



Text Part Number: 78-6804-01

# Release Notes for the PIX Firewall Version 4.4(1)

---

## June 1999

This document describes the changes for the 4.4(1) version of the PIX Firewall software.

## Contents

- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Related Documentation
- Cisco Connection Online
- Documentation CD-ROM

In the sections that follow, if an item is associated with a bug fix or workaround, the customer service number follows the note in brackets; for example, [CSCdk00000]. Bugs are summarized in the section "Caveats." If you have a CCO login, you can view additional information about each bug fix at:

<http://www.cisco.com/kobayashi/bugs/bugs.html>

## System Requirements

The information contained in these release notes applies to all PIX Firewall hardware models running software version 4.4 or later.

Version 4.4 requires at least 16 MB (an optional 128 MB upgrade is available). You can verify how much memory you have with the **show version** command.

---

### Corporate Headquarters

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

Copyright © 1999  
Cisco Systems, Inc.  
All rights reserved.

Version 4.4 supports one of the following interface combinations:

- One 4-port Ethernet card and one or two Ethernet or Token Ring cards, which can be intermixed such as a 4-port Ethernet card and two Token Ring cards
- Up to four single-port Ethernet or Token Ring cards, either separate or intermixed
- Two FDDI cards

## New and Changed Information

Version 4.4 includes the following features.

### New Features in Version 4.4(1)

The sections that follow describe the features in version 4.4(1).

#### AAA Server Groups

PIX Firewall lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic; such as, a TACACS+ server for inbound traffic and another for outbound traffic. Another use is where all outbound HTTP traffic will be authenticated by a TACACS+ server, and all inbound traffic will use RADIUS.

AAA server groups are defined by a tag name that directs different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 16 tag groups and each group can have up to 16 AAA servers for a total of up to 256 AAA servers.

The **aaa** command references the tag group. The **aaa-server** command replaces the **radius-server** and **tacacs-server** commands.

---

**Note** The previous server type option at the end of the **aaa authentication** and **aaa accounting** commands has been replaced in version 4.4 with the **aaa-server** group tag. Backward compatibility with previous versions is maintained by the inclusion of two default protocols for TACACS+ and RADIUS. Hence, you can use the default groups and your existing **aaa** commands will work in version 4.4 as they did in previous versions. When you install version 4.4, PIX Firewall will convert your previous use of the **radius-server** and **tacacs-server** command statements to the new **aaa-server** command.

---

Refer to the *Configuration Guide for the PIX Firewall Version 4.4* for a description of the **aaa** and **aaa-server** commands.

#### ActiveX Blocking

ActiveX controls, formerly known as OLE or OCX controls, are components you can insert in a web page or other application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information. These controls cause potential problems for the network clients such as, causing workstations to fail, introducing network security problems, or being used to attack servers.

This feature blocks HTML `<object>` tags and comments them out within the HTML web page. This functionality has been added to the **filter** command with the **activex** option.

---

**Note** The <object> tag is also used for Java applets, image files, and multimedia objects, which will also be blocked out by the new command.

---

**Note** If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, PIX Firewall cannot block the tag.

---

**Note** ActiveX blocking does not occur when users access an IP address referenced by the **alias** command.

---

## FDDI

PIX Firewall supports two FDDI network interfaces. These interfaces cannot be used with Ethernet or Token Ring interfaces.

The Cisco FDDI card complies with ANSI specification ASC X3T9.5, which is a peer to the Ethernet IEEE802.3 or Token Ring IEEE802.5 specifications. The FDDI driver supports failover. The **show interface** and **show version** commands indicate that a FDDI card is installed.

## PIX 515

The new PIX 515 provides an entry into the low-cost firewall market and contains two Ethernet 10/100 interfaces on its motherboard, 16 MB Flash memory, and 32 MB of RAM. The basic model with 32 MB of RAM will accept up to 68,000 simultaneous connections.

---

**Note** If you purchase optional feature licenses, you can upgrade the PIX 515 to add failover access, additional system memory to 64 MB or 128 MB, a Private Link VPN card, and additional Ethernet interfaces up to the version 4.4 maximum of 6 interfaces. Installing additional interface cards or upgrading the system memory requires opening the chassis. Without the feature licenses, additional boards, failover, or memory upgrades are ignored. The PIX 515 has two PCI slots available for Private Link and an Ethernet card, or for two Ethernet cards.

---

Images are downloaded via TFTP across the network from any interface.

---

**Note** In version 4.4, the PIX 515 only accepts Ethernet interface cards.

---

Refer to the “PIX 515” section in the “Important Notes“ section for more information.

## Feature-Based License Key

For the PIX 515, there are two available license keys. The basic key allows the use of two Ethernet interfaces without failover support, while the unrestricted key enables use of failover and up to six Ethernet interfaces.

### Four-Port Ethernet Card Support

PIX Firewall now supports an optional Cisco 4-port Ethernet interface card. This component provides four 10/100 Ethernet connections and has autosense capability. Connectors on the 4-port card are numbered top to bottom sequentially; however, the actual device number depends on the slot in which the 4-port card is installed. Table 1 shows how the top connector is numbered.

**Table 1**                    **Numbering Devices With a 4-Port Connector**

Slot 0 Contains	Slot 1 Contains	Slot 2 Contains	4-Port Top Connector is:
4-Port	Any	Any	ethernet0
Ethernet	4-Port	Any	ethernet1
Ethernet	Ethernet	4-Port (required location on PIX 515)	ethernet2
Token Ring	4-Port	Any	ethernet0
Token Ring	Token Ring	4-Port	ethernet0
Token Ring	Ethernet	4-Port	ethernet1
Ethernet	Token Ring	4-Port	ethernet1

---

**Note** With the 4-port card, having a card in slot 3 makes the number of interfaces greater than six; while the card in slot 3 cannot be accessed, its presence does not cause problems with the PIX Firewall.

---

### Six Interfaces

With the inclusion of a 4-port Ethernet card and two single port Ethernet or Token Ring interface cards, the PIX Firewall can support up to 6 interfaces.

### TCP Half-Close Timeout

TCP half-close connections can now be separately managed with the new **half-closed** option to the **timeout** command. Also, half-close connections now do not add to the maximum connection count that you can set with the **nat** and **static** commands.

### Telnet Authentication Prompts

The **auth-prompt** command can now display separate authentication prompts for user authentication via Telnet depending on whether the login is accepted or rejected.

### TFTP Image Download

Because the PIX 515 does not have a diskette drive, you need to send a binary image to the PIX 515 using the Trivial File Transfer Protocol (TFTP). The PIX 515 has a special mode called monitor mode that lets you retrieve the binary image over the network. When you power on or reboot the PIX 515, it waits 10-seconds during which you can send a BREAK character or press the Escape key to activate monitor mode. While in monitor mode, you can enter commands that let you specify the location of the binary image, download it, and reboot the PIX 515 from the new image. If you do not activate monitor mode, the PIX 515 boots normally from Flash memory.

Refer to the **monitor** command page in Chapter 5, "Command Reference" in the *Configuration Guide for the PIX Firewall Version 4.4* for more information on this feature.

## New Commands

The following are new commands in version 4.4(1):

- **aaa-server**—lets you specify AAA server groups. Refer to “AAA Server Groups” for more information.
- **clear blocks**—keeps the maximum count to whatever number is allocated in the system and equates the low count to the current count.
- **clear conduit**—removes all **conduit** command statements from your configuration.
- **clear establish**—removes all **establish** command statements from your configuration.
- **clear fixup**—removes **fixup** commands from the configuration that you added. Does not remove the default **fixup protocol** commands.
- **clear interface**—resets all of the statistics for FDDI, Token Ring, and Ethernet interface cards except those that count normal traffic.

## Changed Commands

Table 2 lists command changes in version 4.4.

**Table 2** Command Changes

Command	Change	Version
<b>aaa</b>	<p><b>1</b> The last parameter in an <b>aaa</b> command is now the <b>aaa-server</b> group tag. An example of how this parameter is used is as follows:</p> <pre>aaa-server AuthOut protocol radius aaa-server AuthOut (inside) host 10.1.1.2 abc123 timeout 5 aaa authentication any outbound 0 0 0 0 AuthOut</pre> <p>In this example, the <b>AuthOut</b> server group tag is created with the <b>aaa-server</b> command and then referenced by the <b>aaa authentication</b> command.</p> <p><b>2</b> The <b>aaa authentication serial console</b> command lets you require authentication verification to access the PIX Firewall’s serial console. This command also logs to a syslog server changes made to the configuration from the serial console. The <b>serial</b> option requests a username and password before the first prompt on the serial console connection. The <b>aaa telnet</b> option forces you to specify a username and password prompts before the first command line prompt of a Telnet console connection. The <b>enable</b> option requests a username and password before the enable prompt for serial or Telnet connections.</p>	4.4(1)
<b>auth-prompt</b>	<p><b>1</b> The new <b>accept</b> and <b>reject</b> options let you specify different prompts when Telnet user authentication attempts are accepted or rejected.</p> <p><b>2</b> The new <b>prompt</b> option lets you specify the prompt. For backward compatibility, this option is not required.</p>	4.4(1)
<b>filter</b>	<p><b>1</b> The <b>activex</b> option lets you block ActiveX controls in an HTML web page. The format for the command is:</p> <pre>filter activex port local_ip mask foreign_ip mask</pre> <p><b>2</b> When the <b>filter url allow</b> option is in use, the PIX Firewall now will attempt to switch to another WebSENSE server when a server goes offline.</p>	4.4(1)
<b>show interface</b>	Information is shown for FDDI and 4-port adapters.	4.4(1)

**Table 2 Command Changes (Continued)**

Command	Change	Version
<b>show version</b>	Lists information for FDDI, the license type, and the PIX Firewall model type.	4.4(1)
<b>sysopt</b>	<p>The <b>sysopt connection enforcesubnet</b> command now applies only to inbound connections.</p> <p>To configure the PIX Firewall to detect spoofed IP addresses, use explicit <b>conduit deny</b> command statements in the configuration; for example:</p> <pre>conduit deny ip any in_host_net1 in_host_net1_mask conduit deny ip any in_host_net2 in_host_net2_mask</pre> <p>Replace <i>in_host_netn</i> with the addresses on the internal network.</p>	4.4(1)
<b>terminal</b>	Sets the width for displaying command output. The terminal width is controlled by the command: <b>terminal width nm</b> , where <i>nm</i> is the width in characters. Permissible values are 0, which means 511 characters, or a value in the range of 40 to 511. If you enter a line break, it is not possible to backspace to the previous line.	4.4(1)
<b>timeout</b>	The <b>half-closed hh:mm:ss</b> option lets you set the duration that a TCP half-close connection can exist before being freed.	4.4(1)
<b>write memory</b>	<p><b>1</b> Previous PIX Firewall versions halted traffic during the execution of the <b>write memory</b> command; version 4.4 lets traffic continue while this command completes.</p> <p><b>2</b> If another PIX Firewall console user tries to change the configuration while you are executing the <b>write memory</b> command, the user receives the following messages:</p> <pre>Another session is busy writing configuration to memory Please wait a moment for it to finish</pre> <p>After the <b>write memory</b> command completes, PIX Firewall lets the other command complete.</p>	4.4(1)

## Removed Components

The following commands have been removed in version 4.4:

- **radius-server**—replaced by the **aaa-server** command.
- **tacacs-server**—replaced by the **aaa-server** command.

In addition, the PIX Firewall Setup Wizard and the PIX Firewall Manager products have been dropped from the PIX Firewall product line.

---

**Note** PIX Firewall Manager version 4.3(2)b now works with version 4.4 but does not support the new features in version 4.4. The *PIX Firewall Manager Release Notes Version 4.3(2)b* are only available online in CCO (Cisco Connection Online).

---

## Installation Notes

PIX Firewall only supports configuration upgrades from version 4.2(x) and later. With versions previous to 4.2(x), save your configuration to an ASCII text file using your terminal configuration program before upgrading, and write down your activation key. Table 3 lists the upgrade path to use to get to the current version.

**Table 3 Upgrade Paths for Older Versions**

If Your Pix Firewall Version is:	Install This Version:
2.7.x	3.0, then upgrade to the next version
3.0	4.0.7, then upgrade to the next version
4.0.7	4.1(7), then upgrade to the next version
4.1(5) or later	4.2(x), then upgrade to the next version
4.2(x)	4.4

- Before upgrading, copy your configuration to diskette with the **write floppy** command and write down your license activation key. You must have a copy of your activation key to restore a previous version from diskette.
- If you are installing a 4-port Ethernet card, the card appears to have a slot connector longer than a PCI slot. The card does work in the PCI slot with overhang at the rear of the connector. Do not try to insert it in one of the larger ISA slots.

## Limitations and Restrictions

This section contains critically important information.

- For Ethernet, PIX Firewall only supports the Intel 10/100, Cisco 4-port, and 3Com 3c590 and 3c595 cards. All other Ethernet cards generate an error message and the card is ignored. [CSCdm05900]
- The PIX Firewall Manager (PFM) will be replaced by another GUI management tool later this year, and PFM will not be upgraded with version 4.4 changes. PFM version 4.2(3)b has been issued, which works with PIX Firewall version 4.3 and 4.4.

## Important Notes

The following sections contain usage information not included in other documentation or requiring special emphasis.

### Interface Names

The maximum length of an interface name is 48 characters, not 255 as stated in the previous *Configuration Guide for the PIX Firewall Version 4.3*, or 49 as stated in the error message in the software.

### Interface Types

The startup messages and the **show interface** and **show version** commands now list the Ethernet card type correctly. Formerly, all Ethernet cards were listed as i82557.

## Maximum Configuration Size

The maximum size of a configuration is 1 MB. This is true for both the PIX 515 with its 16 MB Flash memory card, the PIX 520 with its 2 MB Flash memory card, and any previous PIX Firewall models with the 2 MB Flash memory card.

## MD5 Authentication for the link Command

The **md5** option to the **link** command does not work as described in the online help for the **link** command and will cause spurious results if used as described. [CSCdm42633]

To use the **md5** option:

**Step 1** Create a link with the associated key.

**Step 2** Specify the **md5** option.

For example:

```
link (inside) 192.150.49.133 1 123abc
link (inside) 192.150.49.133 md5
```

The first **link** command statement creates an encrypted path from the current Private Link-equipped PIX Firewall to the remote PIX Firewall at 192.150.49.133. The encryption key is in the first (of 7) key group and has the value 123abc. The second **link** command statement specifies that MD5 authentication will be required for this link.

## PAT

One Port Address Translation (PAT) **global** statement is permitted per interface, but not two or more for a specific interface. This feature has been available since version 4.2(4) but was not documented.

## PFSS

- The PIX Firewall Syslog Server (PFSS) now puts the disk empty watch and disk full watch settings in the pfss.log file. In version 4.3, viewing these settings required use of the Windows **regedit** command. [CSCdk90988]
- Also in version 4.4, when the PFSS detects a full disk, it causes the Windows NT system to repeatedly beep. PFSS also causes the Windows NT system to beep each time the duration of the `disk_full_watch_timer` completes. (The `disk_full_watch_timer` duration is set with **-f** parameter from the **Start>Settings>Control Panel>Services** menu on the Windows NT system.)

## PIX 515

- In version 4.4, the inside and outside interfaces are those attached to the motherboard. The two additional slots must be used for perimeter interfaces.
- When using the **monitor** command (available in boot mode) to download a TFTP image, only one line can be pasted into the **monitor** command buffer from your terminal at a time. If more than one line is pasted, the first line is accepted, the second line is truncated, and the other lines are ignored.

## Telnet Access to PIX Firewall Console

Telnet access to the PIX Firewall's console is available from all internal interfaces, but not the outside interface. [CSCdk91375]

## Caveats

Refer to the previous versions of the PIX Firewall release notes for information on bugs in previous releases. On the Web, you can view previous versions of the PIX Firewall release notes at:

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

If you have CCO access, you can view additional information about each open or resolved caveat at:

<http://www.cisco.com/kobayashi/bugs/bugs.html>

## Open Caveats

The open caveats for version 4.4(1) are:

- CSCdm42633—There is a dependency when using the **link** command that is not mentioned in the online help. If Private Link is incompletely configured with just the **md5** option specified (as **link (if\_name) ip\_address key-id md5**), then an incomplete entry appears in the link table (viewable with the **show link** command). In addition, the message “Unable to find key” appears on the PIX Firewall command line for every interval specified by the **age** command until you either complete the Private Link configuration or reboot the PIX Firewall.
- CSCdm41218—If you use the **nat 0** or **static** command to give outbound access to a host on the inside, the PIX Firewall changes the destination address on the echo-request. The problem only manifested itself when trying to access a perimeter interface. Using a combination of **nat** and **global** command statements solves the problem.
- CSCdm40856—The **no aaa authentication telnet** command reboots the PIX Firewall. You must specify at least the **no aaa authentication telnet console** command to successfully use this command. Cisco recommends saving your configuration to Flash memory when changing the configuration.
- CSCdm36005—The **logging on** command does not propagate from the Active unit to the Standby unit when the units are synchronized. The workaround is to enter the **logging on** command on the Active unit after the Standby unit is online.
- CSCdm35429—The maximum configuration size is 1 MB. This is true for both the 2 MB Flash memory units on the PIX 520 and earlier models, as well as the 16 MB unit on the PIX 515.
- CSCdk91107—Setting the MTU on an interface to greater than or equal to the physical MTU causes Private Link to fail.

Also, open caveats in version 4.3(2) still apply to this product with the exception of those fixed in version 4.4(1). The version 4.3(2) open caveats can be viewed online at:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v43/pixrn43.htm#xtocid778260](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pixrn43.htm#xtocid778260)

## Resolved Caveats

Table 4 lists resolved DDTS bug reports that need clarification or those reports that change the command interface.

If you have CCO access, you can view additional information about each open or resolved caveat at:

<http://www.cisco.com/kobayashi/bugs/bugs.html>

**Table 4**      **Resolved Caveats**

DDTS Number	Description	Fixed in Version
CSCdm39607	PIX Firewall now reports the correct number of outbound SNMP packets in the MIB-II ifOutUcastPkts object.	4.4(1)
CSCdm37763	During TCP close, when connection information is not provided from an internal host, RESET is now sent with the RESET packet. This helps the internal application know that the connection was dropped by the remote host. Previously, the application would hang with packets ping-ponging between the firewall and the host, which caused the 106013: deny tcp (no connection) syslog message to be sent hundreds of times.	
CSCdm35458	80-byte blocks were increased from 80 to 400 to ease congestion. This problem indicates that WebSENSE traffic stopped; however, the configuration showed that syslog servers were specified in the configuration, but the hosts did not actually have syslog servers on them. This slowed performance significantly.	4.4(1)
CSCdm33323	A TFTP transfer of a large configuration initiated from a Telnet console session no longer causes a failover.	4.4(1)
CSCdm29338	The username has been added to syslog message 3030002. This message appears when a user successfully downloads data from an FTP site. This message is sent to a syslog server when the <b>logging trap 6</b> or <b>logging trap 7</b> commands are used to start sending messages to a syslog server.	4.4(1)
CSCdm28487	The watchdog timer no longer expires when transferring large configurations to Flash memory. In addition, where previous PIX Firewall versions would halt traffic during the execution of the <b>write memory</b> command; version 4.4 lets traffic continue while this command completes. Another feature of this fix is that if another PIX Firewall console user tries to change the configuration while you are executing the <b>write memory</b> command, the user receives the following messages:  <pre>Another session is busy writing configuration to memory Please wait a moment for it to finish</pre> <p>After the <b>write memory</b> command completes, PIX Firewall lets the other command complete.</p>	4.4(1)
CSCdm28416	ActiveX blocking does not occur when users access an IP address referenced by the <b>alias</b> command.	4.4(1)
CSCdm26420	The number of licensed connections no longer displays in the startup messages.	4.4(1)
CSCdm26280	The <b>debug packet</b> command no longer causes the firewall to fail.	4.4(1)
CSCdm24909	Token Ring interfaces no longer stop transmitting and reset.	4.4(1)
CSCdm24665	The <b>write memory</b> command was improved to make the write to Flash memory twice as fast.	4.4(1)
CSCdm24379	A large TFTP configuration transfer no longer causes failover to the Standby unit.	4.4(1)
CSCdm22473 and CSCdj06431	The 302001 syslog message was enhanced to add the originating IP address. An example of this message is:  <pre>302001: Built outbound TCP connection 18 for faddr 192.150.50.153/80 gaddr 214.31.17.38/1115 laddr 10.0.0.3/1115</pre>	4.4(1)
CSCdm21227	PIX Firewall no longer produces non-existent framing errors on Token Ring.	4.4(1)
CSCdm21198	PIX Firewall no longer drops packets greater than 1512 KB with Token Ring.	4.4(1)
CSCdm20741	A 16-character TFTP server name no longer causes <b>write net</b> to fail or causes the PIX Firewall to reboot automatically after you enter the <b>write net</b> command.	4.4(1)
CSCdm16148	The <b>filter url</b> command no longer depends on the presence of the <b>fixup protocol http</b> command.	4.4(1)
CSCdm14861	The <b>sysopt connection enforcesubnet</b> command now applies only to inbound connections.	4.4(1)
CSCdm14393	AAA TACACS+ with failover no longer causes intermittent failover or Telnet timeout failures.	4.4(1)

Table 4 Resolved Caveats (Continued)

DDTS Number	Description	Fixed in Version
CSCdm13521	A syslog message is now sent each time a URL server is no longer available.	4.4(1)
CSCdm11244	The <b>clear config all</b> command now clears <b>rip</b> command settings.	4.4(1)
CSCdm10667	The <b>clock set</b> command now displays an error message if a year is entered outside the range of 1998 to 2097.	4.4(1)
CSCdm06039	When a WebSENSE server goes down, the PIX Firewall now switches to the next server faster than the previous time of 2 to 3 minutes.	4.4(1)
CSCdm05900	For Ethernet, PIX Firewall only supports the Intel 10/100, Cisco 4-port, and 3Com 3c590 and 3c595 cards. All other Ethernet cards generate an error message and the card is then ignored.	4.4(1)
CSCdm05752	The number of 256-byte blocks increased from 80 to 160.	4.4(1)
CSCdm05309	PIX Firewall returns the following error message <code>No such interface and direction</code> when the obsolete <b>any</b> option is entered with the <b>console</b> option of the <b>aaa authentication</b> command: This means that the <b>any</b> option cannot be used in this context.	4.4(1)
CSCdm04819	TFTP now works correctly with configuration records delineated with CR/LF or LF.	4.4(1)
CSCdm04627	Telnet sessions through the PIX Firewall are no longer dropped after the second uauth timeout.	4.4(1)
CSCdm02200	The <b>global</b> command no longer assigns the same global address to two different local addresses.	4.4(1)
CSCdk93596	The new <b>clear blocks</b> and <b>clear interface</b> commands were created to clear the counters to improve troubleshooting.	4.4(1)
CSCdk91375	Telnet access to the PIX Firewall's console is available from all internal interfaces, but not from the outside interface.	4.4(1)
CSCdk91107	An improperly configured Private Link MTU setting (one greater than or equal to the physical MTU setting on the relevant PIX Firewall interface) causes Private Link to fail.	4.4(1)
CSCdk90988	The PIX Firewall Syslog Server (PFSS) now puts the disk empty watch and disk full watch settings in the pfss.log file. In version 4.3, viewing these settings required use of the Windows <b>regedit</b> command.	4.4(1)
CSCdk84953	The startup messages and the <b>show interface</b> and <b>show version</b> commands now list the Ethernet card type correctly. Formerly, all Ethernet cards were listed as i82557.	4.4(1)
CSCdk84863	The <b>logging host</b> command now displays protocol values correctly. Previously these values were always 0.	4.4(1)
CSCdk82814	The <b>aaa authentication</b> command now only lets you enter port ranges for the TCP and UDP protocols.	4.4(1)
CSCdk76685	The <b>aaa authentication enable</b> command is no longer parsed incorrectly as the <b>aaa authentication any</b> command.	4.4(1)
CSCdk67889	The Atmel Flash driver can now write to the second megabyte of the Flash memory.	4.4(1)
CSCdk59836	Syslog messages 111001, 111003, 111004, 111005, 111007, and 199001 now list the IP address of the host issuing the command.	4.4(1)
CSCdk58988	The <b>show failover</b> command output has been added to the <b>show tech-support</b> command.	4.4(1)
CSCdk52804	The <b>fixup protocol smtp</b> command handles ESMTP by responding with <code>500 unrecognized command</code> , which causes the client to drop down to SMTP.	4.4(1)
CSCdk44171	Creates the <b>terminal width</b> command to let you specify the width of display output.	4.4(1)
CSCdk43210	After adding a <b>conduit</b> or <b>static</b> command statement, the standard procedure is to use the <b>clear xlate</b> command. Under very unusual circumstances and after waiting at least five minutes to see if the previous addresses clear, you may have to reboot the PIX Firewall.	4.4(1)
CSCdk41405	Outbound lists can now use the gopher protocol.	4.4(1)
CSCdk40788	Prompts in the startup messages now echo what you enter. Previously, when you entered a response, the startup messages resumed without displaying your response.	4.4(1)

**Table 4 Resolved Caveats (Continued)**

DDTS Number	Description	Fixed in Version
CSCdk37916	When an outbound connection is denied based on an <b>outbound</b> command setting, PIX Firewall no longer waits for a timeout to occur. Now the connection is refused immediately and the following message appears:  106002: TCP connection denied by outbound list	4.4(1)
CSCdk19979	PIX Firewall no longer assigns a single global address to multiple local IP addresses.	4.4(1)
CSCdk05686	Previously PIX Firewall silently dropped an input NAT entry if it was a duplicate of an existing one. PIX Firewall now displays a message if this happens.	4.4(1)
CSCdj86678	Syslog messages for inbound denies are now consistent with those sent because of NAT and PAT events. The 106001 message has been changed to:  106001 Inbound TCP connection denied from address/port to [global] PAT address address/port flags flags  For an unassigned NAT address, the message is:  106001 Inbound TCP connection denied from address/port to [global unused] NAT address address/port flags flags	4.4(1)
CSCdj06431	Refer to fix for CSCdm22473 for resolution of this problem.	4.4(1)

## Related Documentation

Use this document in conjunction with the following PIX Firewall documents:

- *Configuration Guide for the PIX Firewall Version 4.4*
- *Installation Guide for the PIX Firewall*
- *Regulatory Compliance and Safety Information for the PIX Firewall Version 4.4*
- *System Log Messages for the PIX Firewall Version 4.4*
- *Release Notes for the PIX Firewall Manager Version 4.3(2)b*—applies to both versions 4.3 and 4.4.

All of these documents, including these release notes, apply to all PIX Firewall hardware versions, including the PIX Firewall, PIX10000, PIX 510, PIX 515, and PIX 520 models.

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@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, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

---

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

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9905R)

Copyright © 1999, Cisco Systems, Inc.  
All rights reserved.