Cisco PIX Firewall Series

Cisco Systems' high-performance, stateful PIX Firewall series brings unparalleled security

The Cisco PIX Firewall series delivers strong security and high performance for corporate networks. These firewalls allow you to thoroughly protect your internal network from the outside world—providing full firewall security protection. Unlike typical CPU-intensive proxy servers that perform extensive processing on each data packet, the Cisco PIX Firewalls use a non-UNIX, secure, real-time, embedded system. The Cisco PIX Firewall series, therefore, delivers outstanding performance of more than 16,000 simultaneous connections, dramatically greater than any general-purpose operating system.

Figure 1 PIX Firewall Series

To provide the platform extensibility you need without sacrificing the benefits of an embedded system, the PIX Firewall series now supports three separate network interface cards. For simplified management, the Cisco PIX Firewall series includes the easy-to-use Firewall Manager, a configuration and management tool with an intuitive graphical user interface (GUI). Administrators simply click on the icon representing the desired PIX Firewall to retrieve, edit, and centrally manage security policies. With management reports, network managers can perform statistical analysis on unauthorized users, amounts of traffic, and event logging for potential cost accounting. Network managers can also audit Universal Resource Locator (URL) logs to monitor which Web sites their users visit most. And by setting thresholds, administrators automatically receive real-time alerts through e-mail or pager notification when the firewall has been hit by hackers.

Cisco Systems

Maximum Performance and Number of Connections

The heart of the high performance of the Cisco PIX Firewall series is a protection scheme based on the adaptive security algorithm (ASA), which effectively protects access to the internal host network. 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 and outbound packets are compared against entries in the table. Access is permitted through the Cisco PIX Firewall series only if an appropriate connection exists to validate passage, providing internal users and authorized external users transparent access to an organization while protecting the internal network from unauthorized access.

The Cisco PIX Firewall series supports over 16,000 simultaneous sessions, supporting thousands of users without impacting end-user performance. Fully loaded, the Cisco PIX Firewall series (PIX10000 model) operates at greater than 90 megabits per second (Mbps), supporting two T3 speeds. These speeds are an order of magnitude faster than those of firewalls based on general-purpose operating systems.

The Cisco PIX Firewall series gains this dramatic performance advantage through an enhanced authentication feature called cut-through proxy. Whereas UNIX-based proxy servers can provide user authentication and maintain "state" (information about the origin and destination of a packet) to offer security, their performance suffers because they process all packets at the application layer of the Open System Interconnection (OSI) model, which is highly CPU intensive.

The cut-through proxy feature of the Cisco PIX Firewall series, on the other hand, challenges a user initially at the application layer, like a proxy server. But after the user is authenticated against an industry-standard database based on Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) and policy is checked, the Cisco PIX Firewall series shifts the session flow. All traffic thereafter flows directly and quickly between the two parties, while session state is maintained and security over traditional proxy-based firewalls is uncompromised. This cut-through capability allows the Cisco PIX Firewall series to perform dramatically faster than proxy servers. For many organizations, cut-through proxy also leverages the already-existing TACACS+ or RADIUS database used for the network access server. Cisco Systems offers such an enterprise management authorization database/server: the CiscoSecure access control server.

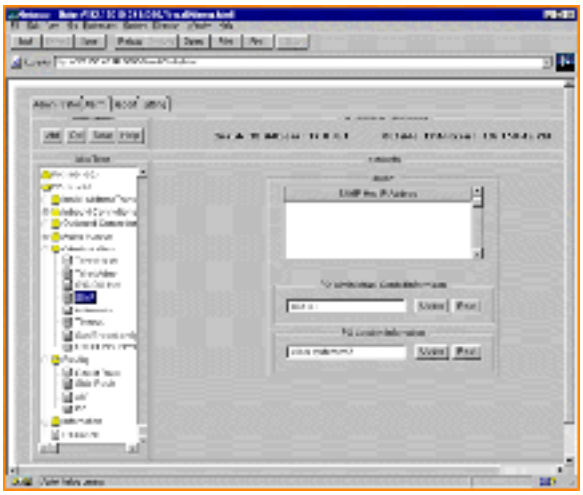
Strongest Security with Simple Administration

Beyond this high level of performance, the real-time embedded system also enhances the security of the Cisco PIX Firewall series. Although UNIX servers are ideal open- development platforms with widely available source codes, such general-purpose operating systems provide less-than- optimum performance and security. The dedicated Cisco PIX Firewall series is designed specifically for secure, high- performance protection.

For even higher reliability, the Cisco PIX Firewall series is available 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 Cisco PIX Firewall series transparently maintains security operations.

Administrators using the Firewall Manager tool can easily configure and manage multiple PIX Firewalls from a single location. A general security policy can be implemented in as little as six commands. Ongoing maintenance is dramatically reduced, as there is virtually no day-to-day management required for the Cisco PIX Firewall series.

Figure 2 Firewall Manager User Interface



For configuration simplicity, all you need is a Java-enabled browser to access the Firewall Manager, which runs on a Windows NT system. When authorized and connected, you see a graphic representation of all the PIX Firewalls on your network in one portion of the window. Another portion of the window lists the available configuration commands. After you click on a Cisco PIX Firewall, you select the appropriate configuration function and begin configuring the firewall. Alternatively, for those already familiar with the Cisco IOS user interface, customers can choose a Cisco IOS-based command-line interface.

The Firewall Manager also helps you analyze and account for Cisco PIX Firewall series activity. Now you can generate accounting reports that provide such information as the date and time of a connection, total time connected, per-user throughput (bytes and packets), application mix (port numbers), and other valuable data. You can use these reports for planning purposes or to charge back costs to various departments.

Content-Specific Capabilities for Maximum Control

To enable secure database access, the PIX Firewall series allows Oracle SQL*Net-based client/server applications to communicate through the firewall both with and without network address translation (NAT). This industry first enables mobile users to access corporate information servers located behind the firewall. This capability also simplifies deploying secure extranets, linking vendors and their customers for electronic commerce.

To help eliminate the threat of hostile Java applets, the PIX Firewall series includes a Java applet filter. With this filter, you can block Java applets, thereby limiting hostile attacks.

Further controlling incoming traffic content is Mail Guard, a feature that enables the secure transfer of mail directly to an internal mail host—eliminating the need for a costly mail relay host. Mail Guard allows connections to an internal mail host via TCP port 25 only. It logs all Simple Mail Transfer Protocol (SMTP) activity, and allows only the minimum SMTP server commands found in RFC 821, Section 4.5.1.

Data encryption provides the ultimate in content control. With the Cisco PIX Private Link encryption card, companies can build virtual private networks (VPNs) for sending encrypted IP packets over any public IP-based network such as the Internet. This linking of trusted networks can consolidate and dramatically reduce the telecommunications costs associated with previous leased-line or other dedicated networks. With a Cisco PIX Private Link encryption card at each PIX Firewall site, companies can be assured of secure communications through the Internet, and manage up to 256 remote sites. The encryption card uses the Data Encryption Standard (DES) algorithm and the Internet Engineering Task Force's (IETF's) Authentication Header/Encapsulating Security Payload (AH/ESP) protocols (RFCs 1826 and 1827, respectively).

A Remedy for the IP Address Shortage

The Cisco PIX Firewall series 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 series also can selectively allow a mix of addresses to be translated or not be translated, as needed. Cisco also ensures that NAT works with all the other

features of the PIX Firewall series, such as multimedia application support. Multimedia and NAT can be mutually exclusive features with competing firewalls.

The Cisco PIX Firewall series also supports port address translation (PAT) with "port-level multiplexing"—a method to further conserve IP addresses. With PAT, users' inside local addresses are automatically converted to a single outside local address using different port numbers to distinguish between each translation. Over 64,000 inside hosts can be served by a single outside IP address with PAT.

But what happens when unregistered addresses overlap with the identical IP address space of a registered address? Net Aliasing resolves this conflict by keeping track of which addresses are from which network, assuring delivery of data to the proper network.

Features and Benefits Summary

Table 1 Features and Benefits of the PIX Firewall Series, Software V.4.1

Features	Benefits
Adaptive Security Algorithm	• Provides stateful security for all TCP/IP sessions to protect sensitive, private resources
Cut-Through Proxy	• Offers highest authentication performance in the industry • Lowers cost of ownership by reusing existing authentication database
Secure, Real-Time, Embedded System	• Stronger security than open, standards-based operating systems such as UNIX and NT workstations • No CERT alerts
Supports more than 16,000 Simultaneous Connections	• Dramatically outperforms proxy servers—results in having to deploy fewer firewalls
Third Network Interface	• Strong security for WWW server, mail server, and any others publicly accessible in the perimeter network
Microsoft PPTP support	• Build client VPN solution integrated with security policy enforcement
Oracle SQL*Net Access	• Mobile users can reach secure information servers located behind the firewall
Firewall Manager GUI Software Tool	• Saves time and money in reduced network downtime and installation costs
Management Reports; URL Accounting	• Saves time and money in reduced network installation costs and maintenance
Java Applet Filter	• Ability to stop potentially dangerous Java applications on a per-client or per-IP address basis
Mail Guard	• Removes need for external mail relay in the perimeter network and eliminates service denial attacks on external mail relays
IETF AH/ESP Compatibility	• Standards-based encrypted connections are the foundation for multivendor VPNs
Multimedia Support	• Reduces administrative time and cost required to support these protocols • No special client configurations required
Service Denial	• Secures all transactions and services against service denial attacks
Failover/Hot Standby	• High availability to maximize network reliability
Network Address Translation	• Saves costly IP renumbering • Expands network address space
Nontranslation	• Allows client identity with strong security using existing IP addresses
Certifications/Audits	• Third-party validation of security strength—NCSA certified, security audit from SRI

Cisco PIX Firewall Series Specifications

Hardware Platforms

- PIX Firewall 10000—200-MHz, >90-Mbps performance
- PIX Firewall—133-MHz, 45-Mbps performance

Hardware Specifications

—	PIX Firewall	PIX Firewall 10000
Hardware Case	19-in. rack-mounted enclosure	19-in. rack-mounted enclosure
DB-9 EIA/TIA-232 Console Port	—	—
3.5-in. Floppy Disk Drive	—	—
Lockable Front Panel	—	—
Physical Dimensions		
Height	7 in.	7 in.
Width	19 in.	19 in.
Depth	18.5 in.	18.5 in.
Weight	21 lb	21 lb
Power Requirements		
Autoswitching from Low Range	90-135 VAC	90-135 VAC

—	PIX Firewall	PIX Firewall 10000
Autoswitching from High Range	180-270 VAC	180-270 VAC
Frequency	47-63 Hz	47-63 Hz
Maximum Power	253 Watts	253 Watts
Current		
115-VAC Input, Full Load	4.2 A max	5.4 A max
230-VAC Input, Full Load	0.5 A max	2.7 A max

—	PIX Firewall	PIX Firewall 10000
AC output		
115-VAC Output	1.0 A max	—
230-VAC Output	0.5 A max	—
Operating Environment		
Operating	0 to +45C	**0 to +45C**
Storage	–10 to +75C	– **10 to +75C**
Heat Dissipation (worst case with full power usage)	863.27 BTU/hr	863.27 BTU/hr
Safety Agencies		
UL-1950 Standard	—	—
CSA-EB-1402C Standard	—	—
IEC-380/VDE-0806 Standard	—	—
IEC-950/VDE-0805 EN-60-950 Standard	—	—

Available Software Sessions

(Based on simultaneous TCP/IP connections)

- 64, 1024, and 16384

Network Support

- 10/100BaseT Ethernet
- 4-/16-Mbps Token Ring

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
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
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 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 · Czech Republic · Denmark Finland · France · Germany · Hong Kong · Hungary · India · Indonesia · Ireland · Israel · Italy · Japan · Korea · Malaysia · Mexico The Netherlands · New Zealand · Norway · Philippines · Poland · Portugal · Russia · Singapore · South Africa · Spain · Sweden Switzerland · Taiwan, ROC · Thailand · United Arab Emirates · United Kingdom · Venezuela

- Internet Protocol standards: IP, TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP)