



Text Part Number: 78-5144-06

# Release Notes for the PIX Firewall

---

**August 1999**

**Versions: 4.2(0), 4.2(1), 4.2(2), 4.2(3), 4.2(4), 4.2(5)**

This document describes the changes for all 4.2(x) versions of the PIX Firewall software.

## Contents

- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Documentation Updates
- 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, [CSCdm00000]. Bugs are summarized in the section "Resolved Caveats."

## System Requirements

Version 4.2(3) and later requires that the PIX Firewall be equipped with a 2 MB Flash card.

Version 4.2(1) and later supports up to four Ethernet interfaces. Three Token Ring interfaces have been tested with the PIX Firewall.

Versions 4.2(4) and 4.2(5) support up to four interfaces, which may be either Token Ring or Ethernet.

---

### Corporate Headquarters

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

Copyright © 1998-1999  
Cisco Systems, Inc.  
All rights reserved.

# New and Changed Information

Version 4.2 includes the following features.

## New Features in Version 4.2(5)

No new features were added for this version—only bugs were fixed. The resolved bugs are CSCdk19979, CSCdk33996, CSCdm02200, CSCdm12973, CSCdm17608, CSCdm18870, CSCdm24909, CSCdm26456, CSCdm40856, CSCdm45461, CSCdm48728, CSCdm62060, and CSCdm69567. Refer to the section, “Resolved Caveats” for information on each bug. One open caveat was found in this release and is described as the first entry in the section, “Open Caveats.”

## New Features in Version 4.2(4)

### AAA Authorization Port Ranges

The *port* parameter to the **aaa authorization** command now supports port ranges for UDP and TCP ports; for example, you can authorize access to ports 1024 to 5000 for TCP by specifying **tcp/1024-5000**.

### Global Command Upgrade Improvements

During upgrade from version 4.1 to 4.2(4) when the previous configuration is converted to the new version, the **global** command now displays a warning message if the start or end addresses in the **global** command statement are on different subnets. The **global** command statement is accepted, with the provision that any network or broadcast addresses specified by the mask for this global are not included in the list of available translation slot addresses. The default value for the **netmask** parameter in the converted command statement is the mask of the interface’s IP address for this global. The default value can be overridden by using the **netmask** parameter to the **global** command. [CSCdk88776]

### IP Fragmentation Feature Disabled by Default

The **sysopt security fragguard** command that was formerly enabled in version 4.2(3) is now disabled by default.

### MTU Support for **linkpath** Command

The **linkpath** command now lets you specify the MTU for a Private Link session. Refer to “Changed Commands” for more information.

### Memory Upgrade Support

The PIX Firewall can now be upgraded to contain 128 MB of RAM. This permits approximately 260,000 simultaneous connections. Installation instructions are provided with the memory upgrade and can be viewed online in the *Quick Installation Guide for the PIX Firewall Version 4.3* at:

**[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v43/pix43qig.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43qig.htm)**

The memory upgrade information in this document also applies to version 4.2(3).

You can use the memory upgrade if:

- You have installed 4.3 or later code and you have only 8 MB of memory on your PIX Firewall.
- You have installed 4.2(3) or later, have a UR license, and would like to support up to approximately 260,000 simultaneous connections.

The memory upgrade is not needed if:

- You are using software PRIOR to version 4.2(3). The upgrade will not help even if you have a UR license—PIX Firewall will recognize the memory but not use it.
- You have version 4.2(3) or later, less than a UR license, and do not want to violate the connection license purchased from Cisco.

---

**Note** PIX Firewall cannot exceed 128 MB. If more is installed, PIX Firewall will not boot.

---

**Note** The only memory upgrade is 128 MB—smaller quantities are not available from Cisco.

---

**Note** Cisco recommends that you purchase the 128 MB upgrade because it lets you manage all future code enhancements without concern for running out of memory.

---

### NAT Parsing Changed

The parsing for the **nat** command has changed to fix reported errors. Refer to “NAT (Network Address Translation)” for more information.

### PIX 520 Revision B Support

Due to a change in the manufacture of the PIX Firewall motherboards, a new version of motherboard is being introduced that will be supported by the PIX Firewall version 4.2(4) software. Use of this motherboard will not affect any use of the PIX Firewall or use of any peripheral boards or hardware. However, if you downgrade the software from version 4.2(4) to an earlier version that does not support this motherboard, the slots will be addressed in a different order. The order for the PIX 520 revision A (the version number is listed at the rear of the unit) starting from the leftmost slot, is outside, inside, perimeter1, perimeter2. If you downgrade a PIX 520 revision B unit to earlier software, the slot order will become inside, perimeter1, outside, perimeter2.

### TFTP Configuration Improvements

The TFTP configuration feature that lets you store or load the configuration via TFTP has been improved for speed and reliability.

### Token Ring Improvements

The Token Ring driver now supports frame sizes greater than 1500 bytes per frame. In addition, former problems with high traffic volumes causing failures is now fixed.

## New Features in Version 4.2(3)

### AAA Reauthenticate By User

Forces a specified user to reauthenticate with the **clear uauth user** command.

### Connection License Counting

Only TCP connections from a higher security level interface to a lower security level interface are counted against the connection license; for example, from the inside to the outside, inside to a perimeter interface, a perimeter interface to the outside, or a higher security level perimeter interface to a lower security level perimeter interface. (Security levels are set with the **nameif** command.) Inbound connections are not denied if the connection license count is exceeded.

### IP Frag Guard

Protects PIX Firewall from IP fragmentation attacks. Refer to the **sysopt** command description in the *Configuration Guide for the PIX Firewall* for information. This same command also lets you set the TCP maximum segment size and add additional cleanup time to connections that close simultaneously. You should increase the TCP maximum segment size when you have both Token Ring and Ethernet interface cards in your PIX Firewall.

### Telnet Idle Timer

Lets you set the number of minutes a Telnet console session can be idle before PIX Firewall disconnects the session. The default is 5 minutes. Use the **telnet timeout** command to change the value or the **show telnet timeout** command to view the current setting.

### Trace Channel

Permits **debug icmp trace** and **debug sqlnet** command output to display on a Telnet console session. You can also use the Telnet console session to start and stop **debug packet** command output.

### Translation Information

The **show xlate** command now only displays translation information. To view connection information, use the **show conn** command. To view only the number of used and remaining connections, use the **show conn count** command.

### Unused Interfaces

PIX Firewall sets the IP address of unused interfaces to 127.0.0.1 and the subnet mask for these interfaces to 255.255.255.255.

## New Features in Version 4.2(1)

### DNS Guard

Identifies an outbound DNS resolve request and only allows a single DNS response. A host may query several servers for a response (in the case that the first server is slow in responding), but only the first answer to the specific question is allowed. All additional answers from other servers are dropped.

### Flood Defender

Protects PIX Firewall from SYN flood attacks. This feature lets you configure the maximum number of connections and embryonic connections with the **static** or **nat** commands. This feature lets a maximum number of unanswered SYN's accumulate before those connection attempts are dropped.

### Flood Guard

Controls the AAA services' tolerance for unanswered login attempts. This prevents a Denial of Service attack on AAA services. This command is enabled by default with the **floodguard** command.

### Four Interfaces

PIX Firewall supports up to four single-port 10/100BaseT Ethernet interfaces. Three 4-/16-Mbps Token Ring NICs (Network Interface Cards) have been tested with PIX Firewall. You can also mix Ethernet and Token Ring NICs in the same PIX Firewall.

### PIX Firewall Setup Wizard

Simplifies initial configuration of the PIX Firewall. Refer to Appendix C, “Installing the PIX Firewall Setup Wizard” in the *Configuration Guide for the PIX Firewall* for installation instructions at:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v42/pix42cfg/pix42apc.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42apc.htm)

### PIX Firewall Manager

Provides a centralized configuration and management GUI (Graphical User Interface).

### WebSENSE URL Filtering

Supports the WebSENSE URL filtering and accounting technology with the **filter**, **url-cache**, and **url-server** commands.

## New Commands

The new commands described in this section were added starting with version 4.2(1).

- Version 4.2(4) and later: **aaa authentication serial** console lets you require AAA authentication access to the PIX Firewall console and that all changes to the configuration made from the serial console be sent to syslog at syslog level 4.
- **auth-prompt** lets you change the text that appears before the AAA username and password prompts.
- Version 4.2(4) and later: **clear interface** clears the **show interface** counters.
- **filter** lets you enable or disable outbound URL filtering for use with WebSENSE servers.
- **fixup protocol** lets you view, change, enable, or disable application level protocol analysis through the PIX Firewall.
- **floodguard** lets you protect your network from TCP SYN attacks.
- **logging** replaces the **syslog** command. This command lets you specify which syslog message levels will be delivered to the SNMP server, the console, and an internal logging buffer.
- **perfmon** lets you monitor the PIX Firewall’s performance.
- **service** lets you reset inbound connections.
- **show version** lets you view the PIX Firewall’s software version, operating time since last reboot, processor type, Flash memory type, interface boards, and serial number (BIOS ID).
- **show tech-support** lists information that technical support analysts need to diagnose PIX Firewall problems.
- Version 4.2(3): **sysopt** enables advanced system functions including the IP Frag Guard feature that prevents IP fragmentation attacks. In version 4.2(3), the **sysopt security fragguard** command is enabled by default. In version 4.2(4) and later, it is disabled.
- **url-cache** lets you cache URL filtering requests on the PIX Firewall when using a WebSENSE server.
- **url-server** lets you set the IP address for WebSENSE servers.

## Changed Commands

Table 1 lists command changes in version 4.2. All commands are documented in the *Configuration Guide for the PIX Firewall*.

**Table 1**      **Command Changes**

Command	Change
All commands	For all commands, the following changes apply: <ul style="list-style-type: none"> <li>• Interface names—Commands requiring an interface name can use any available interface in the PIX Firewall.</li> <li>• Network mask—Commands referencing a network mask can use an arbitrary subnetwork mask.</li> <li>• TCP and UDP port services—Commands requesting a TCP or UDP service can accept either a port number or literal name for most protocols or services.</li> </ul>
<b>aaa</b>	<ol style="list-style-type: none"> <li>1 The <b>aaa</b> command provides authentication and accounting services for use with TACACS+ and RADIUS servers, and authorization services for use with TACACS+ servers.</li> <li>2 New <b>accounting</b> option enables or disables accounting services with an authentication server.</li> <li>3 New <b>aaa authentication telnet console</b> command lets you require authentication for access to the PIX Firewall console via Telnet or via both Telnet and the serial console.</li> <li>4 Version 4.2(4) and later: The <b>aaa authentication serial console</b> command lets you require authentication and have changes made to the configuration from the serial console be logged to a syslog server. The <b>serial</b> option requests a username and password before the first prompt on the serial console connection. The <b>telnet</b> option requests a username and password before the first 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.</li> <li>5 The <i>port</i> parameter to the <b>aaa authorization</b> command now supports port ranges for UDP and TCP ports; for example, you can authorize access to ports 1024 to 5000 for TCP by specifying <b>tcp/1024-5000</b>.</li> </ol>
<b>clear uauth</b>	You can force a user to reauthenticate by specifying the user's login name with the <b>clear uauth</b> and <b>show uauth</b> commands; for example: <pre>clear uauth myuser</pre>
<b>conduit</b>	<ol style="list-style-type: none"> <li>1 The <b>conduit</b> command provides new syntax to add, delete, or show conduits through the firewall for incoming connections.</li> <li>2 The <b>conduit</b> command provides new ICMP access control.</li> </ol>
<b>configure</b>	The <b>primary</b> , <b>secondary</b> , and <b>all</b> options are added to the <b>clear config</b> command.
<b>debug</b>	<p>Version 4.2(3): The <b>debug icmp trace</b> and <b>debug sqlnet</b> commands now send output to the Trace Channel feature. The Trace Channel determines where the output displays depending on whether or not a Telnet console session is running. If a Telnet console session is running, all the output displays on the first Telnet console session; otherwise, the output displays on the serial console session. The <b>debug packet</b> command only displays on the serial console session, but the <b>debug packet</b> command can be started and stopped from a Telnet session.</p> <p>The downside of this feature is that if two different administrators are using the PIX Firewall, one on the console and one on a Telnet session, the Trace Channel can cause the appearance that the <b>debug</b> commands are not working on the console, and the Telnet session will unexpectedly receive the output.</p>

**Table 1 Command Changes (Continued)**

Command	Change
<b>failover</b>	<ol style="list-style-type: none"> <li>1 The failover IP address is now required to specify the standby PIX Firewall.</li> <li>2 The <b>reset</b> option is added to the <b>failover</b> command. To take a unit out of the “failed” state, cycle the power or use the <b>failover reset</b> command.</li> <li>3 The <b>show failover</b> command displays the time, in seconds, that a PIX Firewall has been the active host.</li> <li>4 The <b>timeout</b> option lets the secondary PIX Firewall obtain translation slots for the traffic through the firewall. This lets traffic only be disrupted for 45 seconds or less before the secondary PIX Firewall becomes active.</li> </ol>
<b>global</b>	<ol style="list-style-type: none"> <li>1 The <b>global</b> command includes a global <b>netmask</b> option that applies to global entries in the command syntax. This allows you to extend the pool of global entries across network boundaries. Version 4.2(4) and later: The <b>netmask</b> parameter is only added to the configuration if it was entered by the user or existed in the configuration at load time. If the default is used at load time, it will continue to be used moving forward. PIX Firewall units upgraded from version 4.1 using software prior to version 4.2(4) will have a <b>netmask</b> parameter added to the configuration, even if the <b>global</b> command statement otherwise matched the default. [CSCdk91549]</li> <li>2 Version 4.2(4) and later: A PAT (Port Address Translation) <b>global</b> command statement now displays in the configuration with only the single address not the address as a range. [CSCdk91549] For example, if the PAT IP address is 204.31.17.5, the command statement now displays in the configuration as: <pre>global (outside) 1 204.31.17.5</pre> Prior to version 4.2(4), the IP address would display as 204.31.17.5-204.31.17.5.</li> </ol>
<b>ip address</b>	The <b>show ip address</b> command displays system IP addresses and current IP addresses which identify the Active unit when the failover feature is in use.
<b>link</b>	<ol style="list-style-type: none"> <li>1 The <b>link</b> command lets you specify that a Private Link tunnel can terminate on an interface other than the inside interface.</li> <li>2 The version 4.1 <b>link</b> command’s <b>ip</b> and <b>AUTO</b> options for key generation are no longer supported.</li> </ol>
<b>linkpath</b>	<ol style="list-style-type: none"> <li>1 The <b>linkpath</b> command lets you specify <b>0.0.0.0</b> for both the <i>foreign_internal_ip</i> and <i>netmask</i> to establish a default route to another PIX Firewall using Private Link.</li> <li>2 Version 4.2(4) and later: The <b>linkpath</b> command now lets you specify the MTU value for a Private Link session. The command syntax is: <pre>linkpath foreign_internal_ip netmask foreign_external_ip mtu</pre> Replace the <i>foreign_internal_ip</i>, <i>netmask</i>, and <i>foreign_external_ip</i> parameters as shown in the <i>Configuration Guide for the PIX Firewall</i>, on the “link/linkpath/age” command page in Chapter 5, “Command Reference.” Replace the <i>mtu</i> parameter with the number of bytes for the MTU (maximum transmission unit) value. The default for Ethernet is 1500 bytes minus Private Link overhead; the Token Ring default is 8192 bytes minus the overhead. The overhead is computed as the length of the IP header, AH header, and the ESP header, plus 12 bytes.</li> <li>3 The MTU of all linkpaths associated with a Private Link tunnel is updated when a PIX Firewall receives an ICMP fragmentation needed message (ICMP message type 3, code 4). [CSCdk87134]</li> </ol>
<b>name</b>	Version 4.2(3): the <b>name</b> string can now be 16 characters or less and cannot contain a dash (-).
<b>nat</b>	Version 4.2(4) and later: the <b>nat</b> command parser was changed so that the network mask is the primary key and the IP address is the secondary key. PIX Firewall sorts the list with most specific masks at the beginning, and the least specific masks at the end. If masks match, PIX Firewall puts the entries in ascending IP address order. Note that the <i>nat_id</i> has nothing to do with the sorting. [CSCdm00435]

**Table 1 Command Changes (Continued)**

Command	Change
<b>show</b>	<ol style="list-style-type: none"> <li>1 The <b>show</b> command has several options: <b>show blocks</b>, <b>show checksum</b>, <b>show conn</b>, <b>show history</b>, <b>show memory</b>, <b>show processes</b>, <b>show tech-support</b>, <b>show traffic</b>, and <b>show version</b>.</li> <li>2 In version 4.2(3), the <b>show conn</b> command lists the number of licensed connections and the active connections.</li> <li>3 In version 4.2(3), the <b>show xlate</b> command lists only translation slots and not connections.</li> </ol>
<b>snmp-server</b>	Up to five SNMP servers can be specified. In version 4.2(4) and later, if you attempt to enter a sixth <b>snmp-server</b> command statement, an error message displays.[CSCdk63835]
<b>static</b>	The <b>static</b> command lets you optionally specify a pair of interface names as [(if_name,if_name)] and an arbitrary network mask for configuring network statics.
<b>telnet</b>	<ol style="list-style-type: none"> <li>1 Version 4.2(3): The <b>telnet timeout minutes</b> option was added. This option lets you specify the duration that a Telnet session to the PIX Firewall console can be idle before being logged off. The <i>minutes</i> option must be from 1 to 60 minutes. The default is 5 minutes.</li> <li>2 The PIX Firewall console can now be accessed via Telnet from the inside and perimeter interfaces. The originating host can be on any subnet accessible to the internal interface including those beyond the next hop router.</li> </ol>
<b>timeout</b>	<ol style="list-style-type: none"> <li>1 The <b>timeout</b> command provides the new <b>inactivity</b> and <b>absolute</b> qualifiers to the <b>uauth</b> option. These qualifiers cause users to have to reauthenticate after either a period of inactivity or an absolute duration.</li> <li>2 Timeout values changed in version 4.2(2). The xlate timer default is now 3 hours and the conn timer default is now 1 hour.</li> </ol>
<b>write</b>	The <b>standby</b> option is added to the <b>write</b> command and applies to PIX Firewall failover configurations.

## Removed Commands

The following version 4.1 commands are obsolete in version 4.2:

- **groom**—only works with 512 K Flash memory cards. Version 4.2 and later requires a 2 MB Flash memory card.
- **http**—the PIX Firewall built-in management interface has been replaced by the PIX Firewall Manager.
- **mailhost**—use the **static** and **conduit** commands to create a mapping from a global address to a local host. The Mail Guard feature is enabled by default with the **fixup protocol smtp 25** command.
- **show hw**—use the **show version** command to view hardware information.
- **show serial**—use the **show version** command to view the serial number for your PIX Firewall.
- **syslog**—use the **logging** command instead.
- Version 4.2(4) and later: **tunnel**—formerly used by third-party product that is no longer supported.
- **uptime**—use the **show version** command to view how long the PIX Firewall has been up.
- **version**—use the **show version** command to view version information.

## Installation Notes

PIX Firewall only supports configuration upgrades from version 4.1(5) and later. With versions previous to 4.1(x), save your configuration to an ASCII text file using your terminal configuration program before upgrading, and write down your activation key. Table 2 lists the upgrade path to use to get to the current version.

**Table 2 Upgrade Paths for Older Versions**

<b>If Your Pix Firewall Version Is:</b>	<b>Install This Version:</b>
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(3), 4.2(4), or 4.2(5)

To upgrade from a previous PIX Firewall version:

- Before upgrading, copy your configuration to diskette with the **write floppy** command.
- If you cut and paste your configuration from a text file into the PIX Firewall, some statements from the original may be lost due to buffer overflow on the PIX Firewall. Check your configuration afterwards to be sure all lines were copied, and paste back in any that were lost. [CSCdk39478]
- Upgrades from version 4.1.3 to 4.2(4) and later increase the size of the configuration. If the 4.1.3 configuration is close to the maximum of 400 KB, the configuration may not run correctly.
- Version 4.2(4) and later: During upgrade from version 4.1 to 4.2(4) and later when the previous configuration is converted to the new version, the **global** command now displays a warning message if the start or end addresses in the **global** command statement are on different subnets. The **global** command statement is accepted, with the provision that any network or broadcast addresses specified by the mask for this **global** command are not included in the list of available translation slot addresses. The default value for the **netmask** parameter in the converted command statement is the mask of the interface's IP address for this global. The default value can be overridden by using the **netmask** parameter to the **global** command. [CSCdk88776]
- If you have CCO access, you can download the most current version of the PIX Firewall software. Refer to Chapter 2, "Configuring PIX Firewall" in the *Configuration Guide for the PIX Firewall* for information on downloading software from CCO.
- Before installing version 4.2(x) from 4.1(x), save your configuration to diskette and write down your license activation key. You must have a copy of your activation key to restore a previous version from diskette.
- Version 4.2(4) and later, PIX 520 revision B: If you downgrade the software from version 4.2(4) and later to an earlier version that does not support the PIX 520 revision B motherboard, the slot order starting from the leftmost slot will become inside, perimeter1, outside, perimeter2. Refer to "PIX 520 Revision B Support" for more information.
- If failover is not configured and you read a configuration in from diskette, PIX Firewall displays messages such as: `IP address '0.0.0.0': already in use`. These messages can be ignored.
- If you have a failover cable connected to a secondary PIX Firewall, remove the failover cable before upgrading to a new version of PIX Firewall. Once the new software is installed, reconnect the cable, and reboot the two systems. The Primary unit will automatically update the Secondary unit with the new configuration.

- If you use failover, add the IP address of the other PIX Firewall to the **failover** command. Both PIX Firewalls must run the same PIX Firewall software version and be the same PIX Firewall model.
- After you install version 4.2, PIX Firewall automatically converts your version 4.1 configuration for use with version 4.2. Before testing PIX Firewall on the network, check the configuration to ensure all statements converted correctly and fix any that did not.
- Add the **conduit permit icmp any any** command to permit outbound and inbound ICMP access.
- Note that the command history and the commands for accessing previous commands have changed. Refer to Chapter 1, “Introduction” in the *Configuration Guide for the PIX Firewall* for more information. You can view this chapter online at:  
**[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v42/pix42cfg/pix42int.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42int.htm)**
- Both ends of the Private Link must run the same PIX Firewall software version and be the same PIX Firewall model. Also ensure that both ends have the same number of keys.
- If necessary, fix the **established** command. In version 4.2, the **established** command without the **permitfrom** option is interpreted as **established protocol ... permitfrom protocol any\_port**.
- If necessary, fix the **timeout** command. In version 4.2, the **timeout uauth** command defaults to **absolute**.
- Check the **conduit** commands created when the version 4.2 conversion script converts the **mailhost** command to the **conduit permit tcp host ip\_address eq smtp any** command.
- Set the netmask in **global** for IP addresses in the range of 0 to 127 to 255.0.0.0. For addresses 128 to 191, use 255.255.0.0. For addresses 192 to 254, use 255.255.255.0.
- For the **static** command, use a netmask of 255.255.255.255 for all ranges of host IP addresses.
- Downgrades from version 4.2(x) to version 4.1(7) are not supported because of syntax differences in the command sets. Reverting to an earlier, fully-configured version of the PIX Firewall is only possible if a configuration built with the earlier version is available. Therefore, before upgrading always save your configuration on diskette with the **write floppy** command.

## Limitations and Restrictions

This section contains critically important information.

- 1 If your PIX Firewall has a serial number of 06002015 or earlier, do not attempt to load PIX Firewall version 4.2(2), 4.2(3), 4.2(4), or 4.2(5) software. If you have one of these units, you must upgrade your Flash memory to the 2 MB Flash memory card. Contact Cisco Customer Support about how to obtain the 2 MB Flash memory card.

To determine your Flash memory size, reboot your PIX Firewall and look for the following statement:

```
Flash=string
```

If *string* starts with “AT”; for example, `Flash=AT29C040A`, then you have the 2 MB size and the PIX Firewall version 4.2(x) software will load correctly. If *string* starts with “i”; for example, `Flash=i28F020`, then you have the older 512 KB size and must replace it before loading PIX Firewall version 4.2(x) software.

- 2 Versions 4.2(4) and 4.2(5): connections are not counted against the PIX Firewall license.  
Version 4.2(3): the only connections counted toward the PIX Firewall license are outbound TCP connections from the inside or perimeter interfaces. Inbound connections are not denied regardless of the number of outbound connections. (“Outbound” means from any higher security level interface to any lower security level interface.) [CSCdj82405]
- 3 PIX Firewall supports up to four Ethernet interfaces. Three Token Ring interfaces have been tested with PIX Firewall. If you use a mixed Token Ring and Ethernet environment, use the **sysopt connection tcpmss 4056** command to increase the TCP maximum segment size for use with the IP Frag Guard feature (version 4.2(3) only).
- 4 The maximum size of the configuration in a 2 MB Flash memory card is 400 KB. To view the number of characters in the configuration, use the UNIX **wc** command or a Windows word processing program, such as Microsoft Word. Previously the release notes reported a greater maximum configuration size for the 2 MB Flash memory card.
- 5 Version 4.2(3): the **sysopt security fragguard** command is enabled by default but does not appear in the configuration when enabled. Use the **show sysopt** command to determine if this command is enabled.
- 6 If a Telnet console session and serial console session are running at the same time, the **debug icmp trace** and **debug sqlnet** output will stop displaying without warning on the serial console and begin appearing on the Telnet session. Before running the **debug** commands from the serial console session, use the **who** command to determine if Telnet sessions are present, and then inform other users that you will begin using **debug** commands. In addition, if both sessions are paging through output at the same time, the Telnet session may hang and cause the PIX Firewall to fail on your next attempt to use the **write memory** command. [CSCdk69399]
- 7 PIX Firewall can sustain approximately 350 AAA transactions per minute.
- 8 PIX Firewall supports up to 300 URL filtering transactions per minute without impacting normal NAT throughput. If your requirement exceeds this range, use the **url-cache** command, which can provide significant relief depending on your cache-hit ratio. If the **url-cache** command does not improve capacity, you should consider purchasing additional PIX Firewall units.  
The **url-cache** command does not update the WebSENSE accounting logs.
- 9 If you upgrade from a previous PIX Firewall software version, PIX Firewall converts your configuration to the new commands. Before using the PIX Firewall on a network, verify that no commands were lost from your configuration during the conversion process.
- 10 PIX Firewall has been tested with 100 Mbps, full-duplex Ethernet only with Cisco switches. If the PIX Firewall is connected to a non-Cisco switch, half duplex settings may be required to maintain 100 Mbps throughput.
- 11 When the PIX Firewall is operating with heavy traffic, do not set the **logging console** level to 7, **debugging**. This feature may cause PIX Firewall to fail. Use the **logging buffered** command to store messages and the **show logging** command to view them.
- 12 Do not use the **established** command without the **permitto** and **permitfrom** options. Without these options, the **established** command can let users attack protected areas of your network. [CSCdk23441]
- 13 To use the PIX Firewall serial console simultaneously with console Telnet sessions, disable paging at the serial console with the **no pager** command. Otherwise, a contention problem can arise between Telnet console sessions using More and the serial console using More, which causes the PIX Firewall to fail. [CSCdk69399]
- 14 If the TACACS+, RADIUS, syslog, or URL servers go offline, the PIX Firewall will continue to send ARP requests for them and exhaust 256-byte memory blocks.

- 15 The PIX Firewall Manager (PFM) is not compatible with Cisco Resource Manager (CRM) and PFSS, because all three use syslog UDP port 514. Do not run all three applications at the same time.
- 16 Version 4.2(2): Define all interfaces on your PIX Firewall. For example, if three interface cards are installed, you must have **interface** and **ip address** statements in your configuration for each interface, even if a network cable is not connected to an interface.  
  
In version 4.2(3), PIX Firewall sets the default IP address for non-configured interfaces to 127.0.0.1, which identifies itself as a localhost. In addition, the network masks for these interfaces is set to 255.255.255.255, which does not permit traffic through the interface.
- 17 A host **static** without a **conduit** cannot be pinged.
- 18 Before installing the current version from a previous release, save your configuration on floppy disk and write down your license activation key. You must have a copy of your activation key to restore a previous version from floppy disk.

## Important Notes

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

---

**Note** Use the **clear xlate** command after changing or removing these commands: **alias**, **conduit**, **global**, **interface**, **ip address**, **nameif**, **nat**, **outbound**, and **static**. If after using the **clear xlate** command, the previous behavior is unchanged, save your configuration with the **write memory** command, and reboot the PIX Firewall.

---

## AAA

- When the AAA server is unreachable or offline, the PIX Firewall makes four attempts to access the server. Thereafter, you can gain access to the serial console by entering the **pix** username and the enable password.
- RADIUS is only supported for authentication and not for authorization.
- For the **aaa**, **radius-server**, and **tacacs-server** commands, 16 TACACS+, RADIUS, or URL servers are supported. [CSCdk37223 and CSCdk34853]
- For the **aaa authentication telnet console** command, the maximum password length for accessing the console is 16 characters. [CSCdk36498]
- The **clear radius-server** and **clear tacacs-server** commands do not have arguments. In addition, before using these commands, remove the **aaa** commands from the configuration that references the AAA servers. [CSCdk36092]
- If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. [CSCdk33420] An example authorization timeout message in Telnet is:  

```
Unable to connect to remote host: Connection timed out
```
- The maximum timeout value for the **radius-server** and **tacacs-server** commands is 30 seconds. [CSCdk35899]
- Do not use the **virtual http** command when an inside client is configured to access the Web via a proxy server located on another interface of the PIX Firewall. [CSCdk16222] Accessing a proxy server and having your browser configured for proxy are different.

## Access Control Lists

When using the **outbound** command, the default behavior is to permit access to all services. [CSCdk34668]

Refer to the **outbound** command page in the *Configuration Guide for the PIX Firewall* for more information on **outbound** command rules. You can view this information online at:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v42/pix42cfg/pix42cmd.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42cmd.htm)

## Aliases

- Ensure that the **alias** address agrees with other configuration statements. For example, if you use 192.159.1.7 as an alias for 192.150.50.7, a source host on the outside, use 192.159.1.7 in any **conduit** statements allowing access to 192.150.50.7.
- An example of using **alias** is for a web server on the inside at 10.1.1.11 and a static for it at 204.31.17.11. The source host is on the outside with address 192.150.50.7. A DNS server on the outside has a record for www.caguana.com as follows:

```
www.caguana.com.      IN      A      204.31.17.11
```

The period at the end of the domain name is required.

The **alias** command is:

```
alias 10.1.1.11 204.31.17.11 255.255.255.255
```

PIX Firewall doctors the nameserver replies to 10.1.1.11 for inside clients to directly connect to the web server.

The **conduit** you would expect to use is:

```
conduit permit tcp host 204.31.17.11 eq telnet host 192.150.50.7
```

But with the **alias** command, use this command:

```
conduit permit tcp host 204.31.17.11 eq telnet host 192.159.1.7
```

## Attacks

- To prevent the SYN flood or denial of service attacks, always set the connection limit and embryonic limit options on the **nat** and **static** commands.
- Use the **sysopt security fragguard** command to prevent IP fragmentation attacks. Use the **show sysopt** command to see if this command is enabled.
- Do not use the **established** command without the **permitto** and **permitfrom** options. Without these options, outside users can attack your network through **conduit** access. [CSCdk23441]

## Automatic Recovery

On PIX Firewall units equipped with Token Ring interfaces, if a network error occurs that places the PIX Firewall in a state where it cannot receive or transmit information and which causes the unit to stop passing packets for 15 seconds, the PIX Firewall automatically reboots.

---

**Note** During automatic recovery, all connections are lost, and all Telnet console sessions or PIX Firewall Manager sessions are suspended and need to be restarted after the unit is back on line.

---

### Command Lines

- The maximum number of characters that can be entered on the command line is 512. Additional characters past this limit are ignored.
- Version 4.2(4) and later: Control-z can now be used to exit configuration mode.

### Configuration

- If you cut and paste text from your console computer into the configuration, check it carefully afterwards. Some lines may be dropped during the process due to buffer overflow. [CSCdk39478]
- In PIX Firewall units with 3Com interface boards and BNC connectors, the **show interface** command can report that an interface is up but the line protocol is down. You can ignore the error message; 3Com drivers do not detect link integrity on boards with BNC connectors.
- The PIX Firewall model 520 supports up to 64,000 connections.
- When you start the PIX Firewall, you may notice that multiple interface cards share the same interrupt vector. Because Intel network interface cards are polled rather than interrupt driven, interrupt vectors can be shared without conflict.

### Connections

- Version 4.2(3): only outbound connections from the inside or any perimeter interfaces are counted toward your connection license. Inbound connections are *not* denied when the number of outbound connections exceed the license count. Use the **show conn** command to view the number of connections in use.
- Version 4.2(4) and later: PIX Firewall no longer closes connections when a single FIN is received. Instead, it now waits for two FINs before closing the connection. [CSCdk79683]
- Version 4.2(4) and later: Connections are not terminated as long as SYN-SYN/ACK-SYN is received, even if data has not been received. [CSCdk77341] In versions prior to 4.2(4), a connection was terminated after two minutes if data was not received.
- Version 4.2(4) and later: The embryonic connection timeout was formerly hardcoded at 150 seconds. This timer has been changed so that the embryonic state excludes the data that has been seen; as long as a 3-way SYN is accepted, the connection is now subject to the duration set by the **timeout conn** command. [CSCdk76293]

### Cookies

Version 4.2(4) and later: PIX Firewall now supports the HTTP **POST** command during proxy authentication. [CSCdk83285]

### DHCP

If you are using DHCP to configure IP addresses for the hosts on the inside network, the DHCP server must provide the IP address, netmask, and gateway (default route) IP address. The default route must point to the PIX Firewall, either directly or via a router.

## DLSw

Version 4.2(4) and later: PIX Firewall provides support for inbound DLSw (data-link switching) via the use of the **static** and **conduit** commands. Special provision for this protocol was made by letting connections stay open as long as SYN-SYN/ACK-SYN is received, even if data has not been received. [CSCdk77341]

## DNS

- When a DNS server is outside the PIX Firewall, use the **alias** command to let the PIX Firewall translate addresses returned by the DNS server into inside addresses.
- When DNS traffic is logged with syslog, the ID field in the DNS response packet appears in the source port field. [CSCdk36912]
- If using the **alias** command, there must be an A (address) record in the DNS zone file for the “dnat” address of the **alias** command.

## established Command

The **established** command can potentially open a large security hole in the PIX Firewall if not used with discretion. Whenever you use this command, if possible, also use the **permitto** and **permitfrom** options to indicate ports to which and from which access is permitted. Without these options, users outside the PIX Firewall can access any ports on servers behind the firewall that are accessible with the **conduit** and **static** commands.

The following example illustrates this problem:

```
static (inside,outside) 204.31.17.42 192.168.1.42 netmask 255.255.255.255
conduit permit tcp host 204.31.17.42 eq http any
established tcp
```

In this example, inside host 192.168.1.42 can be accessed from the outside interface for Web access as permitted by the **conduit** statement. Because this is a web server (using the HTTP port), access permission is granted to any outside host. However, the **established** command modifies the effect of the **conduit** statement and lets any user access any port on the 192.168.1.42 server. [CSCdk23441]

## Failover Option

- Refer to Chapter 3, “Advanced Configurations,” in the *Configuration Guide for the PIX Firewall* for new version 4.2 failover information, including how to update failover from PIX Firewall version 4.1 to 4.2. You can view this information online at:  
[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v42/pix42cfg/pix42adv.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42adv.htm)
- PIX Firewall now supports failover in a switched environment.
- Version 4.2(4): A message now displays when the configurations are synchronized reminding you to not disturb the units during the process. [CSCdk78041]

## Flood Guard Feature

The **floodguard** command helps protect the AAA Cut-Through Proxy service by reclaiming the PIX Firewall “tcpusers” resource, which is used for the Cut-Through Proxies. Use **floodguard 1** to enable this feature.

### FTP Port

For AAA, the FTP port must be 21.

### Global Addresses

Consult with your ISP (Internet service provider) to make sure that all addresses used in globals are routed to your outside router before configuring the PIX Firewall with global addresses.

### IDENT Connections

PIX Firewall does not support the use of the **established** command with a PAT IP address for the IDENT service. Use the **service resetinbound** command to reset incoming IDENT connections.

### Licenses

PIX Firewall provides the following connection licenses:

- Entry level—128 connections
- Midrange—1024 connections
- Unrestricted—up to 65,536 connections (with the PIX Firewall 520; earlier versions of PIX Firewall are limited to 16,384 connections, while the PIX10000 and PIX Firewall 510 support 32,768 connections in this license category).

Only TCP connections from a higher security level interface to a lower security level interface are counted against the connection license.

### Mail Guard Feature

This feature is only compliant with the RFC 821 section 4.5.1 commands. The RFC 1651 EHLO command returns a “500 command unrecognized” reply code.

### MTU Requests

PIX Firewall now correctly handles path MTU (maximum transmission unit) requests. Path MTU relies on the PIX Firewall to generate an ICMP host unreachable message (code=3) on reception of a packet that needs to be fragmented but has the Don't Fragment flag set in the IP header (type=4). PIX Firewall formerly discarded these packets without returning the host unreachable message. [CSCdk38353]

### Multimedia Applications

PIX Firewall supports the following multimedia and video conferencing applications:

- Intel Internet Video Phone
- Microsoft NetMeeting
- Microsoft NetShow
- RealNetworks RealAudio and RealVideo
- VDOnet VDOLive
- VXtreme WebTheater
- VocalTec Internet Phone
- White Pine CU-SeeMe
- White Pine MeetingPoint
- Xing StreamWorks

## NAT (Network Address Translation)

- Version 4.2(4) and later: the **nat** command now parses the network mask as the primary key and the IP address as the secondary key. PIX Firewall sorts the list with the most specific masks at the beginning, and the least specific masks at the end. If masks match, PIX Firewall puts the entries in ascending IP address order. Note that the *nat\_id* has nothing to do with the sorting. [CSCdm00435]
- The NAT feature in the PIX Firewall differs from the Cisco IOS NAT feature with regard to the traffic types that they support. All protocols which do not have embedded IP (TCP, UDP, ICMP, and so on) should work on the PIX Firewall. Application protocols handled by the **protocol fixup** command are FTP, H.323, SQL\*Net, Telnet, SMTP, and SunRPC.
- Plan your NAT groups carefully and allow ample global addresses. One NAT group cannot access another NAT group's global addresses.

## PAT (Port Addressed Translation)

- PAT does not work with H.323 applications, multimedia applications, and caching nameservers.
- PAT works with DNS, FTP and passive FTP, HTTP, mail, RPC, rshell, Telnet, URL filtering, and outbound traceroute.
- Version 4.2(2): There is no support for outbound passive FTP. This version requires using an **outbound** command with ports 1024-65535 open as a workaround.
- Version 4.2(2): There is no support for PAT if IP data packets arrive in reverse order. In version 4.2(3), this was fixed so that PAT works with reverse-ordered IP data packets.

## pager Command

Using **pager 0** disables screen paging in PIX Firewall.

## Ping Use

- If you are upgrading from version 4.1(5), refer to "Installation Notes" for information on the need to add a **conduit** for ICMP to your configuration.
- A host **static** without a **conduit** cannot be pinged.
- The **conduit permit icmp any any** command lets inbound and outbound pings work.
- ICMP packets arriving, departing, and traversing PIX Firewall are all visible now with the **debug icmp trace** command. Also visible are the ICMP packets to the PIX Firewall's own interfaces. [CSCdj70621] The **debug** command only works from the PIX Firewall serial console and not when you access the console with Telnet or PIX Firewall Manager.
- If 80-byte blocks are used up, PIX Firewall will not be able to get enough memory to form a ping echo reply. Use the **show blocks** command to view available blocks.

## Private Link Option

- PIX Firewall selects the next Private Link encryption key by the “round-robin” method. The **age** command determines the length of time a key is current.
- A new parity feature has been added so that an additional 8 bits have been added to the Private Link key for parity to ensure that the key is passed correctly across the link. [CSCdk11848]
- All PIX Firewall units support the PCI Private Link card; however, use of this card restricts the number of available interface cards to three.
- Version 4.2(4) and later: The **linkpath** command now lets you specify the session MTU. Refer to “Changed Commands” for more information.

## Protocol and Application Support

PIX Firewall supports the following TCP/IP protocols and applications:

- Address Resolution Protocol (ARP)
- Archie
- Berkeley Standard Distribution (BSD)-rcmds
- Bootstrap Protocol (BOOTP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Generic Route Encapsulation (GRE)
- Gopher
- HyperText Transport Protocol (HTTP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- Simple Network Management Protocol (SNMP)
- SQL\*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Telnet
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)

Refer to the “Protocols” section in Chapter 1, “Introduction” in the *Configuration Guide for the PIX Firewall* for information on supported protocols. You can view the configuration guide online at:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v42/pix42cfg/pix42int.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42int.htm)

## Routing and RIP

- If you configure RIP passive on a perimeter interface using the **rip** command, the PIX Firewall passively listens for RIP information on that interface; however, that information is not used to make forwarding decisions.
- PIX Firewall has the capability to advertise a RIP V1 default route out any of its interfaces; however, the PIX Firewall will not advertise any routes other than itself as the default route.

## RPC Use

- For SunRPC, PIX Firewall now dynamically listens to the incoming and outgoing portmapper or **rpcbind** RPC port and creates an incoming UDP or TCP connection to a specific internal host and port for the desired service. [CSCdk29475 and CSCdk25383]

To configure NFS for inbound use:

- (a) Create a **static** to let the outside hosts access the inside server.
- (b) Create a UDP **conduit** for the portmapper port, UDP port 111.
- (c) Create a UDP **conduit** for the NFS port, UDP 2049.

PIX Firewall then manages the connection dynamically. Examples of the **conduit** statements are:

```
conduit permit udp host 204.31.17.1 eq 111 any
conduit permit udp host 204.31.17.1 eq 2049 any
```

Notes:

- A **conduit** for portmapper is necessary for the initial port discovery message to come to the internal network.
  - A **conduit** for NFS 2049 port is necessary because NFS over UDP does not generate a “keep alive” message to keep the PIX Firewall from cleaning idle UDP connection.
  - All dynamically negotiated ports will allow the specific outside host to connect back to only the specific port allowed by the internal portmapper.
- Microsoft’s MSRPC uses TCP port 135 and requires high ports 1024-65535 to be open. Examples of the **conduit** statements are:

```
conduit permit tcp host 204.31.17.1 eq 135 any
conduit permit tcp host 204.31.17.1 range 1024 65535 any
```

- On SunRPC, you can test for RPC traffic with the UNIX **rpcinfo -u** command.
- While there is not a **fixup** command for SunRPC, PIX Firewall handles it transparently.

## Server Access

If RADIUS, SNMP, SMTP, syslog, TACACS+, or URL servers go down or are powered off, the PIX Firewall will ARP for the servers and may exhaust all 256-byte blocks. Traffic through the PIX Firewall will then stop. The workaround is to remove the statements for the servers from your configuration when they go down or are put out of service. [CSCdk34295]

## show version Command

The **show version** command now lists the processor speed. [CSCdj57072]

## SPX

PIX Firewall does not pass SPX packets across it.

## Statics

- Net statics take precedence over use of the **nat 1 0 0** and **global** command pair. This means that **nat 1 0 0** only grants outbound access to hosts not specified in the net **static** statement.
- Use a netmask of 255.255.255.255 for all ranges of IP addresses.

### Syslog Feature

- The **logging** command replaced the **syslog** command. The new **logging** command lets you send syslog messages to hosts on any interface, not just the inside.
- When DNS traffic is logged, the ID field in the DNS response packet appears in the source port field. [CSCdk36912]
- Syslog failover and reset messages were moved to **logging** command's level 1 alerts. Formerly, these messages were in levels 2 and 6 respectively. [CSCdk06673]
- Syslog message PIX-2-108002 now displays the IP addresses in the correct order. [CSCdk83802]
- The former syslog message %PIX-3-202002: Unable to find translation for SRC=*ip\_address* DEST=*ip\_address* has been changed to:  

```
%PIX-3-305005: No translation group found for packet_shown_as_text  
%PIX-3-305006: xlate_type translation creation failed for packet_shown_as_text
```

where:
  - *packet\_shown\_as\_text* includes the IP type, IP source and destination interfaces, the protocol specific port for UDP or TCP, or the type and code for ICMP.
  - *xlate\_type* is **identity**, **inbound static**, **outbound static**, **portmap**, or **regular**.
- In version 4.2(4) and later, the former syslog message %PIX-2-106006: Deny inbound UDP has been dropped. [CSCdk92804] This message was a duplicate of message %PIX-3-106010, which has been enhanced to now state:  

```
%PIX-3-106010: Deny inbound (No xlate) udp src outside:ip_addr/port  
dst inside:ip_addr
```

### Telnet Console Sessions

- Version 4.2(3): Display of the **debug** command data in Telnet console sessions now depends on the PIX Firewall Trace Channel. Refer to "Trace Channel" for more information.
- Version 4.2(4) and later: International characters, those above ASCII 127, can now be entered in a Telnet console session. However, such characters will be rejected by the PIX Firewall command interpreter. [CSCdk75115]

### virtual telnet Command

Only use the **virtual telnet** command after the **aaa authentication** command.

### Year 2000 Compliance

PIX Firewall is year 2000 compliant.

### Caveats

The following caveats apply to PIX Firewall release 4.2(*n*). Refer to the previous versions of the PIX Firewall release notes for information on bugs in previous versions. You can view previous versions of the PIX Firewall release notes online 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 following issues are unresolved in this release:

- Sending packets greater than 1432 bytes over a Private Link Token Ring interface causes the PIX Firewall to fail. [CSCdm51619]
- A problem exists between AAA and the **virtual http** command that causes PIX Firewall to not check authorization on the first connection that is authenticated if the **virtual http** command is enabled. [CSCdm05429]
- Autonegotiation of connection duplex is not always successful. The PIX Firewall detects half duplex when a Cisco 7206, Cisco Catalyst 5000, or Bay Switch 5000 are set at full duplex. In addition, when the PIX Firewall has been configured for full duplex at 100 Mbps Ethernet, during autonegotiation, the Cisco Catalyst 5000 detects the PIX Firewall as half duplex. [CSCdk32876]
- PIX Firewall does not check the validity of **static** command statement IP addresses. [CSCdj92811] For example, PIX Firewall lets you enter the following two **static** commands for different host addresses:

```
static (inside,outside) 204.31.17.1 10.1.1.2
static (inside,outside) 204.31.17.1 10.9.9.9
```

- PIX Firewall does not check the validity of the **ip address** statement and will let you enter a subnet mask of 255.255.255.255 for an interface which prevents traffic from using the interface. [CSCdk69403]
- To use the PIX Firewall serial console simultaneously with console Telnet sessions, disable paging at the serial console with the **no pager** command. Otherwise, a contention problem can arise between Telnet console sessions using More and the serial console using More that causes the PIX Firewall to fail. [CSCdk69399]
- When a DNS server is on the outside and users on the inside need to access a server on the perimeter interface, you would use the **alias** command to permit DNS responses to resolve correctly through the PIX Firewall. However, in this case, you must reverse the parameters for the local IP address and foreign IP address. [CSCdk50579]

For example:

```
alias (inside) 192.168.1.4 204.31.17.121 255.255.255.255
```

Host inside 10.1.1.1 goes to www.example.com which resolves at an outside ISP DNS to 204.31.17.121. The PIX Firewall fixes this DNS response sending the host a response of 192.168.1.4. The host uses its gateway (the PIX Firewall) to go to 192.168.1.4 which the PIX Firewall now aliases back to the 204.31.17.121. Because this is actually 192.168.1.4, a server on the perimeter interface of the PIX Firewall, the packet is dropped because the PIX Firewall sent the packet to the outside interface, which is the incorrect interface.

Workaround: Reverse the alias parameters as follows:

```
alias (inside) 204.31.17.121 192.168.1.4 255.255.255.255
```

This works properly because everything happens backwards. The DNS is now modified to 204.31.17.121 and the host inside uses its gateway (the PIX Firewall) to get there, the PIX Firewall aliases this back to 192.168.1.4 and routes it out the perimeter interface to the correct host and the TCP connection is established.

## Resolved Caveats

Table 3 lists resolved version 4.2(*n*) DDTS bug reports.

**Table 3** Resolved Bugs

DDTS Number	Description	Release
CSCdm69567	Use of an HTTP <b>POST</b> command now works correctly without causing a failure. Previously, customers with short uauth timeouts in their configuration or with a large number of authenticated users were more likely to be affected by this problem.	4.2(5)
CSCdm62060	The <b>outbound</b> command's <b>except</b> option now works correctly.	4.2(5)
CSCdm48728	The PIX Firewall now correctly updates its ARP cache when a gratuitous ARP broadcast is sent on the network.	4.2(5)
CSCdm45461	A Cisco IOS TN3270 client now echoes characters correctly when passing through a PIX Firewall.	4.2(5)
CSCdm40856	Entering the <b>no aaa authentication telnet</b> command no longer causes the PIX Firewall to fail.	4.2(5)
CSCdm26456	Currently the <b>virtual http</b> command redirects by IP address after authenticating. So if a user accesses a web site, after they are authenticated, they are sent to the IP address of the web site. This can cause problems at certain web sites, particularly those that use cookies to authenticate, because the browser will not be sent the cookie unless it sees a hostname it recognizes.	4.2(5)
CSCdm24909	Token Ring interfaces no longer stop transmitting and reset.	4.2(5)
CSCdm18770	The <b>virtual http</b> command now works correctly after the <b>clear uauth</b> command is executed.	4.2(5)
CSCdm17608	PIX Firewall no longer replies to gratuitous ARP requests unless the address exists on a PIX Firewall interface. This fix allows a Windows NT system to pass a gratuitous ARP to test to see if another host has taken its IP address. If the address belongs to a PIX Firewall interface, the PIX Firewall replies to the ARP request. Other regular ARP queries are still proxied if they are in the global or static pool.	4.2(5)
CSCdm12973	Entering two Class B addresses in a <b>global</b> command caused the "watchdog timer" to expire, which then caused the PIX Firewall to fail. The following is an example command that caused a failure:  <pre>global (outside) 2 172.168.0.1-172.168.255.254</pre>	4.2(5)
CSCdm03318	The <b>outbound</b> command now checks the protocol so that a protocol-unspecific best match will be replaced when a more specific protocol statement was found and matched with the packet being checked. Formerly, an implicit permit could override an explicit deny; this is no longer the case.	4.2(4)
CSCdm02200	One global pool address is no longer assigned to two or more local IP addresses	4.2(5)
CSCdm00435	The <b>nat</b> command parser was changed so that the network mask is the primary key and the IP address is the secondary key. PIX Firewall sorts the list with most specific masks at the beginning, and the least specific masks at the end. If masks match, PIX Firewall puts the entries in ascending IP address order. Note that the <i>nat_id</i> has nothing to do with the sorting.	4.2(4)
CSCdk92804	The former syslog message %PIX-2-106006: Deny inbound UDP has been dropped. This message was a duplicate of message %PIX-3-106010, which has been enhanced to now state:  <pre>%PIX-3-106010: Deny inbound (No xlate) udp src outside:ip_addr/port dst inside:ip_addr</pre>	4.2(4)
CSCdk92547	PIX Firewall no longer fails during a passive FTP session that runs longer than the duration set by the <b>timeout xlate</b> command.	4.2(4)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk91549	The display of the network mask in PAT <b>global</b> command statements in the configuration changed. Refer to “Changed Commands” for more information.	4.2(4)
CSCdk88776	During upgrade from version 4.1 to 4.2(4) when the previous configuration is converted to the new version, the <b>global</b> command now displays a warning message if the start or end addresses in the <b>global</b> command statement are on different subnets.	4.2(4)
CSCdk87134	The MTU of all linkpaths associated with a Private Link tunnel is updated when a PIX Firewall receives an ICMP fragmentation needed message (ICMP message type 3, code 4).	4.2(4)
CSCdk87045	Command parsing is fixed so that PIX Firewall no longer fails when commands are entered with just three arguments. This bug noted that entering <b>no tacacs (inside)</b> caused PIX Firewall to fail.	4.2(4)
CSCdk84226	PIX Firewall now explicitly filters directed network layer broadcasts to address 255.255.255.255. These multicast broadcasts could pass through the PIX Firewall’s data link layer when incorrect ARP mapping occurred by other hosts. The bug noted that the inside interface was passing broadcasts through the PIX Firewall.	4.2(4)
CSCdk83802	Syslog message PIX-2-108002 now displays the IP addresses in the correct order.	4.2(4)
CSCdk83300	Outbound lists now work correctly when the mask is different than the class of the IP address. For example, the <b>outbound</b> command would have previously failed if configured with Class C netmask for a Class B IP address as follows:  <b>outbound 1 deny 172.16.6.0 255.255.255.0 0 tcp</b>	4.2(4)
CSCdk83285	When proxy authenticating HTTP, PIX Firewall now correctly recognizes the <b>POST</b> command. The <b>POST</b> command transmits HTML cookies.	4.2(4)
CSCdk82957	Remote shell (rsh) now functions correctly with an HP 9000 if the EFT <b>sysopt connection safeclose</b> command is used.	4.2(4)
CSCdk81282	Syslog no longer displays incorrect characters in syslog messages, such as negative port numbers. This condition formerly existed while an <b>outbound</b> command statement was denying outbound access through a PAT global.	4.2(4)
CSCdk79683	PIX Firewall no longer closes connections when a single FIN is received. Instead, it now waits for two FINs to close the connection.	4.2(4)
CSCdk78956	The <b>outbound</b> command now permits a mask of 255.255.255.255.	4.2(4)
CSCdk78707	Under conditions such as low memory or memory corruption, PIX Firewall no longer generates frequent syslog messages containing the phrase, “PIX-2-SYS-CHUNKBOUNDS attempted to exceed freelist causing failover.”	4.2(4)
CSCdk78398	Inbound mail is no longer denied when conduits are present. This problem occurred because an internally-coded embryonic connection timer was set too low. The embryonic state has been changed to track initial SYN sequences and not when data begins to flow. Also the embryonic connection timer continues to be updated until both sides of a TCP connection have begun the close down sequence.	4.2(4)
CSCdk78041	When the failover Primary and Standby configurations are synchronized, a message displays reminding you not to disturb the units.	4.2(4)
CSCdk77349	Token Ring no longer stops transmitting packets when the buffer index is incremented.	4.2(4)
CSCdk77341	Connections are not terminated as long as SYN-SYN/ACK-SYN is received, even if data has not been received.	4.2(4)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk77068	The <b>telnet timeout</b> command was changed from being an absolute timer to an inactivity timer. The version 4.2(3) documentation erroneously reported that the timer was an inactivity timer.	4.2(4)
CSCdk76744	The <b>sysopt security fragguard</b> is now disabled by default. If enabled, and a high amount of traffic is experienced, this command may cause the PIX Firewall to fail.	4.2(4)
CSCdk76293	The embryonic connection timeout was formerly hardcoded at 150 seconds. This timer has been changed so that the embryonic state excludes the data that has been seen; as long as a 3-way SYN is accepted, the connection is now subject to the duration set by the <b>timeout conn</b> command.	4.2(4)
CSCdk75115	International characters, those above ASCII 127, can now be entered in a Telnet console session. However, such characters will be rejected by the PIX Firewall command interpreter. Formerly entering these characters caused the PIX Firewall to fail.	4.2(4)
CSCdk74427	PIX Firewall no longer fails when receiving a UDP packet with length 0 or less, and when there is a server listening on the port.	4.2(4)
CSCdk72479	Syslog message "108001: SMTP made noop" has been improved to eliminate garbage characters at the end of the message.	4.2(4)
CSCdk72461	PIX Firewall now checks IP addresses and network masks for correct syntax. Formerly, nonsensical values could be added such as a netmask of 1.2.3.4. This affects the <b>global</b> , <b>ip address</b> , <b>outbound</b> , <b>route</b> , and <b>static</b> commands.	4.2(4)
CSCdk67488	PIX Firewall no longer reboots repeatedly when supplied with a long list of <b>name</b> statements.	4.2(3)
CSCdk66685	The <b>fixup protocol smtp</b> command now works correctly with multiline SMTP banners.	4.2(3)
CSCdk66556	Inbound pings through an authorized connection now work correctly. This formerly failed over a <b>static</b> when NAT was disabled ( <b>nat 0</b> ).	4.2(3)
CSCdk66331	PIX Firewall no longer puts the wrong subnet mask in the routing table when the <b>rip inside passive</b> command is enabled.	4.2(4)
CSCdk65675	The <b>show failover</b> command no longer causes an assertion error.	4.2(3)
CSCdk65454	PIX Firewall now delimits HTTP headers with CR-LF-CR-LF to make it HTTP 1.1 compliant, which is described in Section 4.1 of RFC-2068.	4.2(3)
CSCdk63839	The <b>snmp-server</b> command now lets you enter the <b>contact</b> and <b>location</b> strings with spaces. Formerly, the spaces were compressed out of the string.	4.2(4)
CSCdk63835	Up to five SNMP servers can be specified. In version 4.2(4), if you attempt to enter a sixth server command statement, a clear error message displays. Formerly, the error message was "SNMP ioctl() error, unable to set."	4.2(4)
CSCdk61913	PIX Firewall now permits multiple shared subnets on the same wire. This change permits backward compatibility with the behavior of version 4.0.7. To accomplish this change, PIX Firewall no longer rejects <b>route</b> statements when the next hop route destination is on the same subnet. In addition, the interface specifications in the <b>static</b> and <b>global</b> statements are used to select the correct routing table.	4.2(3)
CSCdk61170	Inbound SQL*Net now works correctly.	4.2(3)
CSCdk60423	Duplicate entries in the <b>outbound</b> are now ignored.	4.2(3)
CSCdk59508	The <b>show xlate</b> and <b>show conn</b> commands now list different information than previous PIX Firewall versions.	4.2(3)
CSCdk59467	The <b>failover</b> command now correctly recovers if an automatic update of the two units is interrupted.	4.2(3)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk59306	The <b>alias</b> command now creates the correct netmask if a mask is not specified.	4.2(3)
CSCdk59304	The new <b>sysopt connection timewait</b> command adds an additional 15 seconds to a connection being closed to let simultaneous closes complete successfully.	4.2(3)
CSCdk59286	For Telnet console access, in pages 10 and 11 of RFC 854, a CR character must be sent as a two-character sequence CR-NULL with the exception of CR-LF which represents a “single logical” new line command when in NVT ASCII mode.  Unfortunately, the QVT Telnet client does not follow this requirement in the RFC. To be compatible, Telnet console access has been modified for this exception with CR-LF now produces a “logical newline.”  CR-NULL produces “CR only” and the exception to NVT ASCII is: <i>CR-any_character</i> , which is a CR followed by <i>any_character</i> .	4.2(4)
CSCdk58699	The <b>pager</b> command now displays the proper number of lines before prompting you to continue.	4.2(3)
CSCdk58145	The <b>name</b> command now works correctly without sporadic failures.	4.2(3)
CSCdk58142	The <b>name</b> command now accepts up to 16 characters for the name, and a dash character no longer is accepted in a name.	4.2(3)
CSCdk57769	PIX Firewall no longer hangs and causes a failover switch while modifying a WebSENSE database.	4.2(3)
CSCdk57230	Large ping packets no longer get dropped in dual NAT ( <b>alias</b> command use).	4.2(3)
CSCdk57153	PIX Firewall no longer reboots during a ping of an outside host through a PAT connection started via user authentication.	4.2(3)
CSCdk57150	Outbound DNS lookups no longer fails with PAT and user authentication.	4.2(3)
CSCdk57107	The <b>alias</b> command now provides the correct netmask when not specified.	4.2(3)
CSCdk55691	The <b>aaa authentication</b> command has a new unsupported EFT feature that lets you prohibit RADIUS UDP access through the PIX Firewall unless specifically permitted. This capability is a precursor for support of RADIUS authorization in a future release. For TACACS+, you can prohibit UDP access with the <b>aaa authorization</b> command. The new command syntax adds the <i>protocol/port</i> options to the <b>aaa authentication</b> command. Refer to the <b>aaa</b> command page in the <i>Configuration Guide for the PIX Firewall</i> for a description of this syntax as it is used with the <b>aaa authorization</b> command.	4.2(3)
CSCdk53627	PIX Firewall no longer fragments packets in a mixed Token Ring and Ethernet environment.	4.2(3)
CSCdk52923	Inbound pings from the outside no longer fail when they have proper authorization.	4.2(3)
CSCdk52863	PIX Firewall no longer lets inbound ICMP fragments pass through firewall.	4.2(3)
CSCdk51545	Private Link now correctly handles large packets with the DF (Don't Fragment) bit set. Formerly, Private Link would drop the packets silently.	4.2(3)
CSCdk50549	PIX Firewall no longer fails when a 15-character IP address is used.	4.2(3)
CSCdk50529	An FTP back connection no longer ignores the norandomseq setting of the parent connection.	4.2(3)
CSCdk50224	UDP IP fragments no longer cause PIX Firewall failure. This bug is the basis of the new IP Frag Guard feature provided with the <b>sysopt security fragguard</b> command.	4.2(3)
CSCdk49981	Use of nslookup from a perimeter interface no longer can query a host on the inside interface without proper authorization.	4.2(3)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk49808	The <b>aaa authorization</b> command's handling of network addresses now works correctly with interfaces other than the inside.	4.2(3)
CSCdk49068	The <b>debug icmp trace</b> command no longer causes spontaneous failover.	4.2(3)
CSCdk47520	SQL*Net now connects correctly through PIX Firewall.	4.2(3)
CSCdk47456	The secondary failover host no longer sends RIP broadcasts while in standby mode.	4.2(3)
CSCdk47341	Unconfiguring RIP with failover active no longer causes the Secondary unit to fail.	4.2(3)
CSCdk47338	The secondary failover host no longer sends RIP broadcasts while in standby mode.	4.2(3)
CSCdk47235	PIX Firewall no longer reboots and crashes sporadically. The previous behavior would show in the syslog messages that PIX Firewall was switching to failover when neither the failover hardware was present or the <b>failover</b> command enabled. This problem was also seen when passing large packets through the PIX Firewall.	4.2(3)
CSCdk47051	PIX Firewall no longer displays an error message on bootup about Token Ring failure. The previous behavior displayed this message: (main.c:2268) cmd_taken(1) failed.	4.2(3)
CSCdk46673	PIX Firewall no longer corrupts e-mail passing through the unit when Mail Guard issues a NOOP command on receipt of a command that is not part of its RFC 821 permitted command set. The corruption caused sections of the email to be replaced with a series of Xs. Syslog messages would contain the statement "SMTP made noop" when the NOOP command was issued.	4.2(3)
CSCdk46553	Entering the <b>mailhost</b> command no longer causes PIX Firewall to fail.	4.2(3)
CSCdk46243	Inbound UDP authorization now requires authentication.	4.2(3)
CSCdk45124	The <b>fixup protocol sqlnet</b> command now works.	4.2(3)
CSCdk44746	When upgrading from a previous PIX Firewall version, <b>global</b> commands in the configuration now receive the correct network mask. The previous behavior ignored subnetting during the command conversion.	4.2(3)
CSCdk44220	PIX Firewall no longer displays the message "Smallest mtu" in the configuration. This was a debugging command that was removed from the code.	4.2(3)
CSCdk42950	PIX Firewall now handles RIF information properly for interaction between Token Ring and HSRP router on the same ring.	4.2(3)
CSCdk42655	The <b>aaa authorization</b> command no longer accepts <b>out</b> as a shortened form of <b>outbound</b> .	4.2(3)
CSCdk42254	The <b>outbound</b> command with a negative <i>list_id</i> no longer causes failures.	4.2(3)
CSCdk41882	Syslog messages are no longer stated to originate from port 0. This bug made it appear that syslog messages were not being received at the syslog server.	4.2(3)
CSCdk41825	The <b>write floppy</b> command no longer crashes failover-equipped PIX Firewalls.	4.2(3)
CSCdk41688	The <b>aaa authorization</b> command now works correctly when outbound UDP authorization is enabled.	4.2(3)
CSCdk40896	Authorization for UDP now works correctly on same port previously authorized for TCP.	4.2(3)
CSCdk40673	Checking failover status no longer causes PIX Firewall to fail.	4.2(3)
CSCdk40528	Failover no longer causes a race condition between the Active and Standby units. To correct the problem, a 10-second delay was added before the <b>no failover active</b> command takes effect.	4.2(2)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk39478	If you cut and paste text from your console computer into the configuration, check it carefully afterwards. Some lines may be dropped during the process due to buffer overflow.	4.2(2)
CSCdk38353	PIX Firewall now correctly handles path MTU (maximum transmission unit) requests. Path MTU relies on the PIX Firewall to generate an ICMP host unreachable message (code=3) on reception of a packet that needs to be fragmented but has the Don't Fragment flag set in the IP header (type=4). PIX Firewall formerly discarded these packets without returning the host unreachable message.	4.2(2)
CSCdk38092	The Private Link key now correctly accepts 14 hexadecimal characters.	4.2(2)
CSCdk37223	For the <b>aaa</b> , <b>radius-server</b> , and <b>tacacs-server</b> commands, 16 TACACS+, RADIUS, or URL servers are supported.	4.2(2)
CSCdk36912	When DNS traffic is logged, the ID field in the DNS response packet appears in the source port field. It is normal to see a UDP state with a "d" flag; such as: <pre>Global 192.159.1.1 Local 10.8.8.11 static nconns 0 econns 0 flags s UDP out 204.31.17.2:12345 in 10.8.8.11:67890 idle 0:01:30 flags d</pre>	4.2(2)
CSCdk36498	The maximum password length for accessing the console is 16 characters with the <b>aaa authentication telnet console</b> command.	4.2(2)
CSCdk36273	Hosts behind the PIX Firewall are no longer subject to DoS attacks to inside static IP addresses. Inside hosts are not susceptible to DoS attacks even when attacked with a high volume of IP fragments to penetrate across statics.	4.2(2)
CSCdk36092	The <b>clear radius-server</b> and <b>clear tacacs-server</b> commands do not have any arguments. In addition, before using these commands, remove the <b>aaa</b> commands from the configuration that references the AAA servers.	4.2(2)
CSCdk35931	Denying one service with the <b>outbound</b> command no longer denies other services.	4.2(2)
CSCdk35899	The maximum timeout value for the <b>radius-server</b> and <b>tacacs-server</b> commands is 30 seconds.	4.2(2)
CSCdk35552	The TCP random sequence value can no longer be predicted.	4.2(2)
CSCdk34855	For the <b>aaa</b> command, four attempts are allowed for Telnet authentication, infinite for HTTP, and only one for FTP.	4.2(2)
CSCdk34853	For the <b>aaa</b> , <b>radius-server</b> , and <b>tacacs-server</b> commands, 16 TACACS+, RADIUS, or URL servers are supported.	4.2(2)
CSCdk34799	The use of the <b>traceroute</b> command through a PAT global now works correctly.	4.2(2)
CSCdk34696	FTP works correctly when two PIX Firewall units' outside interfaces are connected to each other.	4.2(2)
CSCdk34668	PIX Firewall no longer denies access to all services when an <b>outbound</b> command statement is used in the configuration. The default is to permit all services until explicitly denied.	4.2(2)
CSCdk33996	PIX Firewall no longer lets non-dnat addresses go out on an existing dnat connection.	4.2(5)
CSCdk33877	PIX Firewall now correctly handles outbound encapsulated ICMP messages of types 3, 4, 5, 11, and 12.	4.2(2)
CSCdk33802	Failed authentication message no longer displays on the PIX Firewall console.	4.2(3)
CSCdk33420	A workaround has been provided for situations in which an attempt at authorization fails but a second attempt times out. Refer to the "AAA" usage note for more information.	4.2(2)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk32369	The <b>configure floppy</b> command does not check to see if a diskette is present.	4.2(3)
CSCdk31770	PIX Firewall now supports PAT with rsh (Rshell).	4.2(2)
CSCdk31760	PIX Firewall now correctly accesses the next AAA server when the current server becomes inaccessible.	4.2(2)
CSCdk30996	When a SYN packet arrives with PSH bit turned on, PIX Firewall allows the outbound traffic through the firewall.	4.2(2)
CSCdk29494	Denying one service with the <b>outbound</b> command no longer denies other services.	4.2(2)
CSCdk29476	PIX Firewall no longer removes all <b>outbound</b> statements from the configuration when the <b>no outbound 1 permit 0.0.0.0</b> command is issued.	4.2(2)
CSCdk29475	Refer to "RPC Use" in the section, "Important Notes" for more information.	4.2(2)
CSCdk28193	PIX Firewall no longer fails every 5 minutes when the <b>fixup protocol smtp</b> command is enabled.	4.2(2)
CSCdk27770	PIX Firewall now permits passive FTP through a PAT global.	4.2(2)
CSCdk26803	The FTP <b>port</b> command now works correctly with PAT (Port Address Translation). The previous behavior caused FTP sessions to hang when the <b>FTP Is</b> command was entered when the only <b>global</b> statement in the PIX Firewall configuration was for PAT.	4.2(2)
CSCdk25962	PIX Firewall no longer fails after a user upgrades from a previous version of the PIX Firewall software.	4.2(2)
CSCdk25517	The <b>apply</b> command now correctly works with an interface specification in the command.	4.2(2)
CSCdk25487	SNMP MIBs now correctly provide return values when accessed through the PIX Firewall.	4.2(2)
CSCdk25383	Refer to "RPC Use" in the section, "Important Notes" for more information.	4.2(2)
CSCdk23717	PIX Firewall is no longer susceptible to a SYN denial of service attack through AAA authentication.	4.2(2)
CSCdk23711	PIX Firewall no longer fails after the unit is upgraded to version 4.2. The previous failures occurred because FTP mishandled the association between an xlate and a connection.	4.2(2)
CSCdk23441	Only use the <b>established</b> command with the <b>permitto</b> and <b>permitfrom</b> options. Without these options, the <b>established</b> command can be used to gain access to restricted parts of your network.	4.2(3)
CSCdk23329	PIX Firewall now lets FTP work when HTTP authentication is enabled. With this fix, when HTTP authentication is enabled, users are prompted for login credentials when accessing the network with a web browser. In addition, TCP sessions other than HTTP that are not denied by outbound lists are allowed through without requiring authentication.	4.2(2)
CSCdk22976	Telnet to an MS-Exchange server on port 25 across the PIX Firewall no longer causes every character to be accompanied by carriage-return, linefeed characters.	4.2(2)
CSCdk22832	PIX Firewall no longer fails after the <b>aaa accounting</b> command is set to monitor outbound connections. Previously, when an outbound connection started, the PIX Firewall would fail.	4.2(2)
CSCdk22568	Failover now works correctly when the PIX Firewall is configured to broadcast a default route using RIP.	4.2(2)

Table 3 Resolved Bugs (Continued)

DDTS Number	Description	Release
CSCdk22371	The Mail Guard feature now works correctly when sending an SMTP EHLO command to an MS Exchange server. Previously, the MS Exchange server would hang upon receipt of the EHLO command through the PIX Firewall. The Mail Guard feature is enabled on the PIX Firewall with the <b>fixup protocol smtp</b> command. Also refer to bug fix CSCdk09763 for further EHLO improvements.	4.2(2)
CSCdk21511	PIX Firewall now automatically upgrades users with a 64-connection license to a 128-connection license.	4.2(2)
CSCdk21408	AAA authentication no longer becomes inoperable when embryonic connections are exceeded. The previous behavior let inbound and outbound connections through without authentication after the limit was exceeded.	4.2(2)
CSCdk21312	The <b>aaa authentication</b> command now works correctly for inbound user authentication. Previously, use of the <b>aaa authentication except</b> command would fail. For example, the following commands failed so that the mail server at 10.1.1.1 would be challenged for login credentials and would not deliver mail:  <pre>aaa authentication any inbound 0.0.0.0 0.0.0.0 aaa authentication except inbound 10.1.1.1 255.255.255.255</pre>	4.2(2)
CSCdk21113	PIX Firewall no longer converts network <b>conduit</b> statements to host <b>conduit</b> statements when upgrading from a previous PIX Firewall version. Previously, if a 4.1(6) configuration contained the following <b>conduit</b> statement:  <pre>conduit (inside,outside) 204.31.17.0 0 tcp 0 0</pre> The PIX Firewall installation conversion script incorrectly converted the statement to the following by adding the <b>host</b> option:  <pre>conduit permit tcp host 204.31.17.0 any</pre>	4.2(2)
CSCdk20305	Pings to broadcast addresses no longer are answered with the broadcast address as the source address. The previous behavior resulted because PIX Firewall incorrectly swapped the source and destination addresses in the ICMP packet.	4.2(2)
CSCdk20122	PIX Firewall now permits 2,560 <b>aaa authentication except</b> statements.	4.2(2)
CSCdk19979	One global pool address is no longer assigned to two or more local IP addresses.	4.2(5)
CSCdk19656	PIX Firewall no longer fails during failover when PIX Firewall contains 3Com network interface cards.	4.2(2)
CSCdk17897	Use of the <b>conduit</b> command no longer results in random configuration corruption. In one instance, a <b>conduit</b> command was removed and PIX Firewall inserted 8000 identical <b>conduit</b> statements into the configuration.	4.2(3)
CSCdk17808	Syslog output now displays correctly when the <b>write</b> command is issued.	4.2(2)
CSCdk17788	At startup, the PIX Firewall now correctly displays an export control warning message when an encryption device is detected in the unit.	4.2(2)
CSCdk17784	Cisco recommends that you do not change the default port assigned to FTP with the <b>fixup protocol</b> command. Once changed, all traffic into the PIX Firewall will only work on the port you specify. Default FTP traffic through the PIX Firewall will no longer work.	4.2(2)
CSCdk16222	Do not use the <b>virtual http</b> command when an inside client is configured to access a proxy server located on an unprotected interface of the PIX Firewall.	4.2(2)
CSCdk16053	Refer to CSCdk21312 for resolution description.	4.2(2)
CSCdk15978	PIX Firewall no longer fails after the <b>aaa accounting</b> command is set to monitor outbound connections. Previously, when an outbound connection started, the PIX Firewall would fail.	4.2(2)

**Table 3 Resolved Bugs (Continued)**

<b>DDTS Number</b>	<b>Description</b>	<b>Release</b>
CSCdk15527	Failover on PIX Firewall units configured with two Token Ring interfaces now works properly.	4.2(1)
CSCdk14305	Performing a <b>write memory</b> command followed by a <b>reload</b> command no longer changes the <b>outbound</b> command list.	4.2(2)
CSCdk11848	Private Link now accepts the full 56-bit key. Previously 8 bits of the key were ignored. A new parity feature has been added so that an additional 8 bits have been added to the key just for parity to ensure that the key is passed correctly across the link.	4.2(2)
CSCdk11335	PIX Firewall now sends a syslog message when the uauth inactivity timer expires. This feature lets sites charge for connection time starting with the “%PIX-2-109001: Auth start for user” syslog message and ending when the uauth inactivity timer expires.	4.2(2)
CSCdk11011	Syslog no longer shows the amount of data as a negative number.	4.2(1)
CSCdk10909	The host name no longer disappears after reading in a large configuration from diskette.	4.2(2)
CSCdk09763	PIX Firewall now handles UNIX sendmail programs that send the EHLO command without a linefeed even though the RFC specifies that a CRLF must be sent. PIX firewall now sends “500 Command unrecognized” to suppress the negotiation of EHLO commands regardless of whether the sending client sends the EHLO with or without a linefeed.	4.2(2)
CSCdk06673	Syslog failover and reset messages were moved to the <b>logging</b> command’s level 1 alerts. Formerly these messages were in levels 2 and 6 respectively.	4.2(2)
CSCdk05737	The <b>conduit</b> command now correctly accepts a zero in a port field to mean all ports. In version 4.2 and later, you can also specify all ports by not including a port value in the command.	4.2(1)
CSCdk04509	PIX Firewall now correctly handles <b>aaa authentication</b> statements that reference different authentication server types (RADIUS or TACACS+) for inbound and outbound connections.	4.2(2)
CSCdk04242	Outbound user authentication now works correctly with a PAT global address.	4.2(1)
CSCdk04054	The <b>ip</b> protocol is now recognized correctly.	4.2(1)
CSCdk03381	AAA accounting now works when a connection is created.	4.2(3)
CSCdk03375	PIX Firewall no longer runs the <b>aaa accounting</b> routines when this feature is not requested. This fix improves PIX Firewall performance.	4.2(2)
CSCdk00333	PAT now correctly handles ICMP MTU resize packets.	4.2(1)
CSCdj94418	The <b>apply</b> command now works correctly. Previously, outbound lists would not work correctly until the <b>apply</b> statement was removed and then reinserted.	4.2(2)
CSCdj93649	The new <b>linkpath 0 0 ip_address</b> command options let you specify the default Private Link route path. Refer to the <i>Configuration Guide for the PIX Firewall</i> for more information.	4.2(1)
CSCdj92046	Outbound lists denying access to all outbound users except for specifically allowed addresses now block outbound attempts from denied users, including attempts on high ports.	4.2(1)
CSCdj90814	Private Link no longer fails when blasted with prefragmented UDP packets.	4.2(2)
CSCdk85168	The <b>global</b> command now displays a PAT address correctly.	4.2(2)
CSCdj84604	PAT now works correctly with passive FTP.	4.2(2)
CSCdj82419	HP OpenView can now browse perimeter networks on the PIX Firewall.	4.2(1)

**Table 3 Resolved Bugs (Continued)**

DDTS Number	Description	Release
CSCdj70621	PIX Firewall's <b>debug icmp trace</b> command now displays ICMP packets arriving, departing, and traversing the PIX Firewall.	4.2(1)
CSCdj57072	The <b>show version</b> command now lists the processor speed.	4.2(1)
CSCdk54553	PAT now works correctly when a fragmented packet arrives in reverse order.	4.2(2)

## Documentation Updates

The version 4.2(3) *Configuration Guide for the PIX Firewall* describes the **telnet timeout** command as an inactivity timer. For version 4.2(3), it was an absolute timer. In version 4.2(4) and later, it became an inactivity timer as described in the documentation.

## Related Documentation

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

- *Configuration Guide for the PIX Firewall*
- *Quick Installation Guide for the PIX Firewall*
- *Regulatory Compliance and Safety Information for the PIX Firewall*
- *System Log Messages for the PIX Firewall*

All of these documents, including these release notes, apply to the PIX Firewall, PIX10000, PIX 510, and PIX 520 hardware models. Refer to the *Release Notes for the PIX Firewall Version 4.4(1)* for information on the PIX 515.

Cisco provides PIX Firewall technical tips at:

<http://www.cisco.com/warp/public/110/index.shtml#pix>

## 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. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R)

Copyright © 1998-1999, Cisco Systems, Inc.  
All rights reserved.