



# Release Notes for the Cisco Secure PIX Firewall Version 5.1(5)

---

July 2001

## Contents

This document contains the following sections:

- [System Requirements](#)
- [New and Changed Information](#)
- [Installation Notes](#)
- [Limitations and Restrictions](#)
- [Important Notes](#)
- [Caveats](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

## System Requirements

Version 5.1 requires the following:

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, bh515.bin, from Cisco Connection Online (CCO) to let you download the PIX Firewall image with TFTP.
2. PIX Firewall *must* have at least 32 MB of RAM memory or the PIX Firewall unit will not boot. Use the **show version** command to verify how much RAM is in your PIX Firewall unit.



---

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

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

3. PIX Firewall requires at least 2 MB of Flash memory although support is provided for 2 MB, 8 MB, and 16 MB Flash memory. The maximum configuration size with 16 MB Flash memory is 1 MB; with all other Flash memory, it is 340 KB. A PIX Firewall unit equipped with 16 MB Flash memory cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2).
4. If you use mode configuration with the PIX Firewall, any routers on the IPSec connection must run Cisco IOS Release 12.0(6)T or later.
5. If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must obtain 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.)

6. If you are using PFSS (PIX Firewall Syslog Server), we recommend that you install Windows NT Service Pack 6 to fix year 2000 conflicts in Windows NT.
7. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to “[Installation Notes](#)” for new installation requirements.

## PIX Firewall Manager Interoperability

You can use PIX Firewall version 5.1 with the PIX Firewall Manager version 4.3(2)h. Refer to the *Release Notes for the PIX Firewall Manager Version 4.3(2)h* for more information. You can view this document online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/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).

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

## 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 a version 4.2(*n*), 4.4(*n*), or 5.1(*n*) software image.

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>

## New and Changed Information

Version 5.1 consists of bug fixes and new features. More details are provided in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*. You can view this document online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm)

### RFC 2267 DoS Protection Support

You can enable Unicast RPF (Reverse Path Forwarding) protection with the new **ip verify reverse-path** command. With this feature, PIX Firewall provides ingress and egress spoof filtering. This command is described in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

### PIX 506 Support

The PIX 506 is a simplified PIX Firewall unit that supports two Ethernet interfaces without user-customizable access to the inside unit. This unit provides PIX Firewall functionality with support for the full command set except for the **failover** and **session** commands. The PIX 506 contains 32 MB of RAM memory and an 8 MB Flash memory. The maximum configuration size is 340 KB.



**Note**

---

The PIX 506 supports 10BaseT only on both interfaces.

---



**Note**

---

The ACT light on the front of the PIX 506 indicates when the software image successfully loads. On the PIX 515, this light has an alternate meaning relating to use with failover.

---

### Other Release Changes

Additional changes in this release can be found in the following sections of this document:

- [clear configure Command](#)
- [show version Command](#)
- [ISAKMP Notes](#)
- [Syslog](#)
- [Resolved Caveats](#)

The PIX Firewall documentation set has been enhanced to support the PIX 506. In addition, in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*, the information in Chapter 7, formally entitled, “PIX 515 Configuration,” was moved to Chapter 2, “Configuring PIX Firewall” and to the *Installation Guide for the Cisco Secure PIX Firewall Version 5.1*.

### Version 5.1 Features

The sections that follow describe each new feature.

## 16 MB Flash Memory Card Support

PIX Firewall now supports an ISA-bus 16 MB Flash memory card for all PIX Firewall models except the PIX 515 and PIX 506, which already have a Flash memory unit built into the motherboard. Use the new 16 MB Flash memory card to replace your current 2 MB Flash memory card. (You must not use both the old Flash memory card and the new card together.)

Use of the 16 MB Flash memory card increases the maximum configuration size to 1 MB.

The 16 MB Flash memory card driver has been enhanced so that older PIX Firewall models can use the 16 MB card with software version 5.1(1) or later.

## AAA Improvement

The **aaa** command now supports selection by service. See “[aaa Command](#)” for more information.

## Boothelper

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, bh515.bin, from Cisco Connection Online (CCO) to let you download the PIX Firewall image with TFTP. Boothelper only works with version 5.1 or later images and cannot pass the image over a Gigabit Ethernet interface. See “[Installation Notes](#)” for more information. You can view Boothelper information online in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/config.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm)

## Firewall MIB Support

The Cisco Firewall MIB and Cisco Memory Pool MIB are now available. These MIBs provide the following PIX Firewall information via SNMP:

- Buffer usage from the **show block** command
- Connection count from the **show conn** command
- Failover status
- Memory usage from the **show memory** command

For more information, refer to “Using the Firewall and Memory Pool MIBs” in Chapter 3, “Advanced Configurations” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*. You can view this chapter online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/advanced.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/advanced.htm)

## FragGuard and Virtual Re-Assembly

The following virtual re-assembly features are new in version 5.1:

- Version 5.1 enhances IP fragment protection and performs full-reassembly of all ICMP error messages and virtual-reassembly of the remaining IP fragments that are routed through the PIX Firewall. The previous restriction with the FragGuard feature that the initial fragment must arrive first has been lifted.



**Note** Virtual reassembly is currently enabled by default and no mechanism is provided to disable it.

- A new teardrop syslog message has been added to notify of any fragment overlapping and small fragment offset anomalies.

Syslog message, %PIX-2-106020: Deny IP teardrop fragment (size = *num*, offset = *num*) from *IP\_addr* to *IP\_addr* was added in this release to log teardrop.c attacks. This message occurs when the PIX Firewall discards an IP packet with a teardrop signature with either a small offset or fragment overlapping. You should treat this event as a hostile attempt to circumvent the PIX Firewall or the Cisco Secure Intrusion Detection System.

## FTP and URL Logging

You can now log URLs and FTP commands for both inbound and outbound connections. This feature is enabled automatically when you specify syslog level 7 (**debugging**) with the **logging** command.

## Gigabit Ethernet

PIX Firewall now supports 1000 Mbps (Gigabit) Ethernet. The gigabit interface cards use the **gb-ethernet** device name and only have one hardware speed and the following options:

- **1000sxfull**—forces full duplex operation
- **1000basesx**—forces half duplex operation
- **1000auto**—auto negotiates full or half duplex

An example **interface** command for a gigabit interface follows:

```
interface gb-ethernet0 1000auto
```

Gigabit interface cards do not provide information for the extended **show interface** command counters introduced in version 5.0(3).

Gigabit Ethernet uses the same MTU as 10/100 Ethernet.

## Installation Enhancement

See “[Installation Notes](#)” for how to use the Boothelper diskette, and how to download and use a TFTP server, or you can view this information online in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/config.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm)

## IPSec Enhancements

The following IPSec improvements are new to this release:

- IPSec tunnel termination—you can now differentiate UDP IPSec traffic from TCP traffic using the port parameter to the **access-list** command. The use of port ranges can dramatically increase the number of IPSec tunnels. For instance, if a port range of 5000-65535 is specified for a highly dynamic protocol, a possible 60,535 tunnels can be created.

- Multiple interface termination—IPSec now lets you terminate an IPSec tunnel on any and all active interfaces.
- Client termination—you can now enable the PIX Firewall to terminate an IPSec tunnel destined for itself.

The IPSec command interface has the following changes:

1. Any traffic selectable by the **access-list** command and negotiated by IKE can be used. ICMP type and code cannot be used because there is no mechanism to negotiate these selectors by IKE.
2. Multiple **crypto map** command statements can be bound to multiple interfaces. However, only one **crypto map** command statement can be bound to a single interface.
3. **sysopt ipsec pl-compatible** command—the previous need for static routes for non-IPSec traffic is removed.
4. New **debug crypto ipsec** command.

You can view command information online in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/commands.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/commands.htm)

## Java and ActiveX Filtering Improvements

The ActiveX and Java applet filtering implementation has been improved. Formerly, filtering Java applets was handled by the **outbound** command. The new implementation has been placed in the **filter** command and lets users receive a web page but with the Java applets disabled. The previous behavior dropped the connection when an applet was encountered.



### Note

The previous **outbound java** command is being phased out. Cisco recommends that you convert all Java filtering configurations to the **filter java** command.

The ActiveX filtering mechanism, which also is handled by the **filter** command has been improved to more reliably detect objects and screen out their use.

## PPTP Support

Point-to-Point Tunneling Protocol (PPTP) is a layer 2 tunneling protocol which lets a remote client use a public IP network to communicate securely with servers at a private corporate network. PPTP can tunnel the IP protocol. RFC 2637 describes the PPTP protocol.

## RAS V2 Support

RAS (registration, admission, and status) handles multimedia applications such as video conferencing and Voice over IP that require video and audio encoding. PIX Firewall now supports RAS version 2.

## RIP V2 Support

PIX Firewall now supports RIP version 2. This implementation supports Cisco IOS software standards, which conform to RFC 1058, RFC 1388, and RFC 2082 of RIPv2 with text and keyed MD5 authentication.

## Routing Extensions

A number of extensions were added to the **route** command in this release. Refer to [“route Command”](#) for more information.

## RTSP Support

PIX Firewall now provides the **rtsp** option to the **fixup** command. This feature lets PIX Firewall pass RTSP (Real Time Streaming Protocol) packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. See [“fixup rtsp Command”](#) for more information.

## Separate SNMP and Syslog Message Levels

The **logging** command now lets you specify separate message levels for syslog and SNMP. See [“logging Command”](#) for more information.

## System Software Downloads

See [“copy tftp flash Command”](#) for more information on copying a new software image via TFTP. This feature permits remote management where a binary image can be uploaded without accessing monitor mode.

## Xauth Support

The Xauth (Extended Authentication) feature lets you deploy IPsec to remote users to gain the privacy and packet-level authentication available with IPsec. This feature provides authentication by prompting for user credentials and verifies them with the information stored in Cisco Secure Database in the VPN environment (AAA with VPN).

Extended Authentication is negotiated between IKE phase 1 and IKE phase 2 at the same time as mode configuration. Authentication is performed using your existing TACACS+ or RADIUS authentication system.

The extended authentication feature is enabled with the **crypto map** command.

**Note**

---

The Xauth feature requires version 1.1 of the Cisco Secure VPN Client.

---

## XDMCP Support

PIX Firewall now provides support for XDMCP (X Display Manager Control Protocol) to handle an XWindows TCP back connection. XDMCP handling is enabled by default. XDMCP uses UDP port 177. XWindows uses TCP ports 6000 through 6063.

## New Commands

The sections that follow describe the new commands in this release.

## copy tftp flash Command

The **copy tftp flash** command lets you change software images without requiring access to the TFTP monitor mode. An image you download is made available to the PIX Firewall on the next reload (reboot).

The **copy tftp flash** command requires that routing be configured. In certain cases such as with IPSec configuration, a ping from the PIX Firewall to the TFTP server may be successful even without complete routing information. However, the success of the ping command does not guarantee that the **copy tftp flash** command will be successful. This command is described on the **copy tftp flash** command page in Chapter 6, “Command Reference” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

## ip verify Command

You can enable RFC 2267 Denial of Service (DoS) protection with the new **ip verify reverse-path** command. This command is described on the **ip verify** command page in Chapter 6, “Command Reference” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

## vpdn Command

The **vpdn** command implements the PPTP feature. This command is described on the **vpdn** command page in Chapter 6, “Command Reference” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

## Changes to Existing Commands

More details are provided in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*. You can view this document online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm)

## aaa Command

- For HTTP authentication, a username can be up to 30 characters long and a password up to 15 characters long.
- The **aaa include** and **exclude** options let you select which services are permitted or denied from authentication, authorization, and accounting.



### Note

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

## aaa-server Command

The maximum number of AAA servers PIX Firewall lets you specify is 14, not 16 that is described in the **aaa-server** command page in Chapter 6, “Command Reference” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

## access-list Command

- The **show access-list** command now lists a hit count that indicates the number of times an element has been matched during an **access-list** command search.
- The **access-list** command now works correctly with the **name** command so that names can be used in **access-list** commands. [CSCdr46152]

## auth-prompt Command

The maximum length of the prompt string is 235 characters.

## conduit Command

The **show conduit** command now lists a hit count that indicates the number of times an element has been matched during a **conduit** command search.

## clear configure Command

The **clear configure** command no longer sets interfaces into the shutdown state. Previously, the **interface** command for the inside interface would appear as follows after using the **clear configure** command:

```
interface inside auto shutdown
```

## clear interface Command

The **clear interface** command clears gigabit counters and input bytes. It supports gigabit Ethernet interfaces too.

## crypto map client authentication Command

The **crypto map client authentication** command enables the extended authentication (Xauth) feature.

## debug Command

The **debug crypto ipsec** command provides new debug messages. You can display debugging messages with the **logging** command.

## established Command

The **established** command has been enhanced to include a new source port. By designating 0 as the destination port, you can use the **show established** command to display the port as it is allocated. See [“XDMCP Support”](#) for more information.

This change is backward compatible with previous PIX Firewall software versions and will not cause problems with an existing configuration.

## fixup rtsp Command

The **fixup rtsp** command lets PIX Firewall pass RTSP (Real Time Streaming Protocol) packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. PIX Firewall does not support multicast RTSP.

The default port for this command is TCP 554. This command does not fix RTSP UDP connections. PIX Firewall PAT is not supported with the **fixup rtsp** command. PIX Firewall does not yet have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.

## interface Command

The **interface** command now supports the **gb-ethernet** option for Gigabit Ethernet.

## logging Command

The **logging** command now lets you specify different message levels for syslog and SNMP. You can set the message levels for SNMP with the **logging history snmp\_message\_level** command. The **logging trap syslog\_message\_level** command now only sets the syslog message level.

The **logging queue** command lets you specify the number of messages in the syslog message queue. The **show logging queue** command lists the size of the queue, the greatest number of messages in the queue, and the number of messages discarded because queue space was not available to contain them. The size of the queue is limited by available block memory.

## nat Command

The **nat** command has been extended to let you disable NAT and specify an access list that determines which services users on a higher security level interface can access on a lower security level interface. This command lets you mix and match NAT, stateful inspection with the **fixup** command, and the **aaa** command without forcing everything through NAT. The new **nat 0 access-list** command also lets you enable policy NAT based on destination.

## no failover Command

When a failover cable connects two PIX Firewall units, the **no failover** command now disables failover until you enter the **failover** command to explicitly enable failover. Previously, when the failover cable connected two PIX Firewall units and you entered the **no failover** command, failover would automatically re-enable after 15 seconds.

If you reboot the PIX Firewall without entering the **write memory** command and the failover cable is connected, failover mode automatically enables.

## rip Command

Only enabled **rip** command statements appear in the configuration in version 5.1.

## route Command

The following are the extensions to the **route** command:

- The routing table has been improved to let you specify the IP address of a PIX Firewall interface in the **route** command. If the **route** command statement uses the IP address from one of the PIX Firewall unit's interfaces as the gateway IP address, PIX Firewall will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address.
- PIX Firewall also does not accept duplicate routes with different metrics for the same gateway.
- In version 5.1, the CONNECT route entry is supported. (This identifier appears when you use the **show route** command.) The CONNECT identifier is assigned to an interface's local network and the interface IP address, which is in the IP local subnet. PIX Firewall will use ARP for the destination address. The CONNECT identifier cannot be removed, but changes when you change the IP address on the interface.
- You can now enter duplicate **route** command statements with different gateways and metrics.
- You can now enter static **route** command statements with virtual subnets; for example:

```
route outside 10.2.2.8 255.255.255.248 192.168.1.3
route outside 10.2.2.8 255.255.255.255 192.168.1.1
```

This example lets all packets destined to 10.2.2.8/29 be routed to 192.168.1.3 except for packets destined to 10.2.2.8/32, which are routed to 192.168.1.1.

## show failover Command

The items in the top row of the “Standby Logical Update Statistics” section of the **show failover** command are as follows:

- Stateful Obj—PIX Firewall stateful object
- xmit—Number of transmitted packets
- xerr—Number of transmission errors
- rcv—Number of received packets
- rerr—Number of packets received errors

The items in the first column provide an object static count for each statistic:

- General—Sum of all stateful objects
- sys cmd—Logical update system commands; for example, LOGIN and Stay Alive
- up time—Up time, which the Active unit passes to the Standby unit
- xlate—Translation information
- tcp conn—TCP connection information
- udp conn—Dynamic UDP connection information
- ARP tbl—Dynamic ARP table information
- RIF tbl—Dynamic router table information

## show interface Command

The **show interface** command has been enhanced to include eight new status counters. In version 5.1(2) and later, the “unicast rpf drops” counter was added to list the number of packets dropped through use of the new **ip verify reverse-route** command.

## show version Command

The **show version** command now lists the size of Flash memory; for example, the following line appears in the output to indicate 16 MB Flash memory:

```
Flash i28F640J5 @ 0x300, 16MB
```

## show xlate Command

An example of the **show xlate** command output is as follows:

```
Global 10.130.0.101 Local 10.130.0.101 static  
Global 10.130.0.100 Local 10.130.0.100 static
```

The **xlate** command page in Chapter 6, “Command Reference,” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* incorrectly lists connection information in the command output. You can view connection information with the **show local-host** command.

## sysopt connection permit-pptp Command

Allows PPTP traffic to bypass checking of **conduit** or **access-list** command statements. See “[vpdn Command](#)” for more information on PPTP commands and an example of the new **sysopt** command option.

## sysopt ipsec pl-compatible Command

Using the **sysopt ipsec pl-compatible** command no longer requires static **route** statements for every host that needs to start non-IPSec connections through the PIX Firewall. The routing is now handled automatically.

## url-filter Command

The **url-filter** command now can process a URL up to 1024 characters long.

# Installation Notes

1. Refer to either the *Installation Guide for the Cisco Secure PIX Firewall Version 5.1* or Chapter 2, “Configuring PIX Firewall” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* for information on the new Boothelper diskette installation feature and the new configuration version message. Boothelper only works with version 5.1 images. In addition, only specify Boothelper commands in lowercase. You can view this information online at the following website: [http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/config.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm)
2. Do not attempt to load version 5.1 on a PIX Firewall unit containing less than 32 MB of memory. While the PIX Firewall may appear to permit this configuration, upon reboot, the PIX Firewall unit will continuously fail. You can stop this by immediately inserting a previous version diskette into the PIX Firewall unit and then pressing the reboot switch. This note only applies to PIX Firewall units with a diskette drive, not to the PIX 515 or PIX 506.
3. After installing additional memory in a PIX 520, do not remove the memory strips after you install them and have powered on the unit, or the PIX Firewall unit will become inoperable. [CSCdr14559]

4. A PIX Firewall unit containing a 16 MB Flash memory card cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2). [CSCdp38206]
5. Version 5.1 on a PIX 515 cannot be downgraded to pre-version 4.4(1) images. [CSCdp21017]
6. The new **include** and **exclude** options to the **aaa** command are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.

## Limitations and Restrictions

The following limitations and restrictions apply to version 5.1:

1. If you are using a Gigabit Ethernet interface, refer to “[Gigabit Interface Restrictions](#)” for important restrictions on the use of this interface.
2. Loading a PIX Firewall image prior to version 5.1 with Boothelper reboots the PIX Firewall.
3. Only use version 5.1 of the PIX Firewall with version 1.1 or later of the Cisco Secure VPN Client.

## Important Notes

More details are provided in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1*.

## Assertions

Previously, assertions in the code caused an error message to display at the PIX Firewall. In version 5.1, assertions now force the PIX Firewall to fail and display a trace output.

## auth-prompt Command

Web browsers such as Internet Explorer or Netscape Navigator only display the first 23 characters of the string you indicate in the **auth-prompt** command. This limitation is imposed by the browser and is not a PIX Firewall fault. [CSCdp85254]

## Console Access

Under heavy traffic on the 4-port Ethernet board, use of the console becomes much slower. Cisco recommends configuring such units during lighter traffic intervals. [CSCdp14222]

## Default Configuration

The following commands have been added to the default configuration. The default configuration contains the commands that are enabled when you first install PIX Firewall:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
floodguard enable
isakmp identity hostname
```

See “Default Configuration” in Chapter 1, “Introduction” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* for the other commands provided in the default configuration. You can view this chapter online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/config/intro.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/intro.htm)

## DNS Root Name Server Access

A DNS server on a higher level security interface needing to get updates from a root name server on the outside interface cannot use PAT (Port Address Translation). Instead, a **static** command statement must be added to map the DNS server to a global address on the outside interface. [CSCdp48115]

## Failover

The following notes apply to the failover feature:

- All enabled interfaces must be connected between the active and standby units. If an interface is not in use, do not configure the ip address and failover ip address; use the shutdown option to the **interface** command to disable the interface and leave it unconnected. (CSCdr41456)
- The Stateful Failover Logical Update Statistics output that displays when you use the **show failover** command only applies to Stateful Failover, not to the basic failover functionality. The statistics table only displays if a failover link has been configured.
- Failover no longer stops traffic when the 1550-byte pool exhausts. If this pool exhausts and cannot be reallocated on the Standby unit, the Standby unit will now reboot without affecting the Active unit. [CSCdp85718]
- The **failover timeout** command is only used with a non-supported PIX Firewall Engineering feature. To avoid confusion, the **failover timeout** command is not documented, but does appear in the default configuration. You can ignore this command.

## Failure Message

The former PIX Firewall failure message was changed from “Watchdog timer failure - ARF!” to “Watchdog timer failure - Internal system timeout failure -- please provide the output that follows to customer support.”

## FTP

- PIX Firewall now restricts FTP commands so that only FTP servers can submit a 227 reply and only FTP clients can submit a PORT command. Furthermore, the only PORT command permitted can only be one port number lower than the FTP control channel. This change removes the wildcard port for connections created from the PORT command. PIX Firewall now also enforces that the first SYN packet from the dynamic back channel must be from the expected side. [CSCdp86352]
- To access a PAT with passive FTP, use the **fixup protocol ftp strict** command statement with an **access-list** command statement to permit outbound FTP traffic, as shown in the following example:

```
fixup protocol ftp strict ftp
access-list acl_in permit tcp any any eq ftp
access-group acl_in in interface inside
nat (inside) 1 0 0
global (outside) 1 209.165.201.5 netmask 255.255.255.224
```

## Fragment

The **fragment** command provides additional management of packet fragmentation and improves compatibility with NFS.

## Gigabit Interface Restrictions

The following open caveats apply to use of the Gigabit Ethernet interface:

- The Boothelper TFTP image cannot be sent to the PIX Firewall over a gigabit interface. Ensure that the PIX Firewall unit has at least one 10/100 Ethernet interface to convey the image to the PIX Firewall. [CSCdp92050]

## IPSec Notes

The following sections provide useful information about IPSec.

### Certification Authority (CA) Usage

- When using the VeriSign CA, always use the **crloptional** parameter to the **ca configure** command. The following is a sample **ca configure** command:

```
ca configure myca ca 5 15 crloptional
```

In this example, **myca** is the name of the CA and the CA will be contacted rather than the RA. It also indicates the PIX Firewall will wait 5 minutes before sending another certificate request, if it does not receive a response, and will resend a total of 15 times before dropping its request. If the CRL is not accessible, **crloptional** tells the PIX Firewall to accept other peer's certificates.

Without the **crloptional** option, an error occurs when the PIX Firewall validates the certificate during main mode, which causes the peer PIX Firewall to fail. This problem occurs because the PIX Firewall is not able to poll the CRL from the VeriSign CA.

- The lifetime of a certificate and the Certificate Revocation List (CRL) is checked in GMT time. If you are using IPsec with certificates, set the PIX Firewall clock to GMT time to ensure that CRL checking works correctly.
- PIX Firewall only supports the following CA servers:
  - Entrust—PIX Firewall supports the VPN Connector version 4.1 (build 4.1.0.337). Use the **debug crypto ca** command to ensure that the certificate is created correctly. Important error messages only display when the **debug** command is enabled. If you enter the fingerprint value incorrectly, the only warning message that the value is not correct appears in the **debug crypto ca** command output. PIX Firewall supports Entrust/PKI version 4.0b.
  - VeriSign—through the VeriSign Private Certificate Services (PCS) and the OnSite service that lets you establish a CA system for issuing digital certificates. When using VeriSign CA Server, always use the **crloptional** option with the **ca configure** command.

## Cisco Secure VPN Client

Cisco Secure VPN Client version 1.1 or later should only be used with PIX Firewall version 5.1.

When two policies are configured on the Cisco Secure VPN Client for different PIX Firewall interfaces, after the PIX Firewall unit initiates a rekey, the Client loses the ability to differentiate between the interfaces. This condition causes the message, “Cannot match Policy Entry for received IDs” to display and can cause a loss of connections. Once dropped, the tunnels cannot be re-established. [CSCdp88761]

## crypto map Command

The **crypto map** *map\_name* **interface** *if\_name* command causes any currently running SAs (security associations) to be deleted.

## ISAKMP Notes

- Version 5.1(2) and later: When configuring ISAKMP for certificate-based authentication, it is important to match the ISAKMP identity type with the certificate type. The **ca enroll** command used to acquire certificates will, by default, get a certificate with the identity based on hostname. Therefore, Cisco recommends you set each participating peer's identity to hostname. Otherwise, the ISAKMP security association established during IKE phase 1 may fail. [CSCdp93890]
- If an ISAKMP SA expires, the IPsec tunnel for the expired ISAKMP SA continues for the remaining time. If a PIX Firewall peer reboots before the ISAKMP SA expires, the keep alive fails to note that the other peer is not there and packets are silently dropped until the SA expires. [CSCdp86785]
- All **isakmp** command policies now appear in the configuration. Previously, default values were not listed. You can view this information with the **show isakmp policy** command.
- When the Cisco Secure VPN Client is using aggressive mode, the ISAKMP identity of the PIX Firewall should be configured to use the **address** parameter:

```
isakmp identity address
```

Using the **isakmp identity hostname** command on the PIX Firewall with aggressive mode configured on the Cisco Secure VPN Client causes the tunnel setup to fail because of the mismatch in identity.

## Mode Configuration

PIX Firewall does not proxy ARP for addresses in the mode config pool. To enable connectivity of a remote client to the internal network, addresses in the mode config pool cannot overlap with any of the directly connected networks to the PIX Firewall. In addition, static **route** command statements need to be configured on the internal networks to direct traffic destined for the mode config pool to the PIX Firewall.

## SA Lifetimes

If you enter the **show crypto ipsec sa** command and the screen display is stopped with the More prompt, and if the SA lifetime expires while the screen display is stopped, subsequent display information may refer to a stale SA and the SA lifetime values that display will be invalid. [CSCdm59768]

## NAT

The PIX Firewall has an implicit default route to the outside interface for configuring NAT.

## PIX 515 Rear Panel

The LED on the rear panel of a PIX 515 labeled FDX actually shows whether a link is up or down. The LED labeled LINK actually displays network activity. In addition, the four-port Ethernet card contains two LEDs at each interface connector. The left LED indicates 100 Mbps network connectivity and whether the link is up or down and the right LED indicates network activity.

## PFSS

PFSS (PIX Firewall Syslog Server) now renames log files using the last modification date as the file type. For example, if PFSS needs to create a monday.log file and the filename already exists, PFSS checks the last modification date for the original file and finds, for example, that it was last modified on January 24, 2000. PFSS then renames the original file monday.012400 and moves it to the backup directory, which is named "backup." Then PFSS creates monday.log for the current log data.

PFSS attempts to create the backup directory whenever PFSS is restarted. If the directory exists, PFSS adds a message in the pfss.log file as follows:

```
mmm dd yyyy hh:mm:ss ThreadInit: Could not create backup directory
```

where *mmm dd yyyy hh:mm:ss* is a timestamp. This message can be ignored if the backup directory exists. If the directory does not exist and you see this message, then you should determine why the directory cannot be created.

## PIX Setup Wizard

PIX Firewall Setup Wizard disables the **pager** command while configuring the PIX Firewall. After the wizard completes, use the **clear pager** command to return it to the default value. [CSCdr01768]

## SNMP

- Syslog messages generated by the SNMP feature now specify the interface name instead of an interface number.
- The cfwBufferStatTable object does not list 4096-byte blocks. Refer to “Using the Firewall and Memory Pool MIBs” in Chapter 3, “Advanced Configurations,” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* for detailed information on how to view the values in this object.

## SQL\*Net

PIX Firewall uses port 1521 for SQL\*Net. This the default port used by Oracle for SQL\*Net; however, this value does not agree with IANA port assignments. [CSCdp33907]

## Syslog

The following syslog changes occurred in version 5.1:

- Version 5.1(2) and later: If a bad TCP header length is detected, syslog message %PIX-6-302002 reports an incorrect number of bytes transferred. The %PIX-5-500003 syslog message has been added to indicate when a bad TCP header length occurs. The format for the new message is as follows:

```
%PIX-5-500003: Bad TCP hdr length (hdrhlen=bytes, pktlen=bytes) from src_addr/sport to
dest_addr/dport, flags: tcp_flags, on interface int_name
```

Refer to the *System Log Messages for the Cisco Secure PIX Firewall Version 5.1*, which you can view online at the following website:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v51/syslog/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/syslog/index.htm)

- Version 5.1(2) and later: %PIX-4-500004 was added to indicate an invalid transport field for a protocol. The format for the new message is as follows:

```
%PIX-4-500004: Invalid transport field for protocol=ip_proto, from
src_addr/src_port to dest_addr/dest_port
```

- The following messages are new in version 5.1: %PIX-2-106020, %PIX-1-107001, %PIX-1-107002, %PIX-6-110001, %PIX-3-110002, %PIX-3-208005, %PIX-3-213001, %PIX-3-213002, %PIX-3-213003, %PIX-3-213004, %PIX-6-312001, %PIX-4-403101, %PIX-4-403102, %PIX-4-403103, %PIX-4-403104, %PIX-4-403106, %PIX-4-403107, %PIX-4-403108, %PIX-4-403109, %PIX-4-403110, %PIX-5-500001, %PIX-5-500002, %PIX-6-603101, %PIX-6-603102, %PIX-6-603103, %PIX-6-603104, %PIX-6-603105, %PIX-2-709007.
- The following messages were appended with the string “on interface *int\_name*” (the interface name to which the message applies): %PIX-2-106003, %PIX-2-106006, %PIX-6-106015, %PIX-2-106016, %PIX-6-109002, %PIX-6-109005, %PIX-6-109006, %PIX-6-109007, %PIX-6-109008, %PIX-6-109009, %PIX-3-109010, %PIX-2-201003.
- %PIX-1-103002 was incorrectly listed in the version 5.0 documentation as a failover failure message when it actually indicated that the other unit was okay.
- %PIX-2-109011 formerly appeared at severity level 5.
- %PIX-6-302002 now ends with “*duration time bytes num (chars)*.”
- %PIX-5-304001 formerly appeared at severity level 6.
- %PIX-3-304006 changed so that “trying *IP\_addr*” was deleted from the message.
- %PIX-2-304007 formerly appeared at severity level 3.
- %PIX-6-307001 formerly appeared at both severity levels 6 and 3.
- %PIX-7-702301 formerly appeared at severity level 3.
- %PIX-3-702302 formerly appeared at severity level 7.
- The following messages were deleted: %PIX-2-106008, %PIX-2-106009, %PIX-2-106017, %PIX-2-110003, %PIX-3-202002, %PIX-3-202003, %PIX-3-202004, %PIX-3-209001, %PIX-3-209002, and %PIX-3-304006.

**Note**

Some syslog messages contain linefeeds. Because the Solaris version of syslog, known as syslogd, only stores the first line sent, logging information on these messages is incomplete. One such message, appears truncated on a Solaris system as follows:

```
[CSCdp87564]
```

```
%PIX-6-602301: sa created,
```

## URL Logging

Inbound and outbound URLs are now logged by setting the **logging** command to the **debugging** option. However, URL filtering only affects outbound connections.

## URL Size

The maximum length of a URL string passing through the PIX Firewall can now be up to 1024 characters in length.

# Caveats

## Open Caveats

Table 1 lists open caveats for the 5.1(5) release.

**Table 1** Open Caveats

DDTS Number	Description
CSCdu74320	Unable to get CRL from Verisign CA, negotiation fails if CRL is required.
CSCdu71921	PIX Firewall is unable to get certs if /cgi-bin is used instead of cgi-bin.
CSCdu63411	Xauth:IRE rekey using different username/password,uauth remains the same.
CSCdu56940	Trace back (557poll thread) while running IPsec stress tests.
CSCdu53971	Misconfigured failover ifc a.b.c.d lines cause flip-flops.
CSCdu50874	IPsec should not check anti-replay in ESP with no authentication.
CSCdu36628	PIX Firewall neither uses nor discards CRL if time < last CRL update of CA.
CSCdu35560	Netbios does not work with PIX Firewall IPsec.
CSCdt85788	PIX Firewall fails to get CRL after reboot.
CSCdt65603	PIX Firewall gives wrong prompt when doing xauth.
CSCds85080	IKE Main mode proposal flooding reboots PIX.
CSCds62051	Clear config secondary does not clear ca config.
CSCds60270	PIX Firewall unable to establish tunnel with peer if peer changes keys or id.
CSCds56725	Traceback (Crypto CA thread) when retrieving a large CRL.
CSCds25307	NMI (vector 0x0000002 in trace back) during large file transfer.

**Table 1** Open Caveats (continued)

DDTS Number	Description
CSCdr68928	When the certificate request fails it still says pending.
CSCdp73853	Debug crypto ca messages intermixed on console.

## Resolved Caveats

Table 2 lists the open caveats for the 5.1(5) release.

**Table 2** Resolved Caveats

DDTS Number	Description
CSCdu55206	Trace back while trying to establish a PPTP tunnel (scripted).
CSCdu48706	Clear interface clears gigabit interface counters and the input bytes.
CSCdu47003	Able to pass disallowed SMTP command through PIX Firewall, by sending after mail.
CSCdu46309	pix_init should be called after verifying license key.
CSCdu39906	PIX Firewall should not send stateful updates if peer is down.
CSCdu38927	PIX Firewall failover should try to allocate additional blk if possible.
CSCdu38206	Config lines greater than 255 displayed incorrectly by <b>sh conf</b> command.
CSCdu33543	PIX Firewall PPTP rejects dial-in req after abnormal termination.
CSCdu33209	IPSec Antireplay Checking Ineffective 32-64 sequence numbers back.
CSCdu13956	Deleting non-default fixup rtsp port also deletes default port.
CSCdu12321	PIX Firewall fails to do write mem, if a big cmd line exists.
CSCdu05843	<b>ip verify</b> command does not work with IPSec.
CSCdu05694	Invalid <b>global</b> command causes trace back (ci/console).
CSCdu02673	<b>clear config</b> command should be a <b>config mode</b> command.
CSCdu02291	Failover timeout needs to be taken out from failover on line help.
CSCdu01056	Reload while running backup traffic (SQL*Net) through PIX Firewall.
CSCdt86132	709001: FO repliSorry: error message at boot up.
CSCdt82325	Reload due to exhausted memory while URL filtering heavy traffic.
CSCdt75960	ISA fragment method causes PIX Firewall to discard packet.
CSCdt75715	fragment cmd handles input > max inconsistently.
CSCdt71192	Stateful Failover PIX Firewall logs duplicate messages on syslog server.
CSCdt69676	Enable UniRPF for-us traffic.
CSCdt69667	Encryption layer for tcp port 1467 uses up lots of memory.
CSCdt65464	MIB-II object interfaces.ifSpeed not supporting GigE card.
CSCdt62968	Reboot with filter java and nat 0 access-list.
CSCdt60487	PIX Firewall reboots dumping trace.
CSCdt57251	PIX Firewall should not allow frag chain > frag database size.

**Table 2 Resolved Caveats (continued)**

<b>DDTS Number</b>	<b>Description</b>
CSCdt56080	Trace back trying to build PPTP tunnel and RADIUS server unavailable.
CSCdt54951	Standby unit incorrectly creates udp conn and generates 210010 syslogs.
CSCdt49906	Virtual HTTP/Telnet does not work if intf 0 is not in lowest sec level.
CSCdt40837	PIX Firewall show block has 1552 size entry.
CSCdt40713	xlate error when portmap pool exhausted results in rogue conns.
CSCdt39820	Syslog for memory allocation error used improperly in places.
CSCdt39174	vpdn group dns/wins command is not fully replaced by a new one.
CSCdt39076	PIX Firewall does not error if 0.0.0.0/net add is specified for dns in vpdn gp.
CSCdt38616	Rip routes have a metric of one added.
CSCdt38205	Stateful Failover should not generate syslog when out of mem blk.
CSCdt37028	Redundant error checking can cause trace back within first trace back.
CSCdt31630	Block leaks in fragment database.
CSCdt30628	Help static does not mention embryonic connection limit.
CSCdt28399	<b>vpdn group pp</b> followed by anything is accepted. No error msg.
CSCdt22910	Trace back in ISAKMP_RECEIVER when the VPN 3000 client disconnects.
CSCdt22085	PIX Firewall: with names, host route changes to default route on reload.
CSCdt15446	Incorrect interface state on standby unit.
CSCdt11716	clear xlate prints 305007 syslog message on standby unit.
CSCdt06447	PIX Firewall going out of memory block in Stateful Failover.
CSCdt05025	LU look NAT failed -> NAT is disabled.
CSCdt04772	Make fragment database limits configurable.
CSCdt04241	Remove debugging kprint statement from Stateful Failover.
CSCds92738	Standby PIX Firewall print confusing inconsistent xlate debug msg.
CSCds92693	sh loc and/or sh conn during GC could cause list corruption.
CSCds90802	PIX Firewall- NFS-disallow packets of more than 12 fragments.
CSCds90792	Fixup smtp blocks emails when and <CR><LF>are not in the same pack.
CSCds89281	hdb_sweep thread may get starved under heavy system load.
CSCds82096	B flag set for both inbound and outbound connection.
CSCds77371	Static ARP is not static.
CSCds74609	Retransmit causes connection to exit embryonic too early.
CSCds74352	The <b>IP verify</b> command does not work if connection is established.
CSCds74244	Reload if Active and Standby units write mem at same time.
CSCds73666	Copyright notice obscures config problems.
CSCds72499	Assertion and trace back after receiving faulty DHCPDISCOVER packet.
CSCds70898	The <b>Fixup ftp strict</b> does not work some ProFTPD setup.
CSCds67865	WDT on secondary failover PIX Firewall 520.

**Table 2** Resolved Caveats (continued)

DDTS Number	Description
CSCds66550	Out of channels error causes watchdog timeout in logger.
CSCds64958	Strict FTP does not work in active mode with verbose FTP server.
CSCds63626	IP verify fails if ip spoofed packets destined to PIX Firewall outside ifx.
CSCds63569	Max sockets/tcp_channels need to set according to max channels.
CSCds63501	LU updates for UDP conn are not properly propagated to standby unit.
CSCds60165	PIX Firewall NFS mount / sunrpc does not work without opening ports gt 1024.
CSCds59315	Sysopt uauth allow-http-cache needed in 5.1.x.
CSCds55734	Negative byte count in <b>show conn</b> command output.
CSCds54786	<b>interface</b> command does not recognize unit for hw_speed.
CSCds54777	PPTP stops Wrong EchoID and ResultCode transmitted in response to EchoRQ.
CSCds53633	No syslog (603104: PPTP Tunnel created) displayed until tunnel delete.
CSCds52853	Help crypto has two entries for dynamic-map.
CSCds51960	Ping with ICMP identification of zero and PAT failed.
CSCds51955	Tracert does not work with interface PAT.
CSCds50982	PIX Firewall cannot retrieve CRL if first attempt failed because of CA server.
CSCds50002	PPTP: win95 CHAP authentication loops forever when it should fail.
CSCds49991	PPTP: telnet/ftp does not work with win95 client.
CSCds45528	Debug packet output always print tcp hlen field as 0.
CSCds44305	After reboot, PIX Firewall goes to monitor mode.
CSCds38708	Disallowed commands can piggyback through SMTP with the DATA command.
CSCds38456	PIX Firewall timeout function wakeup earlier than the specified timeout value.
CSCds34622	AAA accounting causes panic.
CSCds30449	<b>vpdn/aaa</b> command not returning an error when entered into config.
CSCds25070	Assertion, trace back every two hours when Stateful Failover is enabled.
CSCds21095	PIX Firewall PPTP stop accepting new connections after sometime of operation.
CSCds19078	PIX Firewall key cutter uses ports allowed verbiage.
CSCds16915	Watchdog time-out when doing ping with debug packet on token-ring int.
CSCdr78505	PIX Firewall does not compute the RIP v2 updates for the default route.
CSCdr77921	Opening a web page with ms2000 mail results in continuous authentication.
CSCdr48472	conn needs to be deleted from clear? command page.
CSCdr48266	PIX Firewall assertion t->stack[0] == STKINIT failed, trace back in uauth.
CSCdr04004	Small arp timeouts cause short periods of packet loss.
CSCdp99518	No warning is given when you try to configure unsupported pfs gp5.
CSCdp67764	<b>Show traffic</b> displays incorrect information.

## Related Documentation

Use this document in conjunction with the PIX Firewall documentation available online at the following site:

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

Cisco provides PIX Firewall technical tips at the following website:

[www.cisco.com/public/technotes/serv\\_tips.shtml](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](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](mailto: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.

