PACKET™

CISCO SYSTEMS USERS MAGAZINE

FIRST QUARTER 2001

Security in the 21st Century

Balancing Access and Security in the Internet Age

Instant Internet
Mobilizing the Corporate Troops

IPsec or MPLS?
Why Service Providers Should Use Both

DSL Lockdown
Securing Always-On Access

Cisco Systems

cisco.com/go/packet

PACKET™

CISCO SYSTEMS USERS MAGAZINE

FIRST QUARTER 2001 VOLUME 13 NO. 1

▼ ON THE COVER

Security in the 21st Century

Balancing Access and Security in the Internet Age

▼ NETIZENS

PACKET™

ENTERPRISE SOLUTIONS

SMALL AND MIDSIZED BUSINESSES

TECHNOLOGY

Instant Internet

New Lease on Old Wires

MPLS and IPsec United

FOR SERVICE PROVIDERS: *NEW WORLD NEWS*

NWN

▼DEPARTMENTS

▼IN EVERY ISSUE

Packet magazine

David Ball
EDITOR-IN-CHIEF

Michael Hakkert
PUBLISHER

Jennifer McAllister
MANAGING EDITOR

Joanie Wexler
CONTRIBUTING EDITOR

Gail Meredith
CONTRIBUTING EDITOR

Gary McCavitt
CREATIVE DIRECTOR

Linda Mayer, Bill Littell
PRODUCTION COORDINATORS

Emily Burch
DESIGNER

Ellen Abbott
DIAGRAM ILLUSTRATOR

R.J. Smith
Sunset Custom Publishing
PROJECT COORDINATOR

Larissa Linn, Mark Ryan
Sunset Custom Publishing
PRODUCTION

Cecelia Glover
CIRCULATION MANAGER

Sarah Beaver
ONLINE EDITOR

Chris Gall
COVER ILLUSTRATION

SPECIAL THANKS TO THE FOLLOWING CONTRIBUTORS: David Baum, David Barry, Lawrance Binda, Roger Delacruz, Tom Fermazin, Michael Fuhrman, Sheri Gunderson, Janice King, Gene Knauer, Kurt Kruger, Renee LaBarge, Chris Lonvick, Rhonda Raider, Jen Siegal, Doug Webster

ADVERTISING INFORMATION:
Kristen Bergman, 408 525-2542
kbergman@cisco.com

View *Packet* magazine at cisco.com/go/packet.

PUBLISHER INFORMATION:
Packet magazine is published quarterly by Cisco Systems and distributed free of charge to users of Cisco products.

Direct address corrections and other correspondence to packet@cisco.com or to *Packet* in care of:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California, 95134-1706
USA
Phone: 408 526-4000

This publication is distributed on an "as-is" basis, without warranty of any kind either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This publication could contain technical inaccuracies or typographical errors. Later issues may modify or update information provided in this issue. Neither the publisher nor any contributor shall have any liability to any person for any loss or damage caused directly or indirectly by the information contained herein.

This magazine is printed on recycled paper.

10%
TOTAL RECOVERED FIBER

BROADCAST ADDRESS

Securing Your Future

As more companies move their businesses online to reap the benefits the Internet provides, they also become increasingly more vulnerable to network security threats. Last year's denial-of-service attacks against major Web sites, and the scores of viruses such as "I LOVE YOU" and Navidad, may be fodder for world news, but hundreds more, less-publicized attacks cause billions of dollars worth of damage annually.

The Computer Security Institute (CSI), in its fifth annual survey conducted with the help of the US Federal Bureau of Investigation's (FBI's) Computer Intrusion Squad, found 273 US organizations reporting US$265 million in financial losses over the last year due to computer crime. A full 90 percent of survey respondents, primarily large corporations and government agencies, detected security breaches of their systems within the last 12 months. Seventy-four percent acknowledged financial losses due to computer breaches.

RICHARD PALMER

Cisco customers recognize this as an ongoing—even accelerating—problem, and are progressively seeking guidance from Cisco on how to secure their e-business environments. In the last few years, Cisco has gained a reputation in the security and VPN markets as a leader and trusted partner, offering the broadest range of security products in the industry. Recent market analyst reports cite Cisco as the leading vendor of key security and VPN solutions, including firewalls, intrusion detection systems, VPN devices, and VPN-enabled routers.

Always working to improve the security of its customers' systems, Cisco recently launched SAFE, a flexible security blueprint to help organizations securely compete in the Internet economy (see "Play It SAFE, Sam," page 66).

Speaking of which, in "Security in the Internet Economy," our *Packet* cover story (page 54), Gartner Group's John Pescatore writes about the trends that are driving security deeper into the network fabric. Cisco has already made great strides in this arena, introducing intrusion detection systems, firewalling, and other security features into the Cisco IOS® software and a variety of connectivity devices. New products such as the Catalyst® 6000 IDS Module offer full intrusion detection capabilities in a switched environment. You can read about these and other products for building scalable, secure networks in "Security Blanket: Weaving Security into the Network Fabric" (page 61).

Additional articles in this issue that focus on security topics include "Defensive Attitude: Strategies for Dealing with Hackers and Crackers" (page 71), which provides a psychological profile of the various types of "bad guys" lurking in cyberspace, and what you can do about it. For more on hackers, turn to "The Twilight Zone: Covert Conversations with Dr-K, a Real-Life Hacker" in our Netizens column (page 50).

"End-to-End Confidence" on page 78 offers a case study of the first company to process mortgage loans entirely over the Internet, highlighting HomeSide Lending's critical need for network security. In "PIX of the Litter" (page 75), we introduce you to the PIX 535, the newest and biggest addition to the Cisco Secure PIX Firewall family, as well as a new VPN accelerator card for the firewall line. Finally, Cisco's Jeremy Stieglitz takes us on a quest for selecting the right mix of technology for identifying and verifying users in "Who Goes There," a special, security-focused Technically Speaking column (page 89).

Network security is a concern for all, whether you're an enterprise, small or midsized business, or service provider. As the worldwide leader in networking for the Internet, Cisco is uniquely positioned to help organizations secure their networks as they open more doors to more users in the Internet economy.

Richard W. Palmer, Jr.

Richard Palmer
Vice President and General Manager
VPN and Security Services Business Unit

Mail

The following letters were in response to Networkers technology session articles that ran in the Q4 2000 issue of Packet™. Replies are from the Cisco Networkers session presenters. —Eds.

MPLS, IS-IS, and OSPF

I would like to thank you for your Multiprotocol Label Switching [MPLS] article in *Packet* magazine ["Express Delivery," Q4 2000]. Good job!

I'm in the middle of doing some MPLS investigation on the Great Plains network, an Internet2 GigaPOP regional network. I have two Cisco GSRs running IOS Release 12.0(13) and between them is running IOS 12.1(1)E (for QoS Manager). All three seem to have an odd mix of MPLS-related commands and tag-switching commands. Could you clarify? Should I be using only the MPLS commands now that MPLS is the standard? Will the tag-switching commands be going away?

Also, what, if any, is the difference between IS-IS [Intermediate System-to-Intermediate System] and OSPF [Open Shortest Path First] in an MPLS network? Is one better? We have an OSPF-run network now, and I don't see going to IS-IS unless it's absolutely required.

—Dave Hartzell, Raytheon, USGS EROS Data Center
hartzell@usgs.gov

*Tag switching is really the prestandard flavor of MPLS. Depending on the code you're on, some of the commands that say **tag** perform the same function as the ones that say **mpls**. The only noticeable difference is whether you run Tag Distribution Protocol (TDP) or Label Distribution Protocol (LDP) on a link. On the code you're running, you have no choice but to run TDP; that's all you've got.*

*Check **show tag int** to see what protocol you're running. I bet you'll find that even if you configure **mpls ip** on an interface, it shows up in the config as **tag-switching ip**. For now, don't worry about it. It's only an issue when you have to decide between TDP and LDP.*

Regarding IS-IS and OSPF, there's extremely little functional difference. Visit the URL www.nanog.org/mtg-0006/katz.html for a comparative anatomy of IS-IS and OSPF. Most early adopters of MPLS-TE are running IS-IS, and Cisco fostered this adoption by coming out with some features on IS-IS first. As a general rule, the most important thing about your routing protocol is that you know it. If you're comfortable with OSPF, stay with that. It's far better, especially in an enterprise network like yours, to stick with what you know than to jump from one protocol to another.

—Eric Osborne, Internet Engineering Support Engineer
eosborne@cisco.com

Improve Bandwidth Over QoS?

I read "The Case for QoS" article [Q4 2000] on the Internet. I'm a network analyst at Embratel, an MCI company, and we are choosing a strategy to use video, multicast, and unicast in our corporate network. We have five sites connected by ATM with LANE version 1.0 implemented.

Even though we don't have problems raising bandwidth (links are what we sell), we're going to implement quality of service [QoS] mainly because of e-learning and videoconference applications. We want the video to work properly, but it's a noncritical application compared to our other services. What we expect from QoS is to guarantee that videoconference applications don't hog bandwidth and make it difficult to use other corporate services.

In your article you say, "At some point, having a large enough pool of bandwidth would eradicate network congestion, which is the crux of most service-level degradation." Does this mean, if possible, that it's better to improve bandwidth than expend money and time implementing QoS?

—Alaerte Gladston Vidali, Embratel
alaerte@embratel.com.br

It's a judgment call. You can delay the investment by using QoS, and you can decide what you need to do by performing the QoS analysis. If you make the link be 50 to 70 percent utilized by throwing bandwidth at it, delays will be nominal, as will variation delay. It's your money.

For my money, I'd put voice into a priority queue and video in a queue with a rate on it, and maybe provide two data queues both running Assured Forwarding (AF), and sell the fact that I'm doing so as a service.

Folks can negotiate with you what rates they want for what and still have the insight that as their mission-critical data and video grows, it squeezes other data. This fact then becomes a powerful argument for them to upgrade their overall bandwidth. Apart from that insight, folks tend instead to say "My service provider drops a lot of traffic" without realizing or taking into account their own behavior's interaction with the fact.

But that's me.

—Fred Baker, Cisco Fellow and IETF Chairman
fred@cisco.com

SEND YOUR COMMENTS TO *PACKET*

We welcome your comments and questions. Reach us through e-mail at packet-editors@cisco.com. Be sure to include your name, company affiliation, and e-mail address. Letters may be edited for clarity and length. **Note**: The *Packet* editorial staff cannot provide help-desk services.

Cisco Experts Pinpoint Network Vulnerabilities

Cisco Secure Encyclopedia helps users thwart network attacks.

THE CISCO SECURE CONSULTING Services group routinely tests live customer networks to uncover security holes in operating systems, network services, and authentication schemes. Last year, the group released the *Vulnerability Statistics Report*, a study that evaluated the state of corporate network security based on Cisco assessments of 46 customer networks over a six-month period. Now, Cisco customers, business partners, and other authorized users of the Cisco.com Web site can also access the group's full security vulnerability database—called the *Cisco Secure Encyclopedia*—at cisco.com/cgi-bin/front.x/csec/csecHome.pl as an additional security resource.

The *Cisco Secure Encyclopedia* logs actual security holes found by Cisco consultants in customer networks. There are several other public repositories of security vulnerability information available as well, such as the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon (www.cert.org). "However, with some of these sites, it's unclear if the vulnerability has or ever will be seen outside of a test lab," says David Phillips, a Cisco security consultant who conducts security assessments of Cisco customer networks.

The *Cisco Secure Encyclopedia*, on the other hand, is based on assessments of live production networks. It is intended to help users benefit from others' experiences by providing real-life examples of where security exposures might exist and advising users on the appropriate action to take to minimize or eliminate them.

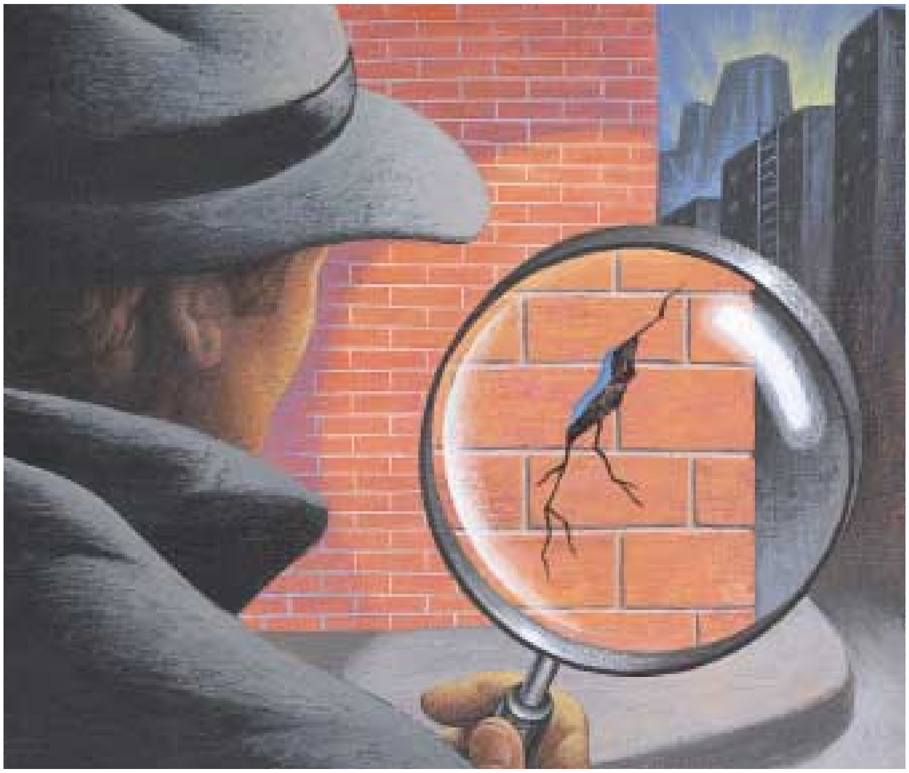


ILLUSTRATION BY GEORGE ABE

The encyclopedia is regularly updated with knowledge garnered from ongoing Cisco customer security assessments. Users can analyze the data in several ways, such as by vertical industry and whether a vulnerability is greater from inside or outside of an organization. There are instructions for how to counteract the vulnerability, and links to downloadable software patches are provided.

The State of Network Security

"You would think that as we enter the 21st century, networks would be getting more secure. But the reality is that the extremes are getting more extreme," observes Phillips. "Some companies are not protecting themselves at all. Others are overcompensating, which can sometimes be unnecessarily expensive for them."

According to Phillips, however, companies can minimize most security exposures by upgrading software and instituting better administrative procedures. Often, services running on Internet-connected devices, for example, can simply be disabled to plug chinks in an organization's security armor.

Top-Ranking Exposures

By conducting its customer security assessments, Cisco Secure Consulting Services has identified the vulnerabilities that tend to hold the greatest potential for misuse.

- **Remote Procedure Call (RPC)**. These programs top the list of services most susceptible to Internet attacks. In cases where Internet-connected RPC programs were uncovered, they were found to be vulnerable 93.4 percent of the time. The reason is that when these programs, which let one computer execute a program on another, are running on systems connected to the Internet, they can leave a port open—a potential access point for network hackers.

"Because [RPC] executes programs as a privileged user, security problems with RPC are generally ranked high," explains Phillips. "Unpatched problems with UNIX RPC give remote attackers complete control over the system."

RPC services with external Internet access are typically not required, so Cisco security consultants recommend disabling the RPC portmapper service—a function that provides information about which RPC network services are configured to run on remote network devices. Alternatively, according to Phillips, companies could deny all incoming RPC requests to TCP port 111. "There is rarely a business justification for running RPC over the Internet," Phillips explains.

- **Simple Mail Transfer Protocol (SMTP).** The second most vulnerable service identified by Cisco network assessments, SMTP, is often compromised by un-

MOST COMMON SERVICES

Ranking	Service	Percentage Found
1	Authentication/ Login	32.6
2	SNMP	23.1
3	NetBIOS	17.1
4	HTTP	8.2
5	FTP	6.5
6	SMTP	5.0
7	DNS	4.1
8	Finger	3.9
9	RPC	3.8
10	TFTP	3.4

Source: Vulnerability Statistics Report (11/5/2000).

WHAT'S EXPOSED? By understanding which of their network services are accessible via the Internet, companies can determine the risk associated with those services and take appropriate action.

MOST VULNERABLE SERVICES

Ranking	Service	Percentage Found
1	RPC	93.4
2	SMTP	61.1
3	Finger	59.6
4	TFTP	57.4
5	DNS	35
6	FTP	33
7	NFS	30.2
8	SNMP	27.1
9	HTTP	26.7
10	X Window System	23.0
11	Authentication/ Login	19.9

Source: Vulnerability Statistics Report (11/5/2000).

HIGH-RISK BEHAVIOR: Cisco consultants ranked the most vulnerable Internet services in customer networks by determining the percentage of instances in which the service was visible and found to have a security problem.

patched Sendmail installs or incorrectly configured Sendmail daemons. If an SMTP server is accepting Internet connections, there's approximately a 61 percent chance that it will be misconfigured or that it's running outdated software that contains security bugs. The ramifications range in severity from giving out user names to allowing an attacker to launch a privileged program.

- **Denial of service (DoS)**. The infamous DoS attack is another form of security problem that can paralyze a corporate server or Web site. According to the Cisco *Vulnerability Statistics Report*, about 5 percent of the 9874 network interfaces at the 46 companies assessed last year were exposed to this form of hacking. Those interfaces together supported more than 33,000 Internet-accessible services.

Most DoS exposures found in Cisco assessments targeted individual workstations or network devices and were attributable to outdated and unnecessary services. For example, DoS exposures often came from the use of the Bootstrap Protocol (BootP) on Internet-connected servers. BootP allows users' computers to automatically configure necessary Internet information from a centrally maintained server. If Dynamic Host Configuration Protocol (DHCP) is supported, network administrators should restrict access to the BootP service from the Internet by disabling it or by filtering it with a firewall, Cisco security consultants advise.

DoS can also be caused by a buffer overflow problem associated with anonymous File Transfer Protocol (FTP) services. Anonymous FTP allows anyone to upload or download files to an FTP server after logging in with the username "anonymous," which can overload a server or grant network access to miscreants. Vulnerable versions of FTP should be upgraded. A more secure solution is to disable anonymous FTP on all network devices accessible by the Internet.

"In addition, outdated services like Discard, Chargen, and Echo, which tend to be preconfigured on UNIX servers and network devices, could be used to cause DoS attacks," adds Phillips. Disabling these, he says, is a good idea.

DoS attacks using Internet services such as these differ widely from the recent distributed DoS (DDoS) attacks that use address spoofing or SYN flooding—whereby a host sends out a large number of TCP/IP packets with an unreachable source address—to compromise a network's infrastructure.

Uncommonly Vulnerable

It's promising to note that several of the services deemed most vulnerable are not necessarily the most frequently deployed with Internet connectivity. Certain services in the assessed customer networks, when active, were often vulnerable, but often were not found to be running on Internet-accessible systems.

A good example of this is Network File System (NFS). In more than 30 percent of the instances in which Cisco consultants found NFS running on Internet-accessible configurations, it was vulnerable to attack. However, encouragingly, Cisco assessments found that most companies realize the futility and risk in using NFS over the Internet and avoid doing it.

"We found that NetBIOS was the third most prevalent Internet service, though we see no reason why NetBIOS should be run across the Internet," says Phillips. His theory is that instances of Internet-connected NetBIOS were commonly found because several companies had no filtering capabilities, making direct access from the Internet into the internal network possible.

◆ ◆ ◆

For more information and findings from the Cisco Secure Consulting group, visit the following URLs:

Cisco Secure Consulting Services:
cisco.com/go/securityconsulting

Cisco *Vulnerability Statistics Report*:
cisco.com/warp/public/778/security/vuln_stats_02-03-00.html. ▲▲

Cisco Headquarters

▸ **Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
USA
www.cisco.com
Tel: 408 526-4000, 800 553-NETS (6387)
Fax: 408 526-4100

▸ **European Headquarters**
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

▸ **Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

▸ **Asia Headquarters**
Cisco Systems Australia Pty., Ltd.
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: 61 2 8448 7100
Fax: 61 2 9957 4350

Cisco Worldwide Events

Jan. 29–Feb. 1	ComNet 2001, Washington DC, USA
February 20–23	Internet World Wireless, New York, New York, USA
March 6–8	Computer Telephony 2001, Los Angeles, California, USA
March 17–22	Optical Fiber Communication, Anaheim, California, USA
March 20–23	Voice on the Net 2001, Phoenix, Arizona, USA
March 22–23	Networkers Seoul, Korea
March 28–30	Networkers Brisbane, Australia
April 11–13	Networkers Japan, Makuhari Messe

cisco.com/warp/public/688/events.html

Cisco Career Recertification Policy Extended, Worldwide Testing Centers Added

Recertification is now available for all Cisco Career Certifications associates and professionals. Previously applicable only to Cisco Certified Internetwork Expert (CCIE™) recipients, certification renewal has been extended to include:

- Cisco Certified Network Associates (CCNA™)
- Cisco Certified Design Associates (CCDA™)
- Cisco Certified Network Professionals (CCNP™)
- Cisco Certified Design Professionals (CCDP™)

CCNA, CCDA, CCNP, and CCDP certifications are valid for three years; CCIE and career specializations are valid for two years. Renewing a Cisco associate or professional certification requires passing the appropriate recertification exam before expiration. Alternatively, certifying for a more advanced level also recertifies an individual's existing certification.

Information on recertification requirements, certification expiration dates, and training opportunities with Cisco Learning Partners are available at the URL cisco.com/go/certifications.

In related news, Cisco has expanded its roster of career certification exam testing centers to include Virtual University Enterprises (VUE). VUE (www.vue.com) provides users with 2400 additional test locations worldwide as well as an Internet-based certification testing system.▲▲

New Web Tool Matches Features to the Right Cisco IOS Release

Is RSVP supported in Cisco IOS® Release 12.0(3)T on a Cisco 3600 router? A new resource from the Cisco Technical Assistance Center (TAC) helps users find the answer quickly and easily. Called Cisco Feature Navigator, this application determines which Cisco IOS software images support a particular set of features or which features are supported in a particular Cisco IOS release or image. Feature Navigator currently supports Cisco IOS releases 11.2, 11.2P, 11.3, 11.3T, 12.0, 12.0T, 12.1, and 12.1T. It's available to all registered Cisco.com users and can be accessed at the URL cisco.com/go/fn.

Tech Tips

Get the scoop on the top support issues. Updated quarterly, the "Top Issues" section of the Cisco Technical Assistance Center (TAC) Web site addresses and resolves the most common networking challenges reported by Cisco customers worldwide. Find out the most common recurring cases in technology areas such as virtual private networks (VPNs), PIX™ firewalls, cable, wireless, and packet voice.
cisco.com/tac

Opening an IP Security (IPsec) LAN-to-LAN tunnel with a Cisco Secure PIX Firewall and VPN 5000 concentrator? From network diagrams to debug and show commands, this sample configuration shows you how.
cisco.com/warp/public/110/pixto5000.html

Lock users into a Cisco VPN 3000 concentrator group. With the Cisco VPN 3000 concentrator lock feature, access restrictions can be applied to various groups configured on the concentrator with assurance that users are locked into that group. This document has the details.
cisco.com/warp/public/471/altigagroup.html

Overcome compatibility issues with interface cards and Catalyst® switches. This how-to guide lays out the steps for troubleshooting common issues associated with network interface cards interoperating with Catalyst switches. Among the topics addressed are slow network performance, auto negotiation, physical connectivity, and data-link errors.
cisco.com/warp/public/473/46.html

Increase your knowledge of Cisco Secure VPN Client View Log. From error message and Internet key exchange (IKE) messages, these technical notes describe Cisco Secure VPN Client View Log messages and explain how to use the messages to troubleshoot problems with establishing IPsec communications.
cisco.com/warp/public/707/csvc_log.html

Using Multiprotocol Label Switching (MPLS) over virtual path tunnels? Look here first. This overview provides the sample setup and commands needed to configure MPLS when using virtual path tunnels.
cisco.com/warp/public/121/mpls_vptunnel.html

Learn the basics of Simple Network Management Protocol (SNMP) traps. A primer on the basic understanding of SNMP traps, this document explains how they're used and the role they play in managing a data network.
cisco.com/warp/public/477/SNMP/snmp_trap.html

Pick up the vernacular on Frame Relay. From "access line" to "trunk line," let the *Frame Relay Glossary* spell it out for you.
cisco.com/warp/public/74/87.html

For more Tech Tips from Cisco, visit the URL cisco.com/public/technotes/serv_tips.shtml.

New Cisco Online Community Provides Forum for Sharing Technical Expertise

Cisco recently launched an online community that enables network managers and other technical users from all-sized businesses to stay up to date on the latest technology and news as well as share their expertise and experiences in an open forum. Called Networking Professionals Connection (cisco.com/go/netpro), the interactive site features sections devoted to “Discussion Forums,” “Tech Talks,” and “Ask the Expert” events. An opt-in biweekly newsletter subscription is also available to users of the site.

“At this site, technical users can offer their ideas and opinions and questions of a worldwide community of networking professionals,” says Helen Lechner, Cisco’s Networking Professionals Site Manager. “Members benefit by getting answers to their questions, learning from the networking experiences and best practices of their peers, as well as getting news and information about technology.”

In addition to “Ask the Expert” question-and-answer sessions on specific networking topics conducted by Cisco technical staff, Networking Professionals Connection offers discussion forums on a variety of topics, including IP telephony, video over IP, and virtual private networks (VPNs) security and network management.

Everyone is welcome to visit the site; however, users must register on Cisco.com to post items on the message boards and participate in question-and-answer sessions.

Live, online technical presentations called “Tech Talks” are also available on a broad range of topics such as Cisco content delivery networks, intelligent network services, and remote-access and site-to-site VPNs. “Tech Talks” are archived on the site.

Visit Networking Professionals Connection at the URL cisco.com/go/netpro.▲▲

Recent Cisco Acquisitions

Acquired	Key Technology	Employees	Location
Active Voice Corporation	*Facilitates unified communications on a single, end-to-end, converged IP network for corporate enterprises.* Unified messaging solutions consolidate voice mail, e-mail, and fax messages into a common mailbox accessible via any Internet-connected device anywhere, anytime.	approx. 210	Seattle, Washington, USA
CAIS Software Solutions	*Helps carriers provide and manage high-speed, broadband Internet services in the multiunit building market.* Server-based software applications complement Cisco’s existing in-building Digital Subscriber Line (DSL), Ethernet, cable, wireless, and VPN network solutions for hotels, apartments, and other multiunit buildings. The broadband service management solutions provide security, authorization, accounting, billing, reporting, policy, and management functionality.	65	San Diego, California, USA
IPCell Technologies, Inc.	*Supports new IP-based integrated voice and data services.* Software for broadband access networks that combine IP and telephony services. An interface between the call control and service layers for voice-over-packet applications helps service providers deliver high-demand IP telephone services.	110	Richardson, Texas, USA
PixStream, Inc.	*Enables reliable distribution and management of digital video and streaming media across broadband networks.* Software solutions that help network service providers and enterprises deliver and manage IP-based entertainment services such as broadcast video, video-on-demand, and multiplayer games over broadband.	156	Waterloo, Canada
Radiata, Inc.	*Expands Cisco’s ability to deliver next-generation wireless networks using the IEEE 802.11a standard.* Semiconductor technology and extensive radio and modem systems expertise for wireless networks that will operate in the unlicensed 5-GHz frequency range and enable wireless communications between devices at speeds up to 54 Mbps	53	San Jose, California, USA and Sydney, Australia
Vovida Networks, Inc.	*Supports development of new voice-over-IP applications for service providers.* Communications software and networking protocols help expand Cisco’s solutions for service providers who want to deliver data, voice, and video services over packet networks.	65	San Jose, California, USA

Acquisitions from August 31, 2000 to December 12, 2000. For more recent details on Cisco acquisitions, visit the URL cisco.com/warp/public/750/acquisition/.

ILLUSTRATION BY JOHN RITTER

Securing the Mobile Enterprise

Cisco Instant Internet Initiative enhances mobile network security and related products.

INCREASED MOBILITY IS A KEY BENEFIT OF an internetworked society. With the proliferation of mobile technologies and devices—forecasts by Forrester Research and others suggest that 50 to 80 percent of mobile devices worldwide will be data-enabled by 2003—Cisco has moved aggressively to extend the wired network through secure mobile technologies that businesses and service providers can take confidence in.

Security barriers to wireless LANs (WLANs) have tumbled, thanks to features such as IP Security (IPsec) and Mobile IP in Cisco IOS® Release 12.0 and higher. Interoperability advances made through the IEEE 802.11 wireless standard—such as the Extensible Authentication Protocol (EAP) and dynamic Wireless Equivalent Privacy (WEP) protocol—also provide key encryption and management options enterprises need to safeguard their mobile networks.

"In the past, security was a big stumbling block to making enterprise resources available to employees on mobile devices outside the firewall," says Prasanna Satarasinghe, a product manager in Cisco's Enterprise Line of Business. "But now we've added reliable security measures like IPsec for virtual private networks and dynamic administration and management of public and private encryption keys. Together, these security features are a big leap forward in providing mobile data access from different venues outside the corporate office."

Greater security, faster WLANs, mobile features added to Cisco IOS software, and an array of mobile networking products are the fuel behind Cisco's Instant Internet Initiative. Cisco Instant Internet is a concerted effort to provide secure mobile network technology in key service areas: the workplace, the home, on the road, and in public venues through wired and wireless network access.

Wired VPNs

Wired virtual private networks (VPNs) have allowed users to connect to their home environments using small, portable devices such as pagers. With recent advancements such as extensions to Internet Control Message Protocol (ICMP)-Router Discovery Protocol (IRDP), products can recognize whether users are at home or on the road and adapt the forwarding of information to fit profiles set up by the users themselves. Such extensions give users the ability to get information they need when they need it, with Mobile IP providing the underlying network service. (See "Mobility for the Masses," page 85.)

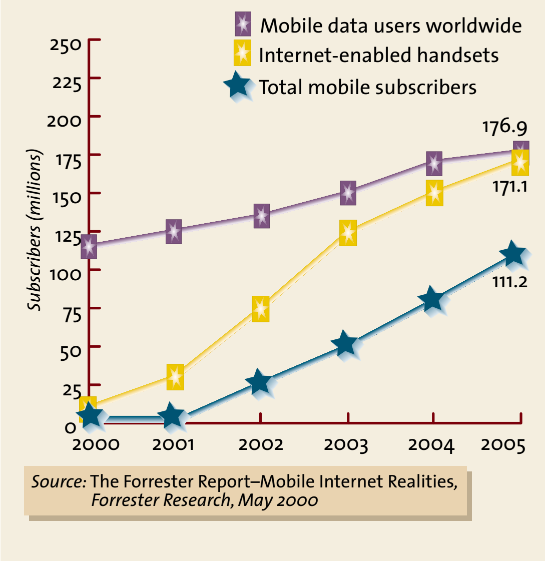
The Cisco Internet Mobile Office

Complementing Cisco's Instant Internet Initiative is the Cisco Internet Mobile Office Initiative, which focuses on providing seamless solutions for road warriors—business professionals in sales, service, marketing, delivery, and other highly mobile roles who are the most likely to be early adopters of mobile access to corporate data. The aim of the Cisco Internet Mobile Office is to install mobile access points in public venues frequented by road warriors such as airports, hotels, and convention centers. For more information on the Cisco Internet Mobile Office, visit cisco.com/go/mobileoffice.

Read more about Cisco Internet Mobile Office in the upcoming issue of *Packet* (Second Quarter 2001).

Fruits of the Cisco Instant Internet Initiative, Cisco's secured mobile solutions give network managers in corporate enterprises and business users who desire wired and wireless access outside of the office the unprecedented benefits of anytime, anywhere, anyway access to corporate information and services from laptops, cellular phones, pagers, and personal digital assistants (PDAs).

MOBILE WORKERS ON THE RISE 2000-2005



Source: The Forrester Report–Mobile Internet Realities, *Forrester Research, May 2000*

Advances in Mobile Security

"The lack of centralized, scalable security and security administration has been a real problem in mobile enterprises," says Kittur Nagesh, a product manager for WLAN technologies at Cisco. "Companies have been very reticent to expose their network resources to mobile access. But our enhanced security services for mobile LANs bring together identification, authentication, and encryption with centralized management. The security features can be easily integrated with enterprise services such as mobility and quality of service."

For example, IPsec became standard fare in Cisco IOS Release 12.0. A set of security protocols developed by the Internet Engineering Task Force (IETF), IPsec provides authentication and encryption over IP networks. Cisco IOS Release 12.0 also includes time-based access control lists (ACLs) that enable network administrators to monitor and grant or deny user access rights based on organizational policies and time of day. Additionally, Java blocking, intrusion detection and prevention, and audit trail features are included in the software.

For business users on the go, Cisco IOS software also integrates Mobile IP, a tunneling-based solution that takes advantage of Cisco's Generic Routing Encapsulation (GRE) tunneling technology. With this approach, Cisco routers at each site encapsulate protocol-specific packets in an IP header, creating a virtual point-to-point link to Cisco routers at other ends of an IP cloud. A router on a user's home subnet can intercept and transparently forward IP packets to users while they roam beyond traditional network boundaries.

This approach is a key enabler of mobility, both for IEEE 802.11 standards-compliant WLANs and for secure transmission of data in concert with an array of cellular standards. When accessing the enterprise using a mobile device, users log in and are prompted for a password. Once authenticated via EAP, the system generates a private encryption key, while a random public key is automatically generated by the system.

In the past, encryption keys for mobile data products had to be manually entered by network administrators, but Cisco-enhanced mobility products employ security options such as WEP for Web-based 40- and 128-bit encryption. Cisco IOS software allows for the mobility keys to be stored on an authentication, authorization and accounting server that can be accessed via Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS). This technique is highly scalable for large numbers of mobile users and provides network managers a single place for maintenance.

Such mobile network security advances have broadened enterprises' mobility far beyond campus LANs to the home and into cellular communications and "extended campuses" that include public venues such as airports, hotels, and conference centers.

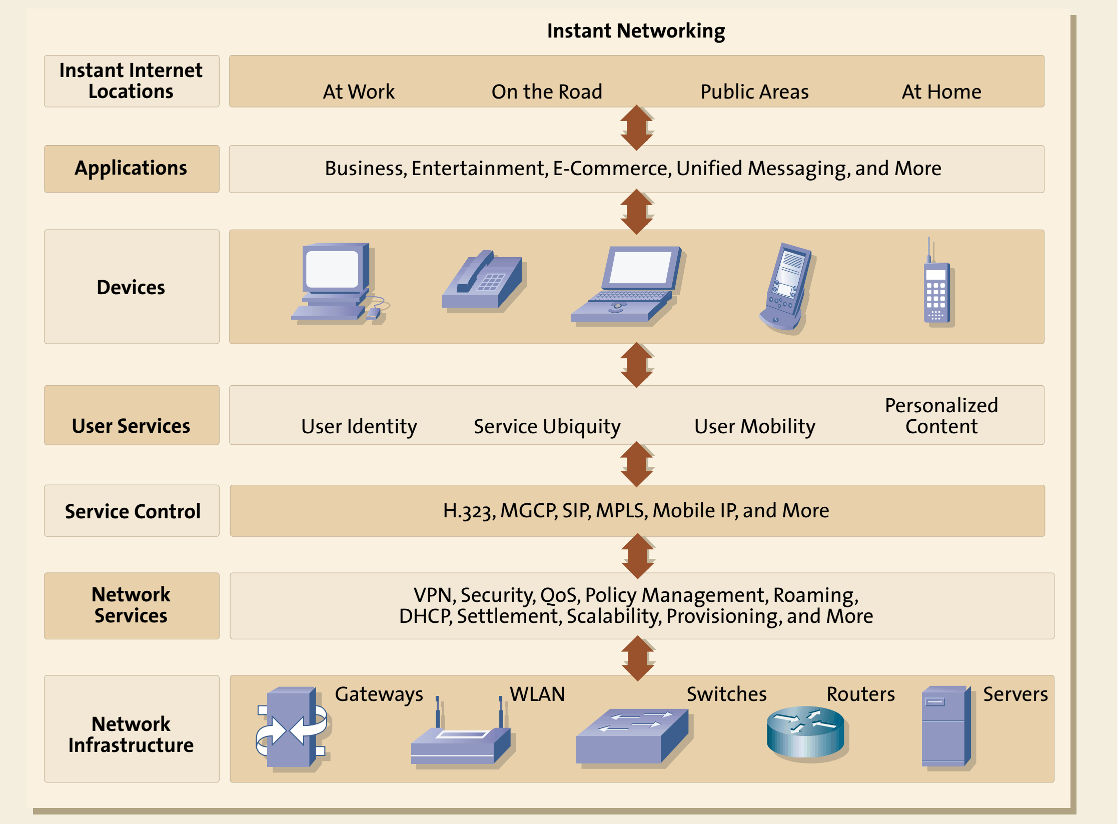
In anticipation of the expected demand from enterprises for WLAN mobility, service providers are gearing up. Cisco's mobility product line for service providers includes the Cisco VPN 5000 concentrator series, which can support 40,000 simultaneous user sessions. The Cisco VPN 3000 concentrator series is designed for enterprises that want to deploy mobile VPN services themselves.

Mobile Workers, Benefits Abound

Certain categories of workers such as those in sales and delivery can especially benefit from mobile access to their company's intranet. Real-time routing, service, and delivery information accessible from the road via a wireless PDA or laptop greatly adds to customer service efficiency. What's more, global companies can use wireless devices

Continued on page 18

CISCO INSTANT INTERNET FRAMEWORK

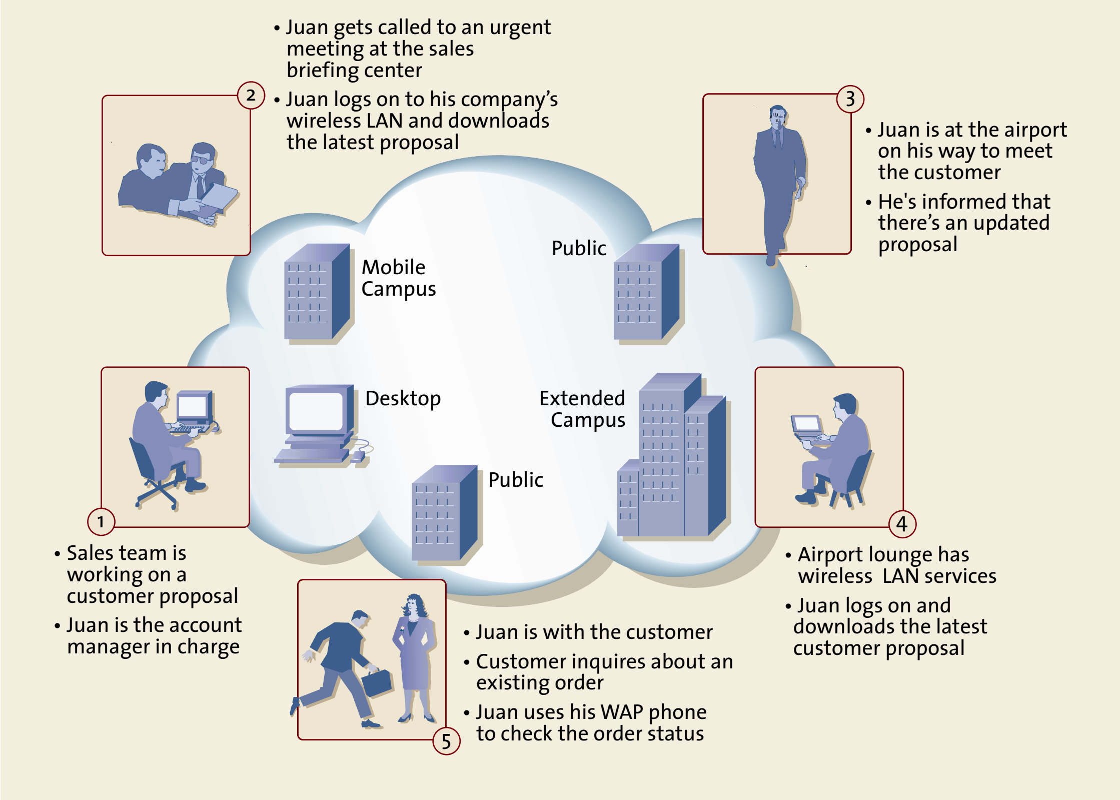


ENTERPRISE MOBILITY: The Cisco Instant Internet Initiative is composed of products, technology, and services that give users anytime, anywhere, anyway access to their corporate information.

Instant Internet, *Continued from page 15*

INTERNET ON THE FLY: Workers such as those in sales and delivery can especially benefit from immediate mobile access to their company's intranet.

INSTANT INTERNET IN ACTION


2
• Juan gets called to an urgent meeting at the sales briefing center
• Juan logs on to his company's wireless LAN and downloads the latest proposal
3
• Juan is at the airport on his way to meet the customer
• He's informed that there's an updated proposal
Mobile Campus
Public
Desktop
Extended Campus
Public
1
• Sales team is working on a customer proposal
• Juan is the account manager in charge
4
• Airport lounge has wireless LAN services
• Juan logs on and downloads the latest customer proposal
5
• Juan is with the customer
• Customer inquires about an existing order
• Juan uses his WAP phone to check the order status

to communicate with employees in different time zones.

To reap the most from these benefits, best-of-breed enterprise mobility solutions must embrace some key requirements. Topping the list is the ability for users to access corporate information from multiple devices securely and with the capability to get a usable, personalized view of the data.

"If you're on the road and want to access your department's phone list or your own spreadsheets, these applications must be available to you securely on whatever mobile device you choose," stresses Satarasinghe. "And the data must be customized to provide you with your own personal view and condensed to fit the reduced screen size of a cell phone, pager, or PDA."

"Cisco's mobile LAN products provide the glue that links wireless technology standards with the existing network infrastructure," says Satarasinghe. "We'll continue to refine security features to include biometrics such as user authentication via voice print analysis. While our solutions are the most sophisticated available to businesses, we're also dedicated to making each mobility feature easy to administer and manage by central network personnel and via intelligence in the network itself." ▲▲

FURTHER READING

To learn more about the technologies and products mentioned in this article, visit the following URLs:

- Wireless Ethernet Compatibility Alliance information on IEEE 802.11 and WLAN interoperability testing: www.wi-fi.org
- Cisco VPN 3000 concentrator series: cisco.com/warp/public/cc/pd/hb/vp3000/
- Cisco VPN 5000 concentrator series: cisco.com/warp/public/cc/pd/hb/vp5000/index.shtml
- Cisco WLAN products in general: cisco.com/warp/public/cc/pd/witc/ao340ap/index.shtml

Direct Connections

Travelocity.com traffic rides first class with InterNAP.

LIKE ITS MORE THAN 24 MILLION registered users, e-commerce giant Travelocity.com seeks the fastest, most direct and reliable routes to destinations near and far. For this immensely popular business-to-consumer travel site, though, the traffic mode isn't a plane, boat, or train. It's an innovative network architecture and peering-bypass service from InterNAP Network Services Corporation.

Travelocity.com is one of many content providers taking advantage of InterNAP's "one-hop" network design to improve their customers' e-commerce experiences. Centrally managed, Cisco-based InterNAP data centers forward Web requests directly to the IP backbone of the Internet service provider (ISP) to which an e-commerce site is connected.

> "In the six-week period ending November 21, 2000, our number of connections refused, connections timed out, connections reset, host/net unreachable, and page timeouts errors were less than half of one percent—which is fewer than half the number of errors that Keynote reported from our primary competitor."
>
> —RICHARD PENDERGAST, VICE PRESIDENT, TRAVELOCITY SYSTEMS

"Our company was created in 1996 to provide high-performance routing across the public Internet in a way that bypasses congestion points such as those often caused by peering," explains Oscar Stiffelman, Senior Software Engineer at InterNAP

Customers like Travelocity.com say InterNAP's network design is proving to be a more efficient setup than requiring requests to traverse multiple backbones, as is standard procedure in the best-effort Internet, which is based around a public ISP peering model.

Sidestepping Congestion

The direct connection from ISP backbone to commerce site via InterNAP data centers shortens the trip across the Internet, sidesteps congested Internet peering points, and consequently improves customer response times. Data to and from the Travelocity.com Web site, for example, bypasses heavily loaded public network-exchange points where thousands of ISPs hand off traffic to one another. InterNAP estimates that it is able to bypass these choke points 90 percent of the time.

"Because the Internet isn't centrally managed, it's often a source of traffic bottlenecks and broken links," says Richard Pendergast, Vice President of Travelocity Systems. "InterNAP's method of identifying the fastest route proves its worth to us daily in the performance and reliability of the applications on our site."

He explains that Travelocity.com, which began using the InterNAP service about a year ago, uses a third-party Web response-time measurement company called Keynote to track its Web site performance.

"One of the ways we measure the quality of our connectivity is by comparing it with our competition," Pendergast notes. "For example, in the six-week period ending November 21, 2000, our number of connections refused, connections timed out, connections reset, host/net unreachable, and page timeouts errors were less than half of one percent—which is fewer than half the number of errors that Keynote reported from our primary competitor."

Alternative to Traditional Peering

As network managers are well aware, customer response times can vary significantly based on the type of access connection used, time of day, and each user's geographic location. To help make user experiences more predictable and consistent, commerce site owners such as Travelocity.com link directly to one or more of InterNAP's 24 worldwide private network access points (P-NAPs). Each P-NAP has high-speed, direct connections to the Internet backbones of the world's ten largest ISPs, including AT&T, UUNET, Genuity, and PSINet.

When a customer sends a request to Travelocity.com, the InterNAP-connected ISP detects it and shuttles the message to the P-NAP, which in turn forwards it to Travelocity.com. The reply from the Travelocity.com Web site to the customer also travels via the P-NAP, sending the message using the customer's own backbone carrier and avoiding ISP-to-ISP peering.

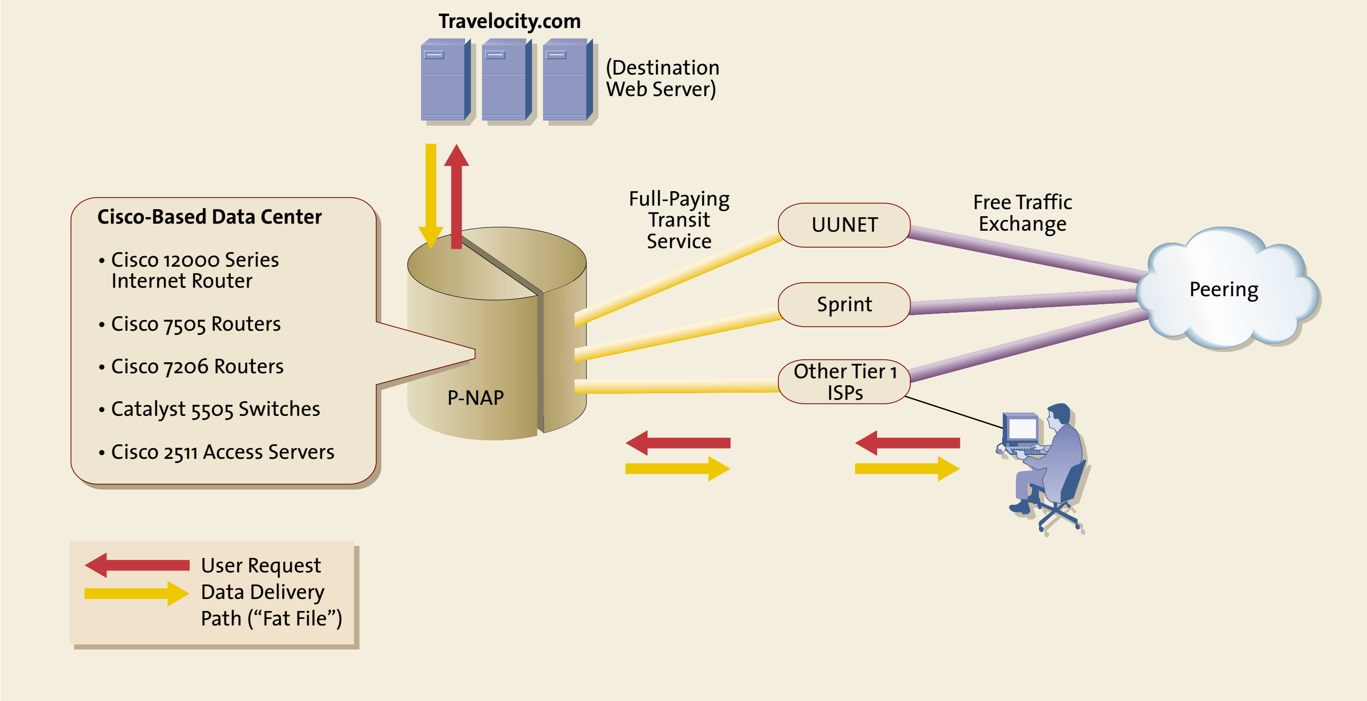
Inside the P-NAP

Supporting Travelocity.com—as well as major Web e-commerce sites such as Amazon.com, Datek Online, and NASDAQ—is a Cisco network infrastructure within InterNAP's P-NAP data centers. The infrastructure runs sophisticated routing protocol enhancements developed by InterNAP. The distributed routing architecture comprises Cisco 7206 series routers with Network Processor Engine (NPE) 200s and 12000 series Internet routers at the network border. These devices communicate via Fast Ethernet to Catalyst® 5505 switches that connect to Cisco 7505 routers in the core.

InterNAP added the Cisco 12000 series Internet routers to its topology recently to accommodate customers such as Travelocity.com that have requested more interfaces and higher speeds. Many major Internet commerce sites are moving from T1/E1 lines as their primary interfaces to fractional and full T3/E3 (45/33 Mbps) and OC-3 (155 Mbps) connections. Cisco 12000 Internet routers switch packets at up to 320 Gbps across their internal network switching fabrics and support as many as 15 WAN interfaces with speeds of up to OC-192c (10 Gbps).

In addition to the throughput and performance of these devices, Cisco IOS® software has enabled the border routers to run quality of service (QoS) features for

INTERNAP'S P-NAP DIRECT ROUTING



SHORTCUT CENTRAL: P-NAPs are at the heart of InterNAP's express IP delivery service. They support high-speed, "paid-not-peered" TCP/IP and enhanced BGPv4 connections to backbone providers using high-speed Cisco routers.

congestion avoidance and advanced queuing techniques to ensure the highest packet throughput without excess packet loss.

Along with its connections to all the major ISPs, a key contributor to InterNAP's ability to accelerate Web user response times is a routing optimization algorithm that interoperates with routers running Border Gateway Protocol version 4 (BGPv4). Developed by InterNAP and called ASsimilator, the software identifies the best-performing paths to any part of the public Internet and ensures that customers' traffic is routed along those paths. ASsimilator can make intelligent routing decisions such as choosing the fastest of multiple backbones across which to route data if the destination is multihomed.

A component of ASsimilator codenamed Cogitator chooses routes for packets in real time, taking into consideration the network conditions of the moment. "That data is then fed into a component of ASsimilator [codenamed Actualizer] that injects the information into Cisco routers, functioning as a bridge between the ASsimilator technology and the BGP world," notes Troy Sprenger, a Network Engineer at Sabre, Travelocity.com's parent company and a worldwide information technology provider to the travel and transportation industry. "The InterNAP system updates Travelocity's BGP routers as traffic conditions change, so traffic flows to the backbone provider along the best route."

The InterNAP design and software add up, in effect, to customer traffic traveling in the Internet "carpool lane."

InterNAP Business Model

InterNAP markets its services to both enterprises and service providers. It charges for the express-delivery service based on contracted QoS.

The business relationship between InterNAP and the large ISP backbone providers plays a big role in InterNAP's ability to deliver its service. InterNAP's connections to these providers don't represent free public or private peering, as has been the Internet delivery model for many years. Instead, InterNAP pays each of these backbone providers for full transit TCP/IP connectivity. This economics-based relationship between InterNAP and the major backbone operators provides customers with something that private and public peering relationships cannot offer: differentiated QoS. It also represents one of the first instances of settlement in the Internet community—a necessary step, say some, to enabling ubiquitous Internet QoS.

Bandwidth Aggregators

A side benefit to the InterNAP approach, according to Pendergast, is that InterNAP arranges for the connections from distributed Travelocity.com Web sites to the many major ISP backbones. This alleviates Travelocity from having to strike and manage relationships with multiple ISPs around the world.

QUICK TRIP: Users of Travelocity.com can make reservations on most of the world's airlines, 46,000 hotels, 50 car rental companies, and 70,000 vacation packages. The site also offers creative features such as the capability to enter a dollar amount and view a US map showing where one can travel for that price. These applications remain fast and stable, thanks to InterNAP-optimized routing technologies and a Cisco infrastructure.

"For us, InterNAP functions much like a consolidator," says Pendergast. "Travelocity could buy services from all of the backbone providers, but InterNAP has the routing algorithm and expertise as well as much more affordable bandwidth due to their volume purchases from the major carriers."

Pendergast adds that the InterNAP service prevents Travelocity.com from having to run its own Internet-connected data center in every country in the world.

InterNAP regularly monitors the major backbone provider networks for latency and congestion and updates Travelocity.com's routers using BGPv4. If the conditions dictate, traffic is routed directly to other ISPs, bypassing InterNAP.

"We have direct links to other ISPs for redundancy, and in some cases it's easier for us to send traffic through a secondary provider because it's closer to particular IP addresses," explains Pendergast. "The InterNAP system will tell us to do that. InterNAP has no vested interest in routing all of our traffic, just in optimizing it." But Pendergast concedes that most of Travelocity.com's traffic goes to InterNAP because of the wide connectivity offered and its routing optimization technology.

"As long as we keep our servers fast, they'll make the connections fast," says Pendergast. "They have the basics—performance and reliability—covered." ▲▲

Security Detail for DSL

Addressing Security Vulnerability of an Always-On DSL Connection

ILLUSTRATION BY SCOTT ROBERTS

Digital Subscriber Line (DSL) is fast becoming a popular technology for the networking needs of small and midsized businesses as well as corporate telecommuters. And for good reason: The benefits of DSL are real. It's affordable, provides connectivity up to 100 times faster than dialup, and can utilize existing copper phone lines and handle voice and data simultaneously over the same line. Perhaps best of all, DSL gives businesses an always-on connection 24 hours a day, seven days a week.

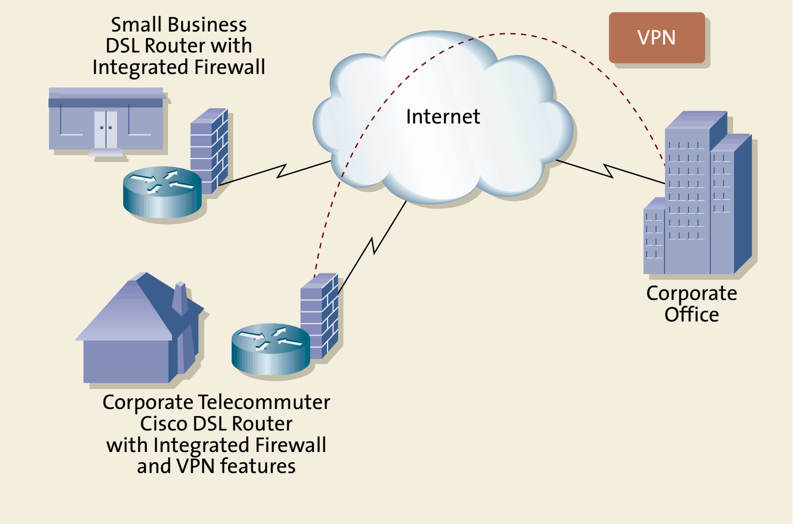
DSL also poses a very real security risk. Its appealing, always-on status leaves companies' private intellectual property vulnerable to unauthorized access. But it doesn't have to be that way.

In addressing the security risk, Cisco offers businesses several options for keeping their proprietary data safe and secure—while enjoying the benefits of DSL.

Vulnerable to Trespassers

The security issues of DSL have gone unnoticed by many users as they've become accustomed to traditional dialup Internet access, which relies on dynamic IP addressing. An analog modem secures a connection for a one-time session, assigning a new IP address each time

DSL SECURITY



PRIVACY PLEASE: Among Cisco's DSL business security solutions is the fixed-configuration Cisco 827 ADSL router with integrated firewall and VPN features for small businesses and corporate telecommuters.

> One of the major risks businesses face in the wake of a cyber security breach is the potential damage to their company's reputation and the erosion of customer confidence.

a user dials in. DSL, by contrast, typically uses static IP addresses, and the fact that the connection is always on potentially gives hackers 24-by-7 access to resources.

"The liability of a static IP address is that it presents a stable, long-term target that hackers, disgruntled employees, or any other unwanted intruders can use to trespass into the network," explains Marc Bresniker, a product marketing manager in Cisco's Premises Communications group. "Unfortunately, there are malicious people out there who probe network connections and IP addresses looking for an opening or vulnerability."

According to research from International Data Corporation (idc.com), one of the major risks businesses face in the wake of a cyber security breach is the potential damage to their company's reputation and the erosion of customer confidence.

"Without the proper security measures in place, a company compromises not only its own resources, but the resources and confidences of its customers and clients," Bresniker points out. "For example, a law firm that doesn't secure its network is putting its client affairs and correspondences at risk."

Firewalls can help eliminate unauthorized access to a company's network. They work by filtering traffic and denying or permitting access based on rules such as source or type of traffic. This process keeps the network perimeter secure. But when using the Internet to communicate between offices or with partners and vendors, businesses must also ensure that their confidential information remains safe while traversing the public network. Virtual private networks (VPNs) keep data safe by using secure tunnels and encryption to connect two networks over the Internet.

"A lot of the information I handle is proprietary," notes Bill Rolland, a business writer who creates scripts, speeches, and Web content for corporations in San Francisco, California, and surrounding cities. "If anyone intercepted my transmissions or had access to my computer, I'd have a huge legal liability on my hands. In most cases, I've signed nondisclosure agreements in which I promised to keep a company's information secure."

Locking the Gate

Businesses have several options for securing their DSL connections. One solution, says Bresniker, is to set up a DSL router with an integrated firewall and VPN features, which can be managed by in-house information technology (IT) staff. Another option is to rely on service providers to deploy, configure, and manage the router and security software or to offer security services through equipment in the provider's central office.

"The DSL security choice for businesses can be compared to getting physical security in your home," suggests Bresniker. "In the home, you can install a private alarm system—which for businesses is using a router with integrated security features—or you can move into a gated community, which is akin to letting service providers handle the security for you. In either case, Cisco has a solution that's reliable, affordable, and easy to deploy."

Install a Private Security System

Nearly all of Cisco's routers can provide integrated security features with support for firewalls and VPNs, which leverage Cisco IOS® software. While firewall and VPN security was once suited mostly to the budgets of large companies, it's now affordable for all-sized enterprises.

"A small business with 20 people, for instance, can add firewall and VPN capabilities to a Cisco 827 ADSL router for just a small additional cost," adds Bresniker.

Or Opt for the Gated Community

With the Cisco 6000 series IP DSL switch deployed from a central office, service providers can deliver additional security and routing intelligence to businesses and residential users. The evolution of existing Cisco smart DSLAMs, the Cisco 6000 IP DSL switch supports intelligent IP and ATM capabilities along with multi-DSL technologies for central offices worldwide, remote terminals, and multidwelling units. In addition to secure, specialized services, VPNs can be enabled in the IP DSL switch for site-to-site communications.

Building Security through Awareness

In addition to hardware and software protection, advises Bresniker, businesses should establish a security policy that lays out guidelines for everything from physical security to user authorization and passwords. The policy should specify how to configure firewalls, when and how to use VPNs, how users should communicate over the Internet, and any other security-related issues unique to individual businesses.

As businesses increasingly leverage DSL to expand telecommuting, improve Internet-based services, and reduce costs, they must take security precautions. While static IP addresses can leave the door open for unwanted intruders to the company network, this vulnerability is easy to correct.

"Whether a business decides to implement DSL security in-house or turn to a service provider for help," concludes Bresniker, "Cisco has the solutions to make businesses confident that their company data will remain private and safe."

For more on Cisco DSL products and news, visit the URL cisco.com/go/dsl. ▲▲

FURTHER READING

To learn more about the products discussed in this article, visit the following URLs:

- Cisco SOHO 77 ADSL Router: cisco.com/warp/public/cc/pd/rt/70/
- Cisco 827 ADSL Router: cisco.com/warp/public/cc/pd/rt/800/index.shtml
- Cisco 1700 series modular access routers: cisco.com/warp/public/cc/pd/rt/1700/index.shtml
- Cisco 2600 and 3600 series modular access routers: cisco.com/warp/public/cc/pd/rt/2600/index.shtml cisco.com/warp/public/cc/pd/rt/3600/index.shtml

Cisco Business DSL Routers

Service providers looking to offer small and midsized businesses and corporate telecommuters value-added security have a number of Cisco routers to choose from. All have some level of firewall support and can be configured and managed by the service provider or by in-house IT staff with minimal fuss. Many of the routers also provide VPN support.

Cisco SOHO 77 ADSL Router. With this affordable, multiuser ADSL access solution for small-office/home-office (SOHO) environments, Internet security is entrusted to a packet-filtering firewall that manages traffic based on access control lists (ACLs).

Cisco 827 ADSL Router. A fixed-configuration router that connects small businesses and corporate telecommuters to the Internet or to a corporate LAN. Business-class security is provided by a stateful inspection firewall, as well as IP Security (IPsec) VPNs with Triple DES encryption.

Cisco 1700 series modular access routers. Designed for small branch offices and small and midsized businesses, the Cisco 1700 series router supports ADSL via a WAN interface card, and can also support an integrated stateful firewall with Cisco IOS software as well as VPNs, including high-speed encryption with an optional hardware encryption card. The modular configuration allows for upgrades and dual WAN links for backup and load sharing.

Cisco 2600 and 3600 series modular access routers. Like the 1700 series, the Cisco 2600 and 3600 series modular access routers support ADSL with an ADSL WAN interface card (card will be available in the first calendar-year quarter of 2001). Both models are suitable for larger enterprise branch offices with the scalability to support additional software and hardware configurations. The 2600 and 3600 series modular access routers can also support an integrated stateful firewall with Cisco IOS software as well as VPNs with high-speed, hardware-based encryption for increased performance.

Service Providers

NEW WORLD News

NWN

ILLUSTRATION BY NIP ROGERS

INSIDE

MPLS and IPsec

United They Stand for Better VPNs

MANAGED VIRTUAL PRIVATE NETWORK (VPN) services are not only a great way to save money, but they also offer the service providers who embrace them a distinct competitive advantage and new sources of revenue from emerging services such as e-commerce, application hosting, videoconferencing, and other multimedia applications. According to Infonetics, revenue from VPN services are predicted to grow from around US$5 billion in 2000 to more than $35 billion in 2004.

Two distinct technologies have emerged as the preeminent building blocks from which to create VPNs. They are Multiprotocol Label Switching (MPLS) and IP Security (IPsec).

VPN CHECKLIST

✓	**Scalability**	Must be able to provision new services rapidly on a global scale, from the smallest office configuration to the largest enterprises.
✓	**Security**	Must offer different levels and methods of security to support wide variety of customers, including tunneling, encryption, traffic separation, packet authentication, user authentication and access control.
✓	**Quality of Service**	Must be able to assign priority to mission-critical or delay-sensitive traffic and manage congestion across varying bandwidth rates. Quality of service (QoS) functions like queuing, network congestion avoidance, traffic shaping and packet classification, as well as VPN routing services utilizing an optimal routing protocol.
✓	**Manageability**	Must have advanced monitoring and automated flow-through systems to quickly roll out new services, enforce security and QoS policies, and support service level agreements (SLA).
✓	**Reliability**	Must offer predictable and extremely high service availability that business customers expect and require.

Service providers are deploying one or the other of these VPN architectures primarily based on the customers and market segments they serve, the value-added services they wish to offer, as well as their own network priorities. So which technology is best? Which one is right for your business model?

"Each technology has its own merits and place in the network," says Kurt Kruger, Senior Manager for Cisco Service Provider VPN Solutions. "They should not be looked upon as adversarial or competitive solutions, but complementary. The question to ask is not 'Which technology should I use?' but 'How do I use both to maximize my market coverage, service offerings, and revenue?'"

Same Destination, Different Paths

While both can be used to build VPNs, MPLS and IPsec were each designed for two completely different tasks and are being handled by different groups within the Internet Engineering Task Force (IETF). The IPsec working group under the Security Area concentrates on the protection of the network layer by designing cryptographic security mechanisms that can flexibly support combinations of authentication, integrity, access control, and confidentiality. The MPLS working group under the Routing Area, on the other hand, develops mechanisms to support higher layer resource reservation, quality of service (QoS), and definition of host behaviors.

The IETF has left the issue of integrating IPsec and MPLS to the discretion of the implementers. As a result, two independent VPN architectures have emerged, with service providers typically using one or the other but not both.

IPsec Strengths

IPsec is a highly secure infrastructure for transporting sensitive information over the public Internet. It provides data privacy through a flexible suite of encryption and tunneling mechanisms that protect packet payloads as they traverse the network. Because it can be deployed across any existing IP network, it is particularly attractive to Internet service providers (ISPs). By operating at the IP layer, IPsec offers the service provider greater choice when it comes to the underlying network structure, offering a wide range of service applications and rapid time to market.

"In an IPsec-based VPN, application modifications are not required," says Kruger, "so there is no need to deploy and coordinate security on a per-application, per-computer basis." In this way, IPsec provides a secure infrastructure without costly changes to every computer on the network.

IPsec functions at the network or packet-processing layer. It is most useful offnet or at the edge of the service provider's network where there is a higher degree of exposure to data privacy. Untrusted public networks are the most likely candidates for applying IPsec's tunneling and encryption technology. "This makes IPsec an excellent solution for securing remote access or creating offnet VPNs," adds Kruger. "As the number of remote and mobile users of corporate networks increases, this capability will become increasingly more valuable to the service providers capable of offering it."

MPLS Strengths

As opposed to IPsec, which functions best at the outer regions of the network, MPLS is best deployed within the core of the service provider's network. This is where QoS, traffic engineering, and bandwidth utilization can be fully controlled. A well-executed MPLS-based VPN implementation provides scalable, robust QoS mechanisms and traffic engineering capabilities, enabling service providers to offer IP-based, value-added services with guaranteed service-level agreement (SLA) compliance.

MPLS also offers great flexibility because it can run on IP, ATM, and Frame Relay network protocols. The labeling algorithms used provide flexibility for network managers, allowing packets to be labeled for specific destinations or to flow along specified routes for balancing loads on the network.

Like IPsec, MPLS also provides end-to-end security for subscriber transmissions. However, it provides security in a different manner, by separating traffic within the provider's network using unique, per-customer labels or route distinguishers (RDs). RDs are assigned automatically when the VPN is provisioned and are transparent to end users. They are placed in packet headers to isolate traffic to specific VPN communities.

According to Kruger, one of the most important qualities of MPLS is its scalability. "Because there is no need for site-to-site peering, a typical MPLS-based VPN deployment is capable of supporting tens of thousands of VPN groups over the same network," Kruger explains. Scalability—both in network capacity and in new service offerings—is a high priority in today's rapidly growing market.

Because most incumbent local exchange carriers (ILECs) and competitive local exchange carriers (CLECs) have existing ATM and Frame Relay infrastructure, MPLS tends to be their technology of choice for building dependable and scalable secure VPNs.

The Need for Both

To maximize your market coverage and VPN service breadth, both MPLS and IPsec will be required in your VPN deployment mix. That's because service providers' business customers are demanding different types of VPNs, each with its own unique uses and requirements.

- **Intranet VPNs** link corporate headquarters to remote offices over a shared, prioritized network and offer an extremely cost-effective alternative to dedicated WANs. They need to scale easily as the organization grows.
- **Extranet VPNs** link network resources with third-party vendors and business partners, extending elements of the corporate intranet beyond the organization. To keep pace with rapidly changing business climates, extranet VPN access needs to be able to be turned on and off on the fly.
- **Access VPNs** connect telecommuters and mobile users securely and cost-effectively to corporate network resources from anywhere in the world over any access technology. Because this traffic may run on untrusted segments outside the service provider's network, it must be encrypted to ensure privacy and security.

The keys to successfully broadening your VPN services marketing lie in your ability to offer intranet and extranet VPNs that scale well and can be quickly and flexibly deployed, along with a broad portfolio of access VPN services with maximum security protection. So knowing how MPLS and IPsec compare by each of these attributes is key to knowing where each technology is best deployed.

MPLS for Scalability and Flexibility

IPsec requires site-to-site peering in order to operate. It assumes you're establishing relationships between known endpoints, with each endpoint communicating to determine and agree upon the same authentication method. Packets are sent back and forth, with each endpoint declaring the encryption method it prefers and which it will accept, until they agree upon the strongest common method between them. For instance, the sender may say "I want to use Triple DES, but I'll accept DES." The receiver answers with "I only use Triple DES," and the encrypted message is transmitted. These relationships must be predefined, explains Kruger. Each endpoint requires the address and security policies of all other endpoints. "Building a fully meshed IPsec network gets increasingly more complex as each existing point needs to be made aware of each new endpoint added to the network."

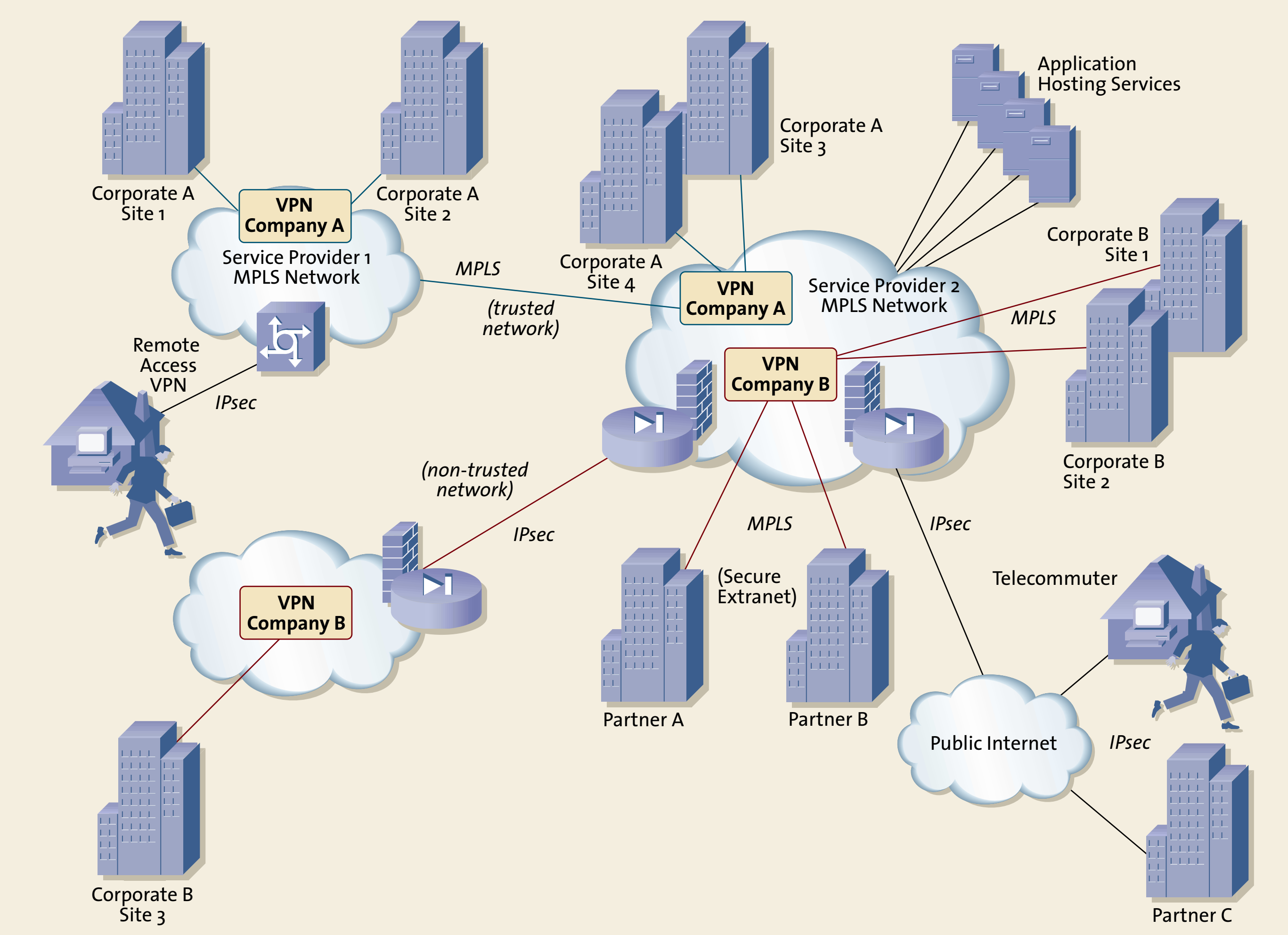
VPNs built using Cisco's MPLS implementation do not require predefined relationships. Packets are labeled for specific VPNs within the network, and only those ports that are part of that specified VPN receive traffic. Cisco MPLS uses the Multiprotocol Border Gateway Protocol version 4 (MP-BGPv4), which, according to Darryl Wortham, a Cisco customer solutions manager, imbues the network with intelligence by making these determinations. Packets need only have the correct label to be sent to other connection points that share the same label.

"Through its use of MPLS MP-BGPv4, Cisco is able to create highly scalable VPNs that connect

Continued on page 41

MPLS and IPsec, Continued from page 39

CISCO INTEGRATED MPLS AND IPsec VPN ARCHITECTURE



DOUBLE FEATURES: Service providers that leverage both architectures can attract customers with a much wider range of needs and priorities, covering the full spectrum of features required for intranet, extranet, and access VPNs.

autonomous networks together, supporting up to 70,000 routes. That's as much as the Internet, which is also based on BGP," says Wortham.

The same attributes that make MPLS a superior technology for building scalable VPNs also makes it the most flexible, as long as all users share the same MPLS network. That's because labeling requires that every network device between sender and receiver run MPLS. Enterprises wishing to add partners or vendors to their extranet VPN can do so on the fly as long as they're all on the same service provider's MPLS network. Otherwise, IPsec must be used to securely connect extranet users on an untrusted public network or between two different service provider's MPLS networks.

IPsec for Security and Mobility

"Last mile connections using MPLS VPNs have the same security characteristics as dedicated ATM or Frame Relay service," says Kruger, "because anyone could tap the line." That's because data running over an MPLS VPN is in clear text. Conversely, with IPsec, even if someone has access to the line, the data they receive will be encrypted and therefore unreadable. Clearly, where mission-critical data is involved or data is traveling on the edge of the network where it is most exposed, IPsec should be used for maximum privacy.

For mobile users, telecommuters, and others who require secure remote access, MPLS is simply not an option. MPLS is a network-based solution and does not go all the way out to endpoint computing devices. MPLS stops at the edge of the service provider network. Therefore, IPsec is the only practical option at present to enable secure remote access VPNs.

Continued on page 43

MPLS and IPsec, Continued from page 41

Putting It All Together

Cisco currently offers service providers both intranet and extranet VPN solutions based on MPLS and IPsec technologies, as well as access VPN solutions based on IPsec. Service providers can build MPLS VPNs using a wide range of Cisco IOS® software routers, from 3600 series routers through the GSR 12000 series Internet routers, and MGX 8850 IP+ATM switches. For IPsec-based VPNs, Cisco offers dedicated routers and concentrators for deployment at the customer premises or service provider edge. For example, the Cisco VPN 3000 concentrator series resides at the customer premises and is purpose-built for remote access IPsec VPNs. For site-to-site VPN applications managed at the customer premises, there's the Cisco 7100 VPN router series as well as a complete line of VPN-optimized routers. Both the dedicated 7100 and VPN-optimized routers include high-performance, hardware-based IPsec encryption, multiple WAN interfaces, and the entire Cisco IOS software feature set, including QoS.

For large-scale, high-throughput IPsec VPN deployments at the service provider edge, there's the Cisco VPN 5000 concentrator series. The VPN 5000 can be deployed for both site-to-site and remote access applications, and allows service providers to segment the platform into multiple, virtual devices, each configurable to meet the unique demands of different customers.

Best of Both Worlds

Cisco also offers solutions that allow service providers to take advantage of both IPsec and MPLS. By co-locating a Cisco VPN 5000 series concentrator with a Cisco IOS MPLS PE router, such as the ESR 10000, MGX 8800, 7500, 7200, or UAC 6400, IPsec sessions can be mapped directly into an MPLS VPN. This enables service providers to extend their secure VPN service beyond the boundaries of their MPLS network. It enables secure traffic to flow from one service provider's network, across its customer's network, through any number of other service provider networks to reach the customer's branch offices or remote sites anywhere in the world. It also allows for secure VPN access for telecommuters and mobile users.

Management and Provisioning

The profitability of a service provider's IP VPN offering is directly tied to its ability to effectively and efficiently provision, bill and monitor the performance of VPN services. The Cisco VPN Solutions Center addresses today's requirements for managing MPLS-based VPNs, allowing provisioning, service auditing, as well as SLA reporting and accounting. With the release of Cisco VPN Solutions Center (VPNSC) Version 2.0 in the first calendar-year quarter of 2001, service providers will also have support for IPsec-based, CPE-to-CPE VPN services.

The current version of VPNSC is integrated with Cisco's Info Center to provide VPN fault management, and Cisco's Provisioning Center, providing multiplayer and multivendor provisioning of services. Through the Cisco New World Ecosystem, integration with a number of Cisco OSS/BSS partners provide for even more robust VPN management, including Concord's Network Health Monitor for VPN performance reporting, and Portal and Belle Systems to provide IP VPN usage-based billing.

End-to-End Game

While service providers can deploy either an IPsec or MPLS-based VPN architecture to deliver new, value-added services, a greater benefit can be realized as they converge. Service providers may choose IPsec for traffic that needs strong authentication and confidentiality, and choose MPLS for its broader connectivity and lower costs compared with traditional Layer 2 private data networking. With both architectures, service providers will be able to cover the spectrum of customer requirements for security, QoS, and traffic prioritization.

To meet burgeoning demand for telecommuting services and access VPNs, service providers require IPsec technology. To seize the growing demand for intranet and extranet access, IPsec again comes into play to secure traffic as it exits the service provider's trusted network to traverse the public Internet.

Additionally, to support a growing number of customers with global VPN requirements and limited bandwidth in some parts of the world, service providers require the traffic engineering and scalability afforded by MPLS-based VPNs. The clear market opportunity for a service provider is to offer access VPNs, intranet VPNs, and extranet VPNs across a common infrastructure and provision, bill, and manage them in an integrated fashion.▲▲

FURTHER READING

To get more information on the products discussed in this article, as well as a chart comparing MPLS and IPsec by the features most important to VPN deployment, visit *Packet Online* at:

cisco.com/go/packet/mplsipsec

PRODUCTS AND TECHNOLOGY

Guaranteed Reservations

Enhanced RSVP in new Cisco IOS release enables voice service.

ONE TECHNICAL CHALLENGE OFTEN faced by service providers deploying voice-over-IP (VoIP) services is the traffic bottleneck potential on the customer access link. Because the access network is usually the slowest segment of the network, it tends to be the most vulnerable to congestion. Congestion leads to latency, which can impact voice quality.

An enhanced version of the Resource Reservation Protocol (RSVP) available in the latest release of Cisco IOS® software, though, resolves this issue. RSVP is an Internet Engineering Task Force (IETF) protocol used for signaling requests (setting up reservations) for Internet services by a customer.

Cisco IOS Release 12.1(5)T, released in November 2000, supports RSVP as a call admission control (CAC) mechanism in Cisco H.323 Version 2-based VoIP networks. The technology synchronizes RSVP procedures with H.323 Version 2 set-up procedures so that the required quality of service (QoS) for a call is maintained, end to end, across the IP network.

Unlike with RSVP implementations for data-only networks, resources can now be reserved before a session ever begins. Service providers offering managed VoIP services, then, can configure Cisco routers at the edges of their networks and their customers' networks to ensure that network resources are available for the duration of voice sessions.

"With this release, RSVP has become the only CAC mechanism to perform end-to-end bandwidth reservation," notes Christina Hattingh, technical marketing engineer in the Cisco IP Access Business Unit.

No More Queuing

In data networks, RSVP has traditionally worked such that a session gets under way (the destination device is alerted), and then the protocol signals the network to request bandwidth resources across every hop in the network. In a data-only environment, if resources are not available somewhere along the way, data is queued or delayed.

This situation usually has little or no noticeable effect on application performance, since most data is not impacted greatly by low levels of latency. In the voice world, however, it is imperative to minimize delay to the degree possible to enable high-quality voice conversations.

"In fact, it is desirable to keep voice traffic off the network entirely until a full path becomes available," says Hattingh.

The RSVP-H.323 synchronization, for example, makes sure that the bandwidth reservation is established in both directions so that the called party's phone rings only after the resources for the call have been reserved. Using RSVP-based admission control, VoIP applications can reserve network bandwidth and react appropriately if bandwidth reservation fails.

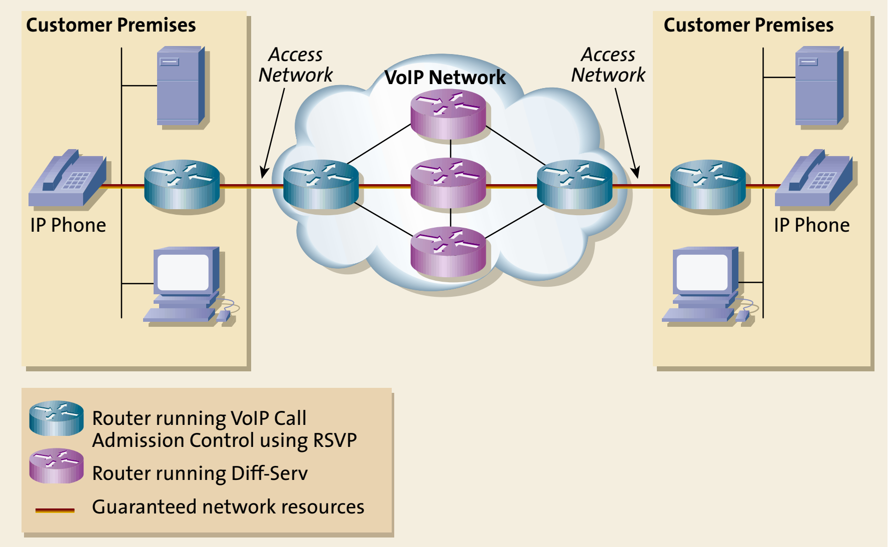
"This CAC feature does not require service providers to turn on RSVP in the places where there are very high speed interfaces, such as in backbones," says Jonathan Davidson, Manager of Technical Marketing in Cisco's Service Provider Line of Business. "In these network segments, it is best to use Diff-Serv." Diff-Serv, or Differentiated Services, is a QoS architecture that marks priority bits on IP packet headers.

"If the edges have the bandwidth necessary, then the call will be admitted to the network," Davidson says.

To support RSVP-based QoS with H.323 Version 2, the originating and terminating gateways must be running Cisco IOS Release 12.1(5)T and H.323-based VoIP capabilities. (The capability has also been available in 12.1(3)XI, an early deployment release.) The feature is supported on Cisco IOS-based gateways and routers, including the Cisco 1750, 2600, 3600, AS5300, AS5800, 7200, and 7500 series devices.

For more information, visit *Packet Online*: cisco.com/go/packet/rsvp.▲▲

RSVP AT THE EDGE



EDGE TACTICS: Service providers can run RSVP CAC mechanisms at the network edge and Diff-Serv in the core.

CASE STUDY

VoIP Goes Global

Equant pioneers integrated IP data/voice services and associated service classes worldwide.

Nowhere is there likely to be greater evidence of the shift to integrated, IP-based networking than in the service portfolio of Equant.

An industry pioneer in the deployment of IP virtual private network (VPN) services based on Multiprotocol Label Switching (MPLS) technology and voice over Frame Relay, Equant this year added several new pace-setting IP services to its arsenal of competitive network offerings. These services include integrated data and voice services, as well as differentiated IP service classes.

To deliver these offerings, Equant—a network operator serving business customers in 220 countries and running an IP network that reaches 130 nations—has deployed Cisco router-based quality-of-service (QoS) technologies in its worldwide IP backbone network. These capabilities have enabled the company to launch IP-based telephony services and tiered classes of service (CoSs) in the 57 countries in which it has regulatory approval to provide voice services.

Equant's Huntley says circuit-switched telephony is becoming outdated around the globe.

"Successfully moving voice traffic over IP technology worldwide is a huge step forward—and it is an early indication that telephone calling over traditional circuit-switched technology is becoming outdated on a global scale," says Laurence Huntley, Equant's Vice President of Strategy and Industry Relations.

Equant has deployed its integrated IP services as a subset of its Cisco MPLS-based IP VPN offering, called Intranet Connect. To provision the new set of IP services—called Integrated Voice and Data (iVAD) for Intranet Connect—Equant uses a combination of intelligent software capabilities found in Cisco routers. These include the following Cisco IOS® software features:

- Differentiated Services (Diff-Serv) on the Cisco 2600 and 3600 modular multiservice routers at customer sites. Diff-Serv enables the marking of IP packets with priority information.
- Traffic Policing on ingress Cisco 7500 series routers at the edge of the Equant network. This capability involves marking packets by setting the Diff-Serv Control Point (DSCP) value for transmission across the Equant backbone.
- Low-Latency Queuing, which creates a priority queue for real-time, high-priority traffic in the egress Cisco 7500 series routers at the edge of the Equant network. This feature works in conjunction with Class-Based Weighted Fair Queuing (CBWFQ) by adding a separate queue for real-time traffic.

Customer Demand Accelerates

Equant says that customer demand was the impetus behind its recent rollout of IP telephony services and tiered IP service classes. On a worldwide basis, Equant says it is seeing VoIP service availability specified in well over 90 percent of the requests for proposal (RFPs) that it receives from both existing and potential new customers. The company notes that the VoIP requests are coming from not only large multinational enterprises wishing to leverage the cost reduction and management benefits of VoIP globally, but also from those looking to get started with the capability in a small number of sites.

"We see a definite trend for customers with a range of coverage requirements wishing to converge their various types of network traffic onto one circuit to save on network access, equipment, and management costs," says Yousaf Hafeez, Equant's Head of IP and Data Marketing. "In addition, there are some parts of the world, such as portions of South America and the Far East, where VoIP represents a significant improvement in voice quality compared with international direct dial services delivered over aging public telephony infrastructures."

Existing Equant customer Det Norske Veritas (DNV) South America says it will probably turn to Equant's IP-based solution for a couple of reasons. DNV is a foundation that acts on behalf of about 110 national maritime authorities to create rules and guidelines for the classification of ships, mobile offshore platforms, and other floating marine structures.

The organization runs a software application whereby

NETWORK VISTA: Personnel in Equant's Paris global network management center (GNMC) have a birds-eye view of the Equant DS-3/OC-48 network. Global management capabilities in the GNMC help Equant to deliver on its end-to-end service-level agreement (SLA) guarantees.

PHOTOS COURTESY OF EQUANT

surveyors all over the world require split-second access to ship histories and class certificates, and it would like to have the ability to prioritize that traffic over its network. "Here, the traffic classification capabilities would be a real advantage," says Marco Antonio Agnese, regional IT manager in DNV's Rio de Janeiro, Brazil, offices.

DNV is using Equant's voice-over-Frame Relay service now, but says it also looks forward to IP telephony. "The reason is that we'd like to phase out our analog PBXs [private-branch exchanges] in the future in favor of IP," Agnese explains.

Equant, a Cisco-Powered Network provider, is currently delivering iVAD for Intranet Connect to about 25 multinational customers, according to Hafeez. Last summer, the company added off-net voice services, whereby VoIP phone calls can be terminated by local public switched telephone network (PSTN) operators throughout the world at standard local calling rates. Equant coordinates the procurement of these local phone services on behalf of its customers and handles the PSTN billing, Hafeez explains.

Shortly after launching the off-net calling capabilities, Equant rolled out end-to-end tiered service classes that include guarantees for the performance of the network access link in addition to the network backbone. Having the access link included in the CoS guarantee is a rarity among service providers.

A Matter of Priorities

To enable its IP-based iVAD service, Equant installs a Cisco 2600 or 3600 series modular multiservice router on a customer's premises and assumes management responsibility for the devices. Customers can simply plug their LAN servers and voice equipment into the routers, which will translate traditional voice signals generated by a PBX or key telephone system into IP voice packets.

The customer's router has the capability to set a DSCP priority bit in an IP header based on corporate policy information that resides in an access control list (ACL) in the router. Marking packets in this way assures that voice and other real-time, delay-sensitive traffic will traverse the network access link ahead of less critical traffic. In addition, the setting of the DSCP bit enables the Equant network to identify priority traffic so that it can give it preferential treatment across the network backbone.

Cisco 7500 series routers use Traffic Policing to find DSCP-prioritized traffic from multiple customers at the ingress edge of the Equant network. In the event of congestion, policing is also used to drop packets. The Cisco 7500 network then invokes Low-Latency Queuing at the egress (or delivery) edge of the network. This capability is activated on Cisco routers using the **priority** command.

Continued on page 49

Equant, Continued from page 47

By looking at the DSCP priority bits set in delay-sensitive packets on the edge of customers' networks, this feature builds a priority queue at the egress side of the network. It identifies high-priority traffic and sees to it that delay-sensitive data such as voice is sent first.

At Layer 2, Equant runs a global ATM backbone infrastructure, but has elected to use IP QoS capabilities rather than mapping IP precedence bits to ATM CoSs. "The drawback we see in using ATM CoSs is that if you are a customer wanting four service classes, you need to purchase and manage four PVCs (permanent virtual circuits)," explains Jon Floyd, IP marketing manager at Equant. By invoking service classes at the IP layer, Floyd explains, all traffic traverses a single PVC from ingress to egress across Equant's IP backbone.

EQUANT SERVICE CLASSES AND PERFORMANCE METRICS

	Class of Service			
Network Metric	Real Time	Interactive	Standard Business	General
Latency	✓	✓	–	–
Jitter	✓	–	–	–
Packet Loss	✓	✓	✓	–
Service Availability	✓	✓	✓	✓

UNDER CONTRACT: Each of Equant's CoSs has a custom SLA associated with it, based on one or more of the four primary network performance metrics. Equant supports the SLAs with detailed reporting of the defined metrics each month.

Business Rationale

With its burgeoning IP service portfolio, Equant says it can offer customers a service combination that most of its competitors cannot:

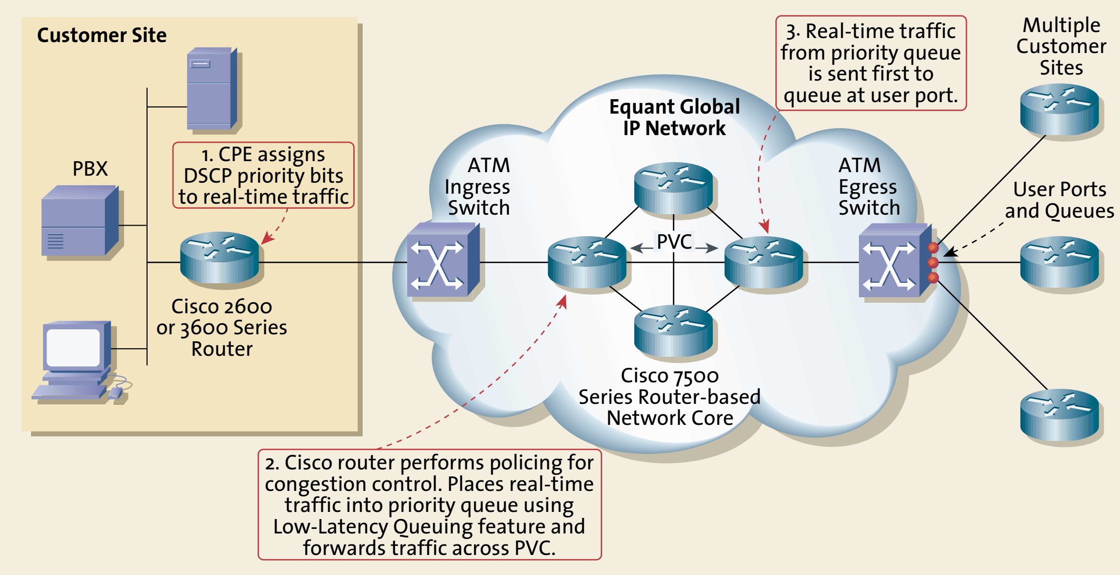
- Users can get any-to-any global connectivity using IP—without having to build expensive leased-line networks or manage complex connection-oriented Layer 2 networks with PVCs.
- Users can leverage the flexibility of Cisco multiservice routers to make quick changes to their network configurations through simple software changes. Equant manages these using a common global network management system.
- Users can get their feet wet with low-latency and interactive IP services that will become competitive requirements in the future. These include Web-based call centers, LAN telephony, unified messaging, collaboration applications, and customer service tools.
- Users are assured high-quality voice service, because of a network design that efficiently prioritizes and allocates bandwidth for voice and data.

Most Equant IP services are deployed in a managed network service scenario and enable customers to converge data and voice on a single access link. Equant's pricing model includes a monthly charge defined by each customer site's access speed, CoS selected by the customer, router model and, if applicable, a VoIP interface.

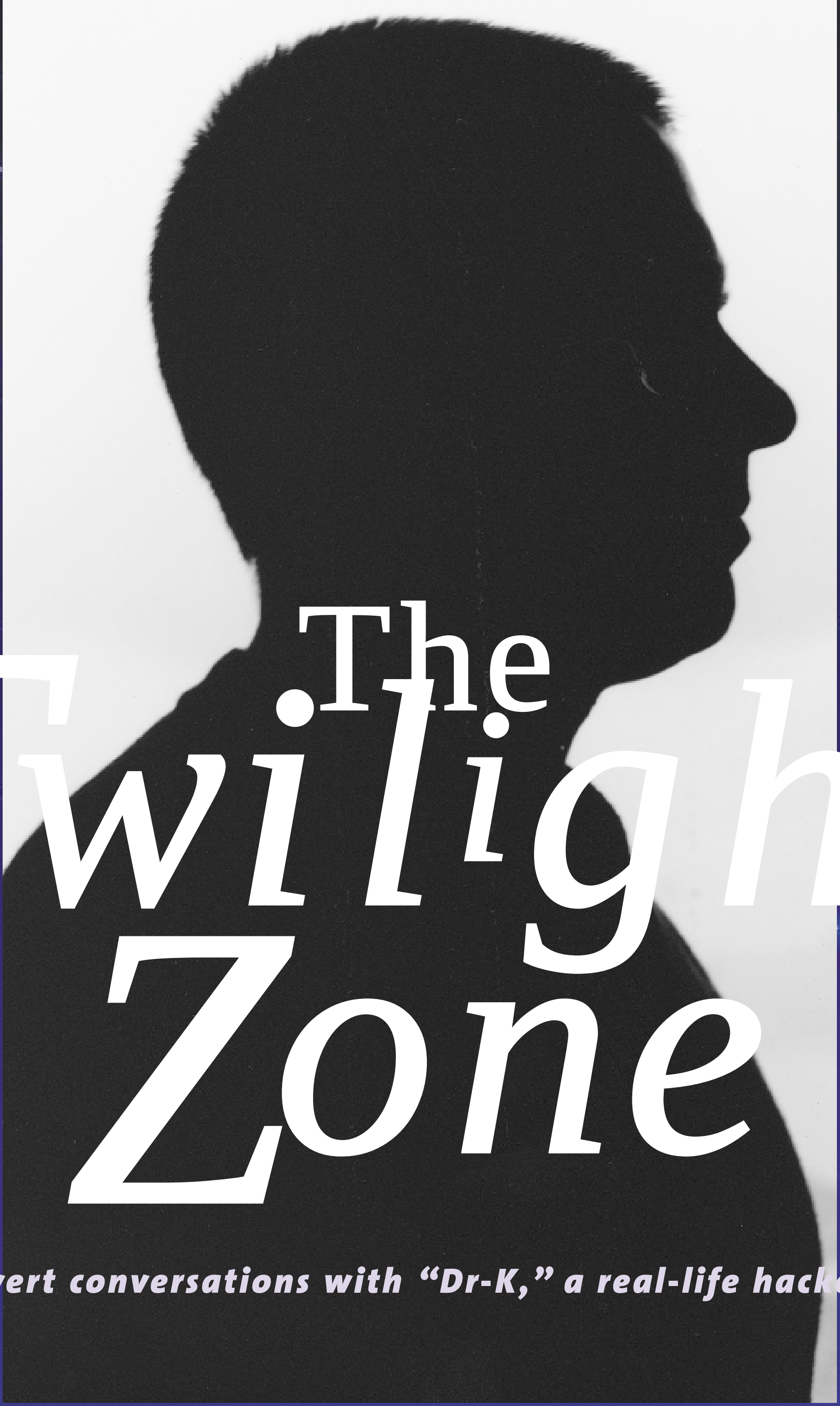
Diff-Serv and Low-Latency Queuing in Cisco routers are among the capabilities that have enabled Equant to make a global guarantee to its entire user base for a network SLA. Equant has contractually committed to 100 percent network availability in more than 80 locations worldwide. It also ensures roundtrip IP packet latency better than required to provide toll-

Continued on page 95

EQUANT'S DIFF-SERV-BASED CLASSES OF SERVICE


Customer Site
PBX
1. CPE assigns DSCP priority bits to real-time traffic
Cisco 2600 or 3600 Series Router
ATM Ingress Switch
Equant Global IP Network
PVC
Cisco 7500 Series Router-based Network Core
3. Real-time traffic from priority queue is sent first to queue at user port.
ATM Egress Switch
Multiple Customer Sites
User Ports and Queues
2. Cisco router performs policing for congestion control. Places real-time traffic into priority queue using Low-Latency Queuing feature and forwards traffic across PVC.

PREFERENTIAL TREATMENT: Equant uses a mix of priority marking and queuing to offer tiered service classes with associated SLAs.



The Twilight Zone

Covert conversations with "Dr-K," a real-life hacker

PICTURE IF YOU WILL, AN ORDINARY CAFÉ. Where an ordinary reporter interviews a not so ordinary man. You see, this man is a hacker. And for the next few minutes, you'll glimpse his peculiar genius as we journey into a wondrous land of imagination whose boundaries do not always end at your network. That's the signpost up ahead. Your next stop: the Hacker Zone.

Q *Packet:* What is hacking all about?

A DR-K: Hacking is just exploration. Most hacking is responsible exploration of computers and computer networks with very little emphasis on breaking system security, stealing credit cards, or crashing computer systems. Above all else, hacking is about that insatiable desire to learn, to understand, to know, and then to learn even more about computers and technology.

Q Are you still part of the hacker community?

A I am a computer networking and security consultant. I dropped out of the hacker scene soon after the high-profile prosecutions of DataStream Cowboy and Maelstrom.

Q Why do you still use an anonymous hacker name?

A White-hat hackers can become a target for black-hat hackers who see them as "sellouts." So even a white-hat hacker needs to be careful when using the Internet.

Q Isn't breaking into someone else's computer system illegal, even if you're just exploring?

A As a white-hat hacker I have legally broken into systems to further my understanding of system security, but I did not specialize in cracking systems security in general. Many of the black-hat hackers I have known are computer enthusiasts who just happen to be most enthusiastic about breaking into computer systems, and whose knowledge of computers and networking protocols is second to none. At the end of the day, which type of hacker you are depends on your ethics, and whether you are breaking the law or not.

Q How can you tell if a cracker is trying to break into your network?

A If you get attacked, the logs on your computer will give away whether the attackers are script kiddies or seasoned crackers. The script kiddies are likely to leave great big footprints all over your logs as they scan every port and test for every CGI hole known to mankind. If you are being attacked by seasoned crackers, the logs will contain far less information—fingerprints rather than footprints. Experienced crackers know that any long-term attack is going to show up in the logs and alert any sensible systems administrator that something is up, so they will spread their attacks across a number of different originating remote sites and across time, so that they minimize any chances of detection.

Q What do crackers usually do after they gain access?

A They will need to get some form of system privileges to make it all worthwhile. A few good reasons why a cracker might want to get privved up include to install bogus users to make getting back easier, to place one or more Ethernet interfaces into promiscuous mode, or to be able to hide their presence on the system by manipulating system tables.

Q How do they go about getting system privileges?

A There are numerous ways of getting system privileges: crashing processes that run with privileges that leave temporary or core dump files, using a Trojan, sniffer or password attack to gain the system administrator's password, or abusing trust relationships between two hosts to move from host C to host B by apparently being a privileged user on host A who has similar rights on host B. Once they have the necessary system privileges they can then take control of the computer and do whatever they need to do.

Q How do crackers avoid getting caught?

A The cracking scene has a level of paranoia and mistrust that few other hackers can match, as crackers have everything to lose and nothing to gain by exposure. The only way not to get caught is not to start cracking in the first place, and when crackers get caught, the rest of the hackers lose out because we all get tarred with the same brush.

Q What are ways to keep abreast of the latest cracking tricks?

A The majority of security holes are found by the computing underground long before security consultants, and keeping up with the computer underground is the best way of assessing new risks yourself. The magazines, websites and ezines coming out of the computer underground are the best source of information to any hackers, black hat or white. Many hackers are more than happy to discuss system security with systems administrators at 2600 meetings or hacker cons, as long as you are "up front" with them.

Continued on page 53

PHOTO BY NICK SCOTT; BACKGROUND IMAGE: PHOTODISC

Twilight Zone, *Continued from page 51*

Kevin Ziese, Cracker Tracker

Cisco's own Kevin Ziese, Computer Scientist in the Office of the Chief Strategy Officer, was a leader of the computer security team within the joint US Air Force Information Warfare Center (AFIWC)–Air Force Office of Special Investigations (AFOSI) formed to find and stop the crackers known as DataStream Cowboy and Kuji in 1994. Ziese tells *Packet* how they hacked a sensitive military computer system and how the Air Force tracked and caught them.

"DataStream Cowboy and Kuji accessed a very sensitive military computer system by phreaking out of the United Kingdom on a British Telecom system down to South America. From South America, they used an improperly secured voicemail system to obtain a dialout line to a modem-based system in Seattle, Washington. Once there, they got onto the Internet and broke into the Air Force system. What attracted our attention was their use of cutouts."

The AFIWC/AFOSI deployed a highly skilled military team that led a three-week, focused investigation. "We knew something was broken into, but we didn't have a way to trace them backwards. People literally were sleeping on the floor inside the secure facility because we had no tools that could notify us remotely about what the hackers were doing. We had to build them all on site."

Once the team realized that a series of systems had been phreaked and hacked, they implemented an aggressive "reverse hacking" strategy to trace the perpetrators. This was the first United States investigation that coordinated the talents of computer scientists and international law enforcement resources. After a conference call with the FBI, the Secret Service, and the Department of Justice, the joint AFIWC/AFOSI team got permission to break into civilian computer systems.

The investigation represents a leap forward in the development and use of real-time tracking systems. "Up to that time, no one had ever been caught in real-time breaking into a computer system, but the commander wanted the technology. We wrote a tool that could find someone intentionally trying to hide himself on a UNIX-based computer." Working backwards during attacks, the Air Force team eventually partnered with New Scotland Yard and British Telecom to track the crackers back to an apartment in London. "We pioneered a new technique for doing a graphic display of hacking. We had New Scotland Yard on the phone at the instant they'd be breaking into the Air Force system." When police showed up to arrest the crackers, they were surprised to discover a pair of thrill-seeking teenage boys.

Exigent circumstances justified AFOSI's need to bend several US laws by hacking backwards through the system. After the incident was over, the US Department of Justice told AFOSI to "pack up all the software. That was great. That was cool. Don't ever do that again." The case convinced the military of the need to better protect resources and hold people accountable for losses. The AFOSI team also worked to "train special assets in different agencies so they knew first, how to identify the problem and second, how to trace people when they did it. You can't put people in jail if you can't catch them and provide proof."

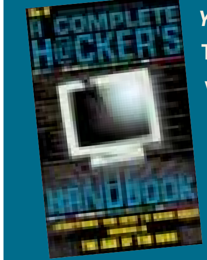
Q What else can network administrators do to protect their systems?

A One of the best ways of finding out if your computer is secure is to think like a cracker and attack your own machine. This is the best way of making sure that your system is safe. Every time you read about a problem in a hacker ezine, a CERT, CIAC, or other advisory, make sure that you understand how the exploit works and make sure that it doesn't work on any of the hosts on your LAN. Keep a database of exploits and make sure that you know which operating systems and which versions of software are open to attack.

Q Should network administrators be afraid of hackers?

A The majority of hackers are interested in increasing computer security to ensure that computers are used responsibly and in ways that do not undermine privacy or abuse information about the ordinary man in the street. Don't believe the media misinformation about "evil hackers"—go out and meet them for yourself. You never know, you might have more in common with them than you thought. ▲▲

FURTHER READING



You have been hacked! **The conversation with Dr-K was based on excerpts from *A Complete Hacker's Handbook—Everything You Need to Know about Hacking in the Age of the Web*, by Dr-K, ©2000, Carlton Books Limited, London. It is available at www.amazon.com.**

COVER STORY

Security

IN THE Internet Economy

SECURITY AND OPENNESS. THE SUCCESS OF YOUR BUSINESS MAY HANG IN THE BALANCE.

“Advocacy and belief go hand in hand. For there can be no true freedom of mind if thoughts are secure only when they are pent up.” —US Justice William O. Douglas

By JOHN PESCATORE

Since the dawn of civilization, security had a singular purpose: keep the bad guys out. For most of history, that meant building strong walls to stop the bad guys, with small, well-guarded doors to provide secure access for the good guys. This strategy worked well for the fortress-like world of mainframe computers, but with the advent of personal computers, LANs and the wide-open world of the Internet, more and larger entrances were required.

ILLUSTRATIONS BY CHRIS GALL

GALL

SECURITY TRENDS LONG TERM

Security in 2000	Security by 2010
Lumpy	Distributed
Visible and intrusive	Transparent and enabling
In the factory	In the product
An overhead cost	A cost of sales
Product oriented	Service oriented

EVOLUTION OF SECURITY: Over the next ten years, security will become less "lumpy," moving from discrete elements to being distributed and transparent throughout the network. Over time, the systems used in the factory to protect our products will be embedded in the very products shipped to customers. Security will become more of a feature and less of a cost.

The firewall became the electronic analogy of the moat and drawbridge, striking a balance between open access and increased security. As e-business continues to grow, finding this balance will be critical as it becomes harder and harder to tell the good guys from the bad guys. The rise of mobile commerce and wireless networks will be like the cannon to castle walls, exploding the old model, demanding that security solutions be seamlessly integrated, more transparent, and more flexible.

In the first wave of computer use, mainframes were kept in well-secured computer rooms and users could connect only via dumb terminals from approved locations over static, point-to-point connections. From a security perspective, life was good. If the rise of LANs and the personal computer rocked the security boat, the Internet threatened to sink it completely. The introduction of the firewall in 1995 allowed successful businesses to balance security with simple outbound access to the Internet (mostly for e-mail and Web surfing) for positive impact to the business bottom line.

This balance was short lived, as the use of extranets—defined by Gartner as the use of Internet technologies to connect internal business processes to external parties—began to grow. Businesses were soon realizing tremendous cost savings by connecting supply chain management and enterprise resource planning systems to business partners, sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to be augmented by intrusion detection, authentication, authorization, and vulnerability assessment systems. Today, successful companies have once again struck a balance by keeping the bad guys out with increasingly complex ways of letting the good guys in.

History Repeats Itself

As in any fast-growing, vibrant industry, static equilibrium is a rare commodity in the Internet economy. A number of trends threaten to rock the balance between security and open access yet again:

- **Privacy concerns.** In 1998, the European Union passed comprehensive Data Privacy Directives that provide consumers with strong control over their personal data. Many countries outside of the US have adopted the equivalents of these privacy principles. In the US, over 1000 privacy-related bills were introduced in state legislatures in 1999 and 2000, and numerous federal-level bills are currently floating around in Congress and the Senate. A privacy backlash is clearly underway.

JOHN PESCATORE

- **Wireless access.** Increasing use of wireless LAN connections and the rapid rise of Internet access from cell phones in Europe and Asia are requiring whole new approaches to security. RF connections don't respect firewalls the way wired connections do—a wall just isn't much defense against an air attack. Moreover, the slow processors, small screens, and non-existent keyboards on cell phones and personal digital assistants (PDAs) break many of the standard approaches to access, authentication, and authorization.
- **The need for speed.** Broadband connections to the Internet from homes are exceeding projections. Many businesses are finding that multiple T1 or E1 connections to the Internet are no longer sufficient. Today's software-based security approaches have problems scaling to OC-1 and higher rates.
- **People shortages.** The IT staffing shortage has hit the security field especially hard. To solve this problem, many enterprises are moving increasingly to outsource day-to-day security management tasks. The application service provider (ASP) business model will become increasingly common in the security world. Therefore, security solutions will need to be more manageable in this outsourced model.

Prepare for Impact

While these trends will clearly alter the way we look at and design security in our networks in the long term, their short-term impact will be felt over the next two to four years as security technologies, products and services evolve to strike a balance once again.

JOHN PESCATORE is Vice President and Research Director of Network Security for Gartner. Prior to joining Gartner, Pescatore was senior consultant for Entrust Technologies and Trusted Information Systems where he founded and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. His 22 years experience in computer, network, and information security includes a stint with the US National Security Agency and the US Secret Service, where he developed secure communications and surveillance systems. He can be reached at john.pescatore@gartner.com.

Firewalls will take on specific roles. Network-focused firewalls operating at high speeds will be designed solely for blocking intrusion attempts. They will be hardware based, embedded in routers, appliances, network interface cards (NICs) and integrated circuits. Application-focused firewalls, on the other hand, will be deployed to process and filter a single protocol or a limited set of protocols. These protocol lookouts will be implemented first as software that runs on general-purpose servers, but eventually will be embedded in server appliances and NICs. Network-focused firewalls will be increasingly managed by outsourced services, and hosting companies will offer virtual firewalls (firewall in the cloud solutions) that provide secured bandwidth without requiring management of individual firewall devices. Application-level firewalling will be primarily adopted and managed by high-end, security-conscious enterprises such as financial institutions, government agencies and other regulated or heavily legislated industries such as healthcare.

> "As e-business continues to grow, finding this balance will be critical as it becomes harder and harder to tell the good guys from the bad guys."

Intrusion detection systems (IDSs) will have a similar split personality. Network-based intrusion detection will remain primarily signature based, while the need for speed will drive IDS sensors to be embedded in high-speed appliances and network routing and switching devices. Host-based intrusion detection will need to focus more on detecting transaction-level incidents, leaving low-level attacks for detection by network-based intrusion detection. Network-based IDS will follow the firewall trend towards outsourcing, while host-based IDS monitoring will remain self managed. Organizations such as banking, insurance, telecommunications, and governments will create transaction-level incident signatures for use with host-based transaction incident management across marketplaces and trading exchanges.

Vulnerability assessment tools will be used primarily by consulting and system integration firms, while most enterprises will use self-service, Web-based vulnerability scans to indicate a vulnerability that requires investigation by an expert. The price of such scans will drop to levels where daily tests will be used to assure that vulnerabilities are rapidly found and rectified. This will provide the logical equivalent of the "check engine" light on the corporate security dashboard.

Encryption will become increasingly commonplace at both the network and application layers. As Windows 2000 with IPsec support (and future releases with IPv6 stacks) become more widespread, the use of smart NICs and VPN-enabled routers will decrease the cost and complexity of continuous network encryption. The use of Secure Sockets Layer (SSL) to secure application-to-application communications tunneled over HTTP using protocols such as the Simple Object Access Protocol (SOAP) will increase rapidly. Crypto acceleration in NIC cards and in load balancing and caching appliances will become the rule.

Security management solutions will need to evolve from device, data and packet monitoring to transaction-level management. Security policy will need to integrate business conditions and priorities with security inputs to define dynamic alert and alarm levels rather than the static levels driven by low-level inputs we have today. Security standards based on Extensible Markup Language (XML) definitions will be used to support the management of multivendor environments and enable the integration of network- and application-level inputs.

Authorization and privilege management systems will become the focus point for integration of network-level "keep the bad guys out" controls and application-level "let the good guys in" controls. By managing Lightweight Directory Access Protocol (LDAP)-based directories that contain user, process, and object security attributes, authorization systems will have architectural mech-

Continued on page 59

Security, Continued from page 57

anisms for implementing security policy driven by business rules across e-business networks and systems. Various methods of authentication, from username/password pairs to digital certificates to biometrics will be used simultaneously, and authorizations will use level-of-authentication attributes as another means to determine access rights. XML-based interfaces will play a major role, providing the lingua franca for security solutions to integrate and interoperate with business platforms and rules.

The Future Is Wide Open

Over the next two to four years, best-of-breed multivendor solutions will dominate in large enterprises, while single-vendor security suites primarily will be deployed in small and mid-sized businesses or those enterprises that buy into large-scale network management frameworks. Vendors who provide architectural solutions and open interfaces, adhere to industry standards, and aggressively partner with third-party security solution providers will obtain leadership positions in the increasingly crowded security industry.

While we can project a logical path for security technologies and products to become more comprehensive and more effective, the most critical element of network security will always be process and people. Business directives and security policies must be integrated right from the start. Security shouldn't be an afterthought once the business plan and network are complete.

Businesses who successfully lead in the information age will be those that efficiently find the balance between protecting corporate and customer information, and making sure good ideas and creativity are not "pent up" and made ineffective. Security managers and administrators must continually refresh their skills to keep ahead of the bad guys without getting in the way of the good guys. Change is constant. Security achieved by fighting change is false security, equivalent to building more walls as the cannons start firing.▲▲

FURTHER READING

For more information, visit the following URLs:

- Gartner Group: www.gartner.com
- Computer Security Resource Center of the National Institute of Standards and Technology: csrc.nist.gov/
- International Computer Security Association's certified product list: www.icsa.net/html/labs
- List of up-to-date vulnerabilities and fixes: securityfocus.com
- Computer Security Institute: gocsi.com
- The System Administration, Networking and Security Institute: sans.org

SECURITY

WEAVING SECURITY INTO THE NETWORK FABRIC

BLANKET

E-BUSINESS IS DRIVING A NEW, TRUSTED communications environment that opens more network doors to both access and vulnerabilities and calls for a more pervasive approach to security. Instead of being layered onto networks as an afterthought or considered a necessity only for organizations with especially sensitive data, security capabilities are beginning to migrate into the core fabric of all network infrastructures.

Having security measures embedded directly into network elements will ensure a certain degree of inherent protection in any communications network. From there, network managers can determine for themselves how to balance their degree of vulnerability with openness, cost, and administrative considerations by activating the security options that make sense for their organizations.

"Traditionally, security technology has been applied as an overlay to network infrastructures," notes Russell Rice, Manager of Technical Marketing for Cisco's security products. "But as networks grow and new types of services emerge—customer care, extranets, and e-learning, to name a few—we're exposing data that has not been opened up in the past. This means that we need to address privacy and security on a much larger scale and at a more fundamental level."

Now that the same network devices used for connectivity are acquiring access control, authentication, and other security features, Rice notes, organizations can deploy secure networks that scale much more easily. He points to evidence of security integration trends in Cisco product development:

- The availability of an intrusion detection system (IDS) module for the Catalyst® 6000 family of campus switches
- The integration of IP Security (IPsec) encryption and support for certificate authority (CA) verification within Cisco IOS® software
- Firewall and IDS capabilities embedded in Cisco IOS software
- Intrusion detection integrated into Cisco Secure PIX™ Firewall
- Private virtual LAN (PVLAN) features on Catalyst 6000 switches for isolating switch ports

Each of these capabilities plays a role in helping network managers deploy appropriate security measures within their organizations. Building security options directly into the connectivity infrastructure enables users to activate these features as required, rather than having to create a security strategy as a separate project—a task many enterprises have traditionally tended to delay.

Intrusion Detection in the Backbone

The Catalyst 6000 campus backbone switches were designed as enterprise application delivery platforms. As such, they represent a significant aggregation point in an organization's network and are an economical spot in the network to add intrusion detection capabilities.

Recently, Cisco added a hardware and software module to the Catalyst 6000 product line that integrates intrusion detection and switching in a single chassis. This integration enables enterprises to "turn on" security in their networks without having to purchase and learn the ins and outs of a separate platform. In addition, the design enables the monitoring of a larger volume of network traffic than the traditional use of one or two switched port analyzer (SPAN) ports, each of which is able to monitor 100 Mbps of traffic.

"The Catalyst switch family, for example, enables the use of up to eight 150-Mbps IDS line cards for gigabit-per-second traffic monitoring," says Joel McFarland, Cisco IDS Product Marketing Manager. The IDS modules monitor copies of switched packets,

Written by Joanie Wexler (joanie@jwexler.com), a contributing editor for Packet *magazine.*

rather than interrupting traffic in the actual switching path, so the function does not interfere with switch performance, McFarland adds.

Detection systems such as the integrated module for the Catalyst 6000 provide around-the-clock network surveillance, much like closed-circuit video cameras and motion sensors do in the physical world. They analyze the packet streams within the network, searching for unauthorized activity. If they detect a suspicious event, they send alarms to a management console.

ACCELERATED MONITORING: Integrating intrusion detection into the Catalyst 6000 switch overcomes the limitations of using SPAN ports. The capability of running as many as eight modules, for example, enables the switch to monitor traffic at gigabit-per-second speeds.

The Catalyst 6000 IDS module monitors more than 300 security conditions, also called "signatures," that are patterns of known misuse. The monitor detects undesirable network activity by comparing traffic flows against a set of rules defined by an organization's network policy, guarding against misuse by both external and internal users.

"The Computer Security Institute in San Francisco (gocsi.com) estimates that between 60 and 80 percent of network misuse comes from inside an enterprise," McFarland says. For every signature monitored, network administrators have granular control over what action is taken, he adds.

For instance, the system can be set up simply to log the event. However, network administrators can also configure if-then responses that allow the system to act autonomously under any number of circumstances.

"However, many situations are not black or white," cautions McFarland. For example, he explains, low-level ping sweeps that are conducted by general network management systems to determine the health of network devices could be falsely interpreted as hacker reconnaissance activity in an automated setup. "If the IDS is configured to always reset the TCP session, the network could be constantly resetting the network management system instead," he explains.

Router-Based Encryption and CA Support

Cisco IOS software Release 11.3(3)T and later supports the ability to encrypt data using IPsec and to make use of centralized CAs. Having these capabilities built right into routers empowers enterprises to quickly build virtual private networks (VPNs) without having to purchase and maintain separate infrastructure products. For example, with integrated tunneling and data encryption capabilities, the Cisco 7100 VPN router removes the need for a separate encryption device and perimeter router when building site-to-site VPNs.

Many organizations are using public keys and centralized CAs to verify each peer router's authenticity, instead of using preshared keys between peer routers. The reason is that preshared keys can be compromised more easily and thus must be changed often to maintain high security levels. The preshared key model also does not scale well, requiring changes to be made network-wide on a router-by-router basis, which can create significant administrative bottlenecks as networks grow larger.

To enable the CA-based approach to security, Cisco IOS software supports industry-standard IPsec Public Key Infrastructure (PKI) capabilities as well as a special certificate management protocol developed jointly by Cisco and VeriSign, Inc. (www.verisign.com). Cisco's Simple Certificate Enrollment Protocol (SCEP)—first supported in Cisco IOS Release 12.0—is widely supported by PKI vendors, and is also moving along the standards track of the Internet Engineering Task Force (IETF).

A customer's WAN router is configured to use SCEP, which enables the router to enroll with a CA. A CA can be a server running SCEP-compliant CA software and maintained by the networked enterprise. Alternatively, a company could tap the services of a service bureau for the CA function.

The CA issues a digital certificate to the customer premises router, where it is stored in a protected, secure part of NVRAM. Digital certificates contain information that identifies a device or a user, such as the name, serial number, company, department, or IP address. The CA authenticates each peer router's certificate every time an IPsec connection is established. Using this approach, should security be compromised in a given router, users would only need to revoke or change the certificate in that router, rather than reconfigure all routers in the VPN.

Embedded Firewall Capabilities

The Cisco IOS Firewall is a security-specific option for Cisco IOS software running on WAN edge routers and switches. Like a standalone firewall appliance such as the Cisco PIX Firewall, the Cisco IOS Firewall acts as a gatekeeper at the edge of an organization's network to filter packets from undesirable or unknown source addresses and to authenticate and authorize users. In this way, enterprises that don't need the dedicated processing power of a standalone PIX have sophisticated firewall options available to them right in their network software.

"Many longtime Cisco customers with growing security requirements have found great value in the fact that these capabilities are inherent in the Cisco routers they've already purchased," says Ruben Rios, Cisco IOS Manager, Cisco IOS security products. "They simply have to upgrade their software version and image type to take advantage of these intrinsic features."

One particularly useful component of the Cisco IOS Firewall is context-based access control (CBAC). CBAC filters packets based on application-layer information, such as the types of commands that are being executed within the session. For example, if the software detects a command that's not supported by the organization, it can deny access to those packets.

CBAC enhances security for TCP and User Datagram Protocol (UDP) applications by enabling the network to dynamically open and close TCP and UDP ports, rather than requiring network managers to write permanent ACLs that grant or deny access based on network- or transport-layer information. The ACL approach leaves firewall doors open and has thus resulted in administrators tending to deny all such application traffic.

Instead, CBAC has the intelligence to understand user-specified application protocols—such as H.323, File Transfer Protocol (FTP), Microsoft Remote Procedure Call (MS-RPC), and Oracle SQL*Net—so that it can dynamically open and close the appropriate ports as necessary. This capability enables customers to use more sophisticated applications, such as Network Address Translation (NAT), across network boundaries.

The Cisco IOS Firewall feature set can also be configured to block Java applets from unknown or untrusted sources to protect against attacks in the form of malicious commands or the introduction of viruses. A Java executable file can steal passwords or otherwise wreak havoc with a system. Filtering applets at the firewall centralizes the filtering function for end users. This process eases administration because it's no longer necessary to disable Javascript on all Web browsers within an organization to protect against Java attacks.

The Cisco IOS Firewall features, including CBAC and Java filtering, are available in Cisco IOS Release 11.2(11)P. However, additional protection and protocol support is added continually, so Cisco encourages users to implement the latest version of the feature set. Cisco IOS Firewall features are available on the Cisco 800, 1600, 1700, 2500, 2600, 3600, 7100, 7200, the Route Switch Module (RSM) for the Catalyst 5000, and 7500 series Route Switch Processor (RSP) router platforms.

IDS Bundled into PIX Firewall and Routers

The Cisco standalone PIX firewall Version 5.2 and most Cisco routers running Cisco IOS Release 12.0(5)T and up have gained intrusion detection capabilities. The Cisco Secure PIX Firewall—designed primarily for high-volume packet filtering—and Cisco IOS software can continuously monitor packets for a subset of the security signatures monitored by standalone IDS appliances and the IDS module for the Catalyst 6000. Administrators can turn on these IDS capabilities at any network perimeter where additional security between network segments is required. The IDS capabilities in the Cisco PIX firewalls and routers identify 53 common types of attacks. The devices respond immediately and can be configured to send an alarm to a syslog server, drop the packet, or reset the TCP connection.

The PIX and router IDS capabilities allow a signature to be acted upon differently depending on the interface on which it was detected. They also allow signatures to be individually disabled if recurring "false positives"—such as a misidentified ping sweep by a network management system—are detected.

Isolating VLAN Ports

Catalyst 6000 switches support an integrated security feature called private VLANs (PVLAN). A PVLAN is a set of ports configured with the features of a normal VLAN (logically arranged LAN user groups that ease physical cabling burdens) that also provide some Layer 2 isolation from other ports on the switch. This prevents traffic from one VLAN from being tapped by a user on another.

There are three types of PVLAN ports:

Continued on page 65

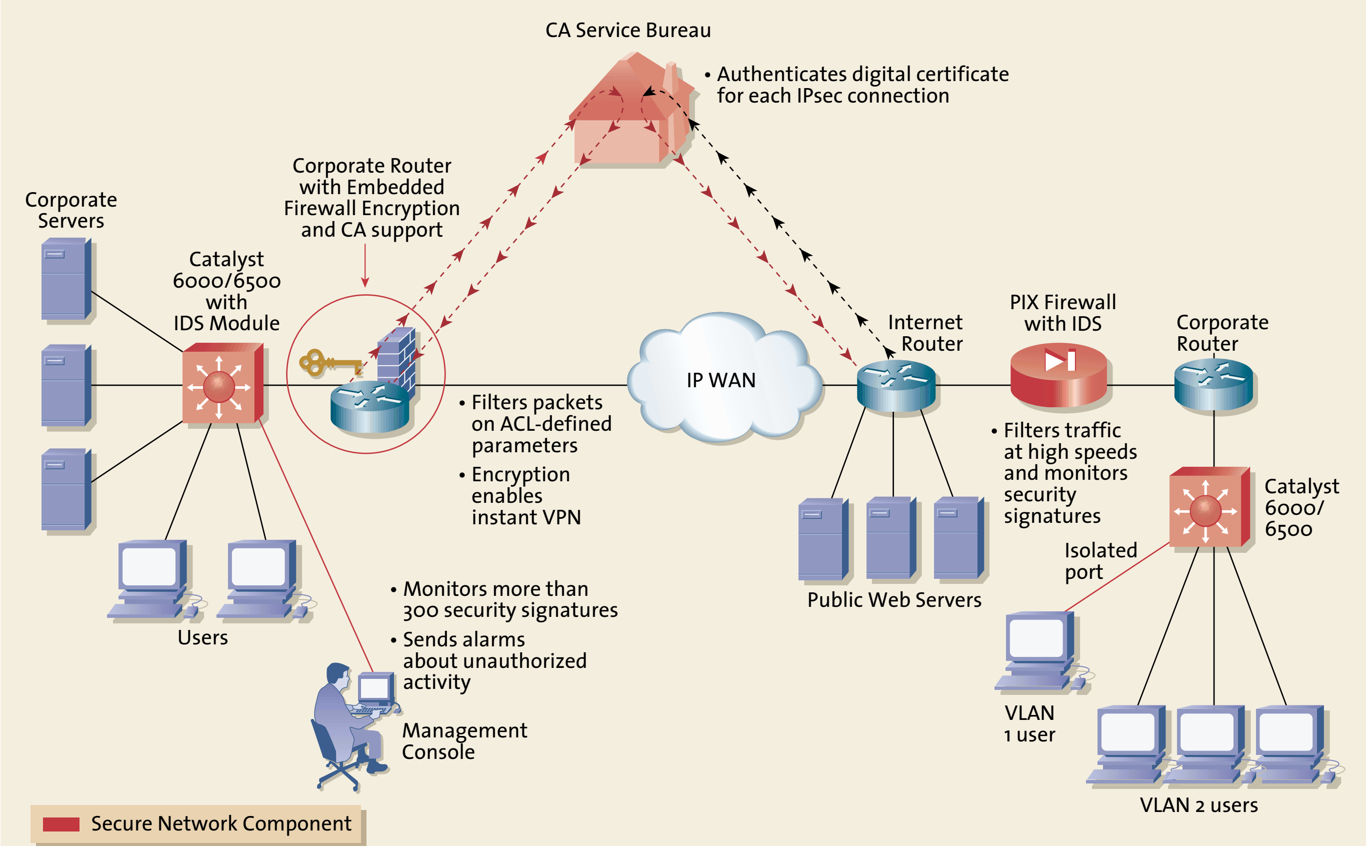
BASIC SECURITY IN THE CISCO IOS FIREWALL

Feature	Description
Context-Based Access Control (CBAC)	Provides access control of traffic crossing network boundaries on a per-application basis
Intrusion Detection	Monitors two-way traffic for 59 network security signatures
Authentication Proxy	Authenticates and authorizes LAN-based and dial-in communications using TACACS+ and RADIUS protocols
Denial-of-Service Detection and Prevention	Checks packet headers and drops suspicious packets
Java Applet Blocking	Protects against unidentified, malicious Java applets
Real-Time Alerts	Logs alerts of denial-of-service attacks or other network conditions. Configurable on a per-application, per-feature basis
Audit Trail	Maintains a transaction report by recording time stamp, source host, destination host, ports, duration, and total number of bytes transmitted
Event Logging	Allows administrators to track potential security breaches or other nonstandard activities in real time
Basic and Advanced Traffic Filtering	Allows administrators to define which traffic is allowed to pass through a network segment using standard and extended ACLs

NO TRESPASSING: Users can turn on Cisco IOS Firewall features on their routers as needed to filter packets and to authenticate and authorize users.

Security Blanket, *Continued from page 63*

SECURITY LANDSCAPE


CA Service Bureau
• Authenticates digital certificate for each IPsec connection
Corporate Servers
Corporate Router with Embedded Firewall Encryption and CA support
Catalyst 6000/6500 with IDS Module
• Filters packets on ACL-defined parameters
• Encryption enables instant VPN
IP WAN
Internet Router
PIX Firewall with IDS
Corporate Router
• Filters traffic at high speeds and monitors security signatures
Catalyst 6000/ 6500
Isolated port
Public Web Servers
Users
• Monitors more than 300 security signatures
• Sends alarms about unauthorized activity
Management Console
VLAN 1 user
VLAN 2 users
🟥 Secure Network Component

MULTIPLE PRIVACY POINTS: Intrusion detection, firewalling, encryption, CAs, and private VLANs combine to make privacy pervasive throughout the enterprise.

- A *promiscuous port* communicates with all other private VLAN ports. It is the port used to communicate with devices such as routers, backup servers, and administrative workstations.
- An *isolated port* has complete Layer 2 separation from other ports on the switch with the exception of the promiscuous port.
- *Community ports* communicate among themselves and with the promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports.

Privacy is granted at the Layer 2 level by blocking outgoing traffic to all isolated ports. All isolated ports are assigned to an isolated VLAN where this hardware function occurs. Traffic received from an isolated port is forwarded to all promiscuous ports only.

A PVLAN comprises pairs of VLANs that share a primary VLAN. Within a PVLAN, there are three distinct classifications of VLAN: a single primary VLAN, a single isolated VLAN, and a series of community VLANs. The primary VLAN conveys incoming traffic from the promiscuous port to all other promiscuous, isolated, and community ports. Isolated ports use the isolated VLAN to communicate to the promiscuous ports. The traffic from an isolated port is blocked on all adjacent ports and can be received only by promiscuous ports.

The community VLAN is used by a group of community ports to communicate among themselves and transmit traffic to outside the group via the designated promiscuous port.

◆ ◆ ◆

This article presents just a few examples of how the ability to activate security mechanisms is making its way into the core fabric of network connectivity infrastructures. Having a mix of security options—intrusion detection, packet filtering, encryption, authentication, and authorization—available within the same network elements that enable network connectivity ensures that security is not a separate, disjointed activity that organizations may or may not get around to implementing. In the open and trusted communications era of the Internet economy, organizations simply can't afford to take a risky attitude toward securing their electronic resources.▲▲

FURTHER READING

For more information on the products and technologies mentioned in this article, visit *Packet Online* at: cisco.com/go/packet/securityblanket

- **Cisco Intrusion Detection Systems**
- **Cisco IOS Firewall, CBAC, and Java blocking capabilities**
- **Cisco Private VLANs**
- **Encryption and Tunneling**

A
HAL B. WALLIS
PRODUCTION
"Casablanca"
CLAUDE RAINS · CONRAD VEIDT · SYDNEY GREENSTREET · PETER LORRE
Directed by MICHAEL CURTIZ

Play it SAFE SAM

Cisco SAFE provides a system-wide security blueprint to mitigate threats in AVVID networks

Anything of value must be safeguarded—and that includes the enterprise network. To make a successful transition into the Internet Age, organizations must open their networks and the resources on them to employees, partners, suppliers, and customers. Yet like the Casablanca of film legend, networks also attract unsavory characters. Along with the many legitimate users come those unwelcome few who would block access to mission-critical resources or worse yet, compromise them. Counteracting "crackers," or malicious hackers, involves preventing them from gaining access or limiting the damage they can do should they penetrate a network. In the past year alone, infamous cracking incidents and the havoc wreaked upon many legitimate businesses have highlighted the need for effective network security. Cisco responds to this need with Cisco SAFE, a blueprint for securing enterprise networks based on Cisco Architecture for Voice, Video and Integrated Data (AVVID) solutions.

Written by Gail Meredith (gmeredit@sonic.net), a contributing editor for Packet *magazine.*

ALL PHOTOS: WARNER/MPTV

"SAFE is not a marketecture; it's real," says David King, Director of Marketing, Security Solutions in the Virtual Private Network (VPN) and Security Business Unit at Cisco. "It has been designed and road-tested in Cisco labs, so we know it works. We've been testing it with our security consultants, making sure it's robust and has high integrity."

Cisco SAFE is a multilevel, defense-in-depth approach to network security. Its system-wide, layered approach is designed and laboratory tested in such a way that the failure of one security system is not likely to lead to compromise of network resources. According to Sean Convery, CCIE Number 4232 and Technical Marketing Engineer in the VPN and Security Business Unit at Cisco, "The focus is on security as an entire system as opposed to a collection of point products. It gets us away from thinking about security in terms of 'Here's my firewall. What do I need to do?' but rather, 'Here's my network. What threats do I have the potential to experience in this network, and how do I mitigate against those threats?'"

"You despise me, don't you?"

Threats can be internal or external (see "Defensive Attitude: Strategies for Dealing with Hackers and Crackers," page 71). News reports may lead people to erroneously believe that the biggest threat is from outside the network. However, though statistics vary, it is an accepted reality that most attacks start inside the network, initiated by disgruntled employees, corporate spies, visiting guests, or the inadvertent user. Threats can turn into attacks that can take many forms, such as simple reconnaissance, distributed denial of service, or IP address spoofing, done with the intent to disrupt business or acquire or alter confidential information.

The Cisco SAFE team recommends that an enterprise first perform a security posture assessment to gauge the greatest areas of weakness in the network. (See "Cisco Experts Pinpoint Network Vulnerabilities," page 5.) Also, "an organization first needs to have a fully fleshed-out security policy before they go in and do any sort of implementation," says Convery.

"We are organized, Monsieur."

Cisco SAFE is deployable because it's divided into logical modules for securing specific network segments and functions. Each module serves as a guideline for mitigating against those threats most likely to affect activities in a specific area. Enterprises can start by securing the most vulnerable areas first, then work their way through the rest of the network according to priority. "We're not recommending that enterprises adopt SAFE carte blanche," says Convery, "but that they examine the modular approach and decide where in their environment that they need more security or different levels of security, and how is their environment similar and dissimilar to the blueprint? Once they understand those relationships, then they can start mapping changes on a module-by-module basis to improve security."

"The Usual Suspects"

Convery points out, "As a network administrator, you have to make sure *all* your systems are secure; whereas a hacker only needs to find *one* that is not. If a hacker finds that one system, how do you make sure that the network design and security infrastructure reduce the impact of that compromise?" To help enterprises understand the targets of security attack and how to mitigate them, Convery and the Cisco SAFE team developed a set of Cisco SAFE axioms:

Routers are targets—potentially a cracker's best friend, routers provide access, so securing them is a critical priority. Some mitigation techniques are locking down telnet and Simple Network Management Protocol (SNMP) access, controlling access through identity protocols such as Terminal Access Controller Access Control System Plus (TACACS+), turning off unneeded services, logging at appropriate levels, and authenticating updates to routing tables.

Switches are targets—especially in internally-originated attacks. In addition to the mitigation techniques used on routers, switches can be secured through a number of trunk port management policies, such as disabling unused ports and deploying private virtual LANs (VLANs) to limit which ports can talk to other ports in the same VLAN.

Hosts are targets—as the most frequently attacked target and one of the most difficult to protect, hosts are appealing and vulnerable because they are visible. Administrators should pay careful attention to the multivendor components placed in host systems, and apply the latest updates and patches after first testing them.

Networks are targets—the worst attack is one you can't stop, as proven during the distributed-denial-of-service attacks on major Web sites in early 2000. Saturating the network with spurious traffic effectively shuts down these sites without causing any direct system damage. The best defense is coordination with the Internet service provider to rate-limit suspect traffic on all links to and from a target site, and apply filters as detailed in RFC 1928 and RFC 2827.

Applications are targets—weaknesses in application coding can be exploited for malicious or criminal purposes. Intrusion-detection systems (IDS) detect and react against suspicious activity to prevent such breaches. Host-based IDS prevents specific attacks at the host, while network-based IDS (such as Cisco Secure IDS) monitors the entire network.

"That is my least vulnerable spot."

The enterprise AVVID network is comprised of two functional areas: the campus and the edge. Cisco SAFE divides these areas into multiple modules according to function. Although modules interconnect much as the network does, they provide a logical basis for deploying robust security solutions in each functional area, allowing a phased deployment strategy starting with the most exposed or vulnerable spots. The management intranet should grow to coincide with each Cisco SAFE module deployed in the network.

For each module, Cisco SAFE defines its overall function, as well as expected threats, and lists all devices (security and otherwise) typically deployed within the module, design guidelines for a secure deployment, and alternatives to account for different architectures. As standard procedure, an enterprise information technology (IT) staff should incorporate security into the original design and deployment of any network segment.

Cisco SAFE blueprints are flexible and detailed enough for administrators to adapt them into existing enterprise networks with minimal disruption. Cisco SAFE allows network design teams to address the security requirements of each network function almost independently. Each module is generally self-contained, and assumes that any interconnected module has a basic security level. Administrators can concentrate on securing the most critical network functions (as determined by the security policy) without re-designing the entire network.

Primarily made up of Cisco security products interwoven with Cisco AVVID devices, Cisco SAFE modules provide a blueprint for security on a system-wide, threat-mitigation basis, rather than as individual products aimed at specific targets. Cisco's comprehensive security portfolio includes industry-leading products in identity, perimeter security, secure connectivity, security monitoring, and security policy management. Some of the newcomers to this lineup include the Cisco Secure PIX™ Firewall 535 (see "PIX of the Litter," page 75) and the Cisco Secure IDS card for Catalyst© 6500 series switches.

"Here's looking at you, kid."

Vigilance does not cease with deployment. It's equally important that security administrators keep up to date with the latest developments in the hacker and security community. Armed with the latest mitigation strategies and software patches, administrators need to maintain and monitor all systems using good system administration practices.

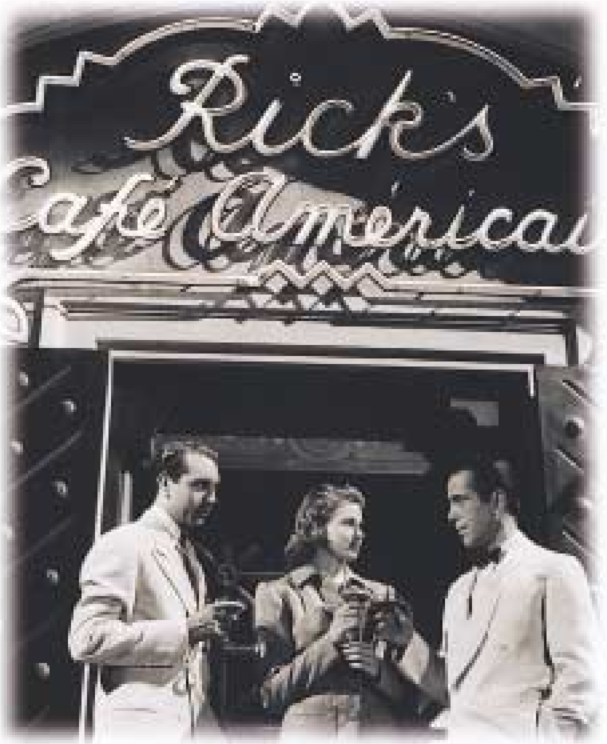
A cornerstone of the SAFE blueprint is an out-of-band management intranet, which facilitates secure management of all devices and hosts within the enterprise SAFE overlay. All devices in the Cisco AVVID network have a dedicated management interface, with direct, local connections to the management intranet wherever possible. "With an out-of-band management network, you can transmit more things in the clear and take advantage of more of the management functions without worrying about the security vulnerabilities that they create," says Convery.

The management intranet should not itself create security issues. Where geographic or system-related issues make a direct connection difficult or impossible, devices should connect with the management network via encrypted tunnels through the production network. With separate management and production networks, any compromise in one network is not likely to affect the other.

The Cisco SAFE management intranet module is comprised of two subnets divided by a firewall and where necessary, a VPN termination device. The segment outside the firewall connects to all devices in the production network, while the internal segment protects the many management host systems such as Cisco Secure IDS Director and Access Control Servers, network monitoring systems, syslog servers, and systems administration consoles. For added security, both segments of the management intranet should have an IP address space completely separate from the production network so that it is not advertised by any routing protocols. Device authentication helps prevent unauthorized configuration changes. Private VLANs on the internal subnet make it impossible for compromised devices to talk to other hosts on the same subnet, while the firewall prevents access to the production network through any "back door" scheme.

"I remember every detail."

With an out-of-band management intranet in place, logging and reporting become straightforward. Syslog data can be invaluable for troubleshooting network problems or security threats. With such data collected into syslog servers in the management subnet, third-party security analysis applications enable granular viewing and reporting on a real-time or daily basis. IDS data can be set to trigger alarms and responses to perceived threats; when dealing with attacks in progress, seconds matter. Configuration change management is also a security concern; when the network is attacked, it is important to know the state of critical network devices and when last-known modifications occurred.



"You think of everything, don't you?"

In addition to the management intranet module, Cisco SAFE currently includes module specifications for several other functional areas in the campus, including core, building distribution, building, server farms, and edge distribution. Along the edge, corporate Internet, VPN and remote access, WAN, and e-commerce modules provide secure connections to the outside world. All modules have been tested and proven in Cisco laboratories using Cisco equipment to assure their effectiveness and viability. This first set of modules covers most of the basic network functions. Along with continual updates to these modules, the Cisco SAFE team will continue to develop and rigorously test future modules to secure additional enterprise network functions.

"The beginning of a beautiful friendship."

One of the most exciting aspects of Cisco SAFE is its inclusion of Cisco's ecosystem partners. Cisco is actively developing key security partnerships with vendors, systems integrators, and tier-2 service providers to accelerate the adoption of robust network security worldwide. Ecosystem partners bring valuable tools and expertise to Cisco SAFE deployments by adding functionality to Cisco AVVID and security solutions, such as virus detection and screening or application-specific security such as content filtering and public key infrastructure (PKI). Partnerships also benefit customers by "regionalizing" security solutions to match national or local regulations or unique customer environments. Programs such as the Security and VPN Associate certification are field-driven, allowing Cisco to respond to market demands, test and validate detailed solutions, and drive rapid adoption of network security.

"As Time Goes By"

Activities are already underway to extend Cisco SAFE blueprints beyond enterprise security to other types of organizations. With changes in scale and scope, the principles readily apply to small and midsized business environments, even home offices. Cisco plans to develop SAFE solutions specifically tailored toward the cost and performance requirements of this growing market.

For service providers, Cisco is refining its Security certification for its Cisco Powered Network program to incorporate SAFE principles, products, and new provider-specific modules. Tier-2 managed service providers offering application hosting and managed security services can receive the greatest initial benefit of applying SAFE solutions to their networks.

Cisco SAFE will also grow to embrace other technologies, such as secure voice over IP, content delivery networking, and mobile networking, along with increased efforts to develop key partnerships. By increasing the number of solution-specific modules available and continually revising and enhancing existing modules, Cisco SAFE will continue to protect Cisco AVVID networks as time goes by. ▲▲

FURTHER READING

For more information on Cisco SAFE and products mentioned in this article, visit the following URLs:

- **Cisco SAFE home page:**
  cisco.com/go/safe
- **Cisco SAFE Axiom Guidelines:**
  Routers:
  cisco.com/warp/public/707/21.html
  Switches:
  www.sans.org/newlook/resources/IDFAQ/vlan.htm
- **Cisco SAFE Networkers session presentation:**
  cisco.com/networkers/nw00/pres/2502_6-28.pdf

Cisco SAFE

Threats Mitigated by Module

MANAGEMENT MODULE

- Unauthorized access—filtering at the Cisco IOS firewall stops most unauthorized traffic in both directions
- Man-in-the-middle attacks—management data crosses a private network, frustrating these attacks
- Network reconnaissance—management traffic does not enter the production network where it could be intercepted
- Password attacks—access control server allows for strong, two-factor authentication at each network management device
- IP spoofing—Cisco IOS firewall stops spoofed traffic in both directions
- Packet sniffers—switched infrastructure limits effective sniffing
- Trust exploitation—private VLANs prevent compromised devices from masquerading as management hosts

CORE MODULE

Packet sniffers—switched infrastructure limits effective sniffing

BUILDING DISTRIBUTION MODULE

- Unauthorized access—attacks against server module resources are limited by Layer3 filtering of specific subnets
- IP spoofing—RFC 2827 filtering stops most attempts
- Packet sniffers—switched infrastructure limits effective sniffing

BUILDING ACCESS MODULE

- Packet sniffers—switched infrastructure and default VLAN services limit effective sniffing
- Viruses and Trojan Horse applications—host-based virus scanning prevents most viruses and many Trojan Horses

SERVER MODULE

- Unauthorized access—host-based intrusion detection and access control mitigate this
- Application-layer attacks—operating systems, devices, and applications are kept current with the latest security fixes and are protected by host-based intrusion detection
- IP spoofing—RFC 2827 filtering prevents source address filtering
- Packet sniffers—switched infrastructure limits effective sniffing
- Trust exploitation—trust arrangements are very explicit; private VLANs prevent hosts on the same subnet from communicating unless necessary
- Port redirection—host-based intrusion detection systems prevent installation of port redirection agents

EDGE DISTRIBUTION MODULE

- Unauthorized access—filtering provides granular control over specific edge subnets and their ability to reach areas within the campus
- IP spoofing—RFC 2827 filtering limits locally initiated spoof attacks
- Network reconnaissance—filtering limits non-essential traffic from entering the campus
- Packet sniffers—switched infrastructure limits effective sniffing

CORPORATE INTERNET MODULE

- Unauthorized access—mitigated through filtering at the service provider edge, edge router, and corporate firewall
- Application-layer attacks—mitigated through intrusion detection at the host and network level
- Virus and Trojan Horse applications—email content filtering and host-based intrusion detection catch most viruses and Trojan Horses
- Password attacks—operating systems and intrusion detection detect threat, making limited services available to brute-force attacks
- Denial of Service—Committed Access Rate at ISP edge and TCP setup controls at the firewall
- IP spoofing—RFC 2827 and RFC 1918 filtering at ISP edge and enterprise edge router
- Packet sniffers—switched infrastructure and host-based intrusion detection limit exposure
- Network reconnaissance—intrusion detection detects this; protocols are filtered to limit its effectiveness
- Trust exploitation—restrictive-trust model and private VLANs limit attacks
- Port redirection—restrictive filtering and host-based intrusion detection limit attacks

VPN AND REMOTE ACCESS MODULE

- Network topology discovery—only Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) are allowed into this segment from the Internet
- Password attack—one-time password authentication reduces the likelihood of a successful password attack
- Unauthorized access—firewall services after packet decryption prevent traffic on unauthorized ports
- Man-in-the-Middle attacks—mitigated through encrypted remote traffic
- Packet sniffers—switched infrastructure limits effective sniffing

WAN MODULE

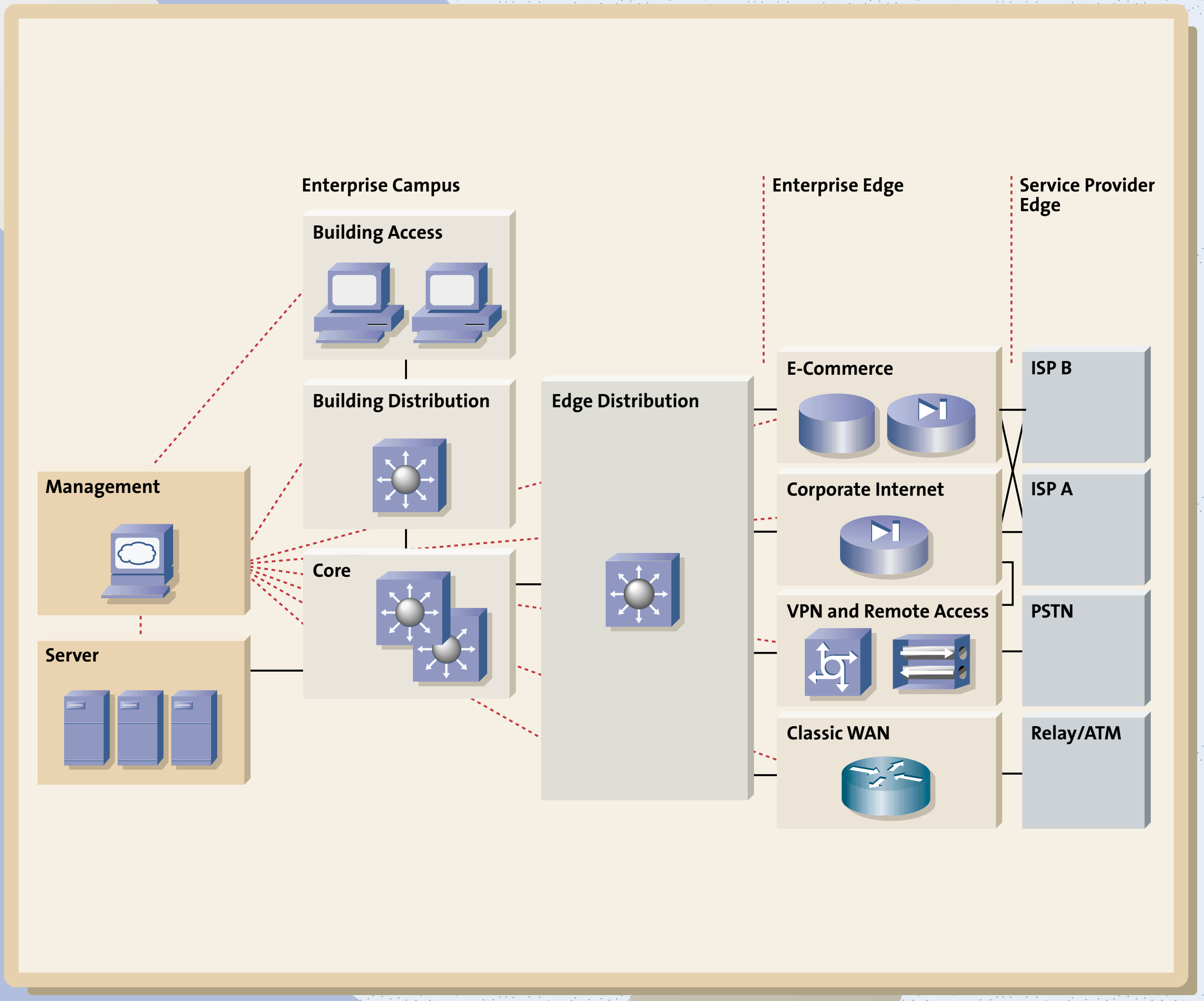
- IP spoofing—mitigated through Layer 3 filtering
- Unauthorized access—simple access control on the router limits the types of protocols that branch offices can access

E-COMMERCE MODULE

- Unauthorized access—stateful firewalling and ACLs limit exposure to specific protocols
- Application-layer attacks—mitigated through intrusion detection
- Denial of Service—ISP filtering and rate limiting reduce (D)DoS potential
- IP spoofing—RFC 2827 and RFC 1918 filtering prevent locally originated spoofed packets and limit remote-spoof attempts
- Packet sniffers—switched infrastructure and host-based intrusion detection limit exposure
- Network reconnaissance—ports are limited to only what is necessary; ICMP is restricted
- Trust exploitation—firewalls ensure communication flows only in the proper direction on the proper service
- Port redirection—host-based intrusion detection and firewall filtering limit exposure to attacks

Cisco SAFE: A Vision for Secure E-Business

Divided into functional modules for scalable, prioritized deployment, the Cisco SAFE Blueprint is designed to mitigate threats specific to each area of the network.

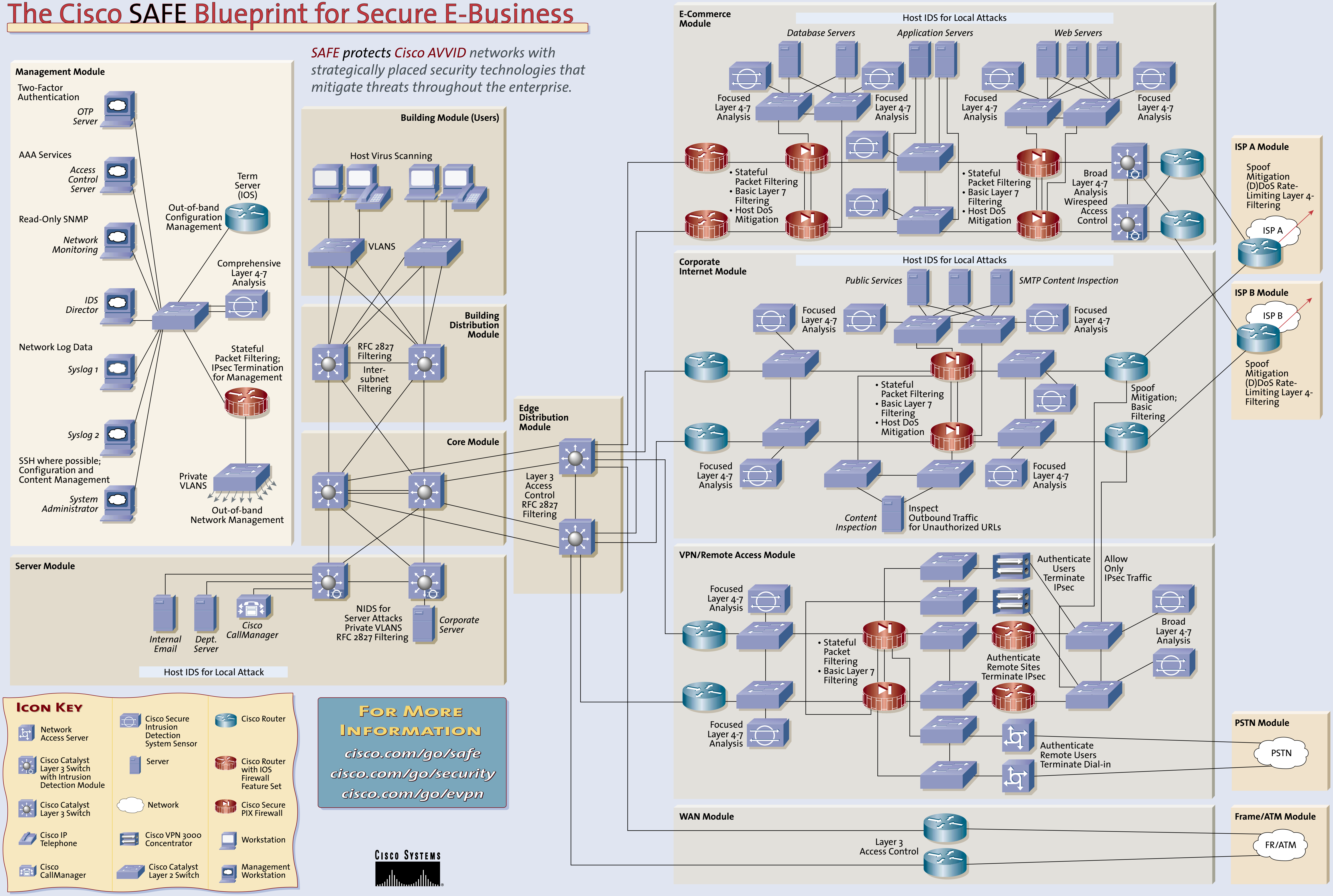


PACKET
CISCO SYSTEMS USERS MAGAZINE

Cisco Systems
cisco.com/go/packet

The Cisco SAFE Blueprint for Secure E-Business

SAFE protects Cisco AVVID networks with strategically placed security technologies that mitigate threats throughout the enterprise.


Management Module
Two-Factor Authentication
OTP Server
AAA Services
Access Control Server
Read-Only SNMP
Network Monitoring
IDS Director
Network Log Data
Syslog 1
Syslog 2
SSH where possible; Configuration and Content Management
System Administrator
Term Server (IOS)
Out-of-band Configuration Management
Comprehensive Layer 4-7 Analysis
Stateful Packet Filtering; IPsec Termination for Management
Private VLANS
Out-of-band Network Management
Building Module (Users)
Host Virus Scanning
VLANS
Building Distribution Module
RFC 2827 Filtering
Inter-subnet Filtering
Core Module
Edge Distribution Module
Layer 3 Access Control RFC 2827 Filtering
Server Module
Internal Email
Dept. Server
Cisco CallManager
NIDS for Server Attacks Private VLANS RFC 2827 Filtering
Corporate Server
Host IDS for Local Attack
E-Commerce Module
Host IDS for Local Attacks
Database Servers
Application Servers
Web Servers
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
• Stateful Packet Filtering • Basic Layer 7 Filtering • Host DoS Mitigation
• Stateful Packet Filtering • Basic Layer 7 Filtering • Host DoS Mitigation
Broad Layer 4-7 Analysis Wirespeed Access Control
ISP A Module
Spoof Mitigation (D)DoS Rate-Limiting Layer 4-Filtering
ISP A
ISP B Module
ISP B
Spoof Mitigation (D)DoS Rate-Limiting Layer 4-Filtering
Corporate Internet Module
Host IDS for Local Attacks
Public Services
SMTP Content Inspection
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
• Stateful Packet Filtering • Basic Layer 7 Filtering • Host DoS Mitigation
Spoof Mitigation; Basic Filtering
Focused Layer 4-7 Analysis
Focused Layer 4-7 Analysis
Content Inspection
Inspect Outbound Traffic for Unauthorized URLs
VPN/Remote Access Module
Focused Layer 4-7 Analysis
Authenticate Users Terminate IPSec
Allow Only IPSec Traffic
Broad Layer 4-7 Analysis
• Stateful Packet Filtering • Basic Layer 7 Filtering
Authenticate Remote Sites Terminate IPSec
Focused Layer 4-7 Analysis
Authenticate Remote Users Terminate Dial-in
PSTN Module
PSTN
WAN Module
Layer 3 Access Control
Frame/ATM Module
FR/ATM
Icon Key
Network Access Server
Cisco Catalyst Layer 3 Switch with Intrusion Detection Module
Cisco Catalyst Layer 3 Switch
Cisco IP Telephone
Cisco CallManager
Cisco Secure Intrusion Detection System Sensor
Server
Network
Cisco VPN 3000 Concentrator
Cisco Catalyst Layer 2 Switch
Cisco Router
Cisco Router with IOS Firewall Feature Set
Cisco Secure PIX Firewall
Workstation
Management Workstation
Cisco Systems

For More Information

cisco.com/go/safe
cisco.com/go/security
cisco.com/go/evpn

Reprinted with permission from *Packet*™ magazine (Volume 13, No. 1), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

Defensive ATTITUDE

Strategies for dealing with hackers and crackers

IS BIG BROTHER WATCHING YOU? PERHAPS NOT, but you may be shocked to discover who is.

As networks grow ever more pervasive and easier to use, they also become easier to compromise. Open computing standards—especially the Internet and its technologies—have transformed the way we do business, the way we communicate, even the way we shop and learn. Yet this ubiquity makes networks and the resources on them vulnerable. Network security is more important than ever.

White Hat or Black Hat?

Hacking is the high-tech iteration of a pastime that's been around since the dawn of time. People are naturally curious, and barriers tempt and taunt them. Since Pandora opened that fateful—and apparently unsecured—box, people have gone to extraordinary measures to see what is private, to go where they are not permitted. Yet the desire to see what's inside the box does not necessarily imply malicious intent. Hacking can do great service or great harm. And that's why members of the hacking community are quick to draw the distinction between "white hats" and "black hats."

The white hats are *true* hackers, and consider themselves part of a noble profession. By discovering and reporting vulnerabilities, hacker groups worldwide play a valuable role in the advancement of security technologies and products. The Cisco Secure Consulting Services team, for example, is a team of white-hat hackers whose mission is to discover vulnerabilities in their clients' networks and recommend ways to secure them. Their activities are invited and legal.

Nevertheless, it's the infamous "black hats" who enjoy a disproportionate share of media attention. True hackers refer to their black-hat counterparts as crackers, vandals, or intruders. Crackers perpetrate crimes for political gain, economic advantage, social status, or simple amusement. They are by nature unpredictable, often malicious, and certainly unwelcome. They deface Web pages, crash computer systems, steal or damage confidential information, and disrupt business.

ILLUSTRATION BY CHRIS GALL

Yet another class of hackers are condescendingly referred to as "script kiddies." These are amateurs who find hacking tools on line and use them without understanding how they work or what damage they can do. Script kiddies can—unwittingly or deliberately—do great harm.

Crunchy Outside, Chewy Inside

"The greatest threat to security comes from those already inside the network," says Michael Fuhrman, Security Consulting Manager, Cisco Secure Consulting Services at Cisco. "The external perimeter is a known risk, and most people have some kind of defense in place. But most LANs have few or no restrictions. Once a cracker is inside the perimeter, he can freely roam the internal network. We describe these networks as 'hard and crunchy on the outside, soft and chewy on the inside.'"

A startling percentage of crackers already have internal access because they are employees. "The 2000 Information Security Industry Survey," a study cosponsored by ICSA.net and Global Integrity, revealed that this year alone nearly twice as many companies suffered insider attacks such as theft, sabotage, and intentional destruction of computer property compared to 1999. The number of companies that dealt with employees who intentionally disclosed or destroyed proprietary corporate information rose 41 percent. The same study reports that 80 percent of the US companies surveyed has been hit this year with some form of cyber attack.

A Matter of Policy

The pressing need for network security starts with formulating a multilayer defense as part of the corporate security policy and continues with instilling secure habits among employees. While it's obvious that people shouldn't post their passwords on computer monitors, many employees are careless when it comes to safeguarding information. "Extremely few companies have a written security policy," says Chris Lonvick, Manager of Consulting Engineering in the office of the Chief Strategy Officer at Cisco. For guidelines on writing effective security policies, Lonvick recommends the Internet Engineering Task Force (IETF) RFC 2196.

Policies define standards for secure network design and defensive actions, allowing network managers to incorporate a consistent multilayer defense strategy into their procedures. In large enterprises, the Cisco Secure Consulting Services group recommends internal measures that separate core business functions to harden that "chewy inside." For example, using firewalls and access control lists to segment corporate finance, the executive staff, and production networks can go a long way toward limiting the amount of information intruders could gather or the damage vandals could do.

Comprehensive security policies should also contain action checklists that network administrators can follow to allay attacks in progress. "When an attack occurs, people without policies tend to randomly shoot at moving targets with equally random success," says Lonvick. "A good procedural checklist can reduce the duration of a denial-of-service [DoS] attack by allowing the staff to quickly identify the source and nature of the traffic and apply filters accordingly."

Defending the Fort

So what do crackers do, and can a network defend itself against them? Attacks take hundreds of forms falling into several categories: reconnaissance attacks, access attacks, and DoS attacks. Many attacks can be prevented or curbed through disciplined systems administration procedures.

Reconnaissance attacks use sniffers, scanners, and other tools to gather information that could be used to compromise assets later. Many crackers run such tools continuously and sort data to identify vulnerable hosts. For example, a cracker could exploit the finger protocol to gather one half of a username/password combination. "Most people don't need the finger protocol anymore," says Fuhrman, "but they may have to go to dozens of hosts to manually turn it off, so they won't bother even though it's a commonly exploited vulnerability." Other common weaknesses are found in programs running under the portmapper, such as rusersd and network file system (NFS) service, and basic mail protocols like Simple Mail Transfer Protocol (SNMP). Most reconnaissance attacks can be deflected through conscientious router and server configurations to turn off unneeded services, especially where they are exposed to the Internet.

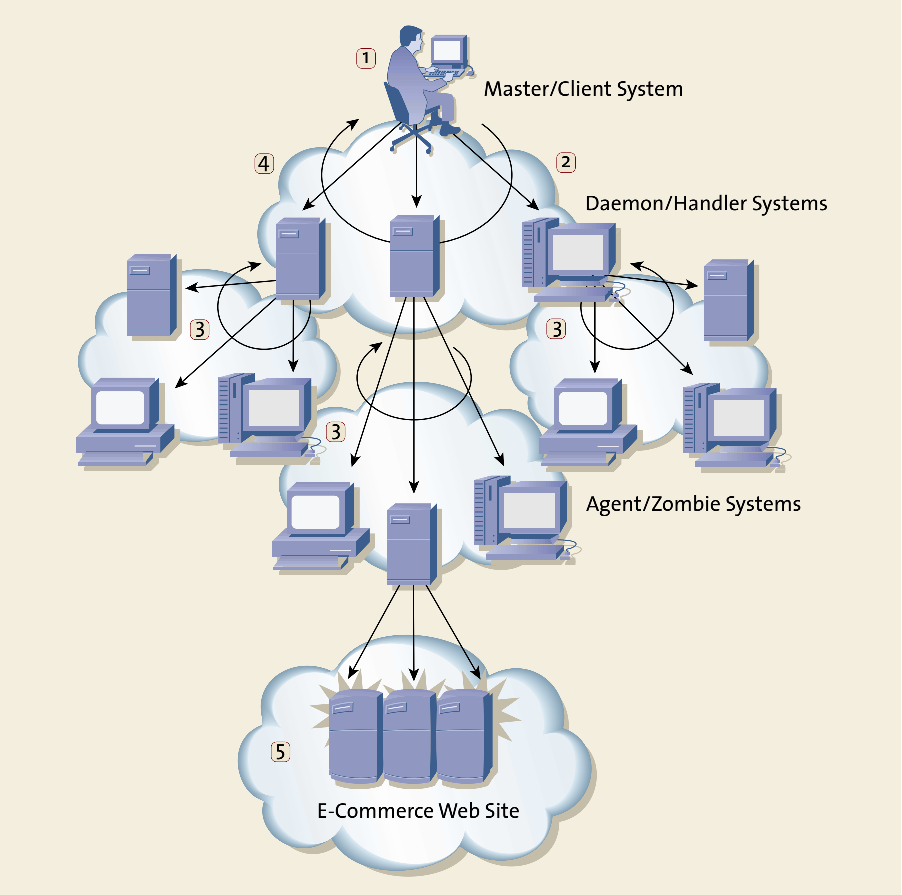
Access attacks exploit known vulnerabilities in authentication services, File Transfer Protocol (FTP) services and Web services to gain entry to Web accounts, confidential databases, and other sensitive information. For example, crackers could deploy a password-cracking tool against known usernames gathered in a reconnaissance attack to gain entry to e-mail. Using such tools, the Cisco Secure Consulting Services group has been able to crack 53 percent of passwords obtained from compromised networks. Preventive actions against access attacks include using strong passwords that combine letters and numbers, protecting Internet mail servers using proxy devices such as firewalls, and filtering incoming TCP requests by allowing only those services that are needed. As a rule, do not allow TCP/IP port 111 or 139 as both have a history of security problems and weak authentication. TCP/IP ports 111 and 139 support the Unix portmapper (or RPC) and Windows NetBIOS services. Both services are rarely deployed over the Internet but are often allowed through Internet filtering devices.

Web services are particularly vulnerable to access attacks. "Web services are usually business critical," says Fuhrman. "You need visibility inside Web traffic to watch for violations." Recent vulnerabilities in such applications as Microsoft's IIS Web server allow attackers to imbed malicious commands inside proper Web requests. An intrusion detection system (IDS) such as Cisco Secure IDS provides the higher-layer packet visibility required for real-time detection and response to such attacks.

DoS attacks grabbed headlines in February 2000 as they blocked access to Web-based companies such as Yahoo! and eBay. Somewhere on the Internet, a DoS is always under way, according to Edward

Written by Gail Meredith (gmeredit@sonic.net), a contributing editor for Packet *magazine.*

DISTRIBUTED DENIAL OF SERVICE ARCHITECTURE



CIRCLING THE WAGONS: Distributed denial-of-service attacks overwhelm the target systems using this general method: 1) The hacker scans for systems to attack; 2) The hacker installs software to scan for, compromise, and infect agents; 3) Agents are loaded with remote-controlled attack software; 4) Hacker issues commands to handlers, which control agents in a mass attack; 5) The resulting traffic generated by Agents overwhelms all interfaces into the target, putting it out of service.

Vielmetti, Consulting Engineer, Office of the Chief Strategy Officer at Cisco. A DoS attack sends a large amount of useless traffic to a particular host or port. While they do not compromise or damage hosts, well-executed DoS attacks can prevent any legitimate traffic from getting through, effectively shutting down its services.

An especially malicious form of DoS attack is distributed denial of service (DDoS), which compromises multiple hosts and enslaves them to send vast amounts of traffic to a target host. These "zombie" attack hosts often reside on unsuspecting public networks such as those found in universities. Network administrators are often unaware that their hosts have become zombies because they only watch for incoming attacks. RFC 2267 specifies ingress and egress filters that can prevent your routers and hosts from becoming the source of a DoS attack.

How DDoS Attacks Occur

DDoS attacks are especially ruthless because there seems to be little that anyone can do to prevent them. Vielmetti suggests a multistep strategy for mitigating attacks in progress. First, "make sure you're friends with your service provider," he advises. "If an attack does happen, you need to be able to react out-of-band." That's often as simple as having a telephone number to someone at the service provider who is familiar with your organization and is committed to working with you to filter DDoS traffic promptly.

Next, it's useful to have detection systems that can readily identify an incoming DoS attack. "Attacks can be disguised to mimic equipment failures," cautions Vielmetti. "It can be difficult to tell whether you're under attack or whether a board has gone bad." In certain cases, the link or host may be saturated with valid traffic, with the same result as a DoS attack. Two famous examples of such an overload are the online Victoria's Secret fashion show and the NASA Mars Lander Web site.

To determine whether an attack is actually in progress, having a service agreement with Cisco puts its Technical Assistance Center (TAC) at your disposal. TAC personnel know how to determine whether a host is under attack, using real-time data analysis tools with Cisco routers to check packet counters and characterize traffic flows. Accurate and timely information is vital to successfully filtering a DoS attack.

After the attack has been identified and characterized, filters can be set in place to clamp the flood of DoS traffic. Filtering is most effective at the service provider's network egress point to the target host using access control lists (ACLs) or Committed Access Rate (CAR). CAR includes a rate-limiting function that can be tuned to stop or slow the offending flow to manageable levels.

Unfortunately, says Vielmetti, DDoS traffic is so varied and can mimic normal traffic so closely that it is very hard to design one CAR or ACL configuration that is good for all circumstances. A network engineer can look at baseline traffic on a link to broadly characterize regular traffic and then use this to set filters when an attack is in progress.

Other keys to preventing widespread DDoS attacks are greater awareness among network administrators and a willingness among the Internet community to work together to deflect such attacks.

A Step Ahead of the G-Men

An adage of the Internet age is that hackers will hack. They hack for benefit and harm. While white-hat hacking will always have a place in the Internet community, it's important to keep a step ahead of the black-hat crackers. Aside from pointers mentioned

Continued on page 99

PIX of the LITTER

New Cisco Secure PIX 535 and VPN accelerator card add higher capacity and performance to Cisco Secure PIX Firewall family

For people who like their firewalls big and powerful, we'd like to introduce you to the Cisco Secure PIX™ 535 Firewall. Delivering carrier-class performance that meets the needs of large enterprise networks as well as service providers, the PIX 535 is definitely the pick of the litter.

The newest member of the market-leading Cisco Secure PIX Firewall family has the ability to support more than 500,000 concurrent connections and 1 Gigabit per second of throughput. With this level of performance in a single system, the PIX 535 eliminates the need to load balance multiple standalone firewalls. This capability significantly reduces network complexity without compromising security.

"The Cisco Secure PIX 535 Firewall enables an enterprise to connect to a single, fat pipe in the network that previously was a choke point for security processing," says Dennis Vogel, product manager for the Cisco Secure PIX Firewall family. "The processing power offered in a single PIX 535 will help enterprises keep pace with ever-growing traffic volumes while assuring reliable, consistent security protection across the network."

Playing It SAFE

The PIX 535 provides important safeguards for large corporate networks against vulnerabilities associated with doing business over the Internet. More importantly, it can be implemented as part of the recently announced Cisco SAFE blueprint for secure e-business.

Developed for real-world network deployment, Cisco SAFE helps companies compete in the Internet economy by integrating scalable, high performance security services throughout the e-business infrastructure. It takes a modular approach to security in which design, solution implementation and management processes are all provided in detail. Companies can choose from several individual modules, or "building blocks," each designed, tested and proven to address specific e-business applications, such as electronic commerce or supply chain management. (See "Play It SAFE, Sam," page 67.)

Firewall Tip: Add an IDS

Deploying an intrusion detection system (IDS) to complement your firewall can significantly enhance your security posture. A firewall's primary function is to control access to services and hosts based on your site security policy. If a connection to a specific host is permitted, the firewall may not be configured to inspect the content of the permitted traffic. For example, all connection requests to a Web server in a demilitarized zone (DMZ) may be permitted by a misconfigured firewall, including malicious traffic designed to exploit a buffer overflow vulnerability in an HTTP server. While some firewalls may not protect against data- or content-driven attacks, an IDS will. An IDS analyzes packet datastreams within a network, searching for unauthorized activity. Furthermore, firewalls typically will not protect you against attacks originating from inside your network or entering your environment from a nonfirewalled ingress point, such as a remote access server. IDS appliances can be strategically deployed to monitor activity from internal sources and other network ingress points without impacting your network performance. Today, network administrators have the choice of deploying dedicated IDS appliances such as the Cisco Secure 4210 IDS appliance and the Catalyst® 6000 IDS module, or turning on IDS capabilities inherent in Cisco IOS® routers and PIX firewalls (see "Security Blanket: Weaving Security into the Network Fabric," page 61).

Which PIX Is Right for You?

From the home office to the central office, there's a Cisco Secure PIX Firewall to meet any environment's security and virtual private network (VPN) requirements.

Cisco Secure PIX 506
Remote office or branch office
Throughput: 9 Mbps
Sessions: 1000
CPU: 200MHz
Interfaces: 2

Cisco Secure PIX 515
Small and midsized business
Throughput: 170 Mbps
Sessions: 128,000
CPU: 200MHz
Interfaces: up to 6

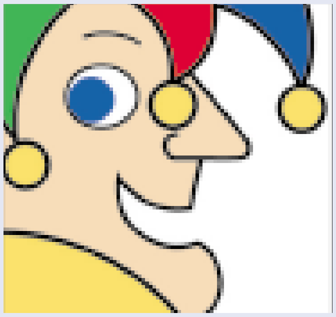
Well-Bred Family

The new PIX 535 extends the line of the market-leading Cisco Secure PIX Firewall family. All PIX firewalls offer built-in IP security (IPsec) encryption, allowing secure site-to-site connectivity or deployment of secure, remote-access VPNs. Like other PIX models, the PIX 535 also supports redundant units with stateful failover capabilities to ensure continued secure processing should the primary unit experience a problem.

Booster Shot—the VPN Accelerator Card

The new VPN accelerator card for the Cisco Secure PIX Firewall family improves the performance of VPNs by offloading IPsec encryption functions from the central firewall processor to dedicated hardware. Installed in a PCI slot inside the PIX chassis, the card works transparently and does not require activation commands nor configuration changes. It is quite literally a "plug and play" process.

The VPN accelerator card encrypts data using the Data Encryption Standard (DES) and Triple DES algorithms at speeds up to 100 Mbps. By handling IPsec-related tasks such as hashing, key exchange, and storing security associations, the card frees the PIX main processor and memory for other perimeter security functions.▲▲

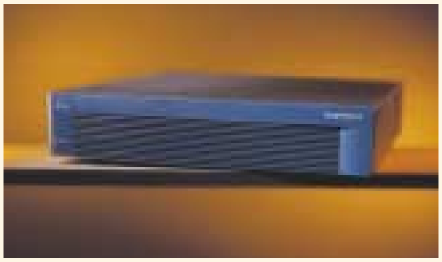


Fools for Security

The Motley Fool recently selected Cisco Secure PIX firewalls to secure its popular financial Web site, Fool.com. The Fool's IT department evaluated several software-based solutions, but decided against them because they were based on general-purpose operating systems. The evaluation team's preference was to go with a robust, hardened, VPN-enabled firewall appliance that wasn't as susceptible to the types of bugs, glitches and vulnerabilities often associated with other firewalls.

"Cisco's PIX is exactly what we wanted," explained Joel Salamone, MIS Director for The Motley Fool. "There is no extraneous software cluttering the operating system that can be exploited." The PIX family's similar management interface and configuration also shortened training time, and guaranteed easier administration. In addition, the number of maximum possible connections running through PIX was more than enough to accommodate the Fool's global network needs. "One of the things we really like about the PIX," said Dwight Gibbs, Chief Technology Officer for The Motley Fool, "is that it enabled us to quickly and inexpensively roll out a VPN linking our offices in the US, UK, and Germany. We can now collaborate securely thanks to the PIX."

Cisco Secure PIX 520
Enterprise
Throughput: 370 Mbps
Sessions: 250,000
CPU: 350 MHz
Interfaces: up to 6



Cisco Secure PIX 525
Large enterprise
Throughput: 370 Mbps
Sessions: 280,000
CPU: 600 MHz
Interfaces: up to 8

Cisco Secure PIX 535
Large enterprise and service provider
Throughput: 1.0 Gbps
Sessions: 500,000
CPU: 1 GHz
Interfaces: up to 8

COMMITTED TO CUSTOMERS: HomeSide Lending network engineers (left to right) Ken Lui, Chris Kane, Rob Miller, and Bill Robinson.

END TO END CONFIDENCE

This large, full-service mortgage lending company keeps customer data safe with a multilayer security architecture.

While all companies must pay close attention to information technology (IT) security, financial services firms that do business on the Internet face especially challenging security requirements. Just ask Robert Spain, LAN/WAN Manager at HomeSide Lending, Inc., one of the largest full-service residential mortgage banking companies in the US. HomeSide Lending (www.homeside.com) is tasked with presenting an open, welcome environment for Web users while ensuring that their personal and financial data isn't viewed by other users or accessed by outsiders. The company must also be mindful of internal employees who might need to transmit sensitive information from the corporate intranet to the outside world.

"Strategically, security has top priority in everything we do," says Spain, who recently led a comprehensive Internet security project to support HomeSide Lending's new system for online loan applications and approvals. "Customers who purchase and refinance their homes appreciate the convenience of conducting business on line, but they need assurances about security. The online financing and loan approval processes involve highly sensitive financial and personal information."

Headquartered in Jacksonville, Florida, HomeSide services more than US$170 billion in home loans for more than 1.6 million homeowners and in 1999, originated more than US$20 billion in new loans. As a wholly-owned subsidiary of National Australia Bank, HomeSide is poised to become the world's first international mortgage company featuring Web-based mortgage approval. Under IT Director Ed Hills, Spain worked with an internal team of four certified networking experts, each with several years of experience, to establish a multilayer security architecture. They created a security system that protects the network at each real and virtual point: from the routers and firewalls to the multilayer switches and load-balancing devices. "The system had to be 24-by-7, scalable, performance-driven, secure, architecturally redundant, highly responsive, and easy to manage," explains Spain. "We had to design a highly resilient security architecture with multiple layers. If an intruder makes it over one hill, he's got several more to climb."

Dollars and Sense

HomeSide is committed to making business easy for its customers. With loans-by-phone and e-commerce services, customers can handle the entire mortgage process from the comfort of their homes. Loans are processed in centralized mortgage-handling facilities. The processing staff and telephone loan officers collect all the required documentation from borrowers, submit loans to underwriting for approval decisions, and schedule loan closings.

In the past, HomeSide relied on a single application-level firewall running on an NT operating system with proxy and load-balancing-specific servers. This multiple operating system platform made integration, upgrades, troubleshooting, and maintenance more complex than it needed to be for HomeSide. So began an extensive evaluation and design process by the HomeSide team. They compared firewall equipment and load-balancing devices from several companies before deciding on an end-to-end Cisco infrastructure.

HomeSide's Bob Spain

"The old firewall had growth limitations and was inefficient," says Spain. "I decided to abandon the application firewall architecture and began a very extensive comparative process analysis of several leading products. There was no preconceived favoring of any product. Moving quickly beyond the marketing hype, I established over 33 critical areas, and we carefully researched each product in relation to those areas. Cisco had the product that best met our needs," sums up Spain.

HomeSide Security Overview

HomeSide's security architecture is designed around two tiers: a demilitarized zone (DMZ) and a corporate network zone. External servers—including World Wide Web, mail, and FTP servers—are in the DMZ tier. Private servers, mail hubs, and internal clients are located in the corporate tier.

The basic network architecture consists of two T1 lines from the Internet that feed into two Cisco 2611 routers running firewalls integrated within the Cisco IOS® software. From the routers, traffic is directed into a Catalyst® 6006 switch with dual-supervisor multilayer switch feature cards fronting dual Cisco Secure PIX™ 520 Firewalls. After passing through the PIX firewalls, traffic is managed by Cisco LocalDirector load-balancing devices and a Cisco Secure intrusion detection system (formerly called Cisco NetRanger) before it reaches the servers in each zone where HomeSide's applications and content are stored.

"Combining the Cisco PIX firewall with Cisco routers running Cisco IOS software gives us a powerful, multilayer security solution with multiple lines of defense," says Spain.

First Line of Defense

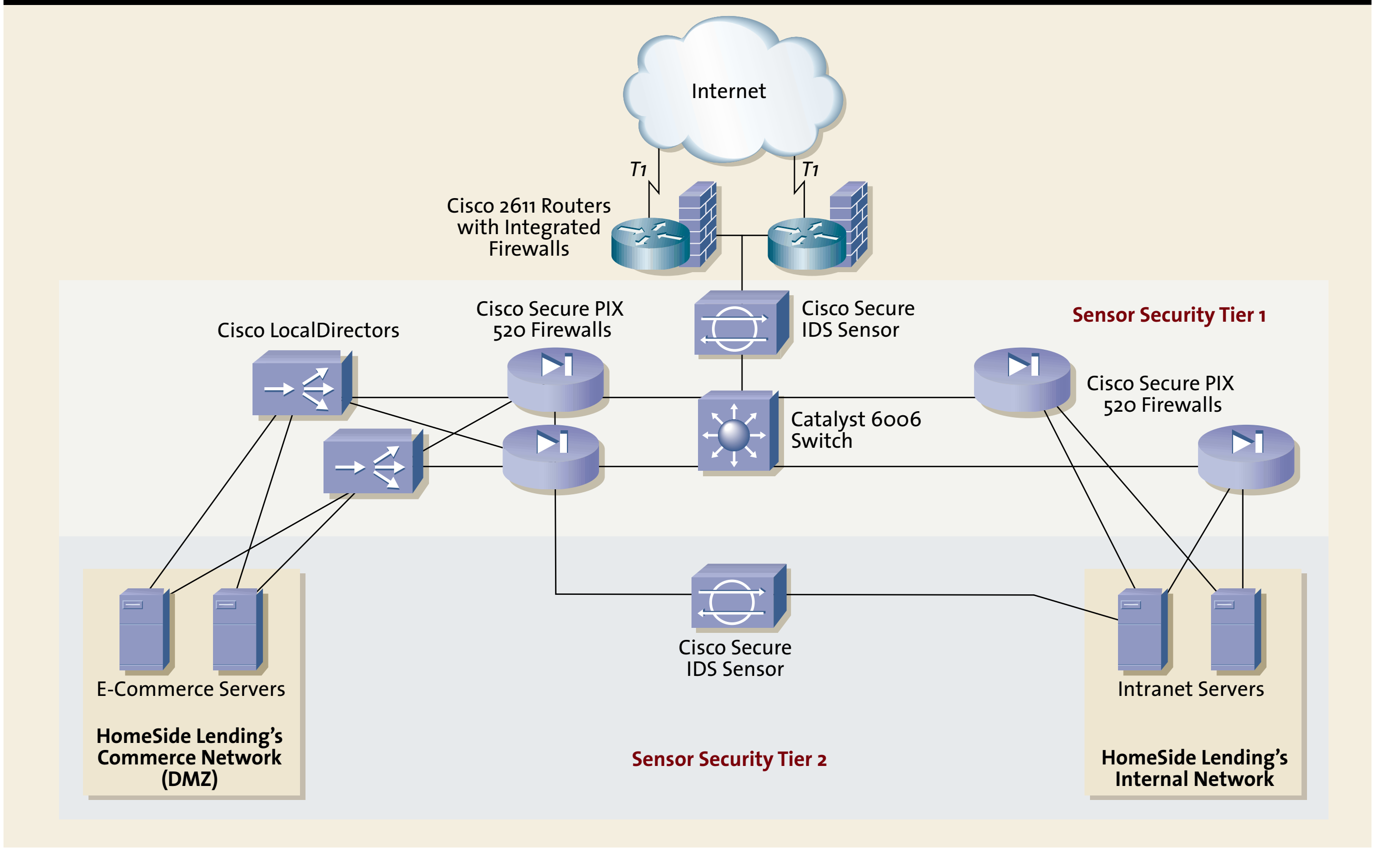
The Cisco 2600 series routers used by HomeSide include Cisco IOS firewalls with the intelligence to recognize and prevent common security attacks. "The Cisco IOS firewall puts up some substantial security elements," explains Ken Lui, Senior Network Communication Engineer at HomeSide Lending. "For example, using the IDS [intrusion detection system] feature along with

Continued on page 81

PHOTOS BY JEFFERY SALTER/SABA

HomeSide Lending, Continued from page 79

TWO-TIER SECURITY ARCHITECTURE


Internet
T1
T1
Cisco 2611 Routers with Integrated Firewalls
Cisco LocalDirectors
Cisco Secure PIX 520 Firewalls
Cisco Secure IDS Sensor
Sensor Security Tier 1
Cisco Secure PIX 520 Firewalls
Catalyst 6006 Switch
Cisco Secure IDS Sensor
E-Commerce Servers
HomeSide Lending's Commerce Network (DMZ)
Sensor Security Tier 2
Intranet Servers
HomeSide Lending's Internal Network

HOME SWEET HOME: HomeSide Lending keeps its customers' mortgage information safe through a multilayer security architecture that protects the network at each real and virtual point, from the routers and firewalls to the multilayer switches and load-balancing devices.

access list restrictions and Committed Access Rate prevents access beyond the routers. The common 59 intrusion signatures, IP spoofing, SYN attacks, and any Internet Control Message Protocol or ping of death will be dropped at the router."

Lui configured the Cisco 2600 series routers for dynamic routing redundancy and load sharing through the Catalyst 6006 switches, using Border Gateway Protocol (BGP) and Enhanced Interior Gateway Routing Protocol (EIGRP) to optimize reliability and performance. "If one T1 goes down, traffic is automatically forwarded by EIGRP to the other route," says Lui. "This setup gives us failover with no performance degradation."

To simplify maintenance, improve performance, and enhance security, Lui shut down routing functions such as IP source-route, IP finger, Cisco Discovery Protocol (CDP), IP domain lookup, Network Time Protocol (NTP), IP-directed broadcast, and Simple Network Management Protocol (SNMP). Beyond the routers is a Catalyst 6006 switch with dual-supervisor multilayer switch feature cards. Multilayer switching is deployed in full-flow mode, using EIGRP for dynamic routing redundancy and load sharing between the routers.

"In the Internet world, if you're down for a few seconds, customers are going to move on," Lui concedes. "So we needed plenty of capacity and scalability for each component. Our architecture supports inherent failover within the routing and switching infrastructure."

Heart of the Matter

The heart of HomeSide's security architecture resides in the Cisco PIX firewalls. These devices provide full firewall protection by concealing the internal corporate network from the outside world. They also allow secure access to the Internet from within the corporate network.

"With PIX, we achieve strong, stateful security without the overhead and performance limitations of OS-based firewalls," says Chris Kane, a Senior Network Engineer at HomeSide. "These systems give us a complete accounting and logging of all transactions, including attempted compromise on the internal network."

As with the other integrated devices, the Cisco PIX firewalls are deployed in an active standby configuration with stateful failover. With Cisco PIX firewall software version 5.2.3, the PIX is enabled with IDS technology that provides added functionality and enables the PIX to protect against the most common attacks. "A common attack might overwhelm a system with SYN requests, causing a server to crash and deny service to other users," says Kane. "FloodGuard and IDS prevents such attacks from happening."

To increase security and assist troubleshooting, all HomeSide's firewalls are set up with a syslog server for tracking and analyzing problems. Network Address

Continued on page 83

HomeSide Lending, Continued from page 81

Translation (NAT) on the e-commerce side protects the Web servers, and Port Address Translation (PAT) on the corporate side protects internal IP addresses.

To control Web access, the team also set up an access control server (ACS) with Terminal Access Controller Access Control System Plus (TACACS+) to work with the PIX firewall. Each time a TCP connection is established from an inside host to access the Internet through the PIX firewall, the information about the connection is logged in a stateful session flow table. Returned packets are compared to session flows in the connection table and permitted through the Cisco PIX firewall only if a appropriate connection exists to validate their passage.

Maintenance on the Fly

Not only does HomeSide's new architecture ensure much tighter security, it's also much simpler to maintain. "With PIX, we can upgrade the software and keep our security systems running," says Rob Miller, a Senior Network Engineer at HomeSide. "For example, during the update to version 5.2.3 of the PIX code, we configured the firewalls one at a time in a single afternoon, with no loss at all due to the statefulness."

"With the application-level firewall, we would either have to lose connectivity to the Internet or compromise security," adds Spain. "In the real world of e-commerce, being able to perform an upgrade without taking the firewalls offline is tremendously significant."

Application-level firewalls are operating system-dependent and thus require not only their own software upgrades but occasional service packs and patches to the operating system itself—in HomeSide's case, Microsoft Windows NT. According to Miller, this process involves removing the firewall software, applying the OS patches, and reapplying the firewall software.

Establishing a proxy-based failover solution would have required another Windows NT server plus Microsoft cluster server software so that two proxy servers could run together in hot standby mode. From a business perspective, says Miller, that approach would've meant purchasing multiple licenses and maintaining multiple devices. HomeSide achieved the same result more economically with the PIX system, which isn't dependent on external servers or operating systems.

Additionally, proxy servers run at the user level and operate by copying data between separate TCP connections. The Cisco PIX firewall operates on the packets directly, resulting in much higher performance. "Working in tandem with routers and Cisco IOS software, the PIX firewall provides a second layer of protection that keeps unauthorized users from accessing our corporate network," adds Miller. "PIX is much less complex and much easier to maintain than a proxy server."

Spain's goal: Redundancy and minimal maintenance

Balancing the Load

Once through the PIX firewall, user requests are managed by Cisco LocalDirector, an integrated hardware and software solution that intelligently balances network traffic across multiple TCP/IP application servers. All physical servers appear as one virtual server, which means that only a single IP address and a single URL are required for an entire server farm.

"By distributing user requests across a cluster of servers, Cisco LocalDirector optimizes responsiveness and system capacity while reducing the cost of network services," notes Bill Robinson, a Network Communications Engineer at HomeSide. "It also has its own integrated security features that are capable of protecting the servers from unauthorized access."

HomeSide deployed two Cisco LocalDirector units to balance the e-commerce load, ensuring that all users get the fastest response time. The systems are set up in an active standby configuration for hot standby redundancy and use TCP Intercept to prevent SYN attacks. HomeSide also uses Cisco LocalDirector's content verification system (CVS) to ensure that its e-commerce URLs are always available. "CVS works by monitoring servers for application availability, application health, and database connectivity. Then it directs traffic only to available applications," Robinson explains.

"We added the CVS system because of a problem we had with server failover. Since the Cisco LocalDirector doesn't actually poll the Web servers' pages to see if they're up or not, CVS gave us a diagnostic tool that automatically tests the page's availability and takes the server out of service after a predetermined time with no page response," notes Robinson. "The CVS server will continue to check availability, and if it receives a response to its query, then it can restore the server to the farm. This ensures no interruption on the customer's part."

In addition to the security built into the routers and PIX devices, HomeSide uses the Cisco Secure IDS to detect, report, and terminate unauthorized network activity. The system captures and analyzes packets, terminating connections that carry any of 250 intrusion signatures. When unauthorized activity traverses the network, the system responds by terminating the offending session and sending an alert back to a central management console.

On the Horizon

HomeSide's network security team plans to enhance its disaster recovery site in San Antonio, Texas. The new site will help HomeSide ensure that its e-commerce services are always available, even in the event of a catastrophe. Cisco LocalDirector will continue to be used for load balancing within data centers, while Cisco DistributedDirector will manage activities between data centers.

For now, however, the team members are pleased with the progress they have made and the positive business results. "Our main goal was to design a layered, totally redundant system that's capable of handling high traffic levels with minimal maintenance," remarks Spain. "After extensive research

Continued on page 99

Mobility for the Masses

The Mobile IP protocol enables cross-network data roaming with continuous connectivity.

Now that user mobility has become a business priority and wireless networks are getting faster, the Mobile IP protocol is starting to gain attention from enterprises and service providers alike.

Mobile IP—defined by Internet Engineering Task Force (IETF) RFC 2002—provides address resolution and tunneling capabilities so that users can securely roam within and outside their enterprise networks while maintaining their home IP addresses and nonstop network connections. For example, if users are strolling from one building to another on an enterprise campus or riding in a delivery vehicle, their sessions stay up when they cross network boundaries. Mobile IP saves users from having to continually request a new address as they move from one wireless coverage area to another.

"Mobile IP capabilities in routers allow users to seamlessly traverse multiple network segments," explains Mark Denny, IP product manager in Cisco's IOS® Technologies Division. "This kind of mobile networking represents significant productivity benefits for roaming LAN and Internet users."

Due to sharply growing volumes of mobile consumers, Mobile IP-enhanced networks hold great potential for stimulating mobile commerce, Denny adds, leading to new revenue streams for service providers.

Service Trends and Opportunities

Data-roaming services using proprietary network technologies have been deployed for many years in vertical markets such as trucking and field service. Now that standards have solidified around Internet protocols, Mobile IP can be used to deliver inexpensively a broad array of mobile networking services to both vertical and horizontal markets.

Mobile IP is enabling service providers to implement widespread data-roaming services at lower costs than has been previously possible, because they can achieve better economies of scale than they could by building proprietary wireless data networks on a per-customer basis. Instead, providers can now use off-the-shelf platforms that can also be managed in conjunction with the rest of their network elements.

Nextel Communications, for example, which has long run a nationwide data network used primarily for dispatch and trucking applications, now offers Nextel Online based on Mobile IP capabilities in Cisco routers. Nextel Online is basically a wireless Web service aimed at the horizontal Internet market, with several optional IP messaging, transaction, and dispatch services layered on top.

Wireless virtual private network (VPN) services for enterprises wishing to extend their wired VPNs are also becoming available on the market. In addition, wireless LAN services, deployed by third-party wireless network operators, are cropping up in public places such as airports and hotels. (See "Securing the Mobile Enterprise," page 13.)

Mobile IP resolves the IP addressing issues that arise when a user leaves a home connection. By doing so, it allows users to be continually connected to their home networks in an always-on manner—as if on a wired LAN or

Written by Joanie Wexler (joanie@jwexler.com), a contributing editor for Packet *magazine.*

dedicated private-line connection. Services that push messages and content to users can take advantage of always-on Mobile IP networks, opening the door for lucrative new services such as unified messaging. Under most business models, WAN usage charges for Mobile IP-based Internet services only accrue when data is actually transmitted, despite the fact that the connection is always on.

Mobile IP has been supported in Cisco routers since Cisco IOS Release 12.0(1)T. New activities under way using Cisco Mobile IP include the following:

- Bundling the protocol into Cisco's Aironet® 340 series wireless LAN access points to create a proxy agent for client devices. Access points are transceivers that function primarily as bridges between a wired Ethernet LAN and wireless LAN client devices. Mobile IP proxy agents in Aironet access points, expected this quarter, will prevent enterprises from having to load Mobile IP client software on each of their portable computing devices to leverage Mobile IP capabilities.
- Creating a Packet Data Serving Node (PDSN), a component to a wireless Code Division Multiple Access (CDMA) WAN. The PDSN serves as an access gateway to the Internet, intranets, and Wireless Application Protocol (WAP) servers in a CDMA2000 network. CDMA2000 is the third-generation ("3G") version of CDMA spread-spectrum mobile WAN technology, which will eventually support airlink speeds of up to 2 Mbps.

Components of a Mobile IP Network

Enterprise applications do not have to change in any way to leverage the benefits of Mobile IP. The protocol provides continuous and secure connections to mobile users through the use of three primary architectural components:

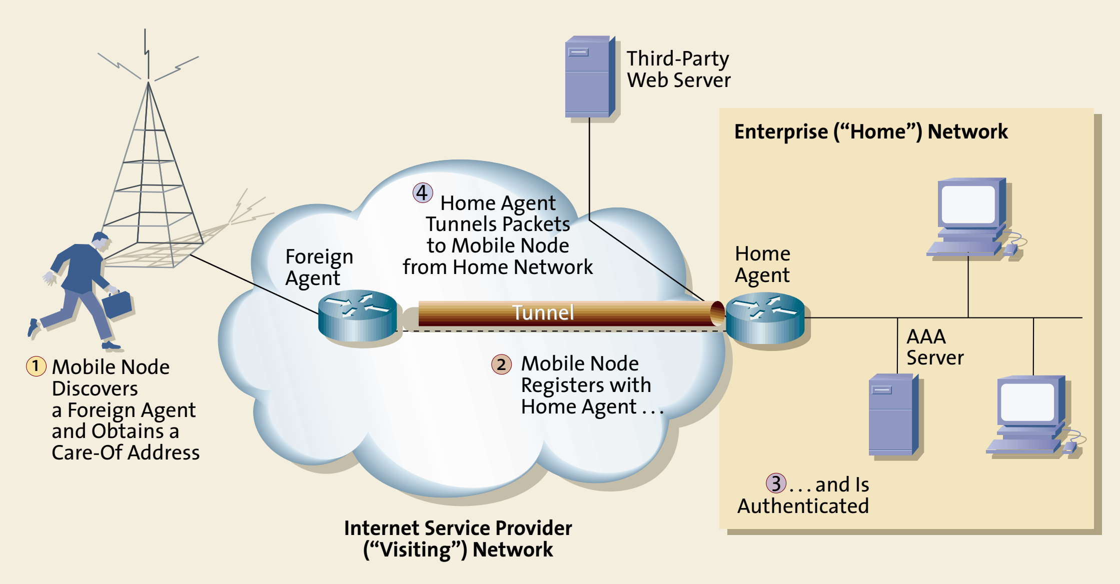
- A *mobile node*, which is an end user's mobile client device. The mobile node is also often called an "IP host."
- A *home agent*, which is a router on the user's home network running Mobile IP software. Home agents may be located within a service provider's network or within an enterprise network.
- A *foreign agent*, which is a router on the network being "visited" by a roaming mobile node. Foreign agents generally reside a single hop away from the user at the edge of a service provider's network. (Routers in the network core do not need to run Mobile IP.) A foreign agent can also be collocated in the mobile node, eliminating the need for them in the provider's network. When a mobile node is connected to its home network via a foreign agent, it uses a special Care-Of Address (COA).

The client device, or mobile node, registers with a home or foreign agent, depending on whether or not it is within coverage of its home network. The device is authenticated by the home agent, a temporary data tunnel is set up between the home agent and COA, and packets are forwarded to the mobile device via the tunnel. Tunneling to mobile nodes can be done using IP encapsulation within IP ("IP-in-IP"), a simple tunneling protocol specified in RFC 2003, or the Generic Routing Encapsulation (GRE) tunneling option in Cisco's Mobile IP software. GRE is specified as an Internet standard in IETF RFC 1701.

Mobile IP uses tunneling from the home agent to

NONSTOP NETWORKING: A combination of registration, authentication, and tunneling enhancements to the IP protocol allow transparent routing of IP datagrams to mobile users.

A BASIC MOBILE IP CONFIGURATION


Third-Party Web Server
Enterprise ("Home") Network
4 Home Agent Tunnels Packets to Mobile Node from Home Network
Foreign Agent
Home Agent
Tunnel
AAA Server
1 Mobile Node Discovers a Foreign Agent and Obtains a Care-Of Address
2 Mobile Node Registers with Home Agent . . .
3 . . . and Is Authenticated
Internet Service Provider ("Visiting") Network

the mobile node's COA, but rarely in the reverse direction, notes Michael DeLeo, Cisco Consulting Engineer. Usually, a mobile node sends its packets through a router on the foreign network and assumes that routing is independent of source address.

"When this assumption is not true, it is useful to establish a reverse tunnel from the COA to the home agent," DeLeo says. Backward-compatible extensions to Mobile IP have been defined by the IETF to support topologically correct reverse tunnels and are supported in Cisco's Mobile IP implementation.

How the Protocol Works

A mobile node determines whether it is on its home network by using extensions to the ICMP Router Discovery Protocol (IRDP), a protocol that uses router-advertisement and router-solicitation messages to discover the addresses of routers on directly attached subnetworks. Routers acting as home or foreign agents regularly advertise their existence. If a mobile node picks up its own home agent's advertisement, it knows it is on its home network and does not need to do anything special to receive its datagrams. If a mobile node receives an IRDP advertisement from another mobility agent, it will register its location via a foreign agent or directly with its home agent, which, in turn, authenticates the device.

The COA identifies the mobile node's current, topological point of attachment to the Internet and routes packets to the mobile node when it is attached to a different network. Mobile IP provides two alternative modes for acquiring a COA:

- The foreign agent provides a COA through its agent advertisement messages. In this case, the COA is the IP address of the foreign agent. The foreign agent is the endpoint of the tunnel and, upon receiving tunneled datagrams, decapsulates them and delivers the inner datagram to the mobile node.
- A collocated COA is acquired by the mobile node as a local IP address. The address may be dynamically acquired as a temporary address using Dynamic Host Control Protocol (DHCP) or may be owned by the mobile node as a long-term address for its use while visiting some foreign network. When using a collocated COA, the mobile node serves as the endpoint of the tunnel and decapsulates tunneled datagrams itself.

Unlike simple IP routing, the foreign agent has a Mobile IP routing table that remains local to the foreign agent router, so updates are not propagated in the traditional manner using routing protocols such as Open Shortest Path First (OSPF), points out DeLeo. "This setup prevents Mobile IP from generating extra network overhead," he notes.

Cisco Enhancements

Support for Mobile IP first became available in Cisco IOS Release 12.0(1)T. Platforms supporting Mobile IP include the Cisco 2500, 2600, 3600, 4000, 7200, and 7500 series routers, as well as the Catalyst 5000 and 6000 campus backbone switches. Cisco IOS platforms can be used as home agents, foreign agents, or both simultaneously.

Security

Cisco IOS software supports the mandatory and optional authentication parameters within Mobile IP: the mandatory mobile node-home agent authentication and the optional foreign agent-home agent and mobile node-foreign agent authentication procedures. These procedures are performed using keyed MD5 hashes, which cover all registration requests and replies. The registration requests and replies are all time-stamped to circumvent replay attacks, in which a hacker might sniff a registration packet and reuse it to gain access to network resources. Because large numbers of mobile devices could make the number of keys required to perform authentication very large, Cisco IOS software allows the mobility keys to be stored on an authentication, authorization, and accounting (AAA) server that can be accessed using TACACS+ or RADIUS protocols. Mobile IP in Cisco IOS software also contains registration filters, enabling companies to restrict who is allowed to register.

Continued on page 95

FURTHER READING

For more information on Mobile IP, visit the following URLs:

- Cisco Mobile IP Features and Configuration Commands:
  cisco.com/univercd/cc/td/doc/product/sofware/ios120/120newft/120t/120t1/mobileip.htm
- Mobile IP Home Agent Redundancy:
  cisco.com/univercd/cc/td/doc/product/sofware/ios120/120newft/120t/120t2/haredun.htm
- Configuring Mobile IP:
  cisco.com/univercd/cc/td/doc/product/sofware/ios121/121cgcr/ip_c/ipcprt1/1cdmobip.htm
- IETF Information on Mobile IP:
  ietf.org/html.charters/mobileip-charter.html
  ietf.cnri.reston.va.us/ids.by.wg/mobileip.html
  ietf.org/rfc/rfc2344.txt

Technology, Continued from page 87

Availability and redundancy

Enterprises and service providers can build redundancy and load-balancing capabilities into Mobile IP networks by configuring redundant home agent routers with Hot Standby Routing Protocol (HSRP). HSRP ensures that user traffic will immediately and transparently recover from first-hop failures in network edge devices or access circuits. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router. This way, one router can transparently assume the routing responsibility of another, if needed. HSRP for home agent redundancy and load-balancing was added in Cisco IOS Release 12.0(2)T.

◆ ◆ ◆

As portable computing devices become smarter, smaller, and more efficient, mobile users are coming to expect boundless data networking capabilities that parallel what they have grown accustomed to with cellular voice communications. In addition, they want to gain access to their enterprise networks and the Internet in the same way regardless of where they are physically located. Mobile IP enables this transparent, nonstop networking, and as such, is a pivotal component of the technology mix for this new networking paradigm. ▲▲

Technically Speaking

Who Goes There?

Questing for the Holy Grail of User Authentication

BY JEREMY STIEGLITZ

“None shall pass.” When networks were private, access from public sources simply did not exist. But in today’s increasingly open world of extranets, virtual private networks (VPNs), remote and mobile users, blocking access to all—like Monty Python’s Black Knight—is simply unworkable. Fortunately, new technologies have emerged to help network managers identify, authenticate, and verify users and their access privileges. But which technology is right for you?

Answer me these questions three

There are three different factors of authentication, commonly known as the “three Ws,” at your disposal. They are: *what you know, what you have, and who you are.*

What do you know?

The *what you know* authentication method typically requires the user to supply a personal identification number (PIN) or password. This method is the easiest to deploy, scales well, and is least expensive. It’s also the least secure because passwords can be stolen, guessed, given away, or written down.

What do you have?

What you have refers to a unique physical or electronic possession, such as a smart card or one-time token (OTT). Cisco identifies its remote workers with one-time passwords. Employees who travel or work from home use a software program that generates a continually changing authentication code used to access the network. *What you have* methods are easy to deploy and are generally considered more secure than passwords. But they are also more expensive.

Who are you?

Who you are identification, also called biometrics, binds the user’s identity to a fingerprint, voiceprint, eyeprint, or other distinguishing physical characteristic. Biometrics provide a high degree of security but equally high infrastructure and deployment costs. Most enterprises lack the equipment and systems to record, measure, and respond to biometric inputs. At Cisco, we evaluate network technologies based on how effortlessly they scale. By this measure, biometrics probably won’t be adopted in any but the most secure networks for quite some time.

One, two, five

When it comes to identity, one plus one does not equal two. Two-factor identification, the technique of using two different identity methods per user, provides substantially more security than either one method alone.

Public key infrastructure (PKI) is a popular example of two-factor identification, requiring users to prove their identity via well-known PIN and password systems, as well as with public key credentials. Companies that adopt PKI designate a trusted organization, called a certificate authority (CA) to issue digital certificates to network users. PKI is appealing because it scales well, is cost effective, and works for a wide range of enterprise applications.

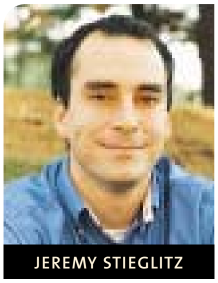
Cisco supports PKIs in its complete line of VPN products, including VPN 3000 and 5000 remote access solutions, Cisco Secure PIX™ Firewalls, and the full line of Cisco IOS® routers.

Ere the other side he see

Before users gain access, the network must evaluate the information that’s been collected. Validating the user’s identification is the job of an access control server (ACS), such as the Cisco Secure Access Control Server for Windows 2000 and NT, and Cisco’s Access Registrar solutions.

You have to know these things when you’re king

The more you know where you’re network is heading, the better you’ll be able to plan your identification strategy. As you open more doors to more users, you’ll need an identity method that scales well and is cost effective. Given the expense required to create an infrastructure for biometrics, a good compromise is two-factor identification: a combination of digital signatures and passwords. Companies that adopt a PKI can do so with minimal expense and protect their kingdom much more effectively than they could with passwords alone. ▲▲


JEREMY STIEGLITZ

JEREMY STIEGLITZ is Product Line Manager for Identity at Cisco Systems. He can be reached at jeremys@cisco.com. Ask him anything you like. Just make sure you bring two forms of identification.

PHOTO BY JOHN LAWLER

New Product Dispatches

Network and Enterprise Core

Cisco Secure PIX 535 Firewall

The Cisco Secure PIX™ 535 Firewall is a high-performance, dedicated firewall appliance designed for large enterprise and service provider environments. The PIX 535 supports 500,000 concurrent connections, unprecedented 1.0-plus Gbps throughput, and Triple DES encryption at 100 Mbps. The PIX 535 Firewall is covered in greater detail on page 75.
cisco.com/go/pix

Cisco Secure IDS 4210 Sensor

A new member of the Cisco Secure intrusion detection system (IDS) product family, the Cisco Secure IDS 4210 sensor is a network security appliance that detects unauthorized activity traversing the network, such as hacker attacks, by analyzing traffic in real time. The IDS 4210 sensor is optimized to monitor 45-Mbps environments and is ideally suited to monitor multiple T1/E1, T3, and Ethernet environments. Simple to install, configure, and maintain the Cisco Secure IDS 4210 sensor is a turnkey, plug-and-play solution.
cisco.com/go/ids

Cisco Secure Policy Manager Version 2.2

Cisco Secure Policy Manager (CSPM) version 2.2 is a scalable, policy-based security management system for Cisco firewalls, IP Security (IPsec) virtual private network (VPN) routers, and IDS solutions. With CSPM, network administrators can define, distribute, enforce, and audit network-wide security policies from a central location.
cisco.com/go/policymanager

Catalyst 6000 IDS Module

The Catalyst® 6000 IDS module is the first in the industry to integrate intrusion detection capabilities directly into the switch backplane. This new module monitors more than 100 Mbps of traffic at approximately 47,000 packets per second (average packet size of 484 bytes), with an arrival rate of 1000 new flows per second. The Catalyst 6000 IDS module is covered in greater detail on page 61.
cisco.com/go/ids

Device Fault Manager Bundle and Add-On for CiscoWorks2000

The recently announced Device Fault Manager (DFM) is now available in a new promotional bundle with the LAN management and routed WAN management solutions, or as an add-on to existing CiscoWorks2000 solutions. DFM provides real-time, detailed fault analysis at the device and virtual LAN (VLAN) levels. When a problem occurs, DFM sends intelligent Cisco traps to an alarm window, a choice of system displays, or an e-mail or pager gateway. DFM supports more than 100 of the most commonly deployed Cisco routers, switches, access servers, and hubs in networks with up to 30,000 Cisco ports.
cisco.com/warp/public/cc/pd/wr2k/dvftmn

Cisco QoS Policy Manager Version 2.0

The Cisco QoS Policy Manager (QPM) version 2.0 provides network managers with new quality-of-service policy management capabilities that make large-scale QoS deployments easier and more reliable. With QPM 2.0, network managers also have greater service-level control for converged data, voice, and video networks and support for several new devices and device software that allow QoS management for a variety of network infrastructures. Cisco QPM version 2.0 also includes a range of features that enable network managers to quickly and easily configure QoS for voice over IP on networks built upon the Cisco Architecture for Voice, Video and Integrated Data (AVVID).
cisco.com/warp/public/cc/pd/wr2k/qoppmn

Cisco 7200VXR NPE-400 Network Processing Engine

To support a variety of applications, bandwidth, and performance requirements, the Cisco 7200 series routers offer a choice of network processors. The new NPE-400 designed for the Cisco 7200VXR router provides processing power of up to 400,000 packets per second—a 33 percent increase over previous processing capability—and high throughput with a 350 MHz processor, 4 MB Layer 3 cache, and up to 32-MB packet memory. The processor is modular to enable upgrades of existing Cisco 7200VXR chassis as well as to simplify future upgrades.

cisco.com/warp/public/cc/pd/ifaa/prossor/prodlit/npe_ds.htm

Cisco Secure Access Control Server for Windows 2000 and NT

The Cisco Secure Access Control Server (ACS) 2000 software supports scalable, centralized access control and accounting for Cisco dialup access servers and firewalls used in virtual private networks (VPNs) and voice-over-IP applications. The ACS2000 software can be installed on a server running Microsoft Windows 2000 or Windows NT. Network administrators can use Cisco Secure ACS2000 to manage user accounts quickly and globally change security levels and network policies for user groups, improving the ability to deploy and scale remote-access services.

cisco.com/go/acs

Catalyst 6000 Family Modules

Several new hardware components are now available for Catalyst 6000 family switches. The new products include the Supervisor Engine 2 module with a multilayer switch feature card that enables Cisco Express Forwarding (CEF) technology; a 16-port Gigabit Ethernet module with dual-fabric interface and distributed forwarding functionality; a 16-port Gigabit Ethernet module with a single fabric-channel interface capable of supporting distributed forwarding; a crossbar switching fabric module; and a daughter card that implements distributed forwarding functionality.

cisco.com/go/catalyst6000

Cisco Metro 1500 Series DWDM Platform: 850 nm Clocked WDM Channel Module

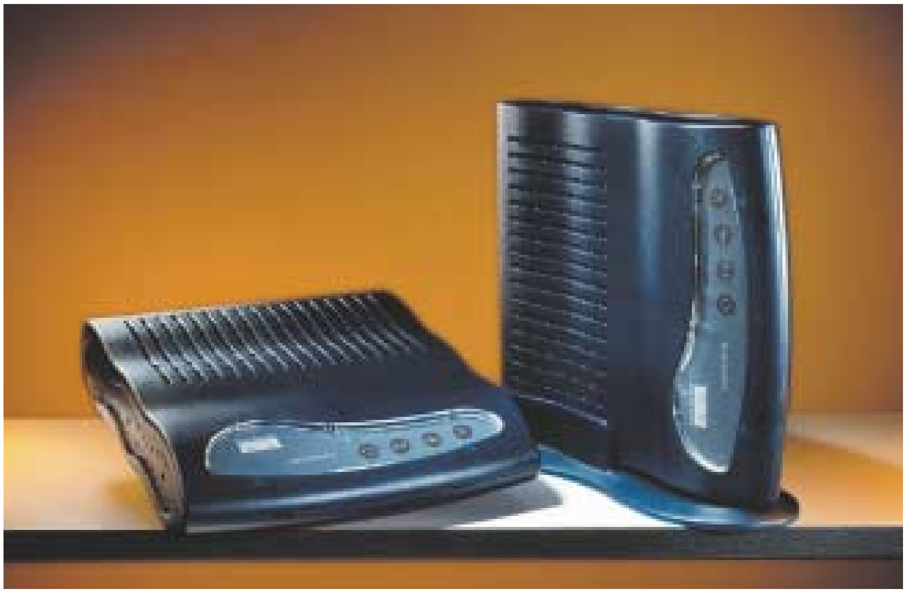
With the introduction of the 850 nanometer clocked wavelength-division multiplexing (WDM) channel module, the Cisco Metro 1500 series dense wavelength-division multiplexing (DWDM) platform now supports low-cost Gigabit Ethernet and Fibre Channel multimode optical interfaces. This support provides a cost-effective solution for applications such as Gigabit Ethernet aggregation and transport, and Fibre Channel-based storage-area networking (SAN) or network-attached storage (NAS). For more about SANs, see related article on page 21.

cisco.com/warp/public/cc/pd/si/me1500

Central Office and Point of Presence

Cisco VPN 5000 Concentrator Series

The Cisco virtual private network (VPN) 5000 concentrator series provides carrier-class solutions for delivering remote-access and site-to-site IP Security (IPsec) VPNs and tunneling mapping services. The new Cisco 5002 (two slots) and Cisco 5008 (eight slots) are modular platforms for the



service providers' network edge that support differentiated VPN services with up to 256 customer virtual contexts (CVCs) per platform. Each CVC provides separate Interior Gateway Protocol (IGP) routing, user authentication and accounting servers, VPN groups, filter sets, and tunnel mappings. The Cisco 5008 concentrator can scale up to 40,000 simultaneous remote-access or site-to-site VPN tunnels, with 760-Mbps Triple DES throughput. In addition, a broad set of IPsec clients are included with the Cisco VPN 5000 concentrator series to facilitate remote access. The Cisco VPN 5001 complements service rollouts as a remote site access device.

cisco.com/warp/public/cc/pd/hb/vp5000/

Cisco 10000 ESR Modules

Two new modules enhance the Cisco 10000 Edge Services Router (ESR) as a solution for Internet service providers worldwide. The single-port, OC-12 ATM interface line card provides performance and density to scale networks efficiently with wire-rate 622-Mbps SONET/SDH Layer 2 connectivity across ATM networks. The four-port, channelized STM-1 interface module supports DS0 and E1 connections on a quad-OC-3 interface to support high-density leased-line services.

cisco.com/warp/public/779/servpro/solutions/aggregation/technical.html

Small and Midsized Businesses, Branch Offices, and Home Offices

Cisco 8110 Broadband Network Termination Unit

The new Cisco 8110 broadband network termination unit is a multiservice access device for IP and ATM networks. It enables delivery of carrier-class managed services cost effectively to enterprises that demand high bandwidth and stringent service-level agreements (SLAs). Previously sold by HyNEX as the HUNT 7100, the Cisco 8110 broadband network termination unit functions as a managed services gateway for a wide range of private line, voice, and video services over a single high-speed ATM link.

cisco.com/warp/public/cc/pd/si/8110/tech/index.shtml

Cisco CVA120 Series Cable Voice Adapters

The Cisco CVA120 series cable voice adapters provide cable modem functionality for accessing voice and high-speed data services over IP-based cable networks. The Cisco CVA120 series integrates communications to support home-office users simply and reliably. Serving as a primary- or second-line voice-over-cable access device, the Cisco CVA120 series offers four voice ports to connect telephones and fax machines. Separate product versions implement the Data-over-Cable Service Interface Specifications (DOCSIS) and EuroDOCSIS standards for data communications.

cisco.com/cable

Cisco 2600 and 3600 Series Routers: VPN Modules

New virtual private network (VPN) modules for the Cisco 2600 and 3600 modular multiservice series routers offload encryption

Continued on page 95

New Products, Continued from page 93

processing from the router CPU for up to ten times greater performance compared to software-only encryption. These VPN modules provide functions for IP Security (IPsec) encryption, application-aware quality of service (QoS) and bandwidth management, and robust perimeter security options. The VPN modules also handle a variety of other IPsec-related tasks—hashing, key exchange, and storage of security associations—freeing the main processor and memory to perform other routing, voice, firewall, and intrusion-detection functions.

cisco.com/warp/public/cc/pd/rt/2600/prodlit/kaos_ds.htm

Cisco SOHO 77 ADSL Router

The Cisco SOHO 77 asymmetric Digital Subscriber Line (ADSL) router gives small-office/home-office (SOHO) users affordable, secure Internet access for multiple users over a single DSL line. The new Cisco SOHO 77 router reduces DSL deployment costs for service providers with a plug-and-play design and a Web-based configuration tool for simple setup.

cisco.com/go/soho70

ADSL WAN Interface Card for Cisco 1700, 2600, and 3600 Series Routers

The new single-port Cisco ADSL WAN interface card enables users to take advantage of the high speed and low cost of ADSL instead of expensive T1 leased lines. Depending on loop length, the ADSL WAN interface card delivers downstream speeds up to 4 Mbps and enables concurrent user sessions on up to 50 virtual circuits. The interface card is available now for Cisco 1700 series routers, with versions planned in the first calendar quarter of 2001 for Cisco 2600 and 3600 modular multiservice series routers.

cisco.com/warp/public/146/kits/smb/dsl_strategy/ADSL_WIC_ds.pdf

ABOUT NEW PRODUCT DISPATCHES

Keeping up with Cisco's myriad new products can be a challenge. To help readers stay informed, *Packet*™ magazine's "New Product Dispatches" provide snapshots of the latest products released by Cisco between October 2000 and January 2001. For real-time announcements of the most recently released products, check the "What's New" section of Cisco's Web site at cisco.com/warp/public/6/.

Equant, Continued from page 49

quality voice, which enables Equant to deliver on its commitment to maintain application performance of time-critical traffic.

As more corporations become global in nature, having end-to-end services that slash the cost of international telephone calls such as iVAD for Intranet Connect—and are managed cohesively to ensure consistent network service quality—will likely become increasingly important to customers. Equant has stepped up to the plate to position its existing and future customers for such capabilities, and in doing so, has raised the competitive bar for service providers around the globe. ▲▲

Written by Joanie Wexler (joanie@jwexler.com), a contributing editor for Packet *magazine.*

Technology, Continued from page 87

Availability and Redundancy

Enterprises and service providers can build redundancy and load-balancing capabilities into Mobile IP networks by configuring redundant home agent routers with Hot Standby Routing Protocol (HSRP). HSRP ensures that user traffic will immediately and transparently recover from first-hop failures in network edge devices or access circuits.

By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router. This way, one router can transparently assume the routing responsibility of another, if needed. HSRP for home agent redundancy and load-balancing was added in Cisco IOS Release 12.0(2)T.

As portable computing devices become smarter, smaller, and more efficient, mobile users are coming to expect boundless data networking capabilities that parallel what they have grown accustomed to with cellular voice communications. In addition, they want to gain access to their enterprise networks and the Internet in the same way regardless of where they are physically located. Mobile IP enables this transparent, nonstop networking, and as such, is a pivotal component of the technology mix for this new networking paradigm. ▲▲

Standards Updates

Reservations, Guaranteed

RSVP-related specifications move ahead.

In the last few months of 2000, a number of Cisco-supported specifications were approved as standards-track protocols by the Internet Engineering Task Force (IETF). Among the proposed standards are RFC 2997 ("Specification of the Null Service Type") and RFC 3006 ("Integrated Services in the Presence of Compressible Flows")—both relate to running Resource Reservation Protocol (RSVP) within an Integrated Services (Int-Serv) architecture. RSVP is a signaling protocol that can be used within the Int-Serv architecture but isn't a required part of it.

Null Service and Int-Serv

Co-authored by Cisco Fellow Bruce Davie, RFC 2997 specifies the role of the Null Service in an RSVP/Int-Serv model. In a typical model, applications request an Int-Serv service type and quantify the resources required for that service. With the Null Service, applications that don't have readily quantifiable resource requirements can identify themselves to network quality of service (QoS) policy agents, using RSVP signaling. Such RSVP usage is particularly applicable in networks that combine Differentiated Services (Diff-Serv) QoS mechanisms with RSVP signaling.

For example, explains Davie, a mission-critical data application, such as enterprise resource planning (ERP), would send an RSVP message into the network where a policy server determines the appropriate Diff-Serv class of service and tells the application how to mark the traffic for the right QoS.

Compressing Apps within Int-Serv

Co-authored by Davie, Cisco Fellow Dave Oran, and Cisco Technical Lead Carol Iturralde, RFC 3006 describes how to make appropriate reservations for applications whose data can be compressed. In this approach, senders of compressible data can provide hints to Int-Serv routers about the compressibility they may obtain. Routers that support appropriate compression take advantage of the hint in their admission control decisions and resource allocation procedures. Other routers ignore the hint.

A typical scenario for this RFC, explains Davie, is a voice-over-IP application that may have its packets compressed using Compression for Real-Time Protocol (CRTP). More calls can be admitted into a link of given bandwidth if the calls are compressed, and RFC 3006 extends the Int-Serv architecture to handle this situation. Doing so ensures that the appropriate number of compressed calls are admitted while excess calls—which would overload the link and possibly degrade service for all voice-over-IP traffic—are rejected.▲▲

FURTHER READING

For more information on the RFCs and topics mentioned in this article, visit the following URLs:

- Full text of RFC 2997, "Specification of the Null Service Type":
  ietf.org/rfc/rfc2997.txt
- Full text of RFC 3006, "Integrated Services in the Presence of Compressible Flows":
  ietf.org/rfc/rfc3006.txt
- Full text of RFC 2998, "A Framework for Integrated Services Operation over Diff-Serv Networks":
  ietf.org/rfc/rfc2998.txt
- IETF RSVP working group:
  ietf.org/html.charters/rsvp-charter.html
- "Implementing QoS for Packet Telephony" by Bruce Davie (*Packet* Second Quarter 2000):
  cisco.com/warp/public/784/packet/aproo/technology.html#title

Defensive Attitude, Continued from page 73

here, it's always good practice to keep server operating system and application software current with the latest updates and patches. Another good strategy is to know the enemy by visiting Web sites frequented by hackers and security-minded professionals.

As with physical security, vigilance and diligence are required to protect what's precious on the network to keep an organization safe and running smoothly. ▲▲

FURTHER READING

To learn more about the topics discussed in this article, visit *Packet Online* at: cisco.com/go/packet/defensive

- **Cisco Secure Consulting Services (CSCS)**
- **CSCS *Vulnerability Statistics Report***
- **Cisco Product Security Incident Response Team (PSIRT)**
- **"The 2000 Information Security Survey," Information Security magazine, September 2000**
- **RFC 2827 Network Ingress Filtering: Defeating DoS Attacks which employ IP Source Address Spoofing**
- **RFC 2196 Site Security Handbook**

HomeSide Lending, Continued from page 83

and analysis, we selected Cisco for its security, performance, redundancy, and ease of administration. And we learned one other important thing along the way: in addition to great products, Cisco has an outstanding organization backing up our needs."

The network security team credits Cisco's high-quality documentation for enabling them to understand the bounds of what's possible, as well as for guidance with the design, testing, and installation of the security system. "Coupled with a high level of expertise by the HomeSide team, each one of our criterion was accomplished before our deadline," Spain says. "We put a lot of effort into ensuring that our design was theoretically sound. The Cisco white papers were a big help as well as the help provided by the Cisco support organization, which was instrumental in assisting us over a few minor hurdles."

PACKET ADVERTISER INDEX

ADVERTISER	URL	PAGE
ADC Telecommunications	www.adc.com	24
ADTRAN	www.adtran.com	12
American Power Conversion (APC)	www.apcc.com	9
Aperian	www.aperian.com	60
Apogee Networks, Inc.	www.apogeenetworks.com	48
Ascolta Training Company	www.ascolta.com	80
BellSouth Business	www.biz.bellsouth.net	36
Cable & Wireless	www.gettheconnection.com	64
Canary Communications	www.canarycom.com	28
Cisco Press	www.ciscopress.com	B, 74
Colorado Computer Training Institute (CCTI)	www.ccti.com	F
Counterpane Internet Security	www.counterpane.com	A
CRYPTOCard	www.cryptocard.com	88
Global Knowledge	am.globalknowledge.com	IFC
Globix	www.globix.com	58
Horizon-MTS	www.horizon-mts.com	4
Infonet	www.infonet.com	Back Cover
Integrated Research	www.ir.com	19
KnowledgeNet	www.knowledgenet.com	2
Mentor Technologies	www.mentortech.com	6, 42
Mind CTI	www.mindcti.com	44
NetOptics	www.netoptics.com	90
netViz	www.netviz.com	82
Panduit	www.panduit.com	IBC
Perform	www.networkqos.com	94
Platform Computing	www.siteassure.com	20
Qwest	www.qwest.com	16, 17
ReadyRouter.com	www.readyrouter.com	D
Skyline Computer Corporation	www.skylinecomputer.com	32
Stardust.com	www.stardust.com	84
SUPPORTmart	www.supportmart.com	96
SurfControl	www.surfcontrol.com	11
Websense	www.websense.com	52
Xacct Technologies	www.xacct.com	40

On Line All the Time

Despite the technical depth and sophistication of HomeSide's Internet security architecture, the team completed all facets of the implementation in four months—three of which were spent in research, design, and planning. The actual deployment and configuration of the equipment took only one month.

With its Internet security architecture fully operational, HomeSide is experiencing faster throughput for all network activities. Spain says the biggest benefit of the end-to-end Cisco solution is its inherent integration and compatibility. "Using Cisco equipment for all of these tasks simplifies configuration, maintenance, and troubleshooting," concludes Spain. "This is a definite advantage when you're running an Internet system that processes and protects sensitive information." ▲▲

Cache File

SNIPPETS OF WISDOM FROM OUT ON THE 'NET

Bridging the Digital Divide

In its October 2000 digital technology status report, the US National Telecommunications and Information Administration (NTIA) found that while Americans are moving rapidly toward full digital inclusion, a digital divide still persists along economic, racial, and educational lines. According to the NTIA report, the share of US households with Internet access climbed from 26.2 percent in December 1998 to 41.5 percent in August 2000. However, the numbers are disproportionately higher among white, higher-income, dual-parent households. To view the full NTIA report, "Falling Through the Net: Toward Digital Inclusion," in .PDF format, go to www.esa.doc.gov/fttn00.pdf.

All the Hack News Fit to Print

From worst virus nightmares to hacker-and-cracker activity reported around the world, the Hacker News Network proffers "real news from the computer underground for the computer underground." For a no-nonsense look at hacker-news-worthy topics, features, and editorials, check out the URL hackernews.com.

Calling on the Internet

Internet-ready cell phones are booming in the US retail arena, according to marketing information firm NPD Intelect. In the second calendar quarter of 2000, 48 percent of cell phones purchased at retail stores were Internet-ready—a near tenfold increase over the same period in 1999. Find out more at intelectmt.com/corp/intelectmt/press/press_000802.htm.

HELLO? HELLO?

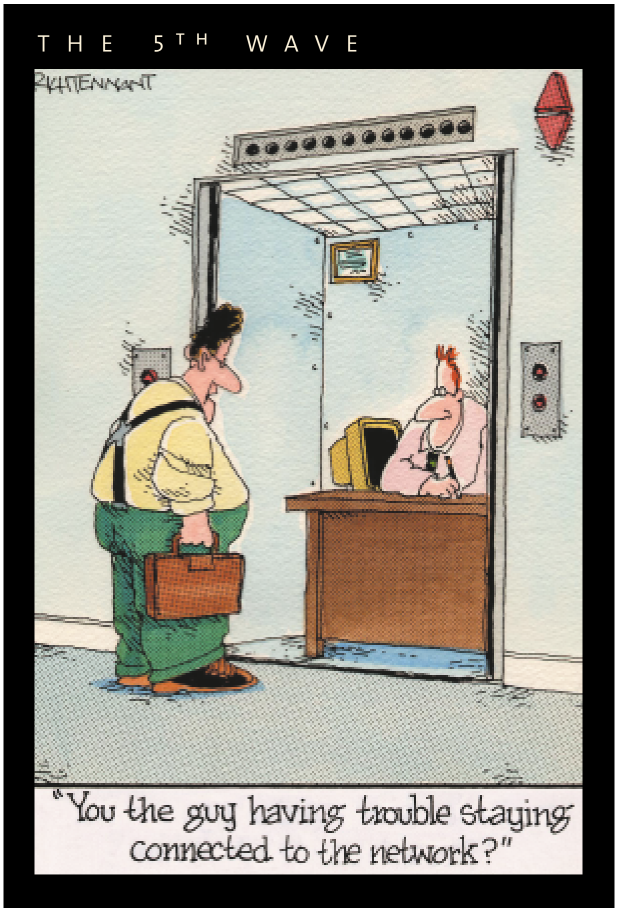
Laganoia—the fear, engendered by network lag, of being ignored, shunned, or left behind. The condition can be triggered by delayed e-mail replies, dead spots in Internet telephony interactions, or out-of-order Usenet posts.

SPAM COLLECTOR

An outfit called Tinaa Technologies offers users a free holding place for suspected spam. When users sign up for a service on the Web that requires an e-mail address—and they suspect that providing one will subject them to spam—they can use the address spam@tinaa.com instead. Tinaa Technologies archives all incoming e-mail on the site's Web server for users to retrieve. To find out more and select your Tinaa access code, visit the URL www.tinaa.com/spam.

Lava Lamp App

Inspired by "The Coming Age of Calm Technology" at the URL www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm, John Heidemann has written an application called LavaPS, which offers a restful, nonintrusive way to monitor what's happening on Linux or FreeBSD systems. Important attributes of system processes are mapped to the size, speed, color, and luminance of dynamic blobs in a window. Blob size is proportional to memory usage, and movement is proportional to CPU usage. Color is a combination of program name and time since the program last ran. The application, which is available at the URL www.isi.edu/~johnh/SOFTWARE/LAVAPS/index.html, strongly resembles the shapes and calming movement of novelty lava lamps.


THE 5TH WAVE
RICHTENNANT
"You the guy having trouble staying connected to the network?"

©The 5th Wave, www.the5thwave.com

Reprinted with permission from *Packet*™ magazine (Volume 13, No. 1), copyright © 2001 by Cisco Systems, Inc. All rights reserved.

Some "Cache File" items based on Keith Dawson's "Tasty Bits from the Technology Front" at tbtf.com.