



Release Notes for the Cisco PIX Firewall Version 5.2(3)

October 2000

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



Note

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.



Introduction

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

System Requirements

The sections that follow list the system requirements for operating a Cisco 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.

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

If you use IKE Mode Config with the PIX Firewall, any routers on the IPSec connection must run Cisco 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 site:

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 Manager and Client Interoperability

PIX Firewall version 5.2 requires Cisco VPN 3000 Client version 2.5 or later and Cisco VPN 3000 Concentrator Manager 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)f. Refer to the *PIX Firewall Manager Release Notes, Version 4.3(2)f* for more information. You can view this document online at the following site:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note09186a008008c1d1.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>

New and Changed Information

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 and Configuration 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 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 Secure Intrusion Detection System (Cisco Secure 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 10.1.1.1/16 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 10.1.1.1 255.255.255.0
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 sites 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 site:

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

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

<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 site:

<http://www.openssh.com>

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

<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 site:

<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 web sites 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:

- **dhcpcd**—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 Secure 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 packetdetailerror** options—Displays detailed information about the DHCP lease.
- **debug** command, **dhcpcd packetevent** 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 an interface.
- **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 Manager

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

- The Cisco VPN 3000 Concentrator Manager 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 Manager. 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 Manager, 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](http://www.cisco.com/cisco.com) to view additional caveat information. You can access this tool at the following site:

http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml

Open Caveats - Release 5.2

- CSCds26054
SSH and failover are not supported for use together in version 5.2. If used together, an RSA key created before failover will not appear on the Standby unit after failover occurs.
- 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 Manager series ignores all keepalive messages originating from the PIX Firewall unit.
- CSCdr75706
PIX Firewall/Cisco VPN 3000 Concentrator Manager: 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.
- CSCdr68251
Port numbers are not appearing in syslog when using ACL.

- 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 Manager, only supports a limited number of IPSec transform sets. The Cisco VPN 3000 Concentrator Manager 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 Secure 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.
- CSCdr15304
The following syslog message incorrectly displays a field as “<>”:

```
%PIX-3-106014: Deny inbound icmp src outside:IP_addr dst <>:IP_addr (type 0, code 0)
```
- CSCdr04004
Small ARP timeouts cause short periods of packet loss.
- 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(3)

- 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)

- 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 PM 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 ISAKMP 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 Manager 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
txdump  Cable xmit message dump (serial console only)
rxdump  Cable rcv message dump (serial console only)
ifc     Network interface status trace
rxip    IP network failover packet rcv
txip    IP network failover packet xmit
get     IP network packet received
put     IP network packet xmitd
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/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

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

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

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

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.

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
- 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
- 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.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQuick Study, iQ Readiness Scorecard, The iQ Logo, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document/website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0008R)

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

