



# Release Notes for the Cisco PIX Firewall Version 5.2(6)

---

July 2001

## Contents

This document includes the following sections:

- Introduction
- System Requirements
- New and Changed Information
- Command Changes
- Syslog Message Changes
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information



# Introduction

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

## System Requirements

The sections that follow list the system requirements for operating a PIX Firewall unit with version 5.2 software.

## Memory Requirements



### Note

All PIX Firewall units *must* have at least 32 MB of RAM memory or the PIX Firewall unit will not boot. In addition, all units except the PIX 506 must have 16 MB of Flash memory to boot. The PIX 506 has 8 MB of memory, which works correctly with version 5.2.

The following table lists Flash memory requirements for this release:

PIX Firewall Model	Flash Memory Required in 5.2	Flash Memory Sold with Unit
PIX 506	8 MB	8 MB (not upgradeable)
PIX 510 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX 515	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 525	16 MB	16 MB
PIX 10000 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX Firewall Classic (discontinued)	16 MB	512 KB or 2 MB (must be upgraded to 16 MB)

## Software Requirements

The following is required for version 5.2:

1. The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, you need to download the Boothelper file, bh521.bin, from cisco.com to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must have an activation (license) key that enables Data Encryption Standard (DES) or the more secure 3DES, which PDM requires for support of the Secure Socket Layer (SSL) protocol.

To obtain a DES (56-bit) license key for the PIX Firewall, use the IPSec 56-bit Customer Registration form. Accessing this form requires prior registration on Cisco.com at <http://www.cisco.com/register>. However, access to this form does not require a purchase or service contract. You can register as a guest and then proceed to fill out the form. The form is available at the following website:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>

You must purchase a 3DES (168-bit) license key, or have a service contract, to obtain a 3DES license key. If you have already purchased a 3DES upgrade, and you have your Cisco PIX Firewall 3DES upgrade document with the entitlement number printed on it, you can register your license key for use on your PIX Firewall with the License Registration form. Accessing this form also requires prior registration on Cisco.com at <http://www.cisco.com/register>. The License Registration form is available at the following website:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=301>

You must also purchase or have a service contract to download PIX Firewall software.

3. If you are using PFSS (PIX Firewall Syslog Server), Cisco recommends you install Windows NT Service Pack 6 to fix year 2000 conflicts in Windows NT.
4. 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.

## Cisco IOS Software Interoperability

The Cisco Secure PIX Firewall supports IOS Release 12.0(6)T or later.

## Cisco Secure Policy Manager Interoperability

Cisco Secure Policy Manager (Cisco Secure PM), version 2.1, provides policy-based management support for PIX Firewall units running version 4.2, 4.4, and 5.1 software images. Cisco Secure PM version 2.2 supports PIX Firewall version 5.2.

Refer to the documentation set for Cisco Secure PM at the following website:

[http://www.cisco.com/en/US/products/sw/secursw/ps2133/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/secursw/ps2133/prod_technical_documentation.html)

## Cisco Secure VPN Client Interoperability

PIX Firewall version 5.2 requires Cisco Secure VPN Client version 1.1. The Cisco Secure VPN Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco Secure VPN Client is not supported for use with Windows 2000.

## Cisco VPN 3000 Concentrator and Client Interoperability

PIX Firewall version 5.2 requires Cisco VPN 3000 Client version 2.5 or later and Cisco VPN 3000 Concentrator version 2.5.2 or later. The Cisco VPN 3000 Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco VPN 3000 Client is not supported for use with Windows 2000.

## PIX Firewall Manager Interoperability

You can use PIX Firewall version 5.2 with the PIX Firewall Manager version 4.3(2)h. Refer to the *PIX Firewall Manager Release Notes, Version 4.3(2)h* for more information. You can view this document online at the following website:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod\\_release\\_note09186a00800f27db.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note09186a00800f27db.html)

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

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

## Determining the Software Version

Use the **show version** command to verify the software version of your PIX Firewall unit.

## Upgrading to a New Software Release

If you have a cisco.com login, you can obtain software from the following site:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>

To register for a cisco.com login, go to the following site:

<http://tools.cisco.com/RPF/register/register.do>

## New and Changed Information

### New Information in Release 5.2(5)

Version 5.2(5) fixes caveat CSCds89077. The PIX Firewall now opens third party H.245 connections by inspecting the H.225 signaling messages to look for the specified H.245 address. The PIX Firewall then uses that address to open the H.245 connection.

### New Information in Release 5.2(4)

Version 5.2(4) fixes caveat CSCds76768. If you configure the onboard Ethernet interfaces (ethernet0 and ethernet1) on a PIX 525 with a serial number of 44480380055 through 44480480044 to full-duplex, interface errors and throughput reductions may occur. If you configure the interfaces to half-duplex or to auto-sense, the speed and duplex function normally without error. Use the new **EEPROM** command to fix the problem. The two variants of the **EEPROM** command are the **show EEPROM** command and **EEPROM update** command.

The **show EEPROM** command displays the current EEPROM setting, and the **EEPROM update** command modifies the settings if necessary. If the **EEPROM** command does update the EEPROM settings, we recommend you reboot the PIX Firewall.

**Note**


---

The **EEPROM** command only works on the PIX 525.

---

The **EEPROM** command verifies the EEPROM register settings and updates them if they are not set to the recommended values. The **EEPROM** command does not update the settings if they are correct and does not recommend a reboot unless the settings are changed.

The **EEPROM update** command checks the contents of EEPROM registers 6 and 10 to ensure they contain the hexadecimal values 0x4701 and 0x40c0, respectively. If these registers contain different values, then all EEPROM register settings except the MAC address registers, which were not affected by the problem causing CSCds76768, are reset to the correct values.

Each register is 16 bits. The correct register values are as follows:

Register	Name	Value
Register 0 to 2	MAC address	Differs on each system
Register 3	Compatibility Bits	0x3
Register 5	Controller and connector type	0x201
Register 6	Onboard PHY type	0x4701
Register 10	Onboard Prom ID	0x40C0
Register 12	Vendor ID, where 8086 is Intel	0x8086

The syntax of the **EEPROM** command is as follows:

**show eeprom**

Displays the current EEPROM register settings on the PIX 525.

**update eeprom**

Updates the EEPROM register settings if they do not match the recommended values.

The **show eeprom** command will display the current EEPROM register settings:

```
PIX525# show eeprom
eeprom settings for ifc0:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x65f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4702
  reg10: 0x40c0
  reg12: 0x8086
eeprom settings for ifc1:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x66f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4702
  reg10: 0x40c0
  reg12: 0x8086reg12: 0x8086
```

If the command is run on a unit that is not a PIX 525, the following will be seen:

```
PIX515# show eeprom
This unit is not a PIX-525.
Type help or '?' for a list of available commands.
```

If the update needs to be run on the PIX 525, the **eeprom update** command returns the following:

```
PIX525# eeprom update
eeprom settings on ifc0 are being reset to defaults:
reg0: 0x5000
reg1: 0xfe54
reg2: 0x65f6
reg3: 0x3
reg5: 0x201
reg6: 0x4701
reg10: 0x40c0
reg12: 0x8086
eeprom settings on ifc1 are being reset to defaults:
reg0: 0x5000
reg1: 0xfe54
reg2: 0x66f6
reg3: 0x3
reg5: 0x201
reg6: 0x4701
reg10: 0x40c0
reg12: 0x8086
*** WARNING! *** WARNING! *** WARNING! *** WARNING! ***
The system should be restarted as soon as possible.
*** WARNING! *** WARNING! *** WARNING! *** WARNING! ***
```

If the update has been run successfully, the **eeprom** command output will look like this:

```
PIX525# eeprom update
eeprom settings on ifc0 are already up to date:
reg0: 0x5000
reg1: 0xfe54
reg2: 0x65f6
reg3: 0x3
reg5: 0x201
reg6: 0x4701
reg10: 0x40c0
reg12: 0x808
eeprom settings on ifc1 are already up to date:
reg0: 0x5000
reg1: 0xfe54
reg2: 0x66f6
reg3: 0x3
reg5: 0x201
reg6: 0x4701
reg10: 0x40c0
reg12: 0x80866
```

## New Information in Release 5.2(3)

Version 5.2(3) fixes caveat CSCds38708 only. If your configuration includes the **fixup protocol smtp port\_number** command and either a **conduit** or **access-list** command statement permitting access to SMTP, you should install version 5.2(3) immediately to counter a vulnerability in the Mail Guard feature.

## New Information in Release 5.2(2)

Version 5.2(2) fixes caveats CSCds30699 and CSCdr91002 only.

## New Hardware Features in Release 5.2(1)

### PIX 525

The new PIX 525 model has the fastest performance and highest capacity of any of the PIX Firewall series.

The PIX 525 provides the following features:

Features	PIX 525—R	PIX 525—UR
Failover	No	Yes
RAM	128 MB	256 MB
Processor	600 MHz	600 MHz
Flash memory	16 MB	16 MB
Fixed 10/100 Mbps interfaces	2	2
PCI slots	3	3
Maximum interfaces	6	8
Supported Interfaces	Fast Ethernet	Fast Ethernet and Gigabit Ethernet
Power Supplies	Single AC power supply	Single AC power supply



#### Note

FDDI interfaces are not supported for use on the PIX 525 in version 5.2.

### Failover Serial Connection

The failover serial connection has been increased from 9600 baud to 117,760 baud (115K). The maximum supported length for the failover serial cable is 6 feet.



#### Note

Use the failover cable that is shipped with the PIX Firewall unit. If you use a replacement cable, it must have the same specifications as the supplied cable (length, type, and pinouts).

### Inside and Outside Port Restriction Change

With the 5.2 software release, there are no longer restrictions on having to use specific Ethernet ports as the inside and outside network ports. Any port, whether fixed or a PCI expansion port, and any interface type, FDDI, Token Ring, Fast Ethernet, or Gigabit Ethernet, can be assigned to be the inside or outside network port.

Use the following notes, restrictions, and instructions for configuring inside and outside network ports:

- Any change to an interface can potentially affect many of the PIX Firewall commands. If you change an interface IP address or the security level, use the **clear xlate** command to purge connection data.
- For the PIX 515 and PIX 525, you do not have to use ETHERNET 0 for the outside network port and ETHERNET 1 for the inside network port. Any of the fixed or expansion ports can be configured to be the inside or outside network ports.
- The outside network port must still be set to security level 0 (zero) and the inside network port must still be set to security level 100.
- This revision does not change the rules for port numbering. Refer to the *Cisco PIX Firewall Installation Guide, Version 5.2* for a description of how ports are numbered for the different PIX Firewall models.
- For backward compatibility, the default configuration will still show Ethernet port 0 as the outside port and Ethernet port 1 as the inside port. Use the **nameif** command to identify which port (using unique port names) that you want to configure as the inside and outside ports. The following is syntax of the **nameif** command:

```
clear|no|show nameif hardware_if if_name security_level
```

The following is an example of the default interface name information using the **show nameif** command:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 PIX/intf2 security10
nameif ethernet3 PIX/intf3 security15
nameif token-ring0 PIX/intf4 security20
nameif gb-ethernet0 PIX/intf5 security25
```

## New Software Features in Release 5.2

The following features are new in version 5.2. Refer to the *Cisco PIX Firewall Configuration Guide, Version 5.2* for information about each software feature. IPSec features are described in the new *Cisco PIX Firewall IPSec User Guide, Version 5.2*.

### AAA access-list Support

The new **match access\_list\_name** option was added to the **aaa** command.

### Broadcast Addresses

PIX Firewall no longer uses network addresses or broadcast addresses in **static** and **global** command statements when creating NAT xlate translations. Broadcast addresses are those addresses with the bit pattern of all ones, when the network mask is applied. Network addresses are those addresses with the bit pattern of all zeros, when the network mask is applied.

For example:

```
global 1 10.1.0.0-10.1.255.255 netmask 255.255.255.0
```

With this command, the network addresses 10.1.0.0, 10.1.1.0, 10.1.2.0, and so forth through 10.1.255.0, are excluded. In addition, the broadcast addresses 10.1.0.255, 10.1.1.255, 10.1.2.255, and so forth through 10.1.255.255, are excluded.

## Certification Authority Servers—Baltimore and Microsoft

In addition to supporting the Entrust and VeriSign certification authority (CA) servers, the PIX Firewall now also supports CA servers developed by Baltimore Technologies and Microsoft.

## Cisco VPN 3000 Client (Formerly the Altiga VPN Client)

Remote access VPN users employing the Cisco VPN 3000 Client, version 2.5, can now securely access their private enterprise network through the PIX Firewall, version 5.2.



**Note**

Be sure to configure the IKE Mode Config prior to configuring support for the Cisco VPN 3000 Client. In configuring IKE Mode Config, specify that the VPN Client initiates the IKE Mode Config.



**Note**

The Cisco VPN 3000 Client does not support Windows 2000 use.

## DHCP Server and Client Support

Support for Dynamic Host Configuration Protocol (DHCP) server and DHCP client within the PIX Firewall is now available with the release of version 5.2.

## Failover Polling Time

The new **failover poll seconds** command lets you determine how long failover waits before sending special failover “hello” packets between the Primary and Standby units over all network interfaces and the failover cable. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds. Set to a lower value for Stateful Failover. With a faster poll time, PIX Firewall can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.

## FTP—Prevent Embedded Commands

The **strict** option to the **fixup protocol ftp** command prevents web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The **strict** option only lets an FTP server generate the 227 command and only lets an FTP client generate the PORT command. The 227 and PORT commands are checked to ensure they do not appear in an error string.

## H.323 V2

H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. H.323 supports H.323 VoIP gateways and VoIP gatekeepers. H.323 version 2 adds the following functionality to the PIX Firewall:

- Fast Connect or Fast Start Procedure for faster call setup
- H.245 tunneling for resource conservation, call synchronization, and reduced set up time

## ICMP Access Lists

Enable or disable pinging to an interface. With pinging disabled, the PIX Firewall cannot be detected on the network. The new **icmp** command implements this feature. This feature is also referred to as configurable proxy pinging.

## IP Fragmentation Syslog Messages

Syslog messages PIX-4-209003, PIX-4-209004, and PIX-4-209005 have been added to disclose IP fragmentation attacks.

## IDS Syslog Messages

Cisco Intrusion Detection System (Cisco IDS) is an IP-only feature that provides some level of flexibility for the user to customize the amount of traffic that needs to be audited and logged.

## PAT Enhancements

The following PAT enhancements were added:

- To specify PAT using the IP address at the interface, specify the **interface** keyword.

**global** [(*int\_name*)] *nat\_id* *address* | **interface**

The following example enables PAT using the IP address at the outside interface in global configuration mode:

```
ip address outside 192.150.49.1
nat (inside) 1 0 0
global (outside) 1 interface
```

The interface IP address used for PAT is the address associated with the interface when the xlate (translation slot) is created. This is important for configuring DHCP, allowing for the DHCP retrieved address to be used for PAT.

When PAT is enabled on an interface, there should be no loss of TCP, UDP, and ICMP services. These services allow for termination at the PIX Firewall unit's outside interface.

- To track usage among different subnets, you can specify multiple PATs using the following supported configurations:

### Mapping Different Internal Subnets to Different PAT Addresses

The following example maps hosts on the internal network 10.1.0.0/16 to global address 192.168.1.1 and hosts on the internal network 10.1.1.0/16 to global address 209.165.200.225 in global configuration mode.

```
nat (inside) 1 10.1.0.0 255.255.255.0
nat (inside) 2 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.1 netmask 255.255.255.0
global (outside) 2 209.165.200.225 netmask 255.255.255.224
```

### Backing Up PAT Addresses

The following example configures two port addresses for setting up PAT on hosts from the internal network 10.1.0.0/16 in global configuration mode.

```
nat (inside) 1 10.1.0.0 255.255.0.0
global (outside) 1 209.165.200.225 netmask 255.255.255.224
global (outside) 1 192.168.1.1 netmask 255.255.255.0
```

With this configuration, address 192.168.1.1 will only be used when the port pool from address 209.165.200.225 is at maximum capacity.

## ping Command Enhancement

The PIX Firewall **ping** command no longer requires an interface name. If an interface name is not specified, PIX Firewall checks the routing table to find the address you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

## Radius Authorization

PIX Firewall now allows a RADIUS server to send user group attributes to the PIX Firewall in the RADIUS authentication response message. Authorization is granted with the **access-list** command statement.

## SIP Support

Session initiation protocol (SIP), as defined by the Internet Engineering Task Force (IETF), enables call handling sessions—particularly two-party audio conferences, or “calls.” SIP works with Session Description Protocol (SDP) for call signaling. SDP specifies the ports for the media stream. Using SIP, the PIX Firewall can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- *SIP: session initiation protocol*, RFC 2543
- *SDP: Session Description Protocol*, RFC 2327

## SSH

SSH (Secure Shell) is an application running on top of a reliable transport layer, such as TCP/IP that provides strong authentication and encryption capabilities. PIX Firewall supports the SSH remote shell functionality as provided in SSH version 1. SSH version 1 also works with Cisco IOS software devices. Up to five SSH clients are allowed simultaneous access to the PIX Firewall console.



### Note

You must generate an RSA key-pair for the PIX Firewall before clients can connect to the PIX Firewall console. To use SSH, your PIX Firewall must have a DES or 3DES activation key.

**Note**

---

SSH permits up to 100 characters in a username and up to 50 characters in a password.

---

**Note**

---

SSH and failover are not supported for use together in version 5.2.

---

## Obtaining an SSH Client

The following websites let you download an SSH v1.x client. Because SSH version 1.x and version 2 are entirely different protocols and not compatible, be sure you download a client that supports SSH v1.x.

- Windows 3.1, Windows CE, Windows 95, and Windows NT 4.0—first download the free Tera Term Pro SSH v1.x client from the following website:

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

Then add the SSH extension to Tera Term Pro, which is available at the following website:

<http://www.zip.com.au/~roca/ttssh.html>

- Linux, Solaris, OpenBSD, AIX, IRIX, HP/UX, FreeBSD, and NetBSD—download the SSH v1.x client from the following website:

<http://www.openssh.com>

- Macintosh (users outside the United States only)—download the Nifty Telnet 1.1 SSH client from the following website:

<http://www.lysator.liu.se/~jonasw/freeware/niftyssh/>

## TCP Intercept

The TCP Intercept feature improves the embryonic connection handling of the PIX Firewall. When the number of embryonic connections exceed the configured threshold, PIX Firewall intercepts and proxies new connections. Previous to version 5.2, PIX Firewall did not allow new connections after the embryonic connection threshold was exceeded.

This feature requires no change to the PIX Firewall command set, only that the embryonic connection limit on the **static** command now has a new behavior.

## Unicast Reverse Path Forwarding

Unicast Reverse Path Forwarding requires that a source IP address is reachable via the receiving interface. This feature provides ingress and egress spoof filtering on the PIX Firewall. For more information, refer to RFC 2267. You can view this RFC at the following website:

<http://www.cis.ohio-state.edu/htbin/rfc/rfc2267.html>

## Websense Filtering by Username and Group

The Websense Server works with the PIX Firewall to deny users from access to websites based on the company security policy.

Websense protocol version 4 enables group and username authentication between a host and a PIX Firewall. The PIX Firewall performs a username lookup, and then the Websense server handles URL filtering and username logging.

Websense protocol version 4 contains the following enhancements:

- URL filtering allows the PIX Firewall to check outgoing URL requests against the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.
- Username lookup enables the PIX Firewall to use the user authentication table to map the host's IP address to the username.

## Command Changes

All new commands, options, and changes are described in the *Cisco PIX Firewall Configuration Guide, Version 5.2*.

### New Commands in Version 5.2

The following commands are new in version 5.2:

- **dhcpd**—Enables the DHCP server feature on a specified PIX Firewall interface allowing the PIX Firewall to function as a DHCP server that provides network configuration parameters to DHCP clients.
- **flashfs**—Prepares Flash memory for downgrade to previous PIX Firewall version.
- **icmp**—Enables or disables pinging a PIX Firewall interface.
- **ip audit**—Configures use of Cisco Intrusion Detection System signatures.
- **ip verify reverse-path**—Implements Unicast Reverse Path Forwarding, also known as reverse route lookups.
- **ssh**—Specifies the host or network authorized to initiate an SSH connection to the PIX Firewall.
- **vpngroup**—Configures a Cisco VPN 3000 Client policy group. Refer to the *Cisco PIX Firewall IPsec User Guide, Version 5.2* for more information.

### New Command Options in Version 5.2

The following command options are new in version 5.2:

- **aaa accounting** command, **match access-list** option—Provides AAA access list support.
- **aaa authentication** command, **match access-list** option—Provides AAA access list support.
- **aaa authentication** command, **ssh console** option—Specifies the group of AAA servers to be used for SSH user authentication.
- **aaa authorization** command, **match access-list** option—Provides AAA access list support.
- **ca crl** command, **no** option—Deletes the CRL within the PIX Firewall.
- **ca zeroize** command, **keypair\_name** option—Deletes a specific RSA key pair.
- **clear flashfs** command, **downgrade 4.x | 5.0 | 5.1** options—Prepares a Flash memory device for use by a previous PIX Firewall software version. Use the **clear flashfs** command before downgrading the PIX Firewall software to versions prior to 5.n. Otherwise, the Flash memory file system will get out of sync with the actual contents on the Flash memory device and cause problems when the unit is reupgraded.

- **debug** command, **dhcpc packet/detaillerror** options—Displays detailed information about the DHCP lease.
- **debug** command, **dhcpcd packet/levent** options—Displays information about the DHCP server input/output (I/O) packets.
- **debug** command—The **debug packet** command sends its output to the Trace Channel. All other **debug** commands do not. Use of Trace Channel changes the way you can view output on your screen during a PIX Firewall console or Telnet session.

If a **debug** command does not use Trace Channel, each session operates independently, which means any commands started in the session only appear in the session. By default, a session not using Trace Channel has output disabled by default.

- **failover** command, **poll seconds** option—Lets you determine how long failover waits before sending special failover “hello” packets between the Primary and Standby units over all network interfaces and the failover cable.
- **fixup protocol ftp** command, **[strict]** option—Prevents web browsers from sending embedded commands in FTP requests.
- **fixup protocol** command, **sip** option—Enables SIP on the PIX.
- **global** command, **interface** option—Specifies that Port Address Translation (PAT) use the IP address of the PIX Firewall interface.
- **ip address** command, **dhcp [setroute]** option—Instructs the PIX Firewall to configure the interface IP address and subnet mask through the DHCP. The optional **setroute** argument tells the PIX Firewall to set the default route using the default gateway parameter the DHCP server returns.
- **logging** command, **standby** option—Let the failover Standby unit also send syslog messages. This option is disabled by default. You can enable it to ensure that the Standby unit’s syslog messages stay synchronized should failover occur. However, this option causes twice as much traffic on the syslog server. Disable with the **no logging standby** command.
- **show ca** command, **crl** option—Displays Certificate Revocation List (CRL) information from a given CA or LDAP server, such as the CRL issuer name, the date of the last CRL update, and the date of the next CRL update.
- **show conn** command, **state sip** option—Displays all active SIP connections.
- **sysopt** command, **route dnat** option—Specifies that when an incoming packet does a route lookup, the incoming interface is used to determine which interface the packet should go to, and which is the next hop.
- **sysopt** command, **uauth allow http-cache** option—Allows the web browser to supply a username and password from its cache for AAA authentication.
- **timeout** command, **sip** option—Modifies duration for **sip** inactivity timer. When this time elapses, the port used by the SIP service closes.
- **timeout** command, **sip media** option—Modifies duration for **sip\_media** inactivity timer. When this time elapses, SIP connections with RTP/RTCP expire.
- **url-server** command, **protocol TCP|UDP version 1|4** options—With **version 4** option, performs a username lookup, and then the Websense server handles URL filtering and username logging. With the **version 1** option, works the same as in previous PIX Firewall versions.

## Command Changes in Version 5.2

- **access-list**—Lets you specify an access list ID shared with an AAA server that provides RADIUS authorization. An **access-group** command statement is not used with this type of access list.
- **aaa-server**—Up to 14 AAA servers are permitted.
- **filter url**—This command accepts a port specification as shown in the following command syntax:

```
filter url portexcept local_ip local_mask foreign_ip foreign_mask [allow]
```

The *port* option was available in past versions but did not appear in the documentation.

- **global**—Lets you have multiple PATs. Also, PIX Firewall no longer uses network addresses or broadcast addresses in **static** and **global** command statements when creating NAT xlate translations.
- **ip local pool**—When a pool of addresses set by the **ip local pool** command is empty, the following syslog message now appears:

```
%PIX-4-404101: ISAKMP: Failed to allocate address for client from pool poolname
```

- **outbound**—The **java** option is no longer supported.
- **outbound**—The maximum *list\_ID* value is 1599. You can now have up to 14,000 **outbound** command statements in a configuration.
- **ping**—The *interface* parameter is now optional. If an interface name is not specified, PIX Firewall checks the routing table to find the address you specify.
- **show config**—ISAKMP keys now appear as follows:

```
isakmp key ***** address ip_addr netmask mask
```

- **show version**—The serial number listed with the **show version** command in version 5.2 and later is for the Flash memory BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the **show version** command, not the chassis number.
- **static**—PIX Firewall no longer uses network addresses or broadcast addresses in **static** and **global** command statements when creating NAT xlate translations.
- **static**—With the new TCP intercept feature, once the optional embryonic connection limit is reached, and until the embryonic connection count falls below this threshold, every SYN segment bound for the affected server is intercepted. For each SYN segment, PIX Firewall responds on behalf of the server with an empty SYN/ACK segment. PIX Firewall retains pertinent state information, drops the packet, and waits for the client's acknowledgement.
- **write terminal**—ISAKMP keys now appear as follows:

```
isakmp key ***** address ip_addr netmask mask
```

## Syslog Message Changes

The sections that follow list changes to syslog messages in version 5.2. All messages are described in detail in *Cisco PIX Firewall System Log Messages, Version 5.2*.

## New Messages in Version 5.2

The following syslog messages are new in version 5.2:

```
%PIX-2-106017: Deny IP due to Land Attack from IP_addr to IP_addr
%PIX-1-106021: Deny num reverse path check from IP_addr to IP_addr on interface int_name
%PIX-1-106022: Deny num connection spoof from IP_addr to IP_addr on interface int_name
%PIX-6-109015: Authorization denied (acl=acl_ID) for user 'username' from
src_addr/src_port to dest_addr/dest_port on interface int_name
%PIX-3-109016: Downloaded authorization access-list acl_ID not found for user 'username'

%PIX-4-209003: Fragment database limit of num exceeded: src = IP_addr, dest = IP_addr,
proto = protocol, id = id
%PIX-4-209004: Invalid IP fragment, size = num exceeds maximum size = size: src = IP_addr,
dest = IP_addr, proto = protocol, id = id
%PIX-4-209005: Discard IP fragment set with more than num elements: src = IP_addr, dest =
IP_addr, proto = protocol, id = id
%PIX-3-313001: Denied ICMP type=type, code=code from IP_addr on interface int_name
%PIX-6-314001: Pre-allocate RTSP UDP backconnection for faddr faddr/fport to laddr
laddr/lport
%PIX-3-315001: Denied SSH session from IP_addr on interface int_name
%PIX-6-315002: Permitted SSH session from IP_addr on interface int_name for user "user_id"
%PIX-6-315003: SSH login session failed from IP_addr on (num attempts) on interface
int_name by user "user_id"
%PIX-3-315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
%PIX-6-315011: SSH session from IP_addr on interface int_name for user "user_id"
terminated normally
%PIX-6-315011: SSH session from IP_addr on interface int_name for user "user_id"
disconnected by SSH server, reason: "text" (status_code_in_hex)
%PIX-4-4000nn: IDS:sig_num sig_msg from IP_addr to IP_addr on interface int_name
%PIX-4-404101: ISAKMP: Failed to allocate address for client from pool pool_idsha
%PIX-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr
faddr[/fport] to laddr laddr[/lport]
%PIX-4-405102: Unable to Pre-allocate H245 Connection for faddr faddr[/fport] to laddr
laddr[/lport]

%PIX-6-604101: DHCP client interface int_name: Allocated ip = IP_addr, mask = mask, gw =
IP_addr
%PIX-6-604102: DHCP client interface int_name: address released
%PIX-6-604103: DHCP daemon interface int_name: address granted MAC_addr (IP_addr)
%PIX-6-604104: DHCP daemon interface int_name: address released MAC_addr (IP_addr)
```

## Removed Messages in Version 5.2

The following syslog messages were removed in version 5.2:

```
%PIX-2-106003: Connection denied src laddr dest faddr due to JAVA Applet on interface
int_name.
%PIX-3-201007: Unable to allocate new udp connections (faddr/fport-laddr/lport)
%PIX-3-203001: ESP Error: No Key SPI hex SRC IP_addr DEST IP_addr
```

## Documentation Changes

All IPSec configuration information is now in the *Cisco PIX Firewall IPSec User Guide, Version 5.2*. This guide is available both online and in the PIX Firewall accessory kit.

# Installation Notes

Always configure a default **route** command statement to the outside interface in every configuration you create. This is especially important for use with IPSec.

## Limitations and Restrictions

No new limitations or restrictions were added in version 5.2.

## Important Notes

### AAA

The **inbound** and **outbound** options to the **aaa** command apply only to the network interfaces in the first two slots of the PIX Firewall.

### CRLs

When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0): Unknown error in cert validation, 0” and packets are lost until PIX Firewall receives the CRL. [CSCdr89880]

## Cisco Secure VPN Client

- The PIX Firewall now supports the **E-mail Address** ID Type used to identify the Cisco Secure VPN Client's peer. The ID Type is configurable within the Security Policy Editor, under **My Identity**. The E-mail Address ID Type is only applicable if you are using digital certificates.
- PIX Firewall behaves differently when used with and without Xauth in combination with IKE Mode Config.

The problem occurs when IKE Mode Config is configured and PIX Firewall runs out of addresses created by the **ip local pool** command and the next VPN client tries to come in.

The behavior is as follows:

- Without Xauth configured—PIX Firewall lets the new VPN client come in and sets up the tunnel with its own internal address.
- With Xauth configured—PIX Firewall denies the new VPN client due to lack of a local address, even if the VPN Client wants to use its own internal address.

This caveat does not exist for the Cisco VPN 3000 Client version 2.5. [CSCdr48442]

## Cisco VPN 3000 Client

The following restrictions apply to using PIX Firewall with the Cisco VPN 3000 Client:

- The **esp-des** and **esp-3des** transform sets do not work without **esp-md5** and **esp-sha**. [CSCdr62289]
- The Cisco VPN 3000 Client does not support AH protocol.
- Only aggressive mode is supported.
- Cisco VPN 3000 Client has to use split tunneling to connect to a remote PIX Firewall unit if the Cisco VPN 3000 Client is going to browse through the private network on the inside of the remote PIX Firewall unit, as well as the local network of the Cisco VPN 3000 Client. [CSCdr74154]
- From within the status window while a tunnel is available, if you press the Space key twice, the client hangs. [CSCdr74915]
- The Cisco VPN 3000 Client requires IKE Mode Config.
- The Cisco VPN 3000 Client does not support Group 2 for IKE transform sets. [CSCdr75514]
- When PIX Firewall creates multiple IPSec SPIs (security parameter indexes), the Cisco VPN 3000 Client uses the latest SPI to send data, but PIX Firewall does not. PIX Firewall does not keep track of the SPIs in the order they were created. PIX Firewall uses the SPI with the highest lifetime, but the latest SPI ends up with less lifetime than the one before.

For example, if you ping from the client and check the inbound and outbound SPIs, Cisco VPN 3000 Client can be seen to use the third (latest) SPI to send the ping, but PIX Firewall uses the second SPI, the one before the last, to respond to the ping. The result is that the ping responses return to the Cisco VPN 3000 Client, but are dropped. [CSCdr83223]

- The Cisco VPN 3000 Client on Windows 95 or Windows 98 does not take the WINS server address pushed to it from the PIX Firewall if an IP address is statically configured on the client. For static configurations, users must manually configure the adapters with WINS information. This works correctly on Cisco VPN 3000 Client on Windows NT. On Windows 95 or Windows 98, dynamic WINS support works with DHCP enabled adapters; that is, PPP or NIC adapters that get their information dynamically. [CSCdr94941]
- On PIX Firewall, you can configure multiple **vpngroup** command statements when using certificates with the Cisco VPN 3000 Client. This can be done only when the name of the **vpngroup** command statements you specify on the PIX Firewall is the same as the Organizational Unit (OU) field of the certificate on the client. When PIX Firewall is processing the client's certificate, it uses the value of the OU field of the certificate to associate with the **vpngroup** command statement and uses that. [CSCdr91010]

## Cisco VPN 3000 Concentrator

The following restrictions apply to use with the Cisco VPN 3000 Concentrator series:

- The Cisco VPN 3000 Concentrator rekeys every time an ISAKMP SA times out, which creates multiple SPIs on a PIX Firewall. [CSCdr74737]
- The AH protocol is not supported.

- Keepalive is not supported between PIX Firewall and Cisco VPN 3000 Concentrator. Keepalive is not a standard. Currently, each vendor has their own definition for keepalives and what it is supposed to accomplish. PIX Firewall keepalives currently work only with other PIX Firewall unit's and Cisco IOS software routers. [CSCdr75726]
- If IPSec traffic is not present between a PIX Firewall to a PIX Firewall, when the IPSec and ISA lifetimes expire, both IPSec and ISA SAs are deleted. If IPSec traffic is not present between a PIX Firewall and a Cisco VPN 3000 Concentrator, when the lifetimes expire, the SAs are not deleted and the units rekey. [CSCds0487]

## Failover

Refer to the “Failover” section in Chapter 3, “Advanced Configurations” in the *Cisco PIX Firewall Configuration Guide, Version 5.2* for a new procedure for configuring failover.

The PIX Firewall DHCP client does not support **failover** configurations.

## FDDI

FDDI interfaces are supported on the PIX 525 with the caveat that no other interface card can be used with FDDI cards. In addition, the Ethernet interfaces on the motherboard must be shut down using the **shutdown** option to the **interface** command.

On the PIX 520 and earlier models, when FDDI interface cards are used, no other interface card can be used on the unit.

The PIX 515 does not support use of any FDDI interface cards.

## License Key Downgrade

If you downgrade your license key from a UR to an R, thereby restricting the number of supported interfaces, PIX Firewall removes all commands from your configuration that reference the unsupported interfaces. In addition, open caveat CSCdr52181 notes that PIX Firewall also removes all **nat** and **static** commands from the configuration.

## SMTP

Multiple SMTP commands contained in a single packet are no longer permitted and are now dropped.

## Token-based Authentication for VPN Clients

The PIX Firewall now supports token-based authentication systems through the use of the **crypto map token authentication** command. PIX Firewall supports the following token-based authentication systems and modes for use with the Cisco VPN 3000 Client:

- Security Dynamics (SDI) SecurID/ACE Server with SDI RADIUS
  - Next Token mode
  - New Pin mode

- SDI with CiscoSecure ACS, NT version
  - Next Token mode
  - New Pin mode
- SDI with CiscoSecure ACS, UNIX version
  - Next Token mode

The PIX Firewall supports the SDI RADIUS token-based authentication system using Next Token mode or New Pin mode for use with the Cisco Secure VPN Client, version 1.1.

Token based authentication has not been verified for the following vendors/products:

- CRYPTOCARD
- SafeWord
- AXENT

For more information about the **crypto map token authentication** command, see the **crypto map** command page in Chapter 12, “Command Reference” of the *Cisco PIX Firewall IPSec User Guide, Version 5.2*.

## Caveats



### Note

Use Troubleshooting Tools on cisco.com to view additional caveat information. You can access this tool at the following website:

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

## Open Caveats - Release 5.2(6)

The caveats in the following table are yet to be resolved in this release:

**Table 1**    *Open Caveats*

DDTS Number	Software Release	
	5.2(6)	
	Corrected	Caveat
CSCds10112	No	Traceback (Crypto PKI RECV) after twice enrolling and getting denied.
CSCds29190	No	PIX Firewall fails over silently while generating RSA key of size 2048.
CSCdt53815	No	SNMP polls timeout. PIX Firewall tears down the UDP connection.
CSCds54310	No	Traceback (ci/console) doing <b>sh map</b> , IPSec tunnel exists.
CSCdu02557	No	Xauth: With ACS+SecurID, new pin mode, not allowed to enter return.

**Table 1** Open Caveats (continued)

DDTS Number	Software Release	
	5.2(6)	
	Corrected	Caveat
CSCdu36628	No	PIX Firewall neither uses nor discards CRL if time < last CRL update of CA.
CSCdu46552	No	PIX Firewall reboots because of Websense.
CSCdu52492	No	Unexpected reload after pressing Ctrl-R and holding down any key.
CSCdu53971	No	Misconfigured failover interface a.b.c.d lines cause flip-flops.
CSCdu60003	No	Websense 4.3/Caching - # of Hits and # Hit Rate does not increment.
CSCdu60033	No	AAA: Telnet console does not allow use of challenge response.
CSCdu60862	No	PIX Firewall URL CACHE does not work with Websense 4.3.
CSCdu61102	No	PIX Firewall URL Filtering Extremely slow 200-400 URLs/sec.
CSCdu63411	No	Xauth: IRE rekey using different username/password, <b>uauth</b> remains same.
CSCdu64148	No	32 MB PIX 520 Backup PAT is not working.
CSCdu67715	No	PIX Firewall is not sending/processing initial contact w/ concentrator/client.
CSCdu66557	No	H.323 Skinny does not properly open 3rd party IP using nat 0 acl.

## Open Caveats - Release 5.2(5)

The following caveats are yet to be resolved:

- CSCds67745

If you configure a network static where the network static is the same as a third party netmask and address, then an outbound H.323 connection fails. The following example clarifies this problem:

The interfaces in the example are as follows:

- Outside interface IP address:10.1.1.6
- Inside interface IP address:10.0.0.5
- Embedded address on inside interface:10.0.0.7

Example network **static** command statement:

```
static (inside,outside) 10.1.1.0 10.0.0.0
```

This command maps the inside host address of 10.0.0.5 to the outside global address of 10.1.1.5, and the inside host address 10.0.0.7 to the outside global address of 10.1.1.7.

If the PIX Firewall encounters a packet from 10.1.1.5 to 10.0.0.5 with the embedded IP address of 10.1.1.7, the PIX Firewall unit will not be able to determine if the embedded IP address belongs to the inside or outside network.

- CSCds10228

PIX Firewall is not able to create an IPsec tunnel with a 2048 RSA key using a PIX Firewall “Classic” model.

- CSCds10022

PIX Firewall fails to get certificates if downgraded from 5.2 when used with the Microsoft Certification Authority.

- CSCds08487

When IPsec traffic is not present between a PIX Firewall to a PIX Firewall, when the IPsec and ISA lifetimes expire, both IPsec and ISA SAs are deleted. When IPsec traffic is not present between a PIX Firewall and a Cisco VPN 3000 Concentrator, when the lifetimes expire, the SAs are not deleted and the units rekey.

- CSCdr96232

H.323 call setup is not supported by failover.

- CSCdr94941

The Cisco VPN 3000 Client on Windows 95 or Windows 98 does not take the WINS server address pushed to it from the PIX Firewall if an IP address is statically configured on the client. For static configurations, users must manually configure the adapters with WINS information. This works correctly on Cisco VPN 3000 Client on Windows NT. On Windows 95 or Windows 98, dynamic WINS support works with DHCP enabled adapters; that is, PPP or NIC adapters that get their information dynamically.

- CSCdr96486

Always configure a default **route** command statement to the outside interface in every configuration you create. This is especially important for use with IPsec.

- CSCdr94034

ICMP types 3, 4, 5, 11, 12, 13, 14, 15, 16, 17, and 18 fail with PAT.

- CSCdr91340

During the PIX Firewall unit's enrollment request to a Baltimore CA server, the process fails. This failure occurs when using the **ca enroll** command to obtain CA-signed certificates for each of the two special-purpose RSA key pairs the PIX Firewall generated (using the **ca generate rsa specialkey** command). When the failure occurs, PIX Firewall displays the following error messages:

```
CRYPTO_PKI: status = 100: certificate is granted
CRYPTO_PKI: Error: Invalid format for BER encoding while
#####In GetRecipientInfo: 315
CRYPTO_PKI: status = 266: failed to open the envelope
The certificate enrollment request failed!
```

- CSCdr89880

When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0): Unknown error in cert validation, 0” and packets are lost until PIX Firewall receives the CRL.

- CSCdr87814

SSH permits up to 100 characters in a username and up to 50 characters in a password.

- CSCdr83223

When PIX Firewall creates multiple IPSec SPIs (security parameter indexes), the Cisco VPN 3000 Client uses the latest SPI to send data, but PIX Firewall does not. PIX Firewall does not keep track of the SPIs in the order they were created. PIX Firewall uses the SPI with the highest lifetime, but the latest SPI ends up with less lifetime than the one before.

For example, if you ping from the client and check the inbound and outbound SPIs, Cisco VPN 3000 Client can be seen to use the third (latest) SPI to send the ping, but PIX Firewall uses the second SPI, the one before last, to respond to the ping. The result is that the ping responses return to the Cisco VPN 3000 Client, but are dropped.

- CSCdr83132

In version 5.1 and prior versions, when you enabled the **debug** command, output messages displayed at an active terminal session, such as the console or a Telnet session.

In version 5.2 and future versions, PIX Firewall supports multiple console sessions, which means that **debug** command output messages can be sent to multiple sessions simultaneously, as long as the sessions are enabled. Each session is enabled or disabled independently and there is no effect on other sessions.

- CSCdr75726

The Cisco VPN 3000 Concentrator series ignores all keepalive messages originating from the PIX Firewall unit.

- CSCdr75706

PIX Firewall/Cisco VPN 3000 Concentrator: traffic does not restart after power cycling the concentrator.

- CSCdr75514

The Cisco VPN 3000 Client does not support Group 2 for IKE transform sets.

- CSCdr74915

From within the Cisco VPN 3000 Client status window, while a tunnel is available, if you press the Space key twice, the client hangs.

- CSCdr74780

Use of the SNMP ip.ipAddrTable entry requires that all interfaces have unique addresses. If interfaces have not been assigned IP addresses, by default, their IP addresses are all set to 127.0.0.1. Having duplicate IP addresses causes the SNMP management station to loop indefinitely. The workaround is to assign each interface a different address. For example, you can set one address to 127.0.0.1, another to 127.0.0.2, and so on.

- CSCdr74760

When starting a SSH session, a dot (.) displays on the PIX Firewall console before the SSH user authentication prompt appears.

The dot appears as follows:

```
PIXfirewall(config)# .
PIXfirewall(config)# .
```

The display of the dot does not affect the functionality of SSH. The dot appears on at the console when generating a server key or when decrypting a message using private keys during SSH key exchange, before user authentication occurs. These tasks can take up to two minutes or longer. The dot is a progress indicator that verifies that the PIX Firewall is busy and has not hung.

- CSCdr74154  
Cisco VPN 3000 Client has to use split tunneling to connect to a remote PIX Firewall unit if the Cisco VPN 3000 Client is going to browse through the private network on the inside of the remote PIX Firewall unit, as well as the local network of the Cisco VPN 3000 Client.
- CSCdr72486  
In version 5.2, when keys and certificates generated with the **crloptional** parameter to the **ca** command are replaced with new ones, ISAKMP negotiation fails. This caveat previously worked correctly in version 5.1. This caveat was observed after creating keys and certificates, sending traffic, and removing the keys and certificates on both PIX Firewall units. After new keys and certificates were created with the **crloptional** parameter to the **ca** command and new traffic started, ISAKMP negotiations failed.
- CSCdr71094  
An **ip local pool** range cannot have multiple subnets.
- CSCdr66093  
If PIX Firewall crashes, it attempts to run the **show tech-support** command. A long configuration can cause further crashes.
- CSCdr64494  
PIX Firewall using RADIUS or TACACS+ requires username and password pairs for authentication, but only authorizes based on IP addresses. Once a multiuser host has been authenticated, all other users on that host are granted authentication. This may allow unauthorized users access to services normally denied them.  
  
Setting the uauth timeout to zero partially solves this problem, but makes Web browsing difficult for authorized users because they must reauthenticate for every new page they view.
- CSCdr62289  
The Cisco VPN 3000 Concentrator, only supports a limited number of IPSec transform sets. The Cisco VPN 3000 Concentrator does not support the AH protocol. The supported transform sets are as follows:  
  

```
esp-des esp-md5-hmac
esp-des esp-sha-hmac
esp-3des esp-md5-hmac
esp-3des esp-sha-hmac
esp-null esp-md5-hmac
```
- CSCdr52181  
If you downgrade your license key from a UR to an R, thereby restricting the number of supported interfaces, PIX Firewall removes all commands from your configuration that reference the unsupported interfaces. In addition, PIX Firewall also removes all **nat** and **static** commands from the configuration.
- CSCdr48442  
PIX Firewall behaves differently when used with and without Xauth in combination with IKE Mode Config when used with the Cisco VPN Client. Refer to the second bullet item in “Cisco Secure VPN Client” for more information.
- CSCdr43729  
The **aaa authorization except** command does not work for UDP.
- CSCdr33945  
Crash in Crypto PKI RECV thread during certificate enrollment.

- CSCdp60588  
Interface routing should be based on the DNAT address.
- CSCdp55755  
Outbound filtering is not working correctly. An example is as follows:

```
outbound 2 permit 0.0.0.0 0.0.0.0 0 tcp
outbound 2 deny 192.168.85.51 255.255.255.255 0 ip
outbound 2 deny 192.168.85.51 255.255.255.255 0 tcp
apply (inside) 2 outgoing_src
```

If you do not have the third command statement, the second line does not stop TCP packets. It may sound logical, the protocol values may be UDP, TCP, or the ICMP protocols. In this case, ip is not a valid protocol, and thus, not evaluated by the PIX Firewall, but it is not denied by PIX Firewall command line parser.

## Resolved Caveats - Release 5.2(6)

The caveats in the following table were resolved in this release.

**Table 2** Resolved Caveats

DDTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCdp73853	Yes	<b>debug crypto ca</b> messages are intermixed on console.
CSCdp99518	Yes	No warning is given when you try to configure unsupported pfs gp5.
CSCdr34819	Yes	<b>clear configure all</b> does not reset <b>arp timeout</b> to default values.
CSCdr43633	Yes	URL size exceeds buffer size.
CSCdr48472	Yes	<b>conn</b> needs to be deleted from <b>clear ?</b> command page.
CSCdr60893	Yes	The <b>clear url-server</b> command is confusing.
CSCdr68928	Yes	When the certificate request fails it still says pending.
CSCdr78189	Yes	No syslog when SSH, Telnet, or PFM connection limit is exceeded.
CSCdr78505	Yes	The PIX Firewall does not compute the RIP v2 updates for the default route.
CSCdr80268	Yes	The SNMP ifTable.ifEntry.ifDescr is not updated after swapping interface names.
CSCdr84397	Yes	The PIX Firewall does not reset the sixth consecutive requested SSH, Telnet, or PFM session.
CSCds11341	Yes	PIX 525 with Gigabit Ethernet card prints console messages and reboots with heavy load.
CSCds18774	Yes	The PIX Firewall should not respond to its own ARP request.
CSCds21095	Yes	The PIX Firewall PPTP stops accepting new connections after periods of trouble-free operation.
CSCds43973	Yes	Cannot Telnet to the PIX Firewall inside interface - 402106. Error reads "Recd packet not IPSEC..."

Table 2 Resolved Caveats (continued)

DTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCds46441	Yes	The PIX Firewall should indicate an error since “ <b>no dhcpd d</b> ” is not unique.
CSCds52853	Yes	<b>help crypto</b> has two entries for dynamic-map.
CSCds60270	Yes	The PIX Firewall is unable to establish a tunnel with peer if peer changes keys or ID.
CSCds63501	Yes	LU updates for UDP <b>conn</b> are not properly propagated to standby unit.
CSCds74244	Yes	Unit reloads if Active and Standby units write to memory at same time.
CSCds81948	Yes	The unit reloads after trying to enroll with a Baltimore certificate and typing in some commands.
CSCds85080	Yes	IKE Main mode proposal flooding reboots the PIX Firewall.
CSCds89281	Yes	hdb_sweep thread may get starved under heavy system load.
CSCds90077	Yes	Unexpectedly reloads while trying to change the transform set.
CSCds90802	Yes	NFS disallows packets of more than 12 fragments needed for Solaris.
CSCdt00162	Yes	Service <b>resetinbound</b> does not work with interface PAT.
CSCdt01808	Yes	ARP does not proxy-arp for ARP alias entry.
CSCdt01825	Yes	PIX Firewall should proxy-arp for alias address.
CSCdt02063	Yes	H.245: PIX Firewall should create new TPKT and discard original if TPKT received only.
CSCdt02132	Yes	The PIX Firewall should check host list on first SYN for Telnet, SSH, PFM and HTTP.
CSCdt02883	Yes	Certificate enrollment request is lost if CA is not available at that time.
CSCdt04772	Yes	Make fragment database limits configurable.
CSCdt05025	Yes	LU look NAT failed; NAT is disabled.
CSCdt06447	Yes	PIX Firewall in Stateful Failover configuration may deplete memory blocks.
CSCdt07794	Yes	Cannot select private key; message prints on standby during synchronization.
CSCdt15446	Yes	Incorrect interface state on standby unit.
CSCdt15819	Yes	Fails to dump UDP connection after DNS reply is seen.
CSCdt16666	Yes	PIX Firewall on reboot will not get address via DHCP if connected through switch to sever.
CSCdt17577	Yes	PIX Firewall cannot send filter URLs to Websense longer than 1159 characters.
CSCdt18433	Yes	H.225: syslog 405104 for signalling protocol is wrong.

Table 2 Resolved Caveats (continued)

DDTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCdt18451	Yes	<b>clear config all</b> does not clear <b>icmp</b> command.
CSCdt22085	Yes	With names in the configuration, host route changes to default route on reload.
CSCdt28073	Yes	PIX Firewall appends two bytes to RADIUS state attribute.
CSCdt28219	Yes	Internal users cannot ping outside hosts with interface PAT.
CSCdt28399	Yes	<b>vpdn group pp</b> followed by anything is accepted. No error message.
CSCdt30628	Yes	<b>help static</b> does not mention embryonic connection limit.
CSCdt31630	Yes	Blocks can wedge into fragment database.
CSCdt32830	Yes	RST always printed for syslog 106015 even if no RST in packet.
CSCdt34923	Yes	Error message when deleting global address pool.
CSCdt35429	Yes	Naptha DoS tool with PIX Firewall SSH daemon causes high CPU load.
CSCdt36491	Yes	<b>debug icmp trace</b> prints invalid type and code for fragmented packet.
CSCdt37028	Yes	Redundant error checking can cause traceback within first traceback.
CSCdt38205	Yes	Stateful Failover should not generate syslog when out of memory.
CSCdt38404	Yes	Wrong character for Account rule in <b>aaa accounting</b> command.
CSCdt38616	Yes	RIP routes have a metric of one added.
CSCdt39076	Yes	PIX Firewall does not generate an error if <b>0.0.0.0/net add</b> is specified for dns in <b>vpdn gp</b> .
CSCdt39174	Yes	<b>vpdn group dns/wins</b> command is not fully replaced by a new one.
CSCdt39820	Yes	Syslog for memory allocation error used improperly in places.
CSCdt39863	Yes	Unexpected reload while enrolling certificate request.
CSCdt39871	Yes	Logging priority consulted only after formatting overhead incurred.
CSCdt40579	Yes	Without IPSec, host can Telnet to PIX Firewall from least-secured interface.
CSCdt40713	Yes	<b>xlate</b> error when portmap pool is exhausted results in rogue connections.
CSCdt40837	Yes	PIX Firewall <b>show block</b> has 1552 size entry.
CSCdt41079	Yes	Telnet, SSH, and TFTP server always assume least-secured interface at level 0.
CSCdt41763	Yes	Using names within a <b>static</b> command results in a misconfiguration.
CSCdt42739	Yes	H.323: PIX Firewall should open connections based on <i>LogicalChannelNumber</i> .
CSCdt45065	Yes	Small block pool causes traffic to stall with Livengood Gigabit card.

Table 2 Resolved Caveats (continued)

DTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCdt47536	Yes	gdb toolchain disappearing from irp-view5.
CSCdt49040	Yes	PIX Firewall does not allow packets with a UDP SRC (source) port of 0.
CSCdt49906	Yes	Virtual HTTPITelnet does not work if interface 0 is not in lowest security level.
CSCdt53291	Yes	Remove unsupported <b>pal</b> command.
CSCdt53742	Yes	Global NAT does not work with VoIP Third Party address.
CSCdt54951	Yes	Standby unit incorrectly creates UDP connection and generates 210010 syslogs.
CSCdt56080	Yes	Traceback occurs when trying to build PPTP tunnel with RADIUS server unavailable.
CSCdt57251	Yes	PIX Firewall should not allow fragment chain > fragment database size.
CSCdt57268	Yes	<b>clear config all</b> does not clear fragment configuration.
CSCdt58805	Yes	PIX Firewall must not change <b>isakmp</b> lifetime in IKE initiators proposal.
CSCdt60308	Yes	Certificate request fails if retried after cancelling.
CSCdt60487	Yes	PIX Firewall reboots, dumping trace.
CSCdt61216	Yes	Naptha (ESTABLISHED) Flooding causes PDM DoS.
CSCdt62968	Yes	Reboot occurs with filter java and NAT 0 access-list.
CSCdt63037	Yes	VoIP: No voice between inside phones (static NAT with no route).
CSCdt64243	Yes	“ike retransmit debug” seen on console even with debug off.
CSCdt64687	Yes	DHCP client does not interoperate with some relay agents or servers.
CSCdt65464	Yes	MIB-II object <b>interfaces.ifSpeed</b> query not supported on Gigabit Ethernet card.
CSCdt65603	Yes	PIX Firewall gives incorrect prompt when performing Xauth.
CSCdt66414	Yes	Remove unused pal_check() function in lu_thread.
CSCdt66614	Yes	SSH allowed after changing hostname and domain name when previous keypair exists.
CSCdt66648	Yes	CA: Does not save .server key to the FLASH with <b>ca save all</b> command.
CSCdt69667	Yes	Encryption layer for TCP port 1467 uses up large amount of memory.
CSCdt69676	Yes	Enable UniRPF for-us traffic.
CSCdt70750	Yes	<b>sysopt connection tcpmss 0</b> behavior changed from 5.0 to 5.1.
CSCdt71192	Yes	Stateful Failover PIX Firewall logs duplicate messages on syslog server.

Table 2 Resolved Caveats (continued)

DDTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCdt73353	Yes	SSH: Need to add CRC-32 compensation attack detection.
CSCdt73358	Yes	Need unique tty number in <b>ssh debug</b> messages.
CSCdt73865	Yes	H.323 message printed on console needs to be removed.
CSCdt74263	Yes	Do not allow more than one RSA key through with different attributes.
CSCdt74520	Yes	<b>uauth</b> cache not working properly with browsers.
CSCdt75715	Yes	<b>fragment</b> command handles input > max inconsistently.
CSCdt75960	Yes	ISA fragment method causes PIX Firewall to discard packet.
CSCdt77108	Yes	Need to selectively allow unencrypted SSH sessions for debugging.
CSCdt77818	Yes	Traceback (crypto CA) if Netscape CA server is misconfigured.
CSCdt82325	Yes	Reloads due to exhausted memory while URL filtering heavy traffic.
CSCdt83142	Yes	SIP: Call does not go through with static network.
CSCdt85788	Yes	PIX Firewall fails to get CRL with VeriSign certificate.
CSCdt86132	Yes	“709001: FO repliSorry: error” message at boot up.
CSCdt86568	Yes	Unexpectedly reloads when URL cache is on and the URL server is unavailable.
CSCdt92339	Yes	BUGTRAQ: PIX Firewall should limit number of <b>uauth</b> sessions per source IP.
CSCdt92450	Yes	Multiple <b>websns keepalive</b> daemon starts.
CSCdt93858	Yes	<b>kprint</b> message to console when fails to allocate memory block.
CSCdt94747	Yes	H.323: PIX Firewall should proxy ACK TPKT if received TPKT only.
CSCdu01056	Yes	Reloads while running backup traffic (SQL*Net) through the PIX Firewall.
CSCdu02291	Yes	Failover timeout needs to be taken out from failover online help.
CSCdu02673	Yes	<b>clear config</b> should be a config mode command.
CSCdu02674	Yes	Issues with the service command.
CSCdu04084	Yes	Traceback while reading certificate from FLASH.
CSCdu05134	Yes	H.323: Call does not go through if calling GW uses slow start.
CSCdu05694	Yes	Invalid global command causes traceback (ci/console).
CSCdu05843	Yes	<b>ip verify</b> does not work with IPSec.
CSCdu06716	Yes	<b>show chunk</b> only shows <b>ulimit chunk</b> .
CSCdu08574	Yes	Certificate enroll request fails after deleting current CA and retrying.
CSCdu11774	Yes	SIP: Call does not go through with IN proxy (Regression).

Table 2 Resolved Caveats (continued)

DTS Number	Software Release 5.2(6)	
	Corrected	Caveat
CSCdu11781	Yes	Reloads during DHCP request when PDM refreshes DHCP Client information.
CSCdu12321	Yes	PIX Firewall fails to do <b>write memory</b> if a big command line exists.
CSCdu12909	Yes	SIP: Connections for Responses to INVITE not opened correctly.
CSCdu13395	Yes	Remove [ <b>nailed</b> ] parameter from static command online help.
CSCdu13956	Yes	Deleting non-default <b>fixup rtsp</b> port also deletes default port.
CSCdu15173	Yes	H.323: RAS routine causes memory corruption.
CSCdu18020	Yes	PIX Firewall-to-PIX Firewall or PIX Firewall-to-Unity connection fails when using certificates.
CSCdu20593	Yes	Xauth: With IRE on rekey, puts internal address entry for <b>uauth</b> .
CSCdu27169	Yes	VoIP: Certain embedded IP addresses do not undergo NAT.
CSCdu33209	Yes	IPSec Antireplay Checking Ineffective 32-64 sequence numbers back.
CSCdu33543	Yes	PIX Firewall PPTP rejects dial-in request after abnormal termination.
CSCdu38206	Yes	Configuration lines greater than 255 displayed incorrectly by <b>sh conf</b> .
CSCdu38927	Yes	PIX Firewall failover should try to allocate additional block if possible.
CSCdu39748	Yes	H.323: Generating 50+ calls causes unexpected reload.
CSCdu39906	Yes	PIX Firewall should not send stateful updates if peer is down.
CSCdu43016	Yes	TCP Intercept sends ARP for every proxied syn-ack.
CSCdu43284	Yes	H.323: Should make use of NELTS and <b>sizeof</b> and remove <b>extern</b> functions.
CSCdu44088	Yes	<b>crypto map set sub</b> command always returns fail.
CSCdu46309	Yes	<b>pix_init</b> should be called after verifying license key.
CSCdu47003	Yes	Able to pass disallowed SMTP command through PIX Firewall by sending after mail.
CSCdu48706	Yes	<b>clear interface</b> does not clear Gigabit interface counters.
CSCdu53473	Yes	H.225 and H.245 messages greater than 1024 bytes are not inspected.
CSCdu54495	Yes	Unexpected reload when using Websense with TCP4 and url-cache.
CSCdu55206	Yes	Traceback while trying to establish a PPTP tunnel (scripted).

## Resolved Caveats - Release 5.2(5)

The following caveats were resolved:

- CSCdt22910  
Previously, if the Cisco VPN 3000 Client forced a disconnect from an IPSec tunnel, the PIX Firewall would crash. This has been fixed.
- CSCdt20809  
In an IPSec PIX Firewall VPN tunnel, the PIX Firewall no longer retransmits the Phase 2 Security Association timers when the tunnel is established.
- CSCds89077  
PIX Firewall now opens third party H.245 connections by inspecting the H.225 signaling messages to look for the specified H.245 address. PIX Firewall then uses that address to open the H.245 connection.

## Resolved Caveats - Release 5.2(4)

The following caveats were resolved:

- CSCdt06176  
When used with the PIX Firewall, NetMeeting now displays audio and video.
- CSCdt04241  
In a Stateful Failover configuration, the PIX Firewall no longer displays the message "skip preallocated port."
- CSCdt00459  
The **debug crypto ca** command output is now displayed correctly.
- CSCds92738  
In a failover configuration, the standby PIX Firewall no longer displays incorrect translation debugs.
- CSCds90792  
The **fixup smtp** command no longer blocks email separated by a packet when the "." and "<CR><LF>" are the termination sequence and are split across multiple TCP frames.
- CSCds88063  
If a standalone PIX Firewall is licensed for failover, it is unable to get an IP address using DHCP.
- CSCds87365  
The PIX Firewall now inspects H.323 Progress messages, which could cause problems with the Cisco Call Manager.
- CSCds82455  
In an IPSec configuration, the quick mode packet will now be retransmitted to the initiator.
- CSCds82103  
It is now possible to manually release or renew a DHCP address.
- CSCds81003  
The **ip audit interface** command now displays the correct output.
- CSCds80481  
Previously a PIX Firewall using FDDI in a failover configuration would show the incorrect MAC address in the **show version** command. This has been corrected.

- CSCds77371  
The **show arp** command will now display the most recent ARP entries first, and will now return an error if an ARP entry is manually entered if the ARP table is full.
- CSCds76768  
Onboard Ethernet interfaces (ethernet0 and ethernet1) on a PIX 525 with a serial number of 44480380055 through 44480480044 set to full-duplex may cause interface errors and throughput reductions. Use the **eprom update** command to fix this problem.
- CSCds74710  
When PIX Firewall hostname or domain name is changed, instead of erasing the RSA key, a warning message will be issued.
- CSCds74352  
If a connection is established, **ip verify** will now work.
- CSCds74142  
The **fixup H.323 ras** command now correctly rejects an ACF message if it has not received an ARQ message, and displays a syslog message warning that the connection for the packet is terminated.
- CSCds73999  
Diagnostic boot messages now display the full text of the offending configuration line information.
- CSCds73818  
The **fixup H.323** command now correctly checks the state of call signalling and displays a **syslog** warning message when required.
- CSCds73769  
When the **write memory** command is executed, the PIX Firewall now saves the correct configuration data, but does not issue a **CA save all**.
- CSCds73666  
The Cisco Systems copyright notice now displays before and not after the configuration-related diagnostic messages in the boot messages.
- CSCds72776  
An H225 packet with an invalid protocol discriminator now generates an informational syslog message:  

```
405103: H225 message from 10.132.4.5/1720 to 10.130.4.250/31776 contains bad protocol discriminator 4
```
- CSCds72713  
H.323 debug messages now display in the syslog and not on the console.
- CSCds70898  
The **fixup ftp strict** command now correctly displays ProFTPD banners.
- CSCds69039  
Valid ICMP error packets are now accepted during the tunnel check post verification in IPSec.
- CSCds69038  
The syslog protocol field now displays correctly.
- CSCds68537

- The **aaa accounting exclude** command now correctly displays local and foreign IP addresses.
- CSCds66550
 

When the maximum number of channels have been allocated in the PIX Firewall, the syslog error it generates no longer causes the logger to time out.
- CSCds65704
 

The **clear filter** command now correctly removes filter command statements from IPSec configurations.
- CSCds64958
 

Performing an active FTP transfer with the **fixup strict ftp** command that generates long reply code will sometimes cause the command to fail. The workaround is to use passive FTP.
- CSCds63626
 

If an ICMP echo request is sent to the PIX Firewall outside interface with an IP source address of the inside broadcast address, the packet will be logged and dropped, except in version 5.1 which will only drop it.
- CSCds63569
 

The maximum number of socket channels is 128 for this release. The maximum number of TCP channels is 320 for this release.
- CSCds62051
 

The **clear config secondary** command now clears CA related configuration information including **ca identity**, **ca configure**, **domain-name**, rsa keys and certificates.
- CSCds61417
 

Previously, if the DHCP client was configured on the PIX Firewall, routes manually entered were not stored in the configuration. This has been fixed.
- CSCds60165
 

The PIX Firewall will now utilize two dynamically prepared UDP connections in order to accommodate an NFS mount with Solaris 2.6.
- CSCds59757
 

Previously, with AAA accounting enabled and high traffic volume, the PIX Firewall could crash. This has been fixed.
- CSCds58358
 

The **sysopt connection enforcesubnet** command is now deprecated correctly.
- CSCds57285
 

An error message is now displayed when a **copy tftp flash** command or **configure net** command is entered and the process does not complete.
- CSCds56725
 

The PIX Firewall no longer crashes when given a large CRL.
- CSCds55770
 

The message ".Config Error" at bootup is no longer displayed.
- CSCds55734
 

The **show connection** command now displays byte count correctly.
- CSCds54886

- The PIX Firewall no longer crashes when using AAA to parse the URL in an HTTP GET.
- CSCds54786  

The **interface** command now allows the entry of **16mbps** and **4mbps** for the speed of a token-ring interface.
- CSCds54451  

The PPTP maximum time out now is calculated correctly.
- CSCds53316  

With the introduction of Cisco VPN 3000 Client compatibility, IPSec Security Associations needed to be manually cleared in a PIX Firewall to PIX Firewall IPSec tunnel configuration after the configured SA timeout occurred. This has been fixed.
- CSCds51960  

A ping with ICMP identification of zero using PAT no longer fails.
- CSCds51957  

The **show xlate** command now correctly displays the ICMP identification.
- CSCds51955  

The **tracert** command now works on an interface with PAT.
- CSCds50982  

The PIX Firewall is now able to retrieve a CRL if the first attempt fails because of an established TCP session.
- CSCds50287  

The PCI base address no longer maps into the heap memory.
- CSCds50002  

CHAP authentication under Microsoft Windows 95 with PPTP now will stop trying to authenticate after 16 tries.
- CSCds49991  

Telnet and FTP now work through PPTP using the Microsoft Windows 95 PPTP client.
- CSCds44839  

The **nameif** command now displays an error when trying to configure an interface that is not licensed.
- CSCds41775  

Hummingbird Exceed XDMCP (Xwindows) now works with PIX Firewall.
- CSCds39293  

The PIX Firewall no longer creates a default route when RIPv2 packet with no mask is used.
- CSCds34732  

The lookup function for the H245 packet length has been corrected so that these packets are now processed.
- CSCds34721  

Previously, the Checkpoint Firewall-1 caused an interop failure when Checkpoint initiated a quick mode IPSec connection to the PIX Firewall. This has been fixed.
- CSCds34475

- The PIX Firewall will now consume pre-allocated connections by direction.
- CSCds32842  
The **fixup H323** command will now NAT a third party local to global translation.
- CSCds31061  
A PIX Firewall can no longer have two pairs of RSA keys at the same time.
- CSCds30523  
The **nat 0** command associated with an access list now denies traffic.
- CSCds30449  
The **vpdn group** command now returns an error when entered incorrectly.
- CSCds29676  
Websense caching now displays correct url-cache statistics.
- CSCds29656  
The PIX Firewall now allows the **nat 0 0 0** command to be used in conjunction with the **nat 0 access-list** command.
- CSCds26568  
There is now contextual help available for the **logging standby** command.
- CSCds26054  
The RSA key no longer disappears on standby PIX Firewall after failover.
- CSCds25070  
The PIX Firewall no longer crashes with Stateful Failover every two hours.
- CSCds24580  
The PIX Firewall now has a configurable Radius port number.
- CSCds23698  
The PIX Firewall no longer checks all the bits in the TCP flags except the urgent, acknowledge, reset, synchronize, and finish bits for session establishment.
- CSCds22194  
The **alias** command now works when a DNS server address is included in the command syntax.
- CSCds21095  
PPTP will no longer stop accepting new connection requests from clients.
- CSCds12925  
The **npdisk** command now works on the PIX 525 platform.
- CSCds11378  
On an H.323 call, the call no longer hangs after 30-40 minutes.
- CSCds09730  
ISAKMP no longer fails if the same network number exists on the remote end of a VPN tunnel.
- CSCds07842  
A FDDI failover configuration now works on a PIX 525.

- CSCds07597  
The PIX Firewall will poll the CRL during first ISAKMP negotiation when CRL is expired. Previously, it would fail if the CRL was expired in the first attempt, and would have to be manually renegotiated.
- CSCdr99484  
Certificate retrieval no longer fails if the transfer of the certificate takes longer than five seconds.
- CSCdr93435  
The PIX Firewall now opens third party Media Channels.
- CSCdr84484  
Previously, the write net command caused 1550 byte block leak, which could prevent traffic flow. This has been fixed.
- CSCdr77921  
Opening a web page with Microsoft Outlook 2000 no longer results in continuous authentication.
- CSCdr76192  
A PIX Firewall using Websense filtering no longer bypasses some HTTP 1.1 URLs that use a keepalive connection.
- CSCdr68251  
Port numbers are now displayed in the syslog when using access lists.
- CSCdr04004  
Previously, small ARP timeouts caused short periods of packet loss. This has been fixed.
- CSCdp67764  
The **show traffic** command now displays correct number of packets information.

## Resolved Caveats - Release 5.2(3)

The following caveat was resolved:

- CSCds38708  
The **fixup protocol smtp** command no longer permits commands it would normally screen out from being appended to the SMTP DATA command.

## Resolved Caveats - Release 5.2(2)

The following caveats were resolved:

- CSCds30699  
PIX Firewall continues to filter SMTP commands if the DATA command fails. Previously, the Mail Guard feature would stop filtering if the DATA command failed. The Mail Guard feature is enabled with the **fixup protocol smtp port\_number** command, which is enabled in the PIX Firewall unit's default configuration.
- CSCdr91002  
Multiple SMTP commands contained in a single packet are no longer permitted and are now dropped.

## Resolved Caveats - Release 5.2(1)

The following caveats were resolved:

- CSCds08316  
H.323 now correctly performs NAT on IP addresses configured with the **alias** command.
- CSCds02965  
The **fixup protocol rtsp** command no longer allocates the wrong server port for QuickTime.
- CSCdr97777  
When using the **fixup protocol ftp strict** command, FTP communications between a server that advertises a big welcome banner, and a Windows 2000 or Netscape Communicator 4.73 client now works correctly.  
  
Previously, these types of FTP connections were treated as intrusion events and dropped. The problem occurred because these clients issued the next command before receiving the complete advertised banner from the server. PIX Firewall treated this as a pipelined command, which with the **strict** option, is treated as an intrusion event.
- CSCdr96658  
PIX Firewall no longer crashes during Cisco Secure Policy Manager configuration downloads.
- CSCdr96442  
All inside interface static **route** command statements now appear in the configuration. Previously, an RIP-generated route overrode the static route and kept it from appearing in the configuration. Now the static route overrides an RIP-generated route.
- CSCdr93006  
PIX Firewall no longer creates two PPTP tunnels for the same client.
- CSCdr92704  
The **configure net** command no longer changes the severity level of the **logging history** command.
- CSCdr91940  
Failover with an Ethernet cross-over cable no longer causes the configuration in the Standby unit to be lost and the network to become temporarily unavailable.
- CSCdr91608  
PIX Firewall now verifies that an xlate is linked to a host object; if not, the “no local host infor” message appears when the **show xlate debug** command is used. Previously, Telnet sessions were being lost during Stateful Failover.
- CSCdr91205  
Creates the **sysopt route dnat** command, which specifies that when an incoming packet does a route lookup, the incoming interface is used to determine which interface the packet should go to and what is the next hop.
- CSCdr91010  
On PIX Firewall, you can configure multiple **vpngroup** command statements when using certificates with the Cisco VPN 3000 Client. This can be done only when the name of the **vpngroup** command statement you specify on the PIX Firewall is the same as the Organizational Unit (OU) field of the certificate on the client. When PIX Firewall is processing the client's certificate, it uses the value of the OU field of the certificate to associate with the **vpngroup** command statement and uses that.

- CSCdr91002  
Multiple SMTP commands contained in a single packet are no longer permitted and are now dropped.
- CSCdr90259  
Uauth now shows the correct address specified by the **ip local pool** command when doing xauth with a VPN client. Previously, this problem noted that ISP assigned address appeared instead of the correct pool address.
- CSCdr90153 and CSCdr87363  
Stateful Failover now supports the **nat 0 access-list** command.
- CSCdr88834  
Specifying an **outbound** command *list\_ID* greater than 1599 no longer causes a crash. The maximum *list\_ID* value is now 1599.
- CSCdr83692  
The **write standby** command now clears the configuration of the Secondary unit and its ARP table. The Active unit then sends each configuration command to the Secondary unit. While sending the commands to synchronize the two configurations, the failover IP addresses are now temporarily disabled (set to 0.0.0.0), which prevents the previous condition that when syslog was enabled, the Secondary unit would ARP for the syslog server and cause confusion on the network.
- CSCdr81757  
PIX Firewall now polls the CRL during ISAKMP negotiation to determine if the CRL has expired.
- CSCdr81437  
The embryonic connection count no longer underflows during Stateful Failover.
- CSCdr80161  
The **inbound** and **outbound** options to the **aaa** command are restricted to first and second interfaces only.
- CSCdr78688  
PIX Firewall now supports up to 14,000 **outbound** command statements in a configuration.
- CSCdr75864  
Syslog message PIX-5-304001 now displays a username. The format of this message is as follows:  
`%PIX-5-304001: user src_addr Accessed JAVA URL|URL dest_addr: url.`
- CSCdr73112  
The **tracert** command now displays hops beyond the PIX Firewall when using PAT.
- CSCdr69366  
PIX Firewall no longer incorrectly NATs embedded IP addresses with a network **static** command statement.
- CSCdr69195  
PIX Firewall no longer fails with an assertion error when 50 or more IPSec static peers are configured. In this case, each peer was configured with individual ISAMKP keys, ISAKMP policies, transform sets, and lines to match address access-lists.

- CSCdr69061  
SIP uses three signaling ports, which caused problems for SIP UDP signaling. SIP can also use TCP, but the problems and solutions only apply to UDP signaling. Normally, SIP with UDP has a configurable timer set by default to 30 minutes. This caused the database and signaling connections to remain until this timer expired.  
  
A new timer and flag were added for transient connections, so that a connection will now time out and be closed in 1 minute when the media ports are assigned and connections are made either in the 183 ringing message or the 200 OK response message.  
  
The call is then moved to the active state and the connection address is saved in the database at this time. When the terminating message arrives on a different connection, the active connection address will be retrieved from the database and the UDP flag will be changed on this connection to the transient flag.
- CSCdr69009  
The ISAKMP lifetime specified on the Cisco VPN 3000 Concentrator series is ignored whether or not the group name is defined on the PIX Firewall. When the Cisco VPN 3000 Client starts a connection without a group ID name (no split tunneling), the ISAKMP timer expires and tries to rekey, when it actually should be ignored and not used.
- CSCdr66278  
Disconnecting the Cisco VPN 3000 Client deletes IPsec SAs on the PIX Firewall.
- CSCdr66129  
The **failover poll seconds** command provides a user-definable failover polling timer.
- CSCdr65059  
PIX Firewall now provides NAT for embedded outside DNAT address in H.225.
- CSCdr63034  
The **no ca identity nickname** command now clears the CRL list.
- CSCdr62751  
The performance of the **fixup** command has been improved.
- CSCdr61892  
Added support for Cisco's proprietary RAS messages to let PIX Firewall interoperate with Cisco's gateways and gatekeepers.
- CSCdr57873  
If a hung Telnet session is killed with the **terminal monitor** command while syslog is enabled, PIX Firewall no longer reboots when a syslog message is sent.
- CSCdr57864 and CSCdr01706  
The **logging monitor** command used on a Telnet console session no longer hangs the console when the screen display pauses with More.
- CSCdr56877  
ISAKMP keys no longer display with the **show config** or **write terminal** commands. The keys now display as follows:  
  

```
isakmp key ***** address ip_addr netmask mask
```

- CSCdr54791  
The **failover active** command now works correctly when the PIX Firewall unit is equipped with FDDI network interfaces.
- CSCdr53808  
Dynamic hookups are now provided for the H.225 call signaling channel.
- CSCdr53799  
If, during an upgrade from version 5.1 to version 5.2, the PIX Firewall detects a version 5.1 **ca identity** cgi-bin path, it will automatically convert the path into the version 5.2 style cgi-bin path.
- CSCdr52802  
Accounting records for DNS now have the correct port number.
- CSCdr49214  
FDDI line protocol no longer resets to “down” after reloading the image.
- CSCdr43633  
PIX Firewall now permits URLs to be up to 1024 characters long.
- CSCdr43490  
When a pool of addresses set by the **ip local pool** command is empty, the following syslog message now appears:  

```
%PIX-4-404101: ISAKMP: Failed to allocate address for client from pool poolname
```
- CSCdr42787  
When the PIX Firewall unit is equipped with Gigabit Ethernet interfaces, the Standby unit in failover no longer fails after using the **clear config all** command.
- CSCdr41431  
PIX Firewall, when creating an IPsec tunnel, now copies the TOS fields from the incoming packets header into the header of the encrypted packet.
- CSCdr38688  
The **clear config** command formerly changed the default interface name from **PIX/intfn** to **intfn**. The caveat resolution now changes the default interface name to **intfn**.
- CSCdr17484

The **debug failover option** command now appears as follows:

```
tx      Failover cable xmit
rx      Failover cable receive
open    Failover device open
cable   Failover cable status
txdmp   Cable xmit message dump (serial console only)
rxdmp   Cable recv message dump (serial console only)
ifc     Network interface status trace
rxip    IP network failover packet recv
txip    IP network failover packet xmit
get     IP network packet received
put     IP network packet xmitted
verify  Failover message verify
switch  Failover Switching status
fail    Failover internal exception
fmsg    Failover message
```

- CSCdr15304  
Syslog message %PIX-3-106014 now correctly displays all information. Previously the message appeared with <> to indicate missing information:  

```
Deny inbound icmp src outside:192.168.8.10 dst <>:192.168.205.2 (type 0, code 0)
```
- CSCdr12538  
PIX Firewall no longer blocks JAVA applets when the **filter java** command is not enabled.
- CSCdp95072  
The **show tech-support** command now includes the **write terminal** command that shows the current configuration. The previous version used the **show config** command that listed the configuration stored in Flash memory.
- CSCdp94136  
Disabling and enabling the **vpdn** command to move access to another interface no longer requires rebooting the PIX Firewall.
- CSCdp93492  
PIX Firewall TACACS+ per-user idle and absolute timeouts now work correctly.
- CSCdp92050  
Boothelper can now TFTP through a gigabit interface.
- CSCdp87564  
Syslog message %PIX-6-602301 no longer is preceded with several linefeeds, which made this message unreadable on some syslog servers.
- CSCdp76529  
If two users try to authenticate at approximately same time, PIX Firewall no longer generates two syslog messages with the same username, even though the IP addresses logged correctly. Also, the **show uauth** command output no longer shows two entries with same username but different IP addresses.
- CSCdp68315  
AAA usernames are now limited to up to 30 characters and passwords are limited to up to 15 characters in length.
- CSCdp42625 and CSCdm71986  
PIX Firewall no longer crashes if a VeriSign CA is accessed without the **crloptional** parameter to the **ca conf** command.
- CSCdm68994  
Formerly, if you made a certificate enrollment request without having first generated your RSA keys, the enrollment request terminated with the following error message:  

```
%Error: router certificate exists.
```

  
The new error message is as follows:  

```
%Error: The signature public key is not found. Abort.  
Type help or '?' for a list of available commands.
```
- CSCdm60725  
PIX Firewall now rejects a received CA certificate if an incorrect fingerprint was entered.

- CSCdm37650  
The **names** command no longer intermittently disables after being configured.
- CSCdj36973  
To track usage among different subnets, you can specify multiple PATs. Before, only one PAT statement could be configured for each configuration.
- CSCdj30303  
To specify PAT using the IP address at the interface, specify the **interface** keyword.  
**global interface id address | interface**

## Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN 3000 documentation at the following sites:

[http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_technical_documentation.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod_technical_documentation.html)

Cisco provides PIX Firewall technical tips at the following site:

[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

### Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

### Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered Network* logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

Copyright © 2000-2001, Cisco Systems, Inc.  
All rights reserved.