



About This Guide

This preface introduces the *Cisco PIX Firewall and VPN Configuration Guide* and contains the following sections:

- [Document Objectives, page xix](#)
- [Audience, page xix](#)
- [Document Organization, page xx](#)
- [Document Conventions, page xxi](#)
- [Obtaining Documentation, page xxi](#)
- [Obtaining Technical Assistance, page xxiii](#)
- [Obtaining Additional Publications and Information, page xxiv](#)

Document Objectives

This document describes how to configure the Cisco PIX Firewall to protect your network from unauthorized use and to establish Virtual Private Networks (VPNs) to connect remote sites and users to your network.

Audience

This guide is for network managers who perform any of the following tasks:

- Managing network security
- Installing and configuring firewalls
- Managing default and static routes, and TCP and UDP services

Use this guide with the installation guide supplied with your PIX Firewall unit.

Document Organization

This guide includes the following chapters and appendixes:

- [Chapter 1, “Getting Started,”](#) describes the benefits provided by PIX Firewall and the technology used to implement each feature.
- [Chapter 2, “Establishing Connectivity,”](#) describes how to establish secure connectivity between an unprotected network, such as the public Internet, and one or more protected networks.
- [Chapter 3, “Controlling Network Access and Use,”](#) describes how to control connectivity between unprotected and protected networks and how to control network use through filtering and other PIX Firewall features.
- [Chapter 4, “Using PIX Firewall in SOHO Networks,”](#) describes how to configure the PIX Firewall as a Cisco Easy VPN Remote device and as a Point-to-Point-Protocol over Ethernet (PPPoE) client. It also describes how to use the PIX Firewall as a Dynamic Host Configuration Protocol (DHCP) server, client, and relay agent.
- [Chapter 5, “Configuring Application Inspection \(Fixup\),”](#) describes how the application inspection function enables the secure use of specific applications and services.
- [Chapter 6, “Configuring IPSec and Certification Authorities,”](#) describes how to configure the PIX Firewall to support Virtual Private Networks (VPNs).
- [Chapter 7, “Site-to-Site VPN Configuration Examples,”](#) provides examples of using PIX Firewall to establish site-to-site VPNs.
- [Chapter 8, “Managing VPN Remote Access,”](#) describes how to configure the PIX Firewall as an Easy VPN Server and how to configure Easy VPN Remote software clients. It also describes how to configure the PIX Firewall to support remote PPTP clients.
- [Chapter 9, “Accessing and Monitoring PIX Firewall,”](#) describes how to implement, configure, and integrate PIX Firewall system management tools.
- [Chapter 10, “Using PIX Firewall Failover,”](#) describes how to implement and configure the failover feature.
- [Chapter 11, “Changing Feature Licenses and System Software,”](#) describes how to upgrade or downgrade your PIX Firewall software image and feature license.
- [Appendix A, “Acronyms and Abbreviations,”](#) lists the acronyms and abbreviations used in this guide.
- [Appendix B, “Configuration Examples for Other Remote Access Clients”](#) describes how to use PIX Firewall with different remote access clients, including MS Windows 2000/L2TP and Cisco Secure VPN Client Version 1.1.
- [Appendix C, “MS-Exchange Firewall Configuration,”](#) describes how to configure PIX Firewall to handle mail transfers across the PIX Firewall from Windows NT Servers on protected and unprotected networks.
- [Appendix D, “TCP/IP Reference Information,”](#) lists the IP addresses associated with each subnet mask value.
- [Appendix E, “Supported VPN Standards and Security Proposals,”](#) lists the standards supported for IPSec, IKE, and certification authorities (CA).

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in *screen* font.
- Information you need to enter in examples is shown in **boldface screen** font.
- Variables for which you must supply a value are shown in *italic screen* font.

Graphic user interface access uses these conventions:

- **Boldface** indicates buttons and menu items.
- Selecting a menu item (or screen) is indicated by the following convention:
Click **Start>Settings>Control Panel**.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/en/US/support/index.html>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/en/US/doctypes/prod_series_index_listing_sitecopy.html

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

