Cisco's High-Performance Stateful Firewall **Delivers Unparalleled Security**

CISCO SYSTEMS' PIX FIREWALL BRINGS DRAMATIC NEW SIMPLICITY AND UNRIVALED SECURITY TO CORPORATE NETWORKS.

Cisco's PIX Firewall

Typically configurable in five minutes or less, the PIX Firewall can thoroughly conceal your internal network from the outside world—providing full firewall security protection. And unlike typical CPU-intensive proxy servers that perform extensive processing on each data packet, the PIX Firewall uses a non-UNIX, secure, real-time, embedded system. This setup allows the PIX Firewall to deliver outstanding performance of more than 16,000 simultaneous connections, dramatically greater than UNIX-based firewalls.

The heart of the PIX Firewall's high performance is a protection scheme based on the adaptive security algorithm (ASA), which effectively hides client addresses from hackers so that they never have access to these addresses. The stateful, connection oriented ASA approach to security builds session flows based on source and destination addresses, TCP sequence numbers (which are randomized), port numbers, and additional TCP flags. This information is stored in a table, and all inbound packets are compared against entries in the table. Access is permitted through Cisco's PIX Firewall only if an appropriate connection exists to validate passage. This setup gives your organization transparent access for internal users and authorized external users, while protecting your internal network from unauthorized access.

Cisco's PIX Firewall further gains this dramatic performance advantage through a new feature called *cut-through proxy.* Whereas UNIX-based proxy servers are an ideal platform and can provide user authentication and maintain "state" (information about a packet's origin and destination) to offer good security, their performance suffers because they process all packets at Layer 7 of the OSI model.

The PIX Firewall's *cut-through proxy*, on the other hand, challenges a user initially at the application layer, like a proxy server. But once the user is authenticated against an industry-standard database based on Terminal Access Controller Access Control System (TACACS)+ or Remote Authentication Dial-In Service (RADIUS) and policy is checked, the PIX Firewall shifts the session flow and all traffic thereafter flows directly and quickly between the two parties, while maintaining session state. This *cut-through* capability allows the PIX Firewall to perform dramatically faster than proxy servers.

Beyond this high level of performance, the real-time embedded system also enhances the PIX Firewall's security. Unlike UNIX-based proxy servers whose source code is widely available and provides hackers with a target for penetration, Cisco's PIX Firewall's dedicated system is designed specifically for secure firewall operation.

MODULARITY
FLEXIBILITY

For even higher reliability, the PIX Firewall can be purchased with a failover/hot standby upgrade option, which eliminates a single point of failure. With two PIX Firewalls running in parallel, if one malfunctions, the second PIX Firewall transparently maintains the security operations.

Fast Performance

Cisco's PIX Firewall supports over 16,000 simultaneous TCP sessions, supporting hundreds of thousands of users without impacting end-user performance. Fully loaded, the PIX Firewall operates at greater than 45 Mbps, supporting T3 speeds. These speeds are an order of magnitude faster than those of UNIX-based firewalls.

Simplicity Brings Low Cost of Ownership

With Cisco's PIX Firewall, companies don't need hard-to-obtain UNIX experts to configure and install expensive, high-end UNIX workstations. Instead, users with little computer training can typically configure the PIX Firewall in less than five minutes. Ongoing maintenance is dramatically reduced as there is virtually no day-to-day management required for the PIX Firewall.

For configuration simplicity, users can operate the PIX Firewall with a graphical user interface (GUI) based on the hypertext markup language (HTML). Alternatively, for those already familiar with the Cisco Internetwork Operating System (Cisco IOS™) user interface, customers can choose a Cisco IOS-based interface.

Cisco also offers encryption using the Cisco PIX Private Link encryption card. With this card, companies can dramatically reduce telecommunications costs by having options to dedicated leased lines and sending encrypted IP packets over any public IP-based network, such as the Internet. With the PIX Private Link encryption card at each PIX Firewall site, companies can be assured of secure communications through the Internet using the Data Encryption Standard (DES) algorithm. The PIX Private Link encryption card also uses standards-based technology by incorporating the Internet Engineering Task Force's (IETF's) Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols (RFCs 1826 and 1827, respectively).

PIX Firewall Remedies IP Address Shortage

Cisco's PIX Firewall also provides a feature to expand and reconfigure IP networks without being concerned about a shortage of IP addresses. Network address translation (NAT) makes it possible to use either existing IP addresses or the addresses set aside in the Internet Assigned Numbers Authority's (IANA's) reserve pool (RFC 1918). The PIX Firewall also can selectively allow a mix of addresses to be translated or not translated, as needed.

Features at a Glance

- Strong, stateful connection oriented security protection restricts unauthorized users from accessing internal network resources
- Access from the outside network to the inside is allowed based on industry-standard authentication protocols such as TACACS+ and RADIUS
- Conceals internal network architecture
- Supports over 16,000 simultaneous connections
- Typical configuration in five minutes
- Two configuration interfaces supported: HTML GUI or Cisco IOS software user interface (UI)
- Secure dynamic and static translation
- Failover/hot standby for high reliability
- True NAT as discussed in RFC 1631
- For networks with registered IP addresses, non translation is available in order to use these registered addresses
- Support of Simple Network Management Protocol (SNMP) traps
- Audit information provided through syslog Management Information Base (MIB) support
- Transparent support for all common TCP/IP Internet services such as World Wide Web (WWW), File Transfer Protocol (FTP), Telnet, Archie, Gopher, and rlogin
- Support of multimedia data types, including RealAudio, Xing Technologies' Streamworks, CuSeeMe, Internet Relay Chat, and VDO Live
- Secure, real-time embedded system
- Multiple login levels supported

Benefits

- Less complex and more robust than packet-filtering firewalls or proxy servers
- No downtime required for installation
- No day-to-day management required
- No upgrading of hosts or routers
- Full outbound Internet access from unregistered internal hosts
- Does not require additional registered IP addresses for network expansion
- Allows use of Address Allocation for Private Internets (RFC 1918) or registered IP addresses
- No user impact—nondisruptive to existing LANs
- Interoperable with Cisco IOS-based routers

PIX Firewall Specifications

Available Software Sessions

(Based on simultaneous TCP/IP connections)

- 32, 256, 1024, 4096, 16,384

Network Support

- 10/100 BaseT Ethernet
- 4-/16-Mbps Token Ring
- Internet Protocol standards: IP, TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP)

Hardware Specifications

- 19-inch rack-mounted enclosure
- DB-9 EIA/TIA 232 console port
- 3.5 in floppy disk drive
- Lockable front panel

Physical Dimensions

- Height: 7 in.
- Width: 19 in.
- Depth: 18.5 in.
- Weight: 21 lb

Power Requirements

- Auto switching from:
  - Low range: 90-135 VAC
  - High range: 180-270 VAC
- Frequency:
  - 47-63 Hz
- Current:
  - 4.2 A max at 115 VAC input, full load
  - 2.0 A max at 230 VAC input, full load
- AC output:
  - 115 VAC output 1.0 A max
  - 230 VAC output 0.5 A max

Operating Environment

- Temperature range:
- Operating:
  - 0 to +45° C
- Storage:
  - -10 to +75° C

Safety Agencies

- UL-1950 standard
- CSA-EB-1402C standard
- IEC-380/VDE-0806 standard
- IEC-950/VDE-0805 EN-60-950 standard

Cisco Systems

Cisco Systems
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
s.a.r.l.
Parc Evolic-Batiment
L1/L2
16, Avenue du Quebec
BP 706-Villebon
91961 Courtaboeuf Cedex
France
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Intercontinental Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-7660
Fax: 408 526-4646

Latin American Headquarters
Cisco Systems, Inc.
790 N.W. 107th Avenue
Suite 102
Miami, FL 33172
Tel: 305 228-1200
Fax: 305 222-8456

Japanese Headquarters
Nihon Cisco Systems K.K.
Fuji Building
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
Tel: 81 3 5219 6000
Fax: 81 3 5219 6010

Cisco Systems has over 190 offices in the following countries. Addresses, phone numbers and fax numbers are listed on the Cisco Connection Online Web site at http://www.cisco.com.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Denmark • Finland • France • Germany Hong Kong • India • Indonesia • Ireland • Italy • Japan • Korea • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Philippines Portugal • Singapore • South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • United Arab Emirates • United Kingdom • Venezuela