



About This Guide

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

- [Document Objectives](#)
- [Audience](#)
- [Document Organization](#)
- [Document Conventions](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

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, “Configuring Application Inspection \(Fixup\),”](#) describes how the application inspection function enables the secure use of specific applications and services.
- [Chapter 5, “Using PIX Firewall in SOHO Networks,”](#) describes how to configure the PIX Firewall as a VPN, PPPoE, or DHCP client and how to use the PIX Firewall DHCP server on its inside interface.
- [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, “Configuring VPN Client Remote Access,”](#) describes specific configuration for using PIX Firewall to establish a remote access VPN and provides configuration examples.
- [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, “Firewall Configuration Forms,”](#) provides forms you can use to plan a configuration before starting to create a configuration.
- [Appendix B, “Acronyms and Abbreviations,”](#) lists the acronyms and abbreviations used in this guide.
- [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,”](#) lists the standards supported for IPSec, IKE, and certification authorities (CA).
- [Appendix F, “Converting Private Link to IPSec,”](#) describes the procedure for converting a Private Link VPN to IPSec.

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

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following 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 is 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.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM 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 corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following 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 types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- 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.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you 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 Web Site, go to the following URL:

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

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires 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 the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

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

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

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). In addition, please have available your service agreement number and your product serial number.