

Cisco Secure PIX Firewall Series

FORMERLY KNOWN AS THE PIX FIREWALL, THE CISCO SECURE PIX[®] FIREWALL SERIES DELIVERS STRONG SECURITY IN AN EASY-TO-INSTALL, INTEGRATED HARDWARE/SOFTWARE APPLIANCE THAT OFFERS OUTSTANDING PERFORMANCE. THE SERIES ALLOWS YOU TO RIGOROUSLY PROTECT YOUR INTERNAL NETWORK FROM THE OUTSIDE WORLD—PROVIDING FULL FIREWALL SECURITY PROTECTION.

Unparalleled Security for Corporate Networks

The Cisco Secure PIX Firewall series delivers strong security in an easy-to-install, integrated hardware/software appliance that offers outstanding performance. The series allows you to rigorously protect your internal network from the outside world—providing full firewall security protection. Unlike typical CPU-intensive full-time proxy servers that perform extensive processing on each data packet at the application level, Cisco Secure PIX firewalls use a non-UNIX, secure, real-time, embedded system. The PIX Firewalls deliver superior performance of up to 256,000 simultaneous connections, over 6,500 connections per second, and nearly 170 megabits per second (Mbps) throughput. This level of performance is dramatically greater than that delivered by other appliance-like firewalls or those based on general-purpose operating systems.

Figure 1 Cisco Secure PIX Firewall Series



VPN Interoperability and Scalability with IPSec

Firewalls have traditionally provided perimeter security by maintaining stateful control of all connections between connected network segments. Today, more and more customers are looking

to the firewall for virtual private network (VPN) services in addition to access control. For IP-layer VPNs, the Internet Engineering Task Force (IETF) IP Security working group has drafted a collection of standards referred to as IPSec.

These emerging IETF IPSec standards are designed to provide secure private communications over the Internet or any IP network. IPSec ensures confidentiality, integrity, and authenticity. With IPSec encryption running on an IOS/IPSec enabled Cisco router, or on the PIX beginning with v 5.0 (Mid-1999), users can support secure VPNs between multiple endpoints, including remote or mobile Windows PCs with VPN client software, Cisco IOS routers, other PIX Firewalls, or encryption devices that are IPSec compliant.

With an IPSec-based VPN, remote users from client computers can securely access corporate networks at low cost. Using the Internet for access dramatically reduces the telecommunications costs associated with previous leased-line or other dedicated networks. Companies also no longer need to maintain large modem banks and access servers—a large capital outlay and administrative headache—to handle remote users dialing in. With just a local phone call to an ISP, users can securely access private corporate intranets over the Internet.

IPSec includes an umbrella of security and authentication protocols, most importantly the Internet Key Exchange (IKE). IKE enables two endpoints to establish secure connections using preshared keys or public key infrastructure (PKI) digital certificates that are administrated by a certificate authority—an

in-house or outsourced service that registers public keys. IKE enables a VPN to scale to thousands of endpoints by using the equivalent of a signed digital ID card to identify each endpoint.

For secure data encryption, Cisco's implementation of IPsec for both routers and the PIX supports both the Data Encryption Standard (DES) and Triple DES algorithms. At this writing, the 56-bit DES version of these IPsec products could be exported from the U.S. to customer locations worldwide. Also exportable but subject to more stringent export regulations are the 168-bit Triple DES products. Check with your Cisco Systems representative for the latest export control information.

Platform Extensibility

To provide the platform extensibility you need without sacrificing the benefits of an embedded system, the Cisco Secure PIX Firewall series includes two hardware platforms, the PIX Firewall 515 and 520, which support a broad range of network interface cards (NICs). Standard NICs include single- or four-port 10/100 Ethernet cards, 4/16 Token Ring cards, and dual-attached multimode FDDI cards. FDDI cards and four-port Ethernet cards are supported in PIX beginning with version 4.4. Check with your Cisco Systems representative for the latest ordering information.

For sites requiring a DC-powered firewall solution, the PIX Firewall 520 is now available with a 48VDC power supply. The PIX Firewall 520-DC is certified to NEBS Level 3 as tested to Bellcore GR-63 and GR-1089 standards.

Graphical Installation and Management

For simplified installation and management, the Cisco Secure PIX Firewall series includes the Setup Wizard and the graphical Firewall Manager. The Setup Wizard runs on Windows 95 and Windows NT and is a graphical program that quickly steps you through initial installation of the PIX Firewall. With the Firewall Manager, network managers can easily configure and manage the PIX Firewall using 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.

A collection of management reports allows network managers to perform statistical analysis on unauthorized users and 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 firewalls are hit by hackers.

Several third-party products offer more extensive management reporting and analysis for use with the Cisco Secure PIX Firewall. Private I from Open Systems Solutions provides a full range of standard day-to-day operational reports based on continuous monitoring of one or more PIX Firewalls. Private I also allows users to create customized reports. Telemate.Net from Telemate Software analyzes firewall logs to relate Internet usage records to a directory of users and departments. You can use Telemate.Net reports to track costs by user and bill them accordingly.

In addition to these reporting capabilities, the PIX Firewall actively filters URLs, thereby controlling which Web sites users can access. URL filtering is provided through integration with NetPartners WebSENSE server software, now with a version for the Cisco PIX Firewall. WebSENSE server software runs either on a Windows NT or UNIX server located on an inside network or a protected perimeter network off the PIX Firewall. Because URL filtering is handled on a separate platform, it doesn't hamper PIX Firewall performance as greatly as it does on competitive firewalls that run URL filtering on the same platform as the firewall itself.

Maximum Performance and Number of Connections

The heart of the Cisco Secure PIX Firewall series' high performance is a protection scheme based on the adaptive security algorithm (ASA), which effectively protects access to the internal host network by comparing inbound and outbound packets to entries in a table. Access is permitted only if an appropriate connection exists to validate passage. Another performance feature is cut-through proxy, which enhances authentication. Cut-through proxy challenges a user initially at the application layer, but once the user is authenticated and policy is checked, the PIX Firewall shifts session flow to a lower layer for dramatically faster performance. (See the Cisco Secure PIX Firewall Overview or PIX Firewall White Paper for more information on ASA and cut-through proxy.)

The Cisco Secure PIX Firewall 515-R (restricted) supports up to 64,000 simultaneous sessions, the PIX 515-UR (unrestricted) supports up to 128,000 simultaneous sessions, and the PIX 520 supports up to 256,000 simultaneous sessions! Each of these PIX models allows you to accommodate thousands of users without affecting end-user performance. Fully loaded, the PIX Firewalls operate at higher speeds and supports more simultaneous connections than competitors, according to the Firebench test suite run by KeyLabs, Inc. The test suite showed

the PIX Firewall could securely accept 6579 connections per second and pass 169 Mbps of FTP and HTTP traffic—sufficient performance to support high-speed campus LANs or multiple T3 WAN environments. These speeds are two to three times faster than that offered by competitive firewalls based on general-purpose operating systems.

Strongest Security with Simple Administration

Beyond this high level of performance, the PIX Firewall real-time embedded system also enhances the security of the Cisco Secure 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 Secure PIX Firewall series is designed specifically for secure, high-performance protection.

For even higher reliability, the Cisco Secure 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 automatically 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.

Figure 2 Firewall Manager User Interface



With the graphical Firewall Manager, you can easily configure and manage multiple PIX Firewalls from a single location. You can also generate accounting reports for planning purposes or to charge back costs to various departments.

For configuration simplicity, all you need is a Java-enabled browser to access the Firewall Manager, which runs on Windows NT systems. Once your system is 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 clicking on a Cisco Secure PIX Firewall, you select the appropriate configuration function and begin configuring the firewall. Alternatively, for those already familiar with the Cisco IOS user interface, the firewall allows users to choose a similar, software-based, command-line interface.

The Firewall Manager also helps you analyze and account for Cisco Secure PIX Firewall series activity. Now you can generate accounting reports on CiscoSecure or other TACACS+ or RADIUS servers that provide information such as the date and time of a connection, total time connected and total number of bytes sent and received, 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 to various departments.

Content-Specific Capabilities for Maximum Control

To enable secure database access, the Cisco Secure 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 a firewall. This capability also simplifies deployment of secure extranets as well as linking vendors and customers for electronic commerce.

To help eliminate the threat of hostile Java applets, the Cisco Secure PIX Firewall series includes a Java applet filter. With this filter, you can block Java applets that are delivered via HTTP (not in archives or otherwise compressed), thereby limiting hostile attacks. More sophisticated filtering of Java and ActiveX is possible with the use of third-party products.

Mail Guard, a feature that enables secure mail transfer directly to an internal mail host, further controls incoming traffic content and eliminates 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. More sophisticated filtering of mail is possible with the use of third-party products.

Ideal for Managed Firewall Services

Service providers can create flexible and scalable managed firewall services using the Cisco Secure PIX Firewall series. The ease of configuration and management and the integrated hardware and software design simplify deploying the PIX Firewall either as customer premises equipment (CPE), at the central office (CO), or at local points-of-presence (POP). Service providers can manage all PIX Firewalls remotely, now that logging and configuration updates can be done from any interface in the chassis. For CO or POP sites requiring a DC-powered firewall solution, Cisco Secure PIX Firewall 520 is now available with a -48VDC power supply. The Cisco Secure PIX Firewall 520-DC is certified to NEBS Level 3 as tested to Bellcore GR-63 and GR-1089 standards.

A Remedy for the IP Address Shortage

The Cisco Secure PIX Firewall series provides a feature to expand and reconfigure IP networks without causing IP address shortage concern. NAT makes it possible to use either existing IP addresses or the addresses set aside in the Internet Assigned Numbers Authority (IANA) reserve pool (RFC 1918). The Cisco Secure PIX Firewall series also can selectively allow a mix of addresses to be translated or not be translated, as needed. Cisco ensures that NAT works with all the other PIX Firewall features, such as multimedia application support. Multimedia and NAT can be mutually exclusive features with competing firewalls.

The Cisco Secure PIX Firewall series 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 single outside local addresses using different port numbers to distinguish between each translation. More than 64,000 inside hosts can be served by a single outside IP address with PAT.

When unregistered addresses overlap with the identical IP address space of a registered address, Net Aliasing software keeps track of which addresses are from which network, assuring delivery of data to the proper network.

Features and Benefits Summary

Features and Benefits of the Cisco Secure PIX Firewall Series, Software V.4.4

Features	Benefits
Adaptive Security Algorithm	<ul style="list-style-type: none"> Provides stateful security for all TCP/IP sessions to protect sensitive, private resources
Cut-Through Proxy	<ul style="list-style-type: none"> Offers highest authentication performance in the industry Lowers cost of ownership by reusing existing authentication database
Secure, Real-Time, Embedded System	<ul style="list-style-type: none"> Provides stronger security than open, standards-based operating systems such as UNIX and NT workstations
Multiple Network Interface Cards	<ul style="list-style-type: none"> Provides strong security for Web and any other publicly accessible servers, multiple extranet links to different partners, protected logging and URL filtering servers, and more
Prevention of Denial-of-Service Attacks	<ul style="list-style-type: none"> Protects the firewall and the servers and clients behind it from disruptive or damaging hackers; secures all transactions and services against service denial attacks
Up to 256,000 Simultaneous Connection Support	<ul style="list-style-type: none"> Dramatically outperforms proxy servers—results in deployment of fewer firewalls
IETF IPsec Support	<ul style="list-style-type: none"> Enables VPN interoperability, scalability, and lower administrative costs
Broad range of supported applications (See Full Listing in TCP/IP Protocol and Application Support under Specifications)	<ul style="list-style-type: none"> Reduces the impact of a firewall on network users
PIX Firewall Manager and Setup Wizard	<ul style="list-style-type: none"> Saves time and money in reduced network downtime and installation costs
Management Reports; URL Accounting	<ul style="list-style-type: none"> Saves time by allowing easy viewing of PIX Firewall activity, including accounting data
URL Filtering	<ul style="list-style-type: none"> Provides the ability to control which Web sites users visit and maintains an audit trail for accounting purposes; has minimum impact on PIX Firewall performance
Java Applet Filter	<ul style="list-style-type: none"> Enables firewall to stop potentially dangerous Java applications on a per-client or per-IP address basis
Mail Guard	<ul style="list-style-type: none"> Removes the need for external mail relay in the perimeter network and eliminates service-denial attacks on external mail relays
Multimedia Application Support	<ul style="list-style-type: none"> Reduces administrative time and cost required to support these protocol Requires no special client configurations
Failover/Hot Standby	<ul style="list-style-type: none"> Delivers high availability to maximize network reliability
Network Address Translation	<ul style="list-style-type: none"> Saves costly IP renumbering Expands network address space
Nontranslation	<ul style="list-style-type: none"> Allows client identity with strong security using existing IP addresses
Certifications/Audits	<ul style="list-style-type: none"> Provides third-party validation of security strength—ICSA certified, security audit from SRI, NSA Common Criteria certification pending

Cisco Secure PIX Firewall Series Specifications

Hardware Platforms and Specifications

	PIX Firewall 515-R	PIX Firewall 515-UR	PIX Firewall 520	PIX Firewall 520-DC
Hardware Case	19-in. rack-mountable (comes with rack-mount hardware)	19-in. rack-mountable (comes with rack-mount hardware)	19-in. rack-mountable (comes with rack-mount hardware)	19-in. rack-mountable (comes with rack-mount hardware)
Random Access Memory	32 MB	64 MB	128 MB	128 MB
Flash Memory	16 MB	16 MB	16 MB	16 MB
Console Port	RJ-45	RJ-45	DB-9 EIA/TIA-232	DB-9 EIA/TIA-232
Boot/Update Device	TFTP only	TFTP only	3.5-in. floppy disk drive	3.5-in. floppy disk drive
Failover Port ¹	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232	DB-25 EIA/TIA-232
Physical Dimensions				
Height	1.72"	1.72"	5.21 in.	5.21 in.
Width	16.82 in.	16.82 in.	16.82 in.	16.82 in.
Depth	11.8 in.	11.8 in.	17.5 in.	17.5 in.
Weight	11 lb	11 lb	21 lb	21 lb
Power Requirements				
Autoswitching	100-240 VAC	100-240 VAC	100-240 VAC	-48 VDC
Frequency	50-60 Hz	50-60 Hz	50-60 Hz	---
Current	1.5-0.75 Amps	1.5-0.75 Amps	4-2 Amps	4 Amps
Operating Environment				
Operating temperature	-5° to +45°C (-25°F to 113°F)	-5° to +45°C (-25°F to 113°F)	-5° to +45°C (-25°F to 113°F)	-5° to +45°C (-25°F to 113°F)
Nonoperational temperature	-25°C to +70°C	-25°C to +70°C	-25°C to +70°C	-25°C to +70°C
Operational humidity	95% relative humidity (RH)	95% relative humidity (RH)	95% relative humidity (RH)	95% relative humidity (RH)
Operational altitude	3000m (9843 feet), 25° C (77° F)	3000m (9843 feet), 25° C (77° F)	3000m (9843 feet), 25° C (77° F)	3000m (9843 feet), 25° C (77° F)
Nonoperational altitude	4570m (15000 feet), 25° C (77° F)	4570m (15000 feet), 25° C (77° F)	4570m (15000 feet), 25° C (77° F)	4570m (15000 feet), 25° C (77° F)
Operational shock	1.88 m/sec (74 in/sec) 1/2 sine input	1.88 m/sec (74 in/sec) 1/2 sine input	1.88 m/sec (74 in/sec) 1/2 sine input	1.88 m/sec (74 in/sec) 1/2 sine input
Nonoperational shock	60G 11 ms 1/2 sine input	60G 11 ms 1/2 sine input	60G 11 ms 1/2 sine input	60G 11 ms 1/2 sine input
Operational vibration	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input
Nonoperational vibration	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input	0.41 Grms ² (5-500 Hz) random input
Heat Dissipation (Worst Case with Full Power Usage)	160.37 BTU/hr	160.37 BTU/hr	863.27 BTU/hr	863.27 BTU/hr

	PIX Firewall 515-R	PIX Firewall 515-UR	PIX Firewall 520	PIX Firewall 520-DC
EMI	CE, VCCI class II, FCC, BCIQ, Austel	CE, VCCI class II, FCC, BCIQ, Austel	CE, VCCI class II, FCC, BCIQ, Austel	CE, VCCI class II, FCC, BCIQ, Austel
Safety Agencies	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950	UL, C-UL, TUV, IEC 950
UL-1950 Standard	3rd Edition	3rd Edition	3rd Edition	3rd Edition
TUV EN 60950	2nd Edition, Am.1-4	2nd Edition, Am.1-4	2nd Edition, Am.1-4	2nd Edition, Am.1-4
IEC-950/VDE-0805 EN-60-950 Standard	Yes	Yes	Yes	Yes
Bellcore	No	No	No	NEBS Level 3 tested to Bellcore GR-63 and GR-1089

¹Failover requires special Cisco cable

Available Software Licensing Choices

For the PIX 515 (version 4.4), licensing is feature-based. All PIX 515 software comes with an unrestricted user license, with the number of simultaneous outbound TCP/IP connections governed by the hardware limits set by each box.

The entry level PIX 515-R (restricted) provides up to 50,000 connections (The PIX 515-R is further restricted by not providing failover and being limited to only two 10/100 ethernet interfaces.) The midrange PIX 515-UR provides up to 100,000 connections, failover, and up to six 10/100 ethernet interfaces.

Pricing for the PIX 520 will remain the same, with entry level, midrange, and unrestricted licenses available. The PIX 520 provides over a quarter of a million connections, failover, and up to six 10/100 ethernet connections or up to four token ring or two FDDI interfaces.

NIC Support

- Single-port 10/100BaseT Ethernet (up to four NICs per PIX Firewall chassis - not available for the PIX 515 with Restricted software)
- Four-port 10/100 BaseT Ethernet (may be combined with one or more single-port 10/100 Ethernet NICs - not available for the PIX 515 with Restricted software)
- 4-/16-Mbps Token Ring (up to four NICs per PIX Firewall chassis - not available for the PIX 515)
- FDDI (limited to two NICs per PIX Firewall chassis - not available for the PIX 515)

Note: Only NICs purchased from Cisco or its authorized resellers can be used in the Cisco Secure PIX Firewall. Attempts to use other cards will void the warranty.

TCP/IP Protocol and Application Support

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Generic Route Encapsulation (GRE)
- Address Resolution Protocol (ARP)
- Domain Name System (DNS)
- Simple Network Management Protocol (SNMP)
- Boot Protocol
- HyperText Transport Protocol (HTTP)
- File Transfer protocol (FTP)
- Trivial File Transfer protocol (TFTP)
- Archie
- Gopher
- Telnet
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- SQL*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Berkeley Standard Distribution (BSD)-Rcmds
- AAA Server Groups

Multimedia Applications

- Microsoft NetShow
- White Pine CU-SeeMe
- RealNetworks RealAudio and RealVideo
- Xing StreamWorks
- VDOnet VDOLive
- VXtreme WebTheater
- VocalTec Internet Phone

Videoconferencing (H.323) Applications

- Microsoft NetMeeting
- Intel Internet Video Phone
- White Pine Meeting Point



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