Installation and Configuration for Common Criteria EAL4 Evaluated Cisco PIX Firewall Version 6.2(2)

January 2003

Contents

This document describes how to install and configure the Cisco PIX Firewall 501, 506/506E, 515/515E, 520, 525 and 535 for use with PIX Firewall software Version 6.2(2) as certified by Common Criteria Evaluation Assurance Level 4 (EAL4).

Note Failure to follow the information provided in this document will result in the PIX Firewall not being compliant with the evaluation and may make it insecure.

This document includes the following sections:

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

Introduction

This document is an addendum to the Cisco PIX Firewall Version 6.2 documentation set, which should be read prior to configuring a PIX Firewall.

Cisco product documentation includes:

- Configuration Guides, which provide a descriptive overview of functions, the commands needed to enable them, and the sequence of operations that should be followed to implement them. The configuration guide should be consulted first when enabling features and functions.
- Command References, which provide a complete and detailed summary of all configuration commands and options, their effects, and examples and guidelines for their use. The command references should be consulted to confirm detailed syntax and functionality options.
- Error Message summaries, which describe all error messages issued by the product.

The following PIX Firewall Version 6.2 documentation is referenced in this document:

- *Cisco PIX Firewall Release Notes, Version 6.2(2)*
- *Cisco PIX 501 Firewall Quick Start Guide, Version 6.2*
- *Cisco PIX 506/506E Firewall Quick Start Guide, Version 6.2*
- *Cisco PIX Firewall Hardware Installation Guide, Version 6.2*
- *Cisco PIX Firewall and Configuration Guide, Version 6.2*
- *Cisco PIX Firewall Command Reference, Version 6.2*
- *Cisco PIX Firewall System Log Messages, Version 6.2*
- *Regulatory Compliance and Safety Information for the Cisco PIX Firewall, Version 6.2*

The Cisco PIX Firewall documentation is available on CD-ROM, in printed-paper form, and online (in both HTML and PDF formats). This document should be used in conjunction with the August 2002 edition of the CD-ROM based documentation. The preceding PIX Firewall documents listed can be found on the CD-ROM:

Network Security >Cisco Security Products >Cisco PIX Firewall >Cisco PIX Firewall OS Software >Version 6.2

Per-platform hardware documentation can be found on the CD-ROM under:

>Network Security >Cisco Security Products >Cisco PIX Firewall >Cisco PIX Firewall OS Software >Version 6.2 > Cisco PIX Firewall Hardware Installation Guide

Audience

This document is written for administrators configuring Common Criteria Certified Cisco PIX Firewall Version 6.2(2) software. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

Supported Hardware and Software Versions

Only the following combinations of hardware listed in Table 1are compliant with the PIX Firewall 6.2(2) EAL4 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than Cisco PIX Firewall Version 6.2(2) will invalidate the secure configuration.

Table 1 Supported Hardware for the Certified PIX Firewall

Models	Optional Hardware Modules	Maximum Number of Interfaces
PIX 501	None	5
PIX 506/506E	None	2
PIX 515[1]/515E[1]	PIX-1FE PIX-4FE	6
PIX 520[1]	PIX-1FE PIX-4FE PIX-1GE-66	6
PIX 525[1]	PIX-1FE PIX-4FE PIX-1GE-66	8
PIX 535[1]	PIX-1FE PIX-4FE PIX-1GE-66	10

1. These models may have AC or DC power supplies.

Security Information

In addition to the *Regulatory Compliance and Safety Information* documentation, the sections that follow provide additional security information for use with a Common Criteria Certified Cisco PIX Firewall.

Organizational Security Policy

Ensure that your PIX Firewall is delivered, installed, managed, and operated in a manner that maintains an organizational security policy. The *Cisco PIX Firewall and VPN Configuration Guide Version 6.2* provides guidance on how to define a security policy.

Security Implementation Considerations

The sections that follow provide implementation considerations that need to be addressed to administer the PIX Firewall in a secure manner.

Certified Configuration

Only Version 6.2(2) of the PIX Firewall software can be used. Only the hardware version combinations listed in Table 1 can be used to implement an evaluated configuration. Changing the software to a different version invalidates the evaluated status of a particular hardware platform.

The Certified Common Criteria PIX Firewall Version 6.2(2) does not support the following features:

- Cut-through proxies
- Failover
- Routing Information Protocol (RIP)
- Remote Management, except via Telnet from a trusted host on an inside interface
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP) Server
- Virtual Private Networks (VPNs)
- Authentication, authorization and accounting (AAA) server to provide identification and authentication

All other hardware and software features and functions of the PIX Firewall are included in the evaluated product configuration and thus can be used in conjunction with the Target of Evaluation (TOE) Security Functions as long as the TOE functions are configured, operated, and managed in accordance with this document.

The configuration of the PIX Firewall should be reviewed on a regular basis to ensure that the configuration continues to meet the organizational security policy in the face of the following:

- Changes in the PIX Firewall configuration
- Changes in the organizational security policy
- Changes in the threats presented from the untrusted network(s)
- Changes in the administration and operation staff or the physical environment of the PIX Firewall

Physical Security

The PIX Firewall must be located in a physically secure environment to which only a trusted administrator has access. The secure configuration of a PIX Firewall can be compromised if an intruder gains physical access to the PIX Firewall. Similarly, any hosts that are used to administer the PIX Firewall via Telnet must be protected either physically or with suitable identification/authentication mechanisms to ensure that only trusted administrators have access.

Administration Access

There are only two methods by which the administrator can manage the PIX Firewall:

- Using the serial interface directly connected to the PIX Firewall
- Using a Telnet session from a trusted host on any internal interface of the PIX Firewall

Access Control

You must set the enable mode password using the **enable password** command. A strong password has a combination of alpha and numeric characters as well as punctuation characters. This password must be at least eight characters. Write down your password and store it in a manner consistent with your site's security policy. Once you change this password, you cannot view it again. Also, ensure that all who access the PIX Firewall console are given this password. If you lose your password, you must contact Cisco TAC.

Servers and Proxies

To ensure complete security when the PIX Firewall is shipped, inbound access to all proxies and servers is initially disabled. After the installation, you must explicitly permit each service and enable the services necessary for your security policy. Refer to the *Cisco PIX Firewall and VPN Configuration Guide Version 6.2* for information on how to configure the PIX Firewall. Certification requires a completely controlled environment in which specified services are allowed and all others denied.

Logging and Messages

Monitoring activity in the log files is an important aspect of your network security and should be conducted regularly. Monitoring the log files lets you take appropriate and timely action when you detect security breaches or events that are likely to lead to a security breach in the future. Use the **logging** command to view log files messages. Refer to the *Cisco PIX Firewall and VPN Configuration Guide, Version 6.2* for information on logging, messaging, and archiving.

Access Lists

The **access-list** command operates on a first-match basis. Therefore, the last rule added to the access list is the last rule checked. Administrators must take note of this when entering the initial rules during the configuration, as it may impact the remainder of the rule parsing.

Note The associated **object-group** command was not evaluated and should not be configured on a certified PIX Firewall.

Trusted and Untrusted Networks

The PIX Firewall can be used to isolate your network from the Internet or from another network. A trusted network is usually your internal network and an untrusted network may be the Internet or any other network. Therefore, the PIX Firewall must be configured so that it acts as the only network connection between your internal network and any external networks. The PIX Firewall will deny any information flows for which no rule is defined. Your security implementation is based on the control of traffic from one network to the other, and should support your security policy.

Public Access Servers

If you are planning to host public access servers, you must decide where they will be located in relation to the PIX Firewall. Placing servers on the network outside the PIX Firewall leaves them open to attack. Placing servers on the internal network means you must open up your PIX Firewall to allow access.

Using FTP

File Transfer Protocol (FTP) is used to retrieve or deposit files on a remote system. Allowing users to access internal FTP servers directly opens the door for abuse. Use of this service should be of concern when designing your security policy.

Monitoring and Maintenance

The PIX Firewall software provides several ways to monitor the PIX Firewall, from logs to messages.

- Ensure you know how you will monitor the PIX Firewall, both for performance and for possible security issues.
- Plan your backups. If there should be a hardware or software problem, you may need to restore the PIX Firewall configuration.
- The configuration of the PIX Firewall should be reviewed on a regular basis to ensure that the configuration meets the organization's security objectives in the face of the following:
  - Changes in the PIX Firewall configuration
  - Changes in the security objectives
  - Changes in the threats presented by the external network.

Auditing Component Requirements

The PIX Firewall interacts with Windows NT for the purpose of storing the audit data. The server should be running Windows NT 4.0 with Service Pack 6a. The auditing machine will provide suitable audit records to the administrator, protect the stored audit records from unauthorized deletion, and will detect modifications to the audit records. It is the responsibility of the administrator to regularly review the audit records provided by the PIX Firewall, and to take any relevant action as necessary to ensure the security of the PIX Firewall. The location of the auditing machine and records should only be accessible to the administrator.

Determining the Software Version

Use the **show version** command to verify the software version of your PIX Firewall unit.

Installation Notes

The following sections in the *Cisco PIX Firewall Hardware Installation Guide* should be followed when installing a certified PIX Firewall:

- *Preparing for Installation* describes the installation overview, safety recommendations, and general site requirements.
- *PIX 501* describes the PIX 501 product overview, and the installation and configuration procedures.
- *PIX 506/506E* describes the PIX 506/506E product overview, installation and configuration, as well as how to connect the PIX 506/506E to a power supply.
- *PIX 515/515E* describes the PIX 515/515E product overview, installation and configuration of the PIX 515/515E, as well as the procedure to remove and replace the chassis cover. This chapter also includes installation procedures for the circuit board and installation of the DC model.
- *PIX 520* describes the PIX 520 product overview, installation, and configuration of the PIX 520, as well as the procedure to remove and replace the chassis cover. This chapter also includes the procedure for installation of the DC model.
- *PIX 525* describes the PIX 525 product overview, installation, and configuration of the PIX 525, as well as the procedure to remove and replace the chassis cover. This chapter also includes installation procedures for the circuit board and installation of the DC model.
- *PIX 535* describes the PIX 535 product overview, installation, and configuration of the PIX 535, as well as the installation procedure for the circuit board and installation of the DC model.

Verification of Image and Hardware

To verify that the PIX Firewall software and hardware was not tampered with during delivery, complete the following steps:

Step 1 Before unpacking the PIX Firewall, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the PIX Firewall on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be will be that of the PIX Firewall. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the PIX Firewall is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 7 There are three alternatives for obtaining a Common Criteria evaluated software image:

- Download a Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/pix
- The PIX Firewall ships with a CD containing all current software images. The Common Criteria evaluated software image Version 6.2(2) is available on this CD.
- Customers can order a CD with all of the current software images from Cisco.com. The part number for this item is PIX-SW-UPGRADE=. There is a charge for this option.

Step 8 Download the pix622.bin file.

Step 9 Once the file is downloaded, verify that it was not tampered with by using an MD5 utility to compute an MD5 hash for the downloaded file and comparing this with the MD5 hash for the image listed in this document or from the Certification Report published by CESG which is available on their website. If the MD5 hashes do not match, contact Cisco TAC.

Figure 1 Example from Cisco Website Showing PIX Firewall Image Details with MD5 Hash Value

Details	
Release	6.2.2.ED
Description	Binary REQUIRES 32 MB RAM AND 8MB FLASH
Size	1658880
BSD Checksum	54684
Router Checksum	0x9ec1
MD5	abf75efd73b4003ba85f334a779a2188
Date Published:	28-JUN-2002

83872

Step 10 Install the downloaded and verified software image onto your PIX Firewall as described in "Installing the Software" in the *Cisco PIX Firewall and VPN Configuration Guide, Version 6.2*.

Step 11 Start your PIX Firewall as described in the *Cisco PIX Firewall and VPN Configuration Guide, Version 6.2*. Confirm that your PIX Firewall loads the image correctly and completes internal self-checks. At the prompt, enter the **show version** command as follows. Verify that the version is 6.2(2). If the PIX Firewall image fails to load, or if the PIX Firewall version is not 6.2(2), contact Cisco TAC.

The following is a sample output from the "**show version**" command output, showing the PIX Firewall release version:

```
pixfirewall> show version
Cisco PIX Firewall Version 6.2(2)
Compiled on Fri 07-Jun-02 17:49 by xxxx
pixfirewall up 9 mins 52 secs
Hardware: PIX-506, 32 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 8MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
0: ethernet0: address is 0004.2746.0b82, irq 11
1: ethernet1: address is 0004.2746.0b83, irq 10
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES: Enabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Limited
IKE peers: Unlimited
Serial Number: 480440942 (0x1ca2f26e)
Running Activation Key: 0xe26a8a59 0xd27673a9 0x8e1fd37f 0x193fcfb0
Configuration last modified by enable_15 at 07:27:01.784 UTC Wed Jul 17
2002
pixfirewall>
```

Configuration Notes

This section contains the following topics:

Saving Your Configuration

The **write memory** command should be used frequently when making changes to the configuration of the PIX Firewall. If the PIX Firewall reboots and resumes operation when uncommitted changes were made, these changes will be lost and the PIX Firewall will revert to the last configuration saved.

Using the Established Command

Administrators are advised not to use the **established** command on the certified PIX Firewall. Incorrect use of this command may give outside users greater access to inside systems than is intended, and for this reason its use is not recommended. For more details go to the following website:

http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/products_security_advisory09186a0080094293.shtml

Enabling Timestamps

By default, all audit records are not stamped with the time and date, which are generated from the system clock when an event occurs. The certified PIX Firewall requires that the timestamp option is enabled. To enable the timestamp of audit events, use the **logging timestamp** command. To ensure that the timestamp option remains the default, use the **write memory** command to save the option into the startup configuration.

Enabling Reliable Logging

By default, auditing events are transported to the remote syslog server over UDP. The certified PIX Firewall requires auditing events to be transported over TCP. The TCP option is configured using the **logging host** interface *ip_address* **tcp**/*port_number* command. With TCP logging configured, new sessions through the certified PIX Firewall will be disallowed if log messages cannot be forwarded to the remote host.

To facilitate the TCP logging function, the PIX Firewall Syslog Server (PFSS) must be configured on a secure Windows NT server. For details on how to obtain and configure PFSS, see "Using the PIX Firewall Syslog Server"

Systems Logs

Cisco PIX Firewall System Log Messages provides details on the PIX Firewall system logs. The following sections are not supported on a certified PIX Firewall:

- PIX Firewall System Log
  - Receiving SNMP requests
  - Sending SNMP Traps
- Other Remote Management and Monitoring Tools
  - Cisco PIX Device Manager
  - Cisco Secure Policy Manager
  - SNMP Traps

Note Telnet is supported on a certified PIX Firewall.

Using the PIX Firewall Syslog Server

The PIX Firewall Syslog Server (PFSS) lets you view syslog messages from a Windows NT system. If you have a Windows NT system, use of the PFSS gives you the additional benefit of reliability through receiving TCP event messages, receiving time-stamped messages, and being able to monitor whether the server is up or down from the PIX Firewall. The PFSS is available without cost from Cisco. com. Installation instructions for the PFSS are provided in the *Installation Guide for the Cisco Secure PIX Firewall, Version 5.2*.

If your PIX Firewall is sending syslog messages via TCP to a PFSS and the Windows NT system disk becomes full, the PIX Firewall will stop all new connections. If you are logging via UDP, the PIX Firewall does not check whether the disk becomes full.

Unless you require that every syslog message sent must be stored on the PFSS, and you can afford the possible network downtime to free the Windows NT disk space, only use UDP logging. If you use TCP logging, ensure that PFSS log files are backed up regularly to minimize the possibility of running out of disk space.

This section contains the following topics:

Configuring PFSS

Complete the following steps to configure the PIX Firewall to use PFSS:

Step 1 If you want to use the reliable syslog feature of the PFSS, whereby the PIX Firewall stops its traffic if the PFSS Windows NT disk becomes full or the system is unavailable, use the tcp option:

```
logging host interface ip_address tcp/port_number
```

Replace interface with the interface on which the server exists, *IP-address* with the IP address of the host, and *port-number* with the TCP port (if different than the default value of 1468). You can verify that the PIX Firewall traffic is disabled due to a PFSS disk-full condition by using the **show logging** command and looking for the “disabled” keyword in the display.

Only one UDP or TCP command statement is permitted for a server. A subsequent command statement overrides the previous one. Use the **write terminal** command to view the **logging host** command statement in the configuration. In the configuration, the UDP protocol appears as “17” and TCP as “6.”

Step 2 Set the logging level with the **logging trap** command:

```
logging trap debugging
```

We recommend that you use the debugging level during initial setup and during testing. Thereafter, set the level from debugging to errors for production use.

Step 3 If needed, set the **logging facility** command to a value other than its default of 20. Most UNIX systems expect the messages to arrive at facility 20, which receives the messages in the local4 receiving mechanism.

Step 4 Start sending messages with the **logging on** command. To disable sending messages, use the **no logging on** command.

If you want to stop sending a message to the syslog server, use the **no logging** *message syslog_id* command. Replace *syslog_id* with a syslog message ID.

Step 5 If you want to send time-stamped messages to the PFSS, use the **clock set** command to set the PIX Firewall system clock and the **logging timestamp** command to enable time stamping. For example:

```
clock set 14:25:00 apr 1 2000
logging timestamp
```

In this example, the clock is set to the current time of 2:25 pm on April 1, 1999, and time stamping is enabled. To disable time-stamp logging, use the **no logging timestamp** command.

Changing PFSS Parameters at the Windows NT System

You can change PIX Firewall Syslog Server (PFSS) parameters at the Windows NT system by clicking **Start>Settings>Control Panel>Services**.

All PFSS parameter values can be viewed by examining the pfss.log file, which PFSS creates in the same directory as the PFSS log files.

The PFSS starts immediately after installation. You can use the Services control panel to enter new parameters, pause the service and then resume the service, or to stop and start the service.

Choose one or more parameters from the following:

- d%_disk_full—The maximum percentage of how full the Windows NT system disk can become before PFSS causes the PIX Firewall to stop transmissions. This is an integer value in the range of 1 to 100. The default is 90.
- t tcp_port—The port that the Windows NT system uses to listen for TCP syslog messages, the default is 1468. If you specify another port, it must be in the range of 1024 to 65535.
- u udp_port—The port that the Windows NT system uses to listen for UDP syslog messages, the default is 514. If you specify Another port, it must be in the range of 1024 to 65535.
- e disk_empty_watch_timer—The duration, in seconds, that PFSS waits between checks to see if the disk partition is still empty. The default is 5 seconds, the range is any number greater than zero.
- f disk_full_watch_timer—The duration, in seconds, that PFSS waits between checks to see if the disk partition is still full. The default is 3 seconds, the range is any number greater than zero.

Follow these steps to set%_disk_full to 35 percent and the disk-full timer to 10 seconds:

Step 1 Open the Services control panel.

Step 2 Click the PIX Firewall Syslog Server service.

Step 3 In the **Startup Parameters** edit box, type `-d 35 -f 10`.

Step 4 Click **Start**. Pressing the **Enter** key closes the Services control panel and does not change the parameters.

PFSS stores syslog messages in one of seven files: monday.log, tuesday.log, wednesday.log, thursday.log, friday.log, saturday.log, sunday.log (according to the day of the week). If a week has already passed since the last log file was created, it will rename the old log file to weekday.mmddyy where weekday is the current day, mm is the month, dd is the day, and yy is the year; for example, monday.103099.

Note PFSS truncates syslog messages longer than 512 characters in length.

Recovering from PFSS Disk-Full

If you have specified that the PIX Firewall send syslog messages via TCP, the Windows NT disk may become full and the PIX Firewall unit will stop its traffic. If the Windows NT file system is full, the Windows NT system beeps and the PFSS disables all TCP connections from the PIX Firewall unit(s) by closing its TCP listen socket.

The PIX Firewall tries to reconnect to the PFSS five times, and during the retry, it stops all new connections through the PIX Firewall. You then need to back up all the log files to another disk or across the network. (While PFSS is receiving messages, the log files must reside on the local disk.)

Complete these steps to recover from the disk-full condition:

Step 1 Back up the files on the Windows NT system.

Step 2 On the PIX Firewall, check that syslog is disabled with the **show logging** command. If the syslog server has disabled the connection, the display contains the “disable” keyword.

Step 3 Disable logging to the PFSS with the **no logging host** command:

```
no logging host dmz1 10.1.1.2
```

Step 4 Restart logging with the **logging host** command:

```
logging host dmz1 10.1.1.2 tcp/1468
```

Step 5 Check that the server is now enabled with the **show logging** command. The “disabled” keyword should no longer be visible.

MD5 Hash Value for the PIX Firewall

The MD5 hash value for the Cisco PIX Firewall 6.2(2) image follows:

abf75efd73b4003ba85f334a779a2188

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/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites 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 regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions 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/univercd/cc/td/doc/es_inpck/pdi.htm

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) 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 send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) 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

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

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 quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating 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. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation" section..