



Text Part Number: 78-6419-01

Release Notes for the PIX Firewall Version 4.3

February 1999

This document describes the changes for all 4.3(x) versions of the PIX Firewall software.

Contents

- “System Requirements” on page 1
- “New and Changed Information” on page 2
- “Installation Notes” on page 5
- “Limitations and Restrictions” on page 6
- “Important Notes” on page 7
- “Caveats” on page 16
- “Related Documentation” on page 20
- “Cisco Connection Online” on page 21
- “Documentation CD-ROM” on page 22

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

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

System Requirements

The information contained in these release notes applies to all PIX Firewall hardware models running software version 4.3 or later.

Version 4.3 requires at least 16 MB (an optional 128 MB upgrade is available).

Version 4.3 supports up to four Ethernet interfaces. Three Token Ring interfaces have been tested with the PIX Firewall.

Corporate Headquarters

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

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

New and Changed Information

Version 4.3 includes the following features.

New Features in Version 4.3(1)

PIX Firewall Syslog Server

The PIX Firewall Syslog Server (PFSS) runs on a Windows NT system and receives syslog messages from up to 10 PIX Firewalls.

Note The Windows NT filesystem where you install PFSS must be an NTFS partition and not FAT.

Note When you install PFSS on the Windows NT system, write down the values you supply for the disk empty timer and the disk full timer. Once PFSS is installed, the only way you can view this information again is by examining the Windows NT Registry with the regedit command and searching for **disk_empty_watch**. Also, if you need to view the information in the Registry, do not change it in the Registry. The information can only be changed from the **Start>Settings>Control Panel>Services** setting. You can view the other parameter values in the pfss.log file that accompanies the daily log files.

Note PFSS and the PIX Firewall Manager cannot be used together even if installed on separate Windows NT systems.

Note If the Windows NT system on which PFSS is installed reaches the percentage of disk full value you set when installing PFSS, the Windows NT system causes the PIX Firewall to stop all of its connections until the log files are removed from the system.

Refer to the **logging** command page in the *Configuration Guide for the PIX Firewall Version 4.3*, Chapter 5, “Command Reference” for additional important information about configuring the PIX Firewall for use with PFSS.

Installation and configuration instructions for the PFSS on the Windows NT system are described in the *Quick Installation Guide for the PIX Firewall Version 4.3*.

Real-Time Clock

The **clock set** command allows you to set the PIX Firewall’s internal clock. The internal clock is used to time stamp syslog messages. You can use the **show clock** command to display the current time.

Note The **clock set** command only works until December 31, 2097.

Telnet Console Access from All Internal Interfaces

You can now access the PIX Firewall console via Telnet from all internal interfaces.

Enable AAA Authentication Console

You can now set the **enable** option on the **aaa authentication console** command. This command requires that access to the PIX Firewall console be authenticated from a TACACS+ or RADIUS server. After authentication is successful, all changes to the configuration from the serial console are logged to the syslog servers at syslog level 5. Changes made from Telnet console sessions are not logged.

If the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the enable password.

New Features in Version 4.3(2)

AAA Port Range Specification

You can now set port ranges for the TCP and UDP protocols with the **aaa authorization** command.

Disabling and Re-Enabling of Syslog Messages

You can now disable specific syslog messages with the **no logging message** *syslog_id* command, and re-enable specific syslog messages with the **logging message** *syslog_id* command. You can display all disabled messages with the **show logging disabled** command, and re-enable all disabled messages with the **clear logging disabled** command.

PIX Firewall SNMP Object ID

An SNMP object ID (OID) for PIX Firewall now displays in SNMP event traps sent from the PIX Firewall. OID 1.3.6.1.4.1.9.1.227 was assigned as the PIX Firewall system object ID.

User-Based Timeout

You can use the **show uauth** command to display CiscoSecure version 2.1 or later idletime and timeout values that provide user-based, rather than global, authentication timeouts.

The Cisco Secure user-based timer durations override the duration set with the **timeout uauth** command.

Virtual Telnet Logout

The **virtual telnet** command lets you log in to the virtual authentication server on first access and log out on second access to the specified IP address.

New Commands

The new commands are:

- **clock set**—which allows you to set the PIX Firewall's internal clock. The current time is used for time stamped syslog messages, which you can set with the **logging timestamp** command.
- **show clock**—which displays the current time.

Changed Commands

Table 1 lists command changes in version 4.3. All commands are documented in the *Configuration Guide for the PIX Firewall Version 4.3*.

Table 1 Command Changes

Command	Change	Version
aaa	<ul style="list-style-type: none"> • aaa accounting—lets you specify a protocol and port for accounting services in the form of <i>protocollport</i>. Accounting now supports both TCP and UDP. • aaa authentication enable console—lets you require authentication to access the PIX Firewall console and lets you log changes made to the PIX configuration from a serial console session. • aaa authorization—lets you specify port ranges which users are authorized to access. 	4.3(1) and 4.3(2)
failover	The show failover command now provides clearer information when the failover feature is disabled. [CSCdk49733]	4.3(2)
floodguard enable/disable	Enables or disables TCP resource control for the AAA authentication proxy.	4.3(2)
linkpath	New MTU option lets you specify the packet size for transmissions between the two Private Link PIX Firewall units.	4.3(2)
logging	<ul style="list-style-type: none"> • logging timestamp—lets you specify that syslog messages sent to a syslog server be marked with the current time. • logging host—lets you send syslog messages by either UDP or TCP. • logging message—lets you re-enable a previously disabled syslog message. • no logging message—lets you disable a specific syslog message. [CSCdk76196] • clear logging disabled—lets you reenable all disabled messages. • show logging disabled—lets you view disabled messages. • show logging—lets you view logging information and whether a PFSS server is disabled. 	4.3(1) and 4.3(2)
show conn	No longer displays the total number of connections that are licensed. This information is now available only in the PIX Firewall reboot startup messages.	4.3(2)
show uauth	Now displays CiscoSecure idletime and timeout values.	4.3(2)
show version	Now lists the BIOS version.	4.3(2)

Table 1 Command Changes (continued)

Command	Change	Version
sysopt	New connection enforcesubnet option [CSCdk62467]. Also, the sysopt security fragguard command is now disabled by default.	4.3(2)
timeout	The minimum duration for the xlite option has been reduced to 1 minute. [CSCdk77361]	4.3(2)
virtual http	The web browser now lists the correct URL instead of the virtual http command's IP address. [CSCdk16222]	4.3(2)
virtual telnet	Lets you log in to the virtual authentication server on first access and log out on second access to the specified IP address.	4.3(2)

Removed Commands

The version 4.2 **tunnel** command is obsolete in version 4.3. This command worked with a third-party vendor's IPSEC card that is no longer supported.

Installation Notes

PIX Firewall only supports configuration upgrades from version 4.2(x) and later. With versions previous to 4.2(x), save your configuration to an ASCII text file using your terminal configuration program before upgrading, and write down your activation key. Table 2 lists the upgrade path to use to get to the current version.

Table 2 Upgrade Paths for Older Versions

If Your Pix Firewall Version is:	Install This Version:
2.7.x	3.0, then upgrade to the next version
3.0	4.0.7, then upgrade to the next version
4.0.7	4.1(7), then upgrade to the next version
4.1(5) or later	4.2(x), then upgrade to the next version
4.2(x)	4.3(2)

To upgrade from a previous PIX Firewall version:

- Before upgrading, copy your configuration to diskette with the **write floppy** command and write down your license activation key. You must have a copy of your activation key to restore a previous version from diskette.
- For failover upgrades, refer to the “Failover” section in Chapter 3, “Advanced Configurations” in the *Configuration Guide for the PIX Firewall Version 4.3*.
- If you cut and paste your configuration from a text file into the PIX Firewall, some statements from the original configuration 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]

- 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 Version 4.3* for information on downloading software from CCO.
- During installation, PIX Firewall converts your 4.2 configuration to the current version. 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 during troubleshooting.
- 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 statement. Without the **permitfrom** option, the **established** command is interpreted as **established protocol ... permitfrom protocol any_port**.
- If necessary, fix the **timeout** command statement. In version 4.2, the **timeout uauth** command defaults to **absolute**.
- Set the **netmask in global** to the specific Class: 255.0.0.0 for Class A (0 to 127), 255.255.0.0 for Class B (128 to 191), and 255.255.255.0 for Class C (192 to 254).
- For the **static** command, use a netmask of 255.255.255.255 for all ranges of host IP addresses unless subnetting is in effect.
- Downgrades 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.
- 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.

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 4.3 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 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 4.3 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 4.3 software.

- 2 PIX Firewall supports up to four Ethernet interfaces. Three Token Ring interfaces have been tested with PIX Firewall.
- 3 The maximum size of the configuration in a 2 MB Flash memory card is 1 MB minus the size of the current software’s .bin file. For example, if the .bin file is 609,000 bytes, the maximum size of the configuration is $1\text{ MB} = 1,048,576 - 609,000 = 439,576$ bytes.

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.

Access Control Lists

Refer to the **outbound** command page in the *Configuration Guide for the PIX Firewall Version 4.3* for more information on **outbound** command rules.

Aliases

- Ensure that the **alias** command 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** command statements allowing access to 192.150.50.7.
- An example of using the **alias** command 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** command you would expect to use is:

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

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

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

Attacks

- In version 4.3(2), PIX Firewall has improved its defense against the land.c or spoofed IP address attacks. The land.c attack, also known as the Land Attack, causes a computer to create a TCP connection to itself, get caught in a loop, and have to be rebooted.
- The new **sysopt connection enforcesubnet** command prevents external users from spoofing internal addresses. This command prevents packets with a source address belonging to the destination subnet from traversing the PIX Firewall. For example, if a packet arrives from the outside but has a source address belonging to the inside subnet, the PIX Firewall does not let the packet through.

Note Do not use the **sysopt connection enforcesubnet** command if the internal and external interfaces are on the same logical subnet as may exist when NAT is disabled.

- 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 (it is disabled by default).
- Do not use the **established** command without the **permitto** and **permitfrom** options. Without these options, outside users can attack your network through **conduit** command access. [CSCdk23441]

Authentication

- RADIUS is only supported for authentication and not for authorization.
- For the **aaa radius-server**, and **tacacs-server** commands, 16 TACACS+ or RADIUS 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]
- You can have a maximum of 16 RADIUS, TACACS+, or URL servers configured on the PIX Firewall. For example, if you have 10 RADIUS servers and 6 TACACS+ servers, and you want to add a URL server, you must disable access to either a RADIUS or TACACS+ server.
- The **clear radius-server** and **clear tacacs-server** commands do not have arguments. In addition, before using these commands, remove any **aaa** commands from the configuration that reference 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.

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 in a command line is 512. Additional characters past this limit are ignored.

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.
- 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.
- The maximum size of the configuration in a 2 MB Flash memory card is 1 MB minus the size of the current software's bin file. For example, if the bin file is 609,000 bytes, the maximum size of the configuration is $1 \text{ MB} = 1,048,576 - 609,000 = 439,576$ bytes.

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.

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. Refer to the "Open Caveats" section under bug CSCdk50579 for more information about using the **alias** command with an external DNS server.
- 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** command 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** command statement and lets any user access any port on the 192.168.1.42 server. [CSCdk23441]

Failover Option

PIX Firewall now supports failover in a switched environment.

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 the **floodguard enable** command 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.

Installation Addendum

The former version *Installation Addendum for the DC PIX Firewall* has been combined into the *Quick Installation Guide for the PIX Firewall Version 4.3*.

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 Meeting Point
- Xing StreamWorks

NAT (Network Address Translation)

- The NAT feature in the PIX Firewall differs from the 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 Address 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.

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** command statement for ICMP to your configuration.
- A host **static** command without a **conduit** command 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.

PIX Firewall Syslog Server (PFSS)

- PIX Firewall Manager (PFM) and PFSS must not be used together. When you install PFSS, it checks for the presence of the PFM on the same system and informs you accordingly.
- To recover use of the PIX Firewall after the Windows NT disk becomes full:
 - Step 1** On the Windows NT system, move the old logs to a new filesystem (or back up and remove them). Make sure this creates enough free disk space for more log messages.
 - Step 2** On the PIX Firewall enter configuration mode and check that the PFSS host is correctly disabled from the PIX Firewall by entering the **show logging** command and look for the “disable” keyword, which means that no new connections are allowed through the PIX Firewall.
 - Step 3** Disable logging to the PFSS host by entering the **no logging host interface ip_address** command for the disabled host.
 - Step 4** Re-enable logging by entering the **logging host interface ip_address tcp/1468** command for the disabled host.
 - Step 5** Check that the PFSS host is now enabled by reentering the **show logging** command. The disable keyword should now be gone.
 - Step 6** Use the **show conn** command to determine if new connections have started. If none have, start a Telnet or FTP session through the PIX Firewall to start new connections.
If new connections do not restart, reboot the PIX Firewall.

Private Link Option

- If you are using Private Link, both PIX Firewall units must run the same software version and be the same hardware models.
- All PIX Firewall units support the PCI Private Link card; however, use of this card reduces the number of possible interfaces to three.

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)
- Sitara Networks Protocol (SNP)
- 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 Version 4.3* for information on supported protocols.

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.

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

PIX Firewall then manages the connection dynamically. An example 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** command for portmapper is necessary for the initial port discovery message to come to the internal network.
- A **conduit** command for NFS 2049 port is necessary because NFS over UDP does not have to generate a “keep alive” message to keep the PIX from cleaning the idle UDP connections.
- 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. An example of the **conduit** command 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]
- You can have a maximum of 16 RADIUS, TACACS+, or URL servers configured on the PIX Firewall. For example, if you have 10 RADIUS servers and 6 TACACS+ servers, and you want to add a URL server, you must disable access to either a RADIUS or TACACS+ server.

Setup Wizard

The information for the Setup Wizard is now listed in the *Quick Installation Guide for the PIX Firewall Version 4.3*.

show version Command

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

SNMP

- Cisco System OID 1.3.6.1.4.1.9.1.227 was assigned as the PIX Firewall system object ID.
- In MIB-II, the state of an interface is now only reported as up if the interface card is available and has a working cable plugged into the interface. [CSCdk81214]

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 the **nat 1 0 0** command only grants outbound access to hosts not specified in the net **static** command statement.
- Use a netmask of 255.255.255.255 for all host IP addresses.

Syslog Feature

- The “%PIX-6-199002: PIX startup completed. Beginning operation.” syslog message cannot be blocked with the new **no logging message** command that lets you block individual syslog messages.
- When DNS traffic is logged, the ID field in the DNS response packet appears in the source port field. [CSCdk36912]
- The new PIX Firewall Syslog Server (PFSS) truncates messages that are longer than 512 characters.
- Syslog failover and reset messages were moved to the **logging** command’s level 1 alerts. Formerly, these messages were in levels 2 and 6 respectively. [CSCdk06673]
- Syslog message 107001 was removed:

```
107001: %I attempted to ping %I (%I)
```

Two new syslog messages were added to replace 107001:

```
106013: Dropping echo request from %I to PAT address %I
106014: Deny inbound %s, pkt_as_ascii()
```

- 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**.

Telnet Console Sessions

The following affect Telnet console sessions:

- Starting with 4.3, Telnet console sessions can occur from any internal interface, but not the outside.
- If the AAA Telnet console login request to authentication times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the password set with the **enable password** command.
- The output of the **show perfmon** command does not appear on the Telnet console.
- The **debug icmp trace** and **show sqlnet** commands output appears on the first Telnet console session. If a Telnet console session is not in effect, the output appears on the serial console session.

TFTP Configurations

For configurations that you download via TFTP, do not put comments in the configuration file because the PIX Firewall may fail while reading the configuration.

Year 2000 Compliance

PIX Firewall is year 2000 compliant.

Caveats

The following caveats apply to PIX Firewall release 4.3(*n*). Refer to the previous versions of the PIX Firewall release notes for information on bugs in previous releases. On the Web, you can view previous versions of the PIX Firewall release notes at:

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

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

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

Open Caveats

The following are major issues in version 4.3(2):

- Installation—to upgrade from version 4.2 to 4.3 requires an intermediary step of upgrading from version 4.1 to 4.2 first. Problems have been reported where the upgrade from 4.1 to 4.2 may cause some **conduit** and **global** statements to be removed from the configuration. After upgrading, check your configuration and add any missing statements before proceeding.
- Token Ring—If the MTU is greater than 1500 bytes, PIX Firewall may fail within a few hours. The workaround is to set the MTU for Token Ring at 1500 bytes.
- Failover—if your configuration is very large, at approximately 250 KB or larger, PIX Firewall may fail during upgrade. The workaround is to reduce the size of the configuration and upgrade. If this succeeds, introduce more of the configuration back in and then synchronize the units as described in the “Failover” section in Chapter 3, “Advanced Configurations” in the *Configuration Guide for the PIX Firewall Version 4.3*.

- Private Link—MTU path discovery is not supported over Private Link. If packets cannot get through on a route, the workaround is to use ping with various packet sizes to find the best MTU to use. In addition, the new **linkpath** MTU option is not written to the configuration and must be re-entered after each reboot. [CSCdk91242]
- AAA—the **aaa authentication enable console** command takes effect correctly, but is written to the configuration as the **aaa authentication any console** command. [CSCdk76685]
- **sysopt security fragguard**—use of this command may cause the PIX Firewall to fail. This command is disabled by default.

Table 3 lists open caveats.

Table 3 Open Caveats

DDTS Number	Description	Noted in Version
CSCdk89056	If TCP syslog is used with the PIX Firewall Syslog Server (PFSS) and failover is present, the PIX Firewall can fail to send syslog messages to the PFSS and may cause traffic to stop on the PIX Firewall.	4.3(2)
CSCdk86695	Putting comments in a configuration downloaded by TFTP can cause the PIX Firewall to fail.	4.3(1)
CSCdk84112	Syslog does not work properly after clear syslog command.	4.3(1)
CSCdk81282	Syslog prints a garbled message when denying outbound access under PAT configuration.	4.3(1)
CSCdk78707	Under conditions such as low memory or memory corruption, PIX Firewall may generate frequent syslog messages containing the phrase, “PIX-2-SYS-CHUNKBOUNDS attempted to exceed freelist causing failover.”	4.3(1)
CSCdk70747	The virtual telnet command hangs after second Telnet attempt is entered quickly.	4.3(1)
CSCdk76685	The aaa authen enable command is parsed as the aaa authen any command.	4.3(1)
CSCdk69851	PIX Firewall does not allow a password change to a shorter length with RADIUS.	4.3(1)
CSCdk68618	Inbound Telnet fails with DNAT uauth to the fourth interface from outside.	4.3(1)
CSCdk68345	Rebooting the failover Standby unit during configuration replication results in configuration loss.	4.3(1)
CSCdk67889	The Atmel Flash driver cannot write to the second megabyte of the Flash memory.	4.3(1)
CSCdk67887	An incorrect byte value appears in TCP teardown syslog messages.	4.3(1)
CSCdk64250	The conduit permit icmp any any command is required to permit Telnet to work between Private Link sites.	4.3(1)

Caveats

Table 3 **Open Caveats (continued)**

DDTS Number	Description	Noted in Version
CSCdk50579	<p>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.</p> <p>For example:</p> <pre>alias (inside) 192.168.1.4 204.31.17.121 255.255.255.255</pre> <p>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.</p> <p>Workaround: Reverse the alias parameters as follows:</p> <pre>alias (inside) 204.31.17.121 192.168.1.4 255.255.255.255</pre> <p>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.</p>	4.3(2)
CSCdk19912	<p>If the packet containing the data being modified in a FTP or SQL*Net packet is retransmitted, the adjustment records twice. This causes the sequence number for all subsequent packets to be incorrect. This can result in failed connections for both FTP and SQL*Net.</p>	4.3(1)

Resolved Caveats

Table 4 lists resolved DDTS bug reports.

Table 4 **Resolved Caveats**

DDTS Number	Description	Fixed in Version
CSCdk90359	Added SNP protocol literal for Sitara Networks Protocol, protocol 109.	4.3(2)
CSCdk90358	Removed the “licensed” count from the show conn command and made the information only available in the startup messages.	4.3(2)
CSCdk88270	Under heavy traffic, Token Ring failover now works correctly.	4.3(2)
CSCdk84226	The inside interface no longer passes broadcasts.	4.3(2)
CSCdk83300	Outbound list now works correctly when the mask is different than the interface.	4.3(2)
CSCdk82957	Remote shell (rsh) now functions correctly with an HP 9000 if the EFT sysopt connection safeclose command is used.	4.3(2)
CSCdk81214	PIX Firewall now only reports the state of an interface as up for SNMP MIB II if the interface card is available and has a working cable plugged in.	4.3(2)
CSCdk78952	A checksum was requested for copying a configuration via TFTP or to diskette. The request was resolved by adding a “Config OK” message to indicate successful completion and syntax validation of the configuration file. An error displays as the “Config Failed” message.	4.3(2)
CSCdk77361	The minimum duration for the xlite option to the timeout command was reduced to 1 minute.	4.3(2)
CSCdk76196	PIX Firewall now lets you block specific syslog messages with the new no logging message command. However, the “%PIX-6-199002: PIX startup completed. Beginning operation.” syslog message cannot be blocked and neither can groups of messages.	4.3(2)
CSCdk62467	PIX Firewall provides the new sysopt connection enforcesubnet command that filters out self route packets directly or indirectly.	4.3(2)
CSCdk62465	Loopback networks no longer pass through the PIX Firewall.	4.3(1)
CSCdk62456	PIX Firewall is no longer susceptible to the land.c attack.	4.3(1)
CSCdk59859	PIX Firewall now denies source broadcast and destination broadcast packets.	4.3(1)
CSCdk59465	PIX Firewall now allows use of Cisco Secure version 2.1 or later user-based absolute and inactivity timers. The show uauth command now lists these and the durations override the timeout uauth command duration.	4.3(1)
CSCdk57557	The aaa accounting command now works for both TCP and UDP.	4.3(2)
CSCdk56811	Cisco System OID 1.3.6.1.4.1.9.1.227 was assigned as the PIX Firewall system object ID.	4.3(2)
CSCdk56401	Syslog message 107001 was removed: 107001: %I attempted to ping %I (%I) Two new syslogs were added to replace 107001: 106013: Dropping echo request from %I to PAT address %I 106014: Deny inbound %s, pkt_as_ascii()	4.3(2)
CSCdk50571	The network browser authentication prompt was improved.	4.3(2)
CSCdk49733	The show failover command has been improved so that when failover is disabled, PIX Firewall provides the following information: Failover Off Cable Status: My side not connected Reconnect timeout: 0:00:00	4.3(2)

Related Documentation

Table 4 Resolved Caveats (continued)

DDTS Number	Description	Fixed in Version
CSCdk16222	<p>The virtual http command now works correctly with an external proxy server. The former behavior caused the “Error 501 Not Implemented” error message to display in the web browser and a syslog message that started with “109001: Auth start for user '???'.”</p> <p>The fix for this bug has an additional benefit in that the requested URL now correctly displays in the web browser, not the virtual http command’s IP address.</p>	4.3(2)
CSCdj92811	<p>The PIX Firewall now checks static command statements to ensure that the interfaces are specified in the correct order as (<i>high,low</i>); for example, (inside,dmz). If entered incorrectly, the following error message appears:</p> <pre>internal_if_name nn has a lower security value than external_if_name nn</pre> <p>The <code>internal_if_name</code> represents the first interface name and <code>external_if_name</code> represents the second interface name. The <code>nn</code> number is the security level of the interface that was set with the nameif command.</p>	4.3(2)

Related Documentation

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

- *Configuration Guide for the PIX Firewall Version 4.3*. You can view this document online at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43cfg/index.htm
- *Quick Installation Guide for the PIX Firewall Version 4.3*. You can view this document online at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43qig.htm
- *Regulatory Compliance and Safety Information for the PIX Firewall Version 4.3*. You can view this document online at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pixrcs43.htm
- *System Log Messages for the PIX Firewall Version 4.3*. You can view this document online at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/syslog/index.htm

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

Cisco Connection Online

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

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

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

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://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. For additional information, contact 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. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or 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, the CCIE logo, CCNA, CCNP, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, the Cisco Technologies logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetRanger Director, NetRanger Sensor, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratm, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, 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 BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, LightSwitch, MICA, Phase/IP, Registrar, StrataSphere, StrataView Plus, and SwitchProbe 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. (9901R)

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