Cisco Secure PIX Firewall Series

Formerly known as the PIX Firewall, the Cisco Secure PIX Firewall™ series is the highest-performance, enterprise-class firewall product line within the Cisco firewall family. The integrated hardware/software PIX Firewall series delivers high security without impacting network performance, scaling to meet the entire range of customer requirements. The Cisco Secure PIX Firewall series is a key element in the overall Cisco end-to-end security solution set and is the leading product line in its segment of the firewall market.

The Internet's growth has resulted in increased security risks to corporate and government networks. Existing solutions such as proxy-based firewalls that run at the application level have many limitations, including slow performance, the need for high-end, costly, general-purpose platforms running a UNIX operating system, and the security risks inherent in using an open system such as UNIX. The Cisco Secure PIX Firewall series overcomes these limitations with its unique combination of high performance and strong security, backed by Cisco's worldwide 7x24 service and support organization.

Key Features of the Cisco Secure PIX Firewall Series

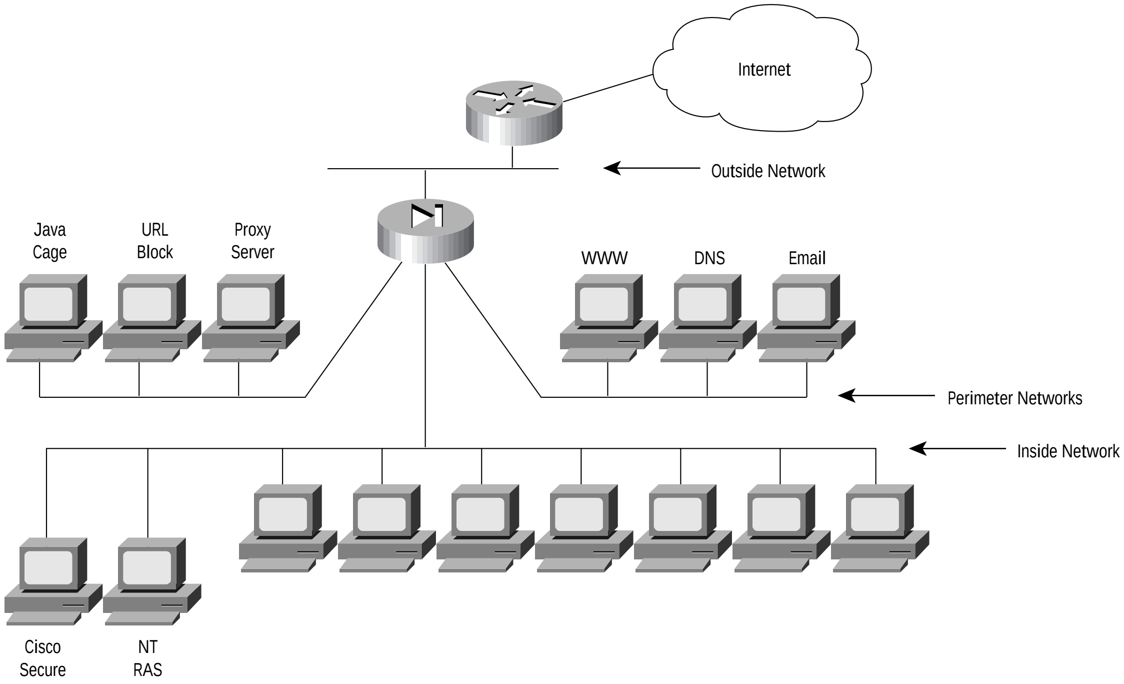
- *Non-UNIX, Secure, Real-Time, Embedded System*—This design eliminates the risks associated with a general-purpose operating system and allows the Cisco Secure PIX Firewall series to deliver outstanding performance—up to 256,000 simultaneous connections, dramatically greater than any UNIX-based firewall.
- *Adaptive Security Algorithm*—The heart of the Cisco Secure PIX Firewall series is the Adaptive Security Algorithm (ASA), which is less complex and more robust than packet filtering. It also offers higher performance and is more scalable than application-level proxy firewalls. ASA maintains the secure perimeters between the networks controlled by the firewall. The stateful, connection- oriented ASA design creates session flows based on source and destination addresses, randomized TCP sequence numbers, port numbers, and additional TCP flags. All inbound and outbound traffic is controlled by applying the security policy to these connection table entries.
- *User Authentication and Authorization with Cut-Through Proxy*—The Cisco Secure PIX Firewall series gains further dramatic performance advantages through cut-through proxy, a patent-pending method of transparently verifying the identity of users at the firewall and permitting or denying access to any TCP- or UDP-based application. This method eliminates the price/performance impact that UNIX system-based firewalls impose in similar configurations, and leverages the authentication and authorization services of the CiscoSecure Access Control Server.
- *Simplified Installation*—The PIX Firewall Setup Wizard speeds initial firewall setup. This Windows application guides the installer through the process with both on-screen descriptions and associated help files.
- *Centralized Configuration and Management*—The PIX Firewall Manager is a Java-based, graphical user interface (GUI) configuration tool that lets administrators click on a PIX Firewall icon to retrieve, edit, and centrally manage firewall

security policies. Separate tabs provide access to configuration information common to all the PIX Firewalls being managed. They also provide access to built-in reports for user-based accounting for Web sites visited and volume of files transferred. The PIX Firewall Manager can automatically provide real-time alerts through e-mail or pager notification when anyone attempts a firewall breach.

- *Standards-Based Virtual Private Network Option*—The PIX Firewall IPSec encryption card, due out in release 5.0 (Q3 FY1999), enables administrators to reduce the costs of connecting mobile users and remote sites to the corporate network over the Internet or other public IP networks. Based on the new Internet Security (IPSec) and Internet Key Exchange (IKE) standards, the PIX VPN implementation is fully interoperable with the corresponding Cisco Internetwork Operating System (Cisco IOS®) software capability. The PIX IPSec solution will include Windows 95 and Windows NT 4.0 client software to enable mobile and remote users to connect securely to the PIX Firewall.
- *URL Filtering*—PIX Firewall URL filtering is provided in partnership with NetPartners WebSENSE server software. The PIX Firewall will check outgoing URL requests with the policy defined on the WebSENSE server running either on Windows NT or UNIX. Based on responses from the NetPartners server, which matches requests against Web-site characteristics deemed inappropriate for business use, the PIX Firewall either permits or denies connections. Because URL filtering is handled on a separate platform, no additional performance burden is placed on the PIX Firewall.
- *Failover/Hot Standby Upgrade Option*—The PIX Firewall failover option ensures high availability and eliminates a single point of failure. With two PIX Firewalls running in parallel, if one malfunctions, the second PIX Firewall automatically maintains security operations.

Please refer to the Cisco Secure PIX Firewall data sheet for a detailed list of PIX Firewall hardware and software features.

Figure 1 When you deploy the Cisco Secure PIX Firewall series with four interfaces, you experience the strongest security available. Public Web and DNS servers can be placed on one network segment, while proxy servers and URL blocking servers are located on another network segment. The inside network is also isolated on a separate interface.



Key Benefits of the PIX Firewall Series

Strongest Security

The Cisco Secure PIX Firewall series adds an unrivaled measure of security to corporate networks. When deployed in a four interface configuration with Cisco router access control lists (ACLs) for packet filtering, the PIX Firewall series provides a strong barrier to unauthorized users. The heart of the PIX Firewall series is a protection scheme based on ASA, which offers stateful connection-oriented security. ASA tracks the source and destination address, TCP sequence numbers, port numbers, and additional TCP flags of each packet. 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 Secure PIX Firewall series only if an appropriate connection exists to validate passage. This setup gives organizations transparent access for internal and authorized external users, while protecting internal networks from unauthorized access. It also offers an unprecedented level of security protection. The Cisco Secure PIX Firewall series relies on a real-time embedded system that is many times more secure than an open, standards-based operating system such as UNIX.

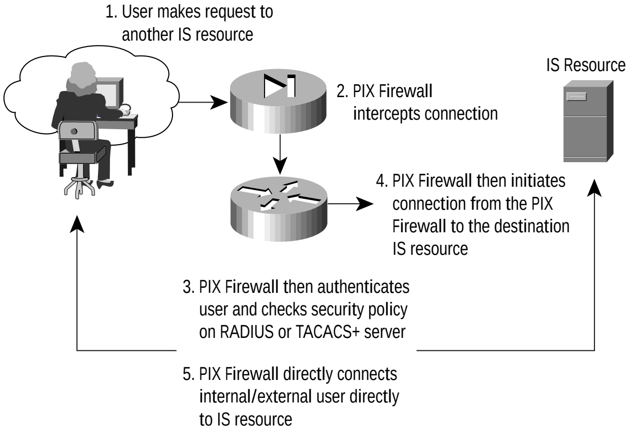
Platform Extensibility

The strong security provided by this real-time embedded system is now complemented by its platform extensibility features. The new, fourth network interface and support in version 4.4 of a four-port 10/100 Ethernet interface card expands the total PIX Firewall security solution while retaining the performance and security attributes. As shown in Figure 1, multiple network interfaces allows publicly accessible Web, mail, and Domain Name System (DNS) servers to be protected by your security policy. Web-based and traditional electronic data interchange (EDI) applications that link vendors and customers are also more secure and scalable when implemented using a physically separate network. As the trend toward building these extranet applications accelerates, the Cisco Secure PIX Firewall is already prepared to accommodate these applications. The many network interfaces could also host a URL filtering server today, and other content filtering servers as they become available. Locating these processing-intensive applications on separate platforms, each on a distinct, secure, and high-performing network segment, provides both performance and security benefits.

Greatest Authentication Performance

The Cisco Secure PIX Firewall series offers performance that is dramatically greater than competing firewalls. It gains speed through a patent-pending process called cut-through proxy, which is the fastest method for a firewall to authenticate a user. Unlike a proxy server, which must analyze every data packet at the application layer of the Open System Interconnection (OSI) model (a time- and process-intensive function), a PIX Firewall first queries a TACACS+ or RADIUS database server for authentication. When a user is approved and policy is checked, the Cisco Secure PIX Firewall series shifts the session flow, and all traffic thereafter flows directly and quickly between the two parties while session state information is maintained. This cut-through proxy capability allows the Cisco Secure PIX Firewall series to perform dramatically faster than proxy servers.

Figure 2 Cut-Through Proxy


1. User makes request to another IS resource
IS Resource
2. PIX Firewall intercepts connection
4. PIX Firewall then initiates connection from the PIX Firewall to the destination IS resource
3. PIX Firewall then authenticates user and checks security policy on RADIUS or TACACS+ server
5. PIX Firewall directly connects internal/external user directly to IS resource

Typical proxy servers also offer limited performance because the server must initiate a process for each TCP connection. With 300 users, 300 processes could be required, and this procedure is CPU intensive. With its real-time embedded system, the Cisco Secure PIX Firewall series can handle over a quarter of a million simultaneous sessions, a level of performance that is dramatically higher than an application proxy firewall. Fully loaded, the PIX model 520 operates at 170 megabits per second, supporting multiple T3 lines.

Lowest Cost of Ownership

The Cisco Secure PIX Firewall series offers the lowest cost of ownership of any security device, including proxy servers. It is simple to install and configure using the Setup Wizard and Firewall Manager software tools, resulting in little network downtime. Competitive offerings are more complex to configure, and they require the network to be down for longer periods. In addition, the Cisco Secure PIX Firewall series permits transparent support of Internet multimedia applications, eliminating the need to physically modify and reconfigure each client workstation or PC—a tremendous administrative burden required by competing firewalls.

Enhanced accounting features help you understand and control usage costs. With the GUI-based Firewall Manager tool, you can analyze PIX Firewall activity and generate graphical, easy-to-read accounting reports that provide information such as the date and time of a connection, total time connected, per-user throughput (bytes and packets), and application mix (port numbers). Use these reports for planning purposes or to charge back costs to various departments. For more sophisticated reporting and analysis requirements, the PIX Firewall supports several third-party applications, including Private I from Open Systems Solutions and Telemate.Net from Telemate Software.

Support of the IETF IPSec standard allows you to scale your VPNs with much lower administrative costs. Part of IPSec includes the use of public digital keys that are administered by a Certificate Authority—a third-party vendor that registers public keys. Beyond allowing much greater scalability, this use of a Certificate Authority dramatically reduces the administrative time and cost now associated with manual key administration.

The Cisco Secure PIX Firewall series is also less expensive to maintain. Because proxy servers are typically based on UNIX, companies must hire costly specialists to maintain these complex systems. In addition, because most Computer Emergency Response Team (CERT) advisories pertain to UNIX, companies must commit continuous resources to tracking these advisories and installing UNIX patches. The Cisco Secure PIX Firewall series, on the other hand, has a small, real-time, secure and embedded system that requires little ongoing maintenance. Also, because all the software runs from Flash memory, no hard drives are required, providing a much higher network uptime and mean time between failure (MTBF).

The Cisco Secure PIX Firewall series is scalable, supporting from 64,000 to 256,000 simultaneous connections. This scenario protects the user’s investment in Cisco technology, because the Cisco Secure PIX Firewall series can scale as companies’ needs grow.

The cut-through proxy feature of the Cisco Secure PIX Firewall series further reduces the cost of ownership. It saves time and money by leveraging a company’s CiscoSecure or other network access server database based on TACACS+ or RADIUS. This savings is significant compared to proxy-based firewalls that may require companies to maintain separate databases--incurring additional installation and maintenance costs.

Cisco offers a cost-effective maintenance program, called SMARTnet maintenance. The SMARTnet program offers customers high value because, unlike competitors who typically cover either firewall hardware or software, SMARTnet covers both hardware and software of the Cisco Secure PIX Firewall series. The maintenance price is significantly lower than the combined costs of the hardware and software support from other firewall manufacturers.

Availability and Orderability

The Cisco Secure PIX Firewall series products are available now. The following table lists the Cisco Secure PIX Firewall series ordering information.

Table 1 Cisco Secure PIX Firewall Series Product

Product Name/Description	Order Number
PIX 515 Firewall, 2 integrated ethernet interfaces, 200MHz processor, 32 MB memory, two expansion slots	PIX-515
PIX 515 Firewall Restricted Software—Supports only two ethernet interfaces, 8MB Flash storage, 32MB RAM. Does not support Failover feature	PIX-515-SW-R
PIX 515 Firewall Unrestricted Software—Supports up to 6 ethernet interfaces and all PIX features. Requires PIX-515-MEM-32	PIX-515-SW-UR
32 MB RAM upgrade for the PIX 515 Firewall	PIX-515-MEM-32
PIX 515 Firewall—Restricted to Unrestricted software upgrade. Requires PIX-515-MEM-32	PIX-515-SW-UPG=
PIX 515; PIX-515-SW-R	PIX-515-R-BUN
PIX 515; PIX-515-SW-R; PIX-515-MEM-32	PIX-515-UR-BUN
PIX 520 Firewall w/extra memory—Max 6 interfaces, 233-MHz processor, 170-Mbps performance, 128 MB memory, four expansion slots	PIX-520
PIX 520 Firewall—233-MHz processor, >90-Mbps performance, -48VDC power	PIX-520-DC
PIX 520 Firewall Entry level license (Up to 100 users, 128 connections)	PIX-CONN-128
PIX 520 Midrange license (100 to 500 users, 1024 connections)	PIX-CONN-1K
PIX 520 Unrestricted license (500+ users, 16,384+ connections)	PIX-CONN-UR
PIX 520 license upgrade from 1024 to unlimited	PIX-CONN-1K-UR=
PIX 520 license upgrade from 128 to 1024 connections	PIX-CONN-128-1K=
PIX 520 license upgrade from 128 to unlimited	PIX-CONN-128-UR=
Failover cable/upgrade kit—software version 3.0 or later	PIX-FO=
PIX software version upgrade for non-support customers	PIX-CONN-VER=
PIX complete documentation set	DOC-PIX=
PIX 10/100 single-port Ethernet card	PIX-1FE
PIX 10/100 single-port Ethernet card, spare	PIX-1FE=
PIX Token Ring card	PIX-1TR
PIX Token Ring card, spare	PIX-1TR=
Private Link 2 56-bit DES encryption card	PIX-PL2
Private Link 2 56-bit DES encryption card, spare	PIX-PL2=
Memory Upgrade to 128MB for PIX Firewalls prior to the 5XX Series	PIX-MEM-UPG-128=
Memory Upgrade to 128MB for PIX 510 and 520 Firewalls (prior to the PIX 520-XM)	PIX-MEM-5XX-128=
Service and Support—Direct	PIX SMARTnet maintenance—all versions
CON-SNT-PIX	PIX SMARTnet enhanced maintenance—all versions
CON-SNTE-PIX	PIX SMARTnet premium maintenance—all versions
CON-SNTP-PIX	PIX onsite maintenance—all versions
CON-OS-PIX	PIX onsite enhanced maintenance—all versions
CON-OSE-PIX	PIX onsite premium maintenance—all versions
CON-OSP-PIX	Service and Support—Two-Tier Products
PIX SMARTnet maintenance---all versions	CON-SNT-PKG12

CISCO SYSTEMS

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 69 18 61 00
Fax: 33 1 69 28 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 200 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/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela