



Release Notes for Cisco Secure PIX Firewall Version 5.1(1)

March 2000

The Cisco Secure PIX Firewall provides secure networking and NAT (Network Address Translation).

Contents

This document contains the following sections:

- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

System Requirements

Version 5.1 requires the following:

1. If you are upgrading from a previous version on a PIX Firewall with a diskette drive, you must create a Boothelper diskette and download the version 5.1 image from TFTP. Attempting to put the image directly on diskette causes the rawrite program to fail.
2. PIX Firewall *must* have at least 32 MB of RAM memory or the PIX Firewall unit will not boot. Use the **show version** command to verify how much RAM is in your PIX Firewall unit.



3. PIX Firewall requires at least 2 MB of Flash memory although support is provided for both 2 MB and 16 MB Flash memory cards. The maximum configuration size with the 16 MB Flash memory card is 1 MB. A PIX Firewall unit containing a 16 MB Flash memory card cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2) without causing irreparable harm to the Flash memory card.
4. If you use mode configuration with the PIX Firewall, any routers on the IPSec connection must run Cisco IOS Release 12.0.6T or later.
5. If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must have a new activation key. Before getting a new activation key, write down your old key in case you want to downgrade back to version 4. You can have a new activation key sent to you by completing the form at the following site:
<http://www.cisco.com/kobayashi/sw-center/internet/pix-56bit.shtml>
6. If you are using PFSS (PIX Firewall Syslog Server), we recommend that you install Windows NT Service Pack 6 to fix Y2K conflicts in Windows NT.
7. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to “Installation Notes” for new installation requirements.

PIX Firewall Manager Interoperability

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/pfm432d.htm

The PIX Firewall Manager (PFM) lets you manage PIX Firewall units; however, it does not let you configure any PIX Firewall features added after version 4.3(2).

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

Cisco Security Manager Interoperability

Cisco Security Manager (CSM), version 1.1, provides policy-based management support for PIX Firewall units running version 4.2(4), 4.2(5), 4.4(1), 4.4(2), and 4.4(3) software images.

Refer to Appendix A, “Using Unsupported PIX Firewall Commands,” in the *Cisco Security Manager Tutorial* for information about the PIX Firewall commands the CSM supports. You can view the CCO version of the *Cisco Security Manager Tutorial* at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/ismg/security/tutorial/index.htm>

New and Changed Information

Version 5.1(1) consists of bug fixes and new features.

Version 5.1(1) Features

The sections that follow describe each new feature.

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm

16 MB Flash Memory Card Support

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

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

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

AAA Improvement

The **aaa** command now supports selection by service. See “aaa Command” for more information.

Boothelper

If you are using a PIX Firewall unit with a diskette drive, the PIX Firewall image no longer fits on a diskette. You need to download the Boothelper file, bh511.bin, from Cisco Connection Online (CCO) to let you download the PIX Firewall image with TFTP. Boothelper only works with version 5.1 or later images and cannot pass the image over a Gigabit Ethernet interface. See “Installation Notes” for more information. You can view Boothelper information online in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm

Firewall MIB Support

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/advanced.htm

FragGuard and Virtual Re-assembly

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

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



Note

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

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

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

- IP packets fragmented into more than 12 elements cannot pass through the PIX Firewall. When detected, the following console message appears:

```
fh_insertb: too many fragments(12) in set
```

FTP and URL Logging

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

Gigabit Ethernet

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

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

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

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

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

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

Installation Enhancement

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm

IPSec Enhancements

The following IPSec improvements are new to this release:

- IPSec tunnel termination—you can now differentiate UDP IPSec traffic from TCP traffic using the port parameter to the **access-list** command. The use of port ranges can dramatically increase the number of IPSec tunnels. For instance if a port range of 5000-65535 is specified for a highly dynamic protocol, a possible 60,535 tunnels can be created.
- Multiple interface termination—IPSec now lets you terminate an IPSec tunnel on any and all active interfaces.
- Client termination—you can now enable the PIX Firewall to terminate an IPSec tunnel destined for itself.

The IPSec command interface has the following changes:

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

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/commands.htm

Java and ActiveX Filtering Improvements

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



Note

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

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

PPTP Support

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

RAS V2 Support

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

RIP V2 Support

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

Routing Extensions

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

RTSP Support

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

Separate SNMP and Syslog Message Levels

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

System Software Downloads

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

Xauth Support

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

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

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



Note

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

XDMCP Support

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

New Commands

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

copy tftp flash Command

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

The **copy tftp flash** command requires that routing be configured. In certain cases such as with IPsec configuration, a ping from the PIX Firewall to the TFTP server may be successful even without complete routing information. However, the success of the ping command does not guarantee that the **copy tftp flash** command will be successful.

vpdn Command

The **vpdn** command implements the PPTP feature.

Changes to Existing Commands

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/index.htm

aaa Command

The **aaa include** and **exclude** options let you select which services are permitted or denied from authentication, authorization, and accounting.



Note

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

access-list Command

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

The previous restriction that prohibited the use of the **access-list** command with the **conduit** or **outbound** commands has been lifted.

auth-prompt Command

The maximum length of the prompt string is 235 characters.

conduit Command

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

clear interface Command

The **clear interface** command clears all interface statistics except the number of input bytes. This command no longer shuts down all system interfaces. The **clear interface** command works with all interface types except gigabit Ethernet.

crypto map client authentication Command

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

debug Command

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

established Command

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

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

fixup rtsp Command

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

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

interface Command

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

logging Command

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

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

nat Command

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

no failover Command

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

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

rip Command

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

route Command

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

- The routing table has been improved to let you specify the IP address of a PIX Firewall interface in the **route** command. If the **route** command statement uses the IP address from one of the PIX Firewall unit's interfaces as the gateway IP address, PIX Firewall will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address.
- PIX Firewall also does not accept duplicate routes with different metrics for the same gateway.
- In version 5.1(1), the CONNECT route entry is supported. (This identifier appears when you use the **show route** command.) The CONNECT identifier is assigned to an interface's local network and the interface IP address, which is in the IP local subnet. PIX Firewall will use ARP for the destination address. The CONNECT identifier cannot be removed, but changes when you change the IP address on the interface.

- You can now enter duplicate **route** command statements with different gateways and metrics.
- You can now enter static **route** command statements with virtual subnets; for example:

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

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

show failover Command

In the output of the **show failover** command, the heading “Standby Logical Update Statistics” changed to “Stateful Failover Logical Update Statistics.”

show interface Command

The **show interface** command has been enhanced to include eight new status counters.

sysopt connection permit-pptp Command

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

sysopt ipsec pl-compatible Command

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

Installation Notes

1. Refer to either the *Installation Guide for the Cisco Secure PIX Firewall Version 5.1* or Chapter 2, “Configuring PIX Firewall” in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.1* for information on the new Boothelper diskette installation feature and the new configuration version message. Boothelper only works with version 5.1 images. In addition, only specify Boothelper commands in lowercase. You can view this information online at the following site:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/config.htm
2. Do not attempt to load version 5.1 on a PIX Firewall unit containing less than 32 MB of memory. While the PIX Firewall may appear to permit this configuration, upon reboot, the PIX Firewall unit will continuously fail. You can stop this by immediately inserting a previous version diskette into the PIX Firewall unit and then pressing the reboot switch. This note only applies to PIX Firewall units with a diskette drive, not to the PIX 515.
3. A PIX Firewall unit containing a 16 MB Flash memory card cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2) without causing irreparable harm to the Flash memory card. [CSCdp38206]
4. Version 5.1 on a PIX 515 cannot be downgraded to pre-version 4.4(1) images. [CSCdp21017]

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

Limitations and Restrictions

The following limitations and restrictions apply to version 5.1(1):

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

Important Notes

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

Assertions

Previously, assertions in the code caused an error message to display at the PIX Firewall. In version 5.1(1), assertions now force the PIX Firewall to fail and display a trace output.

auth-prompt Command

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

Default Configuration

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/config/intro.htm

DNS Root Name Server Access

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

Failover

The following notes apply to the failover feature:

- Failover no longer stops traffic when the 1550-byte pool exhausts. If this pool exhausts and cannot be reallocated on the Standby unit, the Standby unit will now reboot without affecting the Active unit. [CSCdp85718]
- The **failover timeout** command is only used with a non-supported PIX Firewall Engineering feature. To avoid confusion, the **failover timeout** command is not documented, but does appear in the default configuration. You can ignore this command.

Failure Message

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

FTP Change

PIX Firewall now restricts FTP commands so that only FTP servers can submit a 227 reply and only FTP clients can submit a PORT command. Furthermore, the only PORT command permitted can only be one port number lower than the FTP control channel. This change removes the wildcard port for connections created from the PORT command. PIX Firewall now also enforces that the first SYN packet from the dynamic back channel must be from the expected side. [CSCdp86352]

Gigabit Interface Restrictions

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

- The **1000auto** option to the **interface** command does not get written to the configuration. When the PIX Firewall reboots, the gigabit interface is then automatically shut down. As soon as the PIX Firewall reboots, re-enter the **interface** command to restart the interface. [CSCdp64321]
- The Boothelper TFTP image cannot be sent to the PIX Firewall over a gigabit interface. Ensure that the PIX Firewall unit has at least one 10/100 Ethernet interface to convey the image to the PIX Firewall. [CSCdp92050]
- The **clear interface** command clears all interface statistics except the number of input bytes. This command no longer shuts down all system interfaces. The **clear interface** command works with all interface types except gigabit Ethernet. [CSCdp88443]

IPSec Notes

The following sections provide useful information about IPSec.

Certification Authority (CA) Usage

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

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

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

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

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

Cisco Secure VPN Client

Only use version 5.1 of the PIX Firewall with version 1.1 or later of the Cisco Secure VPN Client.

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

crypto map Command

The **crypto map map_name interface if_name** command causes any currently running SAs (security associations) to be deleted.

ISAKMP Notes

- If you are using RSA signatures as your authentication method in your IKE policies, Cisco recommends you set each participating peer's identity to hostname. Otherwise, the ISAKMP security association to be established during phase 1 of IKE may fail. [CSCdp93890]

- If an ISAKMP SA expires, the IPsec tunnel for the expired ISAKMP SA continues for the remaining time. If a PIX Firewall peer reboots before the ISAKMP SA expires, the keepalive fails to note that the other peer is not there and packets are silently dropped until the SA expires. [CSCdp86785]
- All **isakmp** command policies now appear in the configuration. Previously, default values were not listed. You can view this information with the **show isakmp policy** command.

Mode Configuration

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

SA Lifetimes

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

name Command

The **name** command does not support dashes in the name you specify. [CSCdp58692]

NAT

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

PFSS

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

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

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

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

show failover Command

The Stateful Failover Logical Update Statistics output that displays when you use the **show failover** command only applies to Stateful Failover, not to the basic failover functionality. The statistics table only displays if a failover link has been configured.

SNMP

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

SQL*Net

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

Syslog

The following syslog changes occurred in version 5.1:

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

- The following messages were deleted: %PIX-2-106008, %PIX-2-106009, %PIX-2-106017, %PIX-2-110003, %PIX-3-202002, %PIX-3-202003, %PIX-3-202004, %PIX-3-209001, %PIX-3-209002, and %PIX-3-304006.

**Note**

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

```
[CSCdp87564]
```

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

URL Logging

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

Caveats

Open Caveats

Table 1 lists open caveats:

Table 1 Open Caveats

DDTS Number	Description
CSCdp93890	When configuring ISAKMP for certificate-based authentication, it is important to match the ISAKMP identity type with the certificate type. See “ISAKMP Notes” for more information.
CSCdp92050	The Boothelper TFTP image cannot be sent to the PIX Firewall over a gigabit interface. Ensure that the PIX Firewall unit has at least one 10/100 Ethernet interface to convey the image to the PIX Firewall.
CSCdp88761	When two policies are configured on the Cisco Secure VPN Client for different PIX Firewall interfaces, after the PIX Firewall unit initiates a rekey, the Client loses the ability to differentiate between the interfaces. This condition causes the message, "Cannot match Policy Entry for received IDs" to display and can cause a loss of connections. Once dropped, the tunnels cannot be re-established.
CSCdp87564	Some syslog messages contain linefeeds. Because the Solaris version of syslog, known as syslogd, only stores the first line sent, logging information on these messages is incomplete. One such message, appears truncated on a Solaris system as follows: %PIX-6-602301: sa created,
CSCdp86785	If an ISAKMP SA expires, the IPsec tunnel for the expired ISAKMP SA continues for the remaining time. If a PIX Firewall peer reboots before the ISAKMP SA expires, the keepalive fails to note that the other peer is not there and packets are silently dropped until the SA expires.

Table 1 Open Caveats (continued)

CSCdp88443	The clear interface command clears all interface statistics except the number of input bytes. This command no longer shuts down all system interfaces. The clear interface command works with all interface types except gigabit Ethernet.
CSCdp85254	Web browsers such as Internet Explorer or Netscape Navigator only display the first 23 characters of the string you indicate in the auth-prompt command. This limitation is imposed by the browser and is not a PIX Firewall fault.
CSCdp67251	The fixup protocol sqlnet command only works with Oracle, not with NetWare SQLNET.
CSCdp64331	A gigabit interface must not be shut down for more than 5 minutes. After that, the PIX Firewall unit must be rebooted to regain access to the interface.
CSCdp64321	The 1000auto option to the interface command does not get written to the configuration. When the PIX Firewall reboots, the gigabit interface is then automatically shut down. As soon as the PIX Firewall reboots, re-enter the interface command to restart the interface.
CSCdp58692	The name command does not support dashes in the name you specify.
CSCdp48115	A DNS server behind the PIX Firewall cannot use PAT; however, adding a static command statement can be used as a workaround.
CSCdp42625	When using the VeriSign CA, always use the crloptional parameter to the ca configure command.
CSCdp38206	A PIX Firewall unit containing a 16 MB Flash memory card cannot be downgraded to version 4.4(1), 4.4(2), 5.0(1), or 5.0(2) without causing irreparable harm to the Flash memory card.
CSCdm59768	If you enter the show crypto ipsec sa command and the screen display is stopped with the More prompt, and if the SA lifetime expires while the screen display is stopped, subsequent display information may refer to a stale SA and the SA lifetime values that display will be invalid.

Resolved Caveats

Table 2 lists resolved caveats:

Table 2 Resolved Caveats

DDTS Number	Description
CSCdp88122	An SQL*Net version 1 or truncated packet no longer crashes PIX Firewall.
CSCdp86352	PIX Firewall now prevents FTP clients from initiating FTP server commands.
CSCdp85718	Failover no longer stops traffic when the 1550-byte pool exhausts. If this pool exhausts and cannot be reallocated on the Standby unit, it will now reboot without affecting the Active unit.
CSCdp78256	A 1550-byte memory block leak no longer occurs if an incoming SNMP request is invalid.
CSCdp74795	The source IP address in SNMP traps is no longer reversed; for example, 10.1.1.1 no longer displays as 1.1.1.10.

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdp65228	Syslog message %PIX-2-108002 now lists the IP address in the correct order. Previously an IP address such as 10.1.1.1 was listed in the message as 1.1.1.10.
CSCdp60485	If a new peer successfully negotiates an IPSec tunnel to protect the same set of identities as an old tunnel, PIX Firewall switches to the new peer and maintains the old tunnel for 30 seconds to let traffic subside.
CSCdp59021	PIX Firewall no longer continuously reboots after downgrading to the version 4.4(3) image.
CSCdp58991	AAA accounting is no longer unidirectional. Now secondary connection(s) are assigned the same direction as the control connection. This lets uauth associate and dynamically preallocate the connection(s) from the same control connection with the same identity. Accounting will then trigger for the matched identity.
CSCdp57339	The MTU of an interface no longer is set to 0. Previously, entering the write erase command followed by rebooting, and then not explicitly setting the MTU, caused IPSec to initialize the tunnel with an MTU of 0.
CSCdp56795	Syslog message %PIX-2-1006002 only displays the protocol as a number instead of as a name. This is also fixed in all future PIX Firewall versions. The text for this message is now one of the following: <ul style="list-style-type: none"> • 1 Connection denied by outbound list <i>list_ID</i> src <i>laddr/lport</i> dest <i>faddr/fport</i> • 6 Connection denied by outbound list <i>list_ID</i> src <i>laddr/lport</i> dest <i>faddr/fport</i> • 17 Connection denied by outbound list <i>list_ID</i> src <i>laddr/lport</i> dest <i>faddr/fport</i> where 1 means ICMP, 6 means TCP, and 17 means UDP. Previously, PIX Firewall listed the protocol by name in some messages and by number in others. The messages now consistently use the protocol number.
CSCdp56150	The Private Link PL/2 card is now recognized correctly. The use of this card improves IPSec processing speed.
CSCdp55033	When a packet is received with a bad checksum, PIX Firewall now discards the packet without closing the TCP connection. Previously, if after a connection was closed, a subsequent packet arrived, PIX Firewall caused a reset that stopped traffic on the connection.
CSCdp53852	The fixup smtp command now correctly translates multi-line banners.
CSCdp52877	The debug icmp trace command no longer also enables the debug fixup_smtp command.
CSCdp52185	Version 5.1 provides the access-list command port selector for IPSec.
CSCdp51830	Access lists now handle ICMP echo-request and echo-reply correctly.
CSCdp49186	Limited broadcasts sent to 255.255.255.255 now work correctly with the PIX Firewall. While the broadcast is not forwarded through the PIX Firewall, this feature lets RIP updates work correctly.
CSCdp45416	PFSS (PIX Firewall Syslog Server) now renames log files using the last modification date as the file type. For example, if PFSS needs to create a monday.log file and the filename already exists, PFSS checks the last modification date for the original file and finds, for example, that it was last modified on January 24, 2000. PFSS then renames the original file monday.012400 and moves it to the backup directory. Then PFSS creates monday.log for the current log data.

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdp44875	PIX Firewall no longer gets into an unrecoverable crash when reloaded after using the clear flashfs command without loading a new image.
CSCdp41051	The terminal no monitor command now works correctly.
CSCdp38828	The PIX Firewall failure message was changed from “Watchdog timer failure - ARF!” to “Watchdog timeout!”.
CSCdp33907	PIX Firewall uses port 1521 for SQL*Net even though this value does not agree with the IANA port assignments.
CSCdp23931	Adds syslog message %PIX-2-106020: Deny IP teardrop fragment (size = <i>num</i> , offset = <i>num</i>) from <i>IP_addr</i> to <i>IP_addr</i> . This message occurs when the PIX Firewall discards an IP packet with a teardrop signature with either a small offset or fragment overlapping. You should treat this event as a hostile attempt to circumvent the firewall or an intrusion detection system.
CSCdp05727	Allows an interface to be the gateway for the route command. The PIX Firewall now uses ARP to determine the real destination address if the next hop address is the outgoing interface address.
CSCdp00115	All isakmp command policies now appear in the configuration. See “ISAKMP Notes” for more information.
CSCdm79900	Request for separate levels of debug for syslog and SNMP logging. See “Separate SNMP and Syslog Message Levels” for more information.
CSCdm74155	PIX Firewall now supports the copy tftp flash command. See “copy tftp flash Command” for more information.
CSCdm62488	DNS packets are no longer altered by the alias command in both directions. Use the version 5.0 sysopt noaliasdns outboundinbound command to disable DNS Address record fixups from interaction with the alias command. Using a separate command for inbound and another for outbound disables DNS A record fixups.
CSCdm23996	PIX Firewall now has RIP version 2 support to ensure that incorrect routes are not learned from unauthorized neighbors.
CSCdk77815	As of PIX Firewall version 5.0, the show conduit and show access-list commands list a hit count after each ACL (Access Control List) element that indicates the number of times an element has been matched during the access-list or conduit command statement search.
CSCdk76181	The PIX Firewall now has a nat (interface) 0 access-list acl_name that provides no nat capability for both inbound and outbound connections. See “nat Command” for more information.
CSCdk22364	The aaa command statement now accepts a protocol and port specification for what used to be the except option. The except option has been replaced by the include and exclude options. See “aaa Command” for more information.
CSCdk06669	Support for new Cisco Firewall MIB.
CSCdj95449	Support for enhancements to the established command.

Related Documentation

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

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

Cisco provides PIX Firewall technical tips at the following site:

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

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Documentation CD-ROM

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

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Documentation Feedback

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

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate and value 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, Browse with Me, 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 Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, WaRP, Wavelength Router, Wavelength Router Protocol, WebViewer, 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, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates 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. (9912R)

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