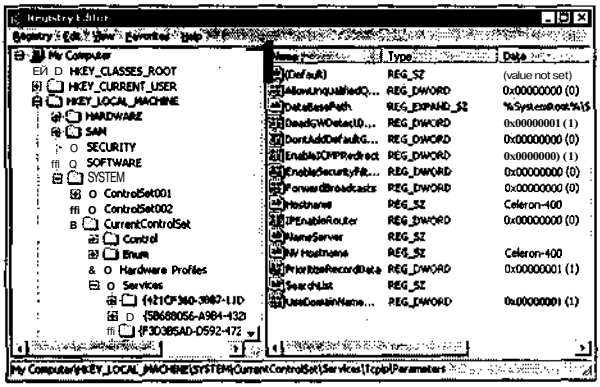


Рисунок 2.3. Программа Regedit позволяет вам просматривать и изменять настройки базы данных системного реестра

Regedit - это инструмент, созданный для применения опытными пользователями и системными администраторами. Работа с ним похожа на работу с Windows Explorer. Работа с системным реестром - это комплексный процесс, выходящий за границы этой книги. Однако вы можете просмотреть *"Руководство по системному реестру Microsoft Windows 2000"* (ISBN: 0-7897-1674-7) и *"Руководство по системному реестру Windows 98"* (ISBN: 0-7897-1947-9) для получения детальной информации о том, как сменить настройки системного реестра.

В следующем списке представлены соответствующие ключи системного реестра для редактирования в зависимости от версии операционной системы и величины времени ожидания.

- для конфигурирования вашего компьютера с Windows 95, 98 или Me с низким временем ожидания установите:

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\XvD\MSTCP\
  DefaultRcvWindow = 32767
  ```

- для конфигурирования вашего компьютера с Windows 95, 98 или Me с высоким временем ожидания установите:

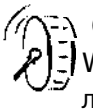
  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\XvD\MSTCP\
  DefaultRcvWindow = 65535
  ```

- для конфигурирования вашего компьютера с Windows NT или 2000 с низким временем ожидания установите:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
  TcpWindowsSize = dword:00007fff
  ```

- для конфигурирования вашего компьютера с Windows NT или 2000 с высоким временем ожидания установите:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
  TcpWindowsSize = dword:0000ffff
  ```



Системный реестр - это база данных, которую операционная система Windows использует для хранения критических настроек системы и приложений. Редактирование вашего системного реестра - серьезное дело, и если вы совершите ошибку, вы можете сделать свой компьютер нефункционирующим. Убедитесь, что вы сделали резервную копию системного реестра, прежде чем вносить в него изменения. Поэтому, если вы не чувствуете себя достаточно уверенно, чтобы вносить эти изменения, я рекомендую попросить кого-либо с опытом работы с системным реестром внести эти изменения за вас.

Установка сетевой интерфейсной платы

Чтобы соединить ваш компьютер с кабельным или цифровым модемом, вам придется установить на компьютер сетевую интерфейсную плату (NIC). В этой главе приводятся основные инструкции для установки вашей сетевой платы. Прежде чем начнете установку, убедитесь, что на вашем компьютере есть по крайней мере одно свободное расширительное гнездо. Расширительные гнезда позволяют вам повысить возможности вашего компьютера с помощью добавления нового аппаратного обеспечения, устанавливающегося на системную плату компьютера. Системная (материнская) плата - это основная плата, связывающая все компоненты вашего компьютера вместе.

Открытие корпуса компьютера и установка нового оборудования может вас испугать. Если вы не чувствуете себя комфортно в этом вопросе, я предлагаю вам позвать кого-либо еще, чтобы он сделал это для вас. Вы можете связаться с магазином, который продал вам вашу сетевую плату, чтобы они установили ее бесплатно. За некоторую сумму ее установит сотрудник сервисного предприятия.

Расширительные гнезда PCI предпочтительнее гнезд ISA. Они представляют собой новейшую технологию и имеют большую пропускную способность, что означает, что они способны обрабатывать больше данных и быстрее. Просмотрите свою компьютерную документацию, чтобы определить, какой тип расширительных гнезд вам доступен, и убедитесь, что купили сетевую карту, которая соответствует типу одного из открытых гнезд.

Производители компьютеров требуют жесткой гарантии того, что установка периферийных устройств, таких, как сетевая карта, не будет выполняться никем, кроме обученных и дипломированных специалистов. Хотя это не останавливает большинство людей от того, чтобы сделать это самим, вы должны учитывать возможные последствия, если что-то пойдет не так. Обычно это означает, что ваша гарантия аннулирована и производитель вашего компьютера может отказать вам в предоставлении технической поддержки.

Следующие шаги обрисовывают в общих чертах процесс физической установки сетевой интерфейсной платы:

1. Открыть и снять корпус компьютера.
2. Снять металлическую заглушку для того, чтобы обеспечить доступ к свободному расширительному гнезду.
3. Прочно вставить и укрепить сетевую плату в расширительном гнезде.
4. Надеть корпус компьютера.
5. Запустить компьютер. Стандарт Windows plug-and-play должен автоматически распознать плату и начать программную часть установки.

Установка программного драйвера

После того как вы выполните физическую установку вашей сетевой платы, вам необходимо установить программное обеспечение, чтобы позволить операционной системе общаться с ней. Это программное обеспечение известно как программный драйвер. Стандарт Windows plug-and-play должен автоматически обнаружить устройство и начать процесс установки программного драйвера сетевой платы, когда вы опять включите ваш компьютер. В случае, если Windows не определит сетевую плату автоматически, вы можете запустить этот процесс вручную с помощью иконки Установка оборудования на Панели управления Windows.

Любое периферийное устройство, добавляемое на ваш компьютер, требует установки дополнительного программного обеспечения, известного как программный драйвер. Поскольку на сегодняшний день существует так много версий операционной системы Windows, трудно описать процесс установки программного драйвера, применяющегося в каждой операционной системе. Следующий процесс описывает в общих чертах выполнение программной части процесса установки.

1. Если стандарт plug-and-play автоматически обнаружит вашу плату, следуйте советам, выдаваемым мастером установки. В ином случае щелкните на Пуск, Настройка, Панель управления, а затем двойным нажатием клавиши мыши вызовите Установку оборудования. Запустится мастер установки нового оборудования.
2. Нажмите Далее и следуйте советам, выданным для начала установки.

3. Windows выведет диалоговое окно, говорящее о том, что выполняется поиск нового оборудования. Затем мастер выведет на экран список нового оборудования, обнаруженного на компьютере. Убедитесь, что ваша сетевая плата находится в списке. Если нет, укажите опцию, позволяющую вам выбрать новое оборудование из списка. Если вы выбрали эту опцию, перед вами появится список производителей оборудования. Выберите производителя сетевой платы из списка, а затем выберите ее модель. Если вы не можете найти информации о производителе или модели, вы можете выбрать опцию Установить с диска, которая предложит вам вставить дискету или CD-диск, прилагающийся к вашей сетевой плате.
4. Вставьте дискеты или CD-диски, которые потребуются в процессе установки.
5. Когда перед вами появится диалоговое окно подтверждения, убедитесь, что все правильно, и нажмите Далее.
6. Windows выполнил установку. Когда потребуется, нажмите Готово. В зависимости от того, какая операционная система Windows у вас установлена, вас, возможно, попросят перезагрузить компьютер для того, чтобы изменения, которые вы внесли, вступили в силу.

Конфигурирование сети

Когда сетевая плата будет установлена, Windows автоматически сконфигурирует себя для работы в сетях, основанных на TCP/IP, таких, как Интернет. Это включает установку ряда программных компонентов. Установка определенных компонентов варьируется в зависимости от версии Windows, установленной на вашем компьютере. Windows 98, Windows Me и Windows 2000 Professional автоматически установят программный драйвер вашей сетевой платы, протокол TCP/IP и Клиент для сетей Microsoft. Назначение каждого из этих компонентов кратко описано ниже.

- Клиент для сетей Microsoft - обеспечивает поддержку соединения с локальными сетями Microsoft и не требуется для поддержки вашего соединения с Интернетом.
- Программный драйвер сетевой платы - обеспечивает операционную систему инструкциями для управления вашей сетевой платой.
- TCP/IP - программная реализация набора правил и стандартов передачи данных, позволяющая вашему компьютеру общаться через Интернет.

Другие программные компоненты устанавливаются в зависимости от версии вашей операционной системы Windows. Вы узнаете больше об особенностях каждого из этих компонентов в главе 4 "Защита сетей в Windows".

Установка вашего высокоскоростного модема

Установка модема - это многошаговый процесс. Во-первых, вы должны физически установить ваш модем. Это включает следующие шаги:

- распаковка модема и подключение его к соединению с Интернетом (например, к кабельным или телефонным проводам);
- подключение модема к электросети;
- запуск мастера установки модема;
- связь с вашим поставщиком услуг Интернета.

Каждый из этих шагов описан в общих чертах далее в этой главе.

Подключение вашего модема

Ваш первый шаг - убедиться, что у вас есть либо телефонный, либо кабельный выход в месте, где вы планируете провести соединение с Интернетом. Если их там нет, вы должны организовать установку одного из них. Следующий шаг - подсоединение вашего модема к вашему компьютеру и его соединению с Интернетом. Этот процесс изображен на рисунках 2.4 и 2.5 и очень прост.

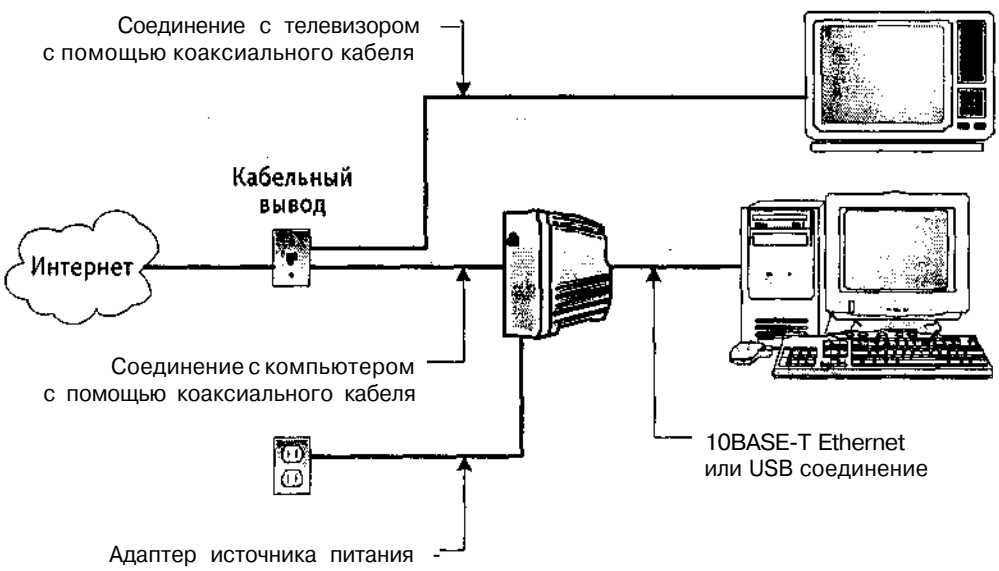


Рисунок 2.4. Изображение процесса подключения вашего кабельного модема

Чтобы приборы работали как можно лучше, постарайтесь избегать размещения вашего модема вблизи от электрических устройств. Каждый электрический прибор производит небольшое количество электромагнитных помех. Модемы - чувствительное оборудование и могут начать работать неправильно, если помещены слишком близко к другим электрическим устройствам.

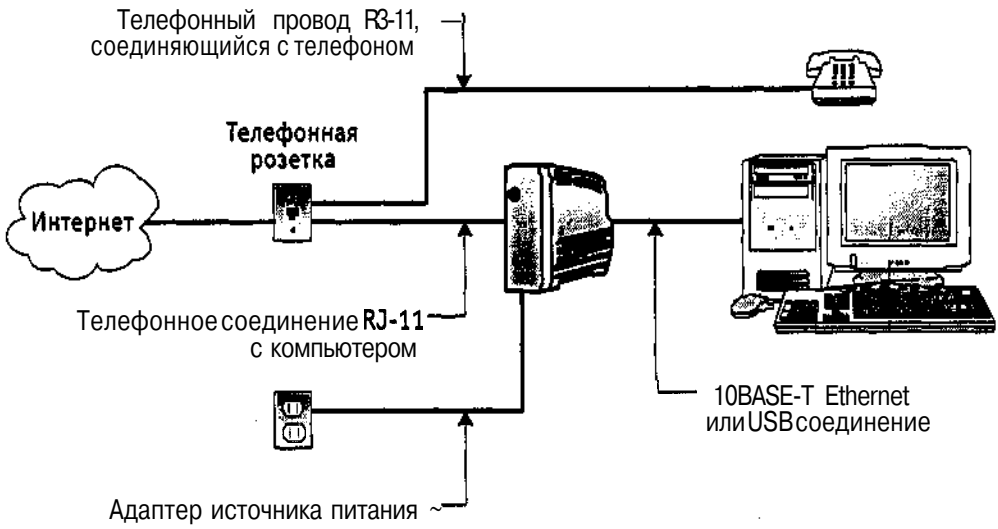


Рисунок 2.5. Изображение процесса подключения вашего цифрового модема

Запуск мастера установки модема

Большинство кабельных и цифровых модемов поставляются вместе с мастером установки, который шаг за шагом проведет вас сквозь процесс установки вашего модема. В противном случае вы должны получить детальные инструкции. Из-за большого количества кабельных и цифровых модемов, доступных в настоящее время, невозможно предоставить вам отдельные инструкции по установке каждого из них. С целью предоставления типичного примера, в этой главе рассматривается процесс установки кабельного модема Toshiba PXC1100. Хотя шаги, задействованные в установке вашего модема, могут различаться, общий процесс должен быть практически одинаковым.

1. Закройте все открытые приложения и вставьте CD-диск, прилагаемый к вашему модему. Мастер установки модема должен запуститься автоматически, как показано на рисунке 2.6.
2. Мастер показывает обзор процесса установки. Начните процесс установки.
3. На экране появится список поставщиков кабельного доступа. Выберите своего поставщика, как показано на рисунке 2.7,
4. Мастер выполнит проверку системы, чтобы подтвердить, что ваш компьютер имеет соответствующее оборудование для поддержки соединения. Сверьте результаты перед тем, как продолжать,
5. Затем вы увидите несколько диалоговых окон, в которых представлены детальные инструкции для физической установки модема. Подтвердите, что вы уже выполнили эти шаги или выполните их теперь.

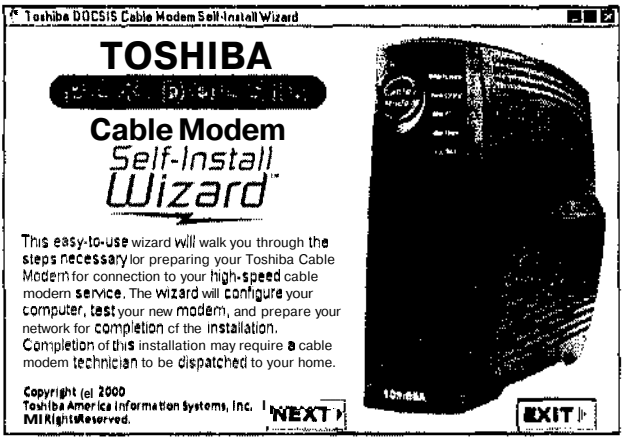


Рисунок 2.6. Большинство модемов с высокоскоростным доступом поставляются вместе с мастером установки, созданным для того, чтобы помочь вам шаг за шагом произвести процесс установки

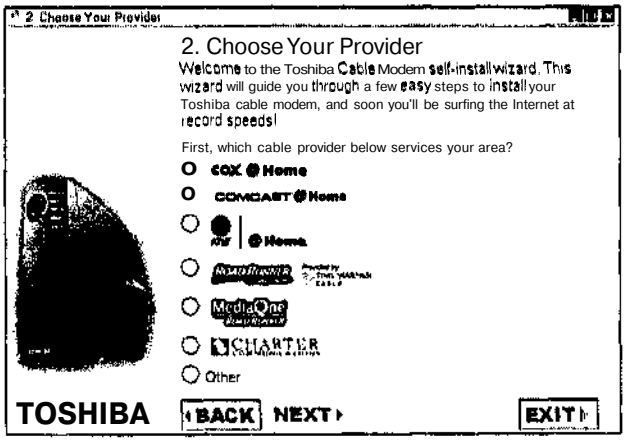


Рисунок 2.7. Мастер предоставляет возможность конфигурирования модемов ряда основных поставщиков, включая поставщиков, не указанных в списке

6. Затем вы увидите несколько диалоговых окон, говорящих о том, что мастер конфигурирует настройки протокола TCP/IP на вашем компьютере и проверяет связь между вашим модемом и компьютером. После завершения конфигурирования вы должны увидеть результаты, сходные с теми, что указаны на рисунке 2.8.
7. Затем мастер укажет внутренний MAC-адрес кабельного модема. Убедитесь, что он идентичен MAC-адресу, написанному на обратной стороне вашего модема.
8. Наконец, мастер завершил изменение конфигурации вашего компьютера. Вас могут попросить перезагрузить ваш компьютер.

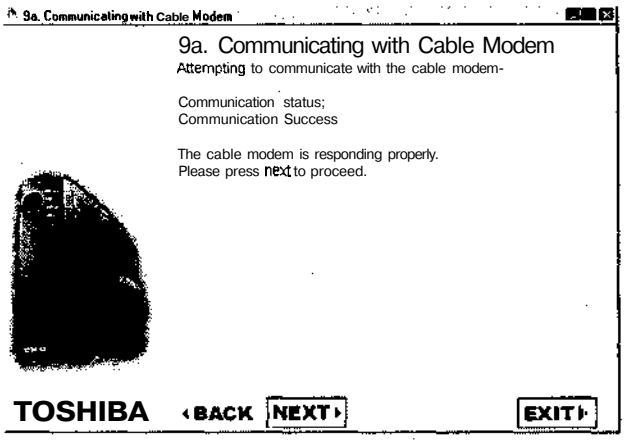


Рисунок 2.8. Мастер закончил установку модема и предоставил подтверждение установки соединения между компьютером и модемом

Связь с вашим провайдером

Последний шаг в активации вашего высокоскоростного доступа в Интернет включает предоставление вашему поставщику услуг Интернета MAC-адреса вашего модема и сетевой платы. Если мастер установки не сообщит вам MAC-адрес вашего модема, вы обычно можете найти его на ярлыке, прикрепленном к модему. Если его нет, адрес должен быть указан в документации, сопутствующей модему.

Если MAC-адрес вашей сетевой интерфейсной платы не указывается мастером установки, вы можете получить его в операционной системе Windows NT или 2000, открыв command prompt (приглашение на ввод команды) и напечатав: IPCONFIG. Найдите выведенную строку, подобную следующей:

```
Physical Address. . . . . : 00-00-00-00-00-00
```

Термин "физический адрес" (physical address) означает MAC-адрес.

Вы найдете MAC-адрес на компьютере с Windows *95,* 98 или Me, щелкнув мышью на Пуск, Выполнить и затем напечатав **WINIPCFG.** Тем самым вы откроете диалоговое окно конфигурации IP, где, среди других данных, будет указан MAC-адрес вашей сетевой интерфейсной платы.

Когда вы свяжитесь с вашим провайдером, у вас спросят ваш MAC-адрес. Ваш поставщик услуг Интернета затем использует ваш MAC-адрес для регистрации вашего личного счета в Интернете. Обычно это мгновенный процесс. После того как вы все это проделаете, вы будете готовы выйти в Интернет.

После того как ваше высокоскоростное соединение начало работать, вы можете захотеть протестировать скорость вашего соединения. Существует ряд Web-сайтов, предлагающих бесплатную проверку скорости соединения. По существу, эти тесты предоставляют вам файл для загрузки и затем измеряют, как долго ваш компьютер загружал его. Чтобы посетить один из этих сайтов, идите на www.toast.com и поищите бесплатно предоставляемые тесты. Однако точность информации, полученной на этом сайте, может варьироваться в зависимости от того, насколько загружен Интернет, а также насколько загружен ваш поставщик услуг Интернета и тестирующий сайт. Запуск проверки поздно ночью или рано утром может дать вам более достоверное представление о вашей скорости связи.

Windows также предоставляет утилиту, которую вы можете использовать для постоянного наблюдения за скоростью вашего соединения. Пользователи Windows 95 или 98 должны найти утилиту под названием монитор сети (Network Monitor Agent), находящуюся на CD-диске с Windows. Пользователи Windows NT и 2000 могут использовать утилиту монитор производительности (Performance Monitor) для отслеживания своих соединений. Выберите Пуск, Программы, Инструменты управления (Administrative Tools) и Объект сетевого интерфейса (Network Interface object).

3

Описание брандмауэров

В этой главе вы узнаете о различиях между аппаратными и программными брандмауэрами и получите сведения, необходимые для определения того, какой тип брандмауэра вам подходит.

Вы также получите краткое описание TCP/IP и узнаете, как брандмауэры пытаются управлять соединениями TCP/IP и защищать их, чтобы оградить ваш компьютер или домашнюю сеть от внешних захватчиков. В этой главе также рассказывается о видах угроз, которым подвергается ваш компьютер при выходе в Интернет и как брандмауэры защищают его от этих опасностей. В конце данной главы брандмауэры разбиваются на несколько категорий для обеспечения полного объяснения их функций и свойств.

В этой главе вы:

- рассмотрите различия между аппаратными и программными брандмауэрами;
- узнаете о протоколе TCP/IP и о том, как он облегчает общение в Интернете;
- и узнаете об опасностях, связанных со сканерами портов, "Троянскими конями" и атаками "отказ от обслуживания";
- откроете, как персональные брандмауэры защищают от внешних и внутренних угроз.

Понятие "персональный брандмауэр"

Персональные брандмауэры - это аппаратные устройства или программы, которые созданы для обнаружения и защиты от внешних и внутренних угроз, угрожающих вашему компьютеру или локальной сети. Как вы узнали в главе 1 "Зачем вам нужен персональный брандмауэр?", каждый компьютер, имеющий выход в Интернет, беззащитен перед возможным нападением, а вероятность нападения возрастает, когда вы переходите с коммутируемого соединения с Интернетом к кабельному или цифровому широкополосному соединению.

Персональные брандмауэры созданы для предоставления вам уровня защиты, который до недавних пор был доступен лишь большим корпорациям.

Свойства персонального брандмауэра

Не все брандмауэры одинаковы. Каждый из них имеет свои сильные и слабые стороны, о которых вы должны узнать прежде, чем покупать один из них. Безотносительно к тому, выбрали ли вы аппаратный или программный брандмауэр, есть определенные свойства, которые вы должны искать и надеяться найти в хорошем персональном брандмауэре. Часто вы можете найти перечисление неко-

торых из этих свойств на обратной стороне коробки, в которой находится программа персонального брандмауэра. Если вы не обнаружили там никаких сведений, просмотрите Web-сайт поставщика для получения более подробной информации, Свойства, которые вы должны искать, включают:

- Мастер настройки и конфигурирования - большинство персональных брандмауэров поставляются вместе с мастером установки, который конфигурирует службы брандмауэра, основываясь на ответах, полученных на несколько простых вопросов.
- Предварительно определенные службы безопасности - это встроенные службы, которые устанавливаются, основываясь на определенных вами критериях.
- Фильтрация всего входящего и исходящего IP-трафика - брандмауэр должен защищать от внешнего нападения, а также от внутренних атак программ "Троянскийконь".
- Автоматическая блокировка общего доступа к файлам из Интернета - брандмауэр должен автоматически отключить общий доступ к файлам и принтерам во всех соединениях с Интернетом,
- Контролируемое использование Интернет-приложений – вы должны точно установить, каким приложениям вы хотите разрешить взаимодействовать с Интернетом, а каким нет,
- Маскировка портов - брандмауэр должен спрятать порты TCP/IP от сканеров портов в Интернете.
- Обнаружение сканеров портов - в случае, если хакеры обнаружат незащищенный порт, брандмауэр должен суметь заметить сканер хакера и доложить о нем.
- Распознавание и защита от атак "отказ от обслуживания" - брандмауэр должен уметь распознавать, когда происходит нападение, и предотвращать его с помощью блокировки доступа нападающего.
- Предупреждение об опасности и регистрация - ваш брандмауэр должен предупреждать вас при обнаружении дыры в безопасности или нападения и создавать подробную запись для вашего просмотра.
- Поддержка домашней сети - некоторые персональные брандмауэры работают с домашними сетями, в то время как другие могут не допускать их функционирования.

Аппаратные брандмауэры

Аппаратные брандмауэры - это внешние устройства, которые представляют собой буферное устройство между вашим компьютером и вашим соединением с Интернетом. Большинство аппаратных брандмауэров созданы для кабельных или цифровых соединений. Аппаратные персональные брандмауэры - это замкнутые устройства, которые взаимодействуют с вашим компьютером с помощью

Web-браузера. Кроме Web-браузера, дополнительного программного обеспечения нетребуется.

Свойства аппаратных брандмауэров, так же как и программных, варьируются в зависимости от поставщика. Набор доступных свойств также варьируется в зависимости от цены вместе с тем, что некоторые поставщики предлагают ряд персональных аппаратных брандмауэров по разным ценам. При минимальных запросах вы можете купить аппаратный брандмауэр, поддерживающий одиночное соединение пользователя ПК, менее чем за 100 долларов. Ненамного дороже стоит аппаратный брандмауэр, который выполняет еще одну функцию как сетевой концентратор/коммутатор, который может поддерживать небольшую локальную сеть в вашем доме. Эта опция также позволяет вам делить одно соединение с Интернетом с другими членами вашей семьи. Чтобы подробнее рассмотреть образцы аппаратных брандмауэров, посетите ваш местный компьютерный магазин. Вы также найдете большое количество информации о них на таких Web-сайтах, как *www.compusa.com* и *www.egghead.com.*

Сетевой концентратор/коммутатор - это внешнее устройство, которое облегчает соединение компьютеров в локальную сеть.

Например, в главе 5 "Аппаратные брандмауэры", демонстрируется использование кабельно-цифрового маршрутизатора Linksys BEFSR41 EtherFast, показанного на рисунке 3.1. Хотя это устройство называется кабельно-цифровым маршрутизатором, оно представляет собой обычный аппаратно реализованный персональный брандмауэр.

Вы можете узнать больше о кабельно-цифровом маршрутизаторе Linksys BEFSR41 EtherFast по адресу: *www.linksys.com.*

Кроме серии персональных брандмауэров Linksys, на рынке существует ряд по-настоящему хороших персональных брандмауэров. Вы можете найти их в большинстве компьютерных магазинов или в Интернете на таких Web-сайтах, как *www.compusa.com* и *www.egghead.com.* Например, вы, возможно, также захотите взглянуть на кабельно-цифровой брандмауэр-маршрутизатор DI-704 Homegateway, созданный компанией "blink". Web-сайт компании "Dlink" находится по адресу: *www.dlink.com.*

Чтобы облегчить чтение, с данного момента для обозначения кабельно-цифрового маршрутизатора Linksys BEFSR41 EtherFast будет использоваться термин "персональный брандмауэр Linksys".

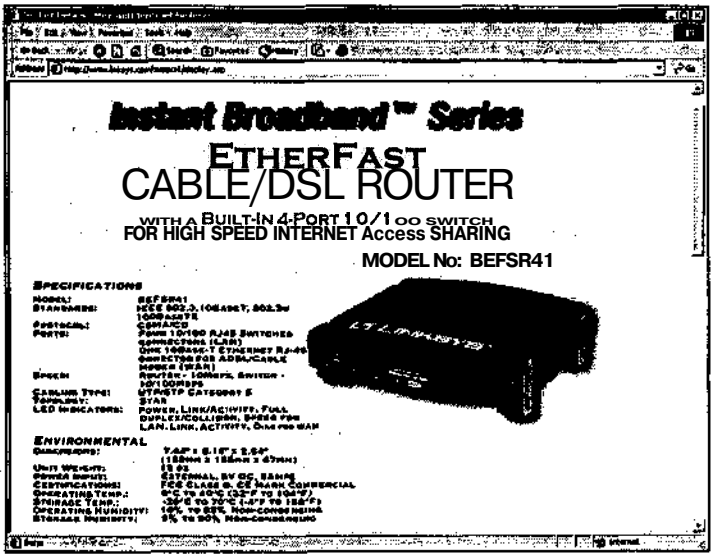


Рисунок 3.1. Кабельно-цифровой маршрутизатор Linksys BEFSR41 EtherFast также является персональным брандмауэром

Аппаратные брандмауэры соединяются с вашим кабельным или цифровым модемом с помощью сетевого соединения Ethernet. Ваш поставщик Интернет-услуг обычно предоставляет оборудование для этого соединения и за дополнительную плату он вам все подсоединит. Прежде всего сетевая плата устанавливается в свободном расширительном гнезде вашего компьютера. Стандарт Windows plug-and-play должен автоматически обнаружить ее и провести вас шаг за шагом сквозь процесс установки сетевой интерфейсной платы. Затем она подсоединяется к аппаратному брандмауэру с помощью кабеля витой пары RJ-45. Затем аппаратный брандмауэр подсоединяется к вашему модему с помощью другого кабеля RJ-45. Эти кабели должны быть предоставлены вместе с вашим модемом и аппаратным брандмауэром. Полная конфигурация показана на рисунке 3.2. Если вы не очень хорошо знакомы с компьютерным оборудованием, вы, возможно, захотите выяснить, не сможет ли ваш поставщик Интернет-услуг установить все это для вас.

Если у вас есть аппаратный брандмауэр, имеющий более одного порта, вы можете соединить с ним остальные компьютеры и создать маленькую домашнюю сеть. Однако ваш провайдер захочет, чтобы вы платили за каждый дополнительный компьютер. К счастью, как вы узнаете в главе 11 "Домашние сети и общее подключение к Интернету", эти устройства имеют встроенные свойства, которые предоставляют способ общего пользования этим соединением без дополнительной оплаты.

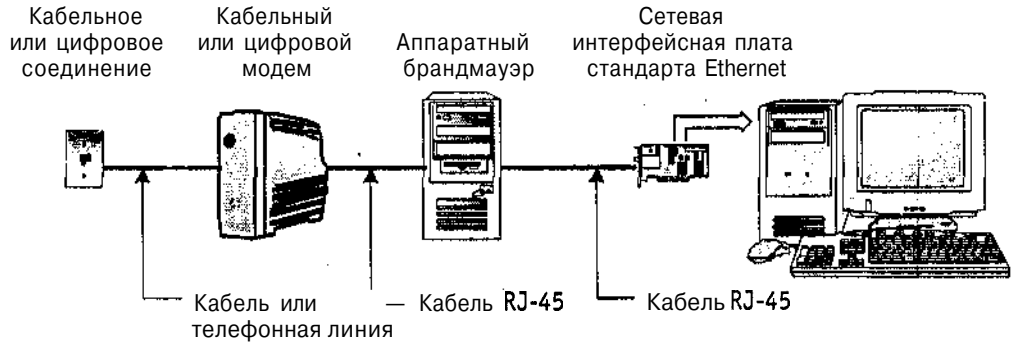


Рисунок 3.2. Типичная установка персонального аппаратного брандмауэра

После установки вы можете поддерживать связь с вашим персональным брандмауэром с помощью IP-адресов, присвоенных им себе самостоятельно, и вашим Web-браузером Netscape или Internet Explorer. Вам, возможно, придется запустить версию 4 или выше этих браузеров. К примеру, персональный брандмауэр Linksys присвоил себе IP-адрес 192.168.1.1. Чтобы начать его конфигурирование, вам достаточно запустить свой браузер и напечатать http://192.168.1.1 в поле URL (строке "Адрес") и нажать Enter. Вас попросят ввести пароль, который вы можете затем изменить, чтобы не допустить возможности того, что кто-нибудь еще будет способен изменить конфигурацию вашего брандмауэра. Все управление с этого момента будет происходить с помощью соединения с браузером. В главе 5 представлен детальный обзор того, как происходит этот процесс.

Получить более подробную информацию о персональном брандмауэре Linksys, включая сведения о *конфигурировании* с помощью его Web-интерфейса, можно в главе 5.

На рынке представлен ряд персональных аппаратных брандмауэров. Большинство из них имеют общий набор характеристик. Эти характеристики включают:

- Кабельно-цифровой маршрутизатор - встроенное программное обеспечение, которое прокладывает маршрут вашего исходящего сетевого трафика (такого, как электронная почта, загрузка файлов и т. д.) в Интернете и получает и передает сетевой трафик Интернета, посланный на ваш компьютер. Трафик Интернета, не адресованный специально вашему компьютеру, автоматически игнорируется.
- Сервер DHCP - протокол динамической конфигурации сетевого узла или DHCP - это программное свойство, используемое людьми с небольшими сетями. Он позволяет аппаратному брандмауэру работать также в качестве сервера DHCP. Серверы DHCP динамически присваивают IP-адреса компьютерам, объединенным в домашнюю сеть, спасая вас от беспокойства о том, как

сделать это вручную. Более подробная информация об этом программном свойстве представлена в главе 1.

- Клиент DHCP - позволяет вашему брандмауэру принимать динамические IP-адреса, предоставленные вашим провайдером для того, чтобы компьютер(ы), который(е) он обслуживает, могли установить соединение.
- Интернет-брандмауэр - программа, которая защищает ваш компьютер или небольшую сеть от нападения злоумышленников при подключении к Интернету.
- Многопортовый концентратор - дополнительные порты для оборудования, встроенные в аппаратный брандмауэр, которые позволяют вам подключать более чем один компьютер и совместно пользоваться соединением с Интернетом. Таким образом вы можете создать маленькую домашнюю сеть.
- Коммутация(switching) - способность устанавливать временное выделенное соединение между двумя локальными компьютерами домашней сети, которое помогает играть в сетевые игры быстрее, поскольку управление их сетевым трафиком происходит более эффективно.
- Интернет-конфигурирование - возможность безопасного конфигурирования вашего брандмауэра через соединение с Интернетом.
- Конфигурирование с помощью браузера - способность конфигурировать ваш брандмауэр с использованием вашего Web-браузера.

Программные брандмауэры

Программные брандмауэры - это программы, установленные на вашем компьютере, которые находятся на жестком диске и загружаются в память, когда компьютер начинает работать. В отличие от аппаратных брандмауэров, программные брандмауэры созданы для работы с вашей текущей аппаратной конфигурацией и так же эффективны для коммутируемых соединений, как для кабельных и цифровых соединений. После установки каждый программный брандмауэр конфигурируется с помощью своего собственного специализированного интерфейса.

В отличие от аппаратных брандмауэров, программные брандмауэры созданы для защиты отдельного устройства и не предоставляют возможности создания локальных сетей. Однако, если у вас нет локальной сети, вы можете найти, что программные брандмауэры предлагают простоту, которая делает их более легкими в работе и управлении, чем их аппаратный аналог.

Программные брандмауэры дешевле, чем аппаратные. Некоторые отличные программные брандмауэры даже бесплатны для индивидуальных пользователей. Например, персональный брандмауэр ZoneAlarm бесплатен, хотя существует также профессиональная версия программы, предоставляющая дополнительные свойства, которая не бесплатна. Вы получите возможность узнать больше о персональном брандмауэре ZoneAlarm в главе 8 "ZoneAlarm".

НОВЫЙ БРАНДМАУЭР ИНТЕРНЕТ-СОЕДИНЕНИЯ MICROSOFT.

Ко времени написания этой книги прошло всего лишь несколько месяцев с тех пор, как корпорация "Microsoft" выпустила домашнюю версию ее новейшей компьютерной операционной системы, названной Windows XP Home Edition. Среди ее многочисленных новых свойств есть встроенный брандмауэр, который корпорация "Microsoft" назвала Брандмауэр Интернет-соединения.

Мастер домашних сетей Microsoft автоматически установит и сконфигурирует как соединение компьютера с Интернетом, так и его персональный брандмауэр. Компания "Microsoft" утверждает, что этот новый брандмауэр будет блокировать незатребованные соединения с Интернетом, отклоняя все соединения, которые появились не на домашнем компьютере. Кроме того, если у вас есть небольшая домашняя сеть, вы можете использовать персональный брандмауэр для ее защиты. Приятно видеть, что компания "Microsoft" признает, что ее операционным системам недостает защищенности при работе в Интернете, однако предложенный брандмауэр поможет только тем, кто установит Windows XP Home Edition, что оказывается довольно дорогостоящим мероприятием. Подобно всем операционным системам Microsoft до этой, свойства Windows XP - это расширившийся набор аппаратных требований, с которыми многие владельцы домашних компьютеров не способны справиться без покупки новых компьютеров. Например, вам нужно минимум 128 Мб памяти, чтобы пользоваться Windows XP.

Программные брандмауэры созданы для работы с определенными операционными системами. Однако большинство основных персональных программных брандмауэров работает с Windows 95, 98, Me, NT 4, 2000 и XP. Программные брандмауэры предоставляют простые в эксплуатации мастера настройки, которые проведут вас шаг за шагом сквозь процессы установки и конфигурирования. Каждый программный брандмауэр предоставляет свой собственный набор заранее определенных служб безопасности, которые позволяют вам устанавливать различные уровни безопасности. Например, брандмауэр "BlackICE Defender" предоставляет четыре предварительно настроенные службы безопасности:

- доверительная (Trusting) - пропускает весь входящий трафик, существенно перегружающий брандмауэр;
- предусмотрительная (Cautious) - блокирует весь незатребованный Интернет-трафик, который пытается получить доступ к ресурсам сети или операционной системы;
- боязливая (Nervous) - блокирует весь незатребованный Интернет-трафик, за исключением определенных типов интерактивного трафика, такого, как загружающиеся мультимедиа;
- параноидальная (Paranoid) - блокирует весь незатребованный Интернет-трафик.

Вы должны ожидать от программного брандмауэра примерно такого же уровня защиты, как и от аппаратного. Основное различие между двумя видами брандмауэров - это то, что аппаратные брандмауэры защищают ваш компьютер, пытаясь блокировать любое нападение, атакующее из любого места, тогда как программный брандмауэр в силу того, что он установлен на самом компьютере, может защищать компьютер от атак, которые уже достигли компьютера. Программные брандмауэры потребляют компьютерные ресурсы, включая пространство на диске и память, и поэтому (даже когда они успешно выполняют свои функции) все же немного влияют на производительность компьютера.

Стандартные требования программных брандмауэров

Аппаратные требования различных программных брандмауэров могут значительно различаться. Аппаратные брандмауэры, с другой стороны, не требуют установки программного обеспечения на компьютере, который защищают. Их единственное требование - это Ethernet-соединение, которое вы создали, установив сетевую интерфейсную плату и соединив ее с вашим кабельным или цифровым модемом, как было описано в главе 2 "Высокоскоростное соединение с Интернетом означает повышенную уязвимость".

В таблице 3.1 перечисляются аппаратные требования программных продуктов, которые будут описаны в данной книге.

Таблица 3.1. Аппаратные требования персональных программных брандмауэров

Брандмауэр	Операционная система	Центральный процессор	Память	Жесткий диск
Кабельно-цифровой маршрутизатор Linksys EtherFast	Нет	Нет	Нет	Нет
Персональный брандмауэр McAfee	W95 и выше	486	32 Мб	4 Мб
BlackICE Defender	W95 и выше	Pentium	16 Мб	10 Мб
Персональный брандмауэр ZoneAlarm	W95 и выше	–	–	–

Обзор организации сетей

Как было указано в главе 2, кабельное или цифровое Интернет-соединение - это соединение с гигантской и запутанной сетью. Чтобы общаться по этой сети, ваш компьютер должен использовать соответствующий сетевой протокол. *Сетевой протокол* - это набор правил, стандартов и процедур для связи и обмена данными по сети. Существует только один набор протоколов, использующийся в Интернете, известный под названием TCP/IP.

Вы можете представить свое высокоскоростное соединение с Интернетом как многоуровневый набор протоколов и приложений, как показано на рисунке 3.3, где каждый уровень протоколов зависит от служб, расположенных на уровень ниже.

Соединение вашего домашнего персонального компьютера с вашим местным поставщиком кабельного или цифрового доступа в Интернет - это Ethernet-соединение. Ethernet также является протоколом. Однако это низкоуровневый протокол и используется для транспортировки высокоуровневого протокола TCP/IP. Это позволяет вашему поставщику Интернет-услуг установить соединение между своим компьютером и вашим. TCP/IP выполняет ряд работ, но на самом элементарном уровне, он облегчает взаимодействие между приложениями, запущенными на двух компьютерах, такими, как Internet Explorer или Outlook Express.

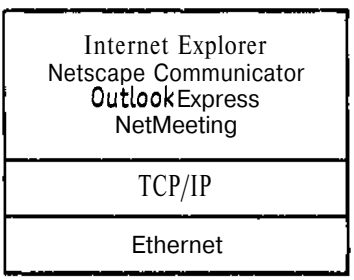


Рисунок 3.3. Изображение типичного широкополосного Интернет-соединения

Описание процесса пересылки данных между сетевыми компьютерами

Взаимодействие через Интернет в конечном счете осуществляется между двумя компьютерами, исходным и удаленным, или, более точно, между сетевой платой на одном компьютере и сетевой платой на другом. Во время сеанса связи, который происходит между двумя компьютерами, они часто меняются ролями. Когда данные посылаются с одного компьютера на другой, они должны пройти по Интернету. Поскольку Интернет - это обширная коллекция компьютеров, данные на самом деле проходят сквозь ряд других компьютеров на пути к указанному удаленному компьютеру. TCP/IP - это протокол, который делает все это возможным.

Для того чтобы компьютеры, находящиеся в Интернете, знали, куда отправить эти данные, они должны быть соответствующим образом адресованы. Важно понимать, что когда вы посылаете что-либо, например, электронное письмо, кому-либо в Интернете, письмо не посылается как единый документ. В действительности TCP/IP разбивает его на более управляемые части, называемые *пакетами*. Отдельные пакеты затем посылаются по Интернету на указанный удаленный компьютер, как изображено на рисунке 3.4,

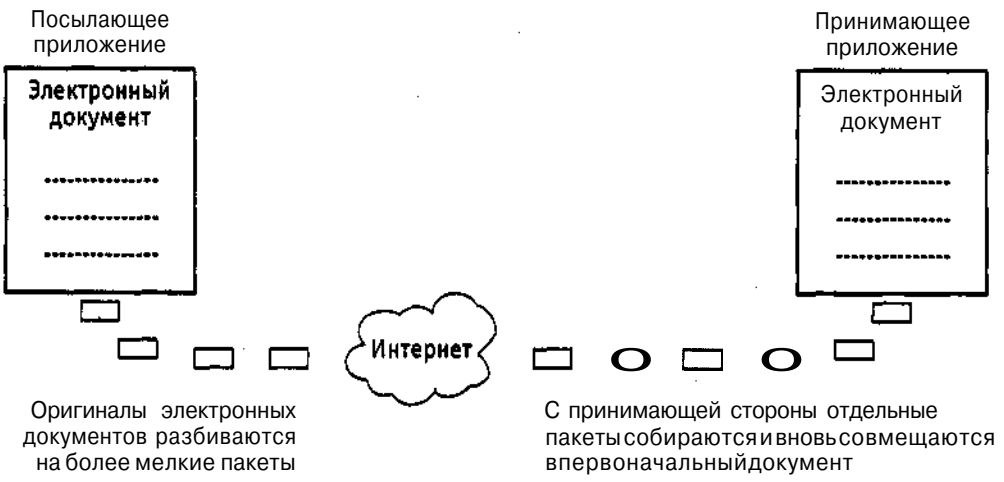


Рисунок 3.4. Изображение того, как файлы разбиваются на множество пакетов и перемешаются по Интернету

Не каждый пакет пойдет одним и тем же путем. На самом деле пакеты, составляющие ваше электронное письмо, могут проходить по многим различным маршрутам по дороге к указанному удаленному компьютеру, где они в конце концов будут получены и вновь собраны протоколом TCP/IP. В итоге, они поступят в электронную почту получателя для просмотра.

Как общаются компьютеры

Каждому компьютеру, соединяющемуся с Интернетом, присваивается уникальный IP-адрес. Этот адрес определяет положение исходного компьютера в Интернете, так же как и адрес удаленного компьютера. Определение адресов места отправления и назначения каждого пакета необходимо для осуществления доставки каждого пакета.

Когда прибывает пакет данных, удаленный компьютер внимательно изучает его. Если пакет адресован этому компьютеру, он принимается и обрабатывается, в противном случае он игнорируется.

Присвоение IP-адресов незаметно для большинства пользователей, поскольку большинство провайдеров использует протокол, известный как DHCP, или *протокол динамического конфигурирования хоста*. DHCP автоматически присваивает IP-адрес вашему компьютеру каждый раз, когда вы включаете в сеть ваш компьютер с кабельным или цифровым соединением с Интернетом. Если вы используете коммутируемое соединение, ваш IP-адрес присваивается каждый раз, когда вы устанавливаете коммутируемое соединение.

Как ваш провайдер использует MAC-адреса

Подобным образом MAC-адрес также не причинит вам беспокойства, если вы не планируете разделить ваше соединение с Интернетом с другими компьютерами небольшой домашней сети. Поставщики кабельного или цифрового соеди-

нения с Интернетом отслеживают число компьютеров, использующих Интернет-соединение, просматривая MAC-адреса пакетов данных, проходящих по соединению. Вот почему вы должны связаться с провайдером и предоставить ему MAC-адреса вашего кабельного модема и сетевой платы, когда вы впервые активизируете ваше кабельное или цифровое соединение. По умолчанию поставщик, предоставляющий услуги кабельного или цифрового соединения с Интернетом, блокирует компьютеры с незарегистрированными MAC-адресами от общего доступа к соединению с Интернетом. Поскольку как ваш кабельный модем, так и компьютер имеют MAC-адрес, вы должны зарегистрировать их до того, как сможете пользоваться своим соединением с Интернетом.

Поставщики услуг кабельного или цифрового соединения с Интернетом требуют дополнительную плату за каждый добавочный компьютер, который пользуется соединением. Эта оплата обычно составляет дополнительные 5-7 долларов в месяц. Вам придется связаться с вашим провайдером, чтобы организовать подключение дополнительных соединений, и предоставить ему MAC-адреса сетевых плат на остальных компьютерах. Как было показано в главе 2, вы можете использовать команду IPCONFIG/A11, чтобы собрать MAC-адреса.

Существует другой способ, с помощью которого вы можете совместно со многими компьютерами пользоваться одним Интернет-соединением без дополнительной оплаты вашему провайдеру. По существу, вы направляете Интернет-трафик через один компьютер, который взаимодействует с Интернетом от лица остальных компьютеров домашней сети с помощью Microsoft Internet Connection Sharing. Эта программа поставляется как компонент Windows 98 Second Edition, Me, 2000 и XP.

Другой вариант - использовать персональный аппаратный брандмауэр, такой, как Linksys BEFSR41, который предоставляет подобную услугу. Вы узнаете больше о настройке общего доступа к соединению с Интернетом в главе 11.

Еще о TCP/IP

TCP/IP - это на самом деле набор многих протоколов, которые работают вместе для обеспечения взаимодействия в больших и малых сетях. TCP и IP - это два протокола в общем наборе TCP/IP. TCP/IP является устанавливаемым по умолчанию протоколом для Windows 98, Me, 2000 и XP и автоматически устанавливается, когда стандарт plug-and-play обнаружит на компьютере сетевую карту или модем.

Сети TCP/IP, такие, как Интернет, находят компьютеры с помощью комбинации IP-адреса и MAC-адреса удаленного компьютера, как уже объяснялось ранее. Как и MAC-адрес, каждый IP должен быть уникален.

IP-адрес - это 32-битный адрес, состоящий из комбинации нулей и единиц. Однако, поскольку люди испытывают затруднения при запоминании 32-битных номеров, IP-адреса преобразовываются в десятичное представление с разделительными

точками, состоящее из четырех десятичных чисел, каждое из которых отделяется точкой. Например, IP-адрес 10000011 01101111 равнозначен адресу 131.111.7.27. IP-адреса могут присваиваться компьютеру статически или динамически. Статический адрес специально присваивается компьютеру и никогда не изменяется. Статические IP-адреса очень редки для соединений с Интернетом. Обычно поставщики услуг Интернета используют присвоение динамических IP-адресов.

Чтобы максимально облегчить вашу задачу, Windows 98, Me, NT 4, 2000 и XP автоматически изменяют свою конфигурацию для присвоения динамических IP-адресов. Например, на рисунке 3.5 показано диалоговое окно свойств TCP/IP для компьютеров с Windows 2000 Professional, который был сконфигурирован для DHCP.

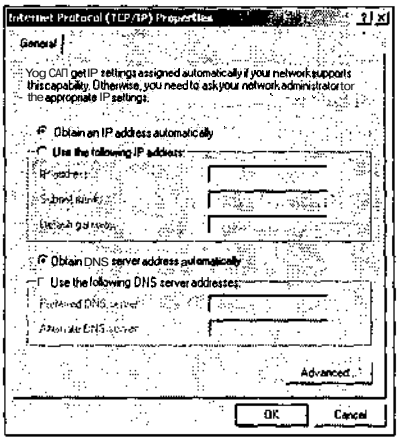


Рисунок 3.5. Конфигурация TCP/IP представлена в диалоговом окне свойств TCP/IP

Порты TCP/IP

Существует один дополнительный компонент, участвующий в процессе коммуникации, который вы должны знать, - это порт TCP/IP. Каждый пакет, посылаемый по сети, также содержит порт назначения, определяющий определенный ресурс на удаленном компьютере, для которого предназначен пакет. Например, когда вы хотите просмотреть Web-сайт, вы пишете адрес, такой, как www.microsoft.com, в поле URL вашего Web-браузера. Когда первоначальное соединение между вашим компьютером и Web-сервером установлено, дружественный адрес Web-сайта автоматически заменяется IP-адресом удаленного компьютера. Ко времени, когда соединение между вашим компьютером и Web-сервером установлено, оба компьютера знают IP-адреса друг друга и автоматически используют их для адресации пакетов данных во время остального сеанса связи.

Например, серверы, предоставляющие HTML-содержимое в Интернете, известны как HTTP-серверы. Чтобы соединиться с ними и получить HTML-содержимое, вы должны использовать порт 80. Даже без вашего сведения, ваш Web-браузер автоматически добавит номер порта в конец IP-адреса. Так что если адрес сервера HTTP Microsoft - 207.46.230.218, ваши пакеты данных в конечном счете адресуются на 207.46.230.218:80.

Проверяя номер порта каждого пакета, удаленный компьютер знает, что данные нужно посылать приложению, которое было приписано к этому номеру порта. В случае запроса HTTP-сервером Web-страницы пакет определит порт 80.

Существует более 60 000 возможных присваиваемых номеров портов на любом компьютере с TCP/IP. Чтобы взаимодействовать через один из этих портов, приложение или служба должна быть приписана к порту и активно просматриваться. Первые 1024 порта, пронумерованные от 1 до 1024, считаются хорошо известными (well-known) портами, и каждому порту в этом диапазоне уже присвоен определенный вид приложения или службы. Порты после 1024 известны под названием эфемерных портов и могут использоваться при необходимости любым приложением, предполагающим, что порт не занят уже другим приложением.

Например, порт 80 назначен HTTP-серверу. Порты 20 и 21 присвоены протоколу передачи файлов или FTP. На рисунке 3.6 изображено назначение портов TCP/IP. Первый порт в списке - порт 80, присвоенный приложению Персональный Web-сервер Microsoft (Microsoft Personal Web-Server), которое позволяет вам превратить ваш компьютер в мини-HTTP Web-сервер. Порты 137-139 являются портами NetBIOS, которые включаются, когда вы активизируете клиента для сетей Microsoft и общий доступ к файлам и принтерам. Вы узнаете больше о портах 137-139 в главе 4 "Защита сетей в Windows". Порт 4444 - это только один из тысяч эфемерных портов, которые могут назначаться любому приложению.

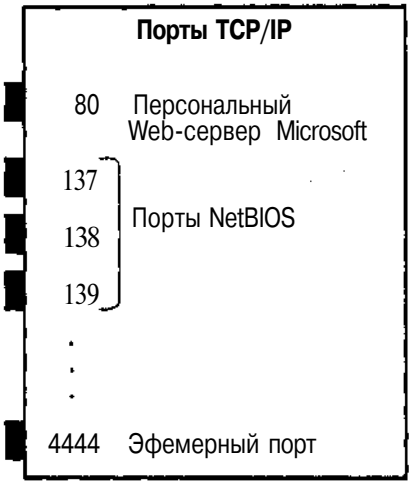
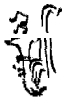


Рисунок 3.6. Изображение назначения Microsoft портов TCP/IP



Если вы хотите просмотреть более полный список портов TCP/IP, идите на *www.iana.org/assignments/port-numbers*.

Порты - основной источник воздействия на любой компьютер через Интернет. Как вы узнаете далее в этой главе, взломщики пытаются получить доступ к вашему компьютеру, разыскивая открытые и незащищенные порты.

Как работают брандмауэры

Брандмауэры работают, изучая содержимое пакетов для того, чтобы решить, пропускать ли пакет или нет. Например, на рисунке 3.6 изображены два приложения, пытающиеся передать данные через Интернет. Данные разбиты на пакеты, которые затем посланы через Интернет. Однако между двумя компьютерами установлен брандмауэр. Брандмауэр в этом примере сконфигурирован на разрешение всего трафика Internet Explorer. Internet Explorer создан так, чтобы взаимодействовать с Web-серверами Интернета с помощью порта 80. Как показано на рисунке 3.7, пакеты, предназначенные для порта 80, были пропущены брандмауэром. Однако на рисунке 3.7 также показано, что приложение "Троянский конь" каким-то образом проникло на компьютер и пытается передать данные на другой компьютер в Интернете, используя порт 4444, который брандмауэр был сконфигурирован блокировать. Кроме того, продемонстрировано, что брандмауэр показывает предупреждающее сообщение и делает запись в лог-файле.

Рисунок 3.7. Ваш персональный брандмауэр может быть сконфигурирован на блокировку трафика и сообщение о любом приложении, которое пытается установить соединение с Интернетом, не позволенное службой безопасности

Правила определения, что позволено пропускать через брандмауэр, а что нет, установлены службой безопасности, установленной на вашем брандмауэре. Различные брандмауэры имеют различные возможности и разные службы безопасности. С помощью соответствующей настройки правильной службы безопасности вы можете надежно обезопасить себя при работе в сети. Однако, неправильно сконфигурировав службы безопасности брандмауэра, вы можете сделать ваш брандмауэр почти бесполезным.

Функции брандмауэра

Ранее в этой главе вы видели список функций, которые должны присутствовать в персональных брандмауэрах. Этот и последующие разделы представят более детальное описание некоторых особых функций брандмауэров и разъяснят, как брандмауэры выполняют их. Основа каждой из этих функций - способность брандмауэра изучать пакеты и осуществлять работу служб безопасности, которые говорят ему, какие пакеты пропустить, а какие блокировать.

Обнаружение вторжения

Некоторые брандмауэры созданы, чтобы запрещать пропуск неразрешенных приложений через брандмауэр. Эти брандмауэры могут эффективно блокировать многие нападения. Тем не менее брандмауэры, в которые встроена программа обнаружения вторжения, предоставляют еще более высокий уровень безопасности.

Проблема с простым исследованием пакетов на предмет сведений о приложении и порте заключается в том, что оно, тем не менее, оставляет компьютер открытым для возможного нападения, запущенного с помощью одобренного приложения. Например, много дыр было обнаружено в таких продуктах, как Microsoft NetMeeting и Personal Web Server (хотя компания Microsoft продолжает закрывать каждую дыру при обнаружении). Эта методика также не защищает от атак "переполнение буфера". Атака "переполнение буфера" происходит, когда нападающий пытается использовать одобренное приложение для переполнения порта. Потенциально это может привести к аварийному отказу назначенного компьютера или сделать его насколько перегруженным, что он не сможет выполнять какую-либо необходимую работу.

Такие брандмауэры, как BlackICE Defender, в которые встроена программа обнаружения вторжения, могут предложить защиту от этих видов нападений. Например, брандмауэр BlackICE способен анализировать сотни видов атак. Программа обнаружения вторжения создана для изучения всего содержимого пакетов и определения их предназначения. Если персональный брандмауэр с программой обнаружения вторжения определит, что его главный компьютер подвергается нападению, он может просто блокировать пропуск пакетов, являющихся причиной нападения.

Определение попыток просканировать ваш компьютер

Взломщики могут использовать один из множества бесплатно доступных инструментов для исследования Интернета в поисках жертвы. Например, существует большое количество приложений ping-sweeper, которые могут быть использованы для поиска в Интернете активных TCP/IP соединений. *PING* - это команда TCP/IP, которая может быть использована для запроса статуса другого компьютера с протоколом TCP/IP и определения, активен ли он. Например, чтобы попытаться сделать это с любым компьютером в Интернете, введите PING

вслед за его именем или IP-адресом. Например, вы можете проделать это с сервером, как показано здесь:

```
C:\>ping www.que.com

Pinging que.com [128.121.231.124] with 32 bytes of data:

Reply from 128.121.231.124: bytes=32 time=100ms TTL=234
Reply from 128.121.231.124: bytes=32 time=100ms TTL=234
Reply from 128.121.231.124: bytes=32 time=100ms TTL=234
Reply from 128.121.231.124: bytes=32 time=100ms TTL=234

Ping statistics for 128.121.231.124:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 100ms, Average = 100ms
```

Вы также можете напечатать его IP-адрес и получить те же результаты:

```
C:\>ping 128.121.231.124

Pinging 128... 121.231.124 with 32 bytes of, data:

•Reply from 128.121.231.124: bytes=32 time=101ms TTL=234
Reply from 128.121.231.124: bytes=32 time=100ms TTL=234
Reply from 128.121.231.124: bytes=32 time=101ms TTL=234
Reply from 128.121.231.124: bytes=32 time=100ms TTL=234

Ping statistics for 128.121.231.124:
    Packets: Sent = A, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 101ms, Average = 100ms
```

Программа ping-sweeper может быть использована для просмотра тысяч IP-адресов в поисках активных компьютеров. После того как хакер нашел список активных компьютеров, другая бесплатная программа, известная как сканер портов, может быть запущена против компьютеров из списка для того, чтобы попытаться установить связь с рядом портов каждого активного компьютера. Более агрессивные атаки могут затем быть запущены против компьютеров, которые имеют открытые порты, позволяющие принять соединение. Если, например, хакер обнаружит, что порты 137-139 открыты, он может легко собрать ряд потенциально полезных частей информации, таких, как ваше имя пользователя и имя компьютера. Если порт 80 был обнаружен открытым и принимающим подключения (поскольку вы запустили Microsoft Personal Web Server), нападающий может пытаться запустить любое количество атак, используя хорошо известные слабые стороны этой службы.

Хороший брандмауэр может обнаружить, что его порты сканируются, зарегистрировать это событие и уведомить вас, если ему это поручено. Например, брандмауэр ZoneAlarm может быть сконфигурирован показывать всплывающее предупреждение каждый раз, когда ваш компьютер сканируется. В этом случае, если ваш жесткий диск внезапно начал вращаться или необъяснимо снизилась скорость работы, вы можете заблокировать нападение с помощью временного прерывания соединения. Брандмауэр BlackICE Defender идет еще дальше и от-

слеживает IP-адрес раздражающего компьютера, с которого был послан сканер, а затем докладывает о нем.

Однако не всегда сканирование - это нападение. Например, кто-то, возможно, случайно ввел неправильный IP-адрес при попытке соединиться с HTTP-сервером или открыть сеанс связи с другом через NetMeeting. Также возможно, что ваш провайдер мог запустить какое-либо тестирование. Другая ложная тревога, как известно, возникает от основанных на использовании технологий Интернета телевизионных услуг, которые иногда случайно соединяются с неправильными IP-адресами.

Важно просматривать журнал безопасности, созданный вашим персональным брандмауэром, и знать, когда ваш компьютер был просканирован. Обязательно просматривайте его, если количество сканирований вашего компьютера внезапно увеличилось.

Зашита от "Троянских коней"

Как вы уже знаете, "Троянский конь" - это программа, которая проникает на ваш компьютер и затем пытается невидимо связаться со своим создателем. Она делает это, пытаясь открыть порт TCP/IP и затем соединяясь с внешним компьютером. Цель программы может заключаться в поиске, нахождении и попытке копирования вашего Microsoft Quicken или других личных файлов, Или ее целью может быть получение контроля над вашим компьютером и использование его в атаке "распределенный отказ от обслуживания". В любом случае, если такая программа проникла на ваш компьютер, ее соединение с Интернетом должно быть заблокировано и вы должны быть проинформированы.

Персональные брандмауэры обнаруживают "Троянских коней", не доверяя ничему, даже сетевому трафику, произведенному вашим компьютером. Это означает, что все пакеты, как входящие, так и исходящие, постоянно изучаются.

Например, персональный брандмауэр McAfee позволяет вам указать список приложений, которым вы хотите разрешить проход через брандмауэр. Любое приложение, которое не находится в списке, но пытается установить связь, блокируется и создается предупреждение об этом. Когда вы получили предупреждение, вы уведомлены об имени исполняемого файла, который пытается установить соединение. Если вы распознаете его как приложение, которому вы хотите разрешить пройти через брандмауэр, вы можете ответить на предупреждение, позволив брандмауэру добавить его в список разрешенных приложений. Если вы подозреваете, что это "Троянский конь", вы можете удалить его и все угрозы, которые могут исходить от него.

Однако не всегда легко определить, не является ли исполняемая программа в действительности частью важного для вас приложения, и, удалив ее, вы можете случайно нарушить работу приложения. Поэтому вы, возможно, захотите переместить программу на дискету или ZIP-диск так, чтобы, если это окажется что-то важное для вас, вы могли бы скопировать это обратно в исходное положение.

Изучение всего сетевого трафика

Персональные брандмауэры должны уметь отличать новые запросы соединения от остального сетевого трафика. Самый первый пакет, посланный между двумя компьютерами при установлении соединения, отличается от всех остальных последующих пакетов. Первый пакет используется для запуска соединения. Все пакеты, которые следуют за первым пакетом, включают пометку подтверждения, которая указывает, что этот пакет был передан в ответ на запрос услуги. Ваш брандмауэр может затем использовать эту информацию, чтобы позволить пакетам пройти.

Это означает, что брандмауэр может быть настроен на блокировку всех незатребованных входящих запросов соединения, позволяя в то же время общение с серверами, с которыми ваш компьютер начал работу. При использовании таким образом персональный брандмауэр делает порты на вашем компьютере невидимыми в Интернете, поскольку, когда сканеры портов или программы ping sweeper попытаются начать сеанс связи с вашим компьютером, ваш брандмауэр будет игнорировать незатребованные запросы соединения. Порт, который не отвечает на запрос соединения, невидим во всех отношениях.

Классификация брандмауэров

Существует ряд технологий сетевой защиты, Некоторые более подходят для персонального использования, чем другие. Однако, краткий обзор каждой технологии может дать представление о технологии сетевой защиты в целом. Различные типы брандмауэров включают:

- шлюз приложений (Application-gateway);
- пакетный фильтр (Packet-filtering);
- уровня соединения (Circuit-level);
- проверки состояния (Stateful Inspection).

Каждый тип брандмауэра проверяет и обрабатывает проходящий пакет с помощью различных технологий. Некоторые персональные брандмауэры, такие как BlackICE, объединяют свойства более, чем одной технологии сетевой защиты. Каждый из этих типов сетевой защиты исследован в следующих разделах.

Брандмауэр - шлюз приложений

Брандмауэр - шлюз приложений - это модель большинства персональных брандмауэров. Эти виды брандмауэров иногда называются *прокси-брандмауэрами.* Эти брандмауэры могут фильтровать, основываясь на IP-адресах и определенных функциях, которые приложение пытается выполнить. Например, эти брандмауэры могут не пропустить определенные приложения, такие, как Microsoft NetMeeting, PCAnywhere или FTP. Просматривая функции приложения, брандмауэр может даже разрешить некоторые операции приложения, в то же время

блокируя остальные. Один из примеров этого - FTP-сайт, который разрешает вам загрузить файлы в указанные директории без разрешения просматривать или изменять файлы в директориях. Например, брандмауэры McAfee, BlackICE и ZoneAlarm имеют свойства шлюза приложений (application gateway).

Брандмауэры - пакетные фильтры

Брандмауэры - пакетные фильтры созданы так, чтобы просматривать пакеты, основываясь на их IP-адресах, и позволять соединение только с определенными IP-адресами. Как вы можете представить, это трудоемкий процесс, который потребует много усилий. Этот тип брандмауэров иногда используется компаниями для разрешения удаленного коммутируемого доступа своим работникам или доверенным клиентам. Но для домашних пользователей, которые, вероятно, путешествуют по всему Интернету и нуждаются в соединениях с любым количеством Web-сайтов, это непрактичный выбор.

Брандмауэры уровня соединений

Брандмауэры уровня соединений пропускают поток трафика с предварительно одобренных IP-адресов, сетей или поставщиков Интернет-услуг. Когда между пользователями на каждой стороне брандмауэра установлен сеанс связи, все остальные пакеты проходят через маршрутизатор непроверенными.

Брандмауэры проверки состояния

Вместо ограниченной проверки пакетов на соответствие требованиям порта или приложения брандмауэры проверки состояния изучают весь пакет целиком и анализируют его содержимое. Брандмауэры проверки состояния пытаются определить тип данных, которые передаются. Если это данные, которые рассматриваются как не несущие угрозы, данные брандмауэры позволяют им пройти. Например, в брандмауэр BlackICE встроен вариант этой технологии сетевой защиты.

Часть II
ПОВЫШЕНИЕ УРОВНЯ ВАШЕЙ БЕЗОПАСНОСТИ

4

Зашита сетей в Windows

Эта глава предоставляет описание того, как работают сети в Windows и как Microsoft реализует TCP/IP и другие свои Интернет-технологии. Вы увидите, как эти компоненты взаимодействуют и влияют на вашу безопасность, когда вы находитесь в Интернете. Эта глава предоставляет объяснение сущности пробелов в безопасности, имеющихся в сетях Microsoft, и показывает шаги, которые вы можете предпринять, чтобы повысить свою безопасность.

Вы также получите обзор различий между работой в сети World Wide Web с помощью Windows 95, 98 и Me и работой с помощью Windows 2000 или XP. Эта глава предоставит вам информацию относительно важности файловых систем Windows и объяснит, как выбор правильной файловой системы может помочь сделать вашу систему более безопасной.

В этой главе вы сможете:

- Проанализировать взаимосвязь сетевых и Интернет-технологий Microsoft;
- Ознакомиться с тем, как упростить вашу сетевую конфигурацию;
- Узнать, как сделать ваш компьютер с Windows более безопасным;
- Просмотреть методы уменьшения привлекательности вашего компьютера для взломщиков;
- Изучить преимущества модернизации вашей оперативной системы до более новой версии.

Обзор сетей Microsoft

Когда вы находитесь в Интернете, вы имеете доступ к мировому изобилию ресурсов. Однако, пока вы не предприняли мер по защите вашего компьютера, вы можете быть удивлены, как много доступа мир имеет к вашему компьютеру. Цель этой главы - показать, что существует ряд вещей, которые вы можете сделать, чтобы помочь защитить себя, до того, как начнете работать в сети World Wide Web

с вашим новым, всегда подключенным, высокоскоростным соединением с Интернетом. Действия, которые вы должны предпринять, чтобы защитить себя, включают:

- удаление ненужных компонентов сетей Microsoft;
- удаление и очистка ваших сетевых привязок (network bindings);
- использование более безопасной операционной системы;
- выбор более сложного пароля;
- установка персонального брандмауэра;
- установка антивирусной программы.

Ознакомление с сетями Microsoft

Сетевое программное обеспечение, встроенное в операционную систему Microsoft, создано для поддержки вашего компьютера в локальной сети, если ваш компьютер в нее входит. *Локальная сеть* ~ совокупность объединенных компьютеров, расположенных на небольшой территории, такой, как дом или здание. Сети Microsoft созданы, чтобы позволять совместное использование ресурсов, таких, как файлы и папки, расположенных на жестких дисках компьютеров, входящих в сеть.

В тексте данной книги ссылки на локальные сети означают обращение к персональным домашним сетям, состоящим из 2-3 компьютеров.

Степень безопасности сетей Microsoft зависит от операционных систем, которые установлены на компьютере. Если домашняя сеть с Windows полностью состоит из компьютеров с Windows NT, 2000 или XP, это намного более безопасно, чем если она состоит из компьютеров с Windows 95, 98 и Me. Это происходит потому, что серия операционных систем Windows NT характеризуется тем, что содержит в себе файловую систему безопасности, известную как *файловая система новой технологии* (NTFS), которая позволяет вам применять значительно более сильную защиту ресурсов диска и принтера. Однако подавляющее большинство домашних пользователей все еще работают с операционными системами Windows 95, 98 или Me, а эти операционные системы не поддерживают файловую систему NTFS.

По определению, кабельные и цифровые соединения с Интернетом являются на самом деле соединениями с локальной сетью. Так что, имеете ли вы домашнюю сеть или нет, ваш компьютер все равно связан с локальной сетью. Операционные системы Microsoft автоматически устанавливают по умолчанию набор сетевых компонентов после установки сетевого соединения, такого, как соединение с Интернетом или с домашней локальной сетью. Эти сетевые компоненты включают:

- клиент для сетей Microsoft;
- общий доступ к файлам и принтерам сетей Microsoft;

- протокол сети Интернет (TCP/IP);
- программный драйвер сетевой платы.

Как вы увидите далее в этой главе, совместное присутствие сетей Microsoft и протокола TCP/IP подвергает ваш компьютер риску при выходе в Интернет.

До появления широкополосного Интернета безопасность доступа причиняла домашним пользователям немного беспокойства. Безопасность была просто хорошим замком на вашей входной двери. После того как вы были соединены с Интернетом, правила изменились. Пока вы не предпримете нескольких базовых мер, дверь вашего компьютера остается широко открытой. И пока вы не установите персональный брандмауэр, ваш компьютер будет постоянно взламываться. Чтобы понять, почему это происходит, вы должны узнать сначала, как различные компоненты сетей Microsoft совмещаются друг с другом, что описывается в следующем разделе.

Как осуществляется работа сетей Microsoft

Программная конфигурация, которая составляет сеть Microsoft, может быть рассмотрена как существующая на трех отдельных различных уровнях. На высшем уровне находятся три программные службы Microsoft, которые предоставляют основные сетевые функциональные возможности, включая возможность соединяться с сетью Microsoft и совместно использовать ее ресурсы. Эти службы содержат:

- Клиент для сетей Microsoft - сетевой компонент, который предоставляет интерфейс домашней сети и позволяет пересылать информацию по этой сети к компьютеру и от него.
- Семейный вход Microsoft - необязательный компонент, доступный в Windows 98 и Me, который используется для входа в сети Microsoft и получения доступа к сетевым ресурсам.
- Общий доступ к файлам и принтерам для сетей Microsoft - необязательный компонент, который позволяет вашему компьютеру делить свои файлы, папки и принтеры с остальными членами сети. По умолчанию эта опция отключается. Однако, за исключением случая, если вы установили вашу операционную систему самостоятельно, вы должны дважды проверить, чтобы убедиться, что эта опция не была включена, как будет показано дальше в главе.

Клиент для сетей Microsoft предоставляет двустороннее соединение с сетью Microsoft. Семейный вход Microsoft предоставляет удобные средства для входа в локальные сети. Общий доступ к файлам и принтерам - необязательный сетевой компонент, который позволяет вам предоставлять общий доступ к ресурсам дисков и принтеров на вашем компьютере. Хотя эти три программные компонента являются ключевыми частями домашней сети Microsoft, они необязательны, если все, что вам нужно, это выход в Интернет. Однако, как уже отмечалось, клиент для сетей Microsoft и семейный вход Microsoft устанавливаются автома-

тически, когда вы настраиваете ваше соединение с Интернетом, оставляя ваш компьютер уязвимым перед нападением. В зависимости от того, кто устанавливал операционную систему на вашем компьютере, общий доступ к файлам и принтерам может быть также установлен и разрешен.

Средний уровень модели сетей Microsoft состоит из сетевых протоколов, поддерживаемых Microsoft. TCP/IP - это протокол, использующийся для доступа в Интернет и большинство других сетей. Как вы узнали в главе 3 "Описание брандмауэров", TCP/IP адресует и направляет данные по сетям, таким, как Интернет. Другие протоколы, такие, как NetBEUI, также могут располагаться на этом уровне.

Протокол NetBEUI - это простой и легкий в обращении протокол для управления процессом передачи данных в домашних сетях. Он не требует конфигурирования и не может быть перенесен на ваше соединение с Интернетом.

Низший уровень модели сетей Microsoft состоит из соединений с различными сетями. Каждый из видов этих соединений кратко охарактеризован здесь:

- соединение с локальной сетью - соединение с домашней сетью;
- коммутируемое соединение - соединение с Интернетом с помощью стандартного модема со скоростью 56 Кб/с;
- широкополосное соединение - постоянно подключенное кабельное или цифровое соединение с Интернетом.

Доверяемые сети Microsoft

По умолчанию сети Microsoft базируются на модели сети, которая предполагает определенный уровень доверия. По существу, операционные системы Microsoft автоматически конфигурируют или объединяют программные компоненты, расположенные на каждом уровне сетевой модели, как показано на рисунке 4.1. Хотя это может быть приемлемо для домашних сетей, этот уровень доверия не подходит для компьютера с постоянно подключенным соединением с Интернетом.

Привязка (binding) - это процесс соединения двух сетевых компонентов так, чтобы они могли общаться друг с другом. Пока два сетевых компонента не связаны, они не могут взаимодействовать. Поэтому снижение числа связанных сетевых компонентов может устранить некоторые из дыр в безопасности операционных систем Microsoft при соединении с Интернетом.

Вы можете просмотреть сетевые привязки для конкретного компонента Windows из диалогового окна Сеть, выбирая и проверяя его свойства. Например, следующая методика показывает, как вы можете просмотреть привязки соединения с Интернетом на компьютере с Windows 95, 98 или Me.

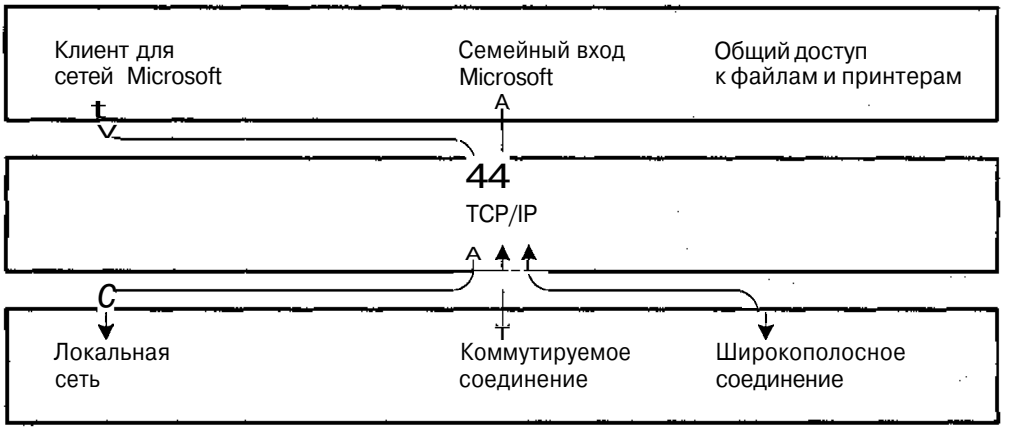


Рисунок 4.1. По умолчанию операционная система Microsoft позволяет всем сетевым компонентам сообшаться и взаимодействовать друг с другом

1. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.
2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети, как показано на рисунке 4.2.

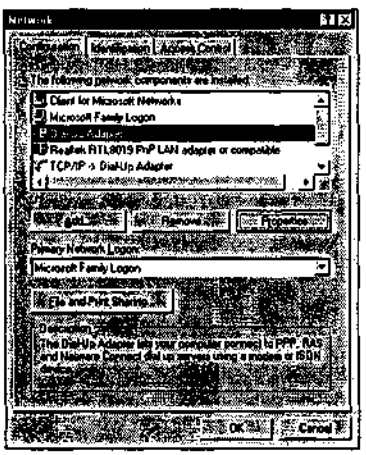


Рисунок 4.2. Изучение сетевых компонентов, установленных на типичном компьютере Microsoft

3. Выберите адаптер, представляющий ваше сетевое соединение, и вызовите Свойства.
4. Выберите пункт меню Привязка, как показано на рисунке 4.3.

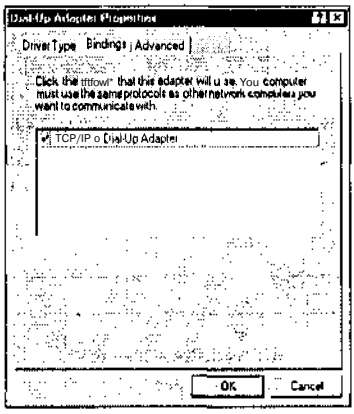


Рисунок 4.3. Просмотр привязок вашего соединения с Интернетом

Как вы можете видеть, соединение с Интернетом привязано к TCP/IP. Если ваш компьютер с Windows 95, 98 или Me соединен с домашней сетью, вы можете просмотреть привязки к вашей сетевой плате следующим образом:

Л. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.

2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети.

3. Выберите сетевой адаптер и вызовите Свойства. Появится диалоговое окно свойств для сетевого адаптера.

4. Выберите пункт меню Привязка, как показано на рисунке 4.4.

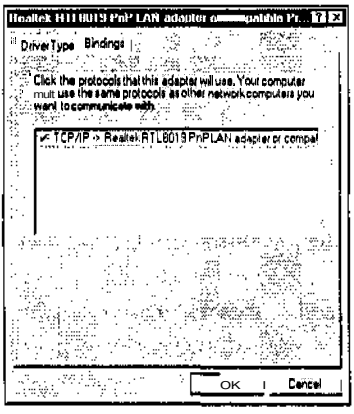


Рисунок 4.4. Просмотр привязок сетевой платы к домашней сети

Как вы можете видеть, сетевая плата привязана к вашему TCP/IP-соединению, таюке как и соединение компьютера с Интернетом. По умолчанию операционные системы Microsoft привязывают все на каждом уровне ко всему на прилегающих

уровнях в сетевой модели. Это делает конфигурацию сети намного проще, но намного менее безопасной. Поэтому появляется возможность для кого-нибудь в Интернете проникнуть в ваш компьютер с помощью вашего TCP/IP-соединения и затем получить доступ к домашней сети, к которой ваш компьютер присоединен.

Чтобы просмотреть существующие привязки между TCP/IP и сетевыми компонентами Microsoft высшего уровня на компьютере с Windows 95, 98 или Me, используйте следующую процедуру:

1. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.
2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети.
3. Выберите либо компонент TCP/IP, связанный с соединением с Интернетом, либо один из связанных с сетевым адаптером, и затем нажмите Свойства. Появится диалоговое окно выбранного компонента TCP/IP.
4. Выберите пункт меню Привязка, как показано на рисунке 4.5.

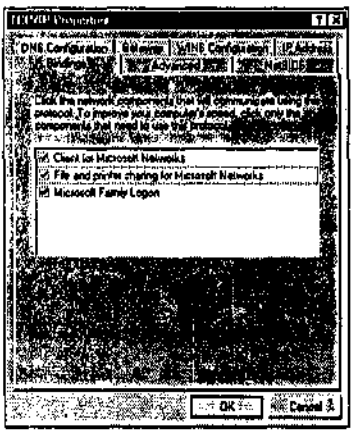


Рисунок 4.5. Просмотр привязок TCP/IP к сетевым компонентам Microsoft высшего уровня

Как вы можете видеть, TCP/IP привязан ко всем программным компонентам Microsoft высшего уровня по умолчанию. Это позволяет компьютеру соединяться с домашней сетью и получать доступ к сетевым ресурсам. Если у вас также есть домашняя сеть, общий доступ к файлам и принтерам Microsoft должен быть разрешен на каждом компьютере, чтобы позволить им объединить их ресурсы с другими компьютерами сети, как показано на рисунке *4.6.*

Если привязки коммутируемого и широкополосного соединений отключены, сетевые соединения, изображенные на рисунке 4.6, будут защищены в силу того факта, что соединение с Интернетом будет отключено. Но как только вы соединитесь с Интернетом, правила изменятся, в особенности если у вас широкополосное соединение.

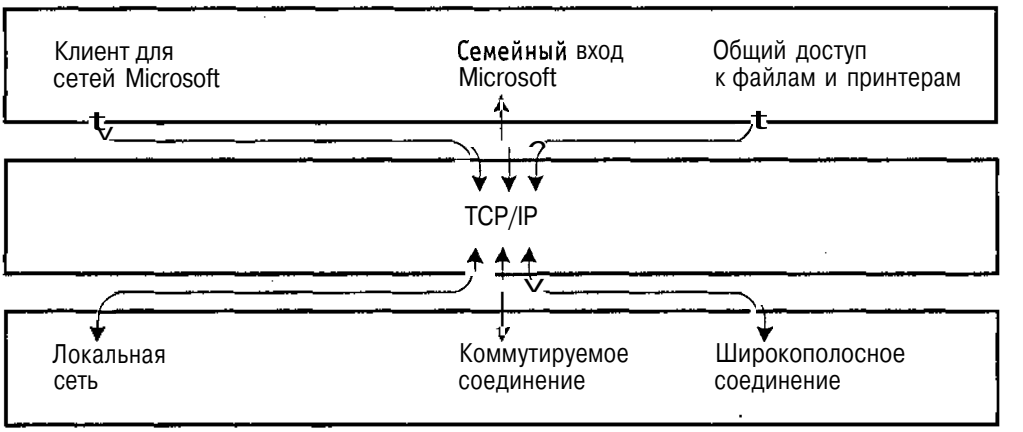


Рисунок 4.6. Просмотр сетевых привязок Microsoft, устанавливаемых по умолчанию, для компьютера, соединенного с Интернетом и домашней сетью

Так как общий доступ к файлам и принтерам и ваше соединение с Интернетом привязаны к TCP/IP, это открывает возможность для взломщика попытаться получить доступ к вашим локальным дискам. Хакер имеет даже возможность получить доступ к домашней сети, если ваш компьютер соединен с ней, поскольку как ваше соединение с Интернетом, так и ваша локальная сеть привязаны к TCP/IP по умолчанию.

Когда TCP/IP установлен впервые, операционные системы Microsoft начиная с Windows 98 выводят на дисплей сообщение, предупреждающее об опасности оставления его привязанным к соединению с Интернетом и предлагающее отключить его. Однако, если вы не установили TCP/IP самостоятельно, вы никогда не увидите этого сообщения, и велики шансы того, что ваш компьютер незащищен.

Закрытие ваших портов NetBIOS

Как уже говорилось ранее в этой главе, Клиент для сетей Microsoft автоматически устанавливается на вашем компьютере всегда, когда операционная система обнаруживает соединение с любым видом сети. Даже если у вас нет домашней сети, операционная система Microsoft установит по умолчанию сетевые компоненты Microsoft, поскольку соединение с Интернетом также рассматривается как сетевое соединение.

Когда Клиент для сетей Microsoft установлен, Microsoft автоматически открывает порты TCP 137, 138 и 139. Это неважно, есть ли у вас домашняя сеть, Microsoft установит их в любом случае. Microsoft использует эти порты наряду с протоколом, называемым NetBIOS, для облегчения коммуникации по сетям Microsoft. Через эти порты такие ресурсы, как папки, дисководы и принтеры, совместно используются в сетях (включая Интернет). Через эти порты компью-

теры в сети также делятся информацией об их общих ресурсах. Это предоставляет любому сетевому компьютеру возможность запрашивать у компьютера информацию о нем. Эти порты и их службы перечислены здесь:

- 137 - служба имени NetBIOS;
- 138 - служба дейтограммы NetBIOS;
- 139 - служба сеанса связи NetBIOS.

К сожалению, NetBIOS не требует авторизации от кого-либо в сети (домашней или Интернете) и поэтому предоставляет некоторую информацию по запросу, включая:

- имя пользователя, в настоящее время находящегося в сети;
- имя компьютера;
- рабочие группы домашней сети, к которой подсоединен компьютер.

Эта информация кое-что говорит хакерам о вас и дает им отправную точку для запуска атаки. Например, если имя вашего компьютера похоже на название телепередачи, то, возможно, ваши пароли, если они есть, основаны на названиях других телепередач. Информация, которую предоставляет NetBIOS, может также действовать как приманка, которая привлекает внимание хакеров. Чтобы защитить себя, подумайте о том, чтобы дать вашему компьютеру имя, настолько неинтересное, насколько это возможно.

Если компьютер, который вы используете для соединения с Интернетом, также соединяется с другим домашним компьютером, вы должны присвоить неинтересные имена и всем общим ресурсам на них.

Зашита ваших принтеров и дисководов от взломщиков из Интернета

Если у вас дома нет локальной сети - это причина не оставлять Клиента для сетей Microsoft, семейный вход Microsoft и общий доступ к файлам и принтерам установленными на вашем компьютере. Они созданы с единственной целью поддерживать соединение с локальной сетью. Простое удаление их сделает вашу систему более безопасной. Их удаление также закроет порты NetBIOS 137-139.

Вы можете получить небольшое дополнительное вознаграждение, удалив эти сетевые компоненты, так как освободите немного памяти и поможете тем самым вашему компьютеру загружаться быстрее.

Как показано на рисунке 4.7, единственное сетевое соединение, которое нужно оставить, это соединение между TCP/IP и коммутируемым или широкополосным соединением, в зависимости от того, которое из них вы используете для соединения с Интернетом.

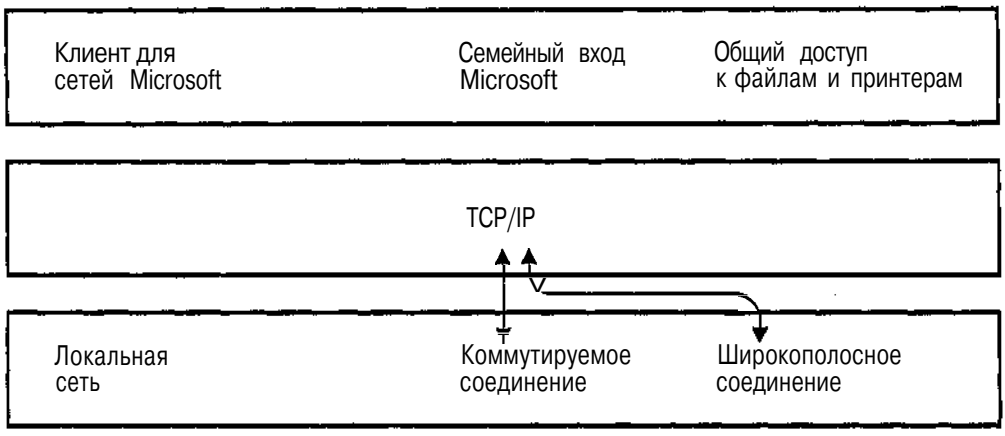


Рисунок 4.7. Единственное соединение, которое должно быть связано, чтобы работали все ваши Интернет-приложения, такие, как Internet Explorer, это соединение между TCP/IP и вашим соединением с Интернетом

Если у вас нет домашней сети, вы должны подумать об удалении сетевых компонентов Microsoft. Следующая процедура кратко описывает процессы удаления этих трех сетевых компонентов Microsoft с компьютеров с Windows 95, 98 или Me.

1. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.
2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети.
3. Выберите Клиент для сетей Microsoft и нажмите Удалить.
4. Выберите Семейный вход Microsoft и нажмите Удалить.
5. Нажмите OK.

Общий доступ к файлам и принтерам, если он установлен, будет автоматически удален при удалении Клиента для сетей Microsoft.

Конфигурирование связи в домашних сетях

Если у вас есть домашняя сеть, вам необходимо обеспечить связь между всеми компьютерами, объединенными в сеть, и в то же время попытаться снизить риск, связанный с вашим соединением с Интернетом. Это означает, что вам необходимо оставить ваши сетевые компоненты Microsoft, установленные на ваших компьютерах, объединенных в сеть. Для снижения незащищенности ваших данных вы должны вручную отсоединить все привязки к TCP/IP так, чтобы протокол TCP/IP мог соединяться только с Интернет-соединением, но не с другими компонентами связи высшего уровня Microsoft.

Если вы не отсоедините ваши привязки к протоколу TCP/IP и сделаете ваши файлы и принтер общими, вы оставите свой компьютер полностью доступным

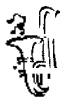
для пользователей сети. В Интернете существуют десятки сканирующих программ. Некоторые из этих сканеров специально созданы для поиска IP-адресов и выискивают компьютеры, у которых доступны порты 137-139.

Если вы знаете, как сделать папку или дисковод общими (смотри главу 11 "Домашние сети и общий доступ к Интернету"), вы знаете, как легко получить доступ к ним через Интернет, Запомните, что когда вы вышли в Интернет, вы соединились с сетью, которая вам неподконтрольна. Если вы не использовали пароли для защиты общих ресурсов, кто угодно, просканировав ваш компьютер и обнаружив, что он незащищен, может скопировать ваши сетевые настройки. На компьютерах с Windows 95, 98 и Me это даст хакерам полный контроль над вашим компьютером, они смогут сделать все, что захотят, включая чтение, копирование, переименование и даже удаление ваших файлов.

Вы, должно быть, слышали о том, что вы можете добавить $ в конце наименования общих ресурсов, чтобы сделать их скрытыми от посторонних глаз. Что ж, это неправда, Добавление знака $ в конец наименования общих ресурсов лишь делает их невидимыми для другой сети, когда они входят в сеть с помощью My Network Neighborhood. Хакерские программы, находящиеся в Интернете, могут видеть все ваши общие ресурсы, добавлен ли знак $ в конец их наименования, или нет.

Даже если ваши совместно используемые ресурсы защищены паролем, вы по-прежнему в большой беде, потому что большинство паролей общих ресурсов могут быть легко взломаны с использованием десятков программ для взлома паролей, свободно доступных в Интернете. Еще хуже, Microsoft не предупреждает вас, когда кто-либо взламывает пароли ваших общих ресурсов.

Персональный брандмауэр со встроенным детектором вторжения может блокировать взломщиков паролей и уведомить вас о том, что произошла атака.



Если вы должны сделать ресурсы полностью доступными для домашней сети, постарайтесь избегать совместного пользования дисководами и ограничить число общих ресурсов настолько, насколько это возможно.

Большинство людей не задают пароли для домашних сетей, поскольку неудобно печатать пароль каждый раз, когда вы хотите получить доступ к ресурсу. Использование одного и того же пароля для защиты всех ресурсов, находящихся в общем пользовании, также не очень хорошая идея, поскольку, как только он взломан, он делает доступным все содержимое вашего компьютера. Единственный вариант - создать уникальный пароль для каждого общего ресурса, а не просто ввести первый попавшийся пароль. Так как программы для взлома паро-

лей имеют возможность взламывать пароли, которые включают общие имена и слова, вы должны создать пароли, которые имеют следующие характеристики:

- они длинны;
- они непонятны (нелегки для отгадывания);
- они включают цифры, заглавные и строчные буквы и специальные символы.

Хорошей идеей является также настройка графика регулярной смены вашего пароля. Таким образом, если хакер взломает его, он или она получит доступ на более ограниченный период времени.

К сожалению, пароли могут быть сложными для запоминания. И когда у вас их более чем несколько, это становится еще более сложным. Кроме того, люди склонны называть общие ресурсы описательными именами, которые указывают на их содержание. Хотя это делает более легким их нахождение, это также облегчает хакерам достижение интересующих их целей. Поэтому имена общих ресурсов должны быть настолько неинтересны, насколько это возможно.

Если у вас есть домашняя сеть, вы должны использовать следующую методику для удаления ненужных сетевых привязок к TCP/IP на компьютерах с Windows 95, 98 или Me:

1. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.
2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети.
3. Выберите либо компонент TCP/IP, связанный с соединением с Интернетом, или один из связанных с сетевым адаптером, и затем нажмите Свойства. Появится диалоговое окно выбранного компонента TCP.
4. Выберите пункт меню Привязка.
5. Удалите каждый из выбранных элементов в сетевых компонентах высшего уровня и нажмите OK.
6. Закройте диалоговое окно Сети и перезагрузите компьютер, когда потребуется.

Теперь, когда вы очистили свои привязки к TCP/IP, вы должны предоставить каждому компьютеру в вашей сети способ передачи информации друг другу. Самый легкий путь достигнуть этого - это сохранить сокращенный набор привязок к TCP/IP, показанный в предыдущем примере, а также загрузить и установить протокол NetBEUI на всех компьютерах вашей домашней сети. Логически, ваши сетевые привязки должны затем выглядеть, как те, которые изображены на рисунках 4.8 и 4.9.

На рисунке 4.8 показано, как сетевые привязки выглядят на сетевом компьютере, который имеет соединение с Интернетом. Как вы можете видеть, установлен и TCP/IP, и NetBEUI. Однако оба протокола связаны с различными ресурсами и привязки между ними нет.

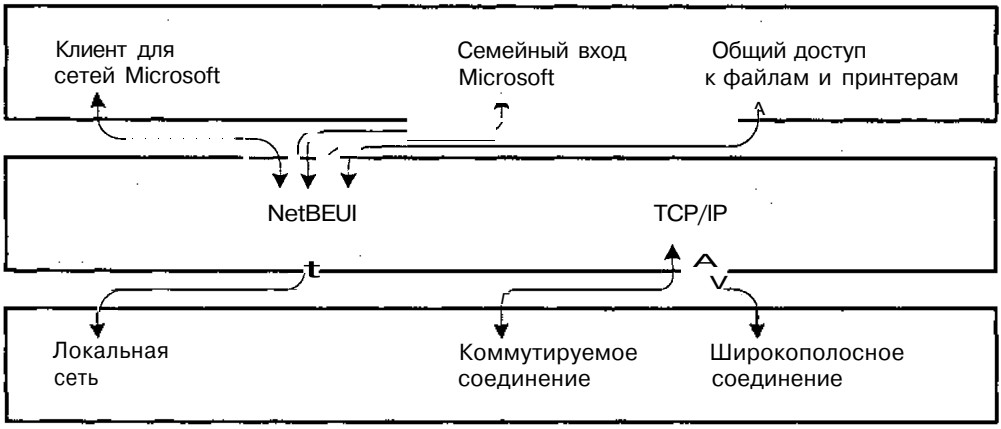


Рисунок 4.8. Использование NetBEUI в качестве протокола вашей локальной сети вместо TCP/IP

На рисунке 4.9 показано, как сетевая привязка выглядит на остальных сетевых компьютерах. Как вы можете видеть, здесь нет TCP/IP.

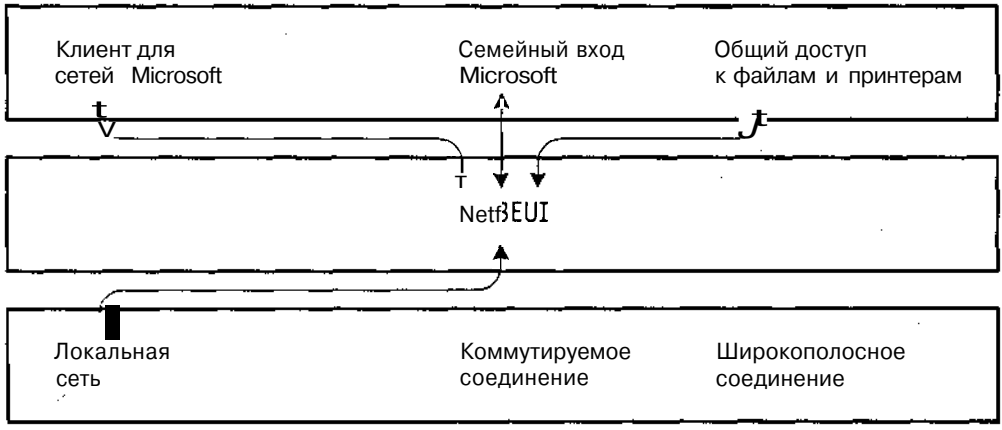


Рисунок 4.9. NetBEUI - отличный протокол локальной сети, который не требует конфигурирования при установке и использовании

Другое решение - это покупка персонального аппаратного брандмауэра и использование его для защиты вашей домашней сети, основанной на TCP/IP, от Интернета. *Более* подробная информация об этой опции доступна в главе 11.

Следующая методика показывает, как установить протокол NetBEUI на компьютеры с Windows 95, 98 и Me:

1. Нажмите Пуск, Настройка и затем Панель управления. Откроется Панель управления Windows.

2. Дважды щелкните мышью по иконке Сеть. Откроется диалоговое окно сети.
3. Нажмите клавишу Добавить. Появится диалоговое окно выбора типа сетевого компонента, как показано на рисунке 4.10.

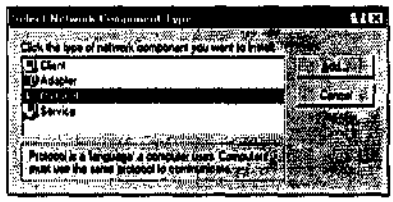


Рисунок **4.10.** Установка нового протокола локальной сети

4. Выберите Протокол и нажмите Добавить. Появится диалоговое окно выбора сетевого протокола, как показано на рисунке 4.11.

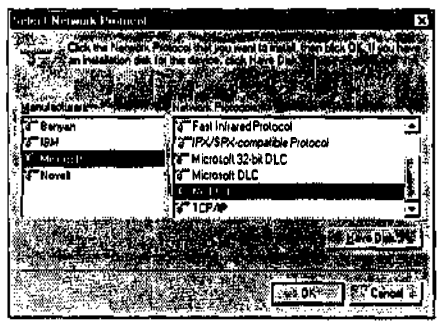


Рисунок 4.11. Выбор протокола Microsoft NetBEUI

5. Выберите Microsoft из списка производителей.
6. Выберите NetBEUI из списка сетевых протоколов,
7. Вновь появится диалоговое окно Сеть. Нажмите OK. Windows начнет установку NetBEUI. Вставьте CD-диск с Windows, если потребуется.
8. Нажмите Да, когда попросят перезагрузить ваш компьютер.

Повышение вашей безопасности

До этого момента в этой главе вы узнали, как сделать ваш компьютер более безопасным с помощью удаления ненужных сетевых компонентов Microsoft или, если у вас есть домашняя сеть, с помощью изменения их конфигурации на более безопасную. Этот раздел посвящен другому способу повышения уровня защиты вашего компьютера: модернизации вашей операционной системы.

Если у вас установлена операционная система Windows 95, 98 или Me, вы, возможно, подумывали о модернизации до Windows 2000 Professional или Windows XP Home Edition с тех пор, как они появились в конце 2001 года. Windows 2000

Professional и XP Home Edition предоставляют поддержку значительно более защищенной файловой системы, которая имеет следующие возможности:

- возможность требовать авторизации пользователя до получения доступа к ресурсам компьютера;
- строгие ограничения прав на файловые системы, которые могут использоваться для управления доступом к отдельным ресурсам, таким, как файлы, папки и дисководы целиком;
- возможность зашифровки файлов таким образом, чтобы только человек, который их зашифровал, мог их расшифровать и получить к ним доступ.

Применение имен пользователя и паролей

В отличие от Windows 95, 98 и Me, Windows 2000 и Windows XP позволяют вам устанавливать требование ввода имен пользователя и паролей, без которых вам или хакеру откажут в доступе к вашему компьютеру и его файловой системе. Эти операционные системы также могут быть сконфигурированы отключать учетную запись пользователя в случае, если хакер пытается запустить против них программу, взламывающую пароли. Например, вы можете сконфигурировать блокировку учетной записи после нескольких неудачных попыток отгадывания или взлома пароля.

Пароль учетной записи должен быть тщательно продуман и никогда не должен состоять из общих имен или слов. Устанавливаемые по умолчанию учетные записи, созданные при установке операционной системы, должны быть переименованы. Это относится и к учетным записям администратора и гостя. Оставление названий этих двух учетных записей без изменений лишь сделает их более легкими для обнаружения хакерами.

Windows 2000 Professional и Windows XP Home Edition также позволяют вам делать общими ресурсы директорий и дисков. Если у вас нет домашней сети, у вас не должен быть установлен общий доступ, а если он у вас установлен, вы должны его удалить. Если у вас есть домашняя сеть, вам нужно использовать все те же методы модификации привязок и применения сложных паролей для общих ресурсов, как и в системах с Windows 95, 98, и Me.

Зашита NTFS

Используемая вами операционная система Windows делает очень многое для защиты вашего компьютера. Различные операционные системы Windows предоставляют поддержку для различных файловых систем, как показано в таблице 4.1.

Таблица 4.1. Поддержка файловой системы операционных систем Microsoft.

ОС	Windows 95	Windows 98	Windows NT	Windows 2000
FAT	Да	Да	Да	Да
FAT32	Только OSR2	Да	Нет	Да
NTFS 4	Нет	Нет	Да	Да
NTFS 5	Нет	Нет	Требует SP4	Да

Windows 95, 98 и Me созданы для работы с версиями файловой системы FAT. *Файловая система* - это механизм, который операционная система использует для организации, хранения и извлечения информации с дисководов.

Файловая система FAT - это 16-битная файловая система, в которой хранятся файлы в виде имен файлов, состоящих из восьми знаков, с необязательным расширением файла, состоящим из трех знаков. Не существует встроенного механизма для защиты файлов, хранящихся на FAT дисководах. FAT32 - это 32-битная версия FAT, поддерживающая длинные имена файлов (до 256 знаков). Как и FAT, FAT32 - это незащищенная файловая система. Поэтому, если вы работаете с Windows 95, 98 или Me при соединении с Интернетом, файлы, хранящиеся на вашем жестком диске, потенциально уязвимы.

Windows NT, 2000 и XP, в свою очередь, поддерживают файловую систему NTFS, значительно более безопасную, чем файловая система FAT. NTFS предоставляет операционной системе возможность защищать файлы, папки и целые дисководы с помощью разрешений безопасности. Правильно применяемый, NTFS позволяет получать доступ к файлам на основе этих разрешений. Это создает большие трудности для хакеров, поскольку, даже если они получили доступ к просмотру содержимого ваших дисководов, открытие, изменение или удаление файлов все равно будет заблокировано для него.

Когда кто-либо пытается получить доступ к файлу в системе с Windows 2000 или XP, он должен сначала получить соответствующее разрешение. Это означает, что если хакер смог получить доступ к вашему компьютеру и справился со взломом одной из его учетных записей, файлы, разрешение на доступ к которым учетная запись не может получить, все еще заблокированы для них.

Вы можете применить разрешения безопасности с помощью нажатия правой клавиши мыши на ресурсы Windows, такие, как файл или папка, выбрать Свойства, вызвать пункт меню Безопасность и затем нажать на клавишу Разрешения. Это откроет диалоговое окно свойств ресурса, как показано на рисунке 4.12.

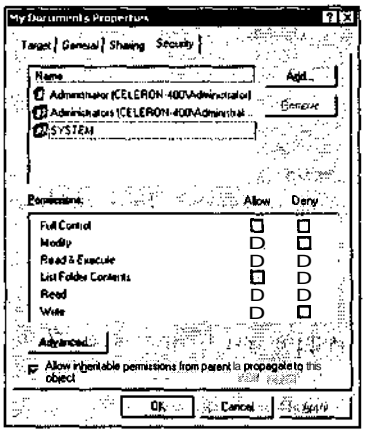


Рисунок 4.12. Конфигурирование файловых разрешений на компьютере с Windows 2000

Чтобы предоставить пользователю или группе пользователей доступ к ресурсам, выберите их из списка учетных записей и нажмите Добавить. Когда вы вернетесь в Свойства Безопасности, выберите Разрешения, которые вы хотите присвоить учетной записи, и нажмите OK.

Чтобы хакеры получили доступ к ресурсу в системе с Windows 2000 или XP, им придется взломать пароль учетной записи, которая содержит соответствующий набор разрешений. Если хакер попытается напасть на учетные записи Windows 2000 и XP с помощью грубой силы словарной атаки, операционная система автоматически отключит учетные записи, когда будет сделано слишком много неправильных попыток.

Сравните эту модель безопасности с той, что используется Windows 95, 98 и Me, в которой хакер нуждается лишь во взломе пароля, присвоенного данному ресурсу (который не отключается при запуске против него программы взлома пароля с помощью грубой силы), и вы увидите, что модернизация вашей операционной системы может сделать ваш компьютер намного более защищенным.

Но до того, как вы оцените и купите Windows 2000 Professional или Windows XP Home Edition, вы должны узнать о нескольких недостатках этих систем. Ни одна из этих систем не бесплатна и обе требуют намного больше ресурсов вашего компьютера, чем Windows 95, 98 или Me. Если вы купили ваш компьютер не в последние несколько лет, вы, возможно, будете неспособны подняться до одной из этих операционных систем без значительной модернизации аппаратных средств или покупки нового компьютера.

Минимальные аппаратные требования этих операционных систем приведены в таблице 4.2.

Таблица 4.2. Аппаратные требования операционных систем Microsoft.

ОС	Windows 98	WindowsMe	Windows 2000	WindowsXP
Память	16 Мб	32 Мб	64 Мб	64/128Мб
Центральный процессор	486	Pentium 150	Pentium 133	Pentium 233/300
Жесткий диск	175 Мб	480 Мб	650 Мб	1.5 Гб

Зашифровка файлов

Еще одно свойство, предоставляемое операционными системами Windows 2000 и Windows XP, - это *система шифрования файлов* (EFS). EFS доступна, только если вы отформатировали ваш жесткий диск с использованием NTFS. EFS позволяет вам зашифровывать отдельные файлы, папки или даже целые жесткие диски. Зашифровка файла делает его более защищенным, поскольку только человек, зашифровавший его, может его расшифровать. Конечно, процесс шифрования связан с небольшими издержками, которые могут немного снизить скорость работы при открытии и закрытии файлов. Однако вы, возможно, никогда этого не заметите.

После зашифровки ваш файл, папка или дисковод выглядят и работают также как всегда, поскольку с этого момента Windows автоматически зашифровывает и расшифровывает их при необходимости, когда вы с ними работаете. Другие пользователи сети и хакеры из Интернета видят изображение вашего жесткого диска, могут просмотреть список ваших зашифрованных файлов, но не могут открыть их.

Хотя вы можете зашифровать отдельный файл или целый жесткий диск, Microsoft рекомендует в общем случае зашифровывать на уровне папок. Когда вы зашифровали папку, любой файл, добавленный в нее, автоматически зашифровывается.

Вы должны, вероятно, зашифровать вашу папку Мои документы, а так же, все остальные папки, где вы храните секретную информацию. Кроме того, вы должны также зашифровать папку Windows Temp, поскольку Windows иногда размещает в этой директории копии файлов, с которыми вы работаете.

Используйте следующую методику при зашифровке папки Мои документы в системе с Windows 2000.

1. Нажмите правую клавишу мыши на папке Мои документы и выберите Свойства. Появится диалоговое окно свойств папки Мои документы.
2. Нажмите пункт меню Общие и выберите клавишу Подробнее, как показано на рисунке 4.13.

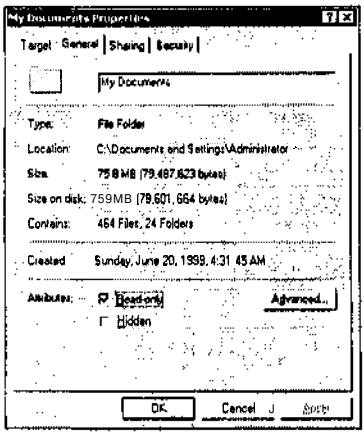


Рисунок 4.13. Пункт меню Общие диалогового окна свойств папки Мои документы

3. Появится диалоговое окно Подробных свойств, как показано на рисунке 4.14.
4. Выберите опцию Зашифровать содержимое для защиты данных и нажмите OK.
5. Нажмите OK, когда возвратитесь в окно Общие.

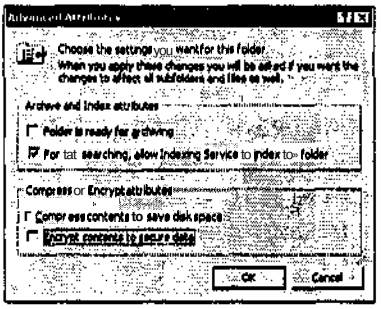


Рисунок 4.14. Зашифровка папки Мои документы в Windows 2000

6. Появится диалоговое окно подтверждения изменения свойств, спрашивающее, должны ли зашифровываться поддиректории, расположенные в папке Мои документы, как показано на рисунке 4.15. Чтобы быть в безопасности, вы должны защищать все. Выберите Применить изменения к этой папке, папкам более низких уровней и файлам и нажмите OK.

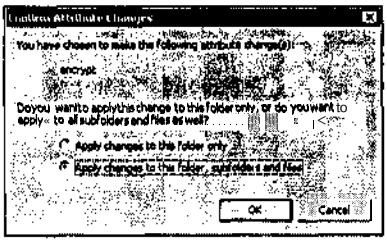


Рисунок 4.15. Добавление зашифровки содержимого папки, включая папки более низкого уровня

Чтобы проверить, что операционная система Windows 2000 зашифровала папку и ее содержимое, отключите компьютер и затем вновь зайдите в систему как другой пользователь и попробуйте получить доступ к файлу в папке Мои документы.

Почему вы все равно должны приобрести персональный брандмауэр

ЕСЛИ после прочтения этой главы и изменения конфигурации вашего домашнего компьютера или домашней сети вы чувствуете себя в безопасности, предупреждаю, что вы все еще не защищены достаточно. То, что вы просто отсоединили сетевые компоненты Microsoft от вашего TCP/IP соединения, не означает, что вы стали "пуленепробиваемым" при путешествиях по Интернету. Все, что вы сделали, это удалили некоторые из целей хакеров. Всегда существуют другие способы, с помощью которых хакеры могут проникнуть на ваш домашний компьютер. Они включают способы, которые уже описывались в этой книге, такие, как использование программы "Троянский конь" и программ-червей, которые

после внедрения на ваш компьютер вызывают появление у вас множества проблем. Другие виды атак могут быть внедрены внутрь нормального Интернет-приложения.

За последние несколько лет ряд пробелов в безопасности, которые позволяют хакерам проникнуть на вашу компьютерную систему, был обнаружен в таких приложениях, как Microsoft NetMeeting. На рисунке 4.16 изображен способ, с помощью которого TCP/IP обеспечивает взаимодействие с программами, установленными на вашем компьютере, и Интернетом.

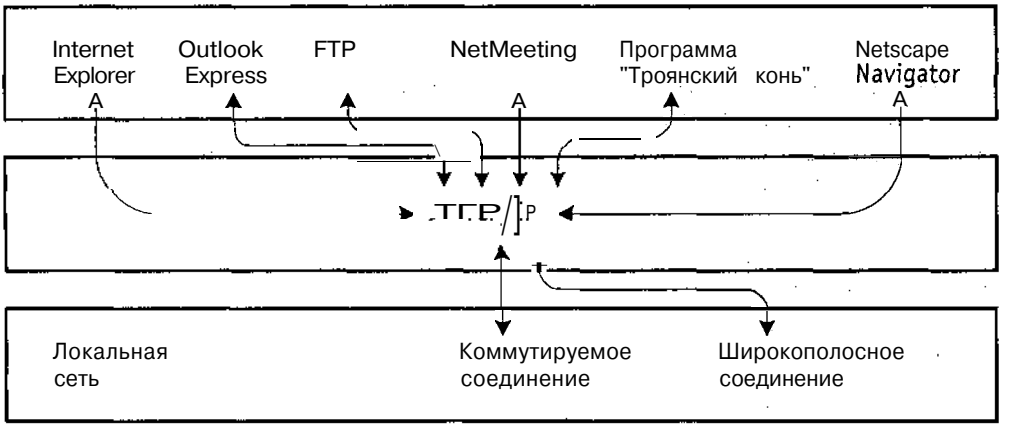


Рисунок 4.16. Любое Интернет-приложение предоставляет хакеру возможность угрожать вашему компьютеру или домашней сети

Во многих случаях вы можете защитить себя от этих видов угроз, поддерживая свою операционную систему и приложения на уровне современных требований. Это может быть сделано с помощью частого посещения Web-сайта обновлений вашей операционной системы Microsoft и Web-сайтов разработчиков ваших Интернет-приложений. Однако у большинства людей нет времени на выполнение этой кропотливой работы. Так что по крайней мере на сегодняшний день единственный путь достигнуть любого уровня безопасности вашего постоянно подключенного соединения с Интернетом - это купить себе хороший брандмауэр. Большинство брандмауэров включают годовую стоимость бесплатных обновлений, и вы можете проинструктировать брандмауэр автоматически загружать и выполнять их для того, чтобы гарантировать, что ваш персональный брандмауэр отвечает современным требованиям и имеет максимально возможную мощность.

5

Аппаратные брандмауэры

Эта глава познакомит вас с аппаратным устройством, известным как широкополосный кабельно-цифровой маршрутизатор EtherFast. В дополнение к некоторым другим свойствам эти устройства выполняют функции персонального аппаратного брандмауэра. Эта глава описывает, как установить и сконфигурировать персональный аппаратный брандмауэр, на примере кабельно-цифрового маршрутизатора Linksys BEFSR41 EtherFast.

Помимо физической установки вы увидите, как брандмауэр конфигурируется с помощью стандартного Web-браузера. Вы также узнаете, как сконфигурировать регистрацию входящего и исходящего трафика брандмауэра, как получить доступ к этим регистрационным записям и просмотреть их.

В этой главе вы сможете:

- узнать, как установить и сконфигурировать типичный персональный аппаратный брандмауэр;
- узнать, как добавить пароль;
- узнать, как спрятать ваши порты TCP/IP;
- узнать, как заблокировать IP-адреса вашей домашней сети от соединения с Интернетом;
- выяснить, как настроить лог-файлы, которые регистрируют все входящие и исходящие IP-адреса, порты и адреса URL.

Аппаратные брандмауэры

Современный персональный аппаратный брандмауэр - это внешнее устройство, которое выполняет ряд операций. Он соединяет ваш компьютер и ваш кабельный или цифровой модем и фильтрует весь входящий и исходящий трафик с Интернетом. Эти устройства обычно называются **кабельно-цифровыми** маршрутизаторами. В список их свойств обычно включаются следующие:

- маршрутизатор - управляет потоком информации между двумя отдельными сетями. В данном случае трафик проходит между вашим компьютером или домашней сетью и Интернетом;
- концентратор - позволяет нескольким домашним компьютерам объединяться в локальную сеть. Концентратор поддерживает одновременно одно соединение, которым могут пользоваться совместно все компьютеры сети;
- коммутатор - позволяет устанавливать временное выделенное соединение между двумя домашними компьютерами, чтобы увеличить пропускную спо-

собность и ускорить передачу игр и мультимедиа, содержимого. Коммутатор способен создавать несколько одновременных сетевых соединений, позволяющих многим компьютерам взаимодействовать одновременно;

- брандмауэр - защищает ваш компьютер или домашнюю сеть от нападения извне.

После того как они должным образом установлены и сконфигурированы, эти устройства представляют собой единственное видимое соединение с Интернетом. Эти устройства обычно стоят от 100 до 250 долларов и могут объединять в домашнюю сеть от одного до пяти компьютеров, которые также могут получить общий доступ к соединению с Интернетом, хотя устройства с более чем пятью портами сейчас легко доступны. Поскольку это единственное видимое сетевое устройство, ваш поставщик услуг кабельного или цифрового доступа в Интернет не сможет определить число компьютеров, подсоединенных к нему, что, таким образом, позволит вам сэкономить на дополнительных месячных выплатах за общий доступ к соединению более чем одного компьютера. Одни эти сбережения могут легко оплатить устройство за год или два, в зависимости от количества компьютеров, которые вы подсоединяете к нему. Более подробная информация о том, как совместно использовать ваше соединение с Интернетом и создать домашнюю сеть, представлена в главе 11 "Домашние сети и общее подключение к Интернету".

Эти сетевые устройства не требуют установки на ваш компьютер дополнительного программного обеспечения. Они оснащены встроенной программой (программой, запрограммированной в комплекте микросхем устройств). Вы можете сконфигурировать устройства с помощью Интернет-браузеров Internet Explorer или Netscape Communicator начиная от версии 4 и выше.

Кабельно-цифровой маршрутизатор BEFSR41 EtherFast

Изображение кабельно-цифрового маршрутизатора Linksys BEFSR41 EtherFast, показанное на рисунке 5.1, можно найти по адресу www.linksys.com, оно иллюстрирует работу типового аппаратного брандмауэра.

На передней панели маршрутизатора BEFSR41 расположен ряд световых индикаторов, которые указывают на состояние устройства и каждого из его соединений. В нижнем левом углу находится индикатор включения в сеть. Три ряда световых индикаторов показывают состояние каждого отдельного соединения. Три индикатора в конце рядов показывают состояние соединения устройства с вашим кабельным или цифровым модемом. Индикатор *Link (Связь)* показывает, что соединение установлено успешно. Индикатор *Act (Активность)* показывает, что данные проходят через устройство. Индикатор *Diag (Диагностика)* показывает, что устройство проводит самодиагностику. Эта проверка запускается всякий раз, когда включается питание устройства.

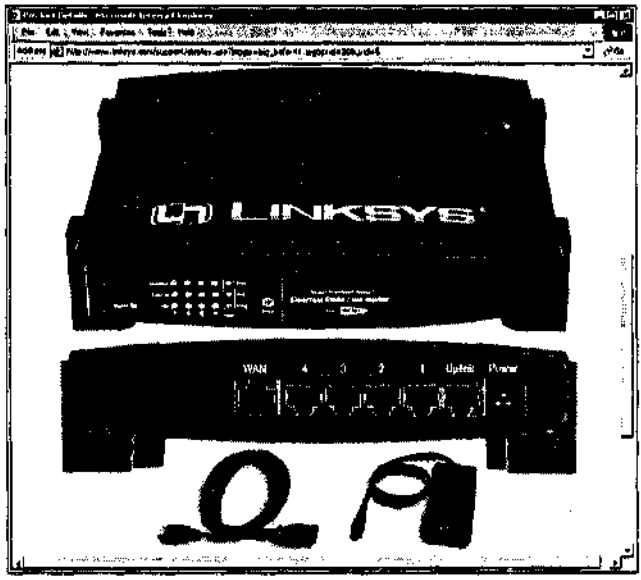


Рисунок 5.1. Кабельно-цифровой маршрутизатор Linksys BEFSR41 EtherFast позволяет вам подсоединять до четырех компьютеров к домашней сети и совместно использовать одно высокоскоростное соединение с Интернетом с помощью встроенной межсетевой зашиты

На обратной стороне устройства вы найдете гнездо подключения к сети и шесть портов для соединений. С левого края расположен порт WAN. Этот порт используется для соединения устройства с вашим кабельным или цифровым модемом с помощью кабеля витой пары RJ-45. Следующие четыре порта используются для подсоединения от одного до четырех компьютеров и создания домашней сети, которая также может совместно использовать соединение с Интернетом. Последний порт соединяет устройство с другим сетевым концентратором. Это позволяет вам расширить размер домашней сети.

Установка аппаратного брандмауэра

Следующие методики кратко описывают процесс установки кабельно-цифрового маршрутизатора BEFSR41 EtherFast для работы с одним домашним компьютером. Хотя эта методика характерна для этого маршрутизатора, она может также использоваться в качестве общего описания установки других подобных устройств. Единственное предварительное условие для выполнения этого процесса - это то, что ваш домашний компьютер должен уже иметь правильно настроенный TCP/IP.

1. Отключите питание вашего компьютера и кабельного модема.
2. Подсоедините маршрутизатор BEFSR41 к вашему кабельному или цифровому модему, вытащив конец кабеля витой пары RJ-45, который в настоящий

момент соединяет ваш компьютер с кабельным или цифровым модемом, и вставив его в порт WAN маршрутизатора BEFSR41.

3. Подсоедините маршрутизатор BEFSR41 к вашему компьютеру, вставив новый кабель витой пары RJ-45 в один из открытых портов на обратной стороне маршрутизатора BEFSR41 и в сетевую карту Ethernet вашего компьютера.

4. Включите маршрутизатор BEFSR41, подсоединив его адаптер источника питания.

5. Включите ваш кабельный или цифровой модем.

6. Включите ваш компьютер.

7. Когда ваш компьютер закончит загружаться, войдите в сеть и откройте ваш Интернет-браузер. Что случится дальше, зависит от вашего поставщика услуг Интернета. Если вы можете соединиться с Интернетом и видите на экране вашу домашнюю страничку, установленную по умолчанию, то все готово. Однако вы, возможно, обнаружите, что на экран выведено сообщение об ошибке, подобное тому, что показано на рисунке 5.2. Большинство провайдеров, предоставляющих кабельное или цифровое соединение с Интернетом, контролируют число активных соединений с Интернетом каждого из своих клиентов с помощью MAC-адреса каждого компьютера, производящего соединение (который вы должны были предоставить, когда настраивали ваше соединение с Интернетом). Маршрутизатор BEFSR41 имеет свой собственный MAC-адрес и поскольку, ваш провайдер не распознал его, он был заблокирован. Чтобы обойти эту проблему, вы можете изменить MAC-адрес маршрутизатора BEFSR41 так, чтобы он соответствовал одному из тех, которые вы зарегистрировали у своего провайдера. Перейдите к шагу 8, чтобы изменить MAC-адрес маршрутизатора BEFSR41.

8. Вы можете сконфигурировать маршрутизатор BEFSR41 с помощью вашего Web-браузера, напечатав `192.168.1.1` в поле URL вашего браузера и нажав Enter. Появится диалоговое окно введения пароля для входа в сеть, как показано на рисунке 5.3.

9. Конфигурирование маршрутизатора BEFSR41 автоматически защищается с помощью пароля. Первоначальный пароль, устанавливаемый по умолчанию, - `admin`. Оставьте поле Имя пользователя пустым, напечатайте `admin` в поле Пароль и нажмите OK.

10. Появится страница установки (Setup) Linksys, как показано на рисунке 5.4.

11. Нажмите на закладку Подробнее (Advanced) наверху окна и затем выберите Копирование MAC-адреса (MAC Address Clone), как показано на рисунке 5.5.

12 Введите MAC-адрес сетевой карты Ethernet вашего компьютера. Это тот же самый MAC-адрес, который вы зарегистрировали у вашего провайдера. Нажмите Добавить (Apply).

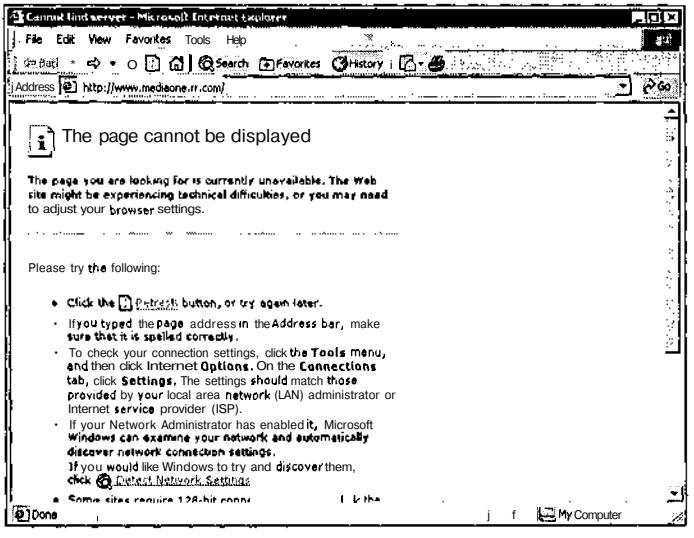


Рисунок 5.2. Поставщик услуг кабельного или цифрового доступа к Интернету заблокировал соединение маршрутизатора BEFSR41, опираясь на его MAC-адрес

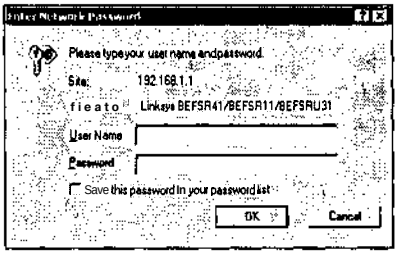


Рисунок 5.3. Конфигурирование маршрутизатора BEFSR41 зашишается паролем

Если вы не помните MAC-адрес сетевой карты Ethernet вашего компьютера, откройте приглашение на ввод команды (command prompt) на вашем компьютере и напечатайте `winipcfg` на компьютере с Windows 95 или 98 или `ipconfig /all` на компьютере с Windows Me, NT 4, 2000 или XP и затем нажмите **Enter.**

13. MAC-адрес маршрутизатора BEFSR41 изменится и появится сообщение, показанное на рисунке 5.6. Нажмите Далее (Continue).

14 Перезагрузите ваш кабельный или цифровой модем, выключив его из сети. а затем включив.

15. Перезагрузите ваш компьютер.

Теперь ваш компьютер должен быть готов к соединению с Интернетом.

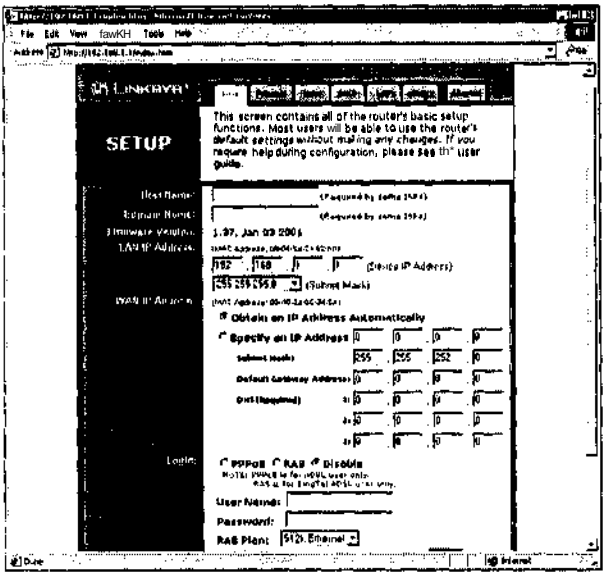


Рисунок 5.4. Главная страница установки Linksys позволяет вам просматривать и изменять настройки конфигурации сети

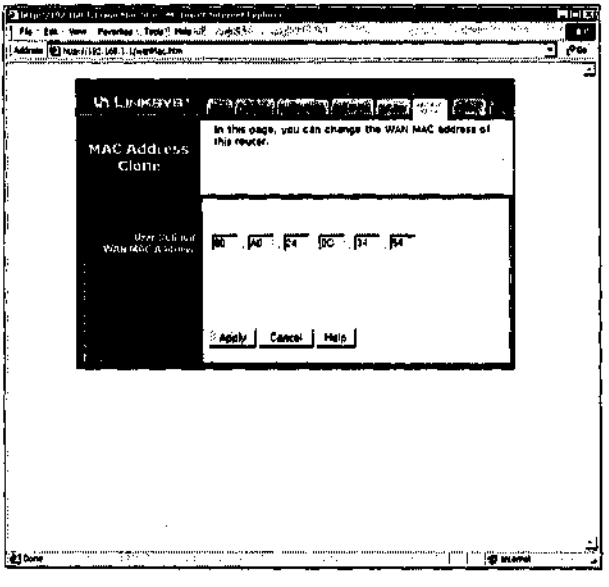


Рисунок 5.5. Изменение MAC-адреса маршрутизатора BEFSR41 на адрес, совпадающий с MAC-адресом сетевой карты Ethernet вашего компьютера

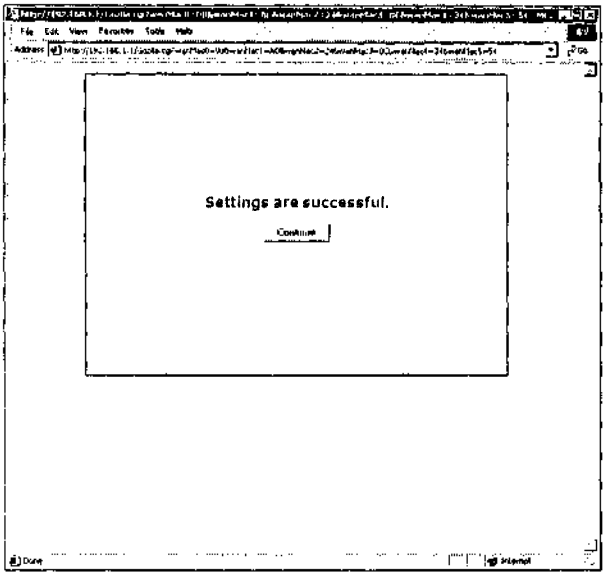


Рисунок 5.6. Вы успешно изменили MAC-адрес маршрутизатора BEFSR41

Конфигурирование с помощью Web-браузера

Как вы видели в предыдущем разделе, кабельно-цифровые маршрутизаторы можно сконфигурировать, напечатав их IP-адрес, устанавливаемый по умолчанию, в вашем Web-браузере и нажав Enter. Маршрутизатору BEFSR41 присвоен адрес 192.168.1.1.

Установка основных настроек конфигурации

По умолчанию кабельно-цифровые маршрутизаторы сконфигурированы принимать от вашего провайдера динамически присваиваемые IP-адреса. Большинство провайдеров присваивает IP-адреса динамически, однако, если ваш провайдер присвоил вам статический или не изменяющийся IP-адрес, вам придется заполнить информацией поля на странице установки (SETUP) Linksys, как показано на рисунке 5.7.

Поля Host Name (Имя хоста) и Domain Name (Имя домена) позволяют вам ввести имена хоста и домена, если они предоставлены вашим провайдером. Однако обычно эти поля оставляются пустыми. В поле Firmware Version (Версия встроенной программы) указывается версия встроенной программы маршрутизатора. В разделе LAN IP Address (IP-адрес локальной сети) указывается MAC-адрес маршрутизатора, IP-адрес и маска подсети, присвоенные маршрутизатору. Эти настройки должны быть оставлены в том виде, в каком они установлены.

Аппаратные устройства могут иметь проблемы с безопасностью. Хорошая идея - проверять время от времени Web-сайт поставщика вашего аппаратного брандмауэра, чтобы убедиться, что у вас установлена последняя версия его встроенной программы. Более подробная информация о модернизации встроенного программного обеспечения будет предоставлена далее в этой главе.

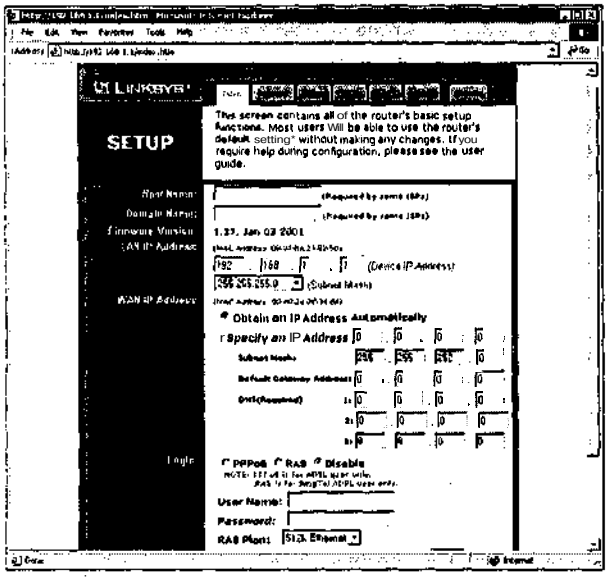


Рисунок 5.7. Изменение конфигурации статического IP-адреса

IP-адрес глобальной сети (WAN IP Adress) устанавливается по умолчанию на автоматическое получение IP-адреса. Чтобы установить конфигурацию статического IP-адреса, присвоенного вам вашим провайдером, выберите опцию Specify an IP Address (Установить IP-адрес) и заполните оставшиеся поля информацией, которая была предоставлена вам вашим провайдером.

Некоторые цифровые соединения используют протокол точка-точка (Point-to-point) через Ethernet или PPPoE для установки соединений вместо DHCP. PPPoE - это безопасный протокол, который требует имя пользователя и пароль для установки соединения. Если ваш поставщик услуг цифрового доступа в Интернет использует этот протокол, выберите PPPoE и введите присвоенное вам имя пользователя и пароль. Некоторые другие поставщики услуг цифрового доступа в Интернет предоставляют соединения с Интернетом, используя сервис удаленного доступа, или RAS. Если ваш провайдер использует этот сервис, выберите RAS и напечатайте ваше имя пользователя и пароль, а затем выберите 256K или 512K из списка ниспадающего меню RAS. В противном случае оставьте выбранную по умолчанию опцию disable (блокировка).

Вы можете выбрать опции Connection on Demand (Соединение по требованию) и Max Idle Time (Максимальное время простоя), чтобы сконфигурировать маршрутизатор для автоматического разъединения с Интернетом, когда вы не используете ваше соединение. Поле Max Idle Time (Максимальное время простоя) дает вам возможность указать время (в минутах) неактивного состояния соединения, которое может пройти до того, как эти свойства вступят в действие. Эта опция предоставляет полную блокировку с помощью брандмауэра исходящего из Интернета трафика. Однако, как только вы запустите Интернет-приложение, соединение с Интернетом автоматически переустановится.

PPPoE соединения с Интернетом могут прерваться раньше времени. Опция Keep Alive (Поддерживать соединение) создана для предотвращения этого путем пересылки нескольких пакетов в заранее указанные интервалы так, чтобы ваш провайдер думал, что вы все еще используете ваше соединение.

Изменение вашего пароля

Важно изменить пароль кабельно-цифрового маршрутизатора, чтобы не допустить изменения ваших параметров настройки конфигурации другими людьми. В противном случае кто-либо, кто имеет доступ к вашему компьютеру или домашней сети, может внести изменения, напечатав IP-адрес маршрутизатора и введя слово admin в качестве пароля.

Страница пароля, показанная на рисунке 5.8, позволяет вам изменять пароль маршрутизатора. Просто напечатайте новый пароль в обоих полях Router Password (Пароль маршрутизатора) и нажмите Apply (Добавить).

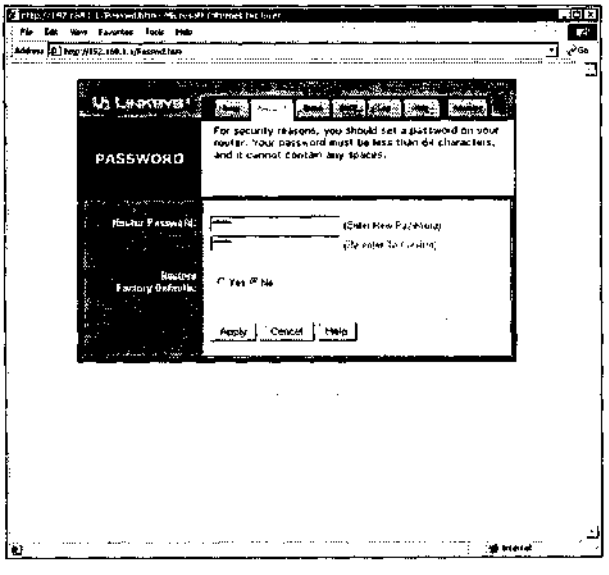


Рисунок 5.8. Изменение пароля предотвращает несанкционированные изменения конфигурации вашего аппаратного брандмауэра

Опция Restore Factory Default (Восстановление настроек по умолчанию) отменит все изменения, которые вы внесли в кабельно-цифровой маршрутизатор BEFSR41 EtherFast. Затем вам придется заново начать изменение конфигурации маршрутизатора. Используйте эту опцию, если у вас возникли проблемы с устройством и вы неспособны обнаружить причину этой проблемы. Тем самым вы отмените любые индивидуальные изменения конфигурации и сможете начать заново.

Проверка состояния вашего маршрутизатора

Страница Status (Состояние), показанная на рисунке 5.9, выводит на экран текущие настройки конфигурации маршрутизатора и отражает элементы, которые вы выбрали на странице установки. Host Name (Имя хоста) показывает присвоенное вам имя хоста (если требуется). Firmware Version (Версия встроенной программы) показывает текущую версию программного обеспечения маршрутизатора. Login (Вход в систему) показывает текущее состояние входа в систему (PPPoE, RAS или Disable (Отключен)).

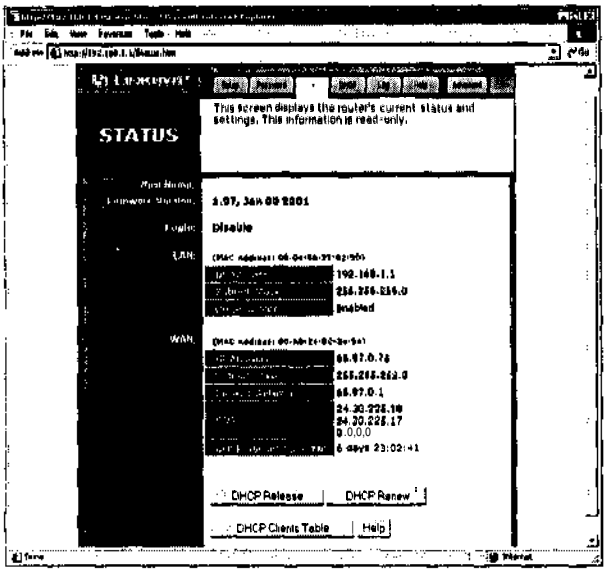


Рисунок 5.9. Изображение текуших параметров настройки конфигурации маршрутизатора

Раздел LAN (Локальная сеть) показывает настройки локального IP-адреса маршрутизатора, тогда как раздел WAN (Глобальная сеть) показывает информацию об IP-адресе, присвоенном вашим провайдером.

Внизу страницы расположены три опции:

- DHCP Release (Отключение DHCP) - приказывает маршрутизатору сообщить вашему провайдеру о том, что вы хотите отключить ваш текущий IP-адрес.

- DHCP Renew (Обновление DHCP) - запрашивает о присвоении нового IP-адреса у вашего провайдера.
- DHCP Clients Table (Таблица клиентов DHCP) - выводит список всех клиентов локальной домашней сети, включая их имена, IP-адреса и MAC-адреса. Эта опция более подробно описывается в главе 11.

Конфигурирование вашей службы DHCP

Страница DHCP, показанная на рисунке 5.10, контролирует службу DHCP маршрутизатора, которая включена по умолчанию.

Опция DHCP Server (Сервер DHCP) позволяет вашему маршрутизатору присваивать любые возможные IP-адреса любому из компьютеров домашней сети. Эта опция включена по умолчанию. Даже если у вас есть только один компьютер, лучше оставить эти опции включенными по умолчанию. Поле Starting IP (Исходный IP-адрес) позволяет вам указать диапазон исходных IP-адресов, которые вы хотите использовать. Максимально возможный диапазон - от 192.168.1.2 до 192.168.1.253. Это означает, что маршрутизатор может теоретически поддерживать домашнюю сеть, которая состоит из более чем 250 компьютеров. По умолчанию IP-адрес настраивается как 192.168.1.100. Если у вас один компьютер, подсоединенный к маршрутизатору, его IP-адрес по умолчанию равен 192.168.1.100. Более подробная информация о том, как IP-адреса присваиваются домашним сетям, доступна в главе 3 "Описание брандмауэров" и главе 11. Клавиша внизу страницы предоставляет связь с таблицей клиентов DHCP.

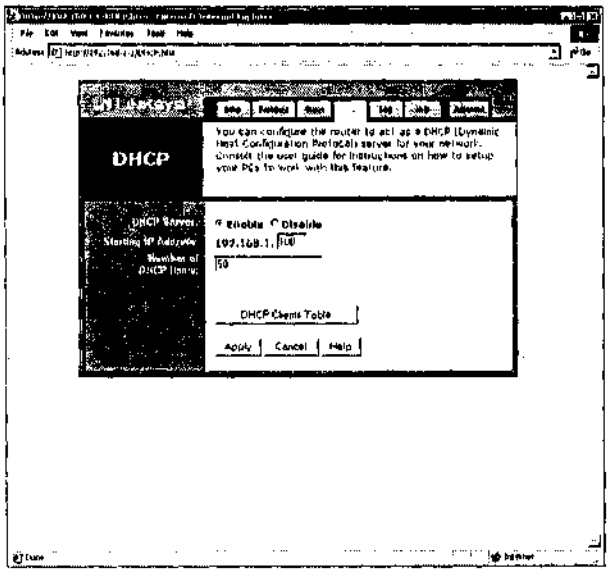


Рисунок 5.10. Конфигурирование встроенной службы DHCP маршрутизатора

Настройка регистрационных записей вашего маршрутизатора/брандмауэра

Страница Log (Регистрация), показанная на рисунке 5.11, позволяет вам установить регистрацию для хранения как входящего, так и исходящего трафика Интернет. Регистрируется следующая информация:

- IP-адреса и порты, связанные со всем входящим трафиком;
- URL и порты, использующиеся вашим компьютером или другими компьютерами в домашней сети при соединении с Интернетом, а также IP-адрес локального компьютера, который устанавливает связь.

По умолчанию опция Access Log (Регистрация доступа) отключена. Если вы ее запустите, вам понадобится также указать IP-адрес локального компьютера, на котором будут создаваться лог-файлы. Вы можете просмотреть весь входящий трафик, нажав Incoming Access Log (Регистрация доступа входящего трафика). Подобным образом вы можете просмотреть исходящий трафик, нажав Outgoing Access Log (Регистрация доступа исходящего трафика).

На рисунке 5.12 показан пример таблицы регистрации входящего трафика. Как вы можете видеть, там перечислены IP-адреса компьютеров из Интернета, пытающихся установить соединение, и номера портов, с которых была предпринята попытка соединения. В этом примере активность выглядит подозрительно, поскольку кажется, что компьютер подвергается систематическому зондированию портов. Это и было в действительности так, однако Зондирование, показанное в примере, было запущено с целью использования бесплатной услуги сканирования портов в Интернете, предлагаемой на *grc.com*. Более подробная информация о сканерах портов доступна в главе 9 "Насколько защищен ваш компьютер?".

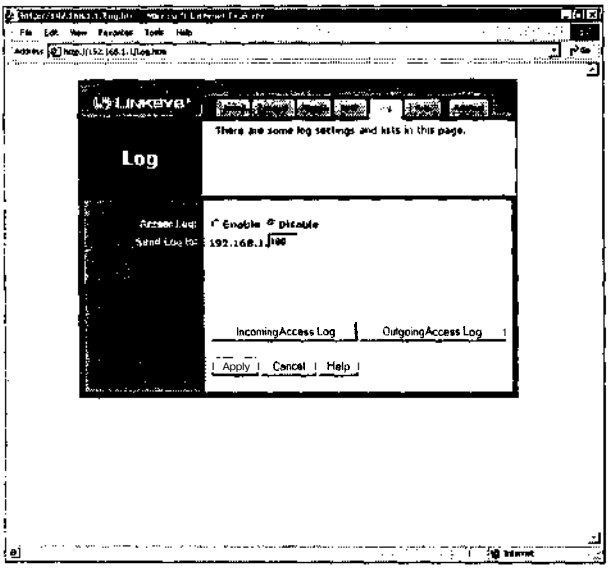


Рисунок 5.11. Настройка лог-файлов для регистрации входящего и исходящего трафика при прохождении его через брандмауэр

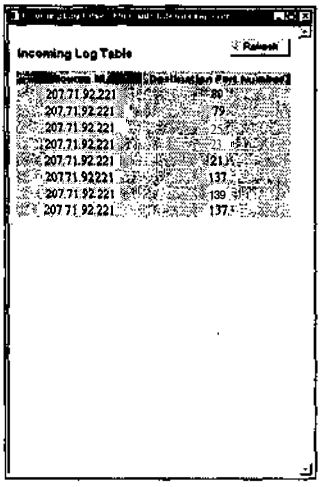


Рисунок 5.12. Визуальное отображение отчета о входящем Интернет-трафике

На рисунке 5.13 показан пример таблицы регистрации исходящего трафика. Как вы можете видеть, там перечислены IP-адреса локальных компьютеров, которые установили соединение с Интернетом, а также универсальные указатели информационного ресурса (URL) или удаленные компьютеры. Примеры URL включают www.microsoft.com и www.quepublishing.com. Если URL недоступен, на экране показывается IP-адрес удаленного компьютера или Web-сайта, который установил связь. В данном случае все указанные записи были HTTP-запросами к различным Web-серверам. Если компьютеры являются частью домашней сети, вы должны также видеть IP-адреса и Web-сайты, к которым получили доступ другие компьютеры.

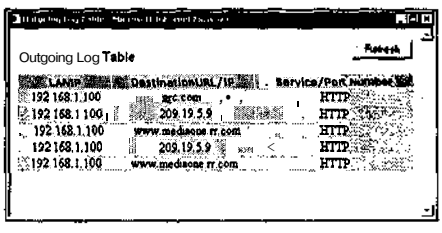


Рисунок 5.13. Изображение списка всех исходящих Интернет-соединений, установленных локальными компьютерами

Расположение справочных страниц

Помощь доступна на большинстве страниц конфигурирования маршрутизатора. Кроме того, вы можете нажать на страницу Help (Помощь), показанную на рисунке 5.14, чтобы найти ссылки на дополнительные ресурсы. В левой колонке находятся ссылки на страницы с информацией по каждой из страниц конфигурирования маршрутизатора. Справа находятся ссылки на дополнительные ре-

сурсы, находящиеся в Интернете, включая ссылку на Web-сайт Linksys и онлайн-копию руководства по маршрутизатору для пользователей.

Linksys предоставляет на своем Web-сайте обновления для встроенных программ маршрутизатора. Обновления бесплатны, но вы будете в них разочарованы, если не испытываете специфических проблем, которые имеют отношение к обновлению. Вы можете добавить обновление после его загрузки, нажав ссылку Upgrade Firmware (Обновление встроенной программы) на странице Help (Помощь). Тем самым вы откроете страницу Upgrade Firmware (Обновление встроенной программы), показанную на рисунке 5.15.

Введите пароль маршрутизатора в поле Password (Пароль), укажите расположение файла обновления в поле File Path (Путь к файлу), нажмите Upgrade (Обновить) и затем следуйте инструкциям по обновлению встроенной программы.

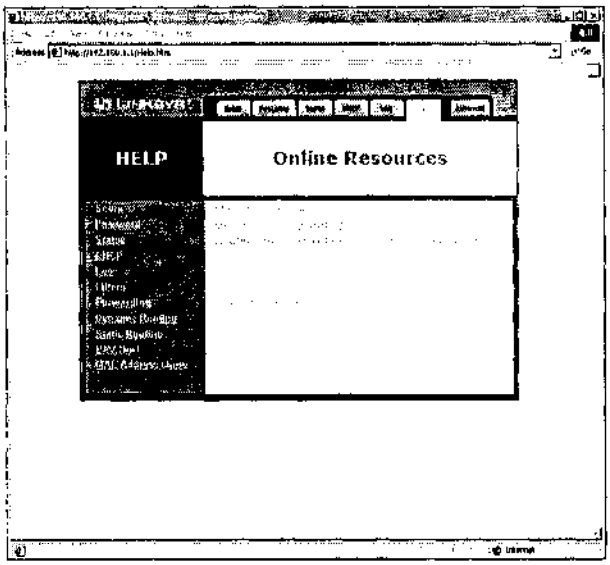


Рисунок 5.14. Получение дополнительной помощи

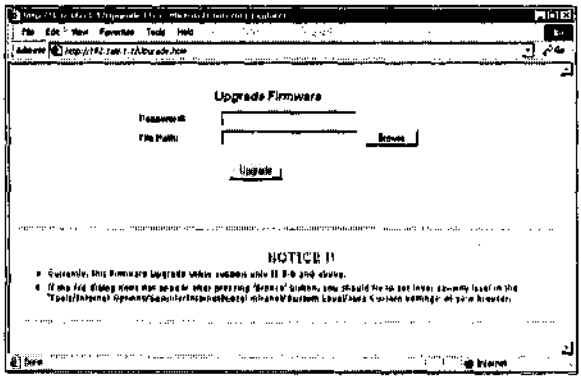


Рисунок 5.15. Обновление встроенной программы маршрутизатора BEFSR41

Другие функциональные возможности кабельно-цифрового маршрутизатора

Если вы нажмете закладку Advanced (Подробнее) после первого открытия страницы конфигурирования маршрутизатора BEFSR41, вы увидите новый набор страниц конфигурирования, как показано на рисунке 5.16. Большинство из этих страниц используются для конфигурирования расширенных свойств сети, которые не описываются в данной книге, за исключением страницы MAC Address Clone (Копирование MAC-адреса), которая была рассмотрена ранее в этой главе, и страницы фильтрации, которая показана на рисунке 5.16.

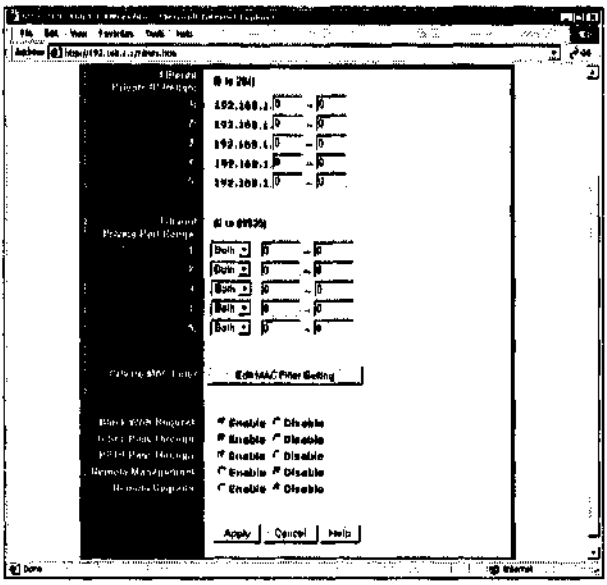


Рисунок 5.16. Страница фильтрации дает вам возможность сконфигурировать ряд опций брандмауэра

Раздел Filtered Private IP Range (Диапазон отфильтрованных частных IP-адресов) дает вам возможность указать до пяти диапазонов IP-адресов, которые должны блокироваться от доступа в Интернет. Очевидно, эта опция применяется только тогда, когда у вас есть домашняя сеть и более чем одному компьютеру позволено пользоваться вашим высокоскоростным доступом в Интернет. Чтобы заблокировать отдельный адрес, напечатайте последнюю часть присвоенного ему IP-адреса в обеих колонках. Чтобы заблокировать ряд IP-адресов, напечатайте последнюю часть первого IP-адреса в диапазоне в первой колонке и последнюю часть последнего IP-адреса в диапазоне в последней колонке. Используя свойство блокировки, вы можете, например, запретить определенным компьютерам доступ в Интернет. Таким образом, если у вас есть домашняя сеть, но вы хотите запретить компьютерам детей доступ в Интернет, вы можете сде-

лать это. Детям придется использовать контролируемые компьютеры мамы и папы для путешествий по Интернету.

Для того чтобы заблокировать IP-адрес компьютера, вы должны присвоить ему статический IP-адрес.

Вы также можете заблокировать определенные порты, указывая до пяти диапазонов портов в разделе Filtered Private Port Range (Диапазон отфильтрованных частных портов). При указании порта укажите также, хотите ли вы заблокировать что-либо из следующего:

в TCP - блокируется указанный диапазон портов TCP;

• UDP - блокируется указанный диапазон портов UDP;

а Both (Оба) - блокируются как порты TCP, так и порты UDP в указанном диапазоне.

Например, клиенты FTP используют порты 20 и 21 при коммуникации с FTP-серверами в Интернете. Если вы хотите запретить любой FTP-трафик, выберите Оба и напечатайте 20 в первой колонке и 21 во второй колонке.

Вы можете даже фильтровать доступ в Интернет, используя MAC-адрес сетевых плат Ethernet вашего сетевого компьютера, нажав пункт меню Edit MAC Filter Setting (Редактирование MAC-фильтра). Тем самым вы откроете диалоговое окно MAC Access Control Table (Таблица контроля доступа к MAC-адресам), в котором вы можете указать до 50 отдельных MAC-адресов.

В дополнение к трем предыдущим вариантам фильтрации вы можете также включить или отключить следующее:

• Block WAN Request (Блокировка запроса глобальной сети) - эта опция блокирует на вашем компьютере программы, используемые для проверки доступности адресата путем передачи ему специального сигнала и ожидания ответа, и ставит ваши порты в режим невидимости, делая их таким образом невидимыми в Интернете. Эта опция брандмауэра включена по умолчанию;

■ IPSec Pass Through (Пропуск IPSec) - эта опция определяет, разрешен ли проход трафика IPSec через маршрутизатор. IPSec в этой книге не рассматривается;

• PPTP Pass Through (Пропуск PPTP) - эта опция определяет, разрешен ли проход трафика PPTP через маршрутизатор. PPTP в этой книге не рассматривается;

• Remote Management (Удаленное управление) - эта опция определяет, хотите ли вы позволить вашему маршрутизатору конфигурирование через Интернет. Она отключена по умолчанию;

• Remote Upgrade (Удаленное обновление) - эта опция определяет, хотите ли вы позволить вашему маршрутизатору обновлять встроенную программу через Интернет. По умолчанию эта опция отключена.

Использование кабельно-иифрового маршрутизатора Linksys BEFSR41 EtherFast в качестве персонального брандмауэра

Как вы видели в этой главе, только некоторые из свойств кабельно-цифровых маршрутизаторов могут рассматриваться как относящиеся к персональным брандмауэрам. Используя маршрутизатор BEFSR41 как пример, в таблице 5.1 перечисляются свойства персонального брандмауэра, предоставляемые кабельно-цифровыми маршрутизаторами.

Таблица 5.1. Определение местонахождения свойств аппаратного персонального брандмауэра.

Свойство персонального брандмауэра	Расположение
Базовая установка	Страница установки
Защита с помощью пароля	Страница пароля
Управление регистрационными записями	Страница регистрационных записей
Фильтрация IP-адресов	Расширенные настройки: страница фильтрации
Фильтрация портов	Расширенные настройки: страница фильтрации
Фильтрация MAC-адресов	Расширенные настройки: страница фильтрации
Блокировка запросов соединений глобальной сети	Расширенные настройки: страница фильтрации
Копирование MAC-адреса вашего компьютера	Расширенные настройки: страница копирования MAC-адреса

Чтобы максимально повысить уровень защиты, вы, возможно, захотите рассмотреть установку как персонального программного брандмауэра, так и персонального аппаратного брандмауэра. Оба брандмауэра будут работать независимо друг от друга и вместе предоставят вам максимально возможную защиту. В главах 6-8 вы узнаете все, что вам необходимо знать, чтобы выбрать и установить программный персональный брандмауэр.

Другие кабельно-цифровые маршрутизаторы

На рынке существует ряд конкурирующих продуктов, которые предоставляют услуги, сходные с теми, которые предоставляет кабельно-цифровой маршрутизатор Linksys BEFSR41. Эти устройства обычно описываются как кабельно-цифровые маршрутизаторы или шлюзы и поддерживают один или больше портов соединения. В таблице 5.2 приведен список некоторых из этих конкурирующих продуктов.

Таблица 5.2. Продукты, которые работают как аппаратные брандмауэры.

Производитель	Номер модели	Web-сайт	Описание
Linksys	BEFSR11	www.linksys.com	Кабельно-цифровой маршрутизатор с 1 портом
Netgear	RT311	www.netgear.com	Кабельно-цифровой маршрутизатор с 1 портом
Netgear	FR314	www.netgear.com	Кабельно-цифровой маршрутизатор с 4 портами
D-Link	DI-704	www.dlink.com	Кабельно-цифровой маршрутизатор с 4 портами

Если у вас уже есть домашняя сеть с концентратором Ethernet, вы можете соединить ее с однопортовым кабельно-цифровым маршрутизатором, чтобы позволить всем компьютерам вашей сети пользоваться вашим высокоскоростным соединением с Интернетом.

6

Персональный брандмауэр McAfee

Эта глава является одной из трех глав, посвященных описанию программных персональных брандмауэров. В этой главе описывается персональный брандмауэр McAfee компании "Network Associates". Описание включает инструкции по установке и конфигурированию этого персонального брандмауэра. Вы также узнаете о том, что McAfee оставляет за сценой при защите вашего компьютера.

В дополнение к обзору его основных свойств в этой главе также обращается внимание на некоторые из свойств, отсутствующих в этом персональном брандмауэре. Конечно, описание не будет полным без обзора возможностей брандмауэра по регистрации и созданию отчетов.

В этой главе вы:

- узнаете, как установить персональный брандмауэр McAfee;
- узнаете, как использовать мастер конфигурирования для установки служб безопасности;
- выясните, как вручную отрегулировать параметры настройки конфигурации;
- узнаете, как управлять Интернет-приложениями;
- узнаете, как читать отчеты лог-файлов.

Описание брандмауэра McAfee

Персональный брандмауэр McAfee предоставляется компанией "Network Associates", которая находится по адресу *www.nai.com.* Этот персональный брандмауэр начал выпускаться как ConSeal Private Desktop компании "Singal9 Solution", но был перекуплен компанией "McAfee" и назван персональным брандмауэром McAfee в январе 2000 года.

Персональный брандмауэр McAfee - это продукт, предназначенный для домашних пользователей. Он создан для фильтрации и блокировки Интернет-трафика, входящего и исходящего с вашего компьютера, основываясь на службах безопасности, которые вы установили. Этот брандмауэр был создан для нетехнических пользователей. Благодаря его мастеру конфигурирования, который запускается сразу после установки брандмауэра, вам придется лишь ответить на несколько простых вопросов, и мастер создаст службы безопасности для вас. Конечно, если вы предпочтете покопаться поглубже, вы можете просмотреть и вручную изменить конфигурацию служб безопасности, чтобы точно подстроить персональный брандмауэр под ваши требования.

Персональный брандмауэр McAfee - это одно из средств межсетевой защиты, предоставляемое компанией "McAfee". Другой персональный брандмауэр - это персональный брандмауэр McAfee.com. Хотя у них много общих свойств, между ними существует одно значительное различие. Персональный брандмауэр **McAfee.com** поставляется как Web-услуга через Интернет, в то время как персональный брандмауэр McAfee устанавливается и запускается как типовое приложение Windows.

Этот персональный брандмауэр управляет вашим сетевым трафиком двумя способами. Во-первых, он отслеживает весь сетевой трафик и блокирует или пропускает его, основываясь на службах безопасности, управляющих использованием сетевых протоколов. Эти службы безопасности представляют собой техническую сторону персонального брандмауэра McAfee. К счастью, строгий отбор служб происходит перед конфигурированием, так что вам, возможно, не придется вносить изменения в эти настройки.

Во-вторых, персональный брандмауэр может защищать ваш компьютер, пропуская или блокируя сетевой трафик на основе списка доверяемых и блокируемых приложений. Любому приложению в списке, отмеченному как доверяемое приложение, разрешается обмениваться информацией через брандмауэр. Любое приложение в списке, отмеченное как блокированное, не пропускается через брандмауэр. Каждый раз, когда приложение, которого нет в списке персонального брандмауэра McAfee, пытается передать информацию в Интернет, приложение временно блокируется, и появляется всплывающее диалоговое окно, спрашивающее, хотите ли вы разрешить приложению обмен информацией.

Персональный брандмауэр McAfee имеет ряд дополнительных свойств, включая:

- блокировку не доверяемых приложений;
- обнаружение программ "Троянский конь";
- регистрацию всей отслеженной активности;
- создание отчетов обо всех сайтах Интернета, которые были посещены;
- запрещение доступа к общим файлам и принтерам;
- идентификацию всех активных соединений пользователя.

Системные требования

На момент написания этой книги был доступен персональный брандмауэр McAfee версии 2.15. Его рабочие аппаратные требования включают:

- 32 Мб памяти;
- 6 Мб места на жестком диске;
- процессор 486 или выше;
- дисковод для компакт-дисков.

Кроме того, вам необходимо иметь коммутируемое, кабельное или цифровое соединение с Интернетом и одну из следующих операционных систем:

- Windows 95 (с WinSock 2);
- Windows 98;
- Windows Me;
- Windows NT 4;
- Windows 2000;
- Windows XP.

WinSock или Windows Sockets - это компонент TCP/IP в Windows, который поддерживает процесс обмена информацией между Интернет-приложениями. Персональный брандмауэр McAfee работает с WinSock посредством программного интерфейса, реализованного для второй версии WinSock Microsoft, WinSock 2. Windows 95 поставляется с WinSock 1. Чтобы использовать персональный брандмауэр McAfee на компьютере с Windows *95,* вам нужно загрузить и установить WinSock 2, который на момент написания этой книги был бесплатно доступен на *www.microsoft.com/windows95/downloads.*

Установка и настройка

Установка персонального брандмауэра McAfee - это простой пошаговый процесс. До того как вы начнете установку, закройте все активные программы, включая те, которые взаимодействуют с Интернетом. Вставьте компакт-диск с McAfee в ваш дисковод для компакт-дисков, и программа автоматического запуска с компакт-диска должна запуститься. Следующая методика описывает в общих чертах шаги, которые необходимо предпринять для выполнения процесса установки.

1. Компакт-диск с McAfee автоматически загрузится. Выберите Install Firewall (Установить брандмауэр).
2. Появится мастер настройки McAfee. Нажмите Next (Далее) для начала процесса установки.
3. Появится лицензионное соглашение McAfee. Прочитайте соглашение, показанное на рисунке 6.1, выберите "I accept the terms of the license agreement" ("Я принимаю условия лицензионного соглашения") и нажмите Next (Далее).
4. Появится диалоговое окно Setup Type (Тип установки), показанное на рисунке 6.2, и предложит вам выбрать между двумя следующими опциями:
   - **Complete (Полная)** - устанавливает все компоненты персонального брандмауэра;
   - **Custom (Выборочная)** - позволяет вам выбрать, какие компоненты устанавливать.

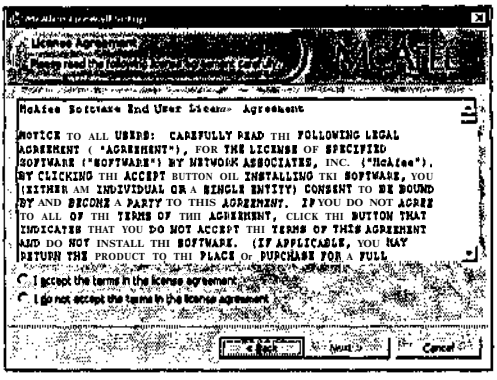


Рисунок 6.1. Вы должны принять условия лицензионного соглашения McAfee для того, чтобы продолжить установку вашего персонального брандмауэра

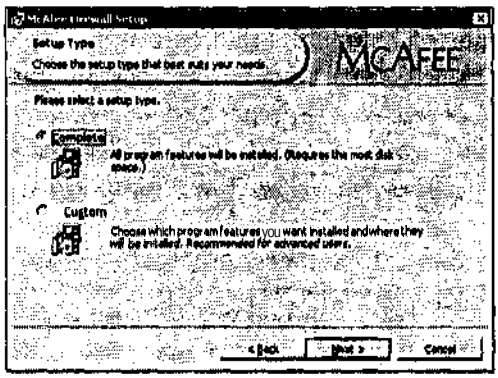


Рисунок 6,2. Вы можете выбрать между полной и частичной установкой

Выберите Complete (Полная) и нажмите Next (Далее).

5. Появится диалоговое окно Post Installation Options (Опции, настраиваемые после установки), показанное на рисунке 6.3, в котором вас спросят, хотите ли вы просмотреть файл McAfee README.TXT после завершения процесса установки. Опция Open README.TXT file (Открыть файл README.TXT) выбрана по умолчанию. Оставьте эту опцию активной и нажмите Next (Далее).

6. Процесс установки продолжится. Графическая строка текущего состояния покажет продвижение процесса установки персонального брандмауэра. Появится всплывающее диалоговое окно, показанное на рисунке 6.4, спрашивающее, хотите ли вы запускать ваш персональный брандмауэр автоматически при загрузке Windows. Нажмите Yes (Да).

7. Затем запустится приложение Windows Notepad (Блокнот) и загрузится текст файла README.TXT. Прочтите файл и закройте Notepad.

8. Процесс установки завершен, появится диалоговое окно, предлагающее вам нажать Finish (Готово).

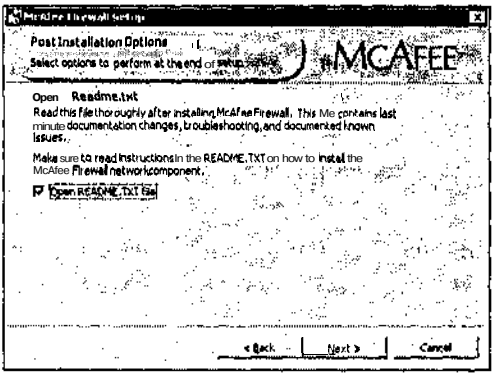


Рисунок 6.3. Хотя прочтение файла README.TXT необязательно, оно весьма рекомендуется

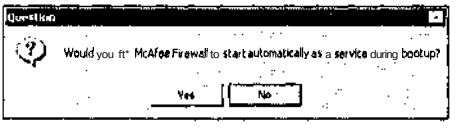


Рисунок 6.4. Установка автоматического запуска персонального брандмауэра McAfee позволяет ему загружаться раньше других приложений, защищая таким образом любое соединение, которое эти приложения могут попытаться предпринять

Теперь ваш персональный брандмауэр McAfee установлен. Однако он не готов к работе. Появится диалоговое окно McAfee Firewall Configuration (Конфигурирование брандмауэра McAfee). Это первое из нескольких диалоговых окон, которые проведут вас по процессу установки служб безопасности, которые управляют работой вашего персонального брандмауэра McAfee. Процесс конфигурирования описан в следующем разделе.

Работа с мастером конфигурирования

Персональный брандмауэр McAfee спроектирован так, что вам не нужно знать много об организации сетей, чтобы сконфигурировать ваши сетевые службы безопасности. Он выполняет эту задачу, задавая вам ряд вопросов, чтобы определить, что вы хотите сделать, и затем настраивает службы безопасности, основываясь на ваших ответах.

Вам предложат сконфигурировать персональный брандмауэр McAfee немедленно после его установки. Следующая методика кратко характеризует этапы этого процесса.

1. Появится диалоговое окно Configuration (Конфигурация) брандмауэра McAfee, показанное на рисунке 6.5.

   Вас попросят выбрать одну из трех настроек Network Control (Управление сетью), которые задают брандмауэру, как фильтровать Интернет-трафик. Эти опции включают:

- Block all traffic - no incoming or outgoing (Блокировать весь трафик - входящий и исходящий) - блокирует весь сетевой трафик при проходе через брандмауэр, эта опция действительно препятствует любому взаимодействию с Интернетом.
- Filter all traffic (Фильтровать весь трафик) - задает персональному брандмауэру McAfee фильтровать, основываясь на настройках его служб безопасности.
- Allow all traffic - all incoming and outgoing (Пропускать весь трафик - входящий и исходящий) - пропускает весь сетевой трафик через брандмауэр - в действительности понижает вашу защиту.

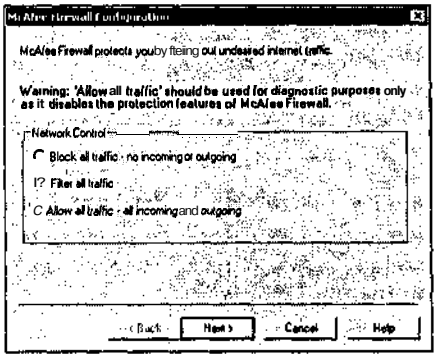


Рисунок 6.5. Три уровня управления сети определяют способ, с помошью которого персональный брандмауэр фильтрует трафик

Опция Filter all traffic (Фильтровать весь трафик) выбирается по умолчанию, и это единственная опция, которая предоставляет безопасное и удобное взаимодействие с Интернетом. Оставьте эту опцию выбранной и нажмите Next (Далее).

2. Затем вам предложат выбрать между двумя опциями, которые устанавливают форму регистрационной деятельности вашего персонального брандмауэра McAfee, как показано на рисунке 6.6.

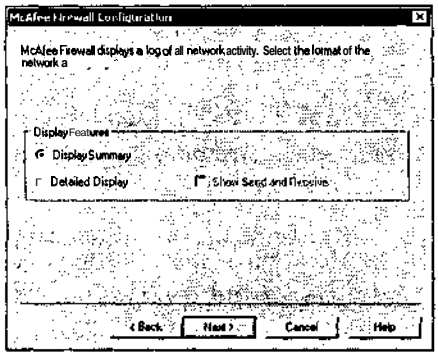


Рисунок 6.6. Определение способа регистрации сетевой активности персональным брандмауэром McAfee

Это следующие опции:

- Display Summary (Показать сводку) - предоставляет доступный уровень информации, предназначенной для чтения домашними пользователями.
- Detailed Display (Подробная информация) - предоставляет возможность подробной записи сетевой информации, имеет уровень сложности, предназначенный для продвинутых пользователей и сетевых администраторов.

По умолчанию выбирается опция Display Summary (Показать сводку). Если вы выбрали Detailed Display (Подробная информация), вам также предоставят возможность выбрать опцию Show Send and Receive (Получено и отправлено), которая регистрирует количество отправленных и полученных байт. Оставьте опцию выбранной по умолчанию и нажмите Next (Далее).

Опция Show Send and Receive (Получено и отправлено) создает дополнительную нагрузку для каждого сетевого пакета, проходящего через персональный брандмауэр, и может немного снизить производительность вашего компьютера. Если вам не нужно это свойство, его отключение может немного повысить производительность вашего компьютера.

3. Затем вам предложат выбрать способ запуска брандмауэра, как показано на рисунке 6.7.

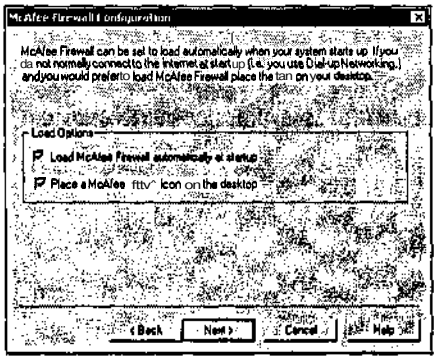


Рисунок 6.7. Вы можете сконфигурировать персональный брандмауэр загружаться при запуске системы или установить его на запуск вручную, поместив иконку на рабочий стол Windows

Доступны следующие опции:

- Load McAfee Firewall automatically at startup (загружать брандмауэр McAfee автоматически при запуске) - уберите выделение этой опции, если вы соединяетесь с Интернетом с помощью коммутируемого соединения и не хотите, чтобы ваш компьютер испытывал нагрузку от работы персонального брандмауэра, когда вы не находитесь в сети.

- Place a McAfee Firewall icon on the desktop (Поместить иконку брандмауэра McAfee на рабочем столе) - оставьте эту опцию выбранной, чтобы поместить иконку вашего персонального брандмауэра на рабочем столе Windows.

По умолчанию обе опции выбраны. Нажмите Next (Далее).

4. Затем появится диалоговое окно, показанное на рисунке 6.8. В нем вы можете указывать любые **приложения,** которым вы хотите позволить или запретить проходить через брандмауэр.

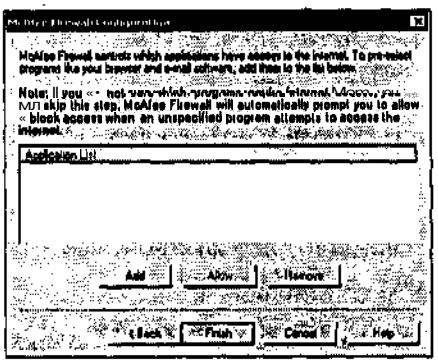


Рисунок 6.8. Вы можете задавать своему персональному брандмауэру любое количество Интернет-приложений и конфигурировать разрешение или блокировку их доступа в Интернет

5. Нажмите Add (Добавить). Появится диалоговое окно приложения Explorer, показанное на рисунке *6.9,* которое позволит вам локализовать и выбирать Интернет-приложения.

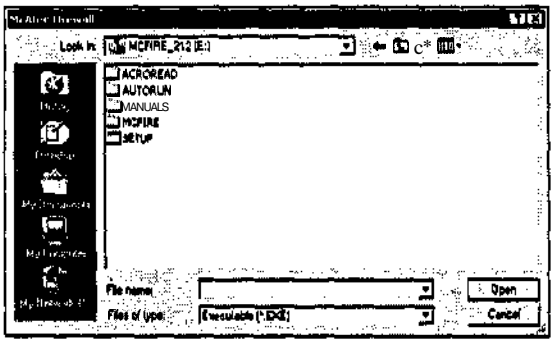


Рисунок **6.9.** Указание имени и пути к Интернет-приложению

6. Когда вы добавите приложение в список, рядом с ним появится маленькая иконка, указывающая, что приложению будет разрешено обмениваться данными через брандмауэр, как показано на рисунке **6.10.**

Рисунок 6.10. Маленькая зеленая иконка указывает на доверяемые приложения

7. Чтобы заблокировать приложение от обмена данными через брандмауэр, выберите его и нажмите Block (Заблокировать). Иконка слева от приложения изменится на красную, показанную на рисунке 6.11, иконку.

Рисунок 6.11. Красная иконка, указывающая на блокированные приложения

Когда блокируемое приложение выбрано, иконка Block (Блокировать) изменится на иконку Allow (Разрешить). Продолжайте добавлять приложения в список, пока вы не добавите все желаемые приложения. Не беспокойтесь о том, что пропустили какие-либо приложения, В первый раз, когда приложение, отсутствующее в этом списке, попытается связаться с Интернетом, брандмауэр перехватит его и спросит у вас, разрешить ли приложению соединиться. Затем брандмауэр добавит приложение в список, опираясь на ваш ответ.

Когда вы закончите добавлять приложения и конфигурировать их доступ, нажмите Finish (Готово). Вот и все, ваш брандмауэр теперь работает и отслеживает весь ваш Интернет-трафик.

Нормальное функционирование

После того как ваш персональный брандмауэр McAfee установлен и сконфигурирован, он разместится в панели задач Windows и будет незаметно работать, отслеживая весь ваш сетевой трафик и блокируя или разрешая обмен данными, основываясь на ваших настройках безопасности. Вы также можете найти его в меню Пуск, нажав Пуск, Программы, McAfee Firewall (Брандмауэр McAfee).

В зависимости от того, насколько хорошо вы задали ваш начальный список приложений, вы можете обнаружить, что время от времени персональный брандмауэр McAfee показывает всплывающее диалоговое окно, показанное на рисунке 6.12, указывающее, что он перехватил приложение, пытающееся соединиться с Интернетом. Диалоговое окно задаст вам вопрос, разрешить ли приложению сделать это.

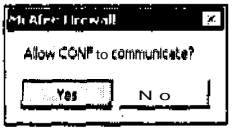


Рисунок 6.12. Персональный брандмауэр McAfee перехватил неопознанное приложение, пытающееся соединиться с Интернетом

Если вы хотите позволить приложению установить связь, нажмите Yes (Да). Нажмите No (Нет), чтобы блокировать приложение. Затем будет создана запись в списке приложений. В случае, показанном на рисунке 6.12, приложение, пытающееся соединиться, является программой Microsoft NetMeeting.

За исключением этих редких всплывающих диалоговых окон, ваш персональный брандмауэр будет работать незаметно для вас. Однако вы, возможно, захотите поработать с ним время от времени, чтобы отрегулировать его параметры безопасности и просмотреть регистрационные записи его деятельности. Вы можете начать работу с персональным брандмауэром, дважды нажав на иконку на рабочем столе или выбрав его из меню Пуск, а также с помощью двух следующих опций:

- двойное нажатие на иконку McAfee в панели задач - открывает главное диалоговое окно брандмауэра McAfee, в котором вы можете конфигурировать свойства брандмауэра и работать с ними.
- нажатие правой клавиши мыши на иконке McAfee в панели задач - предоставляет доступ с одного нажатия к набору наиболее часто используемых свойств брандмауэра.

Двойное нажатие на иконку McAfee в панели задач Windows открывает диалоговое окно брандмауэра McAfee, показанное на рисунке 6.13.

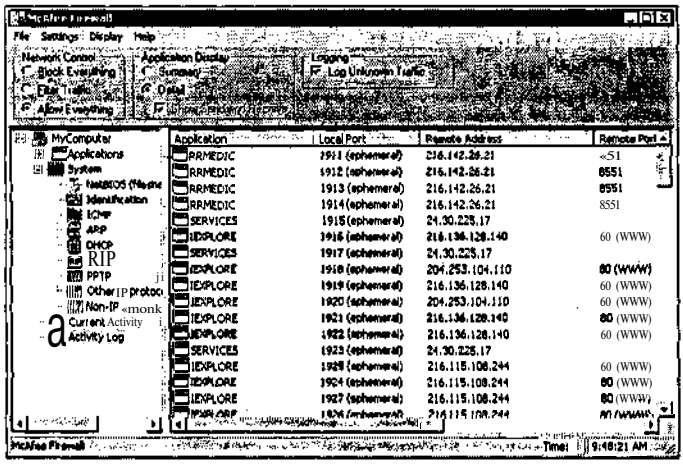


Рисунок 6.13. В диалоговом окне брандмауэра McAfee вы можете конфигурировать все опции брандмауэра и просматривать информацию последних регистрационных записей

В верхней части диалогового окна находятся меню брандмауэра McAfee и предоставлен доступ к параметрам конфигурирования Network (Сеть), Application (Приложение) и Logging (Регистрация). Остальная часть окна предоставляет доступ к древовидному обзору конфигурации брандмауэра. Слева на экране показаны параметры настройки приложений и сети и файлы регистрации деятельности брандмауэра. Вы можете выбрать любую запись в левой части ок-

на, чтобы просмотреть подробную информацию о ней в правой части. Например, при выделении строки Activity Log (Регистрация деятельности) в правой части окна показываются последние 100 зарегистрированных приложений.

Вы можете также работать с брандмауэром, нажав правой клавишей мыши на иконку McAfee в панели задач и выбрав любую из опций, которые появятся в контекстном меню, показанном на рисунке 6.14.

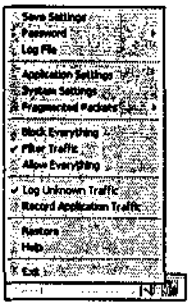


Рисунок 6.14. Персональный брандмауэр McAfee предоставляет ряд опций и окон, с которыми вы можете работать

В следующем разделе описываются опции, находящиеся в диалоговом окне брандмауэра McAfee и его контекстном меню на рабочем столе.

Сохранение изменений конфигурации

Опция Save Settings (Сохранить изменения) в меню File (Файл) позволяет вам сразу же сохранять любые изменения, которые вы внесли в конфигурацию персонального брандмауэра. По умолчанию изменения сохраняются только после того, как будет закрыт брандмауэр.

Зашита изменений конфигурации

Опция Password (Пароль) в меню File (Файл) позволяет вам устанавливать пароль конфигурации вашего персонального брандмауэра. Существуют четыре опции подменю:

- Enter (Ввод) - позволяет вам ввести пароль персонального брандмауэра и работать с его конфигурацией и лог-файлами.
- Purge (Очистка) - используется для выхода из персонального брандмауэра после внесения изменений в конфигурацию. Если вы не используете эту опцию, ваш брандмауэр останется включенным на оставшуюся часть сеанса связи.
- Set (Установка) - позволяет вам изменять пароль, присвоенный персональному брандмауэру McAfee.
- Required (Требуется) - позволяет вам применить пароль для защиты настроек вашего брандмауэра.

Когда вы выбираете опцию Требуется пароль для защиты настроек конфигурации вашего персонального брандмауэра, появляется диалоговое окно Set Password (Установка пароля), показанное на рисунке 6.15. Напечатайте пароль в полях Password (Пароль) и Confirm (Подтверждение) и нажмите OK.

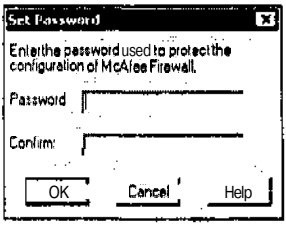


Рисунок 6.15. Зашита конфигурации брандмауэра с помощью пароля

При создании сложного пароля персонального брандмауэра используйте те же правила, которым вы следовали при создании ваших персональных паролей, Например, сделайте их длиннее восьми знаков, и включите комбинацию чисел, специальных знаков, заглавных и строчных букв, и не используйте распространенных терминов.

После того как добавлен пароль, он не разрешает изменять настройки персонального брандмауэра, пока не введен правильный пароль. Файл конфигурации брандмауэра McAfee называется CPD.SFR, он находится в той же папке, где и исходные файлы персонального брандмауэра McAfee, которая по умолчанию располагается в папке Program Files.

Если у вас установлена операционная система Windows NT 4, 2000 или XP, вы должны принять во внимание изменение разрешений папки McAfee, чтобы только доверенные люди имели доступ к ней и ее файлу конфигурации. Поскольку Windows 95, 98 и Me не способны защитить свои файлы и папки с помощью разрешений безопасности NTFS, этим пользователям остается лишь приложить старания и постоянно проверять свои файлы конфигурации, чтобы убедиться, что они не были изменены,

Работа с файлом регистрации персонального брандмауэра McAfee

Опция Log File (Файл регистрации) в пункте меню File (Файл) позволяет вам указать место, куда персональный брандмауэр будет записывать регистрируемую информацию, и указать максимальный размер файла регистрации. Она открывает диалоговое окно McAfee Firewall—Log File (Брандмауэр McAfee - Лог-файл), показанное на рисунке 6.16.

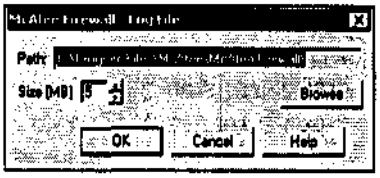


Рисунок 6.16. Конфигурирование расположения и размера лог-файла персонального брандмауэра

По умолчанию лог-файл располагается в той же папке, в которую были установлены исходные файлы брандмауэра McAfee, и его размер ограничивается до 5 Мб. Вы можете изменить любую из этих опций в этом диалоговом окне.

Запуск брандмауэра при начальной загрузке системы

Опция Start automatically when Windows Starts (Автоматический запуск при загрузке Windows) в меню File (Файл) позволяет вам включать и отключать автоматический запуск этого приложения. Когда она активна, появляется маленькая галочка слева от записи в меню.

Закрытие персонального брандмауэра McAfee

Вы можете использовать опцию Exit (Выход) в меню File (Файл), чтобы закрыть персональный брандмауэр McAfee. Закрытие вашего персонального брандмауэра в то время, когда вы все еще соединены с Интернетом, не рекомендуется, так как это оставляет ваш компьютер открытым для нападения. Нажмите Yes (Да), чтобы закрыть ваш брандмауэр, или No (Нет), чтобы оставить его в рабочем состоянии.

Конфигурирование настроек приложений

Опция Applications (Приложения) в меню Settings (Настройки) открывает диалоговое окно, в котором показывается окно свойств Applications (Приложения) брандмауэра McAfee, показанное на рисунке 6.17.

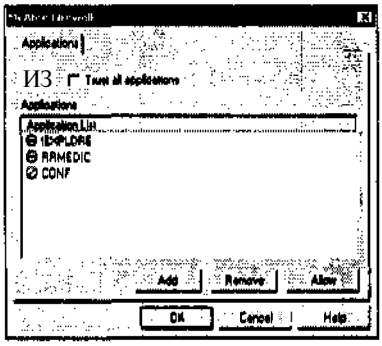


Рисунок 6.17. Изменение списка известных Интернет-приложений

Вы можете использовать это диалоговое окно, чтобы добавлять и удалять приложения из списка известных Интернет-приложений персонального брандмауэра. Чтобы добавить новое приложение в список, нажмите Add (Добавить), определите местоположение приложения и нажмите Open (Открыть). По умолчанию приложение становится доверяемым, что указывается с помощью зеленой иконки слева от записи. Вы можете пометить его как не доверяемое, выбрав его и нажав Block (Блокировать). Если вы случайно добавите неправильное приложение или захотите удалить приложение из списка, выберите его и нажмите Remove (Удалить).

Сверху этого окна свойств находится опция, помеченная как Trust all applications (Доверять всем приложениям). Когда она выбрана, эта опция игнорирует всю информацию о конфигурации приложений и разрешает всем приложениям соединяться с Интернетом. При обычных условиях эта опция никогда не должна быть установлена. Однако, если у вас возникли проблемы, вызванные неправильной работой приложения, вы можете попробовать включить эту опцию. Затем запустите свое приложение вновь, чтобы посмотреть, не мешает ли персональный брандмауэр каким-либо образом его выполнению. Когда завершите проверку, убедитесь, что отменили опцию Trust All Applications (Доверять всем приложениям), чтобы вернуть ваш брандмауэр в рабочее состояние.

Системные настройки

Опция System (Система) в меню Settings (Настройки) открывает диалоговое окно System Settings (Системные настройки), показанное на рисунке 6.18, которое выводит список сетевых устройств на вашем компьютере и позволяет вам выбрать и сконфигурировать, как персональный брандмауэр McAfee будет работать с каждым из них.

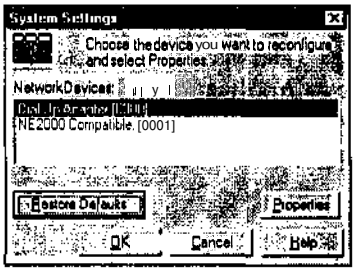


Рисунок 6.18. Обзор системных сетевых устройств

Каждое сетевое соединение обрабатывается отдельно. Таким образом, если у вас есть соединение с Интернетом и соединение с домашней сетью, вы можете применять различные настройки безопасности к каждому из них. Например, если у вас есть коммутируемое соединение с Интернетом и соединение с локальной сетью, вы увидите две записи в разделе Network Devices (Сетевые устройства), и каждое устройство будет иметь свою собственную отдельную конфигурацию.

Это позволяет вам применять более жесткие настройки безопасности к вашему соединению с Интернетом, чем к вашему соединению *с* домашней сетью. Для получения дополнительной информации о домашних сетях просмотрите главу 11 "Домашние сети и общее подключение к Интернету".

Чтобы восстановить исходные сетевые настройки вашего соединения с Интернетом, выберите соединение и нажмите Restore Defaults (Восстановить настройки по умолчанию). Чтобы изменить существующую настройку, выберите ее и затем нажмите Properties (Свойства). Сделав это, вы вызовете диалоговое окно Properties (Свойства).

Сетевые настройки применяются к протоколам TCP/IP, но не к отдельным приложениям. Персональный брандмауэр McAfee может фильтровать ряд настроек TCP/IP, каждая из которых расположена в окне этого диалогового окна, этот процесс описан в общих чертах в следующих разделах. Вы таюке можете сконфигурировать каждую настройку на создание отчетов обо всем разрешенном и заблокированном трафике, по схеме "настройка за настройкой".

NetBIOS через TCP

Окно NetBIOS over TCP (NetBIOS через TCP), показанное на рисунке 6.19, позволяет вам блокировать порты NetBIOS 137-139, которые используются для соединения с общими ресурсами другого компьютера и общими ресурсами на вашем компьютере. Оставив опцию Allow other systems to reach my shares (Разрешить другим системам получать доступ к моим общим ресурсам) чистой, вы можете блокировать любые попытки доступа из Интернета через эти порты NetBIOS. Опция Allow me to reach other systems' shares (Разрешить мне доступ к общим ресурсам других систем) используется для того, чтобы позволить вам соединяться с общими ресурсами других компьютеров.

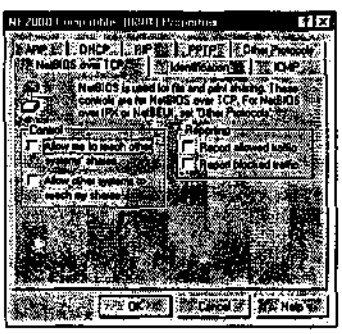


Рисунок 6.19. Конфигурирование работы персонального брандмауэра с NetBIOS через трафик TCP/IP

Если вы конфигурируете соединение локальной сети, вы, возможно, захотите включить эти опции для того, чтобы вы могли делить ваши дисководы и принтеры с другими пользователями локальной сети, а таюке получать доступ к их общим ресурсам.

Если вы конфигурируете ваше соединение с Интернетом, вы должны оставить эти опции неотмеченными, чтобы запретить посторонним лицам доступ на ваши дисководы. Однако, если вы уже совместно используете свои дисководы через Интернет с другими пользователями или получаете доступ к общим ресурсам других людей - и вы хотите продолжать делать это - вам придется оставить эти опции активными. Но делайте это с большой осторожностью. Вы оставляете дыру в безопасности, которую хакер может попытаться использовать для получения доступа к вашим накопителям на дисках. Если вы все равно хотите совместно пользоваться ресурсами через Интернет, убедитесь, что вы подобрали сложные пароли и отключаете ваше соединение с Интернетом каждый раз, когда не используете его долгое время.

Идентификация

Опция Allow Identification (Разрешить идентификацию) в окне свойств Identification (Идентификация), показанном на рисунке 6.20, выбрана по умолчанию и разрешает приложениям подтверждать свою идентичность. Это иногда требуют системы электронной почты и приложения, которые использует Internet Replay Chat (IRC)*. Чтобы повысить вашу конфиденциальность, вы, возможно, захотите отключить эту опцию, в таком случае посмотрите, повлияет ли это на какие-либо из ваших приложений. Если да, вы всегда можете вновь включить ее.

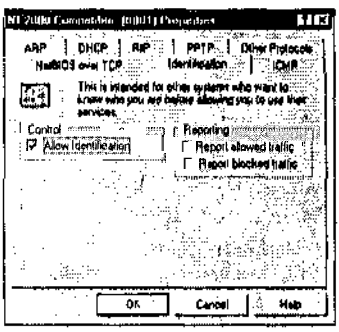


Рисунок 6.20. Установка настройки Allow Identification (Разрешить идентификацию) требуется некоторыми Интернет-системами электронной почты

IRC - это Интернет-служба, которая позволяет двум людям в Интернете общаться с помощью текстовых сообщений, посылаемых друг другу.

ICMP

Окно свойств Internet Control Message Protocol (ICMP) (Протокол управляющих сообщений в Интернете), показано на рисунке 6.21. ICMP - это технический протокол, используемый командой TCP/IP PING для проверки способности достичь удаленного компьютера. К сожалению, он иногда использовался хаке-

* Авторская опечатка: Internet Relay Chat

рами для того, чтобы обмануть сетевое соединение компьютера и обманом вовлечь компьютер во взаимодействие с компьютером, который имитирует другой компьютер.

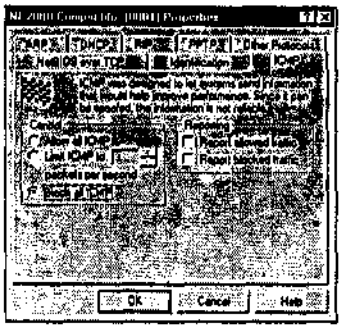


Рисунок 6.21. ICMP - это протокол, который хакеры могут использовать для обмана или мистификации вашего компьютера таким образом, что он думает, что общается с другим компьютером

Вы можете выбрать из опций Allow (Позволить), Block (Блокировать) или Limit (Ограничить) проход пакетов ICMP. Ограничивая число пакетов ICMP, вы сможете оставить проход протокола доступным, в то же время ограничивая способность хакера обмануть вас. По умолчанию выбрана опция Block all ICMP (Блокировать весь трафик ICMP),

ARP

Окно свойств Address Resolution Protocol (ARP) (Протокол разрешения адресов), показанное на рисунке 6.22, используется для того, чтобы помочь двум компьютерам, использующим TCP/IP, определять MAC-адреса друг друга. До настоящего времени никто не заявлял о хакере, использующем ARP, чтобы проникнуть в компьютерную систему. Поскольку он необходим для осуществления процесса коммуникации, опция пропуска протокола включена по умолчанию и должна оставаться включенной.

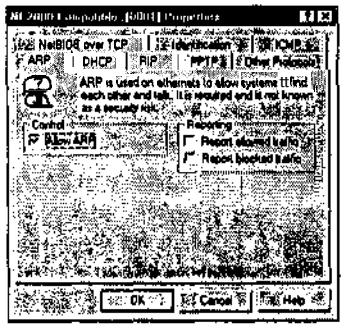


Рисунок 6.22. ARP - это протокол Ethernet, определяющий MAC-адреса

DHCP

Окно свойств Dynamic Host Configuration Protocol (DHCP) (Протокол динамической конфигурации компьютера), показанное на рисунке 6.23, используется провайдерами для выдачи своим клиентам IP-адресов во временное пользование, чтобы они могли соединиться с Интернетом. Вы должны включить эту настройку только для сетевых устройств, которые получают свои IP-адреса с помощью DHCP. Если ваш провайдер использует DHCP, чтобы присвоить вашему компьютеру IP-адрес, и вы блокируете эту опцию, ваше соединение с Интернетом не будет работать.

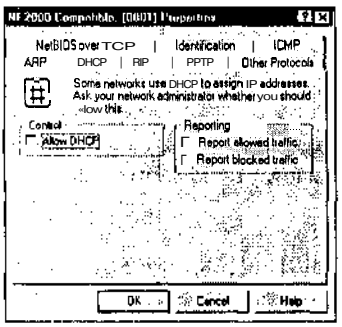


Рисунок 6.23. DHCP - это служба, используемая большинством провайдеров для динамического присвоения IP-адресов своим клиентам

RIP

Окно свойств RIP (Протокол маршрутной информации), показанное на рисунке 6.24, определяет, разрешить ли протоколу RIP, который используется некоторыми сетевыми устройствами для маршрутизации трафика TCP/IP по сети, проходить через брандмауэр. Если ваш провайдер не требует использования этого протокола, вы должны оставить его отключенным.

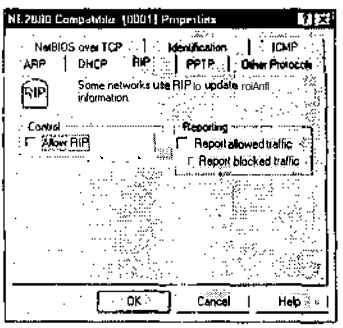


Рисунок 6.24. RIP - это протокол маршрутизации, используемый некоторыми сетями

PPTP

Окно свойств Point-to-Point Tunneling Protocol (PPTP) (туннельный протокол точка-точка), показанное на рисунке 6.25, устанавливает безопасное зашифрованное общение через Интернет между двумя компьютерами. Если вы не используете Интернет для соединения с корпоративными сетями с помощью PPTP, вы должны оставить эту установку отключенной.

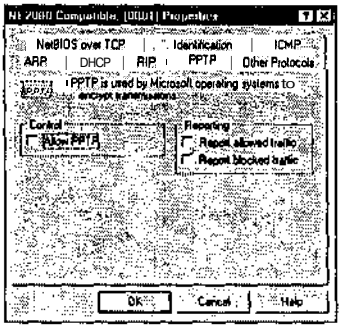


Рисунок 6.25. Туннельный протокол точка-точка устанавливает безопасное соединение между двумя компьютерами в Интернете

Другие протоколы

Персональный брандмауэр McAfee фильтрует основанные на TCP/IP протоколы и допускает или блокирует их общение, основываясь на ваших службах безопасности. Он также может блокировать другие протоколы, не относящиеся к TCP/IP, такие, как NetBEUI. Эти настройки конфигурируются в окне свойств Other Protocols (Другие протоколы), показанном на рисунке 6.26. Персональный брандмауэр McAfee не может фильтровать протоколы, не относящиеся к TCP/IP, и выполнять их детальный анализ. Он просто блокирует или пропускает весь трафик этих протоколов. Чтобы пропускать или блокировать данный протокол, выберите его из списка протоколов и отметьте одну из следующих опций:

- Allow (Разрешить) - пропускает выбранный протокол через брандмауэр.
- Block Incoming Fragments (Блокировать входящие фрагменты) - блокирует фрагментированные пакеты указанного протокола.
- Log Allowed Traffic (Регистрировать разрешенный трафик) - регистрирует все Интернет-коммуникации, которым разрешено проходить через брандмауэр.
- Log Blocked Traffic (Регистрировать блокированный трафик) - регистрирует все предпринятые попытки взаимодействия через Интернет, которые были блокированы брандмауэром.
- Allow Protocols Other Than IP, ARP, and RARP (Пропускать протоколы, отличные от IP, ARP и RARP) - позволяет другим протоколам TCP/IP проходить через брандмауэр.

- Log Non-IP Traffic (Регистрировать не относящийся к IP трафик) - регистрирует весь сетевой трафик протоколов, не относящихся к IP.

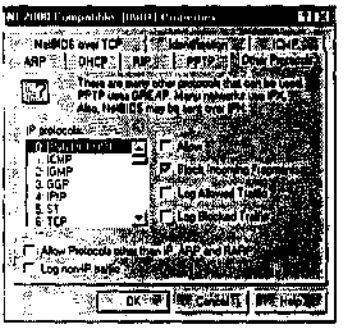


Рисунок 6.26. Персональный брандмауэр McAfee может также блокировать другие протоколы в дополнение к TPC/1P

Фрагментированные пакеты

Опция Fragmented Packets (Фрагментированные пакеты) в меню Settings (Настройки) позволяет вам включать и отключать блокировку входящих фрагментов и определять, регистрируются ли они. По умолчанию входящие фрагменты блокируются и не регистрируются.

Сворачивание в панель задач

Опция Minimize to SysTray (Сворачивание в панель задач) в меню Display (Экран) позволяет вам включать и отключать эту настройку. Когда она включена, она задает персональному брандмауэру McAfee сворачиваться в панель задач. Когда она отключена, брандмауэр сворачивается в панель задач Windows.

Запуск из системной строки

Опция Start in SysTray (Запуск из панели задач) в меню Display (Экран) позволяет вам включать и отключать эту настройку. Когда она включена, она указывает персональному брандмауэру McAfee запустить сворачивание в панель задач. Когда она отключена, брандмауэр показывает диалоговое окно McAfee во время своей работы.

Помощь

Опция Help menu (меню Помощь) открывает систему справочной информации персонального брандмауэра McAfee, как показано на рисунке 6.27.

Здесь вся документация, хранящаяся в Интернете, разделена на основные категории. Если вы нажмете клавишу Index (Указатель), вы увидите стандартные диалоговые окна помощи Microsoft с пунктами меню Index (Указатель) и Find (Найти), которые позволят вам осуществлять поиск по системе справочной информации, основываясь на ключевых словах.

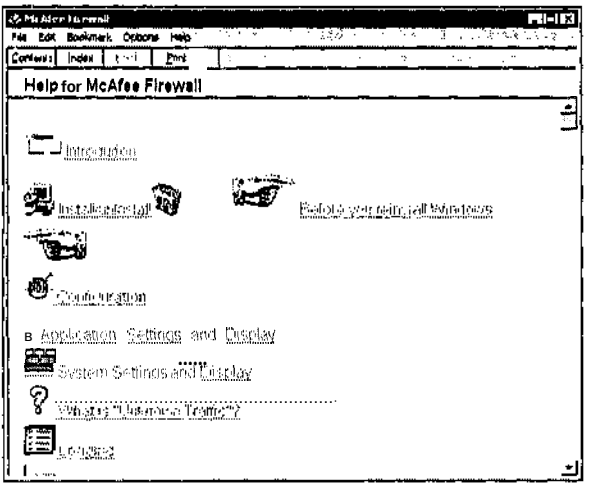


Рисунок 6.27. Подключение системы справочной информации персонального брандмауэра McAfee

Блокировать все

Опция Block Everything (Блокировать все) в разделе Network Control (Управление сетью) позволяет вам блокировать весь входящий и исходящий сетевой трафик. Она может использоваться, когда вы знаете, что не собираетесь подходить к компьютеру длительное время и нуждаетесь в дополнительной безопасности.

Фильтровать трафик

Опция Filter Traffic (Фильтровать трафик) в разделе Network Control (Управление сетью) позволяет вам настроить службы безопасности сети и приложений для того, чтобы вы могли путешествовать по Интернету, в то время как ваш компьютер и его ресурсы будут защищены.

Пропускать все

Опция Allow Everything (Пропускать все) в разделе Network Control (Управление сетью) отключает службы безопасности сети и приложений вашего брандмауэра и позволяет всему сетевому трафику проходить через ваш персональный брандмауэр. Если вы не пытаетесь определить, не мешает ли случайно ваш брандмауэр правильной работе приложения, вы никогда не должны включать эту опцию, поскольку это оставляет вас незащищенным.

Получение сжатой информации о приложениях

Опция Summary (Сводка) в разделе Application Display (Показать приложения) указывает, что персональный брандмауэр McAfee должен записывать в регистрационных файлах только основную суммарную информацию относительно деятельности приложения.

Получение подробной информации о приложениях

Опция Detail (Подробно) в разделе Application Display (Показать приложения) указывает, что в регистрационные файлы должна записываться подробная информация. Это, в частности, может быть полезно, когда вы пытаетесь отследить подозрительную активность.

Существует одна опция, расположенная в контекстном меню персонального брандмауэра McAfee, но не в диалоговом окне McAfee, это опция Record Application Traffic (Регистрация трафика приложений). Она включена по умолчанию и должна быть оставлена включенной. Без соответствующей регистрации вы не сможете получать записи о деятельности вашего персонального брандмауэра и, что *более* важно, о деятельности любых приложений, запущенных на вашем компьютере.

Работа с регистрационными записями

Персональный брандмауэр McAfee может регистрировать три типа информации в зависимости от того, как он был сконфигурирован:

- Application summary or detailed list (Сводка по приложениям или подробный список);
- Network traffic (Сетевой трафик);
- Unknown traffic (Неопознанный трафик).

Диалоговое окно брандмауэра McAfee предоставляет обзор регистрации активности. В окне Current Activity (Текущая деятельность) перечисляются данные о действующих в настоящее время приложениях, а Activity Log (Регистрация деятельности) выдает список последних 100 действовавших приложений. Ни одна из этих регистрационных записей не предоставляет доступ к сетевым событиям. Чтобы просмотреть все зарегистрированные персональным брандмауэром McAfee события, вы должны просмотреть лог-файл. По умолчанию лог-файл располагается в той же папке, что и исходные файлы персонального брандмауэра McAfee (обычно c:\Program Files\McAfee\McAfee Firewall). Лог-файлы имеют имена *yyyymm*, где *yyyy* - это год, а *mm* - месяц записи информации в лог-файл.

По умолчанию лог-файлу присваивается размер 5 Мб, но вы можете его изменить, нажав правой клавишей мыши на иконку персонального брандмауэра McAfee в системной строке Windows, выбрав опцию Log File (Лог-файл) и указав новый размер файла. Если лог-файл заполняется, регистрация приложений и неидентифицированных событий может быть приостановлена. Однако сетевые события будут продолжать записываться. Поэтому очень важно, чтобы вы просматривали лог-файлы и убеждались, что их размер должным образом скорректирован и приспособлен к записи всех ваших событий.

Чтобы дать вам представление о том, какого рода информацию вы увидите в лог-файле персонального брандмауэра McAfee, и помочь вам понять форму ее представления, здесь приводится выдержка из события лог-файла вместе с кратким описанием.

Следующее сообщение показывает, что персональный брандмауэр McAfee начал работу:

```
Starting McAfee Firewall 2.1 on 2001/06/27 4:33:22 PM
```

Оно говорит вам о том, когда ваш брандмауэр начал свою работу. Вы увидите это сообщение каждый раз, когда вы перезапускаете ваш компьютер или когда вы вручную закрыли и вновь открыли ваш брандмауэр. Затем вы увидите сообщение, показывающее расположение лог-файла брандмауэра:

```
C:\Program Files\McAfee\McAfee Firewall\\200106.log
```

Используйте информацию, представленную в этой записи, если вы хотите найти лог-файл для того, чтобы вы могли сделать его копию и в дальнейшем просмотреть. Следующие регистрационные записи указывают сетевые устройства, которые фильтрует брандмауэр:

```
Devices:
Dial-Up Adapter [0000]
NE2000 Compatible..[0001]
```

Главное, что вы должны ожидать, это то, что указываются все сетевые соединения. Следующие регистрационные записи показывают, что сетевые устройства активизированы. В этот раз каждое устройство перечислено с помощью числовой нумерации:

```
Attaching to devices:
0000
0001
```

Следующая запись показывает расположение служб безопасности вашего персонального брандмауэра McAfee:

```
Ruleset file: C:\Program Files\McAfee\McAfee Firewall\CPD.SFR
```

Некоторое число регистрационных записей будет затем показывать текущее состояние ряда настроек брандмауэра. Просмотрите эти регистрационные записи, чтобы убедиться, что установочные параметры брандмауэра настроены правильно. Например, следующая запись показывает, что была установлена сетевая настройка Filter Traffic (Фильтровать трафик):

```
Network Control: Filter
```

Следующая запись показывает, что каждый раз, когда приложение, которого нет в списке известных приложений, попытается соединиться с Интернетом, вы будете уведомлены об этом. Это позволит вам установить и блокировать программы "Троянский конь":

```
Prompt before allowing applications communicate
```

Следующая запись показывает, что вы выбрали запись сжатой информации о событиях на уровне приложений:

```
Summary display
```

Следующая регистрационная запись показывает, что была установлена настройка Log Unknown Traffic (Регистрация неидентифицированного трафика). Она регистрирует сетевой трафик коммуникаций, инициатором которого вы не были:

```
Log unknown traffic
```

Следующие две записи показывают текущие настройки работы с входящими фрагментами пакетов:

```
Incoming fragments will be blocked,
Blocked incoming fragments will not be logged,
```

Следующие регистрационные записи указывают все Интернет-приложения, которые были заданы персональному брандмауэру, и их статус доверяемых или заблокированных. Просмотрите этот список, чтобы убедиться, что вы правильно указали все приложения, которые хотите, чтобы ваш брандмауэр блокировал или пропускал:

```
Allowed Applications:
IEXPLORE
Blocked Applications:
(none)
```

Вы также увидите ряд регистрационных записей, которые показывают параметры настройки сети. Эта информация выдается как длинная таблица с колонками для каждого сетевого протокола. Информация по каждому контролируемому сетевому устройству представлена отдельно. Некоторая информация выводится о каждом устройстве, включая статус каждого протокола (allowed (разрешен) или blocked (блокирован)), а также регистрируются ли пропускаемые или блокируемые пакеты (выберите у (да) или n (нет)).

```
System Settings:
Device                        ARP     DHCP     Identification ICMP
RIP
   OtherIP  PPTP   NonIP     Shares      (Others)
Dial-Up Adapter [0000]       allowed  allowed   allowed   blocked
allowed
    allowed allowed allowed allowed      allowed
Log allowed packets           n      n        n              n
n       n
     n        n      n         n
Log blocked packets           n      n        n              n
n       n
     n        n      n         n
NE2000 Compatible..[0001]    allowed  blocked    allowed  blocked
blocked
   blocked blocked blocked blocked       blocked
Log allowed packets           n      n        n              n
n       n
     n        n      n         n
Log blocked packets           n      n        n              n
n       n
     n        n      n         n
```

Следующая регистрационная запись показывает имя компьютера:

```
MYCOMPUTER
```

Затем перечисляются IP-адреса, присваиваемые каждому сетевому устройству. В этом примере вы можете видеть два IP-адреса. Один IP-адрес присвоен провайдером соединению с Интернетом, а другой принадлежит соединению компьютера с домашней сетью.

```
Assigned IP addresses are:
24.168.255.207
169.254.254.247
```

Следующее сообщение показывает, что персональный брандмауэр McAfee выполнил свою начальную загрузку и теперь фильтрует сетевой трафик. Это говорит вам, что ваш брандмауэр начал защищать ваш компьютер.

```
----------McAfee Firewall is running----------
```

Через некоторое время вы можете внести изменения в настройки конфигурации вашего брандмауэра. Когда вы это сделаете, в лог-файле появятся записи, регистрирующие эти изменения. Например, следующая запись показывает, что уровень регистрации приложений был изменен со Сводки на Подробно.

```
Show Detail
```

Следующая запись показывает, что также была включена настройка Show Send and Receive (Отправлено и принято) в опции Detail logging (Подробная регистрация).

```
Show send and receive
```

При запуске Интернет-приложения в лог-файле регистрируется запись. Например, следующая запись показывает, что приложение Internet Explorer было сохранено на компьютере и что персональный брандмауэр McAfee был сконфигурирован позволять ему проходить через брандмауэр.

```
IEXPLORE running (it will be allowed)
```

Следующие две регистрационные записи представляют собой выборку некоторых записей из тех, которые вы можете увидеть зарегистрированными в вашем лог-файле. В данном случае эти записи показывают, что было установлено соединение *с www.mediaone.rr.com.* Формат этих записей разбивается на следующие данные:

- дата;
- время;
- имя приложения;
- номер используемого локального порта;
- IP-адрес удаленного компьютера;
- порт, используемый удаленным компьютером;

- служба, запущенная на удаленном компьютере;
- продолжительность сеанса связи;
- количество отправленных байт;
- количество полученных байт.

```
2001/06/28 4:40:09 PM: IEXPLORE port 1268 (ephemeral) - 24.30.203.14 port 80
(WWW), lasting 3 second(s), 229 bytes sent, 223 bytes received.
2001/06/28 4:40:15 PM: IEXPLORE port 1269 (ephemeral)- 24.30.203.14 port 80
(WWW), lasting 1 second(s), 288 bytes sent, 864 bytes received.
```

Следующая запись показывает, что приложение Internet Explorer было закрыто:

```
IEXPLORE has stopped
```

Следующая запись появляется, когда вы закрываете свой брандмауэр:

```
----------McAfee Firewall is stopping----------
```

Последняя запись показывает, что персональный брандмауэр McAfee больше не работает или не защищает ваше соединение с Интернетом:

```
Stopping McAfee Firewall on 2001/06/27 4:46:21 PM
```

Ограничения

В общем, персональный брандмауэр McAfee показал себя как надежный персональный брандмауэр. Он отслеживает сетевой трафик и может разрешать или блокировать доступ, основываясь на доверяемых приложениях и настройках сети. Однако существует несколько свойств, которых нет в этом персональном брандмауэре, но которые, однако, присутствуют в некоторых конкурирующих продуктах. Например, в его возможности не включено обнаружение вторжения. Если вы не приобретете привычку просматривать лог-файлы вашего брандмауэра, а большинство людей ее не имеют, вы не будете иметь представление о том, когда ваша система зондировалась сканерами портов.

Кроме того, у этого брандмауэра нет механизма разрешения или блокировки взаимодействия с определенными IP-адресами или диапазоном IP-адресов.

Если у вас есть домашняя сеть или вы планируете ее создать, вам необходимо найти другой персональный брандмауэр, поскольку современная версия персонального брандмауэра McAfee не поддерживает возможность общего доступа к соединению с Интернетом.

Тестирование персонального брандмауэра McAfee

После установки и конфигурирования вашего персонального брандмауэра McAfee вы должны протестировать его, чтобы убедиться, что он работает и защищает ваш компьютер, как и ожидалось.

Запустите Internet Explorer, Netscape Communicator или одно из других приложений, которое вы сконфигурировали как доверяемое, и посмотрите, можете

ли вы соединиться с Интернетом. Если эта проверка пройдена успешно, запустите приложение, которое было указано в списке как недоверяемое. Если все работает как нужно, приложение не сможет установить соединение и покажет сообщение об ошибке.

Если все идет хорошо, попробуйте запустить Интернет-приложение, которое вы не добавляли в список известных Интернет-приложений персонального брандмауэра McAfee. Вы должны увидеть всплывающее диалоговое окно, спрашивающее, хотите ли вы пропустить или блокировать приложение. Сделайте соответствующий выбор. Затем нажмите правой клавишей мыши на иконку McAfee в системной строке и выберите Application Settings (Настройка приложений) и убедитесь, что приложение было добавлено в список правильно.

Если все эти тесты на ваш взгляд работают правильно, самое время запустить Интернет-сканирование защищенности вашего компьютера и посмотреть, как хорошо он защищает ваш компьютер.

Чтобы узнать, как запустить бесплатное Интернет-сканирование вашего компьютера, просмотрите главу 9 "Насколько защищен ваш компьютер?". Кроме того, в приложении Б "Другие Web-сайты, которые проверят вашу безопасность" представлен ряд бесплатных Интернет-сайтов, которые вы можете использовать для дополнительной проверки вашей защищенности в Интернете.

7

BLACKICE DEFENDER

Это вторая из трех глав, посвященных описанию программных персональных брандмауэров. Эта глава посвящена брандмауэру BlacklCE Defender компании "Network ICE". Описание включает инструкцию по установке и конфигурированию персонального брандмауэра BlacklCE. Вы узнаете о том, что происходит внутри брандмауэра и чем он отличается от других брандмауэров, описанных в этой книге. В дополнение к обзору свойств брандмауэра BlacklCE в этой главе также отмечены некоторые области, в которых еще необходимы улучшения.

В этой главе вы:

- узнаете, как установить BlacklCE Defender;
- узнаете, как изменить его параметры конфигурации, установленные по умолчанию;
- узнаете, как собрать информацию о взломщиках;
- узнаете, как конфигурировать и работать с предупреждениями брандмауэра BlacklCE Defender.

Описание

Персональный брандмауэр BlacklCE Defender производится компанией "Network ICE", чей Web-сайт находится по адресу *www.networkice.com.* Этот персональный брандмауэр предназначен для домашних пользователей с коммутируемым, цифровым или кабельным модемным соединением.

Этот персональный брандмауэр работает отлично от других персональных брандмдауэров, описываемых в этой книге. Вместо блокировки определенных приложений и протоколов BlacklCE Defender использует механизм обнаружения и анализа, который исследует содержимое каждого входящего и исходящего пакета и выполняет структурный анализ для определения, несет ли он какую-либо угрозу компьютеру. Брандмауэр BlacklCE Defender пытается идентифицировать природу каждого нападения на ваш компьютер и может предоставить вам подробную информацию о типе атаки и о том, как он на нее ответил. Если брандмауэр определил, что компьютер подвергается нападению, он выполняет ряд действий, включая:

- остановку атаки с помощью блокировки IP-адреса хакера;
- выполнение отслеживания и создание файла события, содержащего всю возможную информацию о нападающем;
- уведомление вас об атаке с помощью графического и звукового предупреждения.

Брандмауэр BlacklCE Defender блокирует IP-адрес нападающего от доступа к вашему компьютеру на 24 часа. После этого блокировка снимается. Таким образом, доступ к настоящему Web-серверу не блокируется навсегда в результате попытки хакера имитировать сервер. Если, проанализировав событие, вы решили, что хотите навсегда блокировать IP-адрес, вы можете сделать это. Вы можете также указать IP-адреса доверяемых компьютеров. Если у вас есть домашняя сеть, использующая TCP/IP как свой протокол, вы можете настроить другие компьютеры в сети как доверяемые системы, позволяя сетевому трафику свободно проходить между компьютерами вашей домашней сети. После того как доверяемый компьютер определен, ему позволяется передавать данные через ваш брандмауэр без проверки пакетов данных. Используйте эту опцию с осторожностью.

Отслеживание - это попытка брандмауэра BlacklCE Defender проследить путь поступивших на ваш компьютер сетевых пакетов от их отправителей. Используя информацию об адресе, содержащуюся в пакетах данных, брандмауэр пытается отследить их путь до отправителя и получить так много информации о хакере, сколько возможно, включая его или ее:

- IP-адрес;
- MAC-адрес;
- имя компьютера.

Эта информация и все остальные данные, которые брандмауэр сможет собрать, затем записываются в файл события. К сожалению, файлы событий требуют специального приложения для чтения. Они также требуют большого опыта работы в сети, необходимого для того, чтобы понять их содержание. Файлы событий не предназначены для чтения домашними пользователями, лучше послать их вашему провайдеру при сообщении о деятельности хакера.

Брандмауэр BlacklCE Defender предоставляет детальный графический анализ сетевой активности в реальном времени, который может помочь вам измерить уровень сетевой активности, возникающей на различных интервалах.

В отличие от многих других персональных брандмауэров, персональный брандмауэр BlacklCE Defender устанавливается без запуска мастера конфигурирования, который задает вопросы о том, как он должен конфигурировать службы безопасности, Вместо этого автоматически по умолчанию устанавливается набор уровней безопасности. Конечно, вы можете в дальнейшем просматривать и изменять их в соответствии с вашими собственными требованиями безопасности.

Брандмауэр BlacklCE Defender имеет четыре настройки безопасности. Каждая настройка предоставляет различный уровень защиты:

- Paranoid (Параноидальный) - эта настройка брандмауэра блокирует весь незатребованный входящий трафик и может привести к проблемам при посещении Web-сайтов, предоставляющих интерактивное содержание. Эта настройка также может разрывать передаваемое в настоящий момент сообщение и аудио/видео.

- **Nervous (Боязливый)** - эта настройка блокирует весь незатребованный входящий трафик за исключением некоторого интерактивного содержимого. Она разрешает проходить через брандмауэр большей части потоковых аудио- и видеофайлов.
- **Cautious (Предупредительный)** - эта настройка блокирует незатребованный входящий трафик, который пытается соединиться со службами сети или операционной системы.
- **Trusting (Доверительный)** - эта настройка безопасности не блокирует никакой трафик и оставляет все порты TCP/IP открытыми и незащищенными.

BlackICE Defender состоит из двух частей:

- **Detection and analysis engine (Механизм обнаружения и анализа) -** фильтрует весь сетевой трафик и защищает компьютер от нападения.
- **Summary Application (Приложение отчетов о деятельности) -** предоставляет интерфейс для просмотра деятельности брандмауэра и сети и конфигурирования настроек брандмауэра.

Это приложение предоставляет доступ к сетевым событиям. Из него вы можете просмотреть информацию о:

- нападениях на ваш компьютер;
- общей сетевой активности;
- собранную информацию о хакерах;
- действиях брандмауэра BlackICE Defender.

Во время написания этой книги компания "Internet Security Systems" приобрела компанию "Network ICE". Хотя персональный брандмауэр BlackICE Defender уверенно лидирует на рынке домашних персональных брандмауэров, возможно, его название или домашний Web-сайт может измениться.

Системные требования

Во время написания этой книги самой последней версией брандмауэра BlackICE Defender была версия 2.1. Его рабочие аппаратные требования перечислены здесь:

- 16 Мб памяти;
- 10 Мб места на жестком диске;
- процессор Pentium;
- дисковод для компакт-дисков.

Установленный размер требуемой брандмауэром BlackICE памяти в размере 16 Мб подходит для Windows 95, 98 и NT Workstation. Однако, такие операционные системы, как Windows Me и Windows 2000 Professional имеют более высокие требования к памяти. Windows Me требует как минимум 32 Мб, в то время как Windows 2000 Professional требует 64 Мб. Чтобы запустить брандмауэр BlacklCE Defender в одной из этих операционных систем, ваш компьютер должен отвечать по крайней мере минимальным требованиям операционной системы к памяти.

Кроме того, вам необходимо коммутируемое, кабельное или цифровое соединение с Интернетом и одна из следующих операционных систем:

- Windows 95;
- Windows 98;
- Windows Me;
- Windows NT 4 с Service Pack (Служебный пакет программ) 4 или выше;
- Windows 2000 с Service Pack 4 или выше;
- Windows XP.

Установка и настройка

Первый шаг в подготовке к установке брандмауэра BlacklCE Defender - закрыть все активные программы, включая те, которые могут соединяться с Интернетом. Вставьте компакт-диск с брандмауэром BlacklCE Defender в дисковод. Через несколько минут активизируется программа автозапуска. Остальной процесс установки брандмауэра BlacklCE Defender кратко описан ниже:

1. Автоматически загрузится компакт-диск с брандмауэром BlacklCE Defender.
2. Программа установки брандмауэра BlacklCE заработает и начнет извлекать файлы, необходимые для процесса установки. Через некоторое время вы увидите мастера установки InstallShield Wizard брандмауэра BlacklCE. Нажмите Next (Далее).
3. Появится лицензионное соглашение BlacklCE. Вам придется согласиться с его условиями для того, чтобы установить брандмауэр. Прочитайте соглашение, а затем нажмите I АССЕРТ (Я ПРИНИМАЮ).
4. Затем вас попросят напечатать лицензионный номер брандмауэра BlacklCE Defender, который был вам предоставлен вместе с вашей копией программы, Напечатайте лицензионный номер точно, как он есть, включая использование заглавных букв, а затем нажмите Next (Далее).

5. Затем вам предложат подтвердить расположение папки, в которой будет установлен брандмауэр BlackICE Defender. По умолчанию она располагается по адресу: C:\Program Files\NetworkICE\BlackICE. Нажмите Browse (Обзор), чтобы указать другое место. Когда все будет готово, нажмите Next (Далее).

6. Затем вам предложат выбрать программную папку, в которой будут храниться иконки брандмауэра BlackICE Defender. По умолчанию это Network ICE. Вы также можете выбрать из нескольких альтернативных папок или ввести новое имя программной папки. После того как вы сделали выбор, нажмите Next (Далее).

7. Появится диалоговое окно, показывающее сводные данные обо всех настройках, которые вы указали. Убедитесь, что все выглядит правильно, а затем нажмите Next (Далее).

8. Процесс установки завершен. Появится диалоговое окно с опцией, спрашивающей, не хотите ли вы просмотреть файл README, поставляемый вместе с брандмауэром BlackICE Defender. Эта опция выбрана по умолчанию. Нажмите Finish (Готово).

9. Откроется окно приложения Notepad, в котором откроется файл README брандмауэра BlackICE Defender. Просмотрите его содержание, а затем закройте.

Теперь брандмауэр BlackICE Defender установлен и защищает ваш компьютер. Вы должны увидеть небольшую иконку BlackICE Defender на вашей панели задач Windows в нижнем правом углу экрана.

Кроме того, если вы нажмете Пуск, Программы и затем Network ICE, вы должны увидеть следующие компоненты:

- BlackICE Defender QuickStart Guide (мастер быстрого запуска брандмауэра BlackICE);
- BlackICE README (файл README);
- BlackICE Utility (утилита брандмауэра BlackICE);
- Install Adobe Acrobat Reader (установка Adobe Acrobat Reader).

Конфигурирование брандмауэра BlackICE Defender

Как упоминалось ранее в этой главе, брандмауэр BlackICE Defender не имеет мастера конфигурирования в отличие от многих других персональных брандмауэров. Вместо этого он устанавливает себя сам с набором параметров настройки безопасности, устанавливаемых по умолчанию. Вы можете просмотреть и изменить эти настройки в любое время.

Настройки брандмауэра BlackICE Defender можно просмотреть из диалогового окна Setting BlackICE (Настройка BlackICE), показанного на рисунке 7.1. Это

диалоговое окно состоит из ряда окон свойств, каждое из которых поддерживает конфигурацию определенного свойства персонального брандмауэра.

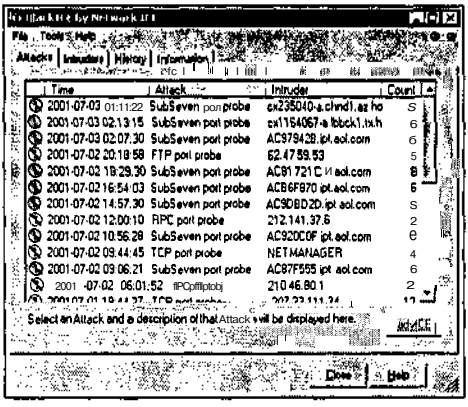


Рисунок 7.1. Настройки конфигурации брандмауэра изменяются с помощью окон свойств в диалоговом окне BlackICE by Network ICE

Вы можете открыть это диалоговое окно двумя способами. Первый - нажать Пуск, Программы, Network ICE и затем BlackICE Utility. Тем самым вы запустите интерфейс приложения для отчетов (Application Summary). Из него нажмите на опцию Edit BlackICE Setting (Редактировать настройки брандмауэра BlackICE) в меню Tools (Инструменты). Другой способ - нажать правой клавишей мыши на иконку BlackICE Defender в панели задач Windows и выбрать Edit BlackICE Setting (Редактировать настройки BlackICE) из появившегося ниспадающего меню, показанного на рисунке 7.2.

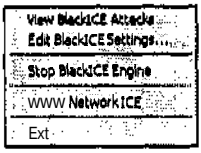


Рисунок 7.2. Вы можете получить доступ к любому свойству брандмауэра BlackICE Defender, нажав правой клавишей мыши на его иконке на панели задач

Настройки безопасности

Окно свойств Protection (Безопасность), показанное на рисунке 7.3, позволяет вам выбрать один из четырех уровней безопасности. Как описывалось более подробно ранее в этой главе, это уровни: Paranoid (Параноидальный), Nervous (Боязливый), Cautious (Предупредительный) и Trusting (Доверительный).

Уровень безопасности, устанавливаемый по умолчанию, - Боязливый.

Внизу окна свойств расположены три дополнительные опции. Это опции:

- **Enable Auto-Blocking (Включить автоблокировку) -** позволяет брандмауэру BlackICE Defender блокировать IP-адрес, с которого исходят серьезные угрозы.

- Allow Internet file sharing (Разрешить общий доступ к файлам из Интернета) - эта настройка позволяет вашему компьютеру делить свои папки и дисководы с другими людьми в домашней сети или в Интернете.
- Allow NetBIOS Neighborhood (Разрешить NetBIOS Neighborhood) - позволяет NetBIOS выдавать информацию о вашем компьютере другим компьютерам.

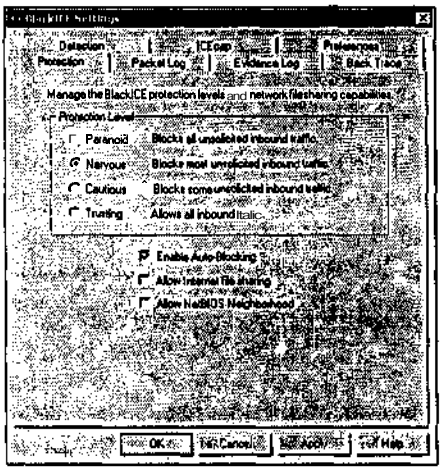


Рисунок 7.3. Выбор одного из уровней безопасности брандмауэра BlackICE Defender

По умолчанию последние две опции отключены. К сожалению, если вы оставите эти настройки в их состоянии по умолчанию, ваш компьютер не сможет делить свои ресурсы с другими компьютерами домашней сети. Еще хуже то, что если вы подключите эти опции, вы подвергнете ваш компьютер воздействию всего Интернета.

Решение этой проблемы - использовать протокол NetBEUI в качестве протокола вашей домашней локальной сети, как объясняется в главе 11 "Домашние сети и общее подключение к Интернету".

Настройка лог-файлов

Окно свойств Packet Log (Регистрация пакетов), показанное на рисунке 7.4, позволяет вам задавать брандмауэру способ управления регистрацией сетевого трафика. Когда опция разрешена, брандмауэр BlackICE Defender регистрирует весь сетевой трафик. Когда файл регистрации заполняется, открывается новый. Этот процесс повторяется до тех пор, пока не будет достигнуто максимальное количество лог-файлов, в этот момент брандмауэр начнет переписывать самый старый файл.

Вы можете сконфигурировать любую из следующих настроек:

- **Logging enabled (Разрешение регистрации)** - позволяет вам включать или отключать регистрацию в лог-файлах. По умолчанию настройка отключена.

- **File prefix (Префикс файла)** - позволяет вам указывать префиксное имя лог-файлов брандмауэра. Префикс по умолчанию - log. Например, когда эта опция выбрана, первому созданному файлу регистрации присваивается имя log000.enc.
- **Maximum size (Максимальный размер)** - указывает максимальный размер лог-файла. Когда достигается максимальный размер, создается новый файл регистрации. По умолчанию размер составляет 0 Кб.
- **Maximum number of files (Максимальное количество файлов) -** указывает максимальное количество лог-файлов, которые будут созданы до того, как брандмауэр начнет переписывать их заново. По умолчанию указывается значение 10.

Регистрационные файлы брандмауэра BlackICE Defender сохраняются как файлы анализатора пакетов (sniffer files) в том же виде, что и файлы событий. Эти файлы не читаются при просмотре в текстовых редакторах. Вместо этого вы должны использовать приложение, анализирующее пакеты (sniffer file application), чтобы проанализировать содержание лога. К сожалению, даже тогда вам будет необходим большой опыт сетевого администрирования, чтобы понять их.

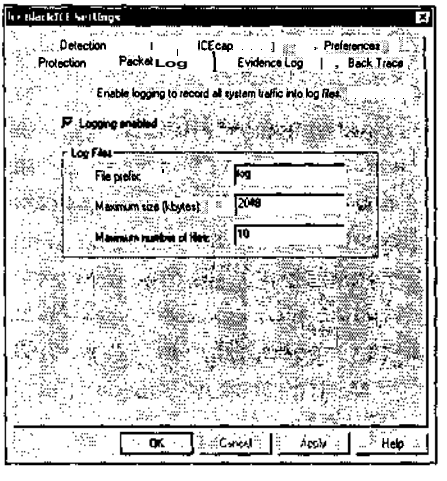


Рисунок 7.4. Вы можете конфигурировать ваш брандмауэр на хранение файлов регистрации и указывать их размер и количество

Настройка регистрации событий

Окно свойств Evidence Log (Регистрация событий), показанное на рисунке 7.5, позволяет вам задавать брандмауэру способ управления созданием файлов регистрации событий. Файлы регистрации событий создаются, когда брандмауэр BlackICE Defender определяет, что против вашего компьютера была запущена атака.

Когда опция включена, вы можете найти эти файлы в той же папке, в которой находятся исходные файлы брандмауэра BlackICE Defender, обычно это папка C:\Program Files\Network ICE\BlackICE. Эти файлы регистрации имеют расши-

рение .enc и могут быть прочитаны только с помощью приложения - анализатора пакетов (sniffer application).

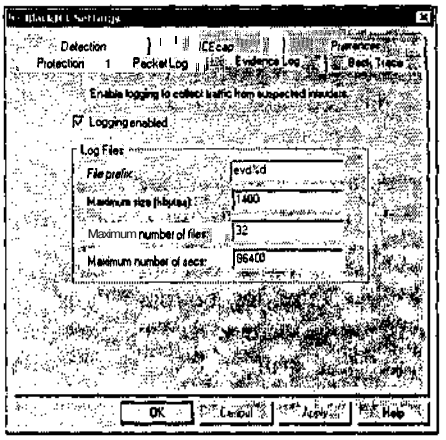


Рисунок 7.5. Брандмауэр может быть сконфигурирован на сбор подробной информаиии о хакерах, нападающих на ваш компьютер

Кроме защиты вашего компьютера или домашней сети одна из наиболее ДОу важных вещей, которую может делать персональный брандмауэр, - это предоставлять вам полезную информацию о регистрационной деятельности. Лог-файлы, регистрирующие пакеты и события, требуют специальных программ для их дешифровки и опыта в сетевом администрировании для того, чтобы понять их, Вы можете предоставить эти лог-файлы вашему провайдеру, когда будет зарегистрировано нападение, но они немногим могут помочь большинству пользователей. К счастью, как вы увидите далее в этой главе, брандмауэр BlackICE Defender предоставляет подробную информацию о регистрации в виде, который понятен для домашних пользователей, с помощью своего интерфейса программного отчета (Application Summary Interface),

Следующие параметры настройки могут быть сконфигурированы в окне свойств:

и **Logging enabled (Разрешить регистрацию)** - позволяет вам включать и отключать регистрацию в лог-файлах. По умолчанию настройка включена.

- **File prefix (Префикс файла)** - позволяет вам указывать префиксное имя файлов регистрации брандмауэра. По умолчанию присваивается префикс evd%d. EVD означает "для событий", а %d - переменное значение, которое подставляется из системной даты каждый раз, когда создается файл регистрации.

N **Maximum size (Максимальный размер)** - указывает максимальный размер файла регистрации. Когда достигается максимальный размер, создается новый лог-файл, а старый файл сохраняется. По умолчанию размер составляет 1440Кб.

- **Maximum number of files (Максимальное количество файлов)** - указывает максимальное количество файлов регистрации, которые будут созданы до того, как брандмауэр начнет переписывать лог-файлы заново. По умолчанию указывается значение 32.
- **Максимальное количество секунд (Maximum number of secs)** — время в секундах, в течение которого брандмауэр собирает сетевые данные при создании файла события. Эта настройка позволяет вам ограничивать размер места на диске, которое занимается одним файлом события.

Сбор информации о нападающих

Окно свойств Back Trace (Отслеживание пути), показанное на рисунке 7.6, позволяет вам задать брандмауэру способ сбора информации о хакерах, которые нападают на ваш компьютер. *Отслеживание пути* - это метод, используемый брандмауэром для отслеживания маршрута пакета данных до их исходного компьютера и сбор как можно более подробной информации о компьютере, который послал их.

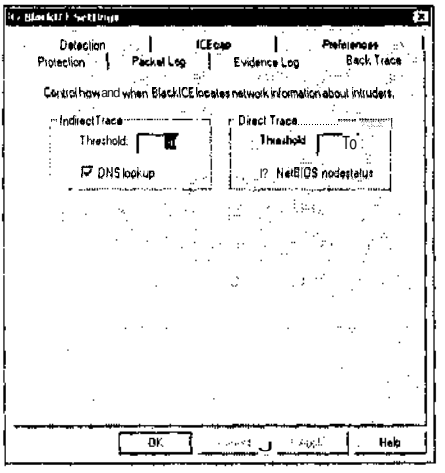


Рисунок 7,6. Указание брандмауэру BlackICE Defender способа, с помощью которого вы хотите собирать информацию об атаках хакера

Могут быть установлены два вида отслеживания пути:

- **Indirect (Непрямой)** - отслеживает путь пакетов данных в Интернете, но никогда не пытается прозондировать компьютер хакера. Этот вид отслеживания невидим для хакера.
- **Direct (Прямой)** - отслеживает путь пакетов данных в Интернете и собирает подробную информацию о хакере. Этот вид отслеживания может быть обнаружен хакером, если он или она установил(а) свой собственный брандмауэр, и может спровоцировать дальнейшие нападения.

Опция непрямого отслеживания включает подопцию, которая позволяет выполнять его в режиме поиска DNS (DNS lookup). Серверы DNS находятся в Интернете и больших сетях и могут иногда использоваться для поиска имени, присвоенного компьютеру. Прямое отслеживание имеет свою собственную подопцию. Когда включена опция NetBIOS node status (Статус узла NetBIOS), она указывает брандмауэру BlackICE Defender выполнять запрос NetBIOS о компьютере хакера.

Настройка Threshold (Предельная величина) определяет, когда начинать выполнение отслеживания пути. По умолчанию событие безопасности с уровнем 30 и выше запускает непрямое отслеживание. Подобным образом событие безопасности на уровне 50 запускает прямое отслеживание пути.

Брандмауэр BlackICE Defender автоматически присваивает уровень серьезности каждому нападению. Определены четыре основных категории событий, каждая из которых представляет различный диапазон угроз безопасности, как показано в таблице 7.1.

Таблица 7.1. Уровни событий безопасности брандмауэра BlackICE Defender.

Категория события	Серьезность	Описание
Critical (Критическое)	75-100	Нападение, созданное для причинения вреда вашему компьютеру или его содержимому
Serious (Серьезное)	50-74	Нападение, созданное для получения информации о вашем компьютере
Suspicious (Подозрительное)	25-49	Не несущая угрозы деятельность, такая, как сканирование портов, которая может указывать на возможную опасность в дальнейшем
Informational (Информационное)	0-24	Не несущее угрозы сетевое событие

Работа с определенными IP-адресами

Окно свойств Detection (Обнаружение), показанное на рисунке 7.7, позволяет вам указывать IP-адреса, которым брандмауэр должен доверять, или атаки, которые должны игнорироваться. Доверие IP-адресу позволяет всему трафику с этого IP-адреса проходить через брандмауэр непроверенным. Указание брандмауэру игнорировать определенные типы атак с определенного IP-адреса позволяют вам фильтровать сетевой трафик, помеченный брандмауэром как опасный, когда на самом деле он неопасен. Например, вы, возможно, захотите исключить сканирование любых портов вашим провайдером.

Каждый IP-адрес указывается на отдельной строке. Каждая запись показывает доверяемый IP-адрес, название доверяемой атаки и ID (идентификационный номер) этой атаки. ID атаки - это номер, присваиваемый каждому известному типу атаки брандмауэром BlackICE Defender.

Чтобы добавить новый IP-адрес в список, нажмите Add (Добавить), чтобы изменить существующую запись, нажмите Modify (Изменить). Чтобы удалить запись, нажмите Delete (Удалить) и Yes (Да), когда вас попросят подтвердить.

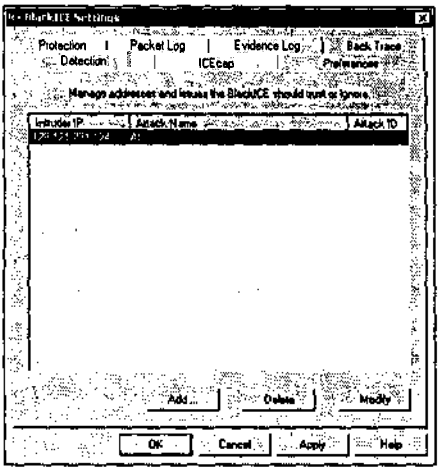


Рисунок 7.7. Указание IP-адресов, которые требуют особого обращения

Опции Add (Добавить) и Modify (Изменить) открывают диалоговое окно Exclude from Reporting (Исключить из отчетов), показанное на рисунке 7.8,

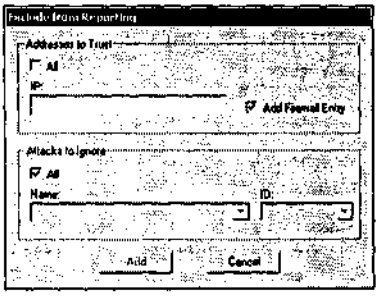


Рисунок 7.8. Добавление IP-адресов в список исключенных

В этом диалоговом окне представлены следующие опции:

- **Addresses to Trust (Доверяемые адреса)**
  - АН (Все) - выберите эту опцию, чтобы указать брандмауэру игнорировать атаку со всех IP-адресов.
  - IP - введите определенный доверяемый IP-адрес.
  - **Add Firewall Entry (Добавить запись брандмауэра)** - указывает брандмауэру позволять все соединения с определенных IP-адресов.
- **Attacks to Ignore (Игнорируемые атаки)**
  - All (Все) - выберите эту опцию, чтобы игнорировать все атаки с определенных IP-адресов.

- Name (Название) - ниспадающий список известных атак. Выберите одну, которая будет игнорироваться.
- ID - вместо указания атаки с помощью ниспадающего списка в поле Name (Название), вы указываете ее, выбрав ID, который BlackICE Defender присвоил атаке.

Окно свойств ICEcap

Окно свойств ICEcap, показанное на рисунке 7.9, отключено. ICEcap - это продукт компании "Network ICE", который создан для установки в корпоративных сетях и объединения информации, полученной от компьютеров, установивших брандмауэр BlackICE Defender, на одном сервере, где она может быть сопоставлена и проанализирована.

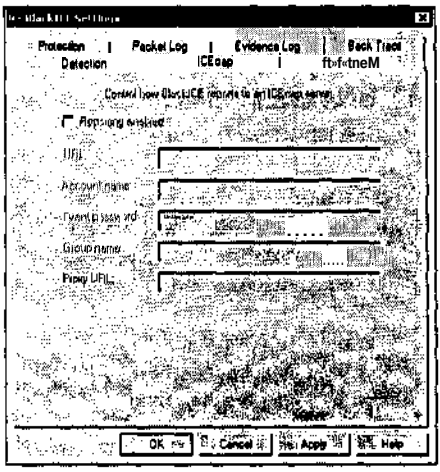


Рисунок 7.9. ICEcap - это продукт компании "Network ICE", созданный для объединения информации с брандмауэров, запушенных в корпоративных сетях

Установка параметров настройки интерфейса и предупреждений

Окно свойств Preference (Настройки), показанное на рисунке 7.10, конфигурирует настройки, управляющие тем, как брандмауэр уведомляет вас об аварийных ситуациях, как он проверяет свои обновления и как он показывает контекстные окна указателя.

Раздел Prompts (Подсказки) позволяет вам решить, будут ли появляться диалоговые окна подтверждения, когда вы будете вносить изменения в конфигурацию. Опция Show tooltips (Показывать всплывающие подсказки) включит показ всплывающих подсказок, когда запустится брандмауэр.

Раздел Update Notification (Уведомление об обновлении) позволяет вам указывать, будет ли брандмауэр BlackICE Defender проверять Web-сайт Network

ICE на предмет обновлений. Опция Interval for Checking (Интервал между проверками) позволяет вам указать, как часто будет осуществляться эта проверка.

Раздел Attack Notification (Предупреждение об атаке) позволяет вам указать, будут ли использоваться графические или звуковые предупреждения. Кроме того, вы можете указать уровни серьезности, требуемые для запуска предупреждения.

Варианты уровней:

- Critical (Критический);
- Critical and serious (Критический и серьезный);
- Critical, serious, and suspicious (Критический, серьезный и предупредительный).

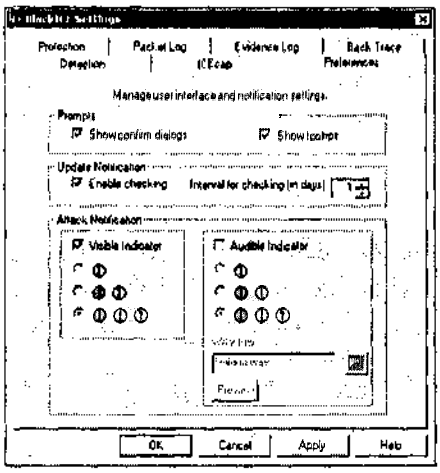


Рисунок 7.10. Конфигурирование опций предупреждения

Опция WAV file (Файл WAV) позволяет вам указать файл WAV, который будет проигрываться при запуске звукового предупреждения. Кнопка Preview (Прослушать) позволяет вам прослушать этот файл WAV.

Поддержание уровня зашиты брандмауэра BlackICE Defender на современном уровне

Время от времени компания "Network Ice" предоставляет обновления для брандмауэра BlackICE Defender. Эти обновления будут поддерживать ваш брандмауэр на современном уровне и позволят ему защищать ваш компьютер от большинства атак, которые были зарегистрированы в последнее время. Вы можете настроить ваш брандмауэр на автоматическую проверку доступных обновлений, а можете выполнять этот процесс вручную. Если вы не имеете привычки регулярно заниматься техническим обслуживанием вашего компьютера и его программного обеспечения, я рекомендую вам настроить все так, чтобы позволить брандмауэру BlackICE Defender позаботиться об этой работе за вас.

Автоматическое обновление вашего персонального брандмауэра

Вы можете сконфигурировать брандмауэр так, чтобы он просматривал Web-сайт Network ICE и сообщал, когда обновление будет доступно для загрузки, по следующей методике:

1. Нажмите правой клавишей мыши на иконку BlackICE Defender в системной строке Windows и выберите View BlacklCE Attacks (Просмотреть атаки BlacklCE).
2. Нажмите опцию Edit BlacklCE Settings (Редактировать параметры установки брандмауэра BlacklCE) в меню Tools (Инструменты).
3. Выберите окно свойств Preferences (Настройки).
4. Выберите опцию Enable checking (Включить проверку) в разделе Update Notification (Уведомление об обновлениях) и укажите, через сколько дней вы хотите проверять Web-сайт.

Интервал, который вы установили, чтобы задать брандмауэру BlacklCE Defender проверять обновления, автоматически сбросится после того, как вы перезагрузите компьютер. Поэтому, если вы не оставляете ваш компьютер включенным на всю ночь, вам придется помнить о проверке обновлений вашего брандмауэра вручную.

Брандмауэр BlacklCE Defender уведомляет вас, что обновление доступно, показывая иконку Ni в верхнем правом углу диалогового окна BlacklCE by Network ICE (Брандмауэр BlacklCE компании "Network ICE"), показанного на рисунке 7.11.

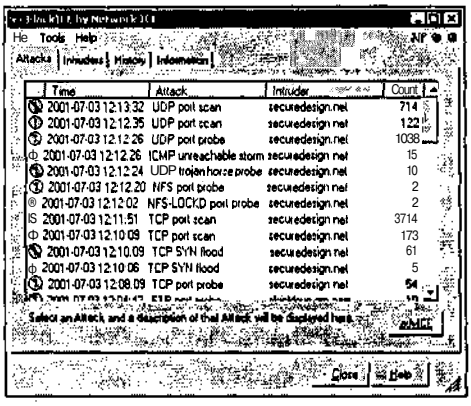


Рисунок 7.11. Имеется новое обновление для персонального брандмауэра BlacklCE Defender

Вы можете загрузить и применить обновление, нажав на иконку Ni. Ваш Интернет-браузер запустится и соединится с Web-сайтом Network ICE. Затем вам предложат сохранить файл обновления на диске или открыть его из текущего места.

Если вы нажмете на опцию загрузить и сохранить файл обновления на диске, вам придется запустить его после выполнения загрузки, чтобы обновить ваш брандмауэр. Если вы выберете опцию открыть файл обновления из текущего места, загрузится мастер конфигурирования брандмауэра BlackICE и покажет приветственное диалоговое окно дополнительной установки брандмауэра BlackICE Defender после того, как файл обновления загрузится.

Следующая методика описывает шаги, которые необходимо предпринять при обновлении вашего брандмауэра:

1. Приветственное диалоговое окно покажет сообщение, определяющее версию брандмауэра BlackICE Defender, установленного на вашем компьютере, как показано на рисунке 7.12. Нажмите Next (Далее), чтобы начать процесс обновления.

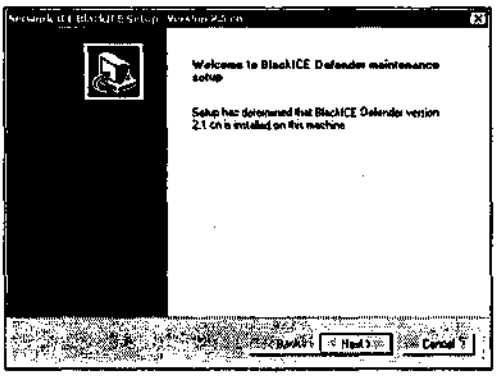


Рисунок 7.12. Приветственное диалоговое окно дополнительной установки брандмауэра BlackICE Defender

2. Затем вам предложат выполнить обновление, как показано на рисунке 7.13. Выберите опцию Upgrade (Обновить) и нажмите Next (Далее).

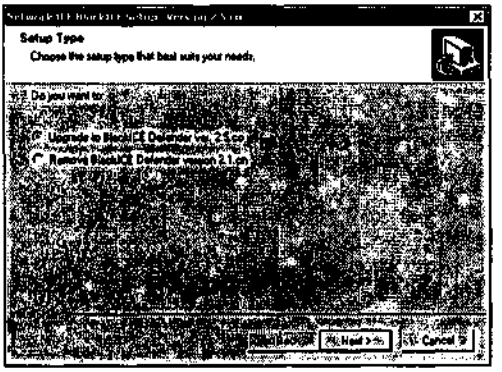


Рисунок 7.13. Выполнение обновления брандмауэра BlackICE Defender

3. Вас попросят подтвердить обновление. Нажмите Yes (Да).

4. Если появится лицензионное соглашение брандмауэра BlackICE Defender, нажмите I АССЕРТ (Я ПРИНИМАЮ).
5. Когда предложат, нажмите Finish (Готово).

Вот и все. Ваш персональный брандмауэр BlacklCE Defender теперь сильнее, чем когда-либо.

Обновление вашего персонального брандмауэра вручную

ЕСЛИ хотите, вы можете выполнить процесс обновления персонального брандмауэра BlacklCE Defender вручную. Если вы собираетесь делать все вручную, вам, вероятно, придется помнить о том, что обновления необходимо проверять каждые 2-3 недели. Методика проведения этого процесса в общих чертах такова:

1. Нажмите правой клавишей мыши на иконку BlacklCE Defender в системной строке Windows и выберите View BlacklCE Attacks (Просмотреть атаки BlacklCE),
2. Нажмите опцию Download Update (Загрузить обновления) в меню Tools (Инструменты).
3. Запустится ваш Интернет-браузер и соединится с Web-сайтом Network ICE. Если обновление доступно, вам предложат сохранить файл обновления на диске или открыть его из текущего места. С этого момента процесс установки будет происходить аналогично автоматическому обновлению.

Если у вас установлена самая последняя версия вашего брандмауэра, вы увидите Web-страницу, на которой будет указано, что у вас уже запущена наиболее современная версия брандмауэра BlacklCE Defender. Кроме того, вы увидите ваш лицензионный ключ и версию программного обеспечения вашего брандмауэра.

Нормальное функционирование

После того как ваш брандмауэр BlacklCE Defender установлен и сконфигурирован, он находится в панели задач Windows, незаметно отслеживая весь ваш сетевой трафик и блокируя или пропуская потоки информации, основываясь на установленных вами параметрах безопасности. Вы также можете запустить его через меню Пуск, выбрав Пуск, Программы и BlacklCE Defender.

Работа с файлами регистрации

После установки и соответствующего конфигурирования брандмауэра BlacklCE Defender вы готовы начать работу с вашим персональным брандмауэром. Самый легкий способ сделать это - нажать правой клавишей мыши на иконку BlacklCE Defender в панели задач Windows. На появившемся меню доступны следующие опции:

- View BlacklCE Attacks (Просмотр списка атак брандмауэра BlacklCE);

- Edit BlacklCE Settings (Редактирование параметров настройки брандмауэра BlacklCE);

и Advanced Firewall Settings (Расширенные настройки брандмауэра);

- Stop BlacklCE Engine (Остановка механизма BlacklCE);
- WWW Network ICE;

m Exit (Выход).

Каждая из этих опций описана в следующих разделах.

Просмотр списка атак брандмауэра BlacklCE

Программа отчетов о приложениях брандмауэра BlacklCE Defender (Application Summary program) предоставляет вам подробные информационные отчеты относительно активности сети и брандмауэра и представляет собой вид онлайнового лог-файла. Функционально программа отчетов о приложениях (Application Summary program) состоит из четырех окон свойств:

- Attacks (Атаки) - предоставляет информацию об атаках и другой подозрительной сетевой активности, нацеленной на ваш компьютер.
- Intruders (Взломщики) - предоставляет информацию, собранную о компьютерах, которые были инициаторами атак или подозрительной сетевой активности, нацеленных на ваш компьютер.
- History (История) - предоставляет графическое изображение сетевого трафика и деятельности хакеров на вашем компьютере.
- Information (Информация) - предоставляет информацию о лицензии и поддержке брандмауэра BlacklCE Defender.

Сверху диалогового окна расположено меню. Оно состоит из четырех подменю:

- File (Файл) - содержит опцию Exit (Выход), которая позволяет закрыть программу отчета о приложениях (Application Summary program).
- View (Вид) - содержит опции, которые позволяют вам фиксировать окно таким образом, чтобы вы могли сосредоточиться на определенном событии. Также позволяет вам фильтровать отображаемые данные, чтобы показать любое сочетание критических, серьезных, подозрительных и информационных событий.
- Tools (Сервис) - содержит опции для управления параметрами настройки брандмауэра, запуска и остановки механизма брандмауэра, очистки списка атак, выполнения обновления вручную и конфигурирования дополнительных параметров настройки брандмауэра.
- Help (Помощь) - предоставляет доступ к системе справочной информации брандмауэра BlacklCE Defender, поддержке онлайн и Web-сайту Network ICE.

В верхнем правом углу находятся две круглые иконки. Левая иконка представляет собой исходящий трафик, а иконка справа - входящий. Эти иконки мигают, когда поток данных проходит через брандмауэр. Постоянное горение показывает на непрерывный поток данных. Оба световых указателя имеют

световую кодировку, показывающую тип системной активности, проходящей через брандмауэр:

- Серая иконка - данные не передаются.
- Зеленая иконка - осуществляется нормальная передача данных.
- Желтая иконка - проходят подозрительные данные.
- Оранжевая иконка - были перехвачены данные, предназначенные для получения информации о вашем компьютере.
- Красная иконка - были перехвачены данные, предназначенные для причинения вреда вашему компьютеру.

В зависимости от уровня сетевого трафика вы можете найти, что работать с диалоговым окном проблематично, поскольку оно обновляется так быстро, что вам сложно сосредоточиться на определенном событии. Вы можете использовать опцию Freeze (Фиксировать), расположенную в меню View (Вид), чтобы временно приостановить обновление событий, Когда вы закончите, вы можете разблокировать показ, выбрав опцию Unfreeze (Разблокировать) в меню Tools (Инструменты).

Через некоторое время вы можете найти, что большие количество показываемых событий привело к тому, что с ними стало сложно работать. Вы можете нажать опцию Clear Attack List (Очистить список атак) в меню Tools (Инструменты), чтобы удалить события с экрана.

Анализ нападений на ваш компьютер

Вы можете просмотреть список всех зарегистрированных брандмауэром BlackICE Defender нападений на ваш компьютер в окне свойств Attacks (Атаки), показанном на рисунке 7,14,

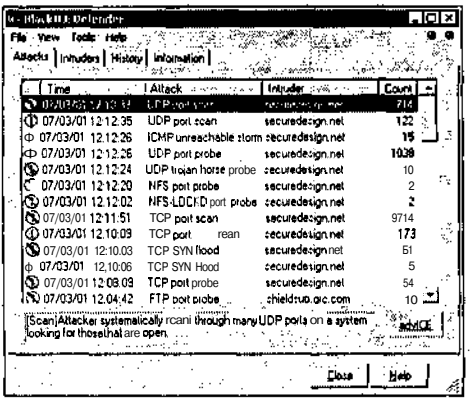


Рисунок 7.14. Окно свойств Attacks (Атаки) предоставляет подробный отчет обо всех недавних нападениях на ваш компьютер

Информация выводится в колонках, которые можно конфигурировать. По умолчанию информация сортируется по времени и по степени серьезности. Вы можете нажать на заголовок любой колонки, чтобы отсортировать по возрастанию. Нажмите на колонку повторно, чтобы отменить эту сортировку. По умолчанию показанные колонки данных включают:

- **Severity (Уровень серьезности)** - представление в виде иконки уровня серьезности события и ответ брандмауэра на событие.
- **Time (Время)** - дата и время, когда событие произошло.
- **Атака (Attack)** - тип атаки.
- **Intruder (Взломщик)** - **имя** (если возможно) или IP-адрес нападающего.
- **Count (Подсчет)** - показывает, сколько раз подряд происходила определенная атака.

В колонке Severity (Уровень серьезности) брандмауэр BlackICE Defender показывает иконку, представляющую собой его интерпретацию опасности, которую влечет за собой атака. В таблице 7.2 показаны эти иконки и их значения.

Таблица 7.2. Иконки уровня серьезности брандмауэра BlackICE Defender

Иконка	Цвет	Описание
	Красный	Критический
	Оранжевый	Серьезный
	Желтый	Подозрительный
	Зеленый	Информационный

Брандмауэр BlackICE Defender совмещает иконки уровня серьезности с иконками, показанными в таблице 7.3, при указании его отклика на атаку.

Таблица 7.3. Иконки отклика брандмауэра BlackICE Defender

Иконка	Статус атаки
	Блокирована
	Неуспешна
	Статус неизвестен
	Возможна
	Успешна

Вы можете предпринять четыре действия для любого события, нажав правой клавишей мыши на него. Это действия:

- **Ignore Attack (Игнорировать атаку)** - предоставляет две подопции, которые позволяют вам задавать брандмауэру игнорировать этот определенный тип атаки либо игнорировать эту атаку при запуске против взломщика, запустившего ее.
- **Block Intruder (Блокировать взломщика)** - указывает брандмауэру блокировать взломщика, который запустил атаку, на любой из следующих периодов времени: на час, на день, на месяц или навсегда.
- **Trust Intruder (Доверять взломщику)** - указывает брандмауэру добавить взломщика, который был инициатором события, в список разрешения или блокировки всего сетевого трафика с IP-адреса взломщика или игнорирования всех атак с этого IP-адреса.
- **Clear Attack List (Очистить список атак)** - позволяет вам очищать все события с экрана в случае, если с ними стало слишком сложно работать.

Кроме просмотра информации об атаке, вы также можете просмотреть информацию о взломщике, который запустил атаку, дважды нажав на любую атаку. Это приведет к переключению в окно свойств Intruder (Взломщик), в котором находится информация о хакере, который был инициатором события.

Вы можете добавлять или удалять колонки из окна свойств Attacker (Взломщик), нажав правой клавишей мыши на заголовок любой колонки и выбрав Columns (Колонки). Появится диалоговое окно Columns (Колонки). Чтобы удалить колонку с экрана, уберите ее выделение. Чтобы добавить колонку, выберите любую из колонок из списка.

Брандмауэр BlackICE Defender показывает краткое описание любой выбранной атаки внизу окна свойств. Вы можете найти более подробную информацию о любой атаке, выбрав ее и нажав advICE. Когда вы нажмете эту кнопку, она запустит ваш браузер и загрузит Web-страницу сайта Network ICE с подробной информацией об атаке и советами о том, что вы можете сделать.

Изучение информации о взломщике

Окно свойств Intruder (Взломщик) позволит вам просмотреть подробную информацию, собранную о компьютерах, находящихся в Интернете, которые были инициаторами событий на вашем компьютере, как показано на рисунке 7.15.

По умолчанию вся информация в этом окне свойств сортируется по имени взломщика, а затем по уровню серьезности. Вы можете нажать на любой заголовок один раз, чтобы отсортировать по нему, и дважды, чтобы вернуть прежний порядок сортировки. Кроме того, вы можете нажать правой клавишей мыши на заголовок любой колонки и выбрать опцию Columns (Колонки), чтобы добавить или удалить колонки из окна свойств.

Когда вы выделите запись о взломщике, вся информация, собранная об этом взломщике, будет показана в правой панели. Эта информация включает IP-адрес взломщика, имя NetBIOS, имя DNS и MAC-адрес.

Вы можете нажать правой клавишей мыши на взломщика в левой панели и ыбрать, блокировать ли взломщика или пропустить, с помощью тех же опций, представленных в окне свойств Attackers (Взломщики).

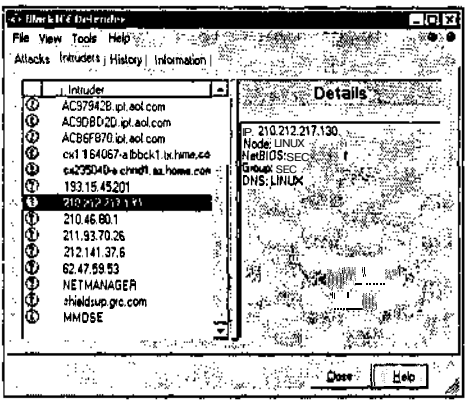


Рисунок 7.15. Отображение информации о взломщиках вашего компьютера

Изучение сетевой деятельности и активности хакеров

Окно свойств History (История) предоставляет вам отображение атак и сетевой активности, как показано на рисунке 7.16. Таким образом, вы можете просмотреть атаки и найти примеры произошедших нападений. Вы можете получить подробную информацию о любой атаке, нажав на точку атаки или нажав на график сетевого трафика. Это приведет к тому, что брандмауэр BlackICE Defender перейдет к окну свойств Attacks (Атаки) и покажет атаки, которые произошли во время, выбранное вами.

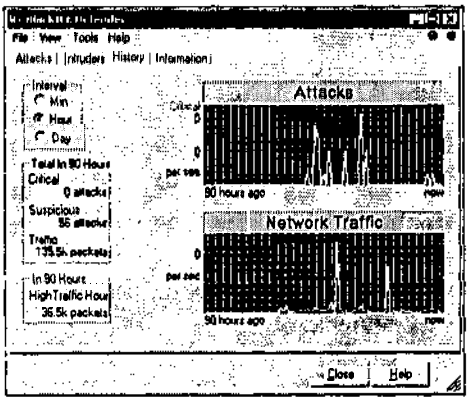


Рисунок 7.16. Графический анализ атак, запушенных против вашего компьютера

Раздел Interval (Интервал) позволяет вам определять период времени, используемый при представлении данных в обоих графиках. Раздел Total In 90 Hours (Итого за 90 часов) разбивает атаки на следующие категории:

- **Critical (Критическая);**
- **Suspicious (Подозрительная);**
- **Traffic (Трафик).**

Раздел In 90 Hours (За 90 часов) показывает наибольшее количество атак, произошедших за любой определенный период времени (такой, как 90 часов).

Просмотр информации о брандмауэре

Окно свойств Information (Информация) показывает информацию о лицензии и оддержке, как показано на рисунке 7.17. В нем также показывается информация о версии брандмауэра BlackICE Defender, которая установлена на вашем компьютере, включая свойства, настройки и изменения, которые были внесены в версию.

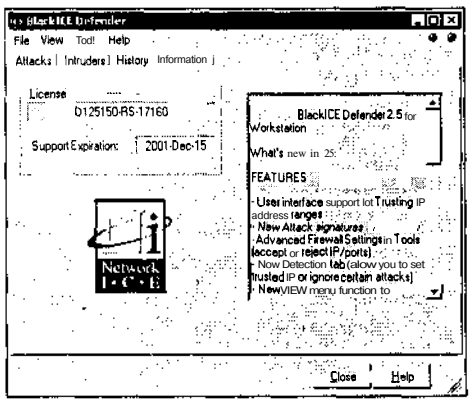


Рисунок 7.17. Просмотр информации о лицензии и поддержке брандмауэра BlackICE Defender

Дополнительные настройки брандмауэра

Опция Advanced Firewalls Settings (Дополнительные настройки брандмауэра) расположенная в меню Tools (Инструменты), Application Summary (Отчет о приложениях), предоставляет доступ к диалоговому окну, в котором вы можете управлять параметрами настройки IP-адресов и портов. На рисунке 7.18 показано окно свойств IP Address (IP-адрес) в этом диалоговом окне. Его информация представлена в нескольких колонках, включая:

Б Icon (Иконка) - зеленая иконка, показывающая доверяемые IP-адреса, и черная иконка, показывающая блокированные IP-адреса.

и Owner (**Владелец**) - показывает, кто создал запись.

Address (**Адрес**) - IP-адрес, который заблокирован.

Е Start Time (Начальное время) - время, когда началась блокировка.

в End Time (Конечное время) - время, когда истекает установленная блокировка.

• Name (Имя) - имя (если доступно), связанное с IP-адресом.

Изображение может быть отсортировано по любой колонке с помощью нажатия на ее заголовок. Кроме того, вы можете нажать правой клавишей мыши на заголовок любой колонки, чтобы добавить или удалить колонки с экрана.

Вы также можете нажать правой клавишей мыши на любую запись и выбрать из следующих опций:

- **Unblock Only (Только разблокировать);**
- **Unblock and Accept (Разблокировать и принять);**
- **Unblock, Accept, and Trust (Разблокировать, принять и доверять);**
- **Modify (Изменить).**

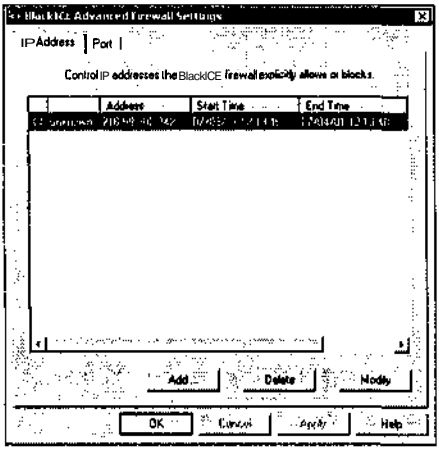


Рисунок 7.18. Управление дополнительными настройками брандмауэра

Кроме того, вы можете нажать кнопки Add (Добавить), Delete (Удалить) или Modify (Изменить), чтобы добавить, удалить или изменить записи в списке IP-адресов.

Окно свойств Port (Порт), показанное на рисунке 7.19, отображает список всех параметров настройки портов TCP/IP. По умолчанию в этом списке нет записей. Это окно свойств позволяет вам устанавливать временную или постоянную блокировку любого протокола TCP или UDP. Чтобы заблокировать порт, нажмите Add (Добавить). Вы можете позже изменить запись, нажав Modify (Изменить), или удалить ее из списка, нажав Delete (Удалить). Когда вы будете добавлять запись, вам предложат ввести имя, представляющее блокировку, номер блокируемого порта, тип протокола (такой, как TCP или UDP), а также спросят, хотите ли вы заблокировать его на время или постоянно.

Остановка механизма BlackICE

Опция Stop BlackICE Engine (Остановить механизм BlackICE) в контекстном меню иконки BlackICE Defender позволяет вам остановить механизм анализа и обнаружения атак брандмауэра BlackICE Defender. Остановка механизма BlackICE Defender оставит ваш компьютер полностью незащищенным при со-

единении с Интернетом. Эта опция должна использоваться с максимальной осторожностью. Однако вы, возможно, захотите использовать эту опцию для того, чтобы определить, не влияет ли как-либо брандмауэр BlacklCE Defender на Интернет-приложение, которое не хочет запускаться.

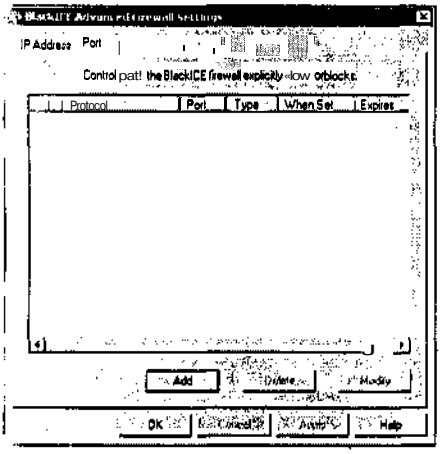


Рисунок 7.19. Блокировка определенных портов TCP и UDP

После остановки программы поверх иконки BlacklCE Defender в панели задач Windows появится красная линия. Вы можете вновь загрузить программу, нажав правой клавишей мыши на иконку и выбрав Start BlacklCE Engine (Запустить механизм BlacklCE).

Вы также можете остановить механизм BlacklCE Defender из приложения - отчета о деятельности (Summary Application), нажав на меню Tools (Инструменты), выбрав BlacklCE Engine (механизм BlackICE), а затем Stop BlacklCE Engine (Остановить механизм BlacklCE).

WWW Network ICE

Выбрав опцию WWW Network ICE в контекстном меню иконки BlacklCE Defender, вы запустите ваш Интернет-браузер и загрузите Web-страницу сайта Network ICE *(www.networkice.com),* где вы сможете найти более подробную информацию о брандмауэре BlacklCE Defender и других продуктах и услугах, предоставляемых компанией "Network ICE".

Выход

Выбрав Exit (Выход) в контекстном меню иконки BlacklCE Defender, вы закроете программу отчета о приложениях (Application Summary program). Это, однако, не приведет к отключению брандмауэра BlacklCE Defender. Чтобы перезагрузить программу отчета о приложениях (Application Summary program), выберите Пуск, Программы, Network ICE и затем BlacklCE Utility.

Ограничения брандмауэра BlackICE Defender

Брандмауэр BlackICE Defender предоставляет вашему компьютеру очень надежную защиту при соединении с Интернетом. Его легко установить и указать настройки безопасности до начала конфигурирования, что позволяет вам начать работу тотчас же. Кроме того, он имеет свойства, которых нет во многих других брандмауэрах, включая обнаружение вторжения и способность отслеживать путь и собирать информацию о хакерах, которые пытаются проникнуть в ваш компьютер.

Однако в этом персональном брандмауэре отсутствует несколько функций, которые обычно присутствуют в конкурирующих продуктах. Например, брандмауэр BlackICE Defender не позволяет вам блокировать определенные приложения от доступа в Интернет. Поэтому правильно написанная программа "Троянский конь" может проникнуть на ваш жесткий диск и отыскать вашу личную информацию.

Кроме того, он не позволяет вам создавать разные настройки безопасности для домашней сети и соединений с Интернетом. Поэтому вы не можете отключить общий доступ к файлам и принтерам через TCP/IP для вашего соединения с нтернетом без того, чтобы также не отключить его для вашей домашней сети. Однако вы всегда можете установить протокол NetBEUI на каждый компьютер вашей домашней сети и объединить ресурсы этим способом. Более подробную информацию об объединении ресурсов домашней сети смотрите в главе 11.

Проверка персонального брандмауэра BlackICE Defender

После установки и конфигурирования вашего персонального брандмауэра BlackICE Defender вы должны запустить несколько тестов, чтобы убедиться, что он работает и защищает ваш компьютер,

Начните проверку, запустив Internet Explorer или Netscape Communicator и убедившись, что вы все еще можете соединиться с Интернетом. Если ваш браузер работает, запустите другие Интернет-приложения и убедитесь, что они также работают.

Затем запустите бесплатное Интернет-сканирование вашего компьютера и посмотрите, насколько хорошо защищен ваш компьютер. Просмотрите главу 9 "Насколько защищен ваш компьютер?", чтобы получить информацию о том, как запустить бесплатный сканер безопасности из Интернета. Также просмотрите приложение Б "Другие Web-сайты, которые проверят вашу безопасность", чтобы найти список различных Web-сайтов, которые предоставляют услуги бесплатного Интернет-сканирования. В общем и целом BlackICE Defender - это надежный брандмауэр, великолепно выполняющий свои функции по защите персональных компьютеров. Его встроенный механизм анализа и обнаружения обеспечивает его более развитыми внутренними логическими функциями, чем у большинства других брандмауэров. Однако из трех программных брандмауэров, описанных в этой книге, он требует наиболее сложных технических познаний, необходимых для того, чтобы полностью реализовать возможности брандмауэра.

Глава 6

ZONEALARM

Это последняя из трех глав, описывающих программные персональные брандмауэры. Эта глава посвящена персональному брандмауэру ZoneAlarm компании "Zone Labs". Вы узнаете, как установить и сконфигурировать этот брандмауэр и как он работает.

Вы также увидите, каким образом брандмауэр ZoneAlarm позволит вам установить различные параметры настройки безопасности для домашней сети и соединений с Интернетом, и узнаете, как можно конфигурировать предупреждения и автоматически блокировать вашу систему, когда вы ее не используете. Вы также узнаете, как применять настройки безопасности системы и приложений и читать содержимое файла регистрации брандмауэра ZoneAlarm.

В этой главе вы:

- узнаете, как конфигурировать предупреждение о тревоге;
- откроете, как конфигурировать файл регистрации брандмауэра ZoneAlarm;
- узнаете, как автоматизировать блокировку вашего компьютера;
- выясните, как отрегулировать параметры безопасности;
- узнаете, как установить доверяемые приложения;
- выясните, как настроить брандмауэр на автоматическую проверку обновлений.

Описание

Персональный брандмауэр ZoneAlarm предоставляется компанией "Zone Labs" *(www.zonelabs.com)*. Этот персональный брандмауэр бесплатен для личного и некоммерческого использования, хотя при использовании брандмауэра в коммерческих целях требуется небольшая плата. Он может защищать коммутируемое, цифровое и кабельное соединение.

Брандмауэр ZoneAlarm - один из двух персональных брандмауэров, предоставляемых компанией "Zone Labs". Второй продукт - это брандмауэр ZoneAlarm Pro, который имеет те же свойства, что и брандмауэр ZoneAlarm, плюс другие, такие, как более детальная настройка параметров безопасности, что также повышает уровень сложности продукта. Эта глава посвящена брандмауэру ZoneAlarm.

Брандмауэр ZoneAlarm защищает вас от программ "Троянский конь", перехватывая любое приложение, которое пытается соединиться с Интернетом. О любом событии он сообщает с помощью графического предупреждения, которое позволяет вам решать, пропускать ли приложение. Когда вы впервые установите

брандмауэр ZoneAlarm, вы обнаружите, что он постоянно держит вас в напряжении, загружая ответами на предупреждения. Однако пройдет немного времени, и он успокоится, узнав, какие приложения вы хотите пропускать, а какие нет.

Вы можете использовать брандмауэр ZoneAlarm для защиты как вашего соединения с Интернетом, так и вашей домашней сети. Он делает это, определяя две зоны безопасности: локальная зона и зона Интернета. Он предоставляет следующие три уровня безопасности, которые вы можете применять отдельно для каждой зоны:

- Low (низкий);
- Medium (средний);
- High (высокий).

Простой механизм настройки отрегулирует параметры безопасности для каждой зоны. Когда вы измените уровень безопасности, появится описание воздействия изменений, которое поможет вам понять, как это изменение повлияет на вашу личную безопасность.

По умолчанию брандмауэр ZoneAlarm использует средний уровень безопасности при защите домашней сети и высокий уровень при защите соединения с Интернетом.

Брандмауэр ZoneAlarm часто использует всплывающие диалоговые окна для общения с вами во время своей работы. Кроме того, вы можете сконфигурировать брандмауэр записывать информацию о событии в файл регистрации для дальнейшего просмотра и анализа.

Системные требования

Во время написания этой книги самой последней версией брандмауэра ZoneAlarm была версия 2.6. Его рабочие аппаратные требования включают:

- 8 Мб памяти;
- 3 Мб места на жестком диске;
- процессор 386 или выше (рекомендуется 486).

Чтобы запустить брандмауэр ZoneAlarm в любой операционной системе Windows, ваш компьютер должен отвечать минимальным требованиям к памяти. Для Windows 95, 98 и NT я бы рекомендовал, по крайней мере, 16 Мб. Для Windows Me вам потребуется минимум 32 Мб. Windows 2000 Professional потребует не менее 64 Мб.

Кроме того, вам необходимо коммутируемое, кабельное или цифровое соединение с Интернетом и одна из следующих операционных систем:

- Windows 95;
- Windows 98;

m Windows Me;

• Windows NT 4 с Service Pack (Служебный пакет программ) 3 или выше;

a Windows 2000;

• Windows XP.

Установка и настройка

Вы можете получить бесплатную копию брандмауэра ZoneAlarm на *www.zonelabs.com*. Имя загружаемого файла - zonalm26 (последние две цифры представляют собой номер версии). Во время написания книги последней версией брандмауэра ZoneAlarm была версия 2.6, и программа ее установки требовала примерно 2,76 Мб.

Первый шаг в подготовке к установке брандмауэра ZoneAlarm - закрыть все активные программы, включая те, что взаимодействуют с Интернетом. Процесс установки состоит из двух частей. Первая часть включает сбор информации, которая будет использоваться для конфигурирования брандмауэра ZoneAlarm, а вторая часть - это фактическая установка. Оба эти процесса кратко описаны здесь:

1. Дважды нажмите на иконку ZoneAlarm Setup (Установка брандмауэра ZoneAlarm).

2. Появится приветственное диалоговое окно ZoneAlarm Installation (Установка ZoneAlarm), как показано на рисунке 8.1. Нажмите Next (Далее).

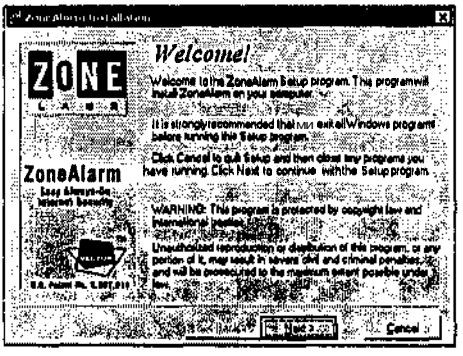


Рисунок 8.1. Приветственное окно установки брандмауэра ZoneAlarm

3. Появится диалоговое окно Информация о продукте (Product Information), показанное на рисунке 8.2, содержащее системные требования, информацию об установке и удалению брандмауэра ZoneAlarm и о том, как запустить приложение. Просмотрите предоставленную информацию и затем нажмите Next (Далее),

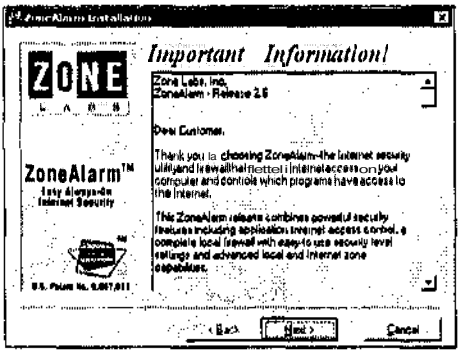


Рисунок 8.2. Просмотр основных сведений о брандмауэре ZoneAlarm

4. Затем вам предложат ввести ваше имя (name), название организации (company name) и адрес электронной почты (e-mail address), как показано на рисунке 8.3.

   Вы также можете выбрать одну из следующих двух опций:

   - I want to register ZoneAlarm so I can download updates (Я хочу зарегистрировать брандмауэр ZoneAlarm, чтобы иметь возможность загружать обновления);
   - Inform me about important updates and news (Информируйте меня о важных обновлениях и новостях).

   Заполните форму и нажмите Next (Далее).

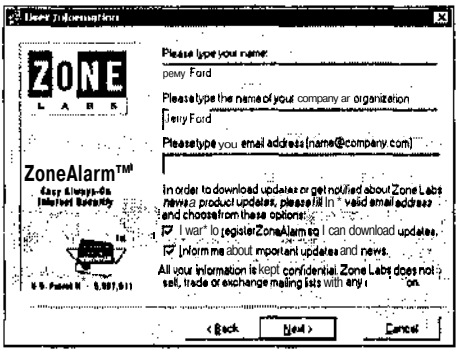


Рисунок 8.3. Регистрация для бесплатных обновлений и получения новостей о брандмауэре ZoneAlarm

5. Появится ZoneAlarm License Agreement (Лицензионное соглашение брандмауэра ZoneAlarm), показанное на рисунке 8,4. Вы должны принять условия этого соглашения, для того чтобы установить брандмауэр ZoneAlarm. Нажмите Accept (Принимаю).

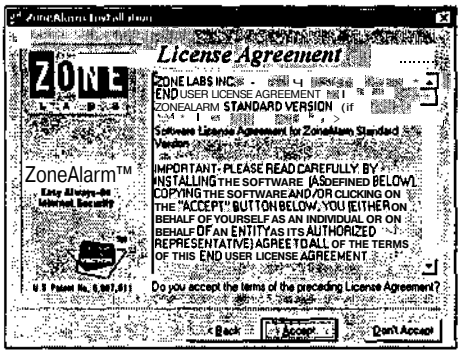


Рисунок 8.4. Просмотр лицензионного соглашения брандмауэра ZoneAlarm

6. Появится окно Select Destination Directory (Выбор директории), показанное на рисунке 8.5. В нем будет указано, сколько свободного места останется на диске после установки. Чтобы изменить папку, в которую будет произведена установка, нажмите Browse (Обзор). Нажмите Next (Далее).

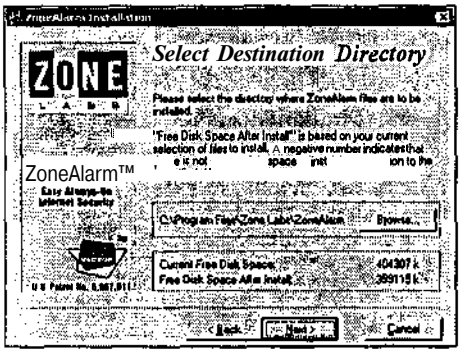


Рисунок 8.5. Выбор папки, в которую будет установлен брандмауэр ZoneAlarm

7. Затем процесс установки начнет поиск Интернет-браузера и, если его найдет, предложит сконфигурировать брандмауэр так, чтобы разрешить ему соединяться с Интернетом, как показано на рисунке 8.6. Выберите Yes (Да), чтобы разрешить соединяться и нажмите Next (Далее).

Если вы не сконфигурировали доступ вашего Интернет-браузера сейчас, вы всегда можете установить его позже.

Если у вас установлен Windows 2000, вам также будет предложено разрешить Microsoft Windows Services и Controller app проходить через брандмауэр.

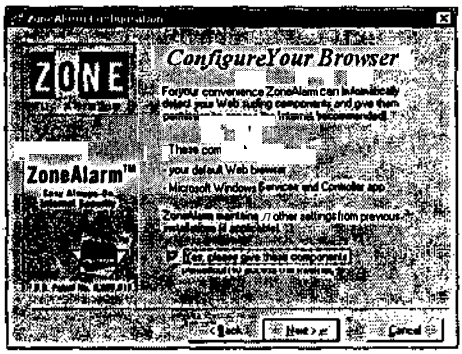


Рисунок 8.6. Конфигурирование автоматического подключения к Интернету вашего Интернет-браузера

8. Появится диалоговое окно Ready to Install! (Готово к установке). Нажмите Next (Далее).

9. Начнется процесс установки файлов брандмауэра ZoneAlarm на ваш компьютер. Появится диалоговое окно User Survey (Настройки пользователя), показанное на рисунке 8.7. Заполните эту форму и нажмите Finish (Готово).

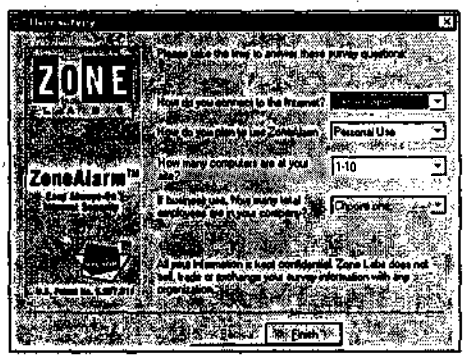


Рисунок 8.7. Установка будет завершена после того, как вы заполните настройки пользователя брандмауэра ZoneAlarm

10. Теперь установка завершена. Появится всплывающее диалоговое окно, спрашивающее у вас, хотите ли вы запустить брандмауэр ZoneAlarm. Нажмите Yes (Да).

Первоначальный запуск ZoneAlarm

Первое, что вы увидите после первоначального запуска брандмауэра ZoneAlarm, - диалоговое окно ZoneAlarm-Getting Started (ZoneAlarm - первоначальный запуск), показанное на рисунке 8.8.

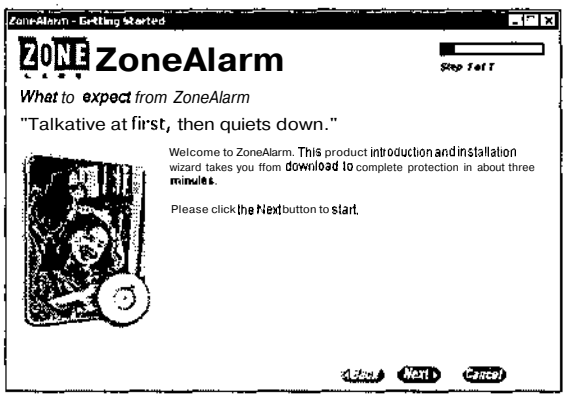


Рисунок 8.8. Совершите короткое путешествие по свойствам брандмауэра ZoneAlarm

Нажимая на кнопку Next (Далее), вы шаг за шагом пройдете по семи окнам, каждое из которых расскажет вам немного о работе с брандмауэром ZoneAlarm. Нажмите Next (Далее), чтобы продолжить, или Cancel (Отменить), чтобы закрыть это диалоговое окно.

Следующее, что вы увидите, - диалоговое окно ZoneAlarm Tips (Подсказки ZoneAlarm), показанное на рисунке 8.9.

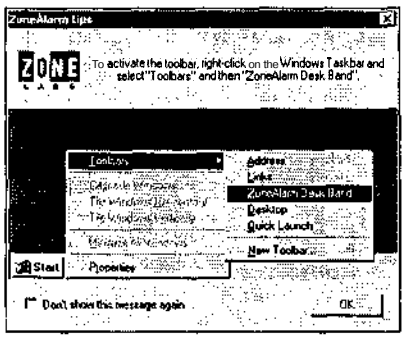


Рисунок 8.9. Просмотр подсказок брандмауэра ZoneAlarm

Эти подсказки появляются каждый раз при запуске брандмауэра ZoneAlarm, пока вы не выберете опцию Don't show this message again (Больше не показывать это сообщение) внизу диалогового окна. Нажмите OK, чтобы закрыть это диалоговое окно.

Кроме главного диалогового окна брандмауэра ZoneAlarm, вы увидите иконку ZA в вашей панели задач Windows. Когда будет происходить обмен информацией по сети или Интернету, иконка ZA изменится на графическую иконку, которая будет светиться красным и зеленым, показывая активность, как изображено на рисунке 8.10.

Рисунок 8.10. Иконка ZoneAlarm в панели задач Windows переключается с ZA на графический индикатор при осуществлении процесса обмена информацией

Кроме иконки ZoneAlarm в панели задач, вы найдете следующие пункты, перечисленные в меню Пуск Windows, нажав Пуск, Программы и Zone Labs.

- **Readme** - ознакомительный файл README брандмауэра ZoneAlarm.
- **Uninstall ZoneAlarm** - соединение с утилитой удаления брандмауэра ZoneAlarm.
- **ZoneAlarm Tutorial** - соединение с диалоговым окном ZoneAlarm - Getting Started (ZoneAlarm - первоначальный запуск).

в **ZoneAlarm** - исполняемая программа ZoneAlarm.

Работа с брандмауэром ZoneAlarm

Исполняемая программа брандмауэра ZoneAlarm называется zonealarm.exe. Если вы не изменили место ее расположения, устанавливаемое по умолчанию при установке, вы найдете ее на c:\Programs Files\Zone Labs\ZoneAlarm.

Чтобы открыть главное диалоговое окно брандмауэра ZoneAlarm, показанное на рисунке 8.11, дважды нажмите на иконку в панели задач Windows или нажмите на Пуск, Программы, Zone Labs, а затем ZoneAlarm.

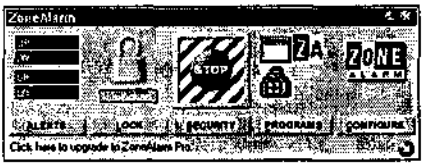


Рисунок 8.11. Главное диалоговое окно ZoneAlarm

Главное диалоговое окно брандмауэра ZoneAlarm состоит из пяти разделов, каждый из которых содержит иконку и соединение:

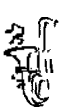
- **Graphs (Графики)** - динамический набор столбчатых диаграмм, иллюстрирующих сетевой трафик. Два верхних графика показывают текущий входящий и исходящий трафик. Два нижних графика показывают движение данных за длительный период времени.
- **Padlock** (Замок) - позволяет вам переключить вашу систему в защищенное состояние, предотвращая любое соединение с Интернетом. Вы можете, тем не менее, освободить приложения от этой блокировки. Зеленая полоса под замком показывает, что он открыт, а ее длина показывает, сколько времени прошло с того момента, как защита была убрана. Красная полоса показывает, что замок закрыт, и ее длина указывает на то, как долго активна блокировка.

- **Stop (Остановка)** - предоставляет вам аварийную кнопку для немедленного запирания доступа к Интернету. Весь Интернет-трафик без исключения подвергается воздействию этой опции.
- **Applications (Приложения)** - показывает набор иконок, представляющих собой активные приложения, в настоящее время соединившиеся с Интернетом.
- **ZoneAlarm Logo (Регистрационные данные брандмауэра ZoneAlarm)** — предоставляет связь с Web-сайтом Zone Labs, на котором доступна помощь.

Под каждой иконкой находится кнопка, которая открывает панель ZoneAlarm, на которой вы можете просмотреть и сконфигурировать параметры настройки брандмауэра. Каждая из этих кнопок перечислена в следующем списке:

- **Alerts (Предупреждения)** - предоставляет настройки файлов регистрации статистики и контроля за день.
- **Lock (Блокировка)** - позволяет вам устанавливать автоматическую блокировку вашего брандмауэра, который начнет работать после предварительно определенного периода бездействия.
- **Security (Безопасность)** - позволяет вам настраивать и конфигурировать зоны безопасности для вашего соединения с Интернетом и домашней сетью.
- **Programs (Программы)** - позволяет вам просматривать и управлять разрешением приложениям проходить через брандмауэр.
- **Configure (Конфигурирование)** - позволяет вам конфигурировать брандмауэр ZoneAlarm на автоматический запуск при загрузке системы и на проверку обновлений.

Когда вы свернете главное диалоговое окно брандмауэра ZoneAlarm, оно свернется на панели задач Windows. Но если вы нажмете на кнопку закрыть, появится диалоговое окно ZoneAlarm tips (Подсказки брандмауэра ZoneAlarm), предупреждающее вас, что вы можете закрыть брандмауэр ZoneAlarm, нажав правой клавишей мыши на его иконку в системной строке и выбрав опцию Shutdown ZoneAlarm (Выключение ZoneAlarm). После закрытия диалогового окна путем нажатия на OK брандмауэр ZoneAlarm свернется в панели задач.



Выберите опцию Don't show this message again (Больше не показывать это сообщение), чтобы диалоговое окно подсказок брандмауэра ZoneAlarm больше не появлялось при нажатии на кнопку закрытия.

Управление Интернет-предупреждениями и регистрацией брандмауэра

Нажатие на клавишу Alerts (Предупреждения) в главном диалоговом окне брандмауэра ZoneAlarm откроет панель Internet Alert (Интернет-предупреждения), показанную на рисунке 8.12. Эта панель включает в себя три раздела. Раздел

Today's Summary (Отчет за текущий день) предоставляет статистику количества отправленных и принятых байтов за текущий день.

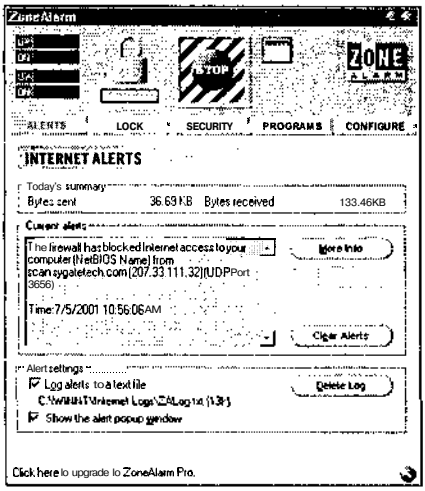


Рисунок 8.12. Панель Internet Alerts (Интернет-предупреждения) позволяет вам конфигурировать параметры настройки предупреждений и регистрационных записей

Раздел Current Alerts (Текущие предупреждения) показывает прокручиваемый список предупреждений, которые появлялись на вашем компьютере. Справа находятся четыре кнопки навигации, которые позволяют вам перейти вперед или назад на одно предупреждение или в начало или в конец списка предупреждений. Над элементами управления навигацией расположена кнопка More Info (Информация). При нажатии эта опция откроет ваш браузер и перешлет выбранную информацию о предупреждениях Zone Labs AlertAnalyzer (анализатору предупреждений Zone Labs), где она будет проанализирована, а затем объяснена, как показано на рисунке 8.13. В то время как некоторые из предупреждений брандмауэра ZoneAlarm не требуют объяснений, многие другие требуют дополнительной информации для понимания. Я рекомендую вам при первой установке брандмауэра ZoneAlarm как можно чаще использовать эту опцию. Этим самым вы ускорите свое обучение и более полно изучите процесс работы персонального брандмауэра.

Под кнопкой навигации находится кнопка Clear Alerts (Очистить предупреждения), которая позволяет вам очистить все записи о предупреждениях.

Внизу панели Internet Alert (Интернет-предупреждения) находится раздел Alert Settings (Настройка предупреждений). Здесь вы можете указывать, будет ли брандмауэр ZoneAlarm поддерживать файлы регистрации или показывать всплывающие предупреждения. Обе эти опции подробно описаны далее в этой главе. Справа от этих кнопок конфигурирования находится кнопка Delete Log (Удалить регистрационную запись), которую вы можете использовать, чтобы удалить файл регистрации брандмауэра ZoneAlarm, когда он станет слишком большим.

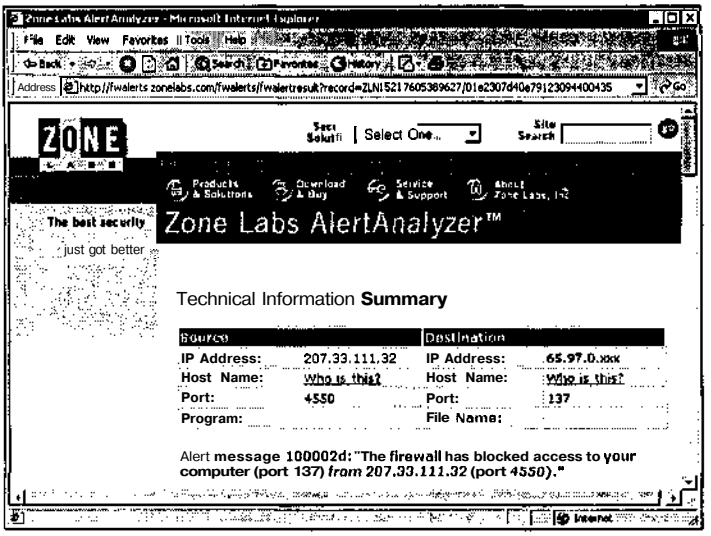


Рисунок 8.13. Вы можете нажать на More Info (Информация), чтобы открыть ваш Web-браузер и получить более подробную информацию о предупреждении с Web-сайта Zone Labs

Работа с параметрами установки блокировки соединений с Интернетом

Нажатием на кнопку Lock (Блокировка) в главном диалоговом окне брандмауэра ZoneAlarm вы откроете панель Internet Lock Settings (Настройка блокировки соединений с Интернетом), показанную на рисунке 8.14. Эта панель разделена на два раздела. Раздел Lock Status (Состояние блокировки) показывает состояние блокировки брандмауэра ZoneAlarm (открыт или заблокирован), а также включена блокировка или отключена.

Раздел Automatic Lock (Автоматическая блокировка) отключен по умолчанию. Когда вы блокируете ваш компьютер, блокируется весь трафик Интернета, как входящий, так и исходящий, независимо от параметров настройки безопасности вашего персонального брандмауэра. Вы можете использовать эту опцию, чтобы установить на вашем компьютере самый высокий из возможных уровней защиты на время, когда вы собираетесь не подходить к компьютеру долгое время. Например, если вы оставляете ваш компьютер включенным, когда вы на работе, вы можете включить эту опцию. Когда вы вернетесь домой и начнете путешествовать по Интернету, вы можете отключить эту опцию и начать работу в Интернете под защитой ваших индивидуальных настроек конфигурации. Если вы решили установить параметры безопасности брандмауэра ZoneAlarm на самом низком уровне, я рекомендую включать эту опцию каждый раз, когда вы не используете ваш компьютер, для дополнительной безопасности. Когда эта опция включена, все настройки в этом разделе становятся доступными. Эти настройки включают следующие:

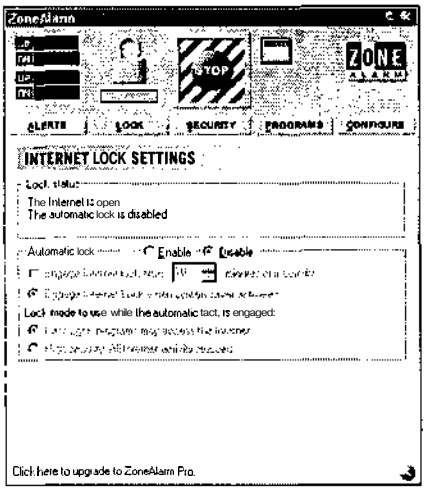


Рисунок 8.14. Панель Internet Lock Settings (Настройка блокировки соединении с Интернетом) позволяет вам включать и выключать ваш персональный брандмауэр

- **Engage Internet lock after____minutes of inactivity (Включать блокировку Интернета через_____минут отсутствия активности)** - автоматически блокирует доступ компьютера к Интернету после указанного периода времени, в течение которого активность со стороны пользователя отсутствовала.
- **Engage Internet lock when screen saver activates (Включать блокировку Интернета при активизации хранителя экрана) -** позволяет вам установить на брандмауэре ZoneAlarm блокировку, которая включается каждый раз при запуске заставки.
- **Pass lock programs may access the Internet (Пропуск блокированных программ к Интернету)** - позволяет вам указать, что программы, которые были сконфигурированы обходить блокировку, могут это сделать, когда она будет включена. Отдельные программы могут конфигурироваться из панели Programs (Программы) с помощью настройки Pass Lock (Пропуск блокировки).
- **High security; all Internet activity is stopped (Надежная безопасность; вся Интернет-активность остановлена)** - задает брандмауэру ZoneAlarm блокировать всю активность Интернета при включении блокировки.

Конфигурирование настроек безопасности

Нажатием на кнопку Security (Безопасность) в главном диалоговом окне брандмауэра ZoneAlarm вы откроете панель Security Settings (Настройка безопасности), показанную на рисунке 8.15. Эта панель разделена на два раздела. Раздел Security Level (Уровень безопасности) показывает настройку безопасности брандмауэра.

Персональный брандмауэр ZoneAlarm разделяет безопасность на две части или зоны, позволяя вам конфигурировать настройки безопасности вашей до-

машней сети (если она у вас есть) отдельно от настроек безопасности Интернета. Слева находятся настройки безопасности домашней сети, а справа - настройки безопасности для вашего соединения с Интернетом.

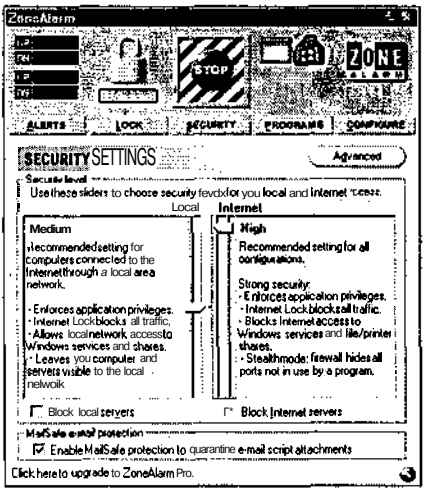


Рисунок 8.15. Панель Security Settings (Настройка безопасности) позволяет вам конфигурировать безопасность вашего соединения с Интернетом и вашей домашней сети

Три уровня безопасности доступны для каждого соединения и конфигурируются путем перемещения линейки прокрутки уровня безопасности вверх и вниз для определенного соединения. По умолчанию уровень безопасности локальной сети устанавливается как средний, а уровень безопасности соединения с Интернетом - как высокий.

В следующем списке дается определение каждого уровня безопасности локальной зоны:

- Low (Низкий) - делает ваш компьютер видимым для других компьютеров домашней сети и разрешает общий доступ к файлам и принтерам. Если иконка Lock (Блокировка) включена, эта настройка блокирует только трафик приложений, как указано на панели Programs (Программы) брандмауэра ZoneAlarm.
- Medium (Средний) - делает ваш компьютер видимым для других компьютеров домашней сети и разрешает общий доступ к файлам и принтерам. Если иконка Lock (Блокировка) включена, эта настойка блокирует весь трафик.
- High (Высокий) - делает ваш компьютер невидимым для других компьютеров домашней сети и запрещает общий доступ к файлам и принтерам.

В следующем списке даны определения каждого уровня безопасности зоны Интернета:

- Low (Низкий) - делает ваш компьютер видимым для Интернета и разрешает общий доступ к файлам и принтерам.

- Medium (Средний) - блокирует службы NetBIOS, но все равно разрешает общий доступ к файлам и принтерам. Тем самым он запрещает сканирующим программам, которые ищут порты NetBIOS 137 - 139, запрашивать у вашего компьютера информацию об общих файлах и принтерах, которые у вас есть, не отключая общий доступ к файлам и принтерам.
- High (Высокий) - делает ваш компьютер невидимым в Интернете, блокирует службы NetBIOS и запрещает общий доступ к файлам и принтерам.

Под настройками безопасности локальной сети и соединения с Интернетом находятся опции для блокировки серверов. Блокировка локального сервера запрещает приложению действовать как сервер при взаимодействии по домашней сети. Блокировка серверов Интернета запрещает приложению действовать как сервер при взаимодействии с Интернетом. Приложение действует как сервер, когда предоставляет услугу другому запрашивающему компьютеру. Например, если на вашем домашнем компьютере установлен Microsoft Personal Web Server и вы используете его для создания своего собственного Web-сайта, ваш компьютер должен уметь работать как небольшой Web-сервер, который принимает входящие запросы соединения для просмотра ваших Web-страничек от других пользователей Интернета.

Внизу диалогового окна Security Setting (Настройка безопасности) находится опция Enable MailSafe protection to quarantine e-mail script attachments (Включить защиту MailSafe для изоляции приложений к электронной почте, содержащих сценарии). Когда она выбрана, эта опция задает брандмауэру ZoneAlarm не допускать открытия приложений к электронной почте, написанных на языке сценариев VBScript. Сценарии VBScript иногда используются для переноса компьютерных вирусов и программ "Троянский конь" внутри приложений электронной почты. Когда эта опция включена, брандмауэр ZoneAlarm изменяет расширение файла, написанного с помощью программы VBScript, на .zl. Это дает вам возможность соединиться с отправителем электронного письма для того, чтобы определить, настоящее ли это приложение, прежде чем открывать его.

Кнопка Advanced (Подробнее), расположенная в верхнем правом углу панели Security Settings (Настройка безопасности), открывает диалоговое окно Local Zone Properties (Свойства локальной зоны). Здесь вы можете указать компьютеры вашей домашней сети, для того чтобы ваш компьютер мог общаться с ними. Чтобы добавить описание компьютера домашней сети, нажмите Add (Добавить) и укажите имя и IP-адрес компьютера. Чтобы изменить запись, выберите ее и нажмите Properties (Свойства). Чтобы удалить компьютер из списка, выберите его и нажмите Remove (Удалить). Более подробная информация о работе с брандмауэром ZoneAlarm в домашней сети представлена в главе 11 "Домашние сети и общее подключение к Интернету".

Управление вашими Интернет-приложениями

Нажатием на кнопку Programs (Программы) в главном диалоговом окне брандмауэра ZoneAlarm вы откроете список всех сконфигурированных Интернет-приложений, о которых знает брандмауэр ZoneAlarm, показанный на рисунке 8.16.

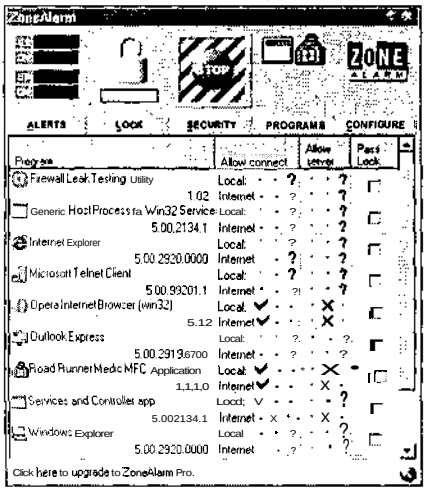


Рисунок 8.16. Просмотр и управление вашими Интернет-приложениями

Каждый раз при запуске Интернет-приложения вам будет предложено задать брандмауэру ZoneAlarm, как им управлять. Информация, собранная от вас, затем записывается здесь. Каждое Интернет-приложение показано в колонке Program (Программа) с номером ее версии. Колонка Allow Connect (Позволить соединение) показывает, разрешено ли приложению соединяться с локальной зоной и зоной Интернета. Зеленая галочка показывает, что приложению разрешено соединяться. Красный значок X показывает, что приложение блокировано от соединения, а черный знак вопроса показывает, что брандмауэр ZoneAlarm запросит вас в следующий раз, когда приложение попытается соединиться, о том, разрешено ли ему это. Вы можете использовать свою мышь, чтобы изменить эти опции конфигурации, нажав на поле колонки каждого приложения, перечисленного на панели. Например, если вы выбрали блокировку приложения от доступа в Интернет, вы можете восстановить его, нажав на первую колонку в разделе Allow Connection (Позволить соединение) для этого приложения. Этим действием вы поместите зеленую галочку в поле, показывающую, что приложение было добавлено в список одобренных приложений.

Вы, возможно, захотите позволить большинству приложений, таких, как Internet Explorer или Outlook Express, доступ в Интернет. Основная цель возможной блокировки этих приложений - предотвратить запуск тайного соединения с Интернетом программы "Троянский конь". Каждый раз, когда прило-

жение, не указанное в списке, попытается соединиться с Интернетом, Netscape* уведомит вас об этом. Если вы не уверены, что это за приложение или что оно пытается сделать, я предлагаю вам указать брандмауэру ZoneAlarm блокировать его, а затем подождать, что же случится. Если все продолжает работать правильно, это может быть приложение "Троянский конь", которое вы можете удалить. Если другое Интернет-приложение, с которым вы хотите работать, внезапно прекратило свою работу, возможно, что приложение, которое вы заблокировали, является нужным и должно быть разблокировано.

Не доверяйте всему, что видите. Некоторые приложения "Троянский конь" присваивают себе имя файла, которое совпадает с именем файла приложения, установленного с вашего согласия, надеясь обмануть вас, чтобы вы позволили ему пройти через ваш персональный брандмауэр. Например, если вы видите предупреждение брандмауэра ZoneAlarm, запрашивающее у вас разрешение пропустить Internet Explorer через брандмауэр, в то время как вы уже добавили приложение в список одобренных приложений, вы, возможно, в действительности видите перед собой "Троянского коня".

Колонка Allow Server (Позволить работу в качестве сервера) указывает, может ли приложение действовать как сервер и принимать входящие соединения. Такие же три опции, имеющиеся в колонке Allow Connect (Позволить соединение), есть и здесь. Колонка Pass Lock (Пропустить блокировку) определяет, разрешено ли приложению обходить блокировку брандмауэра ZoneAlarm, если она была включена.

Вы можете настроить отдельное приложение, нажав правой клавишей мыши на него и выбрав одну из следующих опций:

- **Local Network (Локальная сеть)** - эта опция позволяет вам указывать, разрешить ли выбранному приложению или запретить проходить через брандмауэр, или вы хотите, чтобы вас спросили об этом в следующий раз, когда оно будет запущено. Вы можете также указывать, должен ли брандмауэр ZoneAlarm разрешить или запретить приложению работать как серверу, или спросить вас об этом.
- **Internet (Интернет)** - эта опция позволяет вам применять те же самые настройки, используемые опцией Local Network (Локальная сеть), по отношению к соединению с Интернетом.
- **Pass Lock (Пропуск через блокировку)** - эта опция позволяет вам включать и выключать настройку пропуска приложения через блокировку.
- **Changes Frequently (Частые изменения)** - эта опция позволяет вам указать программу, которая часто изменяется. Например, вы, возможно, используете испытательную версию программы, которую вы загрузили из Интернета. Ес-

---

* По-видимому, здесь опечатка автора. Сообщение выдает не Netscape, а ZoneAlarm.

ли автор программы улучшает ее через каждые несколько недель, и вы постоянно загружаете и устанавливаете ее, она будет помечаться как изменяющаяся программа каждый раз, когда вы загружаете ее, поскольку размеры ее файлов продолжают изменяться. С помощью этой опции вы можете избавиться от проблем, вызванных постоянным повторным одобрением приложения.

- Remove **xxxxxxx** (Удалить xxxxxxx) - эта опция позволяет вам удалять запись о приложении из списка приложений брандмауэра ZoneAlarm.

Базовая конфигурация брандмауэра ZoneAIarm

Нажатие на кнопку Configure (Конфигурация) в главном диалоговом окне брандмауэра ZoneAIarm выводит на экран набор настроек конфигурации, как показано на рисунке 8.17.

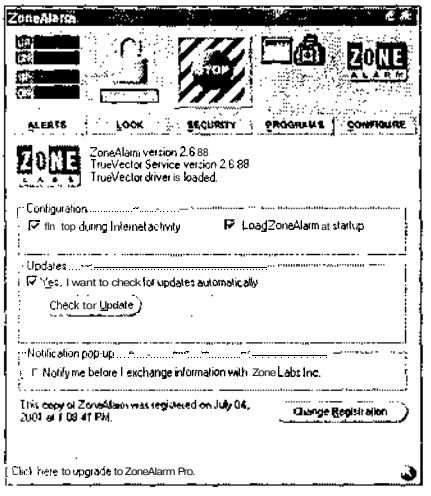


Рисунок 8.17. Работа с настройками конфигурации брандмауэра ZoneAIarm

Эта панель разделена на три раздела. Раздел Configuration (Конфигурация) предоставляет следующие опции:

- **On top during Internet activity (поверх других окон во время работы с Интернетом)** - приводит к появлению главного диалогового окна брандмауэра ZoneAIarm поверх других окон Windows при прохождении Интернет-трафика.
- **Load ZoneAIarm at startup (Запуск брандмауэра ZoneAIarm при** загрузке) - задает брандмауэру ZoneAIarm автоматически запускаться при загрузке компьютера.

Раздел Updates (Обновления) позволяет вам сконфигурировать брандмауэр ZoneAIarm на автоматическую проверку обновлений на Web-сайте Zone Labs. Кнопка Check for Update (Проверка обновлений) позволяет вам выполнять немедленную проверку. Если обновление доступно, активизируется кнопка Get Update (Получить обновление). Нажмите ее, чтобы загрузить обновление.

Всплывающий раздел Notification (Предупреждение) позволяет вам указывать, хотите ли вы, чтобы вас предупреждали, когда ваш брандмауэр обменивается информацией с Web-сайтом Zone Labs. Брандмауэр ZoneAlarm контактирует с Web-сайтом Zone Labs только тогда, когда проверяет наличие на нем обновлений.

Последняя опция на панели - кнопка Change Registration (Изменить регистрационную информацию). При нажатии она показывает диалоговое окно Registration Information (Информация о регистрации), в котором вы можете изменить имя, название организации и адрес электронной почты, которые вы зарегистрировали на Zone Labs.

Работа с панелью инструментов области рабочего стола

Брандмауэр ZoneAlarm автоматически добавляет панель опций к набору панели инструментов Windows при установке. Эта панель инструментов называется панель инструментов области рабочего стола брандмауэра ZoneAlarm (ZoneAlarm Desk Band toolbar). Вы можете использовать следующую методику для ее подключения.

1. Нажмите правой клавишей мыши на чистое пространство панели задач Windows. Появится контекстно-зависимое меню.
2. Выберите опцию Toolbars (Панели инструментов). Откроется подменю, показанное на рисунке 8.18.

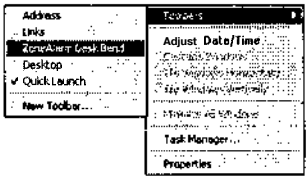


Рисунок 8.18. Конфигурирование панели инструментов области рабочего стола брандмауэра ZoneAlarm

3. Выберите опцию ZoneAlarm Desk Band (Область рабочего стола брандмауэра ZoneAlarm).

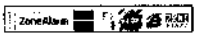


Рисунок 8.19. Панель инструментов области рабочего стола брандмауэра ZoneAlarm

Панель инструментов области рабочего стола брандмауэра ZoneAlarm предоставляет доступ после одного нажатия к каждой иконке в главном диалоговом окне брандмауэра ZoneAlarm, не занимая при этом места на рабочем столе Windows. Я считаю, что это предоставляет очень удобный доступ к брандмауэру ZoneAlarm, и предлагаю вам использовать его, по крайней мере, первые один-

два месяца после установки брандмауэра ZoneAlarm, когда вам, возможно, придется взаимодействовать в основном с брандмауэром. Первая иконка на панели инструментов показывает графическое изображение текущей сетевой активности. Следующая иконка показывает, находится ли брандмауэр в блокированном состоянии. Если он блокирован, поверх иконки блокировки накладывается красный значок X, когда блокировка активна. Третья иконка отображает красную иконку остановки, когда брандмауэр приостановлен. Вслед за иконкой ZoneAlarm появляются иконки для каждого открытого Интернет-приложения.

Предупреждения и лог-файл брандмауэра ZoneAlarm

Брандмауэр ZoneAlarm может предоставлять подробную информацию о событиях по мере их появления в двух видах. Он также может записывать их в файл для поддержания непрерывности архива информации о событиях. Он также может показывать сообщения о событиях в форме всплывающих предупреждений по мере их возникновения. Каждая из этих опций рассматривается в следующих разделах.

Некоторые люди считают включение всплывающих предупреждений брандмауэра ZoneAlarm немного раздражающим и в результате отключают; их. Я рекомендую не делать этого. Вы, возможно, увидите некоторое количество предупреждений в первый месяц или два после установки брандмауэра. Однако, когда брандмауэр ZoneAlarm узнает обо всех приложениях, которым вы доверяете, он постепенно успокоится, оставив только самые нужные сообщения.

Работа с лог-файлом брандмауэра ZoneAlarm

Файл регистрации брандмауэра ZoneAlarm конфигурируется из окна Alerts Settings (Настройка предупреждений) на панели Alerts (Предупреждения), показанном на рисунке 8.20. Отсюда вы можете включать и выключать регистрацию, определять, будут ли всплывающие предупреждения показывать предупреждающие сообщения. Кроме того, кнопка Delete Log (Удалить лог) позволяет вам очистить файл регистрации, когда он станет слишком большим. Я очень рекомендую вам включить регистрацию предупреждений и просматривать ваш лог-файл регулярно.

Рисунок 8.20. Лог-файл брандмауэра ZoneAlarm конфигурируется в разделе Alert Settings (Настройка предупреждений) на панели Alerts (Предупреждения)

Вы, возможно, захотите сделать копию вашего лог-файла до того, как удалите его. Это позволит вам сохранить лог-файл в архиве, чтобы, если вы захотите, вы могли вернуться и изучить предыдущие события.

Лог-файл брандмауэра ZoneAlarm называется ZALOG.TXT. В системах с Windows 95, 98 и Me лог-файл расположен в C:\Windows\Internet Logs. В системах с Windows NT и 2000 он находится в C:\Winnt\Internet Logs.

Брандмауэр ZoneAlarm записывает три вида сообщений в свой лог-файл:

- FWIN - идентифицирует блокированный входящий запрос соединения.
- FWOUT - показывает блокированный исходящий запрос соединения.
- PE - идентифицирует приложение, которое пытается соединиться с Интернетом.

Некоторые лог-сообщения включают один или более флажков TCP, которые предоставляют дополнительную информацию о типе произошедшего события:

- ACK - пакет представляет собой подтверждение полученных данных.
- FIN - пакет представляет собой прекращение соединения.
- PSH - пакет представляет собой данные, "проталкиваемые" в приложение.
- RST - пакет представляет собой сброс соединения.
- SYN - пакет представляет собой запрос соединения.
- URG - пакет содержит важные данные.

При включении в лог-сообщение показывается только первый знак флажка TCP. Например, (flags:A) показывает, что пакет был подтверждением данных, которые были получены.

Следующие примеры логов взяты из типичного лог-файла брандмауэра ZoneAlarm. Первая строчка показывает версию брандмауэра ZoneAlarm, которая запущена на компьютере.

```
ZoneAlarm Logging Client v2.6.88
```

Следующая строчка показывает операционную систему, которая установлена на вашем компьютере.

```
Windows NT-5.0.2195-SP
```

Затем вы увидите строку, в которой указана базовая структура записи лог-файла.

```
type, date, time, source, destination, transport
```

С этого момента то, что вы увидите в своем лог-файле, будет варьироваться в зависимости от вашей индивидуальной конфигурации. Например, следующий отчет зарегистрировал информацию о приложении на компьютере, который пытается общаться с другим компьютером в Интернете посредством этого приложения.

```
PE, 2001/07/04, 12:53:20 -4:00 GMT, Road Runner Medic MFC
Application, 65.97.0.1:0, N/A
```

Предыдущий пример может быть разбит на следующие части:

- PE - показывает тип лог-сообщения.
- 2001 /07/04 - показывает дату, когда событие произошло.
- 12:53:20 - показывает местное время, когда событие произошло.
- -4:00 GMT - показывает время по Гринвичу, когда событие произошло.

- Road Runner Medic MFC Application - показывает приложение, которое послужило причиной события.
- **65.97.0.1:0** - показывает IP-адрес и номер порта, который приложение пытается использовать.
- N/A - в этом поле информация отсутствует.

В следующем примере показана запись в лог-файле, где брандмауэр ZoneAlarm блокирует входящий запрос соединения.

```
FWIN,2001/07/04,12:57:07-4:00 GMT,24.30.225.31:0,65.97.0.75:0, ICMP;
(type:3/subtype:3)
```

Этот пример может быть разбит на следующие части:

- FWIN - показывает тип лог-сообщения.
- **2001/07/04** - показывает дату, когда событие произошло.
- 12:57:07 - показывает местное время, когда событие произошло.
- -4:00 GMT - показывает время по Гринвичу, когда событие произошло.
- **24.30.225.31:0** - показывает IP-адрес и номер порта компьютера в Интернете, который послужил причиной события.
- 65.97.0.75:0 - показывает IP-адрес и номер порта удаленного компьютера.
- ICMP (type:3/subtype:3) - показывает определенную информацию о транспортном протоколе TCP/IP, который используется для передачи пакета.

В последнем примере показано лог-сообщение, которое включает Параметр флажка TCP, указывающий на пакет типа SYN (например, запрос соединения).

```
FWIN, 2001/07/04, 22:31:02 -4:00 GMT, 207.33.111.34:44256, 65.97.0.75:139, TCP
(flags:S)
```

Работа с предупреждениями ZoneAlarm

Кроме показа лог-сообщений, вы можете сконфигурировать брандмауэр ZoneAlarm показывать сообщения в форме всплывающих предупреждений. Вы можете включить предупреждения, выбрав опцию Show the alert pop-up window (Показывать всплывающее окно предупреждения) на панели Alerts (Предупреждения).

Предупреждения брандмауэра ZoneAlarm состоят из следующей информации:

- IP-адрес;
- протокол и порт;
- дата и время;
- отметка(и) TCP;
- тип соединения (входящее или исходящее);
- версия приложения, когда доступна.

Брандмауэр ZoneAlarm создает два типа предупреждений: Program (Программное) и Firewall (Брандмауэрное).

Программные предупреждения

Программные предупреждения регистрируют деятельность программных приложений. Существует четыре вида программных предупреждений, перечисленных здесь:

- New (Новое);
- Changed (Изменившееся);
- Repeat (Повторное);
- Server (Сервер).

Кроме того, брандмауэр ZoneAlarm показывает с каждым предупреждением кнопку More Info (Подробная информация), которую вы можете нажать, чтобы получить более детальную информацию о предупреждении, включая советы по тому, как реагировать на предупреждение. Я рекомендую использовать эту опцию каждый раз, когда вы не уверены в том, что предупреждающее сообщение говорит вам. Это прекрасный способ узнать больше о внутренней работе вашего персонального брандмауэра и Интернета.

Новые предупреждения

Этот тип предупреждения создается, когда приложение пытается получить доступ к Интернету впервые, как показывается на рисунке 8.21. Предупреждение предлагает вам позволить или запретить приложению получить доступ.

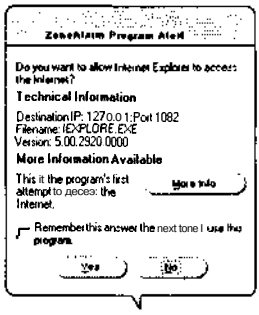


Рисунок 8.21. Брандмауэр ZoneAlarm создает новое предупреждение каждый раз, когда приложение пытается получить доступ к Интернету впервые

Просмотрите Technical Information (Техническая информация), чтобы увидеть название приложения, номер версии и компьютер, с которым оно пытается соединиться. Нажмите More Info (Подробная информация), чтобы узнать больше о предупреждении. Нажав на эту кнопку, вы откроете Интернет-браузер и соединитесь с Web-сайтом Zone Labs, где содержание предупреждения проанализируется и вам предоставят дополнительную информацию.

Чтобы позволить приложению установить соединение, нажмите Yes (Да), чтобы блокировать его, нажмите No (Нет). Кнопка Remember this answer the next

time you use this program (Запомнить этот ответ в следующий раз при использовании этой программы) позволит вам задать брандмауэру всегда разрешать приложению доступ в Интернет.

Предупреждения об изменении

Этот тип предупреждения очень редок и может указывать на программу-червя или "Троянского коня". Я бы обратил особое внимание на одно из этих предупреждений при их появлении. Оно появляется только тогда, когда брандмауэр обнаруживает программу, пытающуюся получить доступ в Интернет, которая уже одобрена, но была изменена некоторым образом. Примеры изменений включают:

- изменение имени программы;
- изменение размера или расположения программного файла;
- изменение номера версии программы;
- изменение имени исполняемого файла программы.

Повторные предупреждения

Повторное предупреждение появляется, когда брандмауэр ZoneAlarm перехватывает приложение, которое было запущено ранее, но не было сконфигурировано как постоянно доверяемое приложение, как показано на рисунке 8.22. Приведенное здесь приложение называется Road Runner Medic MFC.

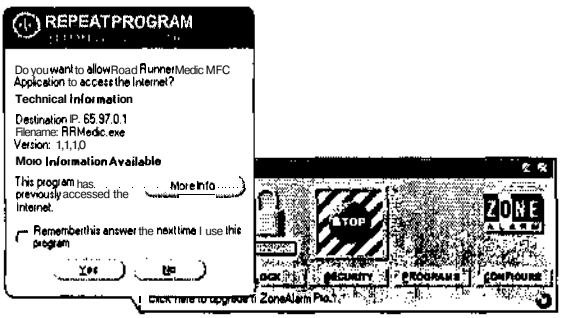


Рисунок 8.22. Брандмауэр ZoneAlarm создает повторное предупреждение, когда он перехватывает известную программу, которая не была сконфигурирована на автоматическое подключение к Интернету

Предупреждения о сервере

Предупреждение о сервере, показанное на рисунке 8.23, появляется, когда программа пытается работать как сервер, и означает, что она хочет принять соединение из Интернета.

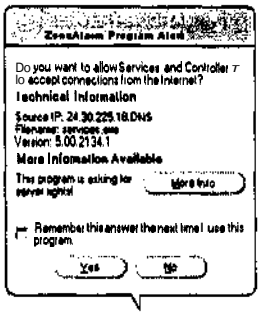


Рисунок 8.23. Брандмауэр ZoneAlarm создает предупреждение о сервере для любой программы, которая намеревается действовать как Интернет-сервер

Брандмауэрные предупреждения

Брандмауэрные предупреждения выглядят почти как программные предупреждения, но предоставляют информацию о входящих пакетах, которые несут угрозу вашему компьютеру. Существует два типа брандмауэрных предупреждений: предостерегающее и экстренное.

Предостерегаюшие брандмауэрные предупреждения

Предостерегающее сообщение показывает наступление события, которое расценивается как потенциально несущее угрозу, но не угрожающее непосредственно вашему компьютеру. На рисунке 8.24 показывается предостерегающее предупреждение. Его заголовок выделен оранжевым цветом. Его данные включают исходный IP-адрес и транспортный протокол, а также дату и время, когда событие произошло.

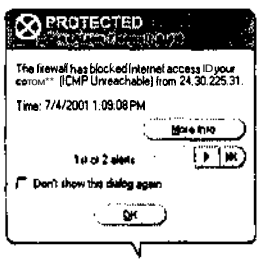


Рисунок 8.24. Предостерегаюшие брандмауэрные предупреждения являются сообщениями о потенциальной угрозе

Экстренные брандмауэрные предупреждения

Экстренное брандмауэрное предупреждение появляется с красным заголовком и указывает на более серьезную угрозу, чем предостерегающее предупреждение. Например, на рисунке 8.25 показано предупреждение, которое создано в результате сканирования Интернет-сканером, запущенным против локального компьютера. Оно показывает имя и IP-адрес сканирующей системы, а также

протокол и порт, которые были просканированы. Такое сканирование может означать хакера, пытающегося собрать информацию о вашем компьютере в качестве подготовки к более серьезной атаке. Брандмауэр блокировал сканирующую программу так, что с вашей стороны больше не требуется дополнительных действий. Однако если вы начали видеть повторяющиеся предупреждения об одном и том же источнике, возможно, вы подвергаетесь нападению. Вы, вероятно, захотите повысить уровень безопасности вашего брандмауэра на высокий, если этот уровень еще не установлен. Возможно, вы захотите отсоединиться от Интернета на время.

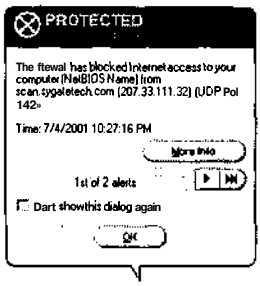


Рисунок 8.25. Экстренное брандмауэрное предупреждение говорит о непосредственной угрозе вашему компьютеру

Ограничения брандмауэра ZoneAlarm

Брандмауэр ZoneAlarm имеет наиболее интуитивный интерфейс из всех персональных брандмауэров, рассматриваемых в этой книге. Это делает его прекрасным вариантом для начинающих пользователей, которые могут чувствовать себя неуютно, работая с более технически ориентированными персональными брандмауэрами, такими, как брандмауэр BlackICE Defender. Кроме того, он предоставляет сильную защиту от хакеров из Интернета. Он поставляется предварительно сконфигурированным с набором служб безопасности, которые компания Zone Labs считает подходящими для домашних пользователей.

В брандмауэре ZoneAlarm нет встроенного мастера конфигурирования. Однако его интуитивный интерфейс и предварительно сконфигурированные настройки безопасности уменьшают потребность в таком инструменте.

Несмотря на его небольшой размер и в чем-то ограниченный набор свойств, брандмауэр ZoneAlarm предоставляет все основные функции, которые вы бы хотели видеть в персональном брандмауэре. В действительности, за исключением встроенного обнаружения вторжения, этот небольшой брандмауэр имеет все необходимые функции. Лучше всего то, что брандмауэр ZoneAlarm бесплатен для личного пользования, что остановило мой выбор на нем.

Проверка вашего персонального брандмауэра Zone Labs

После установки и конфигурирования вашего персонального брандмауэра от компании "Zone Labs" вы должны протестировать его, чтобы убедиться, что он работает и должным образом защищает ваш компьютер. Вы можете сделать это, запустив ваш Интернет-браузер и определив, можете ли вы соединиться с Интернетом. После того как этот тест будет выполнен успешно, запустите другое Интернет-приложение и посмотрите, перехватит ли его брандмауэр ZoneAlarm. Если он это сделает, укажите брандмауэру ZoneAlarm, что вы хотите работать с этим приложением. Вы, вероятно, увидите его иконку, появившуюся в разделе Programs (Программы) главного диалогового окна ZoneAlarm, и с этого момента оно должно работать должным образом.

Затем попробуйте другое Интернет-приложение, такое, которому вы не хотите позволить проходить через брандмауэр. Например, если у вас установлен Microsoft NetMeeting, но вы не планируете его больше использовать или не хотите, чтобы ваши дети его использовали, вы можете блокировать его. Когда вы запустите приложение NetMeeting, брандмауэр ZoneAlarm перехватит его и предоставит вам возможность пометить его как приложение, которому должен быть запрещен доступ к Интернету. Проверьте, что брандмауэр ZoneAlarm блокирует его доступ. Вы должны получить сообщение об ошибке от приложения.

Если у вас возникли проблемы с одним из предыдущих тестов, попробуйте уменьшить настройку безопасности на один уровень и посмотрите, что получится. Если все работает нормально, попробуйте запустить Интернет-сканер на вашем компьютере, чтобы посмотреть, насколько хорошо брандмауэр ZoneAlarm защищает ваш компьютер.

Для получения информации о том, как запускать и анализировать результаты бесплатного Интернет-сканирования, просмотрите главу 9 "Насколько защищен ваш компьютер?". Кроме того, в приложении Б "Другие Web-сайты, которые проверят вашу безопасность" вам представлен ряд бесплатных Интернет-сайтов, на которые вы можете зайти для дополнительной проверки вашей безопасности в Интернете.

9

Насколько зашишен ваш компьютер?

К настоящему моменту вы должны были выбрать персональный брандмауэр, установить и сконфигурировать его в вашей операционной системе Windows. Теперь пришло время заняться тяжелой работой и протестировать его. Эта глава проведет вас шаг за шагом по процессу запуска трех Интернет-тестирований безопасности, чтобы помочь вам определить, насколько в действительности защищено ваше соединение с Интернетом.

Все эти тесты бесплатны. Чтобы облегчить вашу задачу и сделать процесс проверки непрерывным, в этой главе представлены три теста, предоставляемые одним Web-сайтом Интернет-безопасности. Это Web-сайт *grc.com,* он принадлежит исследовательской корпорации "Gibson Research Corporation".

В этой главе вы:

- узнаете, как запускать сканирование безопасности из Интернета и проанализировать его результаты;
- увидите, как запускать сканер, который зондирует ваши порты TCP/IP;
- узнаете, как запускать тест, который имитирует программу "Троянский конь".

Проверка вашей уязвимости перед хакерами из Интернета

Не существует способа узнать, насколько надежна ваша защита, без ее тестирования. Эта глава поможет вам сделать именно это с помощью двух бесплатных сканеров безопасности из Интернета и программной утилиты, представленных на Web-сайте grc.com. Первые два теста запускаются в тот момент, когда персональный брандмауэр отключен. Это укажет вам на слабые места в защите, имеющиеся в компьютере при обычных условиях функционирования. Для иллюстрации запуска всех этих тестов в этой главе в качестве примера используется операционная система Windows 2000 Professional. Эта операционная система намного более безопасна, чем операционные системы Windows 95, 98 или Me, и автоматически включает на компьютере более высокий уровень защиты.

Второй набор тестов запускается после включения персонального брандмауэра. Для иллюстрации выполнения этих тестов в главе используется персональный брандмауэр ZoneAlarm, однако вы можете заменить его любым другим персональным брандмауэром.

Последний тест - это имитация программы "Троянский конь", в нем используется бесплатная утилита с сайта *grc.com* под названием LeakTest. Эта небольшая программа попытается взломать безопасность вашего соединения с Интернетом, проникнув с вашего компьютера в Интернет, где она затем соединится с сервером сайта *grc.com* и передаст несколько не несущих угрозы байт информации.

Выполнение бесплатного сканирования безопасности

Прежде чем запустить первое сканирование, отключите ваш персональный брандмауэр. Поскольку в этой главе используется брандмауэр ZoneAlarm в качестве примера, вы можете сделать это, нажав правой клавишей мыши на иконку ZoneAlarm в панели задач Windows и выбрав Shutdown ZoneAlarm (Закрыть брандмауэр ZoneAlarm). Когда вам предложат подтвердить свой выбор, нажмите Yes (Да). Когда ваш брандмауэр будет отключен, вы можете запустить сканер по следующей методике:

1. Откройте ваш Интернет-браузер и выйдите на Web-сайт *grc.com.*
2. После того как сайт загрузится, нажмите на ссылку Shields UP! (Проверить безопасность!). Тем самым откроется главная Web-страница Shields UP! (Проверить безопасность!). Прокручивайте страницу вниз, пока не увидите опции Test My Shields! (Протестировать мою защиту!) и Probe My Ports! (Прозондировать мои порты!), показанные на рисунке 9.1.

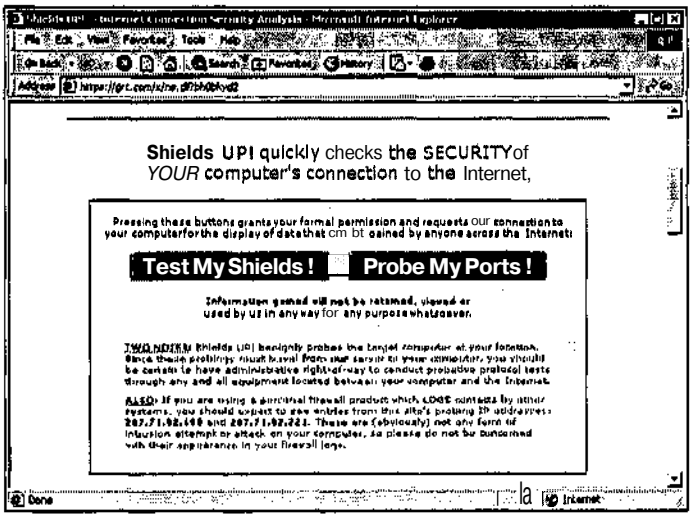


Рисунок 9.1. Web-сайт grc.com предоставляет два теста безопасности соединения с Интернетом

3. Чтобы выполнить общую проверку защиты вашего компьютера, нажмите кнопку Test My Shields! (Протестировать мою защиту!).

Без действующего брандмауэра, защищающего ваш компьютер, тестирование будет проведено очень быстро, обычно за несколько минут. Первое, что вы увидите, это ваш IP-адрес и сообщение, которое попросит вас оставаться в сети, пока Web-сервер Shields UP! (Проверить безопасность!) пытается соединиться с вашим компьютером. Если соединение будет установлено успешно, сервер продолжит испытывать вашу защиту, пытаясь получить более подробную информацию о вашем компьютере и его общих ресурсах. Как показано на рис. 9.2, сервер Shields UP! (Проверить безопасность!) смог соединиться с компьютером через порт NetBIOS 139.

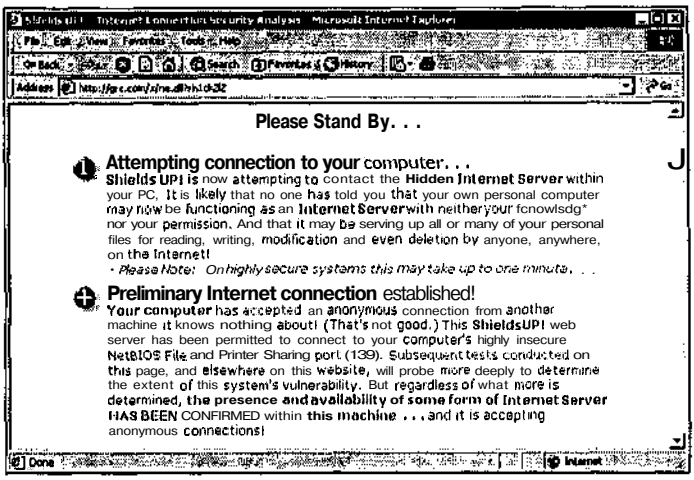


Рисунок 9.2. Этот компьютер, как и большинство незашишенных компьютеров с операционной системой Windows, примет запрос соединения от неизвестного компьютера из Интернета

Затем появится отчёт об остальных действиях сканера безопасности. На рисунке 9.3 показано, что протокол TCP/IP связан с NetBIOS, позволяя любому компьютеру в Интернете видеть этот компьютер и его общие ресурсы.

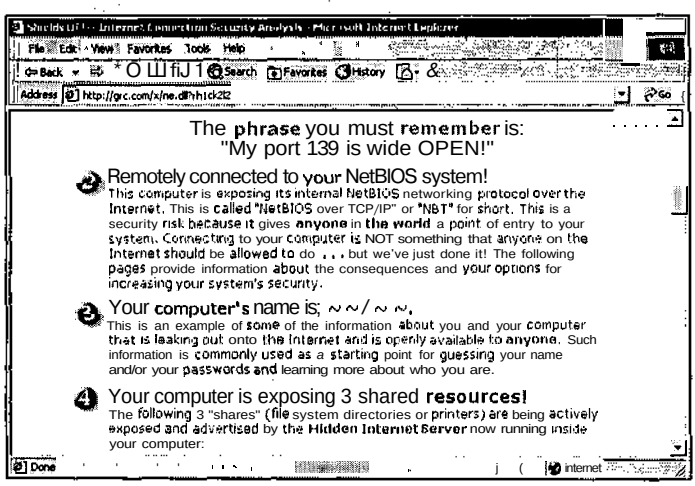


Рисунок 9.3. Если TCP/IP привязан к NetBIOS, ваш компьютер счастлив поделиться информацией о себе с любым компьютером в Интернете, который пожелает ее запросить

В этом тесте сканер не смог определить имя компьютера. Это хорошо, поскольку чем меньше хакеры узнают о вас, тем меньше информации они будут иметь при запуске атаки. К сожалению, сканер обнаружил, что он может видеть все три общих ресурса, принадлежащих компьютеру.

Следующий пункт, показанный в отчете, - это графическое представление об общих ресурсах, обнаруженных сканером, показанное на рисунке 9.4. Как вы

можете видеть, Windows 2000 защитил эти ресурсы паролем. Этого бы не было, будь это системы с Windows 95, 98 или Me.

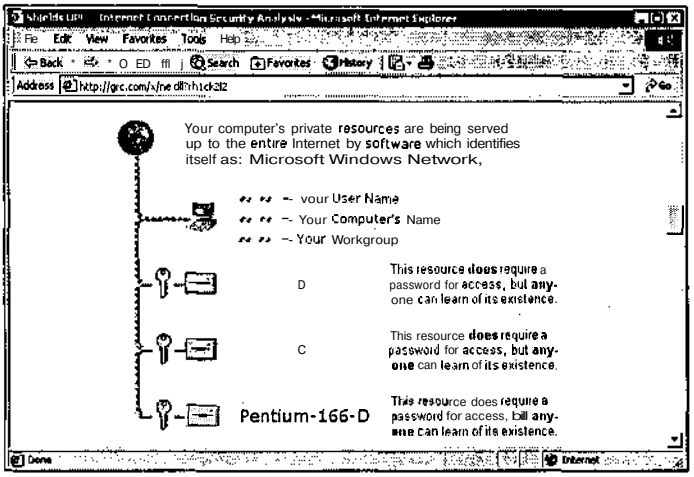


Рисунок 9.4. Все обшие ресурсы компьютера были обнаружены, что предоставляет потенциальному хакеру возможную цель для нападения

Следующее, что вы можете увидеть на рисунке 9.5, это то, что MAC-адрес сетевой карты компьютера был также обнаружен. Даже если ваш IP-адрес меняется время от времени, как происходит в случае коммутируемого соединения, ваш MAC-адрес остается постоянным, давая хакеру средство вашей идентификации.

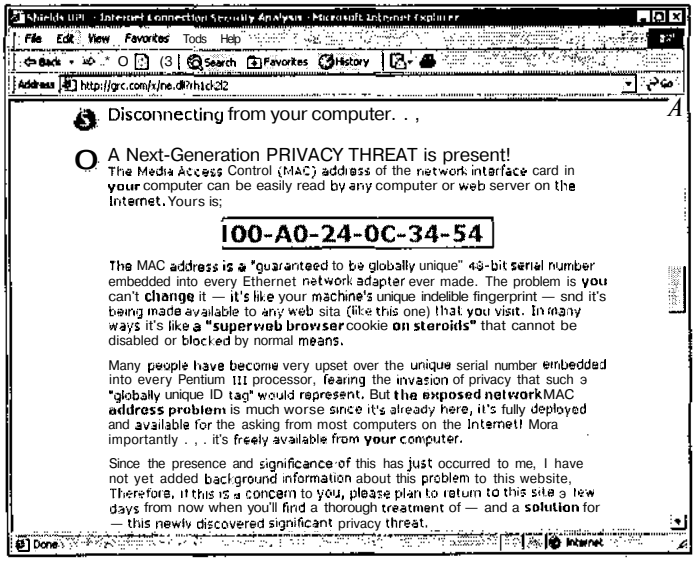


Рисунок 9.5. MAC-адрес вашей сетевой карты - это 48-битное число, с помошью которого ваша сетевая карта отличается от всех остальных

Последняя часть отчета, показанная на рисунке *9.6,* предоставляет итоговую сводку результатов деятельности сканера. Отчет говорит о том, что сканер смог соединиться с компьютером и собрал о нем информацию. В нем также говорится о том, что автоматизированные инструменты хакера могут быть использованы для исследования Интернета и поиска целей, которые предоставляют возможность соединения.

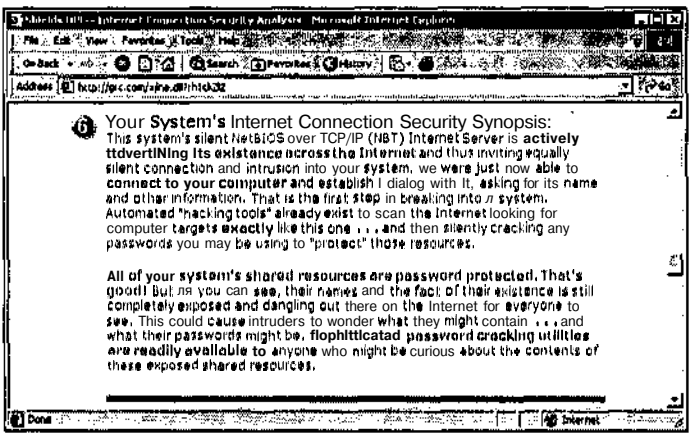


Рисунок 9.6. Последняя часть отчета представляет собой итоговую сводку результатов деятельности сканера

Отчет также предупреждает, что при попытке взлома ваших паролей против вашего компьютера могут быть использованы программы взлома пароля. Если бы это были компьютеры с Windows 95, 98 или Me, они были бы особенно уязвимы к такого рода атакам, взламывающим пароли.

Зондирование портов

Результаты первого Интернет-сканирования менее чем обнадеживающие, поскольку они показывают, что компьютер готов раскрыть слишком много информации о себе. Чтобы завершить анализ безопасности компьютера, запустите Интернет-сканер, специально созданный для зондирования портов TCP/IP компьютера.

Вы можете это сделать с Web-сайта *grc.com,* нажав на кнопку Probe My Ports! (Прозондировать мои порты!) на Web-странице Shields UP! (Проверить безопасность!). Это отнюдь не полное зондирование портов. Это выборочное исследование портов, которые обычно оставляются открытыми. Смотрите Приложение Б "Другие Web-сайты, которые проверят вашу безопасность", чтобы найти информацию о других Web-сайтах Интернет-безопасности, которые предоставляют услуги по более обстоятельному сканированию портов.

На рисунках 9.7 и 9.8 показаны результаты сканирования портов. Все порты закрыты, за исключением порта 139. Порты указаны как закрытые, поскольку на компьютере не установлено ни одного приложения или службы, которая их использует. Однако наличие открытого порта 139 достаточно плохо, чтобы оправдать опасения.

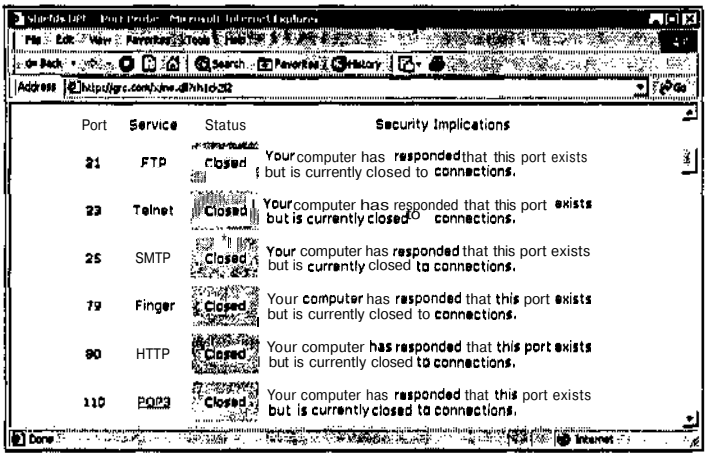


Рисунок 9.7. Все порты, показанные в этом списке, имеют статус закрытых

Сканер портов Shields Up! помечает порты с помощью одного из трех статусов:

- **Open (Открытый)** - порт открыт и допускает соединение.
- **Closed (Закрытый)** - порт виден, но отклоняет входящие запросы соединения.
- **Stealth (Невидимый)** - порт невидим и не обнаруживается из Интернета.

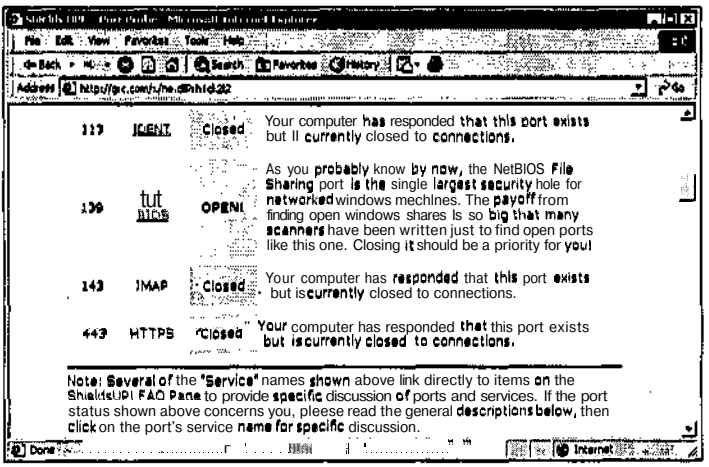


Рисунок 9.8. В этом списке показано, что порт NetBIOS 139 полностью открыт и принимает запросы соединения

Открытые порты - это именно то, что ищут Интернет-сканеры, они быстро привлекут внимание хакера к вашему компьютеру. Закрытые порты - это значительно лучше, но все равно это делает их присутствие явным. Режим невидимости портов может быть достигнут только с помощью персонального брандмауэра. Если все эти порты работают в невидимом режиме, значит, ваш компьютер невидим при зондировании с любой целью.

Тестирование с включенным и работающим персональным брандмауэром

Следующие два теста повторяют первые два, за исключением того, что на этот раз на компьютере включен персональный брандмауэр. В случае, если это персональный брандмауэр ZoneAlarm, вы можете подключить его вновь, нажав Пуск, Программы, Zone Labs, а затем ZoneAlarm. Все тесты, описываемые далее, используют настройку Интернет-безопасности брандмауэра ZoneAlarm High (Высокая), установленную по умолчанию, как показано на рисунке 9.9. Снижение уровня этой настройки без сомнения снизит уровень защиты, предоставляемый брандмауэром, и потенциально подвергнет ваш компьютер воздействию большего количества угроз.

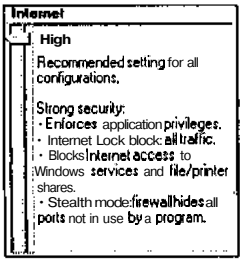


Рисунок 9.9. По умолчанию брандмауэр ZoneAlarm конфигурирует уровень своей Интернет-безопасности на самый высокий

Повторный запуск сканера из Интернета

При первом повторном запуске Интернет-сканера Shields UP! его выполнение займет значительно больше времени. Это происходит потому, что персональный брандмауэр, установленный на вашем компьютере, блокирует попытки службы сканирования проникнуть сквозь вашу систему безопасности. В действительности, после того как пройдет около минуты, сканирование будет прервано и сканер покажет результаты, представленные на рисунке 9.10.

В отчете говорится, что порт 139, который был открыт и принимал соединения в предыдущей проверке, невидим для службы сканирования. В этом тесте сканер Shields UP! не смог проникнуть через персональный брандмауэр и дал оценку компьютеру как очень хорошо защищенному.

Повторное зондирование ваших портов

Четвертый тест заключается в повторном запуске теста Probe My Ports! (Прозондировать порты!) при включенном персональном брандмауэре ZoneAlarm. Очевидно, результаты этого теста покажут, что ни один из портов не открыт. На самом деле, в этот раз все порты компьютера, указанные в списке, были отмечены как невидимые (смотрите рисунок 9.11).

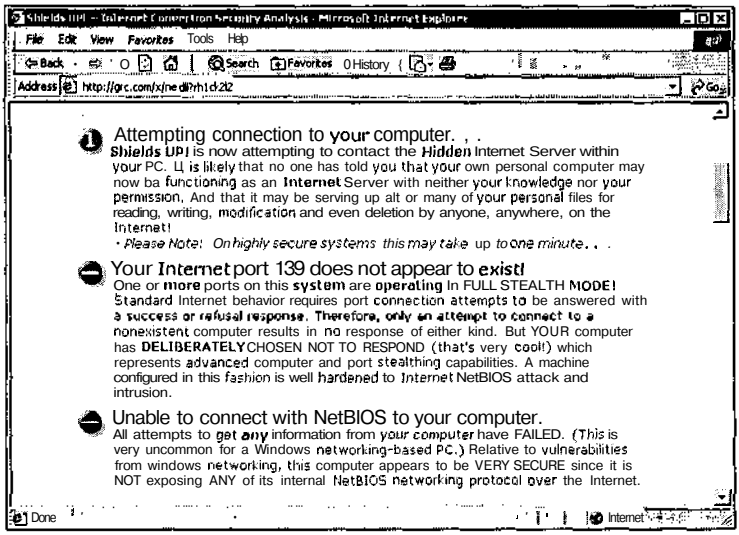


Рисунок 9.10. Сканер не смог установить соединение с компьютером, на котором был установлен персональный брандмауэр ZoneAlarm

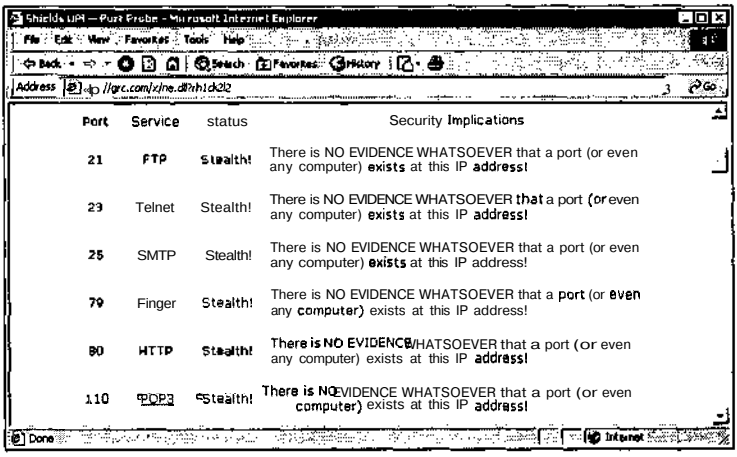


Рисунок 9.11. На этот раз порты компьютера работали в невидимом режиме и были невидимы для сканера портов

Тестирование зашиты от внутренних угроз

До настоящего времени в этой главе описывалась безопасность соединения с Интернетом с точки зрения недопущения возможного доступа к вашему компьютеру. Это, естественно, правильная стратегия. Но сама по себе она недостаточна, поскольку иногда безопасность взламывается изнутри. Программа "Троянский конь" - прекрасный пример хакерского инструмента, который угрожает безопасности вашего компьютера, находясь внутри него. В случае, если ваш персональ-

ный брандмауэр позволяет такой программе проникнуть внутрь и ваш антивирусный сканер не может ее обнаружить, вам потребуется еще одно средство защиты.

Эта дополнительная защита предоставляется в виде отслеживания и фильтрации исходящего трафика. Например, брандмауэры McAfee и ZoneAlarm просматривают все соединения приложений и блокируют неразрешенные приложения, установленные на вашем компьютере, от установки соединения с Интернетом. Когда такое приложение попытается установить соединение, оно будет временно блокировано, вас уведомят об этом и дадут возможность решить, хотите ли вы разрешить ему получить доступ к Интернету.

Брандмауэр BlackICE Defender действует по другому принципу, нежели персональные брандмауэры McAfee и ZoneAlarm. Вместо фильтрации определенных протоколов TCP/IP и приложений он анализирует каждый пакет данных на предмет потенциальных угроз. Этот брандмауэр создан так, что блокирует любую известную ему угрозу и поддерживает установление доверяемых и недоверяемых приложений. Утилита LeakTest, описанная в этом разделе, не отмечается брандмауэром BlackICE Defender как несущая угрозу безопасности, поскольку она в действительности не осуществляет деятельности, несущей угрозу.

Чтобы определить, уязвим ли ваш персональный брандмауэр перед нападениями программы "Троянский конь", загрузите с сайта *grc.com* бесплатную утилиту LeakTest, находящуюся по адресу *grc.com/lt/leaktest.htm*. Утилита LeakTest - это очень простая программа, которая позволяет вам имитировать действия программы "Троянский конь".

Утилита LeakTest действует как клиент FTP, пытаясь установить соединение через порт 21. Если тест пройдет успешно, она перешлет несколько байтов информации на сервер сайта *grc.com*. После того как вы загрузите утилиту LeakTest, вы можете запустить ее, дважды нажав на нее клавишей мыши. Появится диалоговое окно Firewall Leakage Tester (Проверка надежности брандмауэра), показанное на рисунке 9.12.

Чтобы узнать больше об утилите LeakTest, нажмите Help (Помощь), как показано на рисунке 9.13. В дополнение к краткому описанию утилиты вы найдете ссылки на информацию, расположенную на Web-страницах LeakTest.

Чтобы запустить тестирование, нажмите кнопку Test for Leaks (Проверка утечек). Последние версии персональных брандмауэров McAfee и ZoneAlarm блокируют попытку программы LeakTest соединиться с Интернетом.

Если у вас установлен брандмауэр BlackICE Defender, утилите LeakTest удастся установить соединение с Интернетом. Помните, что брандмауэр BlackICE Defender не считает, что LeakTest несет угрозу безопасности.

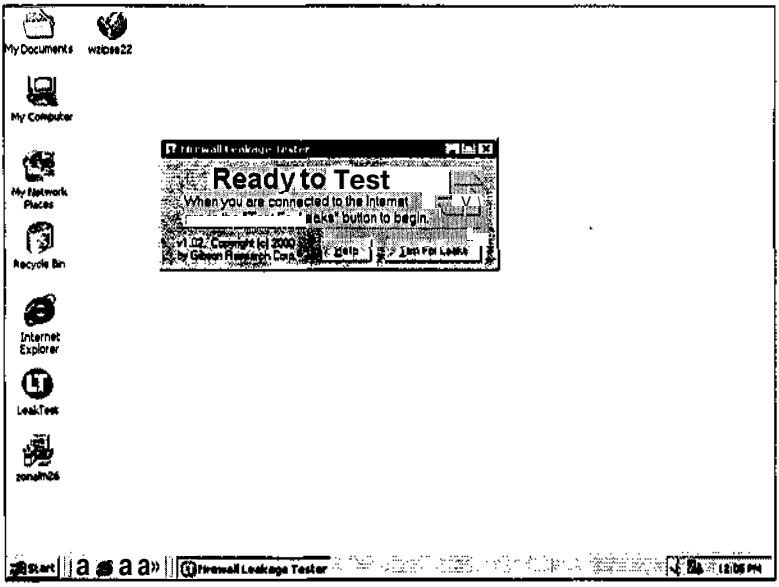


Рисунок 9.12. Запуск бесплатной утилиты тестирования LeakTest класса "Троянский конь"

Рисунок 9.13. Просмотр окна помоши утилиты LeakTest и ссылок на хранящуюся в Интернете информацию об этой бесплатной утилите

Однако недостаточно запустить утилиту LeakTest таким способом. Утилита является тестирующей программой класса "Троянский конь". Поскольку "Троянские кони" обычно проникают на ваш жесткий диск и переименовывают себя так, что выглядят как обычные программы, вы должны сменить название утилиты LeakTest на название, использующееся одним из ваших Интернет-приложений, которому позволено проходить через ваш персональный брандмауэр. Например, попробуйте переименовать программу LeakTest на Internet Explorer и вновь запустите ее.

На рисунке 9.14 показано сообщение, выдаваемое программой LeakTest при блокировке ее соединения с Интернетом. В лучшем случае ваш персональный брандмауэр правильно распознает, что копия программы LeakTest является на

самом деле другой программой, и блокирует ее. Вы также должны увидеть всплывающее диалоговое окно вашего персонального брандмауэра, информирующее вас о попытке соединения. Если оно не появится, значит, либо настройки безопасности вашего персонального брандмауэра слишком низкие, либо он не может обнаружить взлом безопасности.

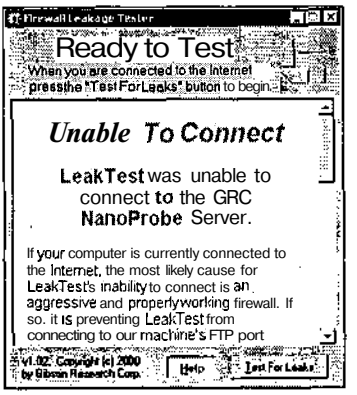


Рисунок 9.14. Соединение с Интернетом программы LeakTest было блокировано персональным брандмауэром

На рисунке 9.15 показано сообщение, выдаваемое программой LeakTest, в случае, если ей удалось пройти через ваш персональный брандмауэр.

Последние версии персональных брандмауэров McAfee и ZoneAlarm успешно справляются с блокировкой утилиты LeakTest. Однако предыдущие версии персонального брандмауэра McAfee, вышедшие до версии 2.15, показали себя уязвимыми перед этим тестом.

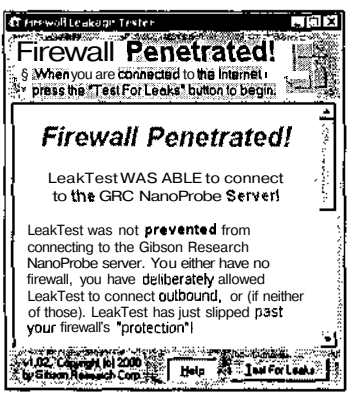


Рисунок 9.15. Утилита LeakTest проникла сквозь вашу защиту и послала информацию другому компьютеру в Интернете

Если вы используете более раннюю версию персонального брандмауэра McAfee, чем версия 2.15, вы должны немедленно обновить ваш персональный брандмауэр!

Программа LeakTest также может работать в невидимом режиме, который вы можете включить, нажав и удерживая клавишу Shift, одновременно нажав кнопку Test For Leaks (Проверка утечек). При работе в невидимом режиме название в строке заголовка LeakTest изменяется, указывая на это. К сожалению, нет никакой информации о разнице между этими двумя режимами.

Окончательный анализ

Персональный брандмауэр - относительно новый программный и аппаратный продукт. Персональные брандмауэры постоянно улучшаются и обновляются. Некоторые брандмауэры более развиты, чем другие, и вы не должны думать, что все брандмауэры одинаковы. Поэтому важно, чтобы вы протестировали ваш персональный брандмауэр, как только вы его установите и запустите. Если он работает неудовлетворительно, это может означать, что настройки безопасности установлены на слишком низком уровне, и вы можете повысить их, чтобы увеличить уровень защиты. Однако также возможно то, что персональный брандмауэр еще не подготовлен для большой нагрузки в настоящее время. Тесты, перечисленные в главе, а также в приложении Б, предоставляют вам инструменты для определения ваших собственных задач тестирования.

10

Навыки путешественников по сети, осознающих необходимость повышения безопасности

Интернет помог людям совершить огромный скачок в области общения и передачи информации. Он позволяет людям по всему миру общаться и получать информацию, что еще несколько лет назад было почти невозможно. Путешествие по сети World Wide Web зависит от вашего личного опыта, ведь так легко потеряться среди миллионов Web-сайтов, ожидающих вас. Однако очень важно, чтобы вы помнили, что даже когда вы в полном одиночестве путешествуете по глобальной сети, вы на самом деле никогда не одиноки. Вас окружают миллионы других людей, совместно пользующихся и работающих с одной и той же сетью.

При поверхностном рассмотрении персональный брандмауэр, возможно, кажется многим пользователям не очень нужным устройством или программой. Он не предоставляет явную помощь, например, такую, как помощь в подготовке налоговых деклараций или убийстве космических пришельцев. Он не помогает в создании и публикации Web-страниц и не дает вам возможности зарабатывать деньги. Он просто занимает место в вашем компьютере, обычно совершенно незаметно. Поэтому крайне важно, чтобы люди имели представление об опасностях, окружающих их в сети.

В этой книге предпринята попытка продемонстрировать опасности, которым подвергается ваш компьютер при взаимодействии с Интернетом, особенно когда вы соединяетесь с помощью кабельного или цифрового высокоскоростного соединения, и показать вам, как вы можете использовать персональный брандмауэр для своей защиты. Цель этой главы - предоставить вам дополнительные рекомендации, которые вы можете использовать для повышения уровня вашей безопасности.

В этой главе вы:

- узнаете, как получить самую последнюю версию операционной системы Microsoft;
- узнаете больше об угрозах, исходящих от компьютерных вирусов, и о том, как вы можете попробовать защитить себя от них;
- узнаете о важности поддержания уровня вашей сетевой защиты на современном уровне;
- исследуете другие виды угроз, исходящих из Интернета, и то, как вы можете бороться с ними.

Обновление вашего персонального брандмауэра

БОЛЬШИНСТВО персональных брандмауэров имеют средства периодического самообновления. Поскольку они - ваше основное средство защиты от хакеров в Интернете, очень важно, чтобы вы постоянно обновляли ваш персональный брандмауэр. Все три персональных брандмауэра, описанных в этой книге, дают вам возможность использовать обновления. Процесс обновления каждого из них кратко описывается в следующих разделах.

Обновление персонального брандмауэра McAfee

Когда вы покупаете персональный брандмауэр McAfee, вам автоматически предоставляется право на одно бесплатное обновление продукта, которое должно произойти в течение 90 дней после покупки. Этим гарантируется, что у вас запущена самая последняя версия этого брандмауэра. Брандмауэр McAfee позволяет загружать обновления со своего Web-сайта.

К сожалению, персональный брандмауэр McAfee не имеет встроенного механизма уведомления о появлении нового обновления. Поэтому вы должны посещать сайт *www.mcafee.com* и проверять его самостоятельно. Вы можете применить обновление, которое вы загрузили, дважды нажав на него и следуя появляющимся инструкциям. Вам, вероятно, придется потом перезагрузить компьютер.

Обновление брандмауэра BlackICE Defender

Вы можете настроить брандмауэр BlacklCE Defender так, чтобы он уведомлял вас о появлении нового обновления этого персонального брандмауэра, как описано в главе 7 "BlacklCE Defender". Брандмауэр BlacklCE Defender уведомляет вас, что обновление доступно, показывая иконку NI в верхнем правом углу главного диалогового окна. Чтобы применить обновление, просто нажмите на иконку и следуйте инструкциям, которые появятся.

Если вы предпочитаете, вы можете отключить свойство автоматического обновления и выполнять проверку вручную. Чтобы запустить обновление вручную, нажмите опцию Download Update (Загрузить обновление) в меню Tools (Инструменты) брандмауэра BlacklCE Defender. Брандмауэр соединится с Web-сайтом Network ICE и определит, доступно ли новое обновление. Если таковое есть, вам предложат установить его.

Обновление брандмауэра ZoneAlarm

Вы можете установить брандмауэр ZoneAlarm на уведомление вас о появлении обновления персонального брандмауэра, как описано в главе 8 "ZoneAlarm". Чтобы загрузить обновления с Web-сайта ZoneLabs, вы должны сначала зарегистрировать вашу копию брандмауэра ZoneAlarm, что вы можете сделать во время установки. Вы также можете запросить сайт ZoneLabs, чтобы он уведомлял вас каждый раз при появлении нового обновления.

Кроме того, вы можете вручную проверять новые обновления брандмауэра, нажимая опцию Check for Update (Проверить обновления) на панели Configuration (Конфигурация) брандмауэра ZoneAlarm. Брандмауэр ZoneAlarm затем соединяется с Web-сайтом ZoneLabs и определяет, существует ли новое обновление. ЕСЛИ оно есть, станет доступной кнопка Get Update (Получить обновление) на панели Configuration(Конфигурация). Нажмитеее, чтобы запустить процесс обновления.

Поддержка вашей операционной системы Microsoft на современном уровне

С появлением высокоскоростного доступа в Интернет люди начали понимать важность персональных брандмауэров. Однако даже большинство домашних пользователей, заботящихся о безопасности, часто забывают об одном из наиболее важных средств защиты: поддержке своей операционной системы на современном уровне.

Дыры в безопасности постоянно обнаруживаются в каждом программном продукте, включая вашу операционную систему. Microsoft активно принимается за решение этих проблем по мере их обнаружения. Затем компания распространяет на своем Web-сайте бесплатные настройки, обновления и служебные пакеты программ, которые вы можете загрузить и установить, чтобы закрыть эти дыры.

Вам, возможно, будет интересно, почему вам нужно беспокоиться о дырах в вашей операционной системе теперь, когда вы установили свой персональный брандмауэр. Как-никак, ничто не может проникнуть сквозь вашу систему безопасности, не так ли? Да, нужно на это надеяться. Однако время от времени хакеры открывают новые технологии проникновения в компьютерные систему. После того как обнаружены новые приемы хакеров, разработчик вашего персонального брандмауэра, скорее всего, быстро справится с ними. Тем не менее, пока вы не загрузите и не установите обновление, вы уязвимы перед новым видом атаки. Поэтому, если кто-либо взломает защиту вашего персонального брандмауэра, вы захотите удостовериться, что хакеру не стало легче работать с вашим компьютером. Вы можете сделать это, закрыв все известные дыры в вашей операционной системе.

С момента появления Windows 98 корпорация "Microsoft" интегрировала в свои операционные системы новое свойство, называемое Windows Update (Обновление Windows), которое помогает вам поддерживать вашу определенную операционную систему обновленной. Вы можете найти Windows Update в меню Windows Пуск. Когда вы нажмете на него, Windows откроет ваш Web-браузер и загрузит сайт Windows Update, который используется для вашей определенной операционной системы Microsoft.

Следующая методика описывает в общих чертах процесс применения свойства Windows Update (Обновление Windows), используя Windows 2000 Professional в качестве примера.

1. Нажмите Пуск, а затем Windows Update (Обновление Windows). Запустится Internet Explorer и загрузит сайт Microsoft Windows Update, соответствующий вашей операционной системе, как показано на рисунке 10.1.

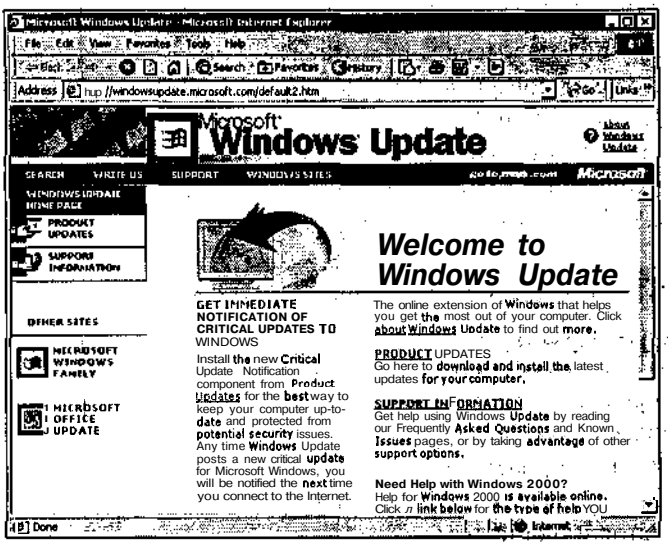


Рисунок 10.1. Web-сайт обновлений каждой операционной системы Windows является единственным местом, где можно найти и загрузить настройки для этой определенной операционной системы

2. Нажмите Products Updates (Обновление продукта). Если вы впервые используете Windows Update, появится диалоговое окно, показанное на рисунке 10.2. Нажмите Yes (Да).

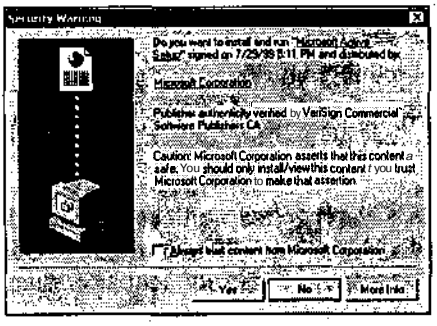


Рисунок 10.2. Если вы используете Windows Update впервые, появится диалоговое окно Security Warning (Предупреждение безопасности)

3. Будет произведен сбор информации о вашей операционной системе. Эта информация используется Web-сайтом Windows Update для определения того, какие обновления не использованы на вашем компьютере. Через несколько минут появится список программных обновлений, применимых к вашему компьютеру, как показано на рисунке 10.3.

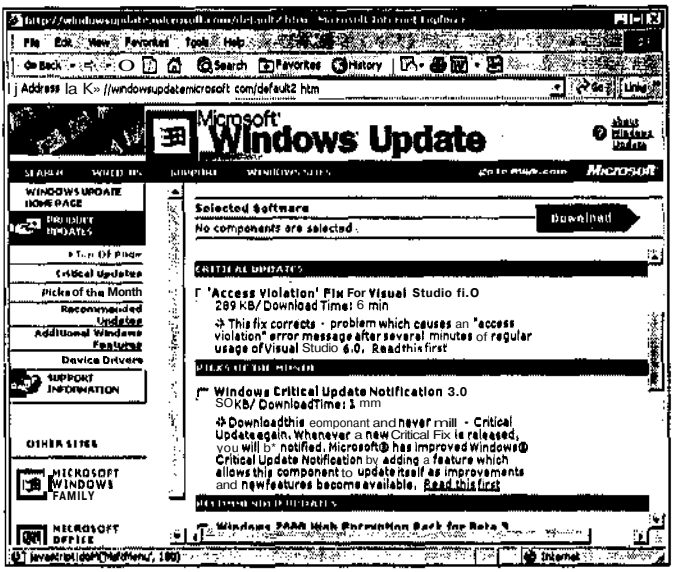


Рисунок 10.3. Сайт Windows Update анализирует вашу операционную систему и предоставляет список обновлений, необходимых для обновления вашего компьютера

Сайт Windows Update распределяет свой список доступных обновлений по различным категориям. Эти категории включают:

- Critical Updates (Наиболее важные обновления);
- Picks of the Month (Главные обновления месяца);
- Recommended Updates (Рекомендуемые обновления);
- Additional Windows Features (Дополнительные свойства Windows);
- Device Drivers (Драйверы устройств).

4. Обратите особое внимание на обновления в категориях Critical Updates (Наиболее важные обновления) и Recommended Updates (Рекомендуемые обновления) и на обновления, которые имеют отношение к безопасности. Если вы найдете такое обновление, вы должны применить его, выбрав обновление и нажав Download (Загрузить). Откроется Web-страница, запрашивающая подтверждение загрузки.
5. Нажмите Start Download (Начать загрузку), чтобы загрузить и применить обновление. Возможно, появится диалоговое окно лицензионного соглашения, это зависит от того, какое обновление вы выбрали. Если необходимо, нажмите Yes (Да), чтобы принять лицензионное соглашение.
6. Обновление, которое вы выбрали, загрузится и установится. В зайисимости от обновления вас, возможно, попросят перезагрузить компьютер.

Поддержание вашей операционной системы надежно защищенной

Операционные системы Windows не очень безопасны при соединении с Интернетом. Microsoft, очевидно, понимает это и начинает предпринимать шаги по устранению этого недостатка в своей новой операционной системе Windows XP Home. За исключением случаев, когда у вас есть домашняя сеть, вам не нужно подключать многие из сетевых компонентов, которые вы найдете установленными на вашем компьютере. Как показано в главе 4 "Защита сетей Windows", вам не нужен клиент для сетей Microsoft и общий доступ к файлам и принтерам Windows. Удалите их. Если у вас есть домашняя сеть, рассмотрите возможность использования NetBEUI в качестве протокола вашей домашней сети и удаления TCP/IP со всех компьютеров, за исключением того, который соединен с Интернетом. Если вы хотите использовать TCP/IP в качестве протокола вашей локальной сети, используйте брандмауэр, такой, как ZoneAlarm, который позволит вам отдельно определять настройки безопасности для домашней сети и соединения с Интернетом.

Другой вариант - рассмотреть покупку аппаратного брандмауэра и использовать его в качестве барьера между вашей домашней сетью и Интернетом. Просмотрите главу 11 "Домашние сети и общее подключение к Интернету" для получения более подробной информации о домашних сетях.

Если ваш бумажник и ваше компьютерное обеспечение могут выдержать это, вы должны также подумать об обновлении операционной системы Microsoft на более современную версию. Windows NT Workstation и Windows 2000 Professional требуют подтверждения права доступа к вашему компьютеру, независимо от того, получает ли он доступ через локальную сеть или через Интернет. Встроенная защита заблокирует учетные записи, когда хакер попытается запустить против них программу взлома пароля. Кроме того, эти две операционные системы позволяют вам применять разрешения безопасности ко всем файлам и папкам, делая их намного более защищенными, чем файлы и папки, хранящиеся в системе с Windows 95, 98 или Me.

Единственный недостаток операционных систем Windows NT и 2000 - это то, что они, возможно, не на все 100% совместимы со всем существующим программным обеспечением. Некоторые программы и многие игры не работают на компьютерах, на которых установлена одна из этих операционных систем. Однако Windows XP, который появился во второй половине 2001 года, совместим с вашим старым программным обеспечением, а также обладает безопасностью и производительностью, предоставляемыми Windows NT и 2000.

Вы также можете устранить еще одно уязвимое место компьютера, удалив любое Интернет-приложение, которое вы не используете. Например, если на вашем компьютере установлен Microsoft Personal Web Server, но вы его не используете, идите на Панель управления Windows и используйте утилиту Установка и удаление программ, чтобы удалить его.

Microsoft Personal Web Server - это "облегченный" Интернет-сервер. Он позволяет вам превратить домашний компьютер, имеющий соединение с Интернетом, в небольшой Web-сервер. Его свойства ограничены, но многие люди используют его для создания опытных образцов Web-сайтов, которые Они создают до загрузки их на реальный Web-сервер в Интернете. Когда Personal Web Server активен, он способен принимать входящие запросы соединения и является для хакеров потайной дверью на ваш компьютер.

Кроме того, вы можете повысить безопасность вашего компьютера, используя следующие процедуры:

- защищайте паролем общие ресурсы;
- используйте сложные пароли, которые включают смесь заглавных и строчных букв, а также цифр и специальных знаков;
- никогда не используйте имена или слова в качестве паролей, которые любая свободно доступная программа для взлома паролей может с легкостью взломать;
- никогда не используйте пароли, которые происходят от легко получаемой личной информации - такой, как ваше имя или имена ваших детей;
- выключайте ваш компьютер, когда вы его не используете, или запускайте блокировку вашим персональным брандмауэром. Как вариант, вы можете активизировать набор самых надежных уровней безопасности вашего персонального брандмауэра;
- воспользуйтесь преимуществами системы шифрования файлов (EFS), если у вас установлен Windows 2000 или XP, для зашифровки ваших важных файлов и папок;
- помните о зашифровке папки Windows C:\Temp при подключении EFS, поскольку Windows часто размещает копии файлов, с которыми вы работаете, в этой папке;
- не игнорируйте вашу безопасность только потому, что у вас коммутируемое соединение, Вы никогда не знаете, не войдете ли вы в сеть в неправильном месте и в неправильное время.

Использование антивирусных программ

Компьютерные вирусы - это программы, которые созданы для нападения на ваш компьютер различными способами. Прежде чем они смогут нанести удар, они должны проникнуть в вашу систему и инфицировать ее. Они могут сделать это различными способами. К примеру, компьютерные вирусы, как известно, прячутся в файлах и программах, загружаемых из Интернета, в приложениях к электронной почте или на дискетах. В отдельных редких случаях компьютерные вирусы могут даже появляться в программах, купленных в магазине.

Когда дело касается борьбы с компьютерными вирусами, у вас нет выбора, вам поможет только хорошая антивирусная программа и немного здравого смысла. В следующем списке представлен ряд золотых правил, которым вы должны следовать, чтобы предотвратить проникновение вирусов через вашу систему защиты:

- Старайтесь не загружать файлы и программы из Интернета, за исключением тех Web-сайтов, которые вы знаете и можете им доверять.
- в Никогда не загружайте программы с дискетки, полученной по почте от кого* либо, кого вы не знаете.
- Оставьте свою антивирусную программу работающей постояннр, и настройте ее проверять все.
- Загрузив приложение к временному файлу, проверьте его антивирусной программой, прежде чем открывать.
- Никогда не открывайте приложения к электронной почте, полученной ртнезнакомца.
- Никогда не открывайте непредвиденное приложение от друга, не удостоверившись сперва, что ваш друг действительно послал его вам.

Некоторые вирусы проникают в компьютерную адресную книгу и посылают себя всем, кто указан в ней - это означает, что вирус выглядит как нормальное сообщение от кого-либо, кого получатель знает!

Борьба с вирусами

Вирус - это программа, которая прячется внутри другой программы для того, чтобы проникнуть на ваш компьютер, где она затем также спрячется. Вирусы также могут проникать на ваш компьютер, прячась в загрузочном секторе дискеты. Загрузочный сектор занимает немного зарезервированного места на дискете или жестком диске, где могут поместиться маленькие исполняемые программы. Вирус, спрятавшийся там, выполняется при загрузке дискеты. После того как вирус активизировался, он ищет другое место на вашем жестком диске, где можно спрятаться, возможно, даже в загрузочном секторе.

Вирусы - это отвратительные, но умные программы, которые обычно не наносят удар немедленно. Как-никак, слишком поспешные действия могут облегчить их отслеживание и повлечь за собой обнаружение места, откуда они исходят. Они спокойно сидят до тех пор, пока не наступит указанное событие, такое, как определенная дата или перезагрузка компьютера. Вирус имеет Две основные функции. Это самовоспроизведение и распространение копий самого себя на другие компьютерные системы и сети и выполнение любых заданий, которые они созданы выполнять, таких, как очистка вашего жесткого диска или показ раздражающих маленьких сообщений.

Некоторые вирусы настолько умны, что способны наносить удар без обнаружения своего присутствия. Например, вирус может отыскать ваши крупноформатные таблицы и случайным образом изменять одно или два числа. Хотя результат такого изменения может быть ужасен, многие люди считают это изменение результатом своей собственной ошибки, произошедшей при наборе данных в таблицу. Поскольку эти программы так умны, единственный способ их поимки - это ваша антивирусная программа.

Вирусы могут распространяться различными способами, например:

- спрятавшись в файл, который рассылается множеству пользователей;
- спрятавшись в загрузочном секторе дискет;
- обнаружив вашу адресную книгу и используя ее записи для рассылки самого себя вашим друзьям и коллегам.

Недавно ставшая популярной новая форма вируса появилась благодаря языку Microsoft VBA (Visual Basic for Applications). Этот язык довольно легок для профессионала и внедряется во многие приложения Microsoft, включая Word и Excel. VBA предназначен для обеспечения пользователей простым в изучении языком сценариев, который может использоваться для создания макросов для автоматизации процесса работы с продуктами Microsoft Office.

Макрос - это небольшая программа, которая автоматизирует определенные программные операции. Эти вирусы обычно передаются как приложения к электронной почте и могут быть распознаны по их расширению .vbs. Появившись на компьютере пользователя, вирус нападает на его адресную книгу и посылает копии самого себя как приложения к адресам, указанным в книге. Эти электронные послания обычно имеют остроумные заголовки, которые содействуют тому, чтобы люди открывали их. Как только приложение .vbs открывается, запускается сценарий VBA и вирус готов вновь распространяться.

Остерегайтесь хитрых программ-вирусов, написанных с помощью языка сценариев VBScript, которые пытаются обмануть вас с помощью умных имен файлов. Например, кто-нибудь может попытаться обмануть вас, заставив думать, что это на самом деле документ Microsoft Word, дав вирусу название, такое, как имя файла.doc.vbs. Документы Microsoft Word имеют расширение .doc. Однако операционная система Microsoft позволяет именам файлов содержать точки и только текст после последней точки в имени файла рассматривается как его расширение. Невнимательно взглянув, многие люди видят часть имени файла .doc и не замечают того факта, что настоящее расширение файла .vbs.

Макросы VBA - это не особо сложные программы и могут состоять всего лишь из нескольких строчек программного кода. Программы Microsoft Office под-

держивают использование макросов. Например, вы можете создать макрос для Microsoft Excel 2000, запустив Excel и выбрав опцию Макрос в меню Сервис, а затем выбрав одну из появившихся опций подменю, как показано на рисунке 10.4.

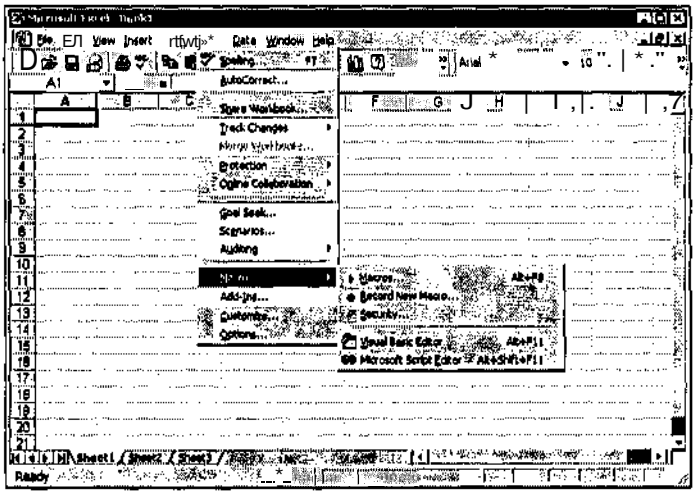


Рисунок 10.4. Создание макроса с помощью Microsoft Excel 2000

Код VBA также может быть внедрен в такие документы, как файлы Microsoft Word или Excel. Это означает, что даже файлы с расширением .doc или .xls могут содержать вирусы.

Если вы не пишете сценарии и у вас нет других программ, которые от них зависят, вы можете отключить поддержку VBA в Windows, удалив Windows Script Host по следующей методике:

1. Нажмите Пуск, Настройка, а затем Панель управления.
2. Дважды нажмите на Установка и удаление программ.
3. Выберите окно свойств Установка Windows (Setup).
4. Дважды нажмите группу Стандартные (Accessories).
5. Удалите Сервер сценариев (Windows Script Host) и нажмите OK.

Удаление Windows Script Host - довольно жесткий процесс и может привести к неправильной работе других нужных программ. Как-никак, не все программы с расширением .vbs являются вирусами. На самом деле лишь очень малая их часть.

Персональный брандмауэр ZoneAlarm предоставляет другую опцию под названием MailSafe. Она дает возможность изолировать все сообщения электронной почты, содержащие приложения с расширением .vbs, и выяснить их происхождение прежде чем решить, хотите ли вы запустить их. Для получения более подробной информации о MailSafe смотрите главу 8.

Борьба с "Троянскими конями"

"Троянский конь" – это тип вируса, который проникает на ваш компьютер и разыскивает вашу личную информацию, которую затем пытается переслать своему создателю. Это кардинально отличает его от стандартных вирусов, поскольку последнее; что он хочет сделать, это привлечь ваше внимание, нарушив работу вашего компьютера.

Персональные брандмауэры McAfee и ZoneAlarm имеют функцию фильтрации приложений, которая позволяет вам указывать, каким приложениям позволить пройти через брандмауэр, а каким нет. Каждый раз, когда неизвестное приложение, такое, как "Троянский конь", попытается соединиться с Интернетом, оно будет временно блокировано, и у вас запросят инструкции. Это дает вам возможность изолировать и удалять программы "Троянский конь". Поскольку брандмауэр BlackICE Defender работает на основе других предпосылок безопасности, он не дает вам возможности указывать доверяемые и не доверяемые приложения.

Наилучший вариантзащиты от программ "Троянский конь"- использовать персональный брандмауэр в сочетании с антивирусной программой. Антивирусная программа старается не пропускать программы "Троянский конь" на ваш компьютер. Если программа "Троянский конь" пройдет через вашу антивирусную программу, ваш персональный брандмауэр обнаружит и блокирует ее попытку связаться со своим создателем.

Не становитесь зомби - помогите предотвратить атаку "Распределенный отказ от обслуживания"

Зомби - это компьютер, на который хакер внедрил программу класса "Троянский конь", которая может быть удаленно активизирована и использована для включения компьютера в массовую атаку на Интернет-сервер. Ваш компьютер-зомби - наряду с десятками, сотнями и тысячами других компьютеров – инструктируют переполнять определенный Web-сайт запросами на обслуживание, не позволяя, в конечном счете, Интернет-сайту выполнять действительно необходимую работу. Лучший способ предотвратить это нападение на ваш компьютер - это установить персональный брандмауэр и поддерживать его постоянное обновление для защиты от последних типов атак "Распределенный отказ от обслуживания".

Берегитесь Cookie

Вы когда-нибудь интересовались тем, каким образом Web-сайты могут приветствовать вас по имени при его повторном посещении? Этот маленький трюк становится возможным благодаря файлам cookie. Cookie - это небольшая запись, которую Web-сайты могут сохранять на вашем компьютере, когда вы посещаете их сайты. Файл cookie может содержать информацию любого рода, включая предпочтения, которые вы установили на Web-сайтах, или ID и пароль, которые вы указали

при посещении сайта. Файл cookie может также хранить информацию о том, что вы делали на определенном Web-сайте. Например, файлы cookie могут отслеживать ссылки, на которые вы нажимали, или картинки, которые вы просмотрели. Короче говоря, файлы cookie могут записывать различную информацию о вашем поведении.

Как Microsoft Explorer, так и Netscape Communicator не очень хорошо работают с файлами cookie. По умолчанию оба браузера позволяют сохранять файлы cookie и извлекать из них нужную информацию. Оба браузера также позволяют вам отключать поддержку файлов cookie. Однако не все cookie плохие. Файлы cookie, которые запоминают ваши настройки пользователя или информацию, которую вы не хотите вводить каждый раз при посещении Web-сайта, очень полезны. Однако многие люди ненавидят использовать файлы cookie, которые позволяют Web-сайтам отслеживать их поведение, поскольку это на самом деле не их дело.

На рисунке 10.5 показано окно свойств Security (Безопасность) браузера Internet Explorer. По умолчанию выбрана Зона Интернета. Внизу окна свойств находится опция Security level for the Internet zone (Уровень безопасности для зоны Интернета). По умолчанию уровень безопасности устанавливается на Medium (Средний). При повышении его до High (Высокий) вы можете отключить все файлы cookie.

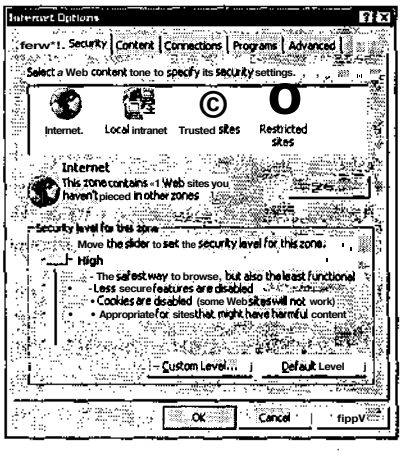


Рисунок 10.5. Конфигурирование поддержки файлов cookie браузера Internet Explorer

На рисунке 10.6 изображено диалоговое окно Preferences (Настройки) браузера Netscape Communicator. Настройка управления файлами cookie находится под категорией Advanced (Дополнительно).

Как вы можете видеть, Internet Explorer и Netscape Communicator предоставляют ограниченный контроль над файлами cookie. К счастью, существуют другие способы управления файлами cookie. Такие компании, как Norton и McAfee, создают программные продукты, предназначенные для управления тем, каким Web-сайтам разрешить сохранять файлы cookie на вашем компьютере и когда Web-сайтам разрешается извлекать информацию из этих файлов. Для получения информации о Norton Internet Security 2001 просмотрите сайт *www.norton.com*. Для получения информации о McAfee Watch Dog посетите сайт *www.mcafee.com*.

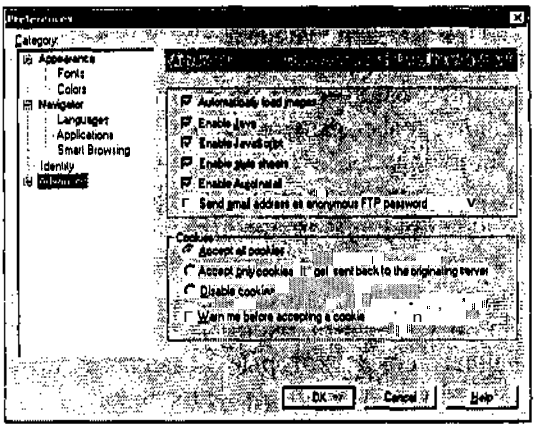


Рисунок 10.6. Конфигурирование настроек файлов cookie в браузере Netscape Communicator

Резервное копирование ваших данных

Хотя эта книга предназначена для того, чтобы помочь вам максимально повысить уровень вашей защиты при соединении с Интернетом, все равно существует возможность, что умный хакер найдет новый способ проникнуть на ваш компьютер. Если ваши личные данные были просмотрены или даже украдены, вы должны написать о преступлении своему провайдеру и, возможно, даже уполномоченным органам власти.

Если намерением хакера было просто удалить все с вашего жесткого диска или выполнить что-либо такое же подлое, вы всегда можете вернуть свои данные, использовав резервные копии, которые вы должны делать постоянно. Имея хороший набор резервных копий, вы всегда сможете вернуть свой компьютер первоначальное состояние.

Операционные системы Windows предоставляют встроенные программы резервирования. Кроме того, любое резервное устройство, которое вы купили, имеет свое собственное программное обеспечение. Хотя вы можете сделать резервную копию всего жесткого диска, все, что вам действительно нужно, это скопировать ваши данные. После того как вторая копия ваших данных сохранена в безопасном месте, все, что вы должны сделать, чтобы восстановить рабочее состояние компьютера, это переустановить вашу операционную систему и приложения с помощью компакт-дисков и дискет, на которых они находятся. Затем установите вашу программу резервного копирования и используйте ее для восстановления ваших данных в их первоначальном месте расположения на вашем жестком диске. Другой вариант: если у вас нет накопителя на магнитной ленте или другого устройства для резервирования, но есть пишущий CD-дисковод, вы можете использовать его для хранения резервной копии вашей личной информации.

Хотя резервное копирование не помешает хакерам красть информацию, оно может гарантировать, что вы никогда не потеряете рабочую информацию, и дает вам чувство безопасности при оставлении вашего компьютера соединенным с Интернетом на длительные периоды времени.

Будьте бдительны и часто проверяйте безопасность

Чтобы проверить свою защищенность, вы, наверное, захотите увидеть свой компьютер так, как его видят хакеры. Как показано в главе 9 "Насколько защищен ваш компьютер?", вы можете сделать это, запустив бесплатное Интернет-сканирование безопасности на вашем компьютере. В приложении Б "Другие Web-сайты, которые проверят вашу безопасность", перечисляется ряд Web-сайтов, которые предоставляют услуги бесплатного сканирования. Многие из этих сканеров проверят ваш компьютер менее чем за минуту. Вы должны подумать о запуске Интернет-сканирования вашего компьютера при возникновении одной из следующих ситуаций:

- чтобы протестировать результаты изменений в службах безопасности вашего персонального брандмауэра;
- каждый раз, когда вы устанавливаете новое программное обеспечение, которое не поставляется известным производителем программного обеспечения;
- каждый раз, когда вы подозреваете, что с вашего компьютера каким-либо образом произошла утечка информации или что на нем находится вирус, "Троянский конь", червь или похожая программа;
- каждый раз, когда вы замечаете, что на вашем кабельном или цифровом модеме горит световой индикатор, говорящий о подозрительной активности Интернета, когда вы не путешествуете по Интернету и не загружаете файл.

11

Домашние сети и обшее подключение к Интернету

В этой главе описываются основы настройки и защиты домашней сети с помощью комбинации аппаратных и программных персональных брандмауэров. Эта глава начинается с объяснения того, как конфигурируется типовая домашняя сеть. Вы получите базовые знания о создании своей собственной сети, включая то, как объединять сетевые ресурсы и получать доступ к таким ресурсам, как накопители на жестких дисках и принтеры.

После получения базовых знаний об организации домашних сетей вы увидите, как легко изменить сеть, чтобы включить общее подключение к высокоскоростному соединению с Интернетом. Кроме того, в главе представлен ряд опций и рекомендаций для защиты вашей сети с помощью персональных брандмауэров.

В этой главе вы:

- просмотрите основные свойства домашних сетей;
- а узнаете, как установить вашу собственную домашнюю сеть;
- *m* узнаете, как сделать общими ресурсы накопителей на дисках и принтеров;
- узнаете, как сделать общим подключение к высокоскоростному соединению с Интернетом;
- s узнаете о различных вариантах защиты соединения с Интернетом вашей домашней сети.

Что такое домашняя сеть?

Домашние сети - это просто небольшие локальные сети, состоящие из равноправных узлов. Сеть равноправных узлов (peer-to-peer network)* - это сеть, в которой все участвующие компьютеры равноправны и сами управляют своими настройками безопасности и управления. Она противоположна сети клиент-сервер, в которой центральный сервер или группа серверов управляет безопасностью сети. Корпоративные компьютерные сети созданы по образцу клиент-сервер и могут объединять до нескольких тысяч компьютеров. В отличие от них, обычные домашние сети состоят из 2-10 компьютеров. Компьютеры, на которых установлены операционные системы Microsoft, созданы для работы в любой сети.

Чтобы установить сеть типа клиент-сервер, вам нужно, чтобы, по крайней мере, на одном компьютере был установлен Microsoft Windows NT 4 Server,

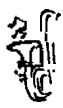
---

* Другое название - одноранговая сеть.

Windows 2000 Server или Windows XP Server. Эти операционные системы стоят намного дороже, требуют большего опыта и знаний в области сетей и слишком мощны для домашних пользователей.

Каждый компьютер в сети равноправных узлов сам отвечает за свою собственную безопасность. Для операционных систем Windows NT, 2000 и XP это означает, что вы можете настроить учетную запись пользователя на каждом компьютере, к которому вы хотите получить доступ из сети. Например, если ваша домашняя сеть состоит из четырех компьютеров, имеющих комбинацию этих трех операционных систем, вам нужно отдельно сконфигурировать учетные записи пользователей на каждой машине, чтобы с нее можно было войти в сеть. После того как вы войдете в сеть, сеть автоматически получит доступ к компьютеру.

Системы с Windows 95, 98 и Me не требуют от вас подтверждения права доступа с помощью предоставления имени пользователя и пароля. В действительности вы можете просто нажать Cancel (Отменить), когда вас попросят зарегистрироваться для входа в систему, и каждая из этих операционных систем с радостью предоставит вам доступ ко всем ресурсам на компьютере. Очевидно, сеть равноправных узлов, состоящая полностью из систем с Windows NT, 2000 и XP, является более защищенной, чем та, что включает другие операционные системы Windows.



Если у вас установлена, по крайней мере, одна система Windows NT, 2000 или XP, поместите на этот компьютер наиболее важные данные, где они будут в большей безопасности.

В создании домашней сети равноправных узлов присутствуют две фазы: аппаратная установка и программное конфигурирование.

В этой главе довольно кратко рассмотрен процесс создания домашней сети, и в ней предполагается, что у читателя уже есть небольшой предыдущий опыт. Если вы чувствуете, что нуждаетесь в дополнительной информации по вопросам, рассматриваемым в этой главе, прочтите *"Практическое руководство по равноправным сетям Windows Microsoft"* Дж. Ли Форда младшего, издательство "Que"; ISBN: 0-7897-2233-X.

Соединение ваших компьютеров в сеть

Вам понадобится кое-какое аппаратное оборудование для соединения всех ваших компьютеров в домашнюю сеть. Для каждого компьютера в сети вам придется купить сетевую плату и кабель RJ-45 (витая пара). Кроме того, вам понадобится купить небольшой сетевой концентратор (hub)*. Концентратор используется для соединения каждого компьютера с сетью. Этот тип сетевого соединения называ-

* Безусловно, существуют и другие технологии создания локальных (домашних) сетей, которые не рассматриваются в данной книге.

ется топология "звезда". Термин "топология" подразумевает физическое расположение вашей сети. В случае топологии "звезда" все компьютеры соединяются с центральной точкой. На рисунке 11.1 изображена типичная домашняя сеть, состоящая из четырех компьютеров и небольшого сетевого концентратора.

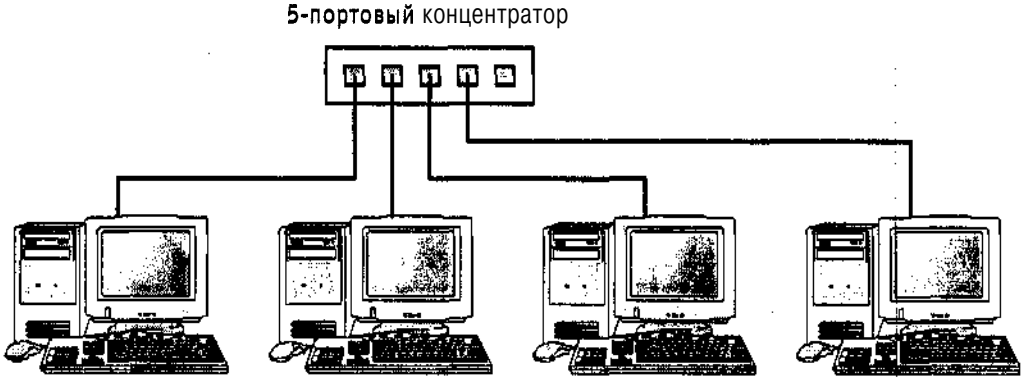


Рисунок 11.1. Изображение типичной домашней сети, состоящей из четырех персональных компьютеров и сетевого концентратора

Как вы можете видеть, концентратор является связующей точкой сети и позволяет каждому компьютеру взаимодействовать с каждым из остальных компьютеров. Устанавливайте вашу сеть по следующей методике:

1. Расположите в центре сетевой концентратор и подсоедините его к источнику питания.
2. Выключите каждый компьютер из сети и установите на нем сетевую плату.
3. Подсоедините каждый компьютер к концентратору с помощью кабеля RJ-45.
4. Включите каждый компьютер в сеть и позвольте стандарту Windows plug and play заняться дальнейшей установкой.

Программное конфигурирование сети

Как только стандарт plug and play сможет автоматически обнаружить ваши сетевые платы, операционная система Windows каждого компьютера должна автоматически установить их. Вас попросят вставить диск или дискету, которая поставляется с каждой сетевой платой, для того, чтобы установить программный драйвер, который необходим Windows для взаимодействия с сетевой платой.

В качестве части процесса установки сетевой платы каждая операционная система Windows автоматически сконфигурирует себя на соединение с сетями Microsoft. Со времени появления Windows 98 все операционные системы Microsoft создаются для основанной на TCP/IP автоматизации их соединения с сетью Microsoft типа клиент-сервер или равноправных узлов. В действитель-

ности вы обнаружите, что каждый компьютер автоматически конфигурирует свое сетевое соединение, оставляя на ваше усмотрение лишь несколько административных вопросов.

Вот что происходит. Ваш компьютер с Windows 98, Me, 2000 или XP обнаруживает новую сетевую плату. Затем он автоматически устанавливает следующее программное обеспечение:

- Программный драйвер сетевой платы - программное обеспечение, предоставляемое производителем сетевой карты, которое указывает Windows, как взаимодействовать с сетевой платой.
- TCP/IP - устанавливаемый Windows по умолчанию сетевой протокол.
- Клиент для сетей Microsoft - программное обеспечение, которое позволяет компьютеру общаться с другими компьютерами вашей домашней сети.

Когда TCP/IP установлен, он автоматически конфигурируется на поиск сервера DHCP в локальной сети и на запрос у него его IP-адреса. Поскольку это домашняя сеть, у вас не будет DHCP-сервера, каждый компьютер с Windows автоматически присвоит себе свою собственную конфигурацию TCP/IP. По умолчанию каждый компьютер присваивает себе IP-адрес между 169.254.0.1 и 169.254.0.255. Тем самым каждый компьютер размещается в сети TCP/IP 169.254.0.0. Причисляя себя к одной сети, каждый компьютер обеспечивает возможность общения с другими компьютерами в сети.

Если на одном из ваших компьютеров все еще установлен Windows 95, вам придется выполнить несколько дополнительных задач. Windows 95 должен автоматически использовать plug and play для обнаружения и установки сетевой платы. Однако вместо установки TCP/IP он устанавливает сетевой протокол NetBEUI. Поэтому вам придется вручную установить и сконфигурировать TCP/IP, что вы можете сделать из диалогового окна Сеть, расположенного на Панели управления Windows 95. Вам также придется вручную настроить конфигурацию TCP/IP компьютера. Убедитесь, что вы присвоили своему компьютеру с Windows 95 IP-адрес, расположенный в диапазоне 169.254.0.1 -169.254.0.255. Если вам необходима дополнительная помощь по конфигурированию TCP/IP в Windows 95, я предлагаю вам просмотреть "*Практическое руководство по равноправным сетям Microsoft Windows*", ISBN: 0-7897-2233-X.

После того как каждый компьютер с Windows сконфигурировал свою новую сетевую плату и соединение с сетью, ваша сеть должна быть готова к работе.

Вам не нужно беспокоиться о фактических IP-адресах, присвоенных вашим компьютерам. Однако, если вам просто интересно, вы можете узнать IP-адрес, присвоенный компьютеру, в Windows Me, 2000 или XP, напечатав **IPCONFIG** */ALL в* приглашении на ввод команды (command prompt) Windows. В системах Windows 95 и 98 введите команду **WINIPCFG**. Более подробная информация о том, как использовать эти команды, доступна в главе 2 "Высокоскоростные соединения с Интернетом означают повышенную уязвимость".

Вы можете протестировать возможность соединения сети, сидя за одним из компьютеров и проводя тестовый опрос (ping) IP-адресов других компьютеров сети. PING - это команда TCP/IP, которая проверяет взаимодействие двух компьютеров. Например, после вычисления IP-адреса, присвоенного другому компьютеру в сети, откройте приглашение на ввод команды Windows, нажав Пуск, Программы, Стандартные, а затем Приглашение на ввод команды (Сеанс MS DOS) и напечатав **PING 169.254.0.*X*** (*X* представляет собой последнюю часть IP-адреса другого компьютера) и нажмите Enter.

Сетевое администрирование

С этого момента домашняя сеть физически собрана, и каждый компьютер должен уметь общаться с каждым из остальных компьютеров с помощью TCP/IP. Однако, прежде чем вы сможете использовать вашу домашнюю сеть, вам необходимо выполнить несколько задач. Эти задачи включают:

- присваивание имени вашим компьютерам и настройку рабочей группы;
- подключение общего доступа к дискам и папкам;
- подключение общего доступа к принтерам.

Настройка рабочей группы и имен компьютеров

Равноправные сети Microsoft основываются на модели рабочих групп. Рабочая группа - это просто логическая организация компьютеров в группы. Размещая компьютеры по рабочим группам, вы можете облегчить членам одной рабочей группы поиск общих дисководов и принтеров друг друга. Например, когда вы дважды нажимаете на Network Neighborhood (Мое сетевое окружение) на компьютерах с Windows 95 или 98, первое, что вы увидите, это список всех компьютеров в вашей рабочей группе. Чтобы просмотреть список других рабочих групп, вы должны нажать на иконку Entire Network (Вся сеть). Подобным образом это происходит в других операционных системах Windows. Например, имея четыре компьютера, вы захотите организовать вашу сеть в две рабочие группы - родители и дети, - как изображено на рисунке 11.2. Вы можете сделать два ком-

пьютера, использующиеся детьми, членами рабочей группы Дети, а остальные два компьютера - членами рабочей группы Родители.

Однако устанавливать две рабочие группы обычно излишне в домашних сетях, достаточно одной-единственной рабочей группы. На рисунке 11.3 изображена домашняя сеть из четырех персональных компьютеров, все они являются членами одной рабочей группы.

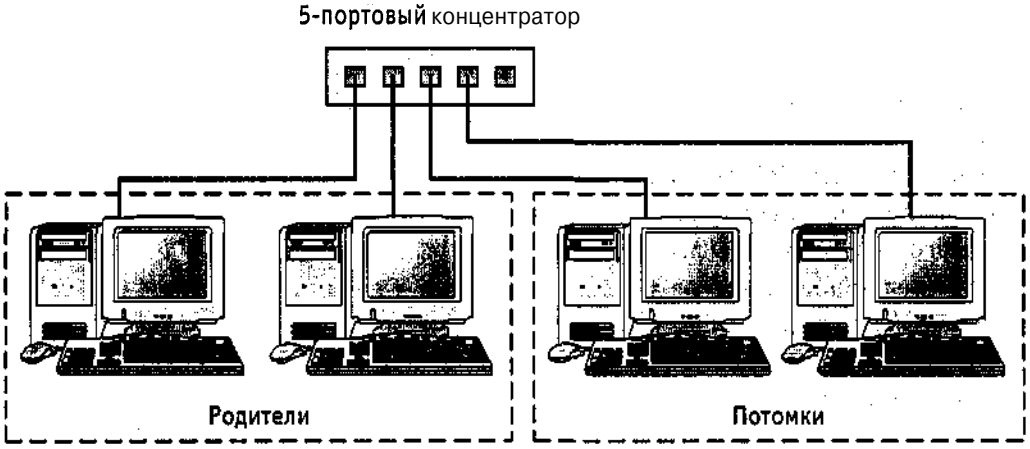


Рисунок 11.2. Организация вашей домашней сети в две рабочие группы

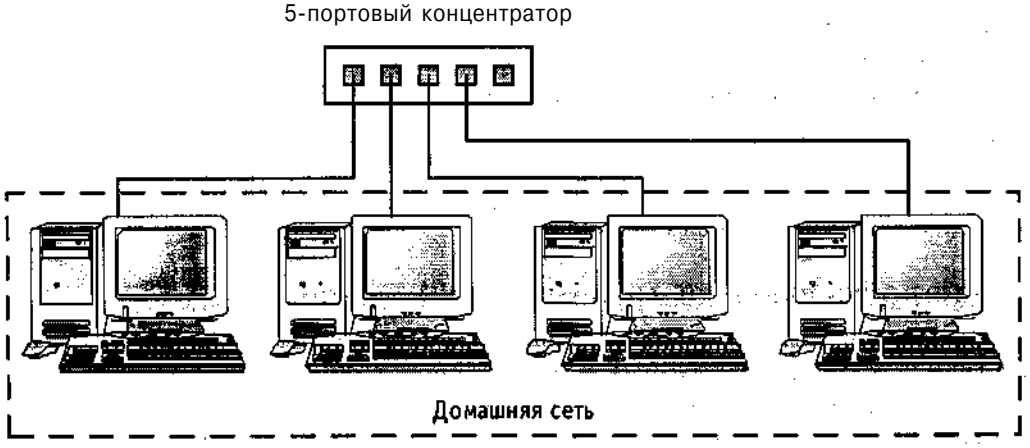


Рисунок 11.3. Изображение равноправной сети, состоящей из одной рабочей группы

Имя рабочей группы может быть каким угодно, если оно не превышает 15 знаков. Например, рабочая группа, изображенная на рисунке 11.3, имеет название FAMILYNET.

Кроме определения общей рабочей группы для вашей домашней сети, вы должны также обеспечить каждый компьютер уникальным именем. Это имя

может содержать до 15 буквенно-цифровых знаков. Следующая методика кратко описывает процесс конфигурирования имен компьютеров и рабочих групп на компьютерах с Windows 95, 98, Me или NT вашей домашней сети.

1. Нажмите Пуск, Настройка, Панель управления и дважды нажмите на иконку Сеть. Появится диалоговое окно Сеть.
2. Откройте окно свойств Идентификация, показанное на рисунке 11.4.
3. Введите имя компьютера и рабочей группы, которые вы хотите присвоить компьютеру, в полях Имя компьютера и Рабочая группа и нажмите OK.
4. Нажмите Да, когда вам предложат перезагрузить ваш компьютер.

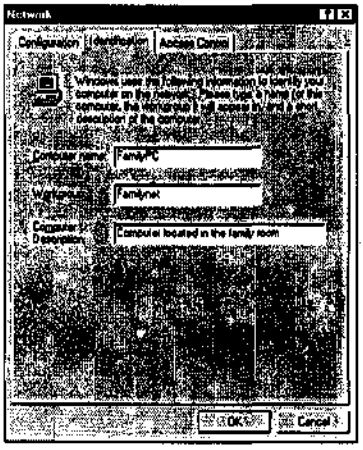


Рисунок 11.4. Присваивание имени вашему компьютеру и задание рабочей группы

Вы можете изменить имя и рабочую группу на компьютере с Windows 2000, открыв Панель управления, дважды нажав на Система, выбрав Идентификация сети и нажав Свойства.

Совместное использование сетевых ресурсов

Теперь, когда ваша сеть работает, имя и рабочая группа каждого компьютера настроены, настало время сконфигурировать ваши общие ресурсы. Существует три типа ресурсов, которыми вы, возможно, захотите поделиться. Это накопители на дисках, принтеры и ваше соединение с Интернетом. Совместное использование накопителей на дисках и принтеров описывается в следующих двух разделах. Общее подключение к Интернету описывается далее в этой главе.

Любая операционная система Windows может предоставлять общий доступ к своим дискам и принтерам. Однако прежде чем вы сможете совместно использовать накопители на дисках или принтеры в системах Windows 95, 98 или ME, вам придется активизировать общий доступ к файлам и принтерам. Вы можете сделать это по следующей методике:

1. Откройте Панель управления Windows и дважды нажмите на иконку Сеть. Откроется диалоговое окно Сеть. По умолчанию показывается окно свойств Конфигурация, показанное на рисунке 11.5.

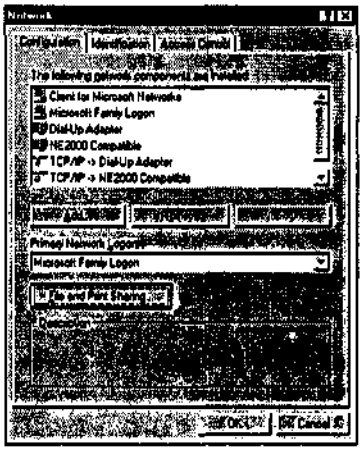


Рисунок 11.5. Диалоговое окно Сеть на компьютерах с Windows 95, 98 и Me

2. Нажмите Доступ к файлам и принтерам. Появится диалоговое окно Доступ к файлам и принтерам, показанное на рисунке 11.6.

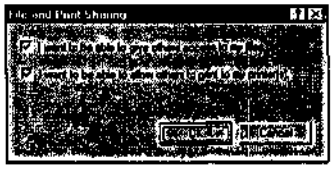


Рисунок 11.6. Подключение обшего доступа к файлам и принтерам на сетевом компьютере

3. Выберите Файлы этого компьютера можно сделать общими, чтобы активизировать общий доступ к накопителям на дисках и папкам, и Принтеры этого компьютера можно сделать общими, чтобы подключить общий доступ к принтерам. Нажмите OK.
4. Нажмите OK, чтобы закрыть диалоговое окно Сеть.
5. Нажмите Да, когда вам предложат перезагрузить ваш компьютер.

Теперь самое подходящее время вернуться к главе 4 "Защита сетей Windows" и просмотреть, как правильно защищать общий доступ к файлам и принтерам Windows. Таким образом **вы** подготовитесь к настройке общего подключения к Интернету, которое описывается далее в этой главе.

Общий доступ к накопителям на лисках

Вы можете предоставить остальным компьютерам вашей домашней сети доступ к любой папке или накопителю на дисках на вашем компьютере. Это великолепный способ предоставить дополнительное дисковое пространство сетевым компьютерам, у которых небольшие жесткие диски. Одна и та же методика используется для подключения общего доступа к флоппи-дисководам, жестким дискам, дисководам для компакт-дисков и папкам.

Процесс подключения общего доступа к дискам или папкам одинаков в любой операционной системе Windows, за исключением того, что Windows NT, 2000 и XP также позволяют вам применять разрешения безопасности к каждому общему ресурсу, чтобы ограничить доступ сетевых пользователей к нему.

Следующая методика описывает, как сделать общим дисковод в системе Windows Me.

1. Дважды нажмите на иконку Мой компьютер на рабочем столе Windows. Откроется окно Мой компьютер, показанное на рисунке 11.7.

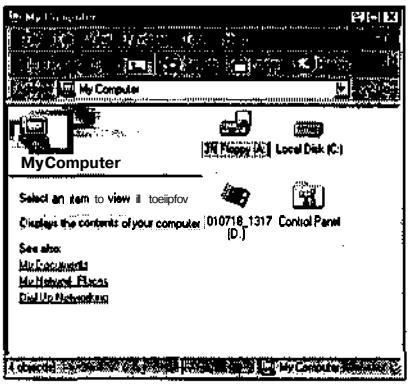


Рисунок 11.7. Окно Мой компьютер показывает, что на локальном компьютере нет общих устройств

2. Нажмите правой клавишей мыши на локальный жесткий диск и выберите в появившемся контекстном меню опцию Доступ. Откроется диалоговое окно Свойства для выбранного дисковода.

Если опции "Доступ" нет, значит, общий доступ к файлам и принтерам Windows не был включен.

3. По умолчанию выбирается опция Локальный ресурс (Not Shared). Чтобы сделать локальный дисковод общим, нажмите опцию Общий ресурс (Share As), как показано на рисунке 11.8. Тем самым вы активизируете несколько полей в диалоговом окне.

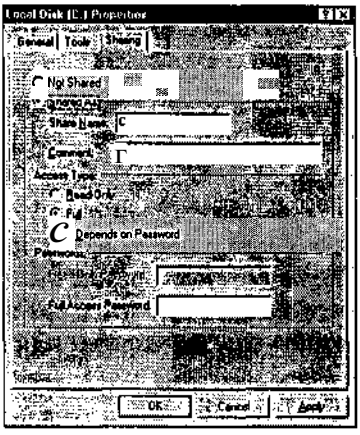


Рисунок 11.8. Подключение общего доступа к локальному жесткому диску на компьютере с Windows Me

4. Общему ресурсу будет предоставлено имя по умолчанию. Вы можете ввести более описательное имя, если хотите. Вы должны также ввести дополнительную информацию в поле Заметки. Выберите подходящий уровень доступа для общего дисковода. Существует три опции:
   - Только чтение (Read only) - позволяет любому пользователю сети получать доступ к диску и читать хранящиеся на нем файлы;
   - Полный (Full) - позволяет любому пользователю сети получать доступ к диску и читать, изменять и удалять его содержимое;
   - Определяется паролем (Depends on Password) - позволяет любому пользователю сети, который знает назначенный пароль, получать доступ для чтения или полный доступ к диску и его содержимому.
5. Нажмите OK - иконка, представляющая диск, изменится, появится изображение руки внизу ее.

Заметьте, что после того как вы установили общий доступ к дисководу, он стал видим для всех сетевых компьютеров и может быть виден с помощью одного из следующих средств:

- Windows Explorer;
- Internet Explorer;
- Сетевого окружения (Network Neighborhood);
- Различных диалоговых окон Windows.

Например, вы можете просмотреть общие накопители на дисках из окна Мое сетевое окружение другого компьютера с помощью следующей методики:

1. Дважды нажмите на иконку Мое сетевое окружение на рабочем столе Windows.

2. Дважды нажмите на иконку, представляющую компьютер, на котором был создан общий дисковод.
3. Вы увидите список всех общих ресурсов на выбранном компьютере. Чтобы просмотреть содержимое данного ресурса, дважды нажмите на него.

Подключение к сети вашего принтера

Подключить общий доступ к принтеру так же легко, как и настроить общий доступ к накопителю на дисках. Во-первых, зайдите на компьютер, где был установлен принтер, и убедитесь, что там подключен общий доступ к файлам и принтерам. Используйте следующую методику, чтобы сделать доступ к принтеру общим с другими компьютерами сети.

1. Откройте папку Принтеры, которая находится на Панели управления Windows.
2. Нажмите правой клавишей мыши на принтер и выберите из появившегося контекстного меню пункт Доступ.
3. Выберите Общий ресурс и введите сетевое имя ресурса. По выбору вы можете ввести заметки о принтере и применить пароль.
4. Нажмите OK. Иконка принтера изменится, внизу появится рука.

Чтобы распечатать что-то на принтере с другого компьютера домашней сети, вы должны сперва создать сетевое соединение с общим принтером. Следующая методика описывает, как это сделать с помощью мастера установки принтера Windows Me.

1. Нажмите Пуск, Настройка, Панель управления, Принтеры и затем на иконку Установить принтер, чтобы открыть мастера установки принтера.
2. Нажмите Далее.
3. Выберите Сетевой принтер и нажмите Далее, как показано на рисунке 11.9.

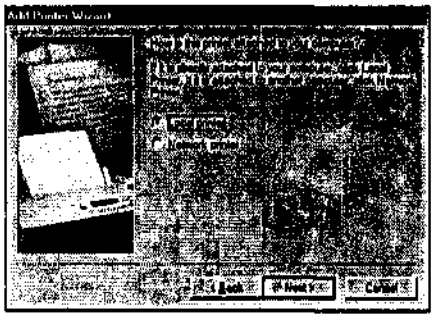


Рисунок 11.9. Мастер установки принтера поддерживает установку локальных и сетевых принтеров

4. Мастер установки принтера спросит о нахождении сетевого принтера. Введите путь в соответствии с методом Соглашения об универсальном назначении имен (Universal Naming Convention (UNC)). Если компьютер, на котором ус-

тановлен принтер, называется FamilyPC, а принтер называется ColorPTR, путь UNC будет \\FamilyPC\ColorPTR. Вы также можете нажать Обзор и просмотреть вашу домашнюю сеть, чтобы найти принтер. После определения местонахождения принтера нажмите OK.

5. Затем вам предложат указать производителя и модель принтера. После того как выберете производителя и тип принтера, нажмите Далее. Если производитель или тип принтера не указан, нажмите кнопку Установить с диска и, когда предложат, вставьте дискету или компакт-диск, на котором содержится драйвер принтера, предоставленный производителем принтера.

6. В конце введите имя, которое ваш компьютер будет использовать для обращения к сетевому принтеру. Если вы хотите, чтобы этот принтер стал компьютером по умолчанию*, нажмите Да. Иначе нажмите Нет. Затем нажмите Готово.

Соединение вашей домашней сети с Интернетом

После того как ваша домашняя сеть заработала, вы готовы установить общий доступ к вашему высокоскоростному соединению с Интернетом. До того как вы сделаете это, убедитесь, что следуете инструкциям, указанным в главе 4, чтобы свести к минимуму угрозы безопасности, исходящие от соединения домашней сети с Интернетом. Самый легкий способ соединить все компьютеры домашней сети с Интернетом - это установить сетевой концентратор с многопортовым кабельно-цифровым маршрутизатором. Кроме простоты, он также предоставляет возможность защиты вашей домашней сети с помощью встроенного свойства аппаратного брандмауэра. Это соединение, изображенное на рисунке 11.10, включает несколько шагов.

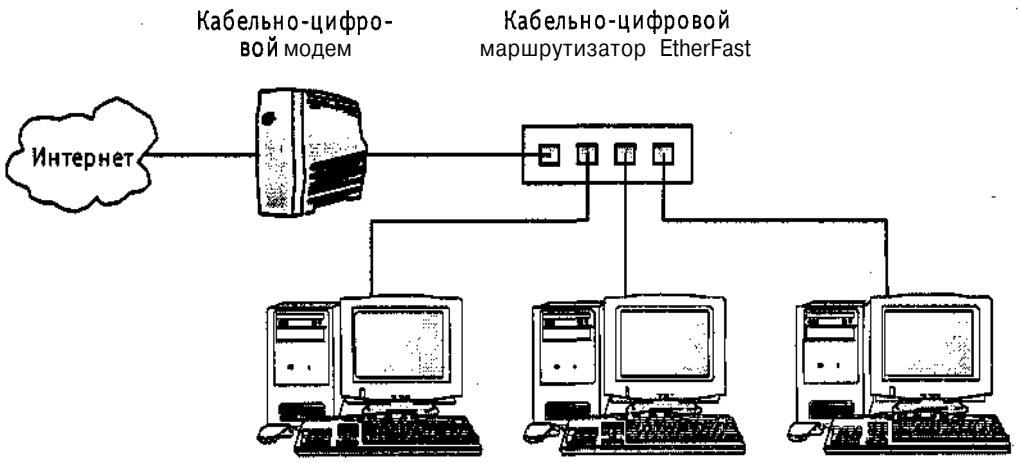


Рисунок 11.10. Подключение всех компьютеров домашней сети к высокоскоростному соединению с Интернетом

* Опечатка автора: не компьютером по умолчанию, а принтером по умолчанию.

Первый шаг - купить и установить кабельно-цифровой маршрутизатор вместо вашего сетевого концентратора. Как вы могли узнать из главы 5 "Аппаратные брандмауэры", одно из встроенных свойств этих устройств - возможность функционирования в качестве сетевого концентратора.

Второй шаг - настроить кабельно-цифровой маршрутизатор на вашего провайдера. Вы можете сделать это одним из двух способов. Вы можете либо настроить его с помощью MAC-адреса сетевой карты одного из компьютеров вашей сети, либо вы можете зарегистрировать MAC-адрес вашего кабельно-цифрового маршрутизатора. Если вы уже зарегистрировали MAC-адрес сетевой карты одного из ваших домашних компьютеров, самое легкое - скопировать MAC-адрес. В другом случае предпочтительнее использовать MAC-адрес маршрутизатора.

Не все провайдеры, предоставляющие кабельный или цифровой доступ в Интернет, требуют регистрации MAC-адреса, в этом случае вы можете пропустить процесс конфигурирования MAC-адреса вашего кабельно-цифрового маршрутизатора.

Ваш провайдер хотел бы, чтобы вы сохранили ваш старый сетевой концентратор и зарегистрировали MAC-адреса дополнительных сетевых компьютеров. Плата за дополнительные компьютеры обычно составляет от 6 до 7 долларов за компьютер в месяц. При домашней сети, состоящей из четырех компьютеров, это может значительно повлиять на вашу месячную плату. Чтобы совместно использовать ваше подключение к Интернету таким образом, вы должны связаться с вашим провайдером и сообщить ему MAC-адреса сетевых карт каждого из ваших сетевых компьютеров. Поскольку компьютеры с Windows автоматически настраиваются на получение динамических IP-адресов, все, что вам придется сделать, это подождать, пока ваш провайдер не сообщит, что дополнительные компьютеры были зарегистрированы. В этом случае вы должны установить программный персональный брандмауэр на каждый компьютер в сети, чтобы защитить вашу сеть.

Более легкий и дешевый способ - это избавиться от вашего старого сетевого концентратора и использовать новый кабельно-цифровой маршрутизатор и позволить его настройкам по умолчанию сконфигурировать вашу сеть для вас.

Кабельно-цифровые маршрутизаторы поставляются предварительно сконфигурированными на предоставление домашним сетям ряда услуг. В качестве сетевого концентратора он может поддерживать соединение с Интернетом всех компьютеров вашей домашней сети. Кабельно-цифровые маршрутизаторы также предоставляют услуги DHCP и преобразование NAT. Как вы узнали в главе 5, многопортовый кабельно-цифровой маршрутизатор автоматически конфигурируется на создание домашней сети, основанной на TCP/IP, с адресом 192.168.1.0. Маршрутизатор автоматически присваивает IP-адрес любому компьютеру, который его об этом попросит. Поскольку все операционные системы Windows, начиная с Windows 98, автоматически конфигурируются на поиск DHCP-сервера

до присвоения им их собственных IP-адресов, изменение сетевых адресов домашней сети с 169.254.0.0 на 192.168.1.0 должно быть понятно вам. За одним исключением, если у вас есть компьютеры с Windows 95 со статическими IP-адресами, вам придется переконфигурировать их на использование DHCP. Поскольку компьютеры с Windows ищут DHCP-серверы по умолчанию, все должно работать автоматически.

Последний шаг в настройке вашей сети - организация общего доступа к высокоскоростному соединению с Интернетом - предназначен для того, чтобы помочь каждому сетевому компьютеру установить свое собственное соединение с Интернетом. Вы можете сделать это, запустив мастера подключения к Интернету на каждом компьютере. Следующая методика описывает в общих чертах процесс установки соединения с Интернетом с помощью этого мастера.

1. Нажмите Пуск, Программы, Стандартные, Связь, а затем Мастер подключения к Интернету. Мастер откроет окно, показанное на рисунке 11.11.

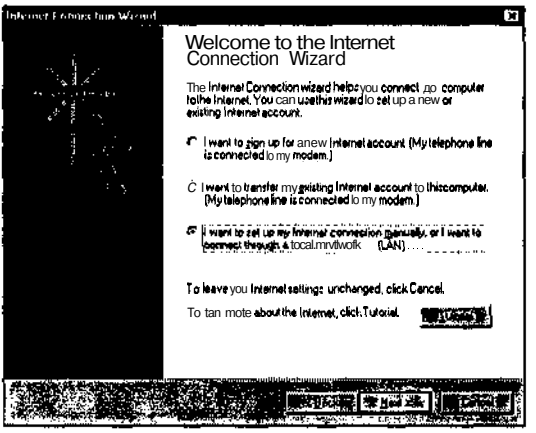


Рисунок 11.11. Настройка соединения с Интернетом каждого сетевого компьютера с помощью запуска мастера подключения к Интернету

2. Выберите Настроить соединение с Интернетом вручную или подключиться к Интернету через локальную сеть (I want to set up my Internet connection manually, or I want to connect through my local area network (LAN)) и нажмите Далее.

3. Затем вам предложат указать, как компьютер будет соединяться с Интернетом. Выберите Я подключаюсь к Интернету через локальную сеть (I connect through a local area network (LAN)) и нажмите Далее, как показано на рисунке 11.12.

4. Следующее диалоговое окно позволит вам задать мастеру способ, с помощью которого он сможет найти прокси-сервер сети. Это ваш кабельно-цифровой маршрутизатор. Убедитесь, что выбрано Автоматическое определение прокси-сервера (Automatic discovery of proxy server) и нажмите Далее, как показано на рисунке 11.13.

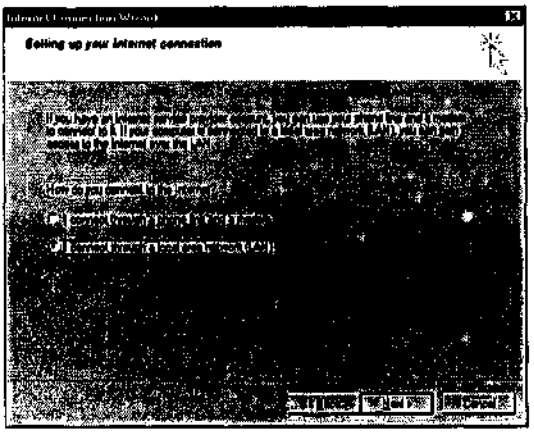


Рисунок **11.12.** Выбор вашей локальной сети в качестве средства подключения к Интернету

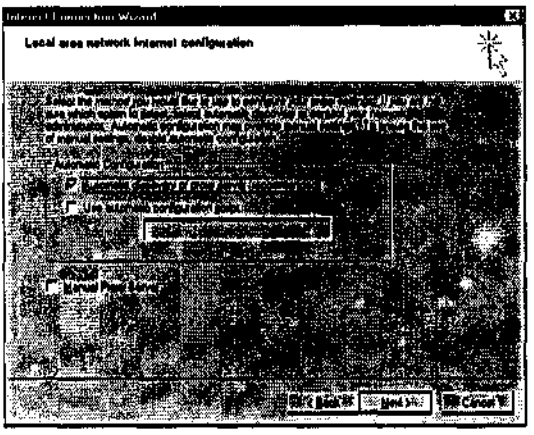


Рисунок **11.13.** Разрешение мастеру автоматически определить ваш **кабельно-цифровой** маршрутизатор

5. Нажмите Нет, когда вам предложат настроить учетную запись почты Интернета, и затем нажмите Далее.

6. Нажмите Готово. Автоматически запустится Internet Explorer и установит соединение с Интернетом.

Одно из **свойств** встроенного программного обеспечения **кабельно-цифрового** маршрутизатора, которое поможет наладить работу, это преобразование сетевых адресов (Network Address Translation) или NAT. Когда компьютер **вашей** домашней сети попытается соединиться с Web-сайтом, его запрос будет перехвачен вашим маршрутизатором. С помощью NAT маршрутизатор создает таблицу всех запросов и компьютеров, с которых они исходят. Маршрутизатор затем соединяется с указанным **Web-сайтом** и, когда Web-страница загружена, маршрутизатор **определяет,** какой компьютер из домашней сети был инициатором запроса,

и передает Web-страницы на этот компьютер. Таким образом, каждый сетевой компьютер работает так, как если бы был соединен с Интернетом напрямую, тогда как на самом деле соединен только один кабельно-цифровой маршрутизатор, как изображено на рисунке 11.14. Все, что может видеть ваш провайдер, это Интернет-трафик, приходящий на один IP-адрес и исходящий с него же. Очевиден тот факт, что ваш маршрутизатор осуществляет соединение от лица многих компьютеров.

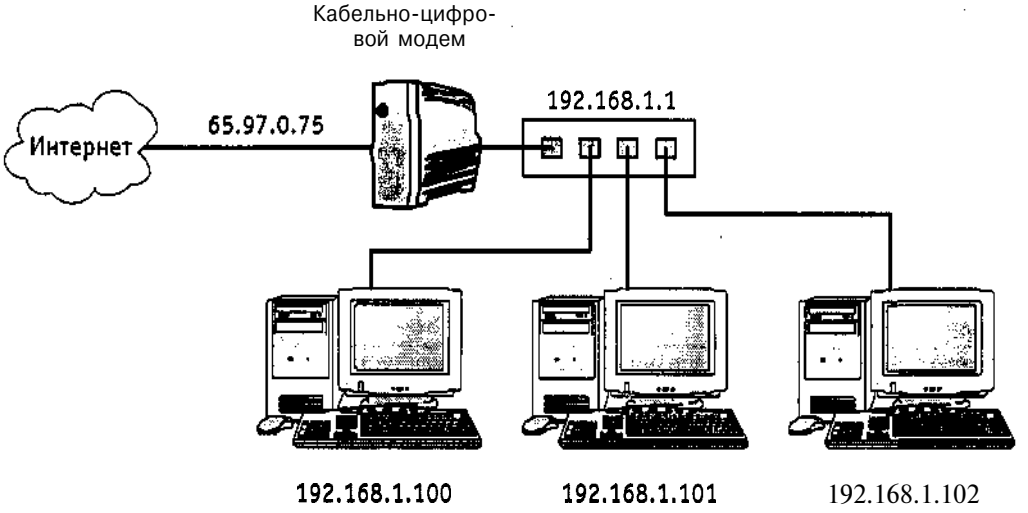


Рисунок 11.14. NAT позволяет вашему кабельно-цифровому маршрутизатору преобразовывать запросы соединения, устанавливаемые между вашей домашней сетью и Интернетом

Ваш кабельно-цифровой маршрутизатор затем получает два IP-адреса, связанные с этим. Первый - это внешний IP-адрес, присвоенный вашим провайдером. В этом примере это IP-адрес 65.97.0.75. Второй IP-адрес - это тот, что маршрутизатор использует для взаимодействия с вашей домашней сетью. Это IP-адрес 192.168.1.1. На рисунке 11.14 также показаны IP-адреса других компьютеров домашней сети. Эти адреса присвоены кабельно-цифровым маршрутизатором, выполняющим роль DHCP.

Например, если компьютер, которому ваш кабельно-цифровой маршрутизатор присвоил сетевой адрес 192.168.0.102, пытается соединиться с сайтом *www.microsoft.com*, маршрутизатор перехватывает запрос, отмечает, кто был инициатором его, затем делает запрос от своего имени. Когда загрузится главная Web-страница сайта *www.microsoft.com,* маршрутизатор определяет, какой сетевой компьютер создал запрос, и направляет Web-страницу на этот компьютер.

Повышение безопасности с помощью второго ряда брандмауэров

К данному моменту ваша домашняя сеть должна быть настроена И работать, и все ваши сетевые компьютеры должны иметь доступ к общему подключению к вашему высокоскоростному соединению с Интернетом. Кроме того, свойства персонального брандмауэра, встроенные в ваш маршрутизатор, защищают всю сеть. В этом разделе описывается, как вы можете дополнительно повысить вашу безопасность, установив персональные брандмауэры на каждый сетевой компьютер.

Кабельно-цифровые маршрутизаторы имеют многие из свойств аппаратного брандмауэра, такие, как способность прятать порты и блокировать внутренние компьютеры от получения доступа к Интернету. Однако, как показано в таблице 11.1, существует ряд свойств, имеющихся у программных брандмауэров, которых нет в этих аппаратных устройствах.

Таблица 11.1. Дополняющие друг друга свойства аппаратных и программных брандмауэров

Аппаратный брандмауэр	Программный брандмауэр
Установление портов в невидимый режим	Установление Портов в невидимый режим (все)
Поддержка подробной регистрации	Поддержка подробной регистрации (все)
Блокировка незатребованного входящего трафика	Блокировка незатребованного входящего трафика (все)
Блокировка внутренних IP-адресов	Внешние IP-адреса (ZoneAlarm и BlackICE)
Блокировка внутренних MAC-адресов	-
Блокировка портов TCP и UDP	Блокировка портов TCP и UDP (все)
Фильтры протоколов	Фильтры протоколов (ZoneAlarm и McAfee)
-	Фильтры приложений (ZoneAlarm и McAfee)
-	Анализ пакетов на предмет угроз (BlackICE)
-	Обнаружение программ "Троянский конь" (ZoneAlarm и McAfee)
-	Предупреждение о произошедшем событии (все)

Как вы можете видеть, хотя некоторые свойства повторяются, аппаратно и программно реализованные брандмауэры предоставляют дополняющие друг друга наборы услуг. Например, аппаратные брандмауэры могут блокировать IP-адреса Интернета, в то время как программные брандмауэры часто позволяют вам блокировать внешние IP-адреса. Аппаратные брандмауэры позволяют вам блокировать указанные порты TCP и UDP, в то время как программные брандмауэры часто позволяют вам блокировать отдельные приложения и указанные протоколы.

Как показано в таблице 11.1, у различных брандмауэров имеются различные свойства. Программные брандмауэры, такие, как McAfee Firewall и ZoneAlarm, фильтруют, основываясь на приложениях и протоколах, в то время как бранд-

мауэр BlackICE Defender анализирует пакеты данных на предмет определенных угроз. Кроме того, существует несколько других коренных различий в трех программных брандмауэрах, представленных в этой книге:

- **Брандмауэр McAfee** - этот брандмауэр позволяет вам конфигурировать отдельные настройки для коммутируемого и сетевого соединений, но не позволяет вам устанавливать отдельные настройки безопасности для домашней сети и соединения с Интернетом. Кроме того, этот брандмауэр не поддерживает общее подключение к Интернету Microsoft (Microsoft Internet Connection sharing), которое описывается в следующем разделе.
- **Брандмауэр BlacklCE Defender** - этот брандмауэр не различает соединение с Интернетом и соединение с домашней сетью, он не позволяет вам указывать различные настройки безопасности для вашего соединения с Интернетом и домашней сетью.
- **Брандмауэр ZoneAlarm** - этот брандмауэр позволяет вам устанавливать различные настройки безопасности для соединения с Интернетом и с домашней сетью, что делает его подходящим вариантом для компьютеров в вашей домашней сети.

Брандмауэры McAfee и BlacklCE Defender не позволяют вам устанавливать различные настройки безопасности для соединения с Интернетом и с домашней сетью. Брандмауэр ZoneAlarm, с другой стороны, предоставляет такую возможность, что продемонстрировано на рисунке 11.15.

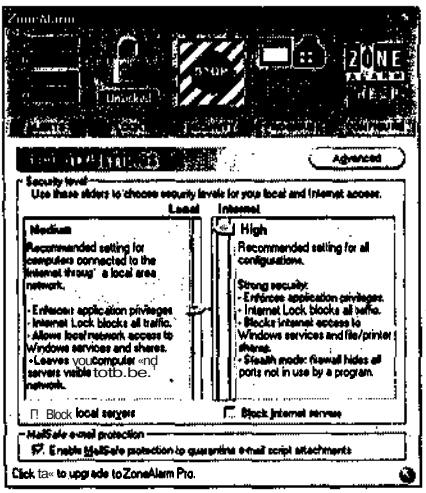


Рисунок 11.15. Брандмауэр ZoneAlarm дает вам возможность установить различные настройки безопасности для вашей домашней сети и соединения с Интернетом

Это свойство в сочетании с тем, что брандмауэр ZoneAlarm бесплатен для личного пользования, делает его великолепным вариантом для использования в вашей домашней сети. Как вы узнали в главе 8 "ZoneAlarm", вы можете вы-

брать одну из трех настроек безопасности для вашего соединения с Интернетом, и другую - для домашней сети. На рисунке 11.16 изображено, как вы можете использовать брандмауэр ZoneAlarm в домашней сети. Эта конструкция дает вам двойную защиту от Интернета, в то же время позволяя вашей домашней сети работать, не подвергаясь воздействию, по своим собственным настройкам безопасности.

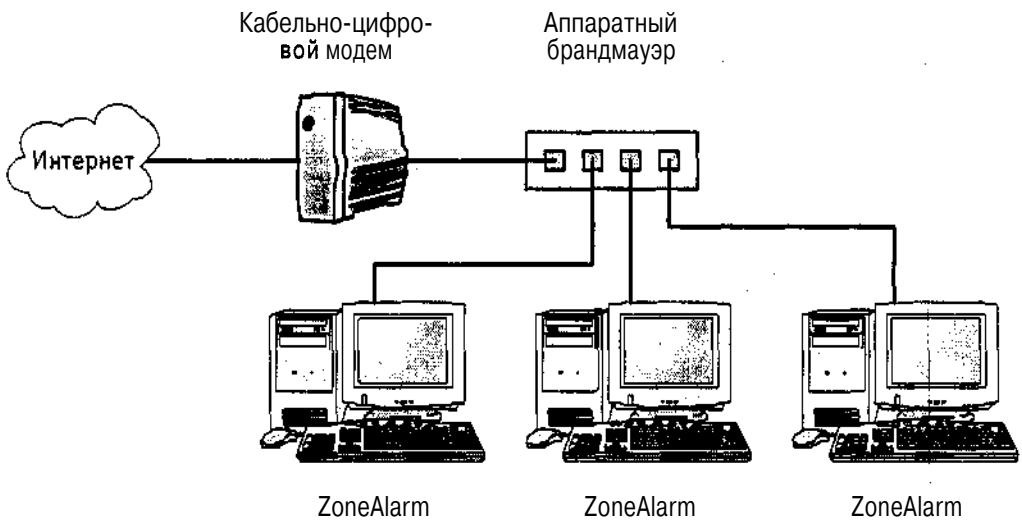


Рисунок 11.16. Использование брандмауэра ZoneAlarm для дополнительной зашиты ваших соединений с Интернетом и домашней сетью

Общее подключение к Интернету Microsoft

Компания "Microsoft" предоставляет альтернативный способ, позволяющий компьютерам домашней сети совместно использовать высокоскоростное соединение с Интернетом. В этом случае требуется стандартный сетевой концентратор. Если вы когда-либо видели, как Общее подключение к Интернету Microsoft (Microsoft Internet Connection Sharing (ICS)) применяется для совместного пользования коммутируемым соединением с Интернетом, вы знаете, что оно позволяет вам конфигурировать коммутируемое соединение. Таким образом компьютер может делить его с другими домашними компьютерами с помощью сетевой карты компьютера, как показано на рисунке 11.17.

Общее подключение к Интернету Microsoft поддерживается в Windows 98 Second Edition, Windows Me и Windows 2000. Оно устанавливается и конфигурируется по-разному в каждой операционной системе. Вы можете обратиться в систему справочной информации Windows для получения инструкций по установке общего подключения к Интернету Microsoft для каждой операционной системы. В общем, вам, прежде всего, нужно установить общее подключение к Интернету с помощью утилиты Установка и удаление программ. Затем вы мо-

жете совместно использовать соединение. После того как оно сконфигурировано, общее подключение к Интернету Microsoft превращает компьютер в DHCP-сервер, который также предоставляет услуги NAT. Остальные сетевые компьютеры могут затем быть сконфигурированы на использование этого соединения с помощью мастера подключения к Интернету,

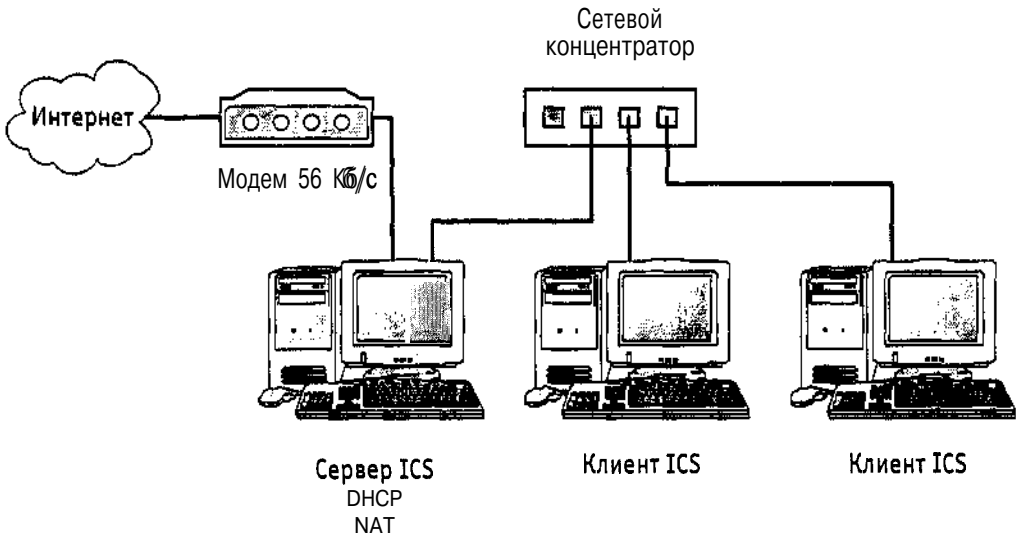


Рисунок 11.17. Применение встроенного компонента Windows Общее подключение к Интернету для совместного пользования коммутируемым соединением

В настоящее время в домашней сети может быть только один активный сервер DHCP. Если вы решили использовать общее подключение к Интернету Microsoft, чтобы совместно использовать ваше подключение к Интернету, вам нужно использовать стандартный сетевой концентратор или отключить службу DHCP на вашем кабельно-цифровом маршрутизаторе.

Существует ряд приложений, таких как WinGate (www.wingate.com), которые также позволяют вам совместно с вашей домашней сетью использовать соединение с Интернетом.

Общее подключение к Интернету Microsoft более сложно конфигурировать при использовании его для совместного использования широкополосного соединения. Как показано на рисунке 11.18, вам нужно установить две сетевые платы на компьютер, на котором установлено общее подключение к Интернету Microsoft. Обе сетевые платы должны соединяться с сетевым концентратором. Одна плата должна быть установлена для управления соединением с Интернетом, а вторая сетевая плата предоставляет возможность обычного сетевого со-

единения. Вы можете затем сконфигурировать ваш компьютер на совместное использование общего подключения к Интернету Microsoft.

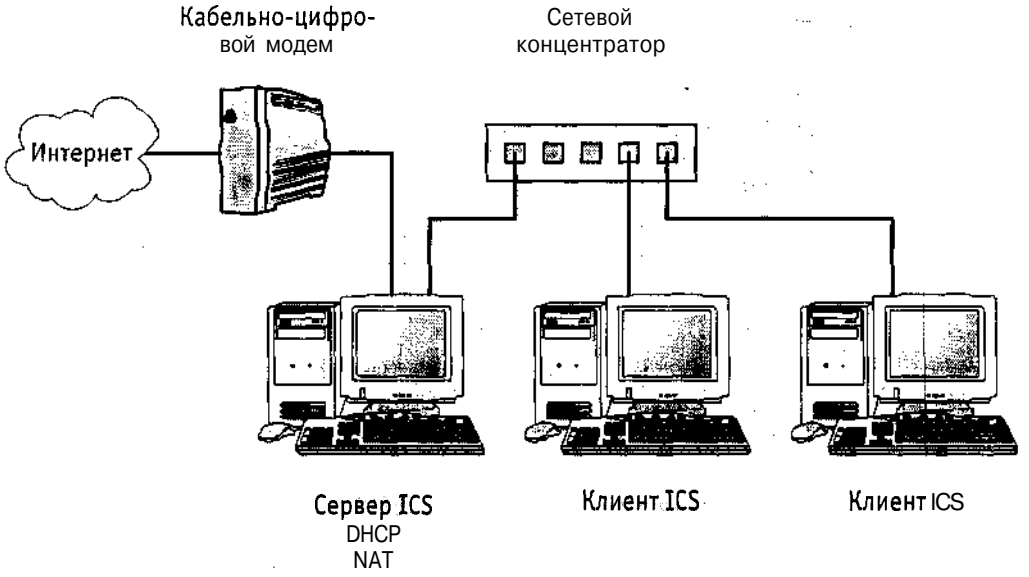


Рисунок 11.18. Применение встроенного компонента Windows Общее подключение к Интернету для совместного пользования коммутируемым соединением через широкополосное соединение требует установки двух сетевых плат

Установка соединения с двумя сетевыми платами и запуск общего подключения к Интернету Microsoft предоставляет общий доступ к Интернету с защитой персонального брандмауэра. Вы должны установить, как минимум, программный персональный брандмауэр на компьютер, предоставляющий общее соединение с Интернетом. Чтобы получить еще большую защиту, вы должны подумать об установке персонального брандмауэра на каждый компьютер в сети.

Брандмауэр McAfee не поддерживает общее подключение к Интернету Microsoft.

Зашита домашних сетей с помошью NetBEUI

На рисунке 11.19 показан другой вариант конфигурирования домашней сети. В этом примере TCP/IP разрешается только на компьютере, требующем доступа в Интернет, что делает домашнюю сеть более защищенной. Протокол NetBEUI с другой стороны устанавливается на каждый сетевой компьютер. Поскольку протокол NetBEUI немаршрутизируемый, хакеры не могут проникать в любой компьютер сети, за исключением того, на котором установлен TCP/IP. Компьютер с соединением с Интернетом может затем быть защищен с помощью установки

персонального брандмауэра. Дополнительная защита может быть применена с помощью замены сетевого концентратора кабельно-цифровым маршрутизатором.

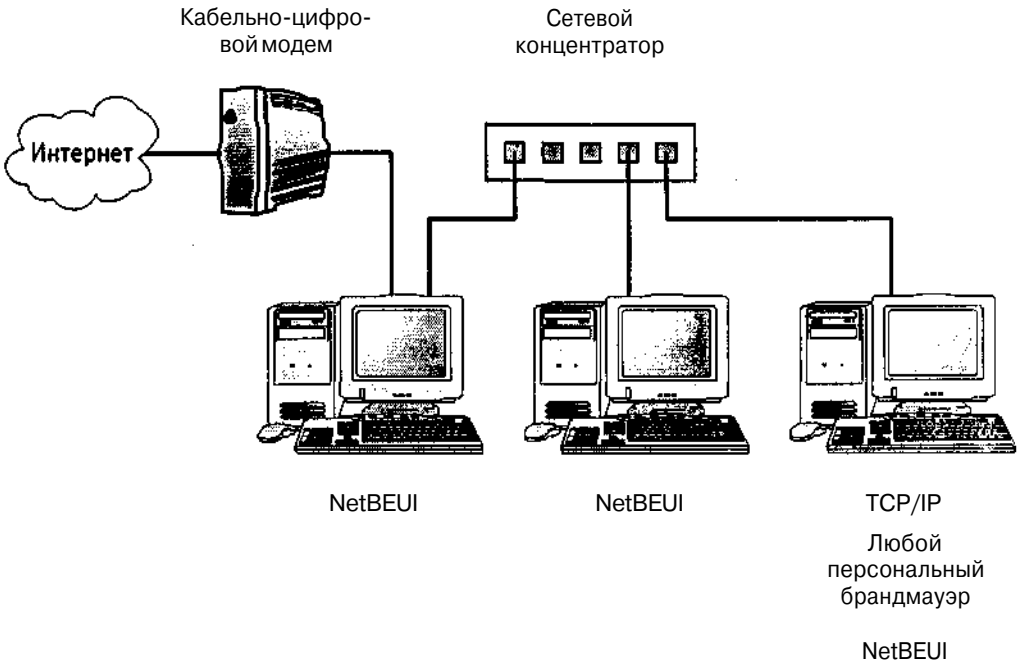


Рисунок 11.19. Использование протокола NetBEUI для отделения вашей сети от соединения с Интернетом

A

Другие брандмауэры

В этом приложении приводится обзор семи дополнительных программных брандмауэров, которые вы, возможно, будете рассматривать при покупке вашего собственного персонального брандмауэра. В то время как некоторые из этих брандмауэров могут быть не так известны, как три персональных брандмауэра, рассмотренных ранее в этой книге, большинство предоставляют такой же уровень защиты и также эффективны. В этом приложении приводится описание каждого персонального брандмауэра и перечислены их свойства. Кроме того, вы найдете указания на Web-сайты каждого продукта, на которых вы сможете получить дополнительную информацию.

Это брандмауэры:

- Aladdin Knowledge Systems eSafe Desktop 2.2;
- Norton Personal Firewall 2000;
- PGP Desktop Security 7.0;
- Symantec Desktop Firewall 2.0;
- Sygate Personal Firewall;
- ConSeal PC Firewall;
- Tiny Wall Personal Firewall.

Брандмауэр Aladdin Knowledge Systems eSafe Desktop 3.0

Брандмауэр Aladdin Knowledge Systems eSafe Desktop 3.0 предоставляется компанией "Aladdin Knowledge Systems", его можно найти на сайте *www.eAladdin.com/esafe*, показанном на рисунке АЛ.

Он бесплатен для личного пользования и имеет ряд свойств, включая:

- встроенное антивирусное приложение;
- фильтр Интернет-содержимого;
- возможности защиты рабочего стола;
- возможности персонального брандмауэра.

Возможности персонального брандмауэра включают способность фильтровать весь сетевой трафик. В него встроены четыре уровня настройки безопасности:

- Off (отключен);
- Low (низкий);

- Normal (нормальный);
- Extreme (экстремальный).

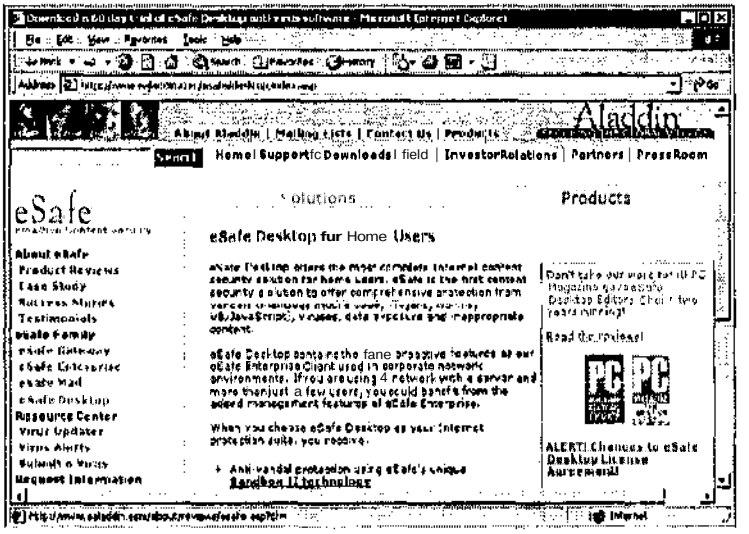


Рисунок **A.1.** Брандмауэр Aladdin Knowledge Systems eSafe Desktop 3.0

Этот персональный брандмауэр обращает основное внимание на ограничение портов и может быть немного более сложен в работе, чем некоторые другие персональные брандмауэры.

Персональный брандмауэр Norton Personal Firewall 2001

Персональный брандмауэр Norton Personal Firewall 2001 предоставляется компанией "Symantec", его можно найти на сайте *www.symantec.com,* как показано на рисунке A.2.

Это один из довольно дорогих персональных брандмауэров. Он имеет четыре уровня настройки безопасности:

- Minimal (минимальный);
- Medium (средний);
- и High (высокий);
- и Custom (выборочный).

Он включает мастера безопасности (Security Assistant wizard), который шаг за шагом проведет вас по процессу конфигурирования вашего персонального брандмауэра. Обнаружение вторжения (Intrusion detection) предупреждает вас о попытках просканировать ваши порты, оно объединено со свойством автома-

тической блокировки (AutoBlock), которое предназначено для блокировки любого компьютера, пытающегося запустить сканирование вашего компьютера.

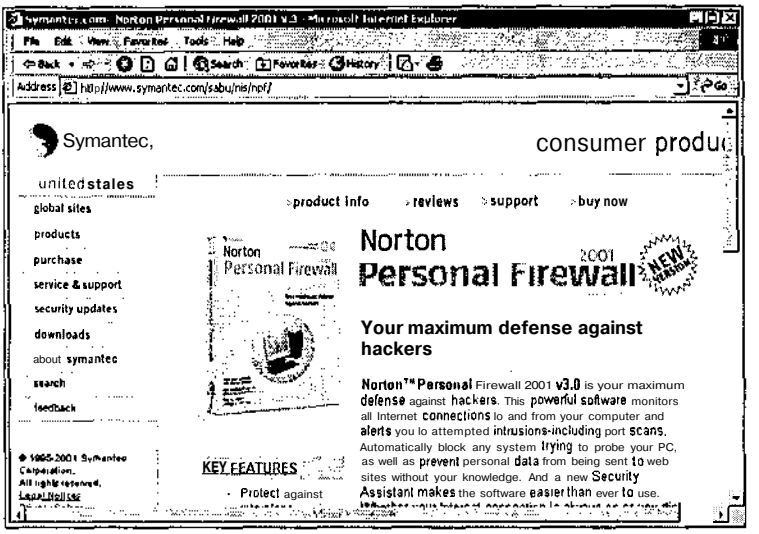


Рисунок А.2. Персональный брандмауэр Norton Personal Firewall 2001

Персональный брандмауэр PGP Desktop Security *7.0*

Брандмауэр PGP Desktop Security 7.0 предоставляется компанией "Network Associates", его можно найти на сайте *www.pgp.com,* как показано на рисунке А.3.

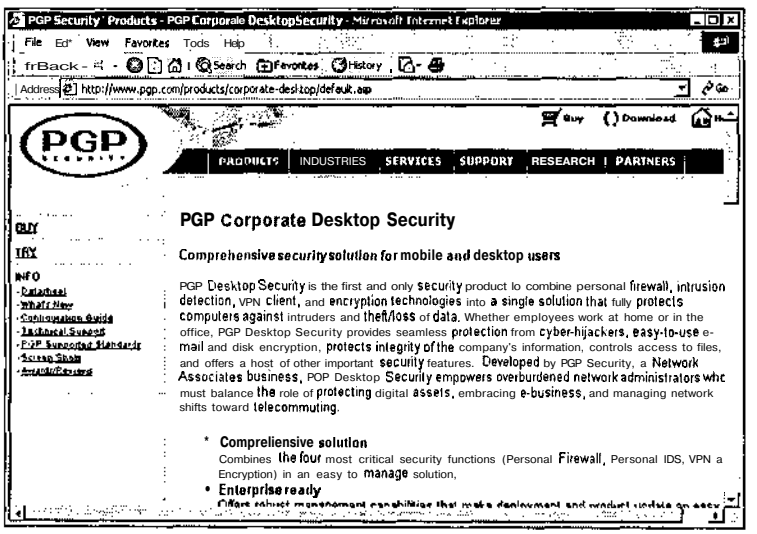


Рисунок А.3. Брандмауэр PGP Desktop Security 7.0

В дополнение к возможностям персонального брандмауэра этот продукт имеет ряд свойств, включая:

- поддержку Виртуальной частной сети (Virtual Private Networking(VPN));
- шифрование диска (Disk encryption);
- шифрование электронной почты (E-mail encryption);
- шифрование передающихся сообщений (Instant message encryption).

Этот персональный брандмауэр имеет свойство обнаружения вторжения ряда атак, может блокировать компьютеры, пытающиеся просканировать ваш компьютер, и даже пытается отслеживать взломщика. У него хорошо разработана система предупреждений и он может даже уведомлять вас о проблемах, связанных с электронной почтой.

Брандмауэр PGP Desktop Security 7.0, по-видимому, предназначен скорее для корпоративных пользователей, чем для домашних пользователей, и является самым дорогим из всех персональных брандмауэров, рассматриваемых в этой книге.

Брандмауэр Symantec Desktop Firewall 2.0

Брандмауэр Symantec Desktop Firewall 2.0 предоставляется компанией "Symantec" и находится на сайте *www.symantec.com,* показанном на рисунке А.4.

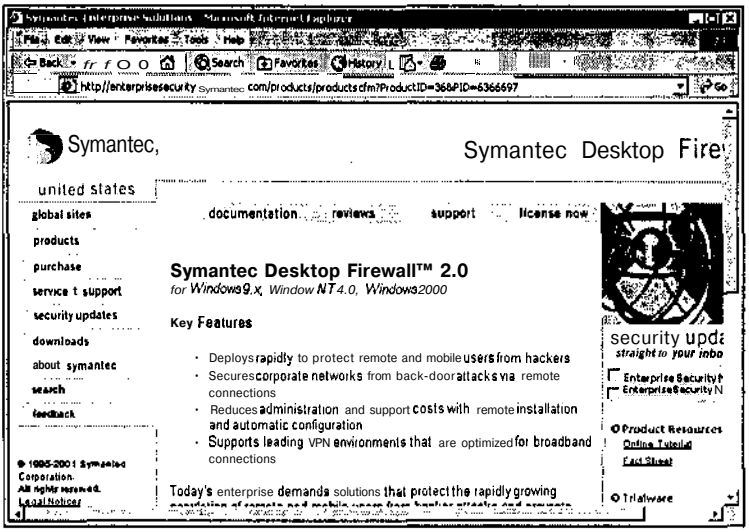


Рисунок А.4. Брандмауэр Symantec Desktop Firewall 2.0

Это один из двух персональных брандмауэров, предоставляемых компанией "Symantec", и он, по-видимому, затмевается другим персональным брандмауэром этой компании, брандмауэром Norton Personal Firewall 2001. Предоставля-

ется бесплатное испытание персонального брандмауэра, так что вы можете получить его для пробной проверки до того, как решите, подходит ли он вам.

Брандмауэр Symantec Desktop Firewall 2.0 позволяет вам блокировать Интернет-трафик, основываясь на приложениях. Вы можете также блокировать определенные IP-адреса или диапазон IP-адресов.

Персональный брандмауэр Sygate Personal Firewall

Персональный брандмауэр Sygate Personal Firewall предоставляется компанией "Sygate Technologies" и может быть найден на сайте *www.sygate.com,* как показано на рисунке А.5. Он создан для персональных пользователей и небольших компаний.

Этот персональный брандмауэр бесплатен для личного пользования. Его характерной чертой является режим обучения, который спрашивает у вас, что делать с каждым приложением, которое пытается соединиться с Интернетом, позволяя вам блокировать любое приложение. Он также позволяет вам установить набор доверяемых IP-адресов и связать их с определенными приложениями. Вы можете также блокировать использование определенных портов и протоколов. Предупреждения он может показывать как с помощью электронной почты, так и посредством всплывающих сообщений.

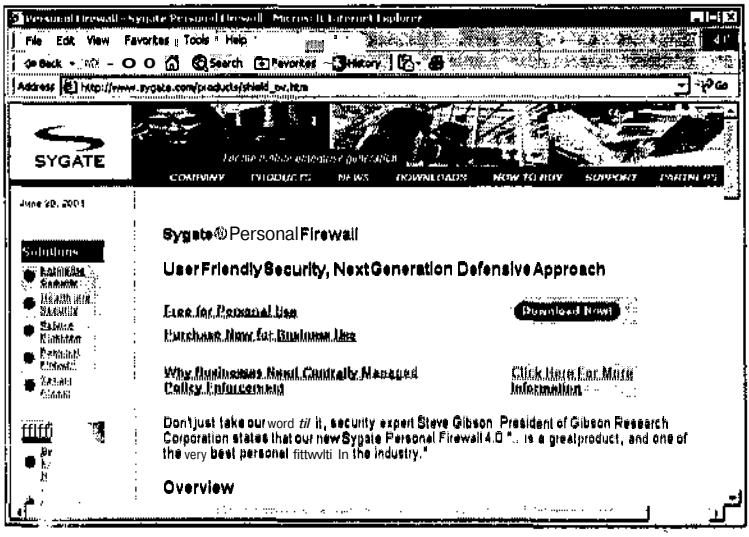


Рис. к А,5. Персональный брандмауэр Sygate Personal Frewall

Персональный брандмауэр Sygate Personal Firewall также позволяет вам установить график, по которому будут применяться правила безопасности. Таким образом вы можете повысить уровень защиты брандмауэра, когда не используете компьютер.

Брандмауэр ConSeal PC Firewall

Брандмауэр ConSeal PC Firewall предоставляется компанией "Sygate Technologies"*, его можно найти на сайте *www.consealfirewall.com*, как показано на рисунке А.6.

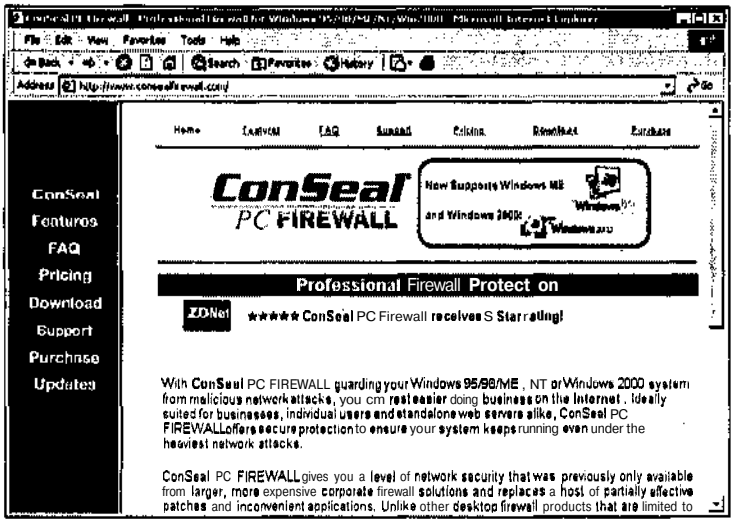


Рисунок А.6. Брандмауэр ConSeal PC Firewall

Этот персональный брандмауэр может фильтровать ряд типов пакетов, включая IP, NetBEUI и IPX компании "Novell". Его характерной чертой является обучающий режим, который запрашивает инструкции и автоматически формирует правила безопасности. Набор правил может быть создан для определенных приложений, сетевых устройств, IP-адресов и служб. Он имеет четыре уровня настройки безопасности:

- Basic (базовый);
- Cable/ADSL (кабельно-цифровой);
- Browse (обзор);
- None (нет),

Вы можете защитить свои настройки безопасности с помощью пароля. Брандмауэр ConSeal PC Firewall - один из более дорогих брандмауэров. Он поставляется в трех версиях:

- ConSeal for Server (ConSeal для сервера);
- ConSeal for Workstation (ConSeal для рабочей станции);
- ConSeal for Desktop (ConSeal для рабочего стола).

Брандмауэр ConSeal for Desktop (ConSeal для рабочего стола) предназначен для домашних пользователей, работающих с Windows 95, 98 или Me. Если у вас

---

* Опечатка автора.

установлена операционная система Windows NT Workstation или Microsoft 2000 Professional, вам необходимо купить версию ConSeal for Workstation (ConSeal для рабочей станции).

Персональный брандмауэр Tiny Personal Firewall

Персональный брандмауэр Tiny Personal Firewall предоставляется компанией "Tiny Software", его можно найти на сайте *www.tinysoftware.com,* показанном на рисунке А.7.

Рисунок А.7. Персональный брандмауэр Tiny Wall

Этот небольшой персональный брандмауэр достаточно невелик, чтобы поместиться на одной дискете, и бесплатен для личного пользования. В него встроен очень хороший мастер установки и автоматическое обнаружение приложений при их попытке получить доступ к Интернету в первый раз. Вы можете определять доверяемые IP-адреса или диапазон IP-адресов, которые должны беспрепятственно проходить через брандмауэр.

Доступны три настройки безопасности:

- Minimal Security (минимальная безопасность) - позволяет всему трафику проходить через брандмауэр.
- Medium Security (средняя безопасность) - уровень безопасности, устанавливаемый по умолчанию, который автоматически позволяет общим приложениям, таким, как Internet Explorer, проходить через брандмауэр.
- Maximum Security (максимальная безопасность) - запрещает неуказанным приложениям устанавливать соединение через брандмауэр.

Кроме того, вы можете защитить с помощью пароля ваши настройки конфигурации и график, в соответствии с которым ваши настройки применяются, позволяя вам повышать уровень защищенности компьютера в то **время,** когда вы на нем не работаете.

Б

Другие Web-сайты, которые проверят вашу безопасность

В этом приложении предоставляется список Web-сайтов Интернета, на которых вы можете получить бесплатные Интернет-сканеры для проверки вашего компьютера. Некоторые сайты предоставляют только быстрое или базовое сканирование, в то время как другие сайты предоставляют сканеры, осуществляющие подробную проверку, которая может занять до 30 минут.

Чтобы протестировать эффективность вашего персонального брандмауэра, запустите сканирование безопасности при отключенном персональном брандмауэре, а затем запустите это же тестирование с включенным брандмауэром и сравните результаты. Запомните, что персональные брандмауэры поставляются с различными уровнями безопасности. Если вы найдете, что результаты сканирования безопасности при включенном брандмауэре неудовлетворительны, попытайтесь просканировать компьютер еще раз после того, как установите более высокий уровень безопасности на своем персональном брандмауэре.

В этой главе рассматриваются следующие сайты:

- HackerWhacker;
- Gibson Research Corporation;
- Secure Design;
- Sygate Online Services;
- Symantec;
- McAfee;
- HackYourself.com.

HackerWhacker

На сайте *www.hackerwhacker.com* вы можете получить сканер, предоставляющий тщательное сканирование вашего персонального брандмауэра, показанный на рисунке Б.1.

Сканер Интернет-безопасности, расположенный на сайте, HackerWhacker, выполняет подробное зондирование вашего компьютера и предоставляет отчет о взломах безопасности. Чтобы запустить сканер HackerWhacker, нажмите на ссылку Want to test your firewall? (Хотите протестировать свой брандмауэр?), которая находится внизу Web-страницы. Вас попросят указать адрес вашей электронной почты. Сайт HackerWhacker использует ваш адрес электронной почты, чтобы выслать вам подробные инструкции по тому, как выполнять сканирование.

Рисунок Б.1. На сайте *www.hackerwhacker.com* находится большая коллекция ссылок на все, что связано с безопасностью персонального компьютера, а также бесплатный сканер безопасности работы вашего компьютера с Интернетом

Gibson Research Corporation

Web-сайт исследовательской корпорации "Gibson", показанный на рисунке Б.2, также предоставляет бесплатное Интернет-сканирование вашего компьютера.

Вы можете найти этот сайт по адресу *http://grc.com.* Чтобы запустить их бесплатные сканеры Интернет-безопасности, нажмите на ссылку Shields UP! Вы найдете большое количество информации на Web-страницах Shields UP. На сайте доступно два бесплатных теста безопасности.

- **Test My Shields! (Протестировать мою защиту!)** - выполняет сканирование вашего компьютера, пытаясь установить соединение и собрать такую информацию, как ваше имя пользователя, имя вашего компьютера и любых общих ресурсов.

m **Probe** My **Ports! (Прозондировать мои порты!)** - выполняет зондирование портов, используя небольшой набор хорошо известных портов TCP/IP и выдавая список всех обнаруженных слабых мест.

Secure Design

Два Интернет-сканера можно найти по адресу *www.sdesign.com,* показанному на рисунке Б.3.

Нажмите Free Security Test (Бесплатное тестирование безопасности) и затем Scan me now (Просканировать мой компьютер). Вы найдете две опции;

и Basic Scan (Базовое сканирование) - запускает сканирование общих файлов Windows и самых известных портов TCP/IP.

Рисунок Б.2. Web-сайт исследовательской корпорации "Gibson" Shields UP1 предоставляет большое количество бесплатной информации и инструментов в дополнение к двум бесплатным сканерам безопасности работы с Интернетом

- **Complete Scan (Полное сканирование)** - выполняет более обстоятельное сканирование вашего компьютера, которое может занять до 30 минут. Прежде чем запустить это сканирование, вам потребуется предоставить ваш IP-адрес.

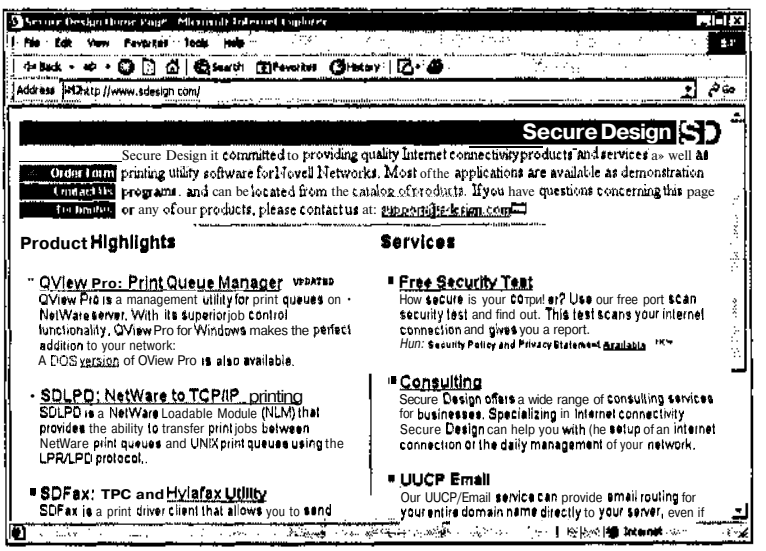


Рисунок Б.3. На Web-сайте Secure Design доступен ряд бесплатных сканеров безопасности работы в Интернете, позволяющих, как быстрое, так и тщательное тестирование зашиты вашего компьютера

Sygate Online Services

Ряд бесплатных сканеров Интернет-безопасности вы можете запустить с Web-сайта Sygate Online Services *(scan.sygatetech.com),* показанного на рисунке Б.4.

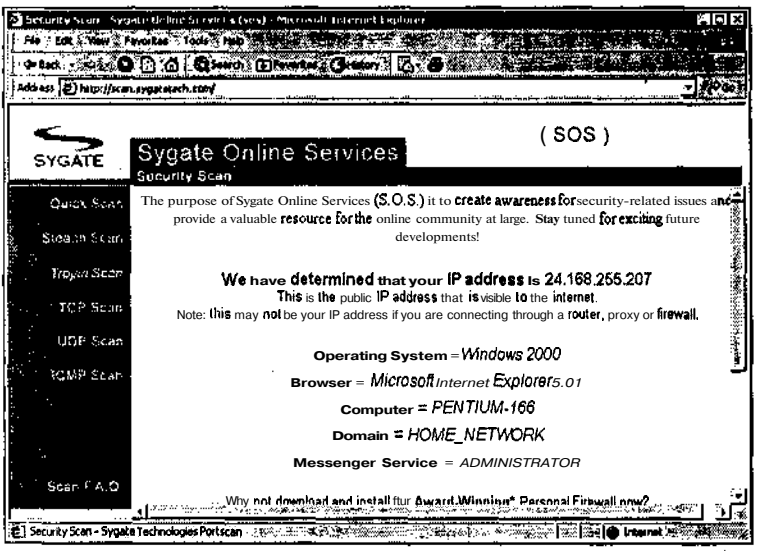


Рисунок Б.4. Web-сайт Sygate предоставляет шесть сканеров Интернет-безопасности, позволяя вам прозондировать безопасность вашего компьютера различными способами

Когда вы впервые загрузите Web-страницу Sygate Online Services, вам предоставят информацию о вашем компьютере, как показано на рисунке Б.4. Слева на экране вы увидите шесть сканеров, которые вы можете запустить. Они включают:

- **Quick Scan (Быстрое сканирование)** - выполняет быстрое сканирование портов вашего компьютера.
- **Stealth Scan (Невидимое сканирование)** - выполняет тестирование, сходное с первым, но использующее техники проникновения через брандмауэры.
- **Trojan Scan (Сканирование "Троянов")** - выполняет поиск программ "Троянский конь".
- **TCP Scan (Сканирование TCP) – сканируют** все 1024 распространенных порта TCP.
- **UDP Scan (Сканирование** UDP) - выполняет проверку того, как хорошо защищены ваши порты UDP.
- **ICMP Scan (Сканирование ICMP)** - выполняет проверку того, блокирует ли ваш брандмауэр попытки пропинговать его. Во время написания этой книги этот тест не был доступен.

Symantec

Вы также можете получить бесплатный сканер Интернет-безопасности на Web-сайте Symantec, расположенный по адресу *www.symantec.com/securitycheck*, показанный на рисунке Б.5.

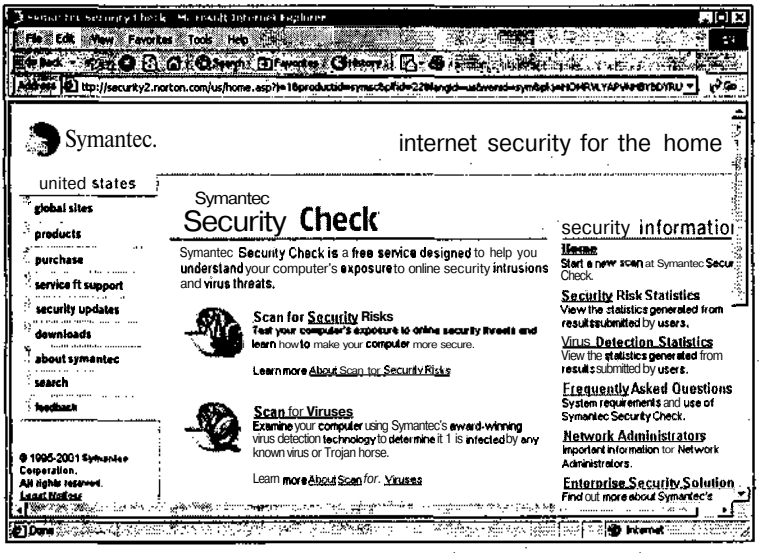


Рисунок Б.5. Сканер безопасности Symantec разбивает анализ слабых мест вашего компьютера на несколько категорий

Чтобы запустить сканер, нажмите Scan for Security Risks (Сканирование угроз безопасности). Вы увидите ваш IP-адрес, показываемый все время, пока вы ждете результатов сканирования. Затем появится отчет о слабых местах компьютера, уязвимых перед следующими угрозами:

V Network vulnerability (сетевая незащищенность);

- NetBIOS availability (доступность NetBIOS);
- Active Trojan horses (активные троянские кони).

Вы можете нажать на ссылку Show Details (Подробнее) на любой этой категории для получения подробной информации относительно результатов определенного теста.

McAfee

Создатели персонального брандмауэра McAfee, описанного в главе 6 этой книги, также предоставляют бесплатное Интернет-сканирование безопасности на своем Web-сайте, который находится по адресу *www.mcafeeasap.com,* как показано на рисунке Б.6.

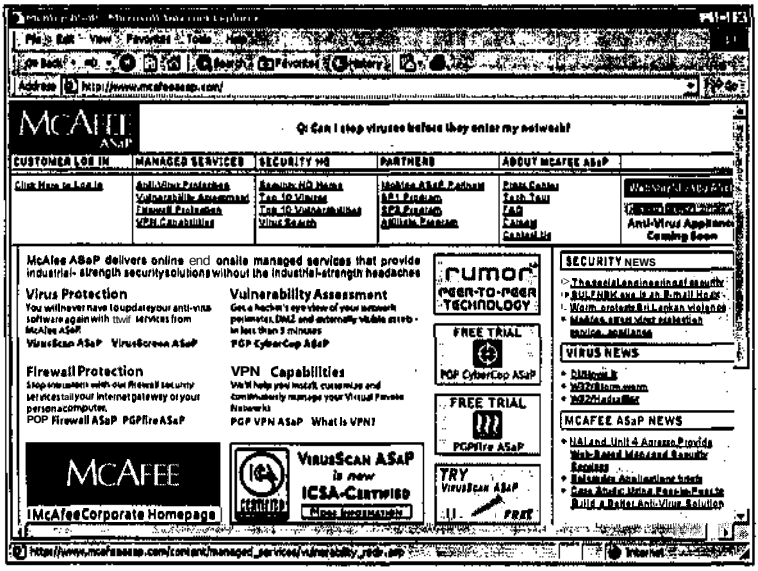


Рисунок Б.6. McAfee предоставляет услугу бесплатного Интернет-сканирования безопасности и позволяет вам запускать бесплатный пробный тест

Чтобы запустить сканер безопасности McAfee, нажмите на ссылку Vulnerability Assessment (Определение слабых мест в безопасности) под CyberCop ASaP, а затем нажмите на Free Trial (Бесплатный пробный запуск). Вам придется предоставить адрес своей электронной почты, имя, номер телефона, имя компьютера и пароль для запуска сканера. Затем нажмите на Submit (Послать). Затем запустится сканирование, и вы получите электронное письмо со ссылкой, показывающей на расположение результатов сканирования вашего компьютера. Вам придется ввести пароль, который вы предоставили McAfee, чтобы просмотреть результаты сканирования вашего компьютера,

HackYourself.com

Сайт HackYourself.com, расположенный по адресу *www.hackyourself.com,* предоставляет в основном ту же информацию, что и на сайте *www.hackerwhacker.com.* Кроме того, он предоставляет бесплатное быстрое Интернет-сканирование вашего компьютера, не требуя от вас адреса электронной почты. Смотрите рисунок Б.7.

Чтобы запустить быстрое сканирование, нажмите Want to Test Your Firewall? (Хотите протестировать ваш брандмауэр?), введите ваш IP-адрес, когда попросят, и нажмите GO (Начать). Когда тест будет выполнен, нажмите Report Details (Подробный отчет), чтобы просмотреть результаты тестирования.

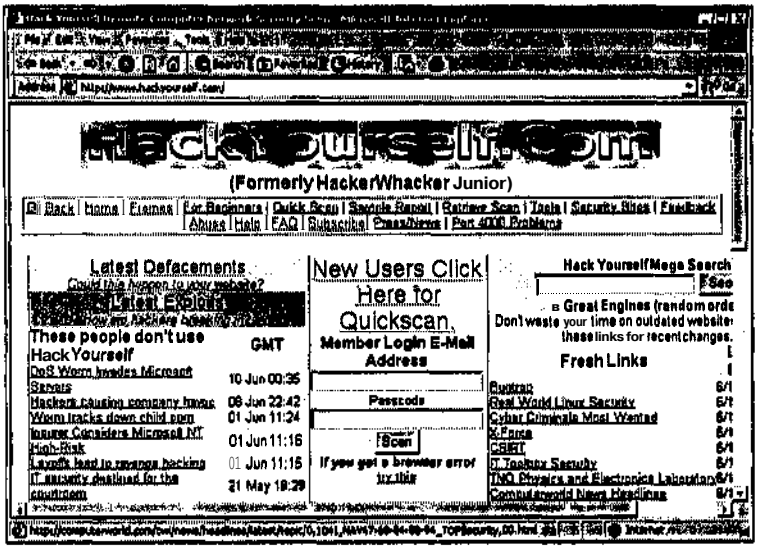


Рисунок Б.7. Сайт www.hackyourself.com предоставляет быстрое сканирование средств зашиты вашего компьютера против нападающих из Интернета

В

Домашние сети в России

В России DSL-соединения распространены значительно меньше, чем в США и Западной Европе, но уже сейчас намечается тенденция к их развитию. Связано это, в частности, с тем, что, по анализам различных статистических агентств, появляется все больше людей, не желающих мириться с низким качеством соединения по традиционным коммутируемым линиям связи и согласных платить больше за скорость и качество. Интернет-провайдеры, в свою очередь, идут им навстречу. Шаг в сторону DSL-услуг делают также телефонные компании, желающие расширить спектр своих услуг. В качестве примеров можно указать проекты Точка Ру *www.tochka.ru* (Москва), Вэб Плас *www.wplus.ru* (Санкт-Петербург), проекты в Екатеринбурге. Предоставляются DSL услуги и в странах ближнего зарубежья (Беларусь, Казахстан, Украина).

К сожалению, стоимость предоставления DSL-услуг пока достаточно велика из-за высокой стоимости развертывания инфраструктуры, которую провайдер, в конечном счете, возьмет с потребителя, а также из-за отсутствия серьезной конкуренции на этом рынке. Однако, как показывает практика, постепенно они будут становиться все более доступными. В качестве подтверждения этого предположения можно вспомнить, что несколько лет назад, на заре развития массовых Интернет-коммуникаций в России, стоимость 1 часа коммутируемого соединения с Интернетом в Москве составляла $5-$7, а сейчас - не более $1, при поддержке максимальной скорости соединения 56 Кбит/с вместо казавшихся тогда небывало высокими 28.8 Кбит/с.

Другой, набирающий все больше поклонников, способ качественного подключения к Интернет - через домашние сети (другие названия - домовые сети и территориальные сети). На момент издания этой книги (март 2002 года) на сайте *www.homenetworks.ru,* посвященном домашним сетям, было зарегистрировано 263 сети, со средним количеством 76 пользователей в одной сети. Согласно информации с сайта *www.mosnet.ru* в Москве было зарегистрировано 130 сетей. Существует информация о домашних сетях Санкт-Петербурга, Нижнего Новгорода, Екатеринбурга и других городов.

В отличие от DSL-соединений для создания домашней сети необходимо приложение значительно меньших усилий и средств, что делает их очень доступными. Однако необходимо отметить, что домашняя сеть не обязательно имеет соединение с Интернетом - как правило, она создается любителями компьютерных игр для возможности играть друг с другом по сети, не выходя из дома, не платя за компьютерное время в игровом клубе или за подключение к Интернету. В этом случае игрок ищет единомышленников в своем доме, совместными усилиями прокладывает кабель и организует сеть, причем сделать это можно за не-

сколько часов, а дальнейшего администрирования такая сеть практически не требует. Можно создать и сеть в пределах одной квартиры, такую часто можно встретить у людей, профессионально занимающихся компьютерами, у которых дома стоит не один, а несколько ПК, объединенных в сеть и имеющих общий выход в Интернет. Процесс создания одноквартирной сети рассмотрен в Главе 11 данной книги.

Изначально подключение к Интернету домашней сети может быть по обычным коммутируемым линиям, однако при увеличении количества пользователей пропускной способности 56 Кбит/с начинает не хватать, и перед организаторами сети встает вопрос об организации высокоскоростного канала связи. Он может быть реализован самыми разными способами - через оптоволоконные линии, радиоканал, уже упоминавшиеся DSL-соединения и т.д. Аренда канала связи, организация совместного доступа, поддержка работоспособности сети - все это требует значительно больших усилий и средств, чем в сети с двумя - пятью узлами, в результате чего с новых абонентов начинают брать плату. Часто домашние сети не приносят прибыли ее организаторам, но иногда такой в прямом смысле "доморощенный" бизнес начинает давать плоды.

Если Вы хотите узнать, есть ли в Вашем доме такая сеть, то можно посоветовать поискать эту информацию в Интернете, на доске объявлений в подъезде или спросить об этом Ваших знакомых, занимающихся компьютерами и живущих в Вашем или соседнем доме. При подключении к домашней сети остаются актуальными все те опасности, которые автор перечисляет в этой книге, и остается актуальным вопрос об установке персонального защитного экрана.

Таким образом, если Вы житель Москвы, Санкт-Петербурга или другого крупного города, то перечисленные в книге способы качественного подключения к Интернету должны быть Вам доступны (во всяком случае, технически). Если же в Вашем населенном пункте еще нет ни DSL-услуг, ни домашних сетей, то не отчаивайтесь - это дело будущего, а пока Вы можете попробовать организовать свою собственную домашнюю сеть, а в будущем, может быть, и стать крупнейшим провайдером в своем регионе, в конце концов, многие современные компьютерные корпорации начинали свой путь с нуля!

Глоссарий

#

@Home - компания, один из двух крупнейших поставщиков услуг кабельного доступа в Интернет в Северной Америке.

A

ADSL (Assymetric Digital Subscriber Line - асимметричная цифровая абонентская линия) - тип соединения с помощью цифровой абонентской линии, предназначенный для индивидуальных пользователей или малого бизнеса. Обладает меньшей пропускной способностью для передачи данных удаленному компьютеру, чем для загрузки данных на собственный компьютер.

Aladdin Knowledge Systems eSafe Desktop 3.0 - программный продукт, включающий технологию персонального брандмауэра, созданный для защиты вашего широкополосного или коммутируемого соединения.

B

BlackICE Defender - программный персональный брандмауэр, созданный для защиты вашего компьютера с широкополосным или коммутируемым соединением при работе в Интернете.

C

CableLabs - организация, на которую возложена ответственность по обеспечению соответствия кабельного модема DOCSIS техническим условиям стандарта, маркирующая проверенные кабельные модемы лейблом "Аттестовано компанией "CableLabs" ("CableLabs Certified").

D

DHCP (Dynamic Host Configuration Protocol - протокол динамической конфигурации хоста) - протокол TCP/IP, используемый поставщиками услуг Интернета для динамичного присвоения IP-адресов пользователям их Интернет-услуг.

DOCSIS (Data **Over Cable Systems Interface Specification)** - стандарт модемов для кабельного соединения, введенный в 1998 году и принятый в индустрии кабельного соединения.

DSL (Digital Subscriber Line - цифровая абонентская линия) - постоянно подключенное высокоскоростное соединение с Интернетом, предоставляемое вашей местной телефонной компанией по имеющимся у вас телефонным линиям с использованием цифрового модема.

E

EFS (Encrypted File System - система шифрования файлов) - свойство Windows 2000 и Windows XP, которое позволяет вам зашифровать содержимое файлов, хранящихся на жестких дисках, для того чтобы предотвратить недозволенный доступ к ним.

Ethernet - низкоуровневый протокол, используемый для соединения компьютеров в локальную сеть, также используется для установления соединения между вашим компьютером и вашим высокоскоростным кабельным или цифровым доступом.

F-H

FAT - исходная файловая система Windows и MS DOS. Эта файловая система обеспечивает незащищенную группировку и хранение файлов, используя формат имен файлов **8/3.**

FAT32 - 32-битная версия файловой системы FAT, которая включает поддержку длинных имен файлов и больших накопителей на дисках.

FTP - протокол TCP/IP, используемый серверами Интернета для передачи файлов.

I-K

IDSL (Integrated Digital Subscriber Line - объединенная цифровая абонентская линия) - вид цифрового соединения, предназначенный для клиентов, находящихся более чем в трех милях от главного офиса. Предоставляет более низкий уровень обслуживания, чем другие виды цифрового соединения.

IP (Internet Protocol - Интернет-протокол) - один из протоколов в наборе протоколов TCP/IP, который отвечает за транспортировку пакетов по Интернету.

IP-адрес (IP address) - уникальный 32-битный адрес, состоящий из комбинации нулей и единиц, который определяет положение компьютеров и сетевых устройств в Интернете.

IPX - протокол, который имеет сходные функциональные возможности с возможностями протокола TCP, принадлежащий сетям NetWare.

ISA (ISA **slot)** - более ранний тип расширительного гнезда, расположенный внутри компьютера, который позволяет вам увеличить его возможности с помощью установки периферийных устройств в гнездо.

L

Linksys EtherFast, кабельно-цифровой маршрутизатор (Linksys EtherFast cable/DSL router) - аппаратно реализованный персональный брандмауэр, который защищает ваш компьютер при широкополосном соединении с Интернетом.

M

MAC-адрес (MAC **address)** - 48-битный адрес, закодированный на каждой сетевой интерфейсной плате (NIC), который обеспечивает ее уникальным идентификатором. В конечном счете все сетевые коммуникации основаны на определении **MAC-адреса** посылающего и принимающего компьютеров, независимо от того, какой сетевой протокол используется.

McAfee Personal Firewall - программный персональный брандмауэр, который создан для защиты вашего компьютера с широкополосным или коммутируемым соединением при работе в Интернете.

N

NetBEUI (NetBIOS Extended User Interface - расширенный пользовательский протокол NetBIOS) - протокол локальной сети, созданный для поддержки сетевых коммуникаций небольшой сети, не требующий конфигурирования.

NetBIOS - протокол сетевой коммуникации, который находится поверх TCP, UDP и NetBEUI и помогает совместно использовать ресурсы Microsoft, включая принтеры и жесткие диски.

NIC (Network Interface Card - сетевая интерфейсная плата) - периферийное устройство, которое позволяет вашему компьютеру соединяться с сетью компьютеров. Она также используется для установки сетевых соединений между компьютером и кабельным или цифровым модемом.

Norton 2000, персональный брандмауэр (Norton Personal Firewall 2000) - программный персональный брандмауэр, созданный для защиты вашего компьютера с широкополосным или коммутируемым соединением при работе в Интернете.

NTFS (New Technology File System - файловая система новой технологии) - файловая система, предоставляемая операционными системами Windows NT, 2000 и XP, которая дает вам возможность защищать файлы с помощью расширенного набора разрешений безопасности.

0-Q

PCI (PCI slots) - 32-битные расширительные гнезда внутри компьютера, которые позволяют вам увеличить возможности компьютера с помощью установки в гнездо периферийных устройств.

PGP Desktop Security 7.0 - программный продукт, который включает технологию персонального брандмауэра, созданный для защиты вашего широкополосного или коммутируемого соединения с Интернетом.

Ping - команда TCP/IP, которая позволяет вам проверить присутствие другого компьютера в сети. Вы можете попытаться пропинговать любой компьютер в Интернете, напечатав PIN6 вслед за его именем или IP-адресом.

R-S

Regedit - мощная программная утилита, которая позволяет вам просматривать и изменять системный реестр Windows.

RoadRunner - один из двух крупнейших поставщиков услуг кабельного доступа в Интернет в Северной Америке.

SDSL (Synchronous Digital Subscriber Line - синхронная цифровая абонентская линия) - вид цифрового соединения, предназначенный для организаций с большими требованиями к доступу в Интернет. Обеспечивает одинаковую пропускную способность как для загрузки, так и для передачи данных.

Sybergen Networks Secure Desktop 2.1 - программный продукт, который включает технологию персонального брандмауэра, созданный для защиты вашего широкополосного или коммутируемого соединения с Интернетом.

Symantec Desktop Firewall 2.0 - программный персональный брандмауэр, созданный для защиты вашего компьютера с широкополосным или коммутируемым соединением при работе в Интернете.

T

TCP - один из протоколов, включенных в набор протоколов TCP/IP, который создан для установки логических соединений между сетевыми устройствами.

TCP/IP - набор протоколов, обеспечивающий обмен информацией внутри компьютерной сети, такой, как Интернет (в котором TCP и IP являются просто двумя частными протоколами). TCP/IP является протоколом, устанавливаемым по умолчанию, в Windows 98, Me, 2000 и XP.

Tiny Wall - программный персональный брандмауэр, который может быть загружен из Интернета для бесплатного персонального пользования и который имеет многие из свойств, имеющихся у других платных программных персональных брандмауэров.

Tracert - команда TCP/IP, которая позволяет вам проверить ваш уровень времени ожидания. Она показывает число пересылок, которые пакет данных проходит на своем пути к удаленному компьютеру, и выдает список периодов времени, которые занимает каждая пересылка.

U-Z

UDP (User Datagram Protocol - протокол передачи дейтаграмм пользователя) - один из протоколов, которые входят в набор протоколов TCP/IP, созданный для установки обмена данными без организации прямого соединения между сетевыми устройствами.

Winsock - компонент операционной системы Windows, который управляет соединениями TCP/IP с Интернет-приложениями.

ZoneAlarm - программный персональный брандмауэр, который вы можете загрузить из Интернета для бесплатного персонального пользования и который имеет многие из свойств, которые есть в других платных программных персональных брандмауэрах.

A

Адрес (Address) - компонент пакета данных, который идентифицирует отправляющий и принимающий компьютер.

Антивирусная программа (Antivirus program) - программа, созданная для защиты вашего компьютера от компьютерных вирусов с помощью просмотра ваших дисковых накопителей и загружающая файлы для обнаружения вирусов.

Аппаратный брандмауэр (Hardware firewall) - внешнее устройство, подсоединенное к вашему компьютеру и кабельному или цифровому соединению, которое фильтрует трафик соединений с Интернетом.

Атака "Отказ от обслуживания" (Denial-of-service (DoS) **attack)** - атака на другой компьютер, когда компьютер с более быстрым доступом в сеть пытается переполнить указанный компьютер большим количеством сетевых данных, чем тот сможет обработать, для того чтобы не допустить возможности получения и обработки других сетевых запросов или данных.

Атака "Распределенный отказ от обслуживания" (Distributed denial-of-service (DDoS) attack) - атака на сетевой компьютер, запускаемая с помощью получения

контроля над рядом других компьютеров и инструктирования их на переполнение указанной системы данными, чтобы попытаться перегрузить ее возможности обработки данных.

Б

Брандмауэр (Firewall) - аппаратное устройство или программа, созданная для защиты компьютера или сети от внешнего нападения.

Брандмауэр Интернет-соединения (Internet Connection Firewall) - персональный брандмауэр, поставляемый с операционной системой Windows XP Home Edition.

Брандмауэр - пакетный фильтр (Packet-filtering firewall) - вид брандмауэра, созданный для контролирования пакетов, основываясь на их IP-адресах. Позволяет проходить через брандмауэр только заданным IP-адресам.

Брандмауэр проверки состояния (Stateful inspection firewall) – этот вид брандмауэра пытается определить тип передающихся данных и угрозы, возможно, исходящие от них, до того, как позволит им пройти.

Брандмауэр уровня соединений (Circuit-level firewall) - брандмауэр, созданный для разрешения потока трафика с предварительно проверенными IP-адресами, сетями и поставщиками услуг Интернета. Пакеты фильтруются только в то время, пока соединение устанавливается. Когда соединение установлено, пакеты проходят через брандмауэр беспрепятственно.

Брандмауэр - шлюз приложений (прокси-брандмауэры) (Application gateway firewall (proxy firewalls)) - брандмауэр, фильтрующий пакеты данных, основываясь на IP-адресах и определенной функции, которую приложение пытается выполнить. Это модель, реализуемая большинством персональных брандмауэров.

В

Ванаби (Wannabee) - человек, который находится на начальной стадии ларва в своей карьере хакера, и опасный в большей степени из-за своей неопытности.

Взломщики паролей (Password crackers) - программы, созданные для попытки взлома или расшифровки паролей, присвоенных учетным записям пользователей или общим ресурсам компьютера, таким, как общие диски или принтеры.

Вирус (Virus) - программа, созданная для заражения компьютера и причинения различного рода вреда, колеблющегося от простого розыгрыша до полного удаления содержимого вашего жесткого диска.

Вокер (Whacker) - человек, занимающийся хакерством без овладения навыками настоящего хакера. Вокеры менее опытны в своих технических приемах и способности проникать в системы.

Время ожидания (Latency) - это время, требуемое пакету для прохода по Интернету. Высокое время ожидания обычно вызвано загруженностью вашего провайдера или слабым откликом Web-сайта.

Д

Динамический IP-адрес (Dynamic IP address) - IP-адрес, динамически присваиваемый или выдаваемый на время сетевому компьютеру в сети TCP/IP. В случае коммутируемого соединения новый IP-адрес присваивается каждому новому се-

ансу связи, тогда как кабельное или цифровое соединение может, как правило, постоянно автоматически возобновлять один и тот же IP-адрес.

Доверяемое приложение (Trusted application) - приложение, указанное в вашем персональном брандмауэре как то, которому разрешено проходить через персональный брандмауэр и соединяться с Интернетом.

К

Кабельное модемное соединение (Cable modem connection) - всегда подключенное высокоскоростное соединение с Интернетом, предоставляемое вашей местной кабельной компанией, использующей то же кабельное соединение, с помощью которого вам предоставляется кабельное телевидение.

Кабельно-цифровой маршрутизатор (Cable/DSL router) - встроенное свойство, находящееся в большинстве аппаратных персональных брандмауэров, созданное для совместного пользования одним соединением с Интернетом.

Клиент для сетей Microsoft (Client for Microsoft Networks) - программный компонент, использующийся на компьютерах, работающих под операционными системами Microsoft, позволяющий компьютерам соединяться и использовать ресурсы совместно.

Коммутатор (Switch) - свойство, часто присущее сетевым концентраторам, которое создает выделенное соединение между двумя взаимодействующими устройствами и обеспечивает непрерывный поток информации.

Концентратор (Hub) - внешнее сетевое устройство, которое соединяет два или более компьютеров для создания локальной сети.

Кракер (Cracker) - человек, взламывающий компьютерные системы и сети с намерением нанести вред или украсть частную информацию, в противоположность хакеру, который не заинтересован в нанесении вреда, вместо этого его интересует решение технических задач.

Л

Личинка (Larva) - начинающий хакер, который только начал изучать ремесло, идеализирующий настоящих хакеров.

Лог-файл (Log file) - файл, созданный вашим персональным брандмауэром, который содержит ряд данных относительно режима работы брандмауэра и его действий.

Локальная сеть (Local area network (LAN)) - небольшая сеть, состоящая из двух или более компьютеров, которые совместно используют информацию и ресурсы. В тексте данной книги термин локальная сеть равнозначен термину домашняя сеть.

М

Мастер конфигурирования (Configuration wizard) - программная утилита, предоставляемая большинством персональных брандмауэров, поэтапно проводящая вас сквозь процесс установки персонального брандмауэра и устанавливающая параметры настройки безопасности.

Многопортовый **концентратор** (Multi-port hub) - аппаратное устройство, такое, как аппаратный персональный брандмауэр, снабженное более чем одним портом Ethernet с тем, чтобы вы могли создать домашнюю локальную сеть.

Модем (Modem) - устройство, которое подсоединяется к вашему компьютеру и позволяет вам соединяться с другим компьютером или сетью, такой как Интернет.

Н

Невидимый режим (Stealth mode) - способность помещать порты TCP/IP компьютера в режим, в котором они не видны в Интернете. Он запрещает компьютеру откликаться на сканеры портов и открывать свое существование сканерам Интернета.

О

Обнаружение вторжения (Intrusion detection) - возможность, иногда присущая персональным брандмауэрам, которая позволяет вам защищаться от нападений и блокировать доступ компьютеров, пытающихся взломать ваш компьютер. Обнаружение вторжения включает проверку пакетов данных и их содержимого с целью определения, не исходит ли от них какая-либо угроза.

Обший доступ к принтерам (Printer sharing) - процесс получения доступа к содержимому локальных принтеров другими компьютерами в сети.

Обший доступ к файлам (File sharing) - процесс получения доступа к содержимому локальных файлов, папок и накопителей на дисках другими компьютерами в сети.

Обший доступ к файлам и принтерам (File and printer sharing) - служба операционных систем Microsoft, которая, будучи активной, помогает совместно использовать локальные накопители на дисках, папки и принтеры.

Обшее подключение к Интернету (Internet connection sharing) - свойство Windows 98 Second Edition, Windows Me и Windows 2000, которое позволяет этим операционным системам делить соединение с Интернетом с другими пользователями домашней сети.

Окно приема TCP/IP (TCP/IP Receive Window) - элемент TCPJIP, в нем хранятся пакеты данных во время взаимодействия с другими сетевыми компьютерами. Размер окна приема TCP/IP может значительно влиять на эффективность коммуникаций вашего компьютера в Интернете.

Операционная система (Operating system) - программное обеспечение, которое загружается, когда включается ваш компьютер, управляет аппаратными устройствами и приложениями компьютера и предоставляет вам интерфейс для работы с этими ресурсами.

П

Пакет (Packet) - набор данных, посылаемых по сети, который содержит адреса исходного и удаленного компьютеров, а также посылаемые данные.

Пароль (Password) - секретный код, связанный с учетной записью пользователя или ресурсом, с помощью которого пользователь компьютера или сети подтверждает право пользования.

Персональный **брандмауэр** (Personal firewall) - программный продукт или небольшое аппаратное устройство, созданное для защиты домашнего компьютера

или сети от несанкционированного доступа ряда враждебных программ. Персональный брандмауэр также способен запретить внутренним приложениям общаться с внешними сетями.

Полубог (Demigod) - хакер с опытом, исчисляющимся десятилетиями, и всемирной известностью в сообществе хакеров.

Порт (Port) - любое из 65 534 возможных соединений с компьютером или сетевым устройством, на котором установлен TCP/IP.

Провайдер (Поставщик услуг Интернета) (ISP **(Internet service provider))** - компания, предоставляющая доступ в Интернет на условиях аренды.

Программный брандмауэр (Software firewall) - программа, загружающаяся с жесткого диска вашего компьютера, которая создана для защиты от враждебных нападений, запущенных из Интернета. В отличие от аппаратных, программные брандмауэры работают как с широкополосными, так и с коммутируемыми соединениями.

Программный драйвер (Software driver) - небольшая программа, поставляемая с периферийным устройством, таким, как сетевая плата, которая должна быть установлена операционной системой для работы с устройством и управления им.

Протокол (Protocol) - набор правил и стандартов для настройки передачи данных в сети.

С

Самурай (Samurai) - хакер, который решил предоставить свои умения корпорациям, чтобы помочь им повысить сетевую безопасность. Самураям часто платят компании за то, что они пытаются проникнуть в их сети.

Сканер портов (Port scan) - попытка какого-либо человека определить местонахождение и обнаружить присутствие открытых портов TCP/IP на компьютере и проверить возможность установления соединения между этими портами.

Служба (Service) - приложение Windows, выполняющее определенную функцию на системном уровне.

Служба безопасности (Security policy) - встроенная служба персональных брандмауэров, осуществляющая исполнение правил безопасности, основываясь на информации, которую вы предоставили мастеру конфигурирования брандмауэра.

Соединение (Connection) - логический сеанс связи, устанавливаемый между двумя компьютерами, сообщающимися через сеть.

Статический IP-адрес (Static IP address) - IP-адрес, вручную присваиваемый компьютеру, поддерживающему TCP/IP, он не меняется со временем.

Т

Троянский конь (Trojan horse) - программа, созданная для проникновения на ваш компьютер и запуска в невидимом режиме человеком, который внедрил ее, с целью обнаружения личной информации или для получения полного контроля над вашим компьютером. "Троянские кони" часто получают доступ к компьютерам с помощью нелегального проникновения в виде безобидного программного обеспечения или спрятавшись внутри приложения электронной почты.

Ф

Фильтрация (Filtering) - процесс, используемый брандмауэром для проверки каждого пакета, проходящего через сетевое соединение, для того чтобы определить, разрешить ли ему доступ.

Х

Хакер (Hacker) - название, присвоенное человеку, в совершенстве владеющему техническими навыками в компьютерной области, который получает удовольствие от нахождения и решения технических задач, включая проникновение в компьютерные и сетевые системы, в противоположность кракеру, который взламывает компьютерные системы и сети с намерением нанесения вреда или кражи личной информации.

Ч

Червь (Worm) - программа, созданная для проникновения на ваш компьютер и скрытия себя где-то в недрах жесткого диска. После наступления предварительно определенной даты или события (событий) он активизируется и выполняет любые злонамеренные действия, которые в него заложены.

Ш

Широкополосное соединение с Интернетом (Broadband Internet connection) - высокоскоростное соединение с Интернетом с помощью кабеля или цифровой абонентской линии.

Э

Электронная почта (E-mail) - электронные средства передачи сообщений по сетям, например, по Интернету,

Эфемерный порт (Ephemeral port) - порт TCP или UTP выше диапазона хорошо известных портов, который не был официально присвоен службе или приложению.

Предметный указатель

Z

Содержание

Король В. И. Visual Basic 6.0, Visual Basic for Applications 6.0. Язык программирования. Справочник с примерами.
448 с. Станд. 7. Оптовая цена 88 руб.

Мартынов Н. Н., Иванов А. П. MATLAB 5.x. Вычисления, визуализация, программирование.
336 с. Станд. 12. Оптовая цена 66 руб.

Мартынов Н. Н. Введение в MATLAB 6.
352 с. Станд. 9. Оптовая цена 96 руб.

Мельников Д. А. Информационные процессы в современных компьютерных сетях. Модели, стандарты, протоколы, интерфейсы...
256 с. Станд. 30. Оптовая цена 72 руб.

Померанц О. Ядро Linux. Программирование модулей: пер. с англ.
112 с. Станд. 30. Оптовая цена 22 руб.

Пегано Дж. Лечение псориаза - естественный путь.
288 с. Станд. 12. Оптовая цена 132 руб.

Титов С. ArchiCAD 6.5. Справочник с примерами.
352 с. Станд. 9. Оптовая цена 132 руб,

Титов С. ArchiCAD 7.0. Справочник с примерами.
400 с. Станд. 8. Оптовая цена 144 руб.

Титов С. ArchiCAD: полезные рецепты+CD.
272 с. Станд. 12. Оптовая цена 165 руб.

Черкасский В. Т. Эффективная анимация во Flash.
432 с. Станд. 8. Оптовая цена 132 руб.

Щербо В. К. Стандарты вычислительных сетей и их взаимодействия. Справочник.
272 с. Станд. 12. Оптовая цена 88 руб.

ПРИГЛАШЕНИЕ К СОТРУДНИЧЕСТВУ

Издательство «ОЦКУДИЦ-ОБРАЗ» приглашает к сотрудничеству авторов, специалистов, имеющих профессиональные интересы в области вычислительной техники, программирования и использования прикладных систем.

ЗАКАЗ КНИГ НАЛОЖЕННЫМ ПЛАТЕЖОМ

Издательство «ОЦ КУДИЦ-ОБРАЗ» осуществляет рассылку книг по почте.

Заказы принимаются по адресу: 121354, Москва, а/я 18; или по e-mail: ok@kudits.ru

Условия рассылки: При отправке книг наложенным платежом стоимость увеличивается в 1,6 раза от оптовой цены.

Заказы из регионов России с авиадоставкой, а также заказы из стран ближнего и дальнего зарубежья обслуживаются только по предварительной оплате.

Приглашаем к сотрудничеству региональных распространителей книжной продукции.
Действует гибкая система скидок!
Организуем доставку!