



Cisco PIX Firewall Release Notes Version 6.3(2)

July 2003

Contents

The PIX Firewall Version 6.3(2) software release was deferred, for more information refer to, “[Important Notes](#)” section in this document. This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [Important Notes, page 20](#)
- [Caveats, page 22](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation and Submitting a Service Request, page 25](#)

Introduction

The PIX Firewall delivers unprecedented levels of security, performance, and reliability, including robust, enterprise-class security services such as the following:

- Stateful inspection security, based on state-of-the-art Adaptive Security Algorithm (ASA)
- Over 100 predefined applications, services, and protocols for flexible access control
- Virtual Private Networking (VPN) for secure remote network access using IKE/IPSec standards
- Intrusion protection from over 55 different network-based attacks
- URL filtering of outbound web traffic through third-party server support
- Network Address Translation (NAT) and Port Address Translation Support (PAT)

Additionally, PIX Firewall Version 6.3 software supports Cisco PIX Device Manager (PDM) Version 3.0 and adds enhancements to features introduced in earlier releases.



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

System Requirements

The sections that follow list the system requirements for operating a PIX Firewall with Version 6.3 software.

Memory Requirements

The PIX 501 has 16 MB of RAM and will operate correctly with Version 6.1(1) and higher, while all other PIX Firewall platforms continue to require at least 32 MB of RAM (and therefore are also compatible with version 6.1(1) and higher).

In addition, all units except the PIX 501 and PIX 506E require 16 MB of Flash memory to boot. (The PIX 501 and PIX 506E have 8 MB of Flash memory, which works correctly with Version 6.1(1) and higher.)

Table 1 lists Flash memory requirements for this release.

Table 1 Flash Memory Requirements

PIX Firewall Model	Flash Memory Required in Version 6.3
PIX 501	8 MB
PIX 506E	8 MB
PIX 515/515E	16 MB
PIX 520	16 MB (Some PIX 520 units may need a memory upgrade because older units had 2 MB, though newer units have 16 MB)
PIX 525	16 MB
PIX 535	16 MB

Use the PIX-1GE-66 card in systems with a 64-bit/66 MHz PCI bus; for example, in a PIX 535. (If you use the PIX-1GE-66 cards in a PIX Firewall, the system RAM should be at least 128 MB.) For a PIX Firewall with only a 32-bit/33 MHz bus, such as the PIX 520 and PIX 525, use the PIX-1GE card.

Software Requirements

Version 6.3 requires the following:

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 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 Auto Update, IPSec, SSH, PDM, or VPN features or commands, you must have a new 56-bit DES activation key. Before getting a new activation key, write down your old key in case you want to retrograde to Version 4. You can have a new 56-bit DES activation key sent to you by completing the form at the following website:

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

3. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to “[Upgrading to a New Software Release](#)” for new installation requirements.

Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum configuration file size limit is increased to 2 MB for PIX Firewall software Versions 5.3(2) and later. For other PIX Firewall platforms, the maximum configuration file size limit is 1 MB. Earlier versions of the PIX 501 are limited to a 256 KB configuration file size. If you are using PIX Device Manager (PDM), we recommend no more than a 100 KB configuration file because larger configuration files can interfere with the performance of PDM on your workstation.

While configuration files up to 2 MB are now supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as **write term** and **show conf**
- Failover (the configuration synchronization time)
- During a system reload

The optimal configuration file size for use with PDM is less than 100 KB (which is approximately 1500 lines). Please take these considerations into account when planning and implementing your configuration.

Cisco VPN Software Interoperability

Cisco VPN Series	Interoperability Comments
Cisco IOS Routers	PIX Firewall Version 6.3 requires Cisco IOS Release 12.0(6)T or higher running on the router when using IKE Mode Configuration on the PIX Firewall.
Cisco VPN 3000 Concentrators	PIX Firewall Version 6.3 requires Cisco VPN 3000 Concentrator Version 2.5.2 or higher for correct VPN interoperability.

Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco Secure VPN Client v1.x	PIX Firewall Version 6.3 requires Cisco Secure VPN Client Version 1.1. Cisco Secure VPN Client Version 1.0 and 1.0a are no longer supported.
Cisco VPN Client v3.x (Unified VPN Client Framework)	PIX Firewall Version 6.3 supports the Cisco VPN Client Version 3.x that runs on all Microsoft Windows platforms. It also supports the Cisco VPN Client Version 3.5 or higher that runs on Linux, Solaris, and Macintosh platforms.

Cisco Easy VPN Remote Interoperability

Cisco Easy VPN Remote	Interoperability Comments
PIX Firewall Easy VPN Remote v6.3	PIX Firewall software Version 6.3 Cisco Easy VPN Server requires PIX Firewall software Version 6.3 Easy VPN Remote.
VPN 3000 Easy VPN Remote v3.6	PIX Firewall software Version 6.3 Cisco Easy VPN Server requires the VPN 3000 Version 3.6 Easy VPN Remote that runs on the VPN 3002 platform.
Cisco IOS Easy VPN Remote Release 12.2(16.4)T	PIX Firewall software Version 6.3 Cisco Easy VPN Server interoperates with Cisco IOS 806 Easy VPN Remote Release (16.4)T.

Cisco Easy VPN Server Interoperability

Cisco Easy VPN Server	Interoperability Comments
PIX Firewall Easy VPN Server v6.3	PIX Firewall software Version 6.3 Cisco Easy VPN Remote requires a PIX Firewall Version 6.3 Easy VPN Server.
VPN 3000 Easy VPN Server v3.6.7	PIX Firewall software Version 6.3 Cisco Easy VPN Remote requires VPN 3000 Version 3.6.7 Easy VPN Server.
Cisco IOS Easy VPN Server Release 12.2(15)T	PIX Firewall software version 6.3 Cisco Easy VPN Remote works with Cisco IOS Release 12.2(15)T Easy VPN Server in IKE pre-shared authentication and does not work with certificate. It is expected to interoperate using certificate, after CSCea02359 and CSCea00952 resolved and integrated in later versions of Cisco IOS Easy VPN Server.

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 user account, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

New and Changed Information

New Features in Release 6.3(2)

The new features in Release 6.3(2) are:

- [Policy NAT, page 5](#)
- [Ability to Configure TFTP Fixup, page 6](#)
- [DNS Fixup, page 6](#)
- [MIB Support, page 6](#)
- [Support for Instant Messaging Using SIP, page 6](#)
- [Enhanced Show Failover Command, page 7](#)
- [Incomplete Crypto Map Enhancements, page 7](#)
- [Infinite Isakmp Phase 1 Lifetime Support, page 7](#)
- [Enhanced Show Version Command, page 7](#)
- [Per-user-override, page 8](#)
- [Enhanced Fixup Protocol Command, page 8](#)
- [Enhanced aaa proxy-limit, page 8](#)

Policy NAT

PIX Firewall Version 6.3(2) introduces Policy Network Address Translation (NAT). Policy NAT allows you to identify both the source and destination addresses in an access list when specifying the local traffic to translate. This feature lets you use different global addresses for each source and destination pair on an interface, even if the source address is the same for each pair. Without policy NAT, you can only specify a single global address for a given source address, because the destination address is not considered. To configure policy NAT, use either the **static** or **nat** commands.

For configuration information, refer to “Policy NAT” or “Enabling Server Access with Static NAT” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax, refer to the *Cisco PIX Firewall Command Reference*.

Ability to Configure TFTP Fixup

Ability to configure TFTP fixup inspects the TFTP protocol and dynamically creates connection and xlate, if necessary, to permit file transfer between a TFTP client and server. Specifically, the fixup inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).



Note

TFTP Fixup is enabled by default. TFTP Fixup must be enabled if static PAT is used to redirect TFTP traffics.

For more information on this feature, refer to “TFTP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

DNS Fixup

The **[no] fixup protocol dns [maximum-length <512-65535>]** command can be used to enable/disable the DNS fixup.

Based on this maximum-length configured by the user, the DNS fixup checks to see if the DNS packet length is within this limit. Every UDP DNS packet (request/response) undergoes the above check.



Note

The PIX Firewall drops DNS packets sent to UDP port 53 that are larger than the configured maximum length. The default value is 512 bytes.

This feature is added to the **fixup protocol** command in the PIX Firewall Version 6.3(2) software. For configuration information, refer to “DNS” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.



Note

If DNS fixup is disabled, the Address record (A-record) is not NATed and the DNS ID is not matched in requests and responses. By disabling DNS fixup, the maximum length check on UDP DNS packets is bypassed and packets greater than the maximum length configured are permitted.

MIB Support

PIX Firewall Version 6.3(2) adds support to the following additional interface objects of MIB-II:

- ifOutQLen
- ifInUnknownProtos
- ifLastChange

For more information, refer to “MIB Support” in the *Cisco PIX Firewall and VPN Configuration Guide*.

Support for Instant Messaging Using SIP

Fixup SIP now supports the Instant Messaging (IM) Chat feature on Windows XP using Windows Messenger RTC Client version 4.7.0105 only.

This feature support is added to the PIX Firewall Version 6.3(2) software. For more information, refer to “SIP” in the *Cisco PIX Firewall and VPN Configuration Guide*.

Enhanced Show Failover Command

This new feature enhances the **show failover** command to display the last occurrence of a failover.

For more information on this feature, refer to “Using the Failover Command” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Incomplete Crypto Map Enhancements

Every static crypto map must define an access list and an IPsec peer. If either is missing, the crypto map is considered incomplete and a warning message is printed. Traffic not matched to a complete crypto map is skipped, and the next entry is tried. Failover hello packets are now exempt from the incomplete crypto map check; previously they were dropped. Use the **show conf** command to ensure that every crypto map is complete.

For more information on this feature, refer to “Crypto Maps” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Infinite Isakmp Phase 1 Lifetime Support

Infinite isakmp phase 1 lifetime is a feature that allows interoperability with third party VPN vendor gateways that do not support rekeying of the IKE phase 1 SA. To enable it, specify a lifetime value of 0 using the isakmp policy command.



Note

Using infinite phase 1 SA lifetime is relatively less secure, because the phase 1 keys are not periodically refreshed as they normally would otherwise be. Do not enable this feature unless the PIX must communicate with a third party VPN gateway device that cannot be configured with a finite phase 1 SA lifetime.

For more information on this feature, refer to “Internet Key Exchange (IKE)” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced Show Version Command

The 'show ver' output now has two interface-related lines, Max Physical interfaces and Max interfaces. Max interfaces is the total physical and virtual interfaces. Following is an example of the output:

```
pix-1(config)# sh ver

Cisco PIX Firewall Version 6.3(2)

Compiled on Tue 08-Jul-03 10:56 by dramnath

dramnath-pix-1 up 2 hours 51 mins

Hardware: PIX-515, 32 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xffffd8000, 32KB

0:ethernet0:address is 0003.e300.1552, irq 10
1:ethernet1:address is 0003.e300.1553, irq 7
```

```

2:ethernet2:address is 0090.273a.1611, irq 11
Licensed Features:
Failover:                Disabled
VPN-DES:                 Enabled
VPN-3DES-AES:           Enabled
Maximum Physical Interfaces:3
Maximum Interfaces:     5
Cut-through Proxy:      Enabled
Guards: Enabled
URL-filtering:          Enabled
Inside Hosts:           Unlimited
Throughput:             Unlimited
IKE peers:              Unlimited

This PIX has a Restricted (R) license.

Serial Number:5 (0x5)
Running Activation Key:0x2b2bcadc 0xbff80f39 0x71c6c743 0xa06ee021
Configuration last modified by enable_15 at 20:14:25.505 UTC Thu Jul 24 2003
drammath-pix-1(config)#

```

For more information on this feature, refer to the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Per-user-override

This feature allows users to specify a new keyword per-user-override to the **access-group** command. When this keyword is specified, it allows the permit/deny status from the per-user access-list (downloaded via AAA authentication) that is associated to a user to override the permit/deny status from the access-group access-list.

For more information on this feature, refer to the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced Fixup Protocol Command

By default, the **fixup protocol ils** command is disabled. You can use the **fixup protocol** command to enable the ILS fixup and, optionally, change the default port assignment.

For more information on this feature, refer to “ILS and LDAP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced aaa proxy-limit

When the aaa proxy-limit is set to 16, the “aaa proxy-limit 16” line shows up. This feature specifies the number of concurrent proxy connections allowed per user, from 1 to 128. The default value is 16.

For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

New Features in Release 6.3(1)

This section includes the following topics:

- [Enterprise-Class Security Enhancements](#), page 9
- [Small Office, Home Office \(SOHO\) Enhancements](#), page 12
- [Security Fixups \(Application Inspection\) Enhancements](#), page 15
- [Management Enhancements](#), page 16
- [Serviceability Features](#), page 19

Enterprise-Class Security Enhancements

Virtual LAN (VLAN)-based virtual interfaces

802.1Q VLAN support comes to the PIX Firewall, providing added flexibility in managing and provisioning the firewall. This feature enables the decoupling of IP interfaces from physical interfaces (hence making it possible to configure logical IP interfaces independent of the number of interface cards installed), and supplies appropriate handling for IEEE 802.1Q tags.

VLAN feature support is added to the **interface** command in the PIX Firewall Version 6.3 software. For configuration information, refer to “Configuring PIX Firewall with VLANs” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.



Note

The PIX 501 and PIX 506/506E do not provide support for VLANs.

OSPF Dynamic Routing

Route propagation and greatly reduced route convergence times are two of the many benefits that arrive with Open shortest Path First (OSPF). The PIX Firewall implementation will support intra-area, inter-area and external routes. The distribution of static routes to OSPF processes and route redistribution between OSPF processes are also included.

To configure OSPF routing on the PIX Firewall, refer to “Configuring OSPF in the PIX Firewall” in the *Cisco PIX Firewall and VPN Configuration Guide*. The following new commands are added to the PIX Firewall Version 6.3 software to support OSPF routing: **routing interface**, **router ospf**, **route-map**, **prefix-list**, and so on. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.



Note

The PIX 501 does not provide support for OSPF.

Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy

This new feature extends the capabilities of PIX Firewall to securely authenticate HTTP sessions and adds support for HTTPS Authentication Proxy. To configure secure authentication for HTTP sessions, use the **aaa authentication secure-http-client** command. To configure HTTPS Authentication Proxy, use the **aaa authentication include https...** or the **aaa authentication include tcp/0...** commands.



Note

The https authentication sessions are enabled by default for Versions 6.3(1) and higher.

Refer to “Enabling Secure Authentication of Web Clients” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Local User Authentication Database for Network and VPN Access

This feature allows cut-through and VPN (using xauth) traffic to be authenticated using the PIX Firewall local username database (as an alternative in addition to the existing authenticating via an external AAA server).

The server tag variable now accepts the value LOCAL to support cut-through proxy authentication using Local Database. For example:

```
aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 LOCAL
crypto map outside_map client authentication LOCAL
```

For more information on this feature, refer to “User Authentication Using the LOCAL Database” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

HTTPS and FTP Web Request Filtering via Enhanced Websense Integration

This feature extends the existing Websense-based URL filtering to HTTPS and FTP.

The **filter ftp** and **filter https** commands were added to the **filter** command in the PIX Firewall Version 6.3 software. For information on configuring this command, refer to “Filtering HTTPS and FTP Sites” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Advanced Encryption Standard (AES)

This feature adds support for securing site-to-site and remote access VPN connections with the new international encryption standard. It also provides software-based AES support on all supported PIX Firewall models and hardware-accelerated AES via the new VAC+ card on select PIX Firewall Security Appliance models.

The **aes | aes-192 | aes-256** option is added to the **isakmp policy encryption** command in PIX Firewall Version 6.3 software. To configure this command, refer “Configuring IKE” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Support for VPN Accelerator Card+ (VAC+)

PIX Firewall Version 6.3 adds support for the VAC+. VAC+ provides high-speed tunneling and encryption services for Virtual Private Network (VPN) remote access, and site-to-site intranet and extranet applications. The VAC+ is supported on any chassis that runs the Version 6.3 software, has an appropriate license to run VPN software, and has at least one PCI slot available.

For more information on the **show crypto interface [counters]** command, and a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

VPN NAT Traversal

This feature extends support for site-to-site and remote access IPsec-based VPNs to network environments that implement Network Address Translation (NAT) or Port Address Translation (PAT), such as airports, hotels, wireless hot spots, and broadband environments

This feature is added to the **isakmp nat-traversal** command in PIX Firewall Version 6.3 software. To configure this command, refer to “Using NAT Traversal” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

DHCP Server Support on Multiple Interfaces

PIX Firewall Version 6.3 allows as many integrated Dynamic Host Configuration Protocol (DHCP) servers to be configured as desired, and on any interface. DHCP client can be configured only on the outside interface, and DHCP relay agent can be configured on any interface. However, DHCP server and DHCP relay agent cannot be configured concurrently on the same PIX Firewall, but DHCP client and DHCP relay agent can be configured concurrently.

The **[no] dhcpd address ip1[-ip2] if_name** feature now allows dhcp servers to be configured as desired on any interface in the PIX Firewall Version 6.3 software. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Diffie-Hellman (DH) Group 5 Support

PIX Firewall Version 6.3 adds support for 1536-bit MODP Group that has been given the group 5 identifier.

Use the **isakmp policy group** command to specify the Diffie-Hellman group to be used in an IKE policy. To configure this command, refer to “Configuring IKE” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Verify Certificate Distinguished Name

This feature enables PIX Firewalls acting as either a VPN peer, site-to-site, or as an Easy VPN Remote (VPN Hardware Client) to validate that the Easy VPN Server or the other VPN Peer provides a certificate that matches an administrator specified criteria.

This feature was added to the **ca verifycertdn** command in PIX Firewall Version 6.3 software. To configure this command, refer to “Client Verification of the Easy VPN Server Certificate” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Cryptographic Engine Known Answer Test (KAT)

The function of KAT is to test the instantiation of the PIX Firewall crypto engine. The test will be performed every time during the PIX Firewall boot up before the configuration is read from Flash memory. KAT will be run for valid crypto algorithms for the current license on the PIX Firewall. KAT can also be run from the command line in privileged mode, using the **show crypto engine verify** command.

The **show crypto engine verify** command was added to the PIX Firewall Version 6.3 software. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Media Access Control (MAC) Based Authentication

This feature allows hosts to be exempted from a broader authentication requirement, based on their MAC addresses. This is essential for devices like printers and IP phones located inside a firewall.

The **mac-list**, **aaa mac-exempt match <mac-list-id>** and **vpnclient mac-exempt <mac-add_1> <mac_mask_1> [<mac_addr_2> <mac_mask_2>** commands are new commands. To configure this command on the PIX Firewall, refer to “Using MAC-Based AAA Exemption” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Small Office, Home Office (SOHO) Enhancements

DHCP Relay

Acting as a DHCP relay agent, the PIX Firewall can assist in dynamic configuration of IP hosts on any of its interfaces. It receives requests from hosts on a given interface and forwards them to a user-configured DHCP server on another interface. This can work in conjunction with sit- to-site or Easy VPN, enabling businesses to centrally manage their IP address.

To support this feature, the **dhcprelay** command was added to PIX Firewall Version 6.3 software. For more information on the **dhcprelay** command, refer to “DHCP Relay” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

PAT for ESP

PIX Firewall Version 6.3 provides the ability to PAT IP protocol 50 to support single IPSec user outbound access.

To support this feature, the **fixup protocol esp-ike** command was added to PIX Firewall Version 6.3 software. For more information on this command, refer to “IPSec” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Increased Firewall Performance on the PIX 501 and PIX 506E Security Appliances

PIX Firewall Version 6.3 unleashes new performance levels on the PIX 501 and PIX 506E, delivering up to six times more performance than previous software releases.

Increased Number of IPsec VPN Peers Supported on the PIX 501 Security Appliance

PIX Firewall Version 6.3 increases number of site-to-site and remote access VPN peers supported on the PIX 501 from 5 to 10, enabling greater VPN scalability in small office, home office (SOHO) environments.

Unlimited User License for the PIX 501 Security Appliance

With PIX 6.3, you can purchase or upgrade to an “Unlimited User License” for the PIX 501 which does not limit the hosts on the inside of the network that leverage applicable PIX resources. The Unlimited User License also increases the DHCP Server pool size to 256 addresses. Updates have also been made to ensure that the default factory configuration considers the PIX 501 User license installed in the device.

Easy VPN Server Load Balancing Support

The PIX Firewall VPN hardware client can participate in cluster-based concentrator load balancing. It supports VPN 3000 Series Concentrator load balancing with automatic redirection to the least utilized concentrator.

For more information on this command, refer to “Enabling Redundancy” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Dynamic Downloading of Backup Easy VPN Server Information

Support for downloading a list of backup concentrators defined on the head-end.

The `vpngroup group_name backup-server {{ip1 [ip2 ... ip10]} | clear-client-cfg}` command is a new command added to the PIX Firewall Version 6.3 software. For more information on this command, refer to “Enabling Redundancy” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Easy VPN Internet Access Policy

PIX Firewall Version 6.3 changes the behavior of a PIX Firewall used as an Easy VPN Remote device in regard to Internet access policy for users on the protected network. The new behavior occurs when split tunneling is enabled on the Easy VPN Server. Split tunneling is a feature that allows users connected through the PIX Firewall to access the Internet in a clear text session, without using a VPN tunnel.

The PIX Firewall used as an Easy VPN Remote device downloads the split tunneling policy and saves it in its local Flash memory when it first connects to the Easy VPN Server. If the policy enables split tunneling, users connected to the network protected by the PIX Firewall can connect to the Internet regardless of the status of the VPN tunnel to the Easy VPN Server.

For information about configuring the split tunneling policy on a PIX Firewall used as an Easy VPN Remote Server, refer to Chapter 8, “Managing VPN Remote Access,” in the *PIX Firewall and VPN Configuration Guide*.

Custom Backup Concentrator Timeout

This feature constitutes a configurable time out on the PIX Firewall connection attempts to a VPN headend, thereby controlling the latency involved in rolling over to the next backup concentrator on the list.

This feature is added to the **vpngroup** command in PIX Firewall Version 6.3 software. For more information on this command, refer to “Enabling Redundancy” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Easy VPN X.509 Certificate Support

X.509 certificates are used to access secure network systems. Users obtain certificates so they can identify themselves, present their access credentials, and obtain a secure network connection with other approved secure users or systems.

For more information on this command, refer to “Using X.509 Certificates” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Flexible Easy VPN Management Solutions

In PIX Firewall Version 6.3, managing the PIX Firewall using the outside interface will not require the traffic to flow over the VPN tunnel. You will have the flexibility to require all NMS traffic to flow over the tunnel or fine tune this policy.

This feature was added to the **vpnclient management** command in the PIX Firewall Version 6.3 software. For configuration information, refer to “Controlling Remote Administration” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

User-Level Authentication

Support for individually authenticating clients (IP address based) on the inside network of the VPN hardware client. Both static and One Time Password (OTP) authentication mechanisms are supported. This is done through a web-based interface.

This new feature was added to the **vpngroup** command in PIX Firewall Version 6.3 software. For more information on this command, refer to “Using Authentication and Authorization” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Secure Unit Authentication

This feature provides the ability to use dynamically generated authentication credentials to authenticate the Easy VPN Remote (VPN Hardware Client) device.

The secure-unit-authentication feature is added to the **vpngroup** command in the PIX Firewall Version 6.3 software. For configuration information, refer to “Using Secure Unit Authentication” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.

Easy VPN Web Interface for Manual Tunnel Control User Authentication and Tunnel Status

With the introduction of the User-Level Authentication and Secure Unit Authentication, features the PIX Firewall delivers the ability to enter the credentials, connect/dis-connect the tunnel and monitor the connection using new web pages served to users when attempting access to the VPN tunnel or unprotected networks through the PIX Firewall. This is only applicable to the Easy VPN Remote feature.

For configuration information, refer to “Connecting to PIX Firewall Over a VPN Tunnel” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new feature, refer to the *Cisco PIX Firewall Command Reference*.

Security Fixups (Application Inspection) Enhancements

PPTP Fixup

This feature lets point-to-Point Tunneling Protocol (PPTP) traffic traverse the PIX Firewall when configured for PAT, performing stateful PPTP packet inspection in the process.

To configure PPTP Fixup on the PIX Firewall, refer to “PPTP Configuration” in the *Cisco PIX Firewall and VPN Configuration Guide*. The **fixup protocol pptp 1723** command configures PPTP Fixup. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

H.323 Version 3 and 4 Support

With PIX Firewall Version 6.3, the PIX Firewall will support NAT and PAT for H.323 versions 3 and 4 messages, and in particular, the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

This feature is added to the **fixup protocol h.323** command in the PIX Firewall Version 6.3 software. For more information on this command, refer to “H.323” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

CTIQBE Fixup

Known also as TAPI/JTAPI Fixup, this feature incorporates a Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol inspection module that supports NAT, PAT, and bi-directional NAT. This enables Cisco IP SoftPhone & other Cisco TAPI/JTAPI applications to work and communicate successfully with Cisco CallManager for call setup and voice traffic across the PIX Firewall.

This feature is added to the **fixup protocol ctiqbe 2748** command in the PIX Firewall Version 6.3 software. For more information on this command, refer to “Voice over IP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

MGCP Fixup

PIX Firewall Version 6.3 adds support for Media Gateway Control Protocol (MGCP) 1.0, enabling messages between Call Agents and VoIP media gateways to pass through the PIX Firewall in a secure manner.

To configure the **fixup protocol mgcp** command, refer to “Configuration for Multiple Call Agents and Gateways” in the *Cisco PIX Firewall and VPN Configuration Guide*. The following new commands are added to the PIX Firewall Version 6.3 software to support this new command: **debug mgcp**, **fixup protocol mgcp**, and so on. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

PAT for Skinny

This feature allows Cisco IP Phones to communicate with Cisco CallManager across the PIX Firewall when it is configured with PAT. This is particularly important in a remote access environment where Skinny IP phones behind a PIX Firewall talk to the CallManager at the corporate site through a VPN.

This feature is added to the **fixup protocol skinny** command in the PIX Firewall Version 6.3 software. For more information on this command, refer to “SCCP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Configurable SIP UDP Fixup

This provides a CLI-enabled solution for non-Session Information Protocol (SIP) packets to pass through the PIX Firewall instead of being dropped when they use a SIP UDP port (note that SIP UDP Fixup itself has been available since PIX Firewall Version 5.2).

This feature is added to the **fixup protocol sip udp** command in the PIX Firewall Version 6.3 software. For more information on this command, refer to “SIP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Fixup Protocol ICMP Error

PIX Firewall Version 6.3 introduces the ability to NAT ICMP error messages.

The **icmp error** feature was added to the **fixup protocol** command in the PIX Firewall Version 6.3 software. For information on configuring this feature, refer to “ICMP” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Management Enhancements

ACL Editing

The Access Control List (ACL) editing feature provides users flexibility to insert or delete any access list element in an access list. The access list, with line numbers, will be shown with the **show access-list <access-list-id>** command and not with the **show running-config** command or **write terminal** command.

The **line line-num** feature was added to the **access-list** command in the PIX Firewall Version 6.3 software. For information on configuring this feature, refer to “Enabling Inbound Connections” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Syslog by ACL Entry

This feature allows users to configure a specific Access Control List (ACL) entry with a logging option. When such an option is configured, statistics for each flow that matches the permit or deny conditions of the ACL entry are logged.

To configure the log option in the **access-list** command on the PIX Firewall, refer to “Logging Access Control List Activity” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.

Assignable Syslog Levels by Message

PIX Firewall Version 6.3 includes the ability to reassign the level of any syslog, allowing easy grouping of syslogs of interest.

The *level* option in the **logging** command is added to the PIX Firewall Version 6.3 software. For more information on this command, refer to “Enabling Logging to Syslog Servers” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Custom Logging Identifier

Allows a custom firewall identifier to be selected, such as an interface IP address, that will be included in all syslog messages to improve the centralized reporting of firewall events.

This new feature is added to the **logging** command. For configuration information, refer to “Enabling Logging to Syslog Servers” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.

Cisco Logging Format

This feature will help users to log messages in Cisco EMBLEM format to a syslog server. The EMBLEM format is available for both messages with and without timestamp.

This new feature is added to the **logging** command. For configuration information, refer to “Enabling Logging to Syslog Servers” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.

Comments/Remarks in Access Control Lists (ACLs)

This feature allows users to include comments in access lists to make the ACL easier to understand and scan.

To configure the **access-list id [line line-num] remark text** command, in the **access-list** command, refer to “Enabling Inbound Connections” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Interface Name as Address in ACLs

Users running the DHCP client on the PIX Firewall outside interface will no longer have to adjust their access lists every time the outside DHCP address is changed by their ISP.

The **interface** *if_name* command was added to the PIX Firewall Version 6.3 software. For information on configuring this feature, refer to “Enabling Inbound Connections” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Custom Administrative Access Banner Messages

Users will be able to configure a message-of-the-day (motd), a login, and an exec banner that will be presented to users who access the PIX Firewall via the console, SSH, and Telnet.

To configure the **banner** command, refer to “Configuring PIX Firewall Banners” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Console Connection Inactivity Timeout

Protects console from unauthorized administrative access by automatically logging out sessions after a configurable period of inactivity

The **console** command is a new command added to the PIX Firewall Version 6.3 software. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

show Command Output Filter

This feature provides the ability to filter or search through the full output of **show** commands.

For information on the **show command_keywords** [*l* {**include** | **exclude** | **begin** | **grep** [-v]} *regex*] command, refer to Chapter 1, “Getting Started” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Remote Management Enhancements

This feature enables administrators to remotely manage firewalls over a VPN tunnel using the inside interface IP address of the remote PIX Firewall. In fact, administrators can define any PIX Firewall interface for management-access. This feature supports PDM, SSH, Telnet, SNMP, and so on, that requires a dynamic IP address. This feature significantly benefits broadband environments.

The **management-access** command is a new command added to the PIX Firewall Version 6.3 software. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced show version Command

The output of the **show version** command is enhanced to display additional information.

For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Increase Length of the PIX Firewall Host Name

Change the maximum allowed length of the host name to 63 characters. Change the maximum allowed length of the domain name from 64 to 63. This limits the maximum fully qualified domain name (plus terminating 0) to 127 bytes.

This new feature is added to the **hostname** command in the PIX Firewall Version 6.3 software. For configuration information, refer to “Using IKE with Pre-Shared Keys” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for these new commands, refer to the *Cisco PIX Firewall Command Reference*.

Serviceability Features

Stack Trace in Flash Memory

This feature enables the stack trace to be stored in non-volatile Flash Memory, so that it can be retrieved at a later time for debug/troubleshooting purposes.

The **crashinfo** command is a new command added to the PIX Firewall Version 6.3 software. For more information on this new command, refer to “Saving Crash information to Flash Memory” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced show tech Command

This feature enhances the current **show tech** command output to include additional diagnostic information.

For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced debug Command and Support

These commands turn off all active debugs at once, and restore the PIX Firewall to normal operation.

The no **debug all**, **undebg all**, **debug arp**, **crypto vpnclient**, **debug aaa [authentication | authorization| accounting | internal]** commands were added to the **debug** command in the PIX Firewall Version 6.3 software. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Modification to GE Hardware Speed Settings

Modification to GE Hardware Speed Settings - Half duplex option removed. The Gigabit Ethernet cards can be configured by hardware in TBI or GMII mode. TBI mode does not support half duplex. GMII mode supports both half duplex and full duplex. All the i8255x controllers used in the PIX Firewalls are configured for TBI and thus cannot support half-duplex mode, hence the half-duplex setting is removed.

Enhanced arp Command

New features were added to the **arp** command in the PIX Firewall Version 6.3 software. For more information on this new command, refer to “Setting Default Routes” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

Enhanced capture Command

Users can now specify the **capture** command to store the packet capture in a circular buffer. The capture will continue writing packets to the buffer until it is stopped by the administrator.

For configuration information, refer to “Capturing Packets” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new feature, refer to the *Cisco PIX Firewall Command Reference*.

Important Notes

Important Notes in Release 6.3(2)

- PIX Version 6.3(2) software was deferred to fix the Network Address Translation (NAT) caveat. When NAT ID 0 translation rules are configured on a PIX Version 6.3(2), they are executed but are not displayed in the running or startup configurations. If the running configuration is copied to Flash the NAT 0 translation rules are not copied. After the PIX is rebooted, all NAT 0 translation rules disappear completely from the box and no NAT 0 translations takes place. This blocks the traffic that relied on those translation rules making the traffic unable to traverse the PIX Firewall. For more information, refer to “Establishing Outbound Connectivity with NAT and PAT” in the *Cisco PIX Firewall and VPN Configuration Guide*.

NAT 0 translation rules function properly if entered new on a PIX Version 6.3(2), even if they do not appear in the running or startup configurations. You can re-enter the NAT 0 translation rules to systems that lost their NAT 0 translation rules after rebooting, these are retained and executed upon the next reboot. Other options include upgrading to Version 6.3(3) or downgrading to Version 6.3(1). For more information on upgrading or downgrading to or from a previous version go to the *Cisco PIX Firewall and VPN Configuration Guide*.

- Future versions of the PIX Firewall software will not support conduits and outbounds.

Important Notes in Release 6.3

This section describes important notes for Version 6.3.

Interface Settings on the PIX 501 and PIX 506E

With the PIX Firewall Version 6.3, the settings for the following interfaces have been updated as follows:

- PIX 501 outside interface (port 0) - 10/100 Mbps half or full duplex
- PIX 501 inside interface - 10/100 Mbps half or full duplex

- PIX 506E inside interface - 10/100 Mbps half or full duplex
- PIX 506E outside interface - 10/100 Mbps half or full duplex

**Note**

When upgrading the PIX 501 to Version 6.3, the inside interface is automatically upgraded to 100 Mbps full duplex. During the upgrade process the system displays the message “ethernet1 interface can only be set to 100full.”

Upgrading the PIX 506 and the PIX 515

When upgrading a classic PIX 506 or PIX 515 (the non “E” versions) to PIX Firewall OS Version 6.3, the following message(s) might appear when rebooting the PIX Firewall for the first time after the upgrade:

ethernet0 was not idle during boot.

ethernet1 was not idle during boot.

These messages (possibly one per interface) will be followed by a reboot. This is a one-time event and is a normal part of the upgrade on these platforms.

Easy VPN Remote and Easy VPN Server

The PIX 501 and PIX 506/506E are both Easy VPN Remote and Easy VPN Server devices. The PIX 515/515E, PIX 525, and PIX 535 act as Easy VPN Servers only.

The PIX 501 and PIX 506/506E can act as Easy VPN Remote devices or Easy VPN Servers so that they can be used either as a client device or VPN headend in a remote office installation. The PIX 515/515E, PIX 525, and PIX 535 act as Easy VPN Servers only because the capacity of these devices makes them appropriate VPN headends for higher-traffic environments.

PIX 535 Interfaces

These practices must be followed to achieve the best possible system performance on the PIX 535:

- PIX-1GE-66 interface cards should be installed first in the 64-bit/66 MHz buses before they are installed in the 32-bit/33 MHz bus. If more than four PIX-1GE-66 cards are needed, they may be installed in the 32-bit/33 MHz bus but with limited potential throughput.
- PIX-VACPLUS should be installed in a 64-bit/66 MHz bus to avoid degraded throughput.
- PIX-1GE and PIX-1FE cards should be installed first in the 32-bit/33 MHz bus before they are installed in the 64-bit/66 MHz buses. If more than five PIX-1GE and/or PIX-1FE cards are needed, they may be installed in a 64-bit/66 MHz bus but doing so will lower that bus speed and limit the potential throughput of any PIX-1GE-66 card installed in that bus.

The PIX-1GE Gigabit Ethernet adaptor is supported in the PIX 535; however, its use is strongly discouraged because maximum system performance with the PIX-1GE card is much lower than that with the PIX-1GE-66 card. The software displays a warning at boot time if a PIX-1GE is detected.

Table 2 summarizes the performance considerations of the different interface card combinations.

Table 2 Gigabit Ethernet Interface Card Combinations

Interface Card Combination	Installed In Interface Slot Numbers	Potential Throughput
Two to four PIX-1GE-66	0 through 3	Best
PIX-1GE-66 combined with PIX-1GE or just PIX-1GE cards	0 through 3	Degraded
Any PIX-1GE-66 or PIX-1GE	4 through 8	Severely degraded



Caution

The PIX-4FE and PIX-VPN-ACCEL cards can only be installed in the 32-bit/33 MHz bus and must never be installed in a 64-bit/66 MHz bus. Installation of these cards in a 64-bit/66 MHz bus may cause the system to hang at boot time.



Caution

If Stateful Failover is enabled, the interface card and bus used for the Stateful Failover LAN port must be equal to or faster than the fastest card used for the network interface ports. For example, if your inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then your Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. A PIX-1GE or PIX-1FE card cannot be used in this case, nor can a PIX-1GE-66 card be installed in bus 2 or share bus 1 with a slower card.

Caveats

The following sections describe the caveats for the 6.3 release.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:
<https://tools.cisco.com/Support/BugToolKit>

To become a registered cisco.com user, go to the following website:
<http://tools.cisco.com/RPF/register/register.do>

Open Caveats - Release 6.3(2)

Table 3 Open Caveats

ID Number	Software Release 6.3(2)	
	Corrected	Caveat Title
CSCdw04354	No	PIX needs to better handle incomplete authentications.
CSCea43211	No	Potential failure of TCP connection recovery scenario through PIX
CSCea94045	No	ID payload contains protocol 17 but port 0
CSCeb29981	No	PIX in failover mode with banner greater than 480 characters reloads
CSCeb67027	No	Intermittent assert when running OSPF and changing switch duplex.

Resolved Caveats - Release 6.3(2)

Table 4 Resolved Caveats

ID Number	Software Release 6.3(2)	
	Corrected	Caveat Title
CSCea28533	Yes	PIX ospf still advertises the network of shutdown interface
CSCea50882	Yes	PIX allocates more uauth_net objects than necessary.
CSCea52673	Yes	Cannot snmpwalk ipAddrTable using ucd-snmp on Linux
CSCeb60229	Yes	VLAN: Console session hangs when you remove VLAN int with NTP config
CSCea61756	Yes	PIX: Tracebacks in lu_rx thread when peer is running diff ver os
CSCea63999	Yes	IUA with SID in newpin mode on PIX (6.3.1) causes
CSCea64707	Yes	DHCPRelay fails if enable management-access inside
CSCea67630	Yes	Reporting Wrong Originating Caller ID when telnet/SSH into the PIX
CSCea67644	Yes	ospf disallows route w/ same dist, diff metric, diff intf
CSCea70416	Yes	after burst traffic, PIX need to be rebooted
CSCea70434	Yes	Inside to outside DNS server queries translated by PIX(6.3) w/static
CSCea71195	Yes	PIX515E to VPN3000 tunnel stops working after upgrading to 6.3.1
CSCeb71208	Yes	PIX traceback if user configures ospf if no ifx IP is configured
CSCea72383	Yes	PIX reloads with isakmp nat-traversal command
CSCea72691	Yes	NAT-T: Pkts not fwded, err msg, NATed tunnel to non-NATed tunnel
CSCea76209	Yes	SIP: Calls fail if it is not completed after 30 seconds using PAT
CSCea77177	Yes	standby pix reloads with OSPF configured in fover_parse
CSCea79747	Yes	SIP: content-length not modified if body is not SDP & is modified
CSCea81028	Yes	PIX EZVPN: IPsec doesn't work if headend is behind NAT device
CSCea82010	Yes	PIX reloads when you type in failover ip address <int>
CSCea82252	Yes	SIP: PIX does not open the sip_media conn via 180/183 with SDP.

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(2)	
	Corrected	Caveat Title
CSCea83595	Yes	SIP:PIX does not update xlate timer when receiving REGISTER
CSCea84806	Yes	PIX arp for deleted static after clear xlate
CSCea84861	Yes	TCP access will be denied and there is 602101 syslog message output
CSCea86451	Yes	SIP: sip_sessions should be deleted based on Expires:value
CSCea89724	Yes	Investigate sending a warning msg to CLI before making
CSCea89765	Yes	Keepalive/heartbeat do not pass thru PIX, due to incomplete vpn defn
CSCea90382	Yes	SIP: PIX doesn't open dynamic sip_media if call comes from outside
CSCea93797	Yes	PIX - Responds to ARP requests for IP Broadcast Address
CSCeb00027	Yes	Initial PPTP negotiation may fail with fixup pptp enabled
CSCeb01565	Yes	PIX reloads upon receipt of malformed IPSec/ESP packet -
CSCeb01994	Yes	PIX 6.3 password recovery does not remove local aaa
CSCeb02286	Yes	DHCPRA: reloads when release and renew ip address
CSCeb05297	Yes	PIX might reboot with many tunnels after issuing show vpdn
CSCeb06082	Yes	PIX doesn't respond to arps from secondary ip
CSCeb06362	Yes	SIP: transient connections not timing out after 1 minute
CSCeb08126	Yes	OSPF removes PPPoE generated default route
CSCeb11246	Yes	SIP: PIX does not open media when receiving Ack w/ SDP
CSCeb11274	Yes	SIP: PIX drop 200 OK from Transfer Target during Call
CSCeb12458	Yes	PPTP with EAP translation through PAT fails
CSCeb13380	Yes	max uauth queue len too short, users sporadically unable
CSCeb13449	Yes	SIP:PIX drop 202 response of REFER method during Call
CSCeb16907	Yes	SIP:PIX keep unnecessary xlate after SIP calls are
CSCeb23737	Yes	tcp intercept delay when embryonic threshold at max
CSCeb24596	Yes	Download default route via DHCP or PPPoE is saved to config
CSCeb28943	Yes	PIX fails to delete SA when receiving invalid-spi notify
CSCeb33762	Yes	Segmented SMTP traffic not passed thru fixup
CSCeb34373	Yes	PIX should support domain-name with leading digits
CSCeb43714	Yes	Ping reply from management-access int. sourced incorrectly
CSCeb44000	Yes	PIX OSPF Invalid Packet Length
CSCeb46806	Yes	PIX does not pass through SIP session after
CSCeb53322	Yes	PIX with multicast interfere with MS lad-balancing
CSCeb56571	Yes	secure authen not triggered when static portmap with
CSCeb59923	Yes	secured http authen doesn't work when name configured for
CSCeb60911	Yes	DHCP relay does not work on secondary after failover

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN Client Version 3.x documentation at the following websites:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html

Cisco provides PIX Firewall technical tips at the following website:

<http://www.cisco.com/warp/public/707/index.shtml#pix>

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a Cisco.com account you can visit the following websites for assistance:

TAC Customer top issues for PIX Firewall:

http://www.cisco.com/warp/public/110/top_issues/pix/pix_index.shtml

TAC Sample Configs for PIX Firewall:

http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX&s=Software_Configuration

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in “[Related Documentation](#)” section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0304R)

Copyright © 2003 Cisco Systems, Inc.
All rights reserved.