Firewall Security

A Must-Have for Securing Corporate Information and Web Access

With the Cisco PIX Firewall, security begins with a process that removes the source IP address from outgoing traffic and replaces it with a generic IP address. This process protects the internal network, because no direct route back to the source is provided.

Increasingly, companies with a World Wide Web presence are implementing packet-filtering routers to prevent millions of Internet users from perusing their sensitive information resources. This first-level barrier is necessary—but as the criticality of Web-based transactions increases, so too does the need for heightened security.

What is needed in this environment is a robust, dedicated firewall appliance that complements the packet filters of routers. This appliance should extend the security of the router's filtering from the network layer all the way to the application layer, while taking no toll on Web site performance or usability for internal Web users.

While some firewall products may provide the required security, only one—the Cisco Private Internet Exchange (PIX™) Firewall—also meets the performance and support requirements of today's enterprise-wide, business-critical Web connections. The Cisco PIX Firewall provides strong security while operating at speeds that are dramatically faster than any other firewall on the market. And it comes from a company with over a decade of experience in network security: over 80 percent of the Internet backbone routers come from Cisco Systems.

The Cisco PIX Firewall is far more capable of handling dramatically larger networks than multiple smaller firewall products that consume bandwidth and create operating overhead. A single PIX Firewall device can support over 16,000 multiple sessions, or more than 64,000 users without impacting end-user performance. This capability makes the PIX Firewall well-suited for the high-speed (DS3 and E3) connections that Internet service providers require.

Using "stateful" security, the PIX Firewall keeps track of source and destination ports and addresses, Transmission Control Protocol (TCP) sequences, and additional TCP flags. Like telephone calls, *stateful* connections provide details that are tracked and recorded. This stateful security provides strong authentication, verification, and auditing capabilities.

With the Cisco PIX Firewall, security begins with stateful dynamic address allocation, a process that removes the source IP address from outgoing traffic and replaces it with a generic IP address. This process protects the internal network from unauthorized access, because all that's revealed is the firewall address, so no direct route back to the source is provided. This feature is comparable to having telephone service with an unlisted telephone number.

Dynamic address allocation, while secure, is not port-specific and relies on a simple configuration table to track removed addresses. As a result, it does not provide absolute security because a spoofer could, theoretically, initiate a packet from outside the network that travels with a signal coming back through the configuration table; thus the spoofer could obtain all addresses.

To remove this potential weakness of dynamic address allocation, Cisco PIX

re: Part of an End-to-End Solution

Cisco Systems' expertise in security and the Internet allows customers to develop single-vendor security solutions using Cisco's complete portfolio of packet-filtering routers, switching products, and software as well as the Cisco PIX Firewall. This single-vendor approach gives users streamlined purchasing, support, and maintenance.

Firewalls also offer an adaptive security capability that captures the TCP sequence numbers and port numbers of originating TCP/IP connections. In order for spoofers to penetrate the firewall to reach an end server, they would need not only the IP address, but the port number and TCP sequence numbers, too.

To minimize the possibility of unauthorized network penetration, the Cisco PIX Firewall also supports sequence number randomization, a process that prevents potential IP address spoofing attacks, as described in a Security Advisory (CA-95:01) from the Computer Emergency Response Team (CERT). Essentially, this advisory proposes to randomize TCP sequence numbers in order to prevent spoofers from deciphering these numbers and then hijacking sessions. By using a randomizing algorithm to generate TCP sequence numbers, the PIX Firewall makes this spoofing process extremely difficult, if not impossible. In fact, the only accesses that can occur through the Cisco PIX Firewall are those made from designated servers, which network administrators configure with a dedicated conduit through the firewall to a specific server—and that server alone. The PIX Firewall tracks all of these connections using syslog, the standard UNIX logging mechanism, to provide detailed audit trails.

The PIX Firewall is interoperable with any router-based network topology to ensure standards-based interoperability in multivendor environments. In a typical installation, its local port is connected to the private network, while the global port connects the PIX Firewall to the isolation segment where the Internet router resides.

Continued on next page

re: How the Cisco PIX Firewall Works

In operation, the Cisco PIX Firewall works as follows: an Internet-bound packet sent by a host on the inside network follows default routes to the inside interface of the PIX Firewall. Upon receipt of the outbound packet, the source address is extracted and compared to an internal table of existing translations. If the inside host's address does not appear in the translation table, a new entry is created for that host, assigning a globally unique IP number from the pool of available addresses.

The actual translation is accomplished by changing the source address of the packet to this "legal" address. The differences between the original and translated versions of the packet are known, so the checksums are efficiently updated with a simple adjustment rather than complete recalculation. After a user-configurable timeout period during which there have been no translated packets for a particular address-mapping, PIX Firewall removes the entry, freeing the global address for use by another inside host.

This dynamic address allocation is enabled only for connections initiated from the internal network and is port-specific. The translation for an outbound Hypertext Transfer Protocol (HTTP) connection from a Web client, for example, would forward only packets from the external Web server that were destined for port 80 of the client machine. In the case of File Transfer Protocol (FTP) connections, which use a dynamic port for data connection, PIX Firewall notes the port number passively opened by the client's request and only allows inbound FTP data for sessions that were initiated from inside the private network.

This high level of selectivity is enabled by retaining state information for each TCP connection established through the PIX Firewall. A table containing the destination address, port numbers, sequencing information, byte counts, and internal flags for each TCP connection associated with a particular host address translation is maintained for the life of the translation entry. PIX Firewall then compares inbound packets against entries in the connection table and permits their entry only if an appropriate connection exists to validate their passage.

By operating on packet headers, rather than by copying data between processes (as is done in typical proxy servers that run at the user level on a multiuser operating system), the PIX Firewall provides the stateful security of a proxy server without the associated network and administrative overhead or the need for special host or client software.

PIX Firewall, *Continued*

Cisco is currently shipping an Ethernet (10/100 Mbps) version of the product and in September will also offer a Token Ring card, as well as an enhanced-performance version of the Ethernet card. Cisco's PIX Firewall comes in a standard 19-inch rack-mountable package.

Network administrators can configure PIX Firewall in less than five minutes, using five commands. A new, hypertext markup language (HTML) graphical user interface, available during the fourth quarter of 1996, will further simplify the PIX Firewall installation process.

As businesses increasingly rely on the World Wide Web for business-critical transactions, they must protect the integrity of those transactions, as well as their own internal information resources. A robust firewall meets this requirement while leveraging existing security barriers. With Cisco PIX Firewall, router investments are protected; the appliance simply adds a security layer that empowers users to protect valuable information assets.

Cisco PIX Firewall and Network Address Translation Solutions

In 1995, Cisco Systems acquired Network Translation, Inc. (NTI), an early pioneer in network address translation (NAT) and stateful adaptive security. NTI introduced the PIX Firewall product in late 1994—the first firewall to use stateful NAT, a strong security mechanism. In addition to its security capabilities, users can take advantage of another PIX Firewall benefit: support for larger address classes than those assigned by the Internet Assigned Numbers Authority (IANA). By translating bogus addresses into legal IP addresses, NAT makes it possible to use existing legitimate or illegitimate IP addresses to access the Internet. This capability saves users significant time and money by avoiding the need to reconfigure their networks.

Cisco offers two options for NAT support: the PIX Firewall standalone unit and integrated stateful NAT functionality in the Cisco Internetwork Operating System (Cisco IOS™) software on Cisco routers. Offered as a separately priced option to the Cisco IOS, the integrated router solution allows network managers to introduce NAT functionality without adding a new hardware element to a network topology.

questions & answers

How can I build a firewall with my Cisco router?

Complementing the Cisco PIX™ Firewall, the Cisco Internetwork Operating System (Cisco IOS™) software, too, can be configured as a potent firewall. You can combine extended IP access lists for packet filtering, several methods of user authentication, and Cisco's Lock and Key security solution to provide a strong, secure perimeter between "trusted" and "untrusted" networks.

The router can be configured to log security violations to a UNIX host's syslog facility. In Release 11.2 of Cisco IOS™ software, network managers can enable IP network-layer encryption and Network Address Translation (NAT) capability (a separately priced software option) in their router-based firewalls.

For more information on Cisco IOS security solutions, visit the URL http://www.cisco.com/warp/public/732/Security/index.html.

What other configuration options should I enable on the router to secure my network?

Some additional options and the commands that will help protect the router from unauthorized access include:

- Disable proxy arp: **no ip proxy-arp**
- Disable IP source routing: **no ip source-route**
- Enable only required applications, such as the Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), e-mail, outgoing Web client traffic, outgoing File Transfer Protocol (FTP)—for which passive (PASV) mode is most secure—and outgoing Telnet.
- Encrypt router passwords: **service password-encryption** and encrypt the enable password with an MD5 hashing algorithm: **enable secret** *password*
- Apply access lists and passwords to virtual terminal (VTY) ports
- Enable route authentication in supported routing protocols