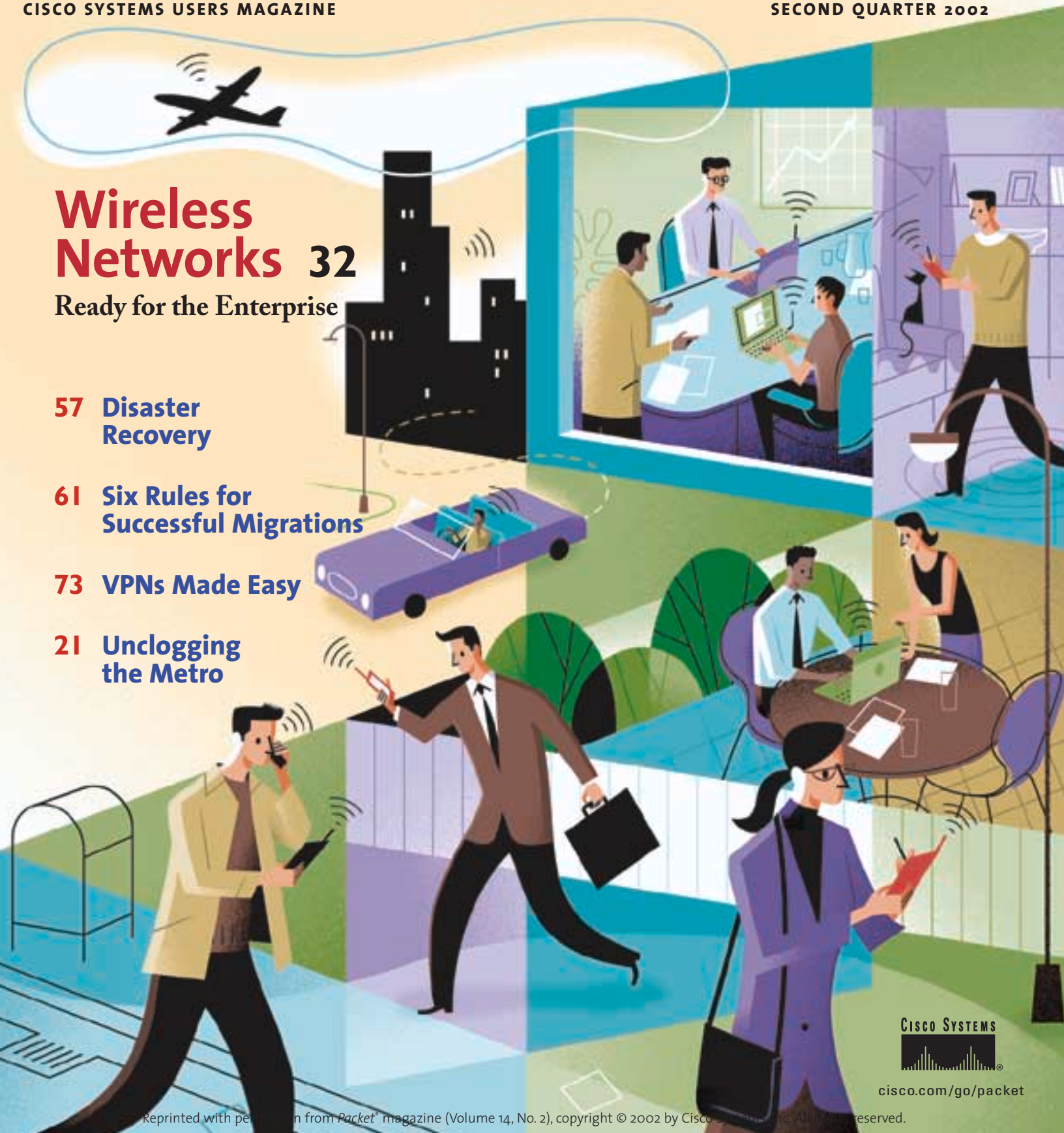
PACKET®

CISCO SYSTEMS USERS MAGAZINE

SECOND QUARTER 2002



Wireless Networks 32

Ready for the Enterprise

CISCO SYSTEMS

cisco.com/go/packet

VPNs Made Easy

Cisco Unified VPN Framework expanded to small offices and enterprise branch office routers.

BY RAFE BROWN

REMOTE VPN CLIENT: One of a pair of new Cisco IOS Software features that simplify configuration and management of VPNs, the Cisco Easy VPN Remote feature runs on a variety of Cisco IOS routers, including the Cisco 800, uBR900, and 1700 Series (pictured here).

TWO NEW FEATURES OF CISCO IOS® Software are making it easy to deploy and manage a virtual private network (VPN) connection in small and midsized office environments. Included in Cisco IOS Software Release 12.2(4)YA and later, the Cisco Easy VPN Remote feature eliminates much of the tedium associated with configuring VPN connections by allowing most VPN parameters to be defined at corporate headquarters and pushed down to the local router.

The new Cisco Easy VPN Server feature, included in Cisco IOS Software Release 12.2(8)T and later, allows Cisco IOS routers to terminate VPN sessions initiated by telecommuters and mobile workers using either the Easy VPN Remote feature, Cisco VPN Software Client, or another Cisco product that can serve as a VPN Client such as the Cisco VPN 3002 Concentrator or PIX® 501 Firewall.

These new IOS software features put employees based in smaller offices on par with their big-office counterparts. And with today's increasingly mobile workforce, this is welcome news to information technology (IT) professionals in small and midsized offices, tasked with providing secure, remote network access to mobile workers.

Custom Fit

The Cisco Easy VPN Remote feature runs on a variety of Cisco IOS routers, including the Cisco 800, 1700, and uBR900 Series. The Cisco 1700 Series modular access routers, in particular, are specifically designed for the needs of small and midsized businesses and enterprise branch offices. The flexibility and manageability of this e-business platform has made it one of the most widely deployed routers in the world, providing VPNs, secure stateful firewall, business-class DSL, and multiservice integration of data, voice, video, and fax.

"By expanding the capabilities of the Cisco 1700 to terminate VPNs from remote workers and streamlining the process of maintaining a VPN tunnel with company headquarters, network administrators now have the tools they need to address issues such as remote access, while reducing costs and maintaining security,"

says Dwayne Thaele, VPN and security product manager in the Cisco Mid-Market Access Business Unit.

On the Go

For mobile workers and telecommuters, it's not enough to have a high-performance connection to the Internet. To be truly effective, these users need complete, secure access to electronic resources at their home office, which means establishing a VPN connection with a high level of authentication and the ability to encrypt data. With the release of the Cisco Easy VPN Server feature, remote workers and telecommuters from small offices or enterprise branch offices can now establish a VPN across the public Internet directly to their home office—making the high-speed network resources they need to do their jobs available to them at a fraction of the cost of alternative secure connections.

Before the Cisco Easy VPN Server feature, providing secure access to remote workers often entailed connecting to their home office through Point-to-Point Tunneling Protocol (PPTP). Although this method allows users to terminate a secure connection to their home office, a PPTP tunnel does not provide users authentication, which can lower the overall security threshold of the connection. Alternative methods of establishing a secure connection were limited because they did not support all platforms across the network.

In addition to the Cisco 800, 1700, and uBR900 Series routers, as part of the Cisco Unified Client VPN Framework, Easy VPN Server supports and maintains VPN connectivity across a broad range of platforms, including Cisco PIX firewalls and Cisco VPN 3000 Series concentrators with the Cisco VPN clients they are supporting.

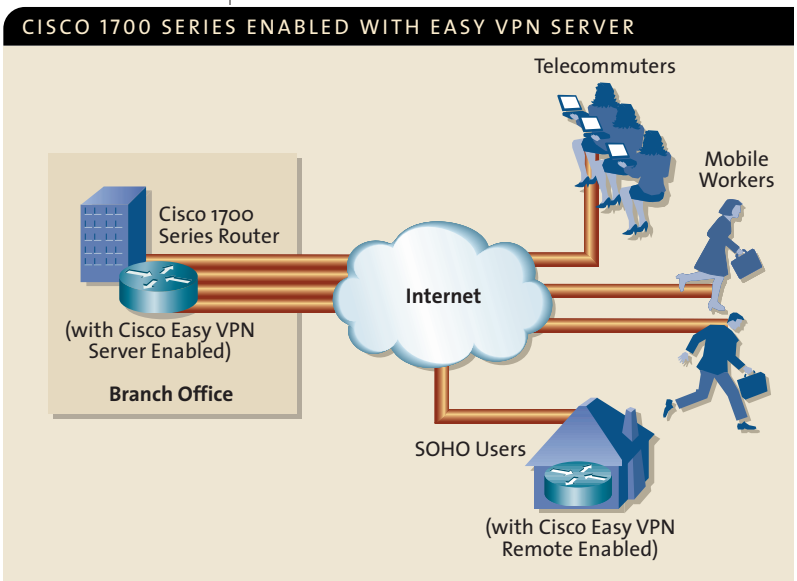


FIGURE 1: With the new Cisco Easy VPN Server feature, routers such as the Cisco 1700 Series can terminate VPN sessions initiated by telecommuters and mobile workers using the Cisco VPN Software Client, or sessions initiated by SOHO users with the Easy VPN Remote feature enabled.

For remote workers to access their home network, they must establish an Internet connection over the public network and then initiate a VPN session with their home office using the Cisco VPN Software Client, an application supported in Windows and other operating systems, running on their laptop (see Figure 1). The VPN tunnel is terminated directly at the Cisco IOS router in the branch office, which means that employees have complete access to network resources from their home office. VPN tunnels initiated by small-office-home-office (SOHO) users can also terminate directly at the branch-office router, with the Easy VPN Remote feature enabled.

Easy VPN

The Cisco Unified VPN Client Framework yields additional benefits for enterprise branch offices, by removing much of the tedium associated with configuring and coordinating VPN parameters between the branch office and an enterprise central site. The central-site router must have security policies configured, to determine which VPN parameters such as encryption algorithms and authentication algorithms, will be used to communicate with remote devices. These security policies are then pushed to remote devices with minimal configuration.

Using Cisco Unified VPN Framework, the Cisco Easy VPN Remote feature allows most VPN parameters of the branch-office router to be automatically defined by a Cisco VPN 3000 Series Concentrator or another Cisco product enabled with Easy VPN Server located at the enterprise central site. In this scenario, the Cisco VPN 3000 Series Concentrator acts as an IP Security (IPsec) server and the branch-office router as the IPsec client. The VPN parameters automatically configured include the following:

- Internal IP address
- Internal subnet mask
- Internal Dynamic Host Control Protocol (DHCP) server address
- Internal WINS server address
- Split tunnel allowed flag

So, for example, after a Cisco 1700 Series Router at the branch office has been configured via Easy VPN Remote, a VPN connection to the Cisco 3000 Series Concentrator at the corporate central office can be created with minimal configuration. The Easy VPN Remote feature initiates the VPN connection to the Easy VPN Server, which pushes IPsec parameters and policies to the Cisco 1700 Series Router and creates the corresponding VPN tunnel connection (see Figure 2).

CISCO 1700 SERIES ENABLED WITH EASY VPN REMOTE

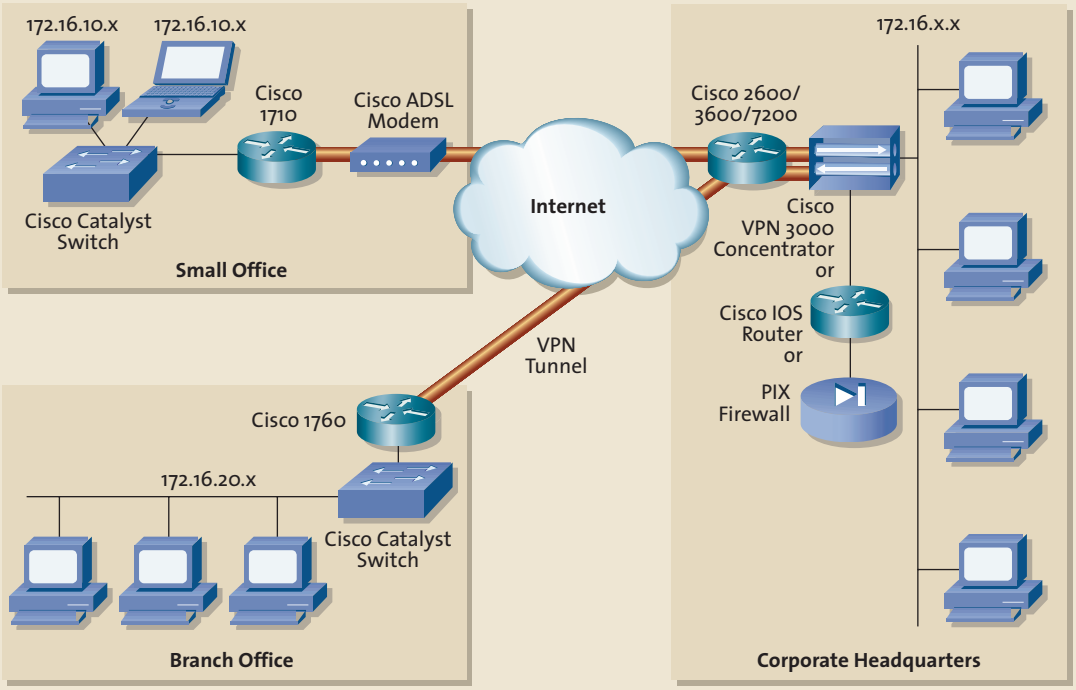


FIGURE 2: Using the Cisco Easy VPN Remote feature, a Cisco 1700 Series Router establishes a connection to a Cisco VPN 3000 Concentrator, IOS router, or PIX firewall at the central office. Through the configuration parameters pushed to the Cisco 1700 Series Router from one of these devices, the PCs and hosts attached to the router can securely access the central office. The result is a seamless extension of the enterprise network.

Because many of the detailed tasks associated with establishing a VPN connection have been automated, the process of establishing the connection has been greatly simplified with the Cisco Easy VPN Remote feature. To suit the networking needs of various users, the Cisco Easy VPN Remote feature can be figured in two different modes:

- *Client mode.* This is the default configuration and allows devices at the client site only to access resources at the central site (where the Cisco VPN 3000 Concentrator or other Cisco VPN server is located). But the central site cannot access networked resources at the client site.
- *Network extension mode.* Users at both the central and client sites can access network resources located at either location.

Make It Happen

For IT professionals installing a new Cisco 1700 Series Router, Cisco 1700 VPN security router bundles are now provided, allowing users to order a Cisco 1700 Series Router with all the necessary VPN components under just one part number. Five new VPN router bundles based on the Cisco 1721, Cisco 1751, and Cisco 1760 modular multiservice router platforms are available. These VPN security bundles include the base router, VPN acceleration module for fast performance, a memory upgrade, and IOS software, which provide not only the required VPN capability but also the IOS firewall that turns the Cisco 1700 Series Router into a stateful firewall.

Users who have existing Cisco IOS routers already installed and a SmartNet contract can download the latest release of Cisco IOS Software from the Cisco Software Center Web site at cisco.com/public/sw-center.

◆ ◆ ◆

By adding Cisco Easy VPN Server termination capabilities to routers often found in small offices and enterprise branch offices, IT professionals can easily and affordably support mobile workers and telecommuters. And with the Cisco Easy VPN Remote feature, establishing and maintaining interoffice VPNs is greatly simplified. ▲▲

Check out the new Cisco 1700 eBusiness Solution Design Tool, developed to guide you through the configuration of a complete Cisco 1700 Series system. To launch the tool, visit the URL cisco.com/warp/public/779/smbiz/service/1700config.

FURTHER READING

To find out more about Cisco Easy VPN Remote and Server features, visit cisco.com/warp/public/cc/pd/sqsw/evpn/index.shtml.