

Cisco Secure PIX Firewall Software v5.2

THE WORLD-LEADING CISCO SECURE PIX FIREWALL™ SERIES PROVIDES TODAY'S NETWORKING CUSTOMERS WITH UNMATCHED SECURITY, RELIABILITY, AND PERFORMANCE. THE INTEGRATED HARDWARE/SOFTWARE PACKAGE DELIVERS FULL STATEFUL FIREWALL PROTECTION, AS WELL AS IP SECURITY (IPSEC) VIRTUAL PRIVATE NETWORK (VPN) CAPABILITIES, WHICH ALLOWS YOU TO RIGOROUSLY PROTECT YOUR INTERNAL NETWORK FROM THE OUTSIDE WORLD.

Overview

Unlike typical CPU-intensive, full-time proxy servers, Cisco Secure PIX Firewalls use a non-UNIX, secure, real-time, embedded system. Its tradition of flexibility and scalability, combined with wide selection of platforms and features, allows the PIX to meet the entire range of customer requirements.

Version 5.2 is the latest release of the Cisco Secure PIX Firewall dedicated operating system (OS). It delivers the latest in PIX functionality, performance, and security improvements, as well as a host of new features.

Eight Ethernet Interfaces

To provide the platform extensibility you need without sacrificing the benefits of an embedded system, the Cisco Secure PIX Firewall series supports a broad range of network interface cards (NICs). Standard NICs include single- or four-port 10/100 Fast Ethernet, Gigabit Ethernet, 4/16 Token Ring, and dual-attached multimode FDDI cards. Using PIX software version 5.2 select PIX Firewalls, such as the 525-UR, can now support up to eight Ethernet interfaces.

Intrusion Detection

The Cisco Secure PIX Firewall now includes intrusion detection technology. It is ideal for any network perimeter, especially for locations where additional security between network segments is required. It also can provide additional visibility at intranet, extranet, and branch-office Internet perimeters.

The PIX Firewall's Intrusion Detection System (IDS) identifies 53 common attacks using signatures to detect patterns of misuse in network traffic. These signatures represent severe breaches of security, including the most common network attacks and information-gathering scans.

With this functionality, PIX acts as an inline intrusion detection sensor. It watches packets and sessions as they flow through the firewall, scanning each for a match with any of the IDS signatures. When suspicious activity is detected, PIX responds immediately and can be configured to:

- Send an alarm to a syslog server
- Drop the packet
- Reset the Transmission Control Protocol (TCP) connection

Developed with flexibility in mind, PIX IDS allows a signature to be acted upon differently depending on the interface on which it was detected on. PIX also allows signatures to be individually disabled when the event that reoccurring false positives are detected.

DHCP Client and Server Support

Dynamic Host Configuration Protocol (DHCP) is now supported within the PIX Firewall. DHCP is a method of automatically assigning a TCP/IP address from a pool of addresses, to a requesting client. DHCP eliminates the need to manually assign static IP addresses. Implementing DHCP client and server features in the PIX significantly eases deployment into cable and digital subscriber line (DSL) broadband environments, where static IP addresses can be costly and cumbersome to maintain.

DHCP Client

Support for DHCP client allows the PIX to dynamically acquire an untrusted interface's IP address, netmask, and optionally the default route from a DSL or cable Internet service provider (ISP). This feature is most useful when a PIX is directly connected to a DSL or cable modem/router.

DHCP Server

PIX can now provide DHCP services for hosts located on the trusted network, allowing it to automatically assign IP addresses to machines that are configured for dynamic addressing.

Cisco VPN 3000 Client

Remote-access VPN users employing the Cisco VPN 3000 Client, version 2.5, can now securely access their private enterprise network through the PIX Firewall.

Unlike the Cisco Secure VPN Client, the Cisco VPN 3000 Client requires the gateway to push policy information to the VPN 3000 Client. To support the VPN 3000 Client, the Internet Key Exchange (IKE) Mode Config feature within the PIX Firewall has been extended to include the downloading of Domain Name System (DNS), WINS, default domain, and split-tunnel mode attributes to the VPN 3000 Client. The split-tunnel mode allows the PIX Firewall to direct packets to a network interface in clear text form or over an IPsec tunnel in encrypted form. New PIX Firewall commands have been added to allow you to configure client policy attributes to be associated with a VPN group name and downloaded to the VPN 3000 Client(s) that are part of the given group. The purpose of these new commands is to configure the VPN 3000 Client policy groups.

When the VPN 3000 Client initiates ISAKMP with the PIX Firewall, the VPN group name and pre-shared key are sent to the PIX Firewall. The PIX Firewall then uses the group name to look up the configured client policy attributes for the given VPN 3000 Client and downloads the matching policy attributes to the client during the IKE negotiation.

Websense Filtering by User Name and Group

PIX Firewall works in conjunction with Websense Enterprise software to actively filter URLs, thereby controlling which Web sites users can access. New to PIX v5.2 is the ability to enable group and username authentication between a host and a PIX Firewall. The PIX Firewall performs a username

lookup, and then the Websense server handles URL filtering and username logging. Websense protocol version 4 contains the following enhancements:

- URL filtering allows the PIX Firewall to check outgoing URL requests against the policy defined on the Websense server
- Username logging tracks username, group, and domain name on the Websense server
- Username lookup enables the PIX Firewall to use the user authentication table to map the host's IP address to the username

Secure Shell

Historically, remotely configuration of a PIX Firewall involved initiating a Telnet connection. This method allowed as much security as Telnet provided, which is lower-layer encryption (for example, IPsec) and application security (username/password authentication at the remote host). PIX now supports Secure Shell (SSH) version 1. SSH is an application running on top of a reliable transport layer, such as TCP/IP that provides strong authentication and encryption capabilities. SSH supports logging onto another computer over a network, executing commands remotely, and moving files from one host to another.

PIX allows up to five SSH clients to simultaneously access the PIX Firewall console. You can define specific hosts or networks that are authorized to initiate an SSH connection to the PIX Firewall, as well as how long a session can remain idle before being disconnected. SSH is only available with a Data Encryption Standard (DES) or triple DES (3DES) activation key.

Certificate Authority Servers

In addition to supporting the Entrust and Verisign Certification Authority (CA) servers, the PIX Firewall now also supports Baltimore's UniCert Certificate Management System, and Microsoft Windows 2000 Advanced Server.

A CA is a third party that is explicitly trusted to validate identities and to create digital certificates. They are responsible for managing digital certificate requests and issuing certificates to participating IPsec network peers. These services provide centralized key management for the participating peers and simplify the administration of IPsec network devices (peers).

TCP Intercept

With the new TCP intercept feature, PIX provides enhanced protection for systems susceptible to TCP SYN attacks. Once the optional embryonic connection limit is reached, and until the embryonic connection count falls below this threshold, every SYN bound for the affected server is intercepted. For each SYN, PIX Firewall responds on behalf of the server with an empty SYN/ACK segment. PIX Firewall retains pertinent state information, drops the packet, and waits for the client's acknowledgment. If the ACK is received, then a copy of the client's SYN segment is sent to the server and the TCP three-way handshake is performed between PIX Firewall and the server. If and only if, this three-way handshake is completed, the connection resumes as normal. If the client does not respond during any part of the connection phase, then PIX Firewall retransmits the necessary segment using exponential back-offs.

Unicast Reverse Path Forwarding

Due to the potential danger of IP spoofing in the IP protocol, measures need to be taken to reduce this risk when possible. Unicast Reverse Path Forwarding (RPF) or reverse route lookups are a good way to prevent such manipulation under certain circumstances. Unicast RPF is an input function that screens inbound packets arriving on an interface. PIX v5.2 lets you specify which interfaces to protect from an IP spoofing attack using network ingress and egress filtering, which is described in RFC 2267.

Ingress Filtering

Ingress filtering checks inbound packets for IP source address integrity. If the incoming packet does not have a source address that is represented by a route, then it is impossible to know whether the packet arrived on the best possible path back to its origin. This is often the case since routing entities cannot maintain routes for every network.

Egress Filtering

Egress filtering verifies that packets destined for hosts outside the managed domain have IP source addresses verifiable by routes in the enforcing entities' local routing table. If an exiting packet does not arrive on the best return path back to the originator, then the packet is dropped and the activity is logged. Egress filtering prevents internal users from launching attacks using IP source addresses outside of the local domain. Because most attacks use IP spoofing to hide

the identity of the attacking host, egress filtering makes the task of tracing the origin of an attack much easier. When employed, egress filtering enforces that IP source addresses are obtained from a valid pool of network addresses. Addresses local to the enforcing entity are easily traceable.

Configurable Failover Polling

The PIX Firewall stateful failover option ensures high availability and eliminates a single point of failure. With two PIX Firewalls running in parallel, should one malfunction, the second PIX Firewall automatically maintains security operations. By default, the two units send failover "hello" packets to each other every 15 seconds. This data provides the unit identification of Primary or Secondary, the power status of the other unit, and serves as a link for various failover communications between the two units. PIX software v5.2 allows you to configure the interval between failover "hello" packets. The minimum value is three seconds and the maximum is 15 seconds. With a faster poll time, PIX Firewall can detect failure and trigger failover faster.

RADIUS Group Access-Lists

PIX Firewall now accepts user-group attributes from a RADIUS authentication server. After the PIX Firewall authenticates a user, it can now use the Cisco Secure Access Control Server (ACS) ACL attribute returned by the authentication server to identify an access list for a given user group. For example, there could be access lists for each department in an organization (sales, marketing, engineering). To maintain consistency, PIX Firewall also provides the same functionality for TACACS+.

ICMP Access Lists

With Internet Control Message Protocol (ICMP) access lists, the PIX can permit or deny ICMP traffic that terminates at the PIX. Essentially, allowing you to enable or disable pinging to an interface. With pinging disabled, the PIX Firewall is virtually undetectable on the network.

IP Fragmentation

Syslog messages have been added to disclose when the following IP fragmentation (also known as Teardrop) attacks have been detected. PIX will also automatically drop all packet fragments in that same IP ID.

- The PIX Firewall or a system behind it is under an IP fragmentation attack, or the PIX Firewall is legitimately receiving more fragments than it can handle because a threshold was put in place to prevent a fragment attack.
- A fragment arrives that reports itself to be larger than a valid IP packet can be; that is, greater than 65535 bytes. This may indicate an attack designed to break IP stacks with known bugs or a packet arrived from a broken IP stack.
- Appears when an IP fragment is discarded.

PAT IP Address Sharing

Now PIX users can have a single global IP address for an outside interface, as well as port address translation (PAT). This is important for configuring DHCP, allowing for the DHCP retrieved address to be used for PAT. When PAT is enabled on an interface, there should be no loss of TCP, User Datagram Protocol (UDP), and ICMP services. These services allow for termination at the Cisco Secure PIX Firewall's outside interface.

SIP

Session Initiation Protocol (SIP), as defined by the Internet Engineering Task Force (IETF), enables call handling sessions—particularly two-party audio conferences or “calls.” SIP works with Session Description Protocol (SDP), which defines the calls prior to call handling. Using SIP, Cisco Secure PIX Firewall can support voice-over-IP (VoIP) and any proxy server using VoIP. Part of the H.323 version 2 protocol suite, which includes H.245 and H.225 protocols for call negotiation, SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

H.323 V2

H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over Local Area Networks (LANs). H.323 version 2 adds the following functionality to the PIX Firewall:

- Fast Connect or Fast Start Procedure for faster call setup
- H.245 tunneling for resource conservation, call synchronization, and reduced set up time
- Call redirection

Compatibility

VPN Client: Cisco Secure VPN Client version 1.1, or Cisco VPN 3000 Client version 2.5 or later. Both clients can be used with Windows 95, Windows 98, and Windows NT version 4.0.

System Requirements

Hardware	
Random Access Memory	32 MB
Flash Memory	16 MB (PIX 506 requires 8 MB)

Ordering Information

Part Number	Description
PIX-SW-UPGRADE=	PIX Software Upgrade for Non-support Customers

Additional Information

Cisco PIX Firewall

<http://www.cisco.com/go/pix/>

Cisco Enterprise Virtual Private Network Solutions

<http://www.cisco.com/go/evpn/>



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
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
<http://www-europe.cisco.com>
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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/go/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

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0005R) 04/00 LW