

# Cisco Secure PIX<sup>®</sup> Firewall Version 6.0



## Overview

The industry-leading Cisco Secure PIX<sup>®</sup> Firewall Series provides today's networking customers with unmatched security, reliability, and performance. The integrated hardware and software package delivers full stateful firewall protection and IP Security (IPsec) virtual private networking (VPN) capabilities, allowing you to rigorously protect your internal network from outside intrusions. 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 a wide selection of platforms and features, allows the PIX to meet the entire range of customer requirements.

Version 6.0 is the latest release of the Cisco Secure PIX Firewall dedicated operating system (OS). It delivers the latest PIX capabilities, performance, and security improvements, as well as a host of new features.

## PIX Device Manager

The Cisco PIX Device Manager (PDM) is a browser-based configuration tool that enables you to set up, configure, and monitor your PIX Firewall graphically, without requiring an extensive knowledge of the PIX Firewall command-line interface (CLI).

## VPN Client Support Additions

### [Cisco VPN Client v3.0 \(Unified VPN Client Framework\)](#)

Simple to deploy and operate, the Cisco VPN Client enables customers to establish secure, end-to-end encrypted tunnels. The client can be preconfigured for mass deployments, and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the Cisco Secure PIX Firewall and pushed to the client when a connection is established, allowing simple deployment and management as well as high scalability. The Cisco VPN Client supports Windows 95, 98, ME, NT 4.0, and 2000.

### [Layer 2 Tunneling Protocol Support](#)

Cisco Secure PIX Firewall provides the capability to terminate VPN tunnels initiated by the Layer 2 Tunneling Protocol (L2TP) client that is embedded in the Windows 2000 operating system. L2TP allows remote clients to use a public IP network to communicate securely with servers at private corporate networks. L2TP provides authentication, and can be used with IPsec to provide an encrypted and secure tunnel for clients.

## Voice Enhancements

### [Skinny Protocol Support](#)

Cisco Secure PIX Firewall application handling has been enhanced to support the Skinny Client Control Protocol (SCCP), used by Cisco IP phones for VoIP call signaling. This capability dynamically opens pinholes for media sessions and Network Address Translation (NAT)-embedded IP addresses. SCCP supports IP

telephony and can coexist in an H.323 environment. An application layer ensures that all SCCP signaling and media packets can traverse the PIX Firewall and interoperate with H.323 terminals.

#### Session Initiation Protocol Enhancements

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. Enhancements in this release include:

- NAT for User Datagram Protocol (UDP) signaling and Transmission Control Protocol (TCP) signaling messages
- Support for SIP proxies

#### Dynamic Shunning

This feature allows a Cisco Secure PIX Firewall, when combined with a Cisco IDS sensor, to dynamically respond to an attacking host by preventing new connections and disallowing packets from any existing connection. A Cisco Secure IDS device instructs the PIX Firewall to shun sources of traffic when those sources of traffic are determined to be malicious. The shun command applies a blocking function to the interface receiving the attack for a user-defined period of time. Packets containing the IP source address of the attacking host are dropped and logged until the blocking function is removed by the Cisco Secure IDS master unit. No traffic from the IP source address is allowed to traverse the PIX Firewall unit and any remaining connections time out. The blocking function of the shun command is applied whether or not a connection with the specified host address is currently active. Shun statistics are available via show commands, syslog messages, and PIX Device Manager (PDM) monitoring.

#### PAT Port Redirection

The Cisco Secure PIX Firewall now provides static Port Address Translation (PAT) capability, enabling you to send multiple inbound TCP or UDP services to different internal hosts through a single global address. The global address can be a unique address, a shared outbound PAT, or shared with the external interface.

#### Stateful Sharing of HTTP Sessions

The Cisco Secure PIX Firewall supports high availability with the deployment of a redundant hot standby unit. This failover option maintains concurrent connections through automatic stateful synchronization. This ensures that even in the event of a system failure, sessions are maintained and the transition is completely transparent to network users. PIX Firewall version 6.0 adds the ability to maintain HTTP (port 80) sessions.

#### CPU Utilization

The ability to monitor the CPU load on the PIX is added in this version. You can use the show command and PDM monitoring to obtain 5-second, 1-minute, and 5-minute CPU utilization statistics.

#### Port Numbers in Access Control List Syslog Messages

TCP/UDP port numbers have been added to syslog messages that result from packets denied by Access control lists (ACLs).

#### Ten Ethernet Interfaces

To provide the platform extensibility you need without sacrificing the benefits of an embedded system, the Cisco Secure PIX Firewall Series supports single- or four-port 10/100 Fast Ethernet, as well as Gigabit Ethernet network interface cards (NICs). Using PIX software version 6.0, a Cisco Secure PIX Firewall 535 with an unrestricted license can now support up to ten Ethernet interfaces; restricted licenses can support up to eight interfaces.

## Technical Specifications

### 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 Platform:* Cisco Secure PIX Firewall 506, 515, 520, 525, or 535

*Random Access Memory:* 32 MB

*Flash Memory:* 16 MB (PIX 506 requires 8 MB)

## Ordering Information

PIX-CONN-VER= PIX Software Upgrade for Non-Support Customers

## Additional Information

For more information about Cisco Secure PIX Firewall, go to <http://www.cisco.com/go/pix>

For more information about Cisco VPN Client Solutions, go to:

<http://www.cisco.com/warp/public/cc/pd/vpnc/vpncl/>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

[www.cisco.com](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

[www.cisco.com](http://www.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

[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia

[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • 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 • Scotland • Singapore • Slovakia  
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001 Cisco Systems, Inc. All rights reserved. Unity is a trademark, and Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)