



Release Notes for the Cisco Secure PIX Firewall Version 5.3(2)

August 2001

Contents

This document includes the following sections:

- Introduction
- System Requirements
- New and Changed Information
- Command Changes
- Syslog Messages
- Documentation Changes
- Important Notes
- Caveats
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

Introduction

This release note describes the new features, restrictions, and caveats for the Cisco Secure PIX Firewall 5.3(2) release.



System Requirements

The following sections describe the system requirements for operating a PIX Firewall unit with version 5.3(2) software.

Memory Requirements



Note

All PIX Firewall units *must* have at least 32 MB of RAM memory or the PIX Firewall unit will not boot. In addition, all units except the PIX 506 must have at least 16 MB of Flash memory to boot. The PIX 506 has 8 MB of Flash memory, which works correctly with version 5.3.

The following table lists Flash memory requirements for this release:

PIX Firewall Model	Flash Memory Required in 5.3	Flash Memory Sold with Unit
PIX 506	8 MB	8 MB (not upgradeable)
PIX 510 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX 515, PIX 525, PIX 535	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 10000 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX Firewall Classic (discontinued)	16 MB	512 KB or 2 MB (must be upgraded to 16 MB)

Software Requirements

The following is required for version 5.3(2):

1. The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, you need to download the Boothelper file, bh531.bin, from Cisco Connection Online (CCO) to let you download the PIX Firewall image with TFTP.
 - If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must have an activation (license) key that enables Data Encryption Standard (DES) or the more secure 3DES.

To obtain a DES (56-bit) license key for the PIX Firewall, use the IPSec 56-bit Customer Registration form. Accessing this form requires prior registration on Cisco.com at <http://www.cisco.com/register>. However, access to this form does not require a purchase or service contract. You can register as a guest and then proceed to fill out the form. The form is available at the following website:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>

You must purchase a 3DES (168-bit) license key, or have a service contract, to obtain a 3DES license key. If you have already purchased a 3DES upgrade, and you have your Cisco PIX Firewall 3DES upgrade document with the entitlement number printed on it, you can register your license

key for use on your PIX Firewall with the License Registration form. Accessing this form also requires prior registration on Cisco.com at <http://www.cisco.com/register>. The License Registration form is available at the following website:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=301>

You must also purchase or have a service contract to download PIX Firewall software.

2. If you are using PFSS (PIX Firewall Syslog Server), Cisco recommends you install Windows NT Service Pack 6. PFSS is not supported on Windows 2000.
3. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* for new installation requirements.

Cisco IOS Software Interoperability

The PIX Firewall supports Cisco IOS Release 12.0(6)T or later.

Cisco Secure Policy Manager Interoperability

Cisco Secure Policy Manager (Cisco Secure PM), version 2.1, provides policy-based management support for PIX Firewall units running version 4.2, 4.4, and 5.1 software images. Cisco Secure PM version 2.2 supports PIX Firewall version 5.3.

Refer to the documentation set for Cisco Secure PM at the following website:

<http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/index.htm>

Cisco VPN Secure Client Interoperability

PIX Firewall version 5.3 requires Cisco Secure VPN Client version 1.1. The Cisco Secure VPN Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco Secure VPN Client is not supported for use with Windows 2000.

Cisco VPN 3000 Concentrator and Client Interoperability

PIX Firewall version 5.3 requires Cisco VPN 3000 Client version 2.5 and Cisco VPN 3000 Concentrator version 2.5.2 or later. The Cisco VPN 3000 Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco VPN 3000 Client is not supported for use with Windows 2000.

PIX Firewall Manager Interoperability

You can use PIX Firewall version 5.3 with the PIX Firewall Manager version 4.3(2)h. Refer to the *Release Notes for the PIX Firewall Manager Version 4.3(2)* for more information. You can view this document online at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>

The PIX Firewall Manager (PFM) lets you manage PIX Firewall units; however, it does not let you configure any PIX Firewall features added after version 4.3(2). PFM is not supported on Windows 2000.

The “Frequently Asked Questions” section in the PFM release notes provides useful troubleshooting information.

Determining the Software Version

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

Upgrading to a New Software Release

If you have a Cisco Connection Online (CCO) login, you can obtain software from the following website:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>

New and Changed Information

The following describes the new software and hardware information in this 5.3(1) release.

New Hardware Features in Release 5.3(1)

The sections describe the new hardware features in the 5.3(1) release.

VPN Accelerator

The VPN Accelerator (PIX-VPN-ACCEL) is a new encryption accelerator board. For more information on the VPN Accelerator, refer to the *Installation Guide for the Cisco Secure PIX Firewall Version 5.3*. Observe the following before installing the VPN Accelerator:

- Do not use a Private Link board and a VPN Accelerator in the same PIX Firewall chassis. If your PIX Firewall has a Private Link board installed, you should remove the Private Link board before installing the VPN Accelerator.
- The VPN Accelerator uses a PCI interface and therefore can only be installed in PIX Firewall platforms with PCI slots.
- Before downgrading from version 5.3(1) to an earlier version, remove the VPN accelerator board from your PIX Firewall unit. The PIX 535 cannot be downgraded to earlier versions.

PIX 535

The new PIX 535 model has the fastest performance and highest capacity of any of the PIX Firewall series.

The following practices must be followed to achieve the best possible system performance on the PIX 535:

- PIX-1GE-66 interface cards should be installed first in the 64-bit/66 MHz buses before they are installed in the 32-bit/33 MHz bus. If more than four PIX-1GE-66 cards are needed, they may be installed in the 32-bit/33 MHz bus but with limited potential throughput.
- PIX-1GE and PIX-1FE cards should be installed first in the 32-bit/33 MHz bus before they are installed in the 64-bit/66 MHz buses. If more than five PIX-1GE and/or PIX-1FE cards are needed, they may be installed in a 64-bit/66 MHz bus but doing so will lower that bus speed and limit the potential throughput of any PIX-1GE-66 card installed in that bus.

The PIX-1GE Gigabit Ethernet adaptor is supported in the PIX 535; however, its use is strongly discouraged because maximum system performance with the PIX-1GE card is much lower than that with the PIX-1GE-66 card. The software displays a warning at boot time if a PIX-1GE is detected.

The following table summarizes the performance considerations of the different interface card combinations.

Figure 1 Gigabit Ethernet Interface Card Combinations

Interface Card Combination	Installed In Interface Slot Numbers	Potential Throughput
Two to four PIX-1GE-66	0 through 3	Best
PIX-1GE-66 combined with PIX-1GE or just PIX-1GE cards	0 through 3	Degraded
Any PIX-1GE-66 or PIX-1GE	4 through 8	Severely degraded



Caution

The PIX-4FE and PIX-VPN-ACCEL cards can only be installed in the 32-bit/33 MHz bus and must never be installed in a 64-bit/66 MHz bus. Installation of these cards in a 64-bit/66 MHz bus may cause the system to hang at boot time.



Caution

If Stateful Failover is enabled, the interface card and bus used for the Stateful Failover LAN port must be equal to or faster than the fastest card used for the network interface ports. For example, if your inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then your Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. A PIX-1GE or PIX-1FE card cannot be used in this case, nor can a PIX-1GE-66 card installed in bus 2 or sharing bus 1 with a slower card.

Additionally, observe the following before installing the PIX 535:

- PIX 535 only supports PIX Firewall software version 5.3 or later. Installing a version earlier than 5.3 using the **copy tftp flash** command causes a condition in which the PIX 535 fails repeatedly. Should this occur, when the PIX 535 unit restarts, press the Escape key on your console workstation to access Monitor mode and load version 5.3 or later before proceeding with the startup.
- A PIX 535 configured with only Gigabit interfaces will not be capable of upgrading an Activation key. Activation key upgrades require Monitor mode for all systems without floppy disk drives. Monitor mode does not support Gigabit interfaces. A Fast Ethernet interface must be installed to use Monitor mode.

A PIX 535 with Gigabit Ethernet should be populated only with PIX-1GE66 Gigabit Ethernet adaptors. The PIX-1GE functions, but with significantly reduced throughput (about 50 percent). The software displays a warning if a PIX-1GE is detected.

If a PIX 535 is ordered with Gigabit interfaces only, an additional Fast Ethernet interface is included with the unit so that the Activation key may be upgraded.

- For the PIX 535, the only supported Ethernet interface types are the i82558 or i82559. You can view the interface type in the second line of the **show interface** command output. The correct interface type displays as “Hardware is i82558 ethernet” or “Hardware is i82559 ethernet.”

For more information on the PIX 535, refer to the *Installation Guide for the Cisco Secure PIX Firewall Version 5.3*.

The PIX 535 provides the following features:

Features	PIX 535—R	PIX 535—UR
Failover	No	Yes
RAM	512 MB	1 GB
Flash memory	16 MB	16 MB
Maximum interfaces	8	10
Supported Interfaces	Fast Ethernet, Gigabit Ethernet, and VPN Accelerator	
Power Supplies	Dual, redundant, hot-swappable AC power supplies	

New Software Features in Release 5.3(1)

The following features are new in version 5.3(1):

- **DHCP**—DHCP Server now supports 32 clients instead of 10 clients.
- **nat 0 access list**—There is no longer a restriction on having **nat 0 access-list** and **nat 0** (Identity NAT) configured at the same time. Both **nat 0** and **nat 0 access-list** may be configured concurrently.
- **RIP Version 2**—RIP Version 2 multicast is now supported on the PIX Firewall.

Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* for complete information about each software feature. IPsec features are described in the *IPsec User Guide for the Cisco Secure PIX Firewall Version 5.3*.

Command Changes

1. **sysopt connection enforcesubnet**—This command has been deleted from the Command Line Interface.
2. **show eeprom**—Displays the current PIX Firewall eeprom contents.
eeprom update—Update the eeprom contents.
3. Global RADIUS port definition option:

aaa-server radius-authport <authport>—Specifies RADIUS server authentication.

aaa-server radius-acctport <acctport>—Specifies RADIUS server accounting.

This is a global setting that specifies the ports the RADIUS service should use. The default ports are 1645 for authentication and 1646 for accounting as defined in RFC 2058. Newer RADIUS servers may use the port numbers 1812 and 1813 as defined in RFC 2138 and 2139. If your server uses ports other than 1645 and 1646, then you should define ports using the **aaa-server radius-authport** and **aaa-server radius-acctport** commands prior to starting the RADIUS service with the **aaa-server** command.

Syslog Messages

The following are new or changed syslog messages in PIX Firewall software version 5.3(1):

- %PIX-3-305008—Free unallocated global IP detected
- %PIX-2-211002—Failed to allocate channel

This syslog message, %PIX-2-211002, is no longer used.

- The following message has been changed from:

```
%PIX-2-106002:protocol# Connection denied by outbound list
list_ID src laddr/lport dest faddr/fport
```

Explanation This is a connection-related message. This message is logged if the specified connection fails because of an **outbound deny** command statement. The *protocol#* variable is 1 for ICMP, 6 for TCP, and 17 for UDP.

To the following:

```
%PIX-2-106002:protocol Connection denied by outbound list
list_ID src laddr dest faddr
```

Explanation This is a connection-related message. This message is logged if the specified connection fails because of an **outbound deny** command statement. The *protocol* variable can be ICMP, TCP, or UDP.

- The following message has been changed from:

```
%PIX-3-106010:Deny inbound from outside:IP_addr to inside:IP_addr chars
```

To the following:

```
%PIX-3-106010:Deny inbound icmp src outside:IP_addr dst inside:IP_addr (type dec, code dec)
```

- The following message has been changed from:

```
%PIX-3-305006:Invalid dst is network/broadcast IP, translation creation failed for protocol src
int_name:IP_addr dst int_name:IP_addr.
```

To the following:

```
%PIX-3-305006:Regular translation creation failed for protocol src int_name:IP_addr/port dst
int_name:IP_addr/port
```

All syslog messages are described in the *System Log Messages for the Cisco Secure PIX Firewall Version 5.3* document.

Documentation Changes

AAA

The **clear aaa** command is shown in the “Command Reference” chapter of the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* as follows:

```
clear aaa [accounting include | exclude authen_service inbound | outbound | if_name group_tag]
```

```
clear aaa [authentication include | exclude authen_service inbound | outbound | if_name local_ip
local_mask foreign_ip foreign_mask group_tag]
```

The description of this command should be shown with a bracket before the **include** and after **exclude**, and before **inbound** and after **outbound**:

```
clear aaa [accounting [include | exclude] authen_service [inbound | outbound] if_name group_tag]
```

```
clear aaa [authentication [include | exclude] authen_service [inbound | outbound] if_name local_ip
local_mask foreign_ip foreign_mask group_tag]
```

Configuring Failover

There is a change in the failover installation instructions in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3*. In the printed document, this change is in the section, “Configuring Failover” in Chapter 3, “Advanced Conversations.” This change may be viewed at this website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/advanced.htm#xtocid57948

- Previous text:
 - Step 2** Ensure that all active network interfaces are connected between both units.
- New text:
 - Step 2** Attach a network cable between the Primary and Secondary units for each network interface to which you have configured an IP address.

Important Notes

The following sections describe important notes for the 5.3(1) release.

16 MB Board

8 MB or more of Flash memory is required to install and run PIX Firewall software version 5.3(1). The purchase and installation of Flash memory upgrade PIX-FLASH-16MB= is required for PIX, PIX10000, PIX 510, or PIX 520 revisions A0 through C0 to install version 5.3(1). PIX 520 revisions may be identified by the Flash memory type as reported in a **show version** command request. 2 MB models contain the AT29C040A Flash OR ATMEL, and 16 MB models contain the i28F640J5 Flash.

AAA

The *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* incorrectly states that the maximum number of AAA servers is 14. This information appears as usage note 15 on the **aaa** command page and in the *group_tag* description for the **aaa-server** command page. Both these command pages appear in Chapter 5, “Command Reference.” You can have up to 16 AAA servers per tag group, up to 14 AAA server tag groups, and a total of up to 224 AAA servers.

Access-list

The new **access-list** option changes the behavior of the **nat 0** command. (Without the **access-list** option, the command is backward compatible with previous versions.) The **nat 0** implemented the identity feature; this new version of the command disables NAT. Specifically, the new behavior disables proxy ARPing for the IP addresses in the **nat 0** command statement.

Cisco Secure Policy Manager

PIX Firewall version 5.1(2) and later, by default, generates the **isakmp identity hostname** command prior to any crypto configuration. Subsequently, when attempting to configure Cisco Secure VPN Client (version 2.1.2), an IPSec tunnel cannot be established because it defaults to an IP address as its default ID Type. This causes failure with the Cisco Secure Policy Manager version 2.1 when it tries to configure the PIX Firewall through an IPSec tunnel.

Cisco Secure VPN Client

When using the Cisco Secure VPN Client with SoftID, the single password challenge prompt only appears for 30 seconds. When two passwords are required, the prompts appear for only 30 seconds each. You must enter your password information promptly before the timeout expires. Refer to caveat CSCds59105 for more information.

DHCP

The following notes apply to DHCP:

- A new DHCP command, **dhcpcd ping_timeout**, is introduced. This command allows setting a ping timeout value before assigning an IP to a DHCP client.

DHCP daemon can be enabled on inside interface only. The DHCP Server on the PIX Firewall does not support clients that not directly connected to the **inside** interface.

The maximum lease supported on PIX is 2147483647, not 0xFFFFFFFF (as in RFC 2131).

- PIX Firewall removes an IP address from the pool of available DHCP IP addresses if a host responds to a ping request that the PIX Firewall sends prior to issuing the IP address to the DHCP client. The address removed from the pool can only be made available again by rebooting the PIX Firewall, or by disabling and then reenabling the DHCP server command statements in the configuration. Refer to CSCds51664 in the Bug Navigator on CCO to view more information.

DNS

PIX Firewall drops DNS packets sent to UDP port 53 that have a packet size larger than 512 bytes.

Failover

Ensure that all PIX Firewall interfaces to which you assign an IP address are connected between the Primary unit and Secondary unit.

Gigabit Ethernet

If, after configuring a PIX Firewall unit for Gigabit Ethernet boards, you replace the boards with 10/100 Ethernet boards, the order of the boards in the configuration changes from what you originally configured. For example, if you configure ethernet0 for a Gigabit Ethernet board assigned to the inside interface and replace this board with a 10/100 Ethernet board, the board may no longer appear as ethernet0.

ISAKMP

- When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0):Unknown error in cert validation, 0” and packets are lost until the PIX Firewall receives the CRL. Refer to caveat CSCdr89880 for more information.
- Use the following information to configure the **isakmp keepalive** command:

isakmp keepalive <seconds> [retry <seconds>]

The keepalive interval can be between 10 and 3600 seconds. The retry interval can be between 2 and 10 seconds, with the default being 2 seconds. The retry interval is the interval between retries after a keepalive response has not been received. For more information on keepalive see the following Cisco IOS software documentation:

http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpne_an.htm

http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/dplip_in.htm

PIX 525

- PIX 525 in version 5.3(1) supports up to eight interfaces with an unrestricted license (UR). The restricted license (R) supports up to six interfaces. The **show version** command lists the maximum number of supported interfaces on the unit. If you add more interfaces than are supported, the additional interfaces are ignored. However, when you first start the PIX 525 unit, the startup messages display the number of installed interfaces followed by two error messages stating that interfaces are disabled. You can ignore these messages and use only the information in the **show version** command to verify the correct number of supported interfaces. Refer to CSCds44827 in the Bug Navigator on CCO to view more information.
- There are no hardware or software limitations regarding using more than 2 Gigabit interfaces in the PIX 525 as of the 5.3 version software release.

There is a performance limitation because the PIX 525 uses a 32-bit PCI bus.

PPTP

If you configure PIX Firewall for 128-bit encryption and if a Windows 95 or Windows 98 client does not support 128-bit or greater encryption, the connection to the PIX Firewall is refused. When this occurs, the Windows client moves the dial-up connection menu down to the screen corner while the PPP negotiation is in progress. This gives the appearance that the connection is accepted when it is not. When the PPP negotiation completes, the tunnel terminates and PIX Firewall ends the connection. The Windows client eventually times out and disconnects.

RAS

H.323 RAS fixups cannot be disabled through the PIX Firewall when the PIX Firewall unit is between the H.323 Gateway and Gatekeeper. When the PIX Firewall is between the Gateway and Gatekeeper, whenever PIX Firewall detects RAS packets, it enables packet checking. Use the **debug h323 ras event** command to determine if RAS packets are passing through the PIX Firewall.

Sample output from the **debug h323 ras event** command appears as follows:

```
57:RAS::RRQ received from 10.130.4.250/51527 to 10.132.4.6/1719
```

```
58:RAS::RCF received from 10.132.4.6/1719 to 10.132.4.250/51527
```

The first line shows that a RAS registration request was received by the PIX Firewall. The next line shows that the request was confirmed.

If the PIX Firewall unit is not between the Gateway and Gatekeeper, you can enable RAS fixups with the **fixup protocol h323 1720** command. If the PIX Firewall unit is not between the Gateway and Gatekeeper, you can disable RAS fixups with the **no fixup protocol h323 1720** command.

However, if the PIX Firewall unit *is* between the Gateway and Gatekeeper, the **no fixup protocol h323 1720** command has no effect and RAS fixups continue automatically.

RIP Version 2

With version 5.3, when RIP version 2 is configured in passive mode, the PIX Firewall accepts RIP version 2 multicast updates with IP destination of 224.0.0.9. For RIP version 2 default mode, the PIX Firewall will transmit default route updates using an IP destination of 224.0.0.9. Configuring RIP version 2 registers the multicast address 224.0.0.9 on the respective interface in order to be able to accept multicast RIP version 2 updates.

Only Intel 10/100 and Gigabit interfaces support multicasting. FDDI and Token Ring will still operate in broadcast mode (IP destination 255.255.255.255 not 224.0.0.9).

When the RIP version 2 commands for an interface are removed, the multicast address is unregistered from the interface card.

RTSP

You can configure NAT for Apple QuickTime 5.0.1 and RealPlayer Basic 8. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside and the server on the inside.

SMTP

As of version 5.1 and later, the **fixup protocol smtp** command changes the characters in the SMTP banner to asterisks except for the “2”, “0”, “0 ” characters. Carriage return (CR) and linefeed (LF) characters are ignored. In version 4.4, all characters in the SMTP banner are converted to asterisks. Refer to CSCds33156 in the Bug Navigator on CCO to view more information.

Token Authentication

For use with the **crypto map token authentication** command, token based authentication for the Cisco VPN 3000 Client connecting to a PIX Firewall has been tested and verified for the following token devices:

- Security Dynamics (SDI) SecurID/ACE Server with SDI RADIUS
 - Next Token mode
 - New Pin mode
- SDI with CiscoSecure ACS NT version
 - Next Token mode
 - New Pin mode
- SDI with CiscoSecure ACS UNIX version
 - Next Token mode
 - New Pin mode does not work

Token based authentication using the SDI RADIUS server has also been tested and verified with the Cisco Secure VPN Client version 1.1 including the following:

- Next Token mode
- New Pin mode

Caveats

The following sections describe the open and resolved caveats for the 5.3(2) release.

**Note**

Please use Bug Navigator II on CCO to view additional caveat information. Bug Navigator II may be accessed at the following website:

<http://www.cisco.com/support/bugtools>

Open Caveats - Release 5.3(2)

The caveats in the following table are yet to be resolved in this release.

Table 1 Open Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCds10112	No	Traceback (Crypto PKI RECV) after twice enrolling and getting denied.
CSCds60366	No	Traceback (isakmp_receiver) when unable to establish a tunnel.
CSCds80846	No	525 FDDI: Standby PIX Firewall in failover goes to failed state.
CSCds83357	No	Traceback (Crypto CA) when unable to establish a tunnel.
CSCdt49040	No	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt53815	No	SNMP polls timeout. PIX Firewall tears down the UDP connection.
CSCdt65603	No	PIX Firewall is giving wrong prompt when doing Xauth.
CSCdt86736	No	PIX Firewall stops forwarding traffic at 30 second intervals.
CSCdu02557	No	Xauth: With ACS+SecurID, new pin mode, not allowed to enter return.
CSCdu26524	No	VPN Client w/Xauth can ping even if not authorized.
CSCdu36628	No	PIX Firewall neither uses nor discards CRL if time < last CRL update of CA.
CSCdu48184	No	Watchdog timeout during show tech dump , following initial traceback.
CSCdu53971	No	Misconfigured failover interface a.b.c.d lines causes flip-flops.
CSCdu56928	No	Assertion violation occurs while running IPSec stress tests.

Table 1 Open Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdu60033	No	Telnet console does not allow use of challenge response.
CSCdu60862	No	PIX Firewall URL CACHE does not work with Websense 4.3.
CSCdu61102	No	PIX Firewall URL Filtering Extremely slow, 200-400 URLs/sec.
CSCdu61691	No	Stateful Failover does not replicate connection for passive FTP using PAT.
CSCdu63411	No	Xauth: IRE rekey using different username/password, uauth remains same.
CSCdu64148	No	32 MB PIX 520 Backup PAT is not working.
CSCdu66557	No	H.323 Skinny does not properly open 3rd party IP using NAT 0 acl.
CSCdu67715	No	PIX Firewall is not sending/processing initial contact with concentrator/client.
CSCdu67799	No	IPSec: PIX Firewall takes long time to create a second IPSec tunnel (1 IKE).
CSCdu68124	No	Intercepted connections timeout prematurely if they are idle.

Open Caveats - Release 5.3(1)

The following caveats are yet to be resolved:

- CSCds80108

Cisco Secure Intrusion Detection System (Cisco Secure IDS) signature number 1101 is not supported by PIX Firewall. When an unsupported signature number is entered, PIX Firewall returns an error message:

```
pixfirewall(config)# ip audit signature 1101 disable usage:ip audit signature number disable
Type help or '?' for a list of available commands.
pixfirewall(config)#
```

- CSCds69891

Before downgrading from version 5.3(1) to an earlier version, remove the VPN accelerator board from your PIX Firewall unit. The PIX 535 cannot be downgraded to earlier versions.

- CSCds67745

If you configure a network static where the network static is the same as a third party netmask and address, then an outbound H.323 connection fails. The following example clarifies this problem:

The interfaces in the example are as follows:

- The outside interface IP address:10.1.1.6
- The inside interface IP address:10.0.0.5
- Embedded address on inside interface:10.0.0.7

Example network static command statement:

```
static (inside,outside) 10.1.1.0 10.0.0.0
```

This command maps the inside host address of 10.0.0.5 to the outside global address of 10.1.1.5 and the inside host address 10.0.0.7 to the outside global address of 10.1.1.7.

If the PIX Firewall encounters a packet from 10.1.1.5 to 10.0.0.5 with the embedded IP address of 10.1.1.7, the PIX Firewall unit will not be able to determine if the embedded IP address belongs to the inside or outside network.

- CSCds59105

When using the Cisco Secure VPN Client with SoftID, the single password challenge prompt only appears for 30 seconds. When two passwords are required, the prompt only appears for approximately 60 seconds. You must enter your password information promptly before the timeout expires.

- CSCds51664

PIX Firewall removes an IP address from the pool of available DHCP IP addresses if a host responds to a ping request that the PIX Firewall sends prior to issuing the IP address to the DHCP client. The address removed from the pool can only be made available again by rebooting the PIX Firewall, or by disabling and then reenabling the DHCP server command statements in the configuration.

- CSCds44827

PIX 525 in version 5.3(1) supports up to eight interfaces with an unrestricted license (UR). The restricted license (R)supports up to six interfaces. The **show version** command lists the maximum number of supported interfaces on the unit. If you add more interfaces than are supported, the additional interfaces are ignored. However, when you first start the PIX 525 unit, the startup

messages display the number of installed interfaces followed by two error messages stating that interfaces are disabled. You can ignore these messages and use only the information in the **show version** command to verify the correct number of supported interfaces.

- CSCds33156

As of version 5.1 and later, the **fixup protocol smtp** command changes the characters in the SMTP banner to asterisks except for the “2”, “0”, “0 ” characters. Carriage return (CR) and linefeed (LF) characters are ignored. In version 4.4, all characters in the SMTP banner are converted to asterisks.

- CSCdr89880

When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0):Unknown error in cert validation, 0” and packets are lost until the PIX Firewall receives the CRL.

- CSCdr82395

PIX Firewall by default generates the **isakmp identity hostname** command prior to any IPsec configuration. Subsequently, when attempting to configure the Cisco Secure VPN Client version 2.1.2, an IPsec tunnel cannot be established because the IPsec tunnel defaults to IP address as its default ISAKMP ID type. This also causes the Cisco Secure Policy Manager version 2.1 to fail when it tries to configure the PIX Firewall through an IPsec tunnel.

- CSCds44827

If two four-port Ethernet boards are inserted in a PIX 525 with an R license, which only supports 6 interfaces, the last two interfaces are ignored. (A UR license supports 8 interfaces.) The following messages appear at startup:

- Ignoring NIC in PCI slot 3
- Ignoring NIC in PCI slot 3

These messages indicate that the PIX Firewall unit detected more interfaces than permitted by the license and ignored the extra two.

- CSCds11526

The following information applies to use of the **crypto map token authentication** command. Token based authentication for the Cisco VPN 3000 Client connecting to a PIX Firewall has been tested and verified for the following:

- Security Dynamics (SDI) SecurID and ACE Server with SDI RADIUS:
 - Next Token mode
 - New Pin mode
- SDI with CiscoSecure ACS Windows NT version:
 - Next Token mode
 - New Pin mode
- SDI with CiscoSecure ACS UNIX version:
 - Next Token mode
 - New Pin mode *does not work*

Token based authentication using the SDI RADIUS server has also been tested and verified with the Cisco Secure VPN Client version 1.1 for Next Token mode and New Pin mode.

Resolved Caveats - Release 5.3(2)

The caveats in the following table are resolved in this release.

Table 2 *Resolved Caveats*

DTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdm49619	Yes	AAA authentication on the console or through Telnet prompts for Telnet password.
CSCdp73853	Yes	debug crypto ca messages are intermixed on console.
CSCdr34819	Yes	clear configure all does not reset arp timeout to default values.
CSCdr43633	Yes	URL size exceeds buffer size.
CSCdr48472	Yes	conn needs to be deleted from clear ? command page.
CSCdr60893	Yes	The clear url-server command is confusing.
CSCdr68251	Yes	Port numbers not included in the syslog when a session is denied by the access-list command.
CSCdr68928	Yes	When the certificate request fails it still says pending.
CSCdr78189	Yes	No syslog when SSH, Telnet, or PFM connection limit is exceeded.
CSCdr78505	Yes	The PIX Firewall does not compute the RIP v2 updates for the default route.
CSCdr84397	Yes	The PIX Firewall does not reset the sixth consecutive requested SSH, Telnet, or PFM session.
CSCds11341	Yes	PIX 525 with Gigabit Ethernet card prints console messages and reboots with heavy load.
CSCds18774	Yes	The PIX Firewall should not respond to its own ARP request.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCds21095	Yes	The PIX Firewall PPTP stops accepting new connections after periods of trouble-free operation.
CSCds29676	Yes	Websense caching not working; -sho url-cache stat displays wrong information.
CSCds43973	Yes	Cannot Telnet to the PIX Firewall inside interface - 402106. Error reads "Recd packet not IPSEC..."
CSCds46441	Yes	The PIX Firewall should indicate an error since " no dhcpcd " is not unique.
CSCds52853	Yes	help crypto has two entries for dynamic-map.
CSCds60270	Yes	The PIX Firewall is unable to establish a tunnel with peer if peer changes keys or ID.
CSCds63404	Yes	There is an unexpected reload after pressing Ctrl-R and holding down any key.
CSCds63501	Yes	LU updates for UDP conn are not properly propagated to standby unit.
CSCds71849	Yes	<code>dbgtrace_is_debug_trace_on()</code> function needs to be optimized.
CSCds74244	Yes	Unit reloads if active and standby units write to memory at same time.
CSCds76768	Yes	The PIX 525 onboard Ethernet card generates errors when connected to switch.
CSCds81948	Yes	The unit reloads after trying to enroll with a Baltimore certificate and typing in some commands.
CSCds82454	Yes	No RIP interface default version 2 will un-configure RIPv2 passive on interface.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCds82455	Yes	VPN: Last QM packet not retransmitted; causes invalid SPI errors.
CSCds82521	Yes	The PIX Firewall should unconfigure the multicast address on the interface when RIPv1 is configured.
CSCds85080	Yes	IKE Main mode proposal flooding reboots the PIX Firewall.
CSCds87365	Yes	H.323: The PIX Firewall does not inspect Progress message.
CSCds88063	Yes	The PIX Firewall DHCP client with failover license fails to get address automatically after reboot.
CSCds89077	Yes	The PIX Firewall does not open a third party H.245 connection.
CSCds89281	Yes	hdb_sweep thread may get starved under heavy system load.
CSCds89340	Yes	Watchdog timeout in dbgtrace thread.
CSCds90077	Yes	Unexpectedly reloads while trying to change the transform set.
CSCds90474	Yes	Assertion error when TCP log server is configured.
CSCds90641	Yes	PIX Firewall alias does not work with PAT.
CSCds90792	Yes	fixup smtp blocks emails when <CR><LF> are not in the same packet.
CSCds90802	Yes	NFS disallows packets of more than 12 fragments needed for Solaris.
CSCds92693	Yes	sh loc or sh conn during GC could cause list corruption.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCds92738	Yes	Standby PIX Firewall prints out confusing, inconsistent xlate debug message.
CSCdt00162	Yes	Service resetinbound does not work with interface PAT.
CSCdt00459	Yes	Debug message for PKI content sent and received from PIX Firewall.
CSCdt01808	Yes	ARP does not proxy-arp for ARP alias entry.
CSCdt01825	Yes	PIX Firewall should proxy-arp for alias address.
CSCdt02063	Yes	H.245: PIX Firewall should create new TPKT and discard original if TPKT received only.
CSCdt02132	Yes	The PIX Firewall should check host list on first SYN for Telnet, SSH, PFM, and HTTP.
CSCdt02883	Yes	Certificate enrollment request is lost if CA is not available at that time.
CSCdt04241	Yes	Remove debugging statement for kprint from Stateful Failover.
CSCdt04636	Yes	Outbound connection was blocked by PAT.
CSCdt04772	Yes	Make fragment database limits configurable.
CSCdt05025	Yes	LU look NAT failed; NAT is disabled.
CSCdt06176	Yes	H.323: No audio or video with NetMeeting.
CSCdt06447	Yes	PIX Firewall in Stateful Failover configuration may deplete memory blocks.
CSCdt07794	Yes	Cannot select private key; message prints on standby during synchronization.
CSCdt09791	Yes	DHCP client configuration lost if the command failed.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt11716	Yes	clear xlate prints 305007 syslog message on standby unit.
CSCdt15446	Yes	Incorrect interface state on standby unit.
CSCdt15819	Yes	Fails to dump UDP connection after DNS reply is seen.
CSCdt16666	Yes	PIX Firewall on reboot will not get address via DHCP if connected through switch to sever.
CSCdt17577	Yes	PIX Firewall cannot send filter URLs to Websense longer than 1159 characters.
CSCdt17646	Yes	rip command should parse all input.
CSCdt18433	Yes	H.225: syslog 405104 for signalling protocol is wrong.
CSCdt18451	Yes	clear config all does not clear icmp command.
CSCdt20809	Yes	“Retransmitting phase 2” message seen when SAs are established.
CSCdt22085	Yes	With names in the configuration, host route changes to default route on reload.
CSCdt23749	Yes	PIX Firewall should send invalid SPI to notify if peer is out of sync.
CSCdt25399	Yes	PIX Firewall cached authentication does not work with UDP connections.
CSCdt26426	Yes	PIX Firewall accepts authentication command for HTTP on non-standard ports.
CSCdt28073	Yes	PIX Firewall appends two bytes to RADIUS state attribute.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt28219	Yes	Internal users cannot ping outside hosts with interface PAT.
CSCdt28399	Yes	vpdn group pp followed by anything is accepted. No error message.
CSCdt30628	Yes	help static does not mention embryonic connection limit.
CSCdt31630	Yes	Blocks can wedge into fragment database.
CSCdt32830	Yes	RST always printed for syslog 106015 even if no RST in packet.
CSCdt34923	Yes	Error message when deleting global address pool.
CSCdt35429	Yes	Naptha DoS tool with PIX Firewall SSH daemon causes high CPU load.
CSCdt36491	Yes	debug icmp trace prints invalid type and code for fragmented packet.
CSCdt37028	Yes	Redundant error checking can cause traceback within first traceback.
CSCdt37366	Yes	Negative syslog line counter.
CSCdt37443	Yes	Discrepancies on 535R maximum interface support.
CSCdt38205	Yes	Stateful Failover should not generate syslog when out of memory.
CSCdt38404	Yes	Wrong character for Account rule in aaa accounting command.
CSCdt38616	Yes	RIP routes have a metric of one added.
CSCdt39076	Yes	PIX Firewall does not generate an error if 0.0.0.0/net add is specified for dns in vpdn gp .
CSCdt39174	Yes	vpdn group dns/wins command is not fully replaced by a new one.

Table 2 Resolved Caveats

DTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt39766	Yes	Erasedisk not supported on PIX 525 platforms.
CSCdt39820	Yes	Syslog for memory allocation error used improperly in places.
CSCdt39863	Yes	Unexpected reload while enrolling certificate request.
CSCdt39871	Yes	Logging priority consulted only after formatting overhead incurred.
CSCdt40579	Yes	Without IPsec, host can Telnet to PIX Firewall from least-secured interface.
CSCdt40713	Yes	xlate error when portmap pool is exhausted results in rogue connections.
CSCdt40837	Yes	PIX Firewall show block has 1552 size entry.
CSCdt41079	Yes	Telnet, SSH, and TFTP server always assume least-secured interface at level 0.
CSCdt41763	Yes	Using names within a static command results in a misconfiguration.
CSCdt42739	Yes	H.323: PIX Firewall should open connections based on <i>LogicalChannelNumber</i> .
CSCdt45065	Yes	Small block pool causes traffic to stall with Livengood Gigabit card.
CSCdt47536	Yes	gdb toolchain disappearing from irp-view5.
CSCdt49040	Yes	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt49906	Yes	Virtual HTTP/Telnet does not work if interface 0 is not in lowest security level.
CSCdt51029	Yes	PIX 535 boot-time panic when multiple GE cards installed.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt53291	Yes	Remove unsupported pal command.
CSCdt53742	Yes	Global NAT does not work with VoIP Third Party address.
CSCdt54951	Yes	Standby unit incorrectly creates UDP connection and generates 210010 syslogs.
CSCdt56080	Yes	Traceback occurs when trying to build PPTP tunnel with RADIUS server unavailable.
CSCdt57251	Yes	PIX Firewall should not allow fragment chain > fragment database size.
CSCdt57268	Yes	clear conf all does not clear fragment configuration.
CSCdt58805	Yes	PIX Firewall must not change isakmp lifetime in IKE initiators proposal.
CSCdt60308	Yes	Certificate request fails if retried after cancelling.
CSCdt60487	Yes	PIX Firewall reboots, dumping trace.
CSCdt61216	Yes	Naptha (ESTABLISHED) Flooding causes PDM DoS.
CSCdt62968	Yes	Reboot occurs with filter java and NAT 0 access-list.
CSCdt63037	Yes	VoIP: No voice between inside phones (static NAT with no route).
CSCdt64177	Yes	PIX Firewall flooded with "cgx_create_cc returned 0x102" messages.
CSCdt64243	Yes	"ike retransmit debug" seen on console even with debug off.
CSCdt64687	Yes	DHCP client does not interoperate with some relay agents or servers.
CSCdt65464	Yes	MIB-II object interfaces.ifSpeed query not supported on Gigabit Ethernet card.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt65603	Yes	PIX Firewall gives incorrect prompt when performing Xauth.
CSCdt66414	Yes	Remove unused pal_check() function in lu_thread.
CSCdt66614	Yes	SSH allowed after changing host name and domain name when previous keypair exists.
CSCdt66648	Yes	CA: Does not save .server key to the FLASH with ca save all command.
CSCdt69667	Yes	Encryption layer for TCP port 1467 uses up large amount of memory.
CSCdt69676	Yes	Enable UniRPF for-us traffic.
CSCdt70750	Yes	sysopt connection tcpmss 0 behavior changed from 5.0 to 5.1.
CSCdt71192	Yes	Stateful Failover PIX Firewall logs duplicate messages on syslog server.
CSCdt73353	Yes	SSH: Need to add CRC-32 compensation attack detection.
CSCdt73358	Yes	Need unique tty number in ssh debug messages.
CSCdt73865	Yes	H.323 message printed on console needs to be removed.
CSCdt74263	Yes	Do not allow more than one RSA key through with different attributes.
CSCdt74520	Yes	uauth cache not working properly with browsers.
CSCdt75715	Yes	fragment command handles input > max inconsistently.
CSCdt75960	Yes	ISA fragment method causes PIX Firewall to discard packet.
CSCdt77108	Yes	Need to selectively allow unencrypted SSH sessions for debugging.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdt77818	Yes	Traceback (crypto CA) if Netscape CA server is misconfigured.
CSCdt82325	Yes	Reloads due to exhausted memory while URL filtering heavy traffic.
CSCdt83142	Yes	SIP: Call does not go through with static network.
CSCdt85788	Yes	PIX Firewall fails to get CRL with Verisign certificate.
CSCdt86132	Yes	“709001: FO repliSorry: error” message at boot up.
CSCdt86568	Yes	Unexpectedly reloads when URL cache is on and the URL server is unavailable.
CSCdt91309	Yes	Interface PAT port detection with for-us traffic ineffective.
CSCdt92339	Yes	BUGTRAQ: PIX Firewall should limit number of uauth sessions per source IP.
CSCdt92450	Yes	Multiple websns keepalive daemon starts.
CSCdt93858	Yes	kprint message to console when fails to allocate memory block.
CSCdt94747	Yes	H.323: PIX Firewall should proxy ACK TPKT if received TPKT only.
CSCdu00856	Yes	Emit a warning if an 82542 Wiseman NIC is found in a PIX 535.
CSCdu01056	Yes	Reloads while running backup traffic (SQL*Net) through the PIX Firewall.
CSCdu02291	Yes	Failover timeout needs to be taken out from failover online help.
CSCdu02673	Yes	clear config should be a config mode command.
CSCdu02674	Yes	Issues with the service command.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdu04084	Yes	Traceback while reading certificate from FLASH.
CSCdu05134	Yes	H.323: Call does not go through if calling GW uses slow start.
CSCdu05694	Yes	Invalid global command causes traceback (ci/console).
CSCdu05843	Yes	ip verify does not work with IPSec.
CSCdu06716	Yes	show chunk only shows ulimit chunk .
CSCdu08574	Yes	Certificate enroll request fails after deleting current CA and retrying.
CSCdu11774	Yes	SIP: Call does not go through with IN proxy (Regression).
CSCdu11781	Yes	Reloads during DHCP request when PDM refreshes DHCP Client information.
CSCdu12321	Yes	PIX Firewall fails to do write memory if a big command line exists.
CSCdu12909	Yes	SIP: Connections for Responses to INVITE not opened correctly.
CSCdu13395	Yes	Remove [nailed] parameter from static command online help.
CSCdu13956	Yes	Deleting non-default fixup rtsp port also deletes default port.
CSCdu15173	Yes	H.323: RAS routine causes memory corruption.
CSCdu18020	Yes	PIX Firewall-to-PIX Firewall or PIX Firewall-to-Unity connection fails when using certificates.
CSCdu20593	Yes	Xauth: With IRE on rekey, puts internal address entry for uauth .

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdu27169	Yes	VoIP: Certain embedded IP addresses do not undergo NAT.
CSCdu33209	Yes	IPSec Antireplay Checking Ineffective 32-64 sequence numbers back.
CSCdu33543	Yes	PIX Firewall PPTP rejects dial-in request after abnormal termination.
CSCdu38206	Yes	Configuration lines greater than 255 displayed incorrectly by sh conf .
CSCdu38221	Yes	Failover usability: Should warn user if OS version is not the same.
CSCdu38927	Yes	PIX Firewall failover should try to allocate additional block if possible.
CSCdu39748	Yes	H.323: Generating 50+ calls causes unexpected reload.
CSCdu39906	Yes	PIX Firewall should not send stateful updates if peer is down.
CSCdu42645	Yes	Kodiak: Some status bits are ignored.
CSCdu42656	Yes	Kodiak: AH decapsulation requests not setup correctly.
CSCdu43016	Yes	TCP Intercept sends ARP for every proxied syn-ack.
CSCdu43284	Yes	H.323: Should make use of NELTS and sizeof and remove extern functions.
CSCdu46309	Yes	pix_init should be called after verifying license key.
CSCdu47003	Yes	Able to pass disallowed SMTP command through PIX Firewall by sending after mail.
CSCdu48706	Yes	clear interface does not clear Gigabit interface counters.
CSCdu49737	Yes	aaa telnet console: Failed login attempts should be limited.

Table 2 Resolved Caveats

DDTS Number	Software Release	
	5.3(2)	
	Corrected	Caveat
CSCdu53473	Yes	H.225 and H.245 messages greater than 1024 bytes are not inspected.
CSCdu54495	Yes	Unexpected reload when using Websense with TCP4 and url-cache.
CSCdu55206	Yes	Traceback while trying to establish a PPTP tunnel (scripted).
CSCdu62647	Yes	Kodiak: IPSec encrypt packet interoperability with Cisco IOS software is not working in FTP.

Resolved Caveats - Release 5.3(1)

The following caveats are resolved:

CSCds66550, CSCds66052, CSCds62734, CSCds58313, CSCds56721, CSCds55734, CSCds55694, CSCds54886, CSCds53316, CSCds51955, CSCds50982, CSCds46349, CSCds38708, CSCds34732, CSCds34622, CSCds34475, CSCds32842, CSCds30699, CSCds29676, CSCds26054, CSCds25070, CSCds24580, CSCds23698, CSCds22194, CSCds21095, CSCds11378, CSCds09730, CSCdr93478, CSCdr93435, CSCdr84484, CSCdr77921, CSCdr48266, CSCdp67764

- CSCdr78383

H.323 RAS fixups cannot be disabled through the PIX Firewall when the PIX Firewall unit is between the H.323 Gateway and Gatekeeper. When the PIX Firewall is between the Gateway and Gatekeeper, whenever PIX Firewall detects RAS packets, it enables packet checking. Use the **debug h323 ras event** command to determine if RAS packets are passing through the PIX Firewall.

This is the expected behavior of H.323 with RAS.



Note

Please use Bug Navigator II on CCO to view additional information for the resolved caveats. Bug Navigator II may be accessed at the following URL:

<http://www.cisco.com/support/bugtools>

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN 3000 documentation at the following sites:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm>

Cisco provides PIX Firewall technical tips at the following site:

http://www.cisco.com/public/technotes/serv_tips.shtml

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships 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 as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered 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 CCO users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
 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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other 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. (0106R)

Copyright © 2000-2001, Cisco Systems, Inc.
All rights reserved.

