



Release Notes for the Cisco Secure PIX Firewall Version 5.3(3)

February 2002

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
- World Wide Web
- Obtaining Technical Assistance

Introduction

This release note describes the new features, restrictions, and caveats for the Cisco Secure PIX Firewall 5.3(3) release.



System Requirements

The following sections describe the system requirements for operating a PIX Firewall unit with version 5.3(3) software.

Memory Requirements


Note

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

Table 1 lists Flash memory requirements for this release:

Table 1 *Flash Memory Requirements*

PIX Firewall Model	Flash Memory Required in 5.3	Flash Memory Sold with Unit
PIX 506/506E	8 MB	8 MB
PIX 515/515E	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 525	16 MB	16 MB
PIX 535	16 MB	16 MB

Software Requirements

The following is required for version 5.3(3):

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.com to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must have a new activation key. Before getting a new activation key, write down your old key in case you want to downgrade back to version 4. You can have a new activation key sent to you by completing the form at the following website:
<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>
3. If you are using PIX Firewall Syslog Server (PFSS), Cisco recommends you install Windows NT Service Pack 6. PFSS is not supported on Windows 2000.
4. 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 Secure VPN Client Interoperability

PIX Firewall version 5.2 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 determine the software version of your PIX Firewall unit.

Upgrading to a New Software Release

If you have a Cisco.com 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 Features in Release 5.3(3)

The PIX 506E and PIX 515E join the PIX Firewall product line. Both the PIX 506E and PIX 515E have faster processors than the PIX 506 and PIX 515. Also, the PIX 506E has a physically different, but functionally equivalent, power supply than the PIX 506.

New 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.

Table 2 summarizes the performance considerations of the different interface card combinations.

Table 2 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

- sysopt connection enforcesubnet**—This command has been deleted from the Command Line Interface.
- show eeprom**—Displays the current PIX Firewall eeprom contents.
eeprom update—Update the eeprom contents.
- 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 Configurations.” 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(3) releases.

**Note**

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

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

The caveat descriptions listed in this section are drawn directly from the DDTS caveat headlines. These caveat descriptions are not intended to be read as complete sentences because the headline field in DDTS is limited in length. In DDTS headlines, some truncation of wording or punctuation may be necessary to provide the most complete and concise caveat description. The only modifications made to these headlines are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Open Caveats - Release 5.3(3)

The caveats in Table 3 are yet to be resolved in this release.

Table 3 *Open Caveats*

DDTS Number	Description
CSCds10112	Traceback (Crypto PKI RECV) after twice enrolling and getting denied.
CSCds60366	Traceback (isakmp_receiver) when unable to establish a tunnel.
CSCds80846	525 FDDI: Standby PIX Firewall in failover goes to failed state.
CSCds83357	Traceback (Crypto CA) when unable to establish a tunnel.
CSCdt49040	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt53815	SNMP polls timeout. PIX Firewall tears down the UDP connection.
CSCdt65603	PIX Firewall is giving wrong prompt when doing Xauth.
CSCdt86736	PIX Firewall stops forwarding traffic at 30 second intervals.
CSCdu02557	Xauth: With ACS+SecurID, new pin mode, not allowed to enter return.
CSCdu26524	VPN Client w/Xauth can ping even if not authorized.
CSCdu36628	PIX Firewall neither uses nor discards CRL if time < last CRL update of CA.
CSCdu48184	Watchdog timeout during show tech dump , following initial traceback.
CSCdu52383	cic_dh_makepair:gen_newpubkey(1) returned 0xd.
CSCdu53971	Misconfigured failover interface a.b.c.d lines causes flip-flops.
CSCdu56928	Assertion violation while running IPSec stress (not 6.0 or later).
CSCdu60033	Telnet console does not allow use of challenge response.
CSCdu60862	PIX Firewall URL CACHE does not work with Websense 4.3.
CSCdu61102	PIX Firewall URL Filtering Extremely slow, 200-400 URLs/sec.
CSCdu61691	Stateful Failover does not replicate connection for passive FTP using PAT.
CSCdu63411	Xauth: IRE rekey using different username/password, uauth remains same.
CSCdu64148	32 MB PIX 520 Backup PAT is not working.
CSCdu66557	H.323 Skinny does not properly open 3rd party IP using NAT 0 acl.

Table 3 *Open Caveats (continued)*

DDTS Number	Description
CSCdu67715	PIX Firewall is not sending/processing initial contact with concentrator/client.
CSCdu67799	IPSec: PIX Firewall takes long time to create a second IPSec tunnel (1 IKE).
CSCdu68124	Intercepted connections timeout prematurely if they are idle.
CSCdv24040	PIX reboots with traceback in isakmp_receiver thread when rekeying.
CSCdv39306	PIX loses ARP entry for HSRP address.
CSCdv57731	H323:should drop msgs w/ invalid TPKT & UIIE lengths.
CSCdv77807	Assertion violation in isakmp_time_keeper thread while running ipsec.
CSCdv86755	icmp type is not correctly interpreted with aaa authentication.

Open Caveats - Release 5.3(2)

The caveats in Table 4 are yet to be resolved in this release.

Table 4 *Open Caveats*

DDTS Number	Description
CSCds10112	Traceback (Crypto PKI RECV) after twice enrolling and getting denied.
CSCds60366	Traceback (isakmp_receiver) when unable to establish a tunnel.
CSCds80846	525 FDDI: Standby PIX Firewall in failover goes to failed state.
CSCds83357	Traceback (Crypto CA) when unable to establish a tunnel.
CSCdt49040	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt53815	SNMP polls timeout. PIX Firewall tears down the UDP connection.
CSCdt65603	PIX Firewall is giving wrong prompt when doing Xauth.
CSCdt86736	PIX Firewall stops forwarding traffic at 30 second intervals.
CSCdu02557	Xauth: With ACS+SecurID, new pin mode, not allowed to enter return.
CSCdu26524	VPN Client w/Xauth can ping even if not authorized.
CSCdu36628	PIX Firewall neither uses nor discards CRL if time < last CRL update of CA.
CSCdu48184	Watchdog timeout during show tech dump , following initial traceback.
CSCdu53971	Misconfigured failover interface a.b.c.d lines causes flip-flops.
CSCdu56928	Assertion violation occurs while running IPSec stress tests.
CSCdu60033	Telnet console does not allow use of challenge response.
CSCdu60862	PIX Firewall URL CACHE does not work with Websense 4.3.
CSCdu61102	PIX Firewall URL Filtering Extremely slow, 200-400 URLs/sec.
CSCdu61691	Stateful Failover does not replicate connection for passive FTP using PAT.

Table 4 Open Caveats (continued)

DDTS Number	Description
CSCdu63411	Xauth: IRE rekey using different username/password, uauth remains same.
CSCdu64148	32 MB PIX 520 Backup PAT is not working.
CSCdu66557	H.323 Skinny does not properly open 3rd party IP using NAT 0 acl.
CSCdu67715	PIX Firewall is not sending/processing initial contact with concentrator/client.
CSCdu67799	IPSec: PIX Firewall takes long time to create a second IPSec tunnel (1 IKE).
CSCdu68124	Intercepted connections timeout prematurely if they are idle.

Open Caveats - Release 5.3(1)

The caveats in Table 5 are resolved in this release.

Table 5 Open Caveats

DDTS Number	Description
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.
CSCds69891	Downgrading PIX515 to <5.3 - Need to remove kodiak card.
CSCds67745	H323: Bad source IP on ACF RAS message using Static Network with NAT.
CSCds59105	Ire client authentication Dlg timing out too soon while using Softid.
CSCds51664	PIX dhcp doesnt release addr once ping address failed.
CSCds44827	Misleading msg stating 8 instead of 6 as ifx supported on 525-R.
CSCds33156	Fixup SMTP: Reply banner does not replace 2 and 0 with *
CSCdr89880	Pix takes long to get the CRL from Verisign CA.
CSCdr82395	PIX generates isakmp identity hostname as default/breaks VPN & CSPM.
CSCds11526	pix & CiscoSecure SDI OTP new pin mode does not work.

Resolved Caveats - Release 5.3(3)

The caveats in Table 6 are resolved in this release.

Table 6 Resolved Caveats

DDTS Number	Description
CSCdu64603	Add enhanced platform support for PIX 515.
CSCdv00738	Add enhanced platform support for PIX 506.

Table 6 Resolved Caveats (continued)

DDTS Number	Description
CSCdv69641	PIX can only recognize 2 interfaces in PIX-515E in monitor.
CSCdv87789	PIX 506E hangs when booting with 64 sector flash.
CSCdw20653	PIX 515E, cannot load image from monitor mode on PCI slots.
CSCdw29965	SSH: Watchdog timeout if receiving huge SSH packets.
CSCdw41000	SSH: PIX tback with big packet and invalid message type.
CSCdw53447	Enhancement: Reduce the boot-up time for the PIX-525.

Resolved Caveats - Release 5.3(2)

The caveats in Table 7 are resolved in this release.

Table 7 Resolved Caveats

DDTS Number	Description
CSCdm49619	AAA authentication on the console or through Telnet prompts for Telnet password.
CSCdp73853	debug crypto ca messages are intermixed on console.
CSCdr34819	clear configure all does not reset arp timeout to default values.
CSCdr43633	URL size exceeds buffer size.
CSCdr48472	conn needs to be deleted from clear ? command page.
CSCdr60893	The clear url-server command is confusing.
CSCdr68251	Port numbers not included in the syslog when a session is denied by the access-list command.
CSCdr68928	When the certificate request fails it still says pending.
CSCdr78189	No syslog when SSH, Telnet, or PFM connection limit is exceeded.
CSCdr78505	The PIX Firewall does not compute the RIP v2 updates for the default route.
CSCdr84397	The PIX Firewall does not reset the sixth consecutive requested SSH, Telnet, or PFM session.
CSCds11341	PIX 525 with Gigabit Ethernet card prints console messages and reboots with heavy load.
CSCds18774	The PIX Firewall should not respond to its own ARP request.
CSCds21095	The PIX Firewall PPTP stops accepting new connections after periods of trouble-free operation.
CSCds29676	Websense caching not working; -sho url-cache stat displays wrong information.
CSCds43973	Cannot Telnet to the PIX Firewall inside interface - 402106. Error reads "Recd packet not IPSEC..."
CSCds46441	The PIX Firewall should indicate an error since " no dhcpd d " is not unique.

Table 7 Resolved Caveats (continued)

DDTS Number	Description
CSCds52853	help crypto has two entries for dynamic-map.
CSCds60270	The PIX Firewall is unable to establish a tunnel with peer if peer changes keys or ID.
CSCds63404	There is an unexpected reload after pressing Ctrl-R and holding down any key.
CSCds63501	LU updates for UDP conn are not properly propagated to standby unit.
CSCds71849	dbgtrace_is_debug_trace_on() function needs to be optimized.
CSCds74244	Unit reloads if active and standby units write to memory at same time.
CSCds76768	The PIX 525 onboard Ethernet card generates errors when connected to switch.
CSCds81948	The unit reloads after trying to enroll with a Baltimore certificate and typing in some commands.
CSCds82454	No RIP interface default version 2 will un-configure RIPv2 passive on interface.
CSCds82455	VPN: Last QM packet not retransmitted; causes invalid SPI errors.
CSCds82521	The PIX Firewall should unconfigure the multicast address on the interface when RIPv1 is configured.
CSCds85080	IKE Main mode proposal flooding reboots the PIX Firewall.
CSCds87365	H.323: The PIX Firewall does not inspect Progress message.
CSCds88063	The PIX Firewall DHCP client with failover license fails to get address automatically after reboot.
CSCds89077	The PIX Firewall does not open a third party H.245 connection.
CSCds89281	hdb_sweep thread may get starved under heavy system load.
CSCds89340	Watchdog timeout in dbgtrace thread.
CSCds90077	Unexpectedly reloads while trying to change the transform set.
CSCds90474	Assertion error when TCP log server is configured.
CSCds90641	PIX Firewall alias does not work with PAT.
CSCds90792	fixup smtp blocks emails when <CR><LF> are not in the same packet.
CSCds90802	NFS disallows packets of more than 12 fragments needed for Solaris.
CSCds92693	sh loc or sh conn during GC could cause list corruption.
CSCds92738	Standby PIX Firewall prints out confusing, inconsistent xlate debug message.
CSCdt00162	Service resetinbound does not work with interface PAT.
CSCdt00459	Debug message for PKI content sent and received from PIX Firewall.
CSCdt01808	ARP does not proxy-arp for ARP alias entry.
CSCdt01825	PIX Firewall should proxy-arp for alias address.
CSCdt02063	H.245: PIX Firewall should create new TPKT and discard original if TPKT received only.

Table 7 Resolved Caveats (continued)

DDTS Number	Description
CSCdt02132	The PIX Firewall should check host list on first SYN for Telnet, SSH, PFM, and HTTP.
CSCdt02883	Certificate enrollment request is lost if CA is not available at that time.
CSCdt04241	Remove debugging statement for kprint from Stateful Failover.
CSCdt04636	Outbound connection was blocked by PAT.
CSCdt04772	Make fragment database limits configurable.
CSCdt05025	LU look NAT failed; NAT is disabled.
CSCdt06176	H.323: No audio or video with NetMeeting.
CSCdt06447	PIX Firewall in Stateful Failover configuration may deplete memory blocks.
CSCdt07794	Cannot select private key; message prints on standby during synchronization.
CSCdt09791	DHCP client configuration lost if the command failed.
CSCdt11716	clear xlate prints 305007 syslog message on standby unit.
CSCdt15446	Incorrect interface state on standby unit.
CSCdt15819	Fails to dump UDP connection after DNS reply is seen.
CSCdt16666	PIX Firewall on reboot will not get address via DHCP if connected through switch to sever.
CSCdt17577	PIX Firewall cannot send filter URLs to Websense longer than 1159 characters.
CSCdt17646	rip command should parse all input.
CSCdt18433	H.225: syslog 405104 for signalling protocol is wrong.
CSCdt18451	clear config all does not clear icmp command.
CSCdt20809	“Retransmitting phase 2” message seen when SAs are established.
CSCdt22085	With names in the configuration, host route changes to default route on reload.
CSCdt23749	PIX Firewall should send invalid SPI to notify if peer is out of sync.
CSCdt25399	PIX Firewall cached authentication does not work with UDP connections.
CSCdt26426	PIX Firewall accepts authentication command for HTTP on non-standard ports.
CSCdt28073	PIX Firewall appends two bytes to RADIUS state attribute.
CSCdt28219	Internal users cannot ping outside hosts with interface PAT.
CSCdt28399	vpdn group pp followed by anything is accepted. No error message.
CSCdt30628	help static does not mention embryonic connection limit.
CSCdt31630	Blocks can wedge into fragment database.
CSCdt32830	RST always printed for syslog 106015 even if no RST in packet.
CSCdt34923	Error message when deleting global address pool.
CSCdt35429	Naptha DoS tool with PIX Firewall SSH daemon causes high CPU load.

Table 7 Resolved Caveats (continued)

DDTS Number	Description
CSCdt36491	debug icmp trace prints invalid type and code for fragmented packet.
CSCdt37028	Redundant error checking can cause traceback within first traceback.
CSCdt37366	Negative syslog line counter.
CSCdt37443	Discrepancies on 535R maximum interface support.
CSCdt38205	Stateful Failover should not generate syslog when out of memory.
CSCdt38404	Wrong character for Account rule in aaa accounting command.
CSCdt38616	RIP routes have a metric of one added.
CSCdt39076	PIX Firewall does not generate an error if 0.0.0.0/net add is specified for dns in vpdn gp .
CSCdt39174	vpdn group dns/wins command is not fully replaced by a new one.
CSCdt39766	Erasedisk not supported on PIX 525 platforms.
CSCdt39820	Syslog for memory allocation error used improperly in places.
CSCdt39863	Unexpected reload while enrolling certificate request.
CSCdt39871	Logging priority consulted only after formatting overhead incurred.
CSCdt40579	Without IPSec, host can Telnet to PIX Firewall from least-secured interface.
CSCdt40713	xlate error when portmap pool is exhausted results in rogue connections.
CSCdt40837	PIX Firewall show block has 1552 size entry.
CSCdt41079	Telnet, SSH, and TFTP server always assume least-secured interface at level 0.
CSCdt41763	Using names within a static command results in a misconfiguration.
CSCdt42739	H.323: PIX Firewall should open connections based on <i>LogicalChannelNumber</i> .
CSCdt45065	Small block pool causes traffic to stall with Livengood Gigabit card.
CSCdt47536	gdb toolchain disappearing from irp-view5.
CSCdt49040	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt49906	Virtual HTTP/Telnet does not work if interface 0 is not in lowest security level.
CSCdt51029	PIX 535 boot-time panic when multiple GE cards installed.
CSCdt53291	Remove unsupported pal command.
CSCdt53742	Global NAT does not work with VoIP Third Party address.
CSCdt54951	Standby unit incorrectly creates UDP connection and generates 210010 syslogs.
CSCdt56080	Traceback occurs when trying to build PPTP tunnel with RADIUS server unavailable.
CSCdt57251	PIX Firewall should not allow fragment chain > fragment database size.
CSCdt57268	clear conf all does not clear fragment configuration.
CSCdt58805	PIX Firewall must not change isakmp lifetime in IKE initiators proposal.

Table 7 Resolved Caveats (continued)

DDTS Number	Description
CSCdt60308	Certificate request fails if retried after cancelling.
CSCdt60487	PIX Firewall reboots, dumping trace.
CSCdt61216	Naptha (ESTABLISHED) Flooding causes PDM DoS.
CSCdt62968	Reboot occurs with filter java and NAT 0 access-list.
CSCdt63037	VoIP: No voice between inside phones (static NAT with no route).
CSCdt64177	PIX Firewall flooded with “cgx_create_cc returned 0x102” messages.
CSCdt64243	“ike retransmit debug” seen on console even with debug off.
CSCdt64687	DHCP client does not interoperate with some relay agents or servers.
CSCdt65464	MIB-II object interfaces.ifSpeed query not supported on Gigabit Ethernet card.
CSCdt65603	PIX Firewall gives incorrect prompt when performing Xauth.
CSCdt66414	Remove unused pal_check() function in lu_thread.
CSCdt66614	SSH allowed after changing host name and domain name when previous keypair exists.
CSCdt66648	CA: Does not save .server key to the FLASH with ca save all command.
CSCdt69667	Encryption layer for TCP port 1467 uses up large amount of memory.
CSCdt69676	Enable UniRPF for-us traffic.
CSCdt70750	sysopt connection tcpmss 0 behavior changed from 5.0 to 5.1.
CSCdt71192	Stateful Failover PIX Firewall logs duplicate messages on syslog server.
CSCdt73353	SSH: Need to add CRC-32 compensation attack detection.
CSCdt73358	Need unique tty number in ssh debug messages.
CSCdt73865	H.323 message printed on console needs to be removed.
CSCdt74263	Do not allow more than one RSA key through with different attributes.
CSCdt74520	uauth cache not working properly with browsers.
CSCdt75715	fragment command handles input > max inconsistently.
CSCdt75960	ISA fragment method causes PIX Firewall to discard packet.
CSCdt77108	Need to selectively allow unencrypted SSH sessions for debugging.
CSCdt77818	Traceback (crypto CA) if Netscape CA server is misconfigured.
CSCdt82325	Reloads due to exhausted memory while URL filtering heavy traffic.
CSCdt83142	SIP: Call does not go through with static network.
CSCdt85788	PIX Firewall fails to get CRL with Verisign certificate.
CSCdt86132	“709001: FO repliSorry: error” message at boot up.
CSCdt86568	Unexpectedly reloads when URL cache is on and the URL server is unavailable.
CSCdt91309	Interface PAT port detection with for-us traffic ineffective.
CSCdt92339	BUGTRAQ: PIX Firewall should limit number of uauth sessions per source IP.

Table 7 Resolved Caveats (continued)

DDTS Number	Description
CSCdt92450	Multiple websns keepalive daemon starts.
CSCdt93858	kprint message to console when fails to allocate memory block.
CSCdt94747	H.323: PIX Firewall should proxy ACK TPKT if received TPKT only.
CSCdu00856	Emit a warning if an 82542 Wiseman NIC is found in a PIX 535.
CSCdu01056	Reloads while running backup traffic (SQL*Net) through the PIX Firewall.
CSCdu02291	Failover timeout needs to be taken out from failover online help.
CSCdu02673	clear config should be a config mode command.
CSCdu02674	Issues with the service command.
CSCdu04084	Traceback while reading certificate from FLASH.
CSCdu05134	H.323: Call does not go through if calling GW uses slow start.
CSCdu05694	Invalid global command causes traceback (ci/console).
CSCdu05843	ip verify does not work with IPsec.
CSCdu06716	show chunk only shows ulimit chunk .
CSCdu08574	Certificate enroll request fails after deleting current CA and retrying.
CSCdu11774	SIP: Call does not go through with IN proxy (Regression).
CSCdu11781	Reloads during DHCP request when PDM refreshes DHCP Client information.
CSCdu12321	PIX Firewall fails to do write memory if a big command line exists.
CSCdu12909	SIP: Connections for Responses to INVITE not opened correctly.
CSCdu13395	Remove [nailed] parameter from static command online help.
CSCdu13956	Deleting non-default fixup rtsp port also deletes default port.
CSCdu15173	H.323: RAS routine causes memory corruption.
CSCdu18020	PIX Firewall-to-PIX Firewall or PIX Firewall-to-Unity connection fails when using certificates.
CSCdu20593	Xauth: With IRE on rekey, puts internal address entry for uauth .
CSCdu27169	VoIP: Certain embedded IP addresses do not undergo NAT.
CSCdu33209	IPsec Antireplay Checking Ineffective 32-64 sequence numbers back.
CSCdu33543	PIX Firewall PPTP rejects dial-in request after abnormal termination.
CSCdu38206	Configuration lines greater than 255 displayed incorrectly by sh conf .
CSCdu38221	Failover usability: Should warn user if OS version is not the same.
CSCdu38927	PIX Firewall failover should try to allocate additional block if possible.
CSCdu39748	H.323: Generating 50+ calls causes unexpected reload.
CSCdu39906	PIX Firewall should not send stateful updates if peer is down.
CSCdu42645	Kodiak: Some status bits are ignored.
CSCdu42656	Kodiak: AH decapsulation requests not setup correctly.
CSCdu43016	TCP Intercept sends ARP for every proxied syn-ack.

Table 7 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdu43284	H.323: Should make use of NELTS and sizeof and remove extern functions.
CSCdu46309	pix_init should be called after verifying license key.
CSCdu47003	Able to pass disallowed SMTP command through PIX Firewall by sending after mail.
CSCdu48706	clear interface does not clear Gigabit interface counters.
CSCdu49737	aaa telnet console: Failed login attempts should be limited.
CSCdu53473	H.225 and H.245 messages greater than 1024 bytes are not inspected.
CSCdu54495	Unexpected reload when using Websense with TCP4 and url-cache.
CSCdu55206	Traceback while trying to establish a PPTP tunnel (scripted).
CSCdu62647	Kodiak: IPsec encrypt packet interoperability with Cisco IOS software is not working in FTP.

Resolved Caveats - Release 5.3(1)

The caveats in Table 8 are resolved in this release.

Table 8 *Resolved Caveats*

DDTS Number	Description
CSCds66550	out of channels error causes watchdog timeout in logger.
CSCds66052	H323: PIX crash trying to decode non-Cisco nonStandard msg.
CSCds62734	improper casting shortens SA lifetimes.
CSCds58313	PIX crash when no memory & using Ciscos Gatekeepers.
CSCds56721	H323: WDT if debug ras asn/event on.
CSCds55734	negative byte count in show conn output.
CSCds55694	Need show commands for H323.
CSCds54886	Traceback in AAA while trying to parse URL in HTTP GET request.
CSCds53316	Unable to re-establish IPsec SA after default 24hr expiration.
CSCds51955	tracert does not work with interface PAT.
CSCds50982	pix cannot retrieve CRL if first attempt failed because of CA server.
CSCds46349	211001: Memory allocation Error during H.323 stress testing.
CSCds38708	Disallowed commands can piggyback through SMTP with the DATA command.
CSCds34732	some H245 packets not processed because of TPKT lookup in PIX.
CSCds34622	AAA accounting causes panic.
CSCds34475	PIX should consume pre-allocate channel by direction.
CSCds32842	Fixup h323 does not nat 3rd party local/global.

Table 8 Resolved Caveats

DDTS Number	Description
CSCds30699	SMTP stop filtering if DATA command failed.
CSCds29676	Websense caching not working -sho url-cache stat displays wrong info.
CSCds26054	RSA key disappears on standby PIX after failover
CSCds25070	Assertion, traceback every two hours when stateful failover enabled.
CSCds24580	pix needs configurable radius port number
CSCds23698	PIX sends RSET in response to tcp connections with ECN bits set
CSCds22194	Alias not working when DNS server address is included in alias address
CSCds21095	pix pptp stops accepting new connections after some time of operation
CSCds11378	H323 call, Call hangs after 30-40 minutes
CSCds09730	ISAKMP does not work if same network exists on different interfaces
CSCdr93478	PPTP tunnel hashtable insert failed
CSCdr93435	PIX does not open 3rd party Media Channel correctly
CSCdr84484	Write net command causes 1550-byte block leak.
CSCdr77921	Opening a web page with ms2000 mail results continous authentication.
CSCdr48266	PIX assertion t->stack[0] == STKINIT failed, traceback in uauth.
CSCdp67764	Show traffic displays incorrect information.
CSCdr78383	No Fixup H323 still does fixup RAS messages.

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 explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

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

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

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

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

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

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, 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. (0201R)

Copyright © 2000-2002, Cisco Systems, Inc.
All rights reserved.