Cisco PIX Firewall Release Notes Version 6.3(4)

July 2004

Contents

This release is provides new features and fixes for a variety of PIX Firewall models and configuration modes, including new VLAN support, AAA fallback administration, and improved syslog messaging and ip address privacy. This document includes the following sections:

Note For more information on the NAT ID rules caveat, refer to "Important Notes" in the *Cisco PIX Firewall Release Notes Version 6.3(2)*.

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

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

- 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.

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

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 Connection Online (CCO) 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 Connection Online (CCO) login, you can obtain software from the following website:

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

New and Changed Information

New Features in Release 6.3(4)

Release 6.3(4) includes the following new features:

VLAN Support Added to the PIX 506/506E

This release introduces VLAN support for PIX 506/506E, enabling these platforms to be a low-cost DMZ enabled solution. With this new PIX support, users may implement additional logical interfaces, allowing them to securely host an external Web site, a secure email server, or even an extranet.

By adding support for the IEEE 802.1q VLAN tags, 506/506E Firewalls now feature added flexibility in managing and provisioning the firewall. This feature enables the decoupling of IP interfaces from physical interfaces, making it possible to configure logical IP interfaces independently.

VLAN feature support is added to the **interface** command.

- A maximum of two logical interfaces may be configured on the 506/506E, thus providing a maximum of four interfaces (2 physical and 2 logical) on these platforms.
- When 506 and 506E are used as VPN hardware clients, logical interfaces on the 506/506E cannot be used to initiate a VPN tunnel.
- If the VLAN ID is set to 4095, the interface name cannot be modified with the **nameif** command. It may not be appropriate to use VLAN ID 4095 because of this issue.

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*.

AAA Fallback for Administrative Access

This release introduces the ability to authenticate and authorize requests to fall-back to a local user database on the PIX Firewall. The requirements and design will factor future compatibility with Cisco IOS-like "method list" support for the PIX Firewall, and deliver the addition of the LOCAL fallback method.

The following commands are now enhanced to create a fallback scenario for AAA administrative access:

aaa authentication console

A. **aaa authorization command**

A. **aaa authorization match**

aaa server

crypto map command

[no] aaa-server <tag> max-failed-attempts <number>

[no] aaa-server <tag> deadtime <minutes>

SNMP Fixup

This release introduces SNMP traffic inspection capabilities, enabling administrators to specify which SNMP version packets are permitted or denied passage through a PIX Firewall.

The following commands were added modified to support this new feature:

snmp deny version

fixup protocol snmp

IKE Syslog Support Improved

This release introduces a small enhancement to IKE syslogging support and a limited set of IKE event tracing capabilities for scalable VPN troubleshooting. These enhancements have been added to allow for new syslog message generation and improved IKESMP command control.

New Syslog Messaging for AAA authentication

This release introduces a new AAA syslog message, which prompts users for their authentication before they can use a service port. This syslog improvement is based on prior configured PIX Firewall policies. The added syslog is as follows:

%PIX-3-109023: User from src_IP_Adress/src_port to dest_IP_Address/dest_port on interface outside must authenticate before using this service

SIP IP Address Privacy Enhancement

This release introduces an enhancement to PIX Firewall IP address privacy issues that affect SIP fixup. Phones connected on the same interface of the PIX Firewall should not have any direct P2P communication. This feature eliminates the ability of a third party computer to take control of (SIP) and voice (RTP/RTCP) traffic flow through the PIX Firewall. Using the PIX Firewall to create the required pin holes for voice traffic, we can eliminate any direct P2P communication between phones working on a PIX Firewall. The new command that provides this functionality is called:

sip ip-address-privacy

New Ability to Assign Netmasks with Address Pools

This release introduces the ability to define a subnet mask for each address pool and pass this information onto the client. The command to define a subnet mask for a local ip pool is:

ip local pool <name> <range> [mask <mask>]

The command which lets you see if a local subnet mask has been defined is:

show ip local pool

Note Downgrade Issue if this feature is implemented: If you downgrade to a software version that does not have this new feature, address ranges will be loaded without the defined subnet mask. If you downgrade, save the configuration, then upgrade, the masks will not be set or returned to the client.

New Features in Release 6.3(3)

This release is mainly to fix the Network Address Translation (NAT) ID rules caveat (CSCeb84163). The new feature in Release 6.3(3) is:

- PIX Outbound/Conduit Conversion Tool, page 7

PIX Outbound/Conduit Conversion Tool

Beginning with Version 5.3, the PIX Firewall uses access lists to control connections between inside and outside networks. Access lists are implemented with the **access-list** and **access-group** commands. These commands are used instead of the **conduit** and **outbound** commands, which were used in earlier versions of PIX Firewall software. In major software releases after Version 6.3, the **conduit** and **outbound** commands are no longer supported. To migrate an obsolete PIX configuration file that contains **conduit** and **outbound** commands to a supported configuration file that contains the equivalent **access-list** commands, a tool is available to help with the conversion process:

- https://cco-dev.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl (online tool)
- http://www.cisco.com/cgi-bin/tablebuild.pl/pix (download tool)

New Features in Release 6.3(2)

The new features in Release 6.3(2) are:

- Policy NAT, page 8
- Ability to Configure TFTP Fixup, page 8
- DNS Fixup, page 8
- MIB Support, page 8
- Support for Instant Messaging Using SIP, page 9
- Enhanced Show Failover Command, page 9
- Incomplete Crypto Map Enhancements, page 9

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 interoperatability 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 @ 0xfffd8000, 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
dramnath-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

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 support OSPF.

Secure HyperText Transfer Protocol (HTTPS) Authentication Proxy

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

In PIX Firewall software prior to 6.3, configurations that include the **aaa authentication include tcp/0** command will inherit the HTTPS Authentication Proxy feature, which is enabled by default with a code upgrade to Version 6.3 or later.

Refer to Chapter 3, "Controlling Network Access and Use," in the "Enabling Secure Authentication of Web Clients" section of 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*.

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 DCHP 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 supprot 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**-*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* [| {**include** | **exclude** | **begin** | **grep** [**-v**]} *regexp*] 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**, **undebug 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.

For more information, refer to "Identifying the Interface Type" in the *Cisco PIX Firewall and VPN Configuration Guide.* For a complete description of the command syntax for this command, refer to the *Cisco PIX Firewall Command Reference.*

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(3)

Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The PIX Outbound/Conduit Conversion tool assists in converting configurations with outbound or conduit commands to similar configurations using Access Control Lists (ACLs). ACL based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefits:

- Access-list Element (ACE) Insertion capability - System configuration and management is greatly simplified by the ACE insertion capability that allows users to add, delete or modify individual ACEs.
- ACL supports remarks - ACL entries can be identified easily within large system configurations using remarks.
- Turbo ACLs - Turbo ACLs provide enhanced performance and scalability for ACL compilation.
- Object-grouping support - Object-groups are not supported by the outbound command
- ACLs are commonly employed by most PIX features to define traffic designated for that feature (IPsec, nat 0, AAA, etc.)
- All the new developments in PIX are geared towards ACL (time based and outbound ACL) based configurations.

Important Notes in Release 6.3(2)

Major releases beyond PIX Firewall Version 6.3 will not support the conduit and outbound commands.

Important Notes in Release 6.3

This section describes important notes for Version 6.3.

ACL Source Address Change When an Alias is Configured

When the **alias** command is used for destination address translation, an inbound message originating from the *foreign_ip* source address is translated to the *dnat_ip* address. If you configure an inbound ACL with an address defined by the **alias** command, you must use the *foreign_ip* address as the ACL source address instead of the *dnat_ip* address, as was used in Release 6.2. The ACL check is now done before the translation occurs, which is consistent with the way the firewall treats other NATed addresses in ACLs.

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 slower 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:

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

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(4)

Table 3 Open Caveats

	Software Release 6.3(4)	
ID Number	Corrected	Caveat Title
CSCed10049	No	Traceback initpix/intf5 in PIX 515E with 4port FE and Kodiak card
CSCef16218	No	PIX alters seq num on ftp control channel with outside nat.
CSCdw04354	No	Cisco PIX FW needs to better handle incomplete AAA authentication
CSCea40885	No	PIX - Capture sometimes records wrong MAC addr for PIXs interface
CSCea43211	No	Potential failure of TCP connection recovery scenario through PIX
CSCeb32807	No	PIX stops receiving high rate traffic at VLAN interface
CSCed11522	No	PIX SMTP fixup and banner hiding issue.
CSCef05997	No	PIX 515 traceback in isakmp_time_keeper.
CSCef07029	No	PIX traceback in Thread Name: listen/telnet_1.
CSCef10485	No	PIX assigns the first time wrong IP address to VPNclient.
CSCef15146	No	RIP may put the routes with bigger metric into the routing table
CSCef17488	No	PIX SIP fixup does not map RTP port correctly
CSCef17703	No	Memory leak and unexpected invalid SPI with dynamic crypto map

Table 3 Open Caveats (continued)

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
CSCef17728,	No	Telnet negotiation may fail with pix intermittently
CSCef16873,	No	No Audio During SIP Gateway Call

Resolved Caveats - Release 6.3(4)

Table 4 Resolved Caveats

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
CSCdy54228	Yes	PIX syslog 611103 incorrectly logged when user never
CSCea94045	Yes	ID payload contains protocol 17 but port 0
CSCeb29981	Yes	Pix FW in failover mode w/banner greater than 512
CSCeb32807	Yes	PIX stops receiving high rate traffic at VLAN interface
CSCeb39437	Yes	rip inside default v2 broken when management-access inside
CSCeb42088	Yes	PIX traceback in https_proxy
CSCeb77142	Yes	OSPF not able to handle fragmented packets
CSCeb78874	Yes	PIX Standby stuck in reboot loop trying to clear
CSCeb78876	Yes	Adverse effects of multiple NTP servers and OSPF
CSCeb81267	Yes	RIPv2 mcast update sent out on a no RIP configure
CSCec03849	Yes	RIPv2 mcast update sent out on a no RIP configure interface
CSCec04989	Yes	SIP PIX sometimes add extra CRLF at the end of SDP body
CSCec09043	Yes	SIP PIX does not translate via address in 200 and 401
CSCec12942	Yes	H.323 ACF/LCF data not changed with fixup
CSCec13051	Yes	PIX might reboot in ci/console thread while doing show cry
CSCec15510	Yes	ICMP type 3 code 4 not sent back to inside with IPSEC +
CSCec19113	Yes	Non-existing hosts counted towards the license on PIX 501
CSCec20284	Yes	PIX crash in thread PIX Garbage Collector in pix_gc
CSCec20686	Yes	H323 issue when rtp endpoints are diff to call control
CSCec20807	Yes	isakmp_time_keeper crash
CSCec24103	Yes	traceback in riprx/1 when enabling rip default inside
CSCec27881	Yes	LCP is not dropped after Authenticate-Request retry
CSCec30203	Yes	[SIP] PIX drops rtp packets for inside to outside calls
CSCec31274	Yes	PIX crash in turboacl_process issuing access-list compiled
CSCec31498	Yes	Vulnerability Issues in SSL
CSCec35886	Yes	One way voice occur after PIX failover during call

Table 4 Resolved Caveats (continued)

	Software Release 6.3(4)	
ID Number	**Corrected**	**Caveat Title**
CSCec42006	Yes	PPPoE can not add default route if OSPF-sourced default
CSCec42449	Yes	PPPoE session doesn't recover from lost PADS packets
CSCec45239	Yes	Standby PIX sends incorrect packet during boot sequence
CSCec45748	Yes	New DNS conns reset the idle timer of previous DNS conns.
CSCec47609	Yes	PIX resets xlate idle counter to 0 even for denied
CSCec50002	Yes	PIX may crash after using ca generate rsa key 1024
CSCec54201	Yes	DNS port translated when using downloadable access-list
CSCec54641	Yes	PPTP tunnels using MPPE and Downloadable ACLs do not work
CSCec55508	Yes	PIX send 0.0.0.0 as caller-id for enable authentication
CSCec59013	Yes	PIX:CTIQBE not opening outbound pin-holes for RTP
CSCec60851	Yes	SIP Fixup does not fix second Contact Field in SDP packet
CSCec61095	Yes	NAT-T doesn't work from MS L2TP over IPSec client /w NAT-T
CSCec61249	Yes	Remark in downloadable ACL crashes the PIX
CSCec63528	Yes	HTTPS stress testing causes 4 byte block depletion
CSCec63822	Yes	Policy NAT does not co-exist with normal nat configuration
CSCec64215	Yes	Very large ACLs (>200K) may not compile, have very poor
CSCec64902	Yes	VIP:3rd party route with no port not NATd if using PAT
CSCec66432	Yes	fixup protocol pptp not aware of change in outside ip
CSCec69869	Yes	Remark:PIX does not remove remark entry with line number
CSCec70390	Yes	PIX traceback after issuing cl cry cmds during heavy vpn
CSCec72561	Yes	sh access-list | grep xxx may cause ping through device to
CSCec72583	Yes	PIX - OSPF learned routes not used in routing decision
CSCec72698	Yes	RADIUS passwords limited to 16 characters max
CSCec73787	Yes	PIX traceback in pix/intf1 thread
CSCec75949	Yes	[SIP] PIX drops RTP because of fail to match CSeq of
CSCec78327	Yes	primary PIX crashes during config update (solsoft)
CSCec79790	Yes	IUA with EZVPN fails - Server PIX sends hostname instead
CSCec82685	Yes	PIX - VPN client fails to connect to PIX when using NAT-T
CSCec86227	Yes	PIX 520 endless reboot running 6.3.3-109 fover_rep thread
CSCec86309	Yes	AES with PPPoE causes invalid fragmentation
CSCed00488	Yes	SIP:UDP checksum not recalc after modifying payload
CSCed00915	Yes	SIP:media port not translated in in-out-in scenario
CSCed02812	Yes	Identity certificate lost after reload of PIX
CSCed02843	Yes	[SIP] PIX does not translate local ip in o header of sdp
CSCed03100	Yes	SIP:m= port not translated when no session c= in SDP of

Table 4 Resolved Caveats (continued)

	Software Release 6.3(4)	
ID Number	Corrected	Caveat Title
CSCed05397	Yes	Traceback in isakmp_receiver thread under load, related to
CSCed07957	Yes	Radius Timers were not used if uauth is denied by
CSCed09193	Yes	PIX:TACACS+ accounting sending START before 3-way
CSCed11976	Yes	[SIP] PIX drops media stream in case of using some kind of
CSCed12098	Yes	pix smtp fixup doesn't handle multiline banners correctly
CSCed12881	Yes	sysName does not return FQDN. Violates RFC spec
CSCed12948	Yes	IPsec SA is created when mismatch subnet mask
CSCed16070	Yes	PIX Split DNS EZVPN - previous NAT is not undone after
CSCed16868	Yes	PIX traceback in small_frag_append with Websense filtering
CSCed17044	Yes	Large number of NTP packets are sent after failover
CSCed17106	Yes	UAUTH:https_proxy thread can get stuck in rare
CSCed18857	Yes	PPPoE:Traceback with sh vpdn pppint with no PPPoE
CSCed24935	Yes	PIX reloads and crashes in fixup_pptp
CSCed25749	Yes	VPNC:Public-Public SA should not be persistent with NAT-T
CSCed25752	Yes	WEBSNS:Incorrect bit field meaning
CSCed26041	Yes	SIP:RTP stream drop when SIP Authentication is enable
CSCed28592	Yes	Linkdown trap does not contain all the mandatory variables
CSCed31165	Yes	The PIX might drop the RELEASE_COMPLETE message
CSCed31179	Yes	Websense LOOKUP_REQUEST corrupted w/ long URL and HTTP
CSCed31689	Yes	TCP checks should verify RST seq number for conns to the
CSCed37136	Yes	OSPF E2 Route Selection in PIX OS Is Different Then Cisco
CSCed38053	Yes	ARP cache on neighbors may get corrupt during partial
CSCed38963	Yes	PIX Config not being written to Secondary PIX flash memory
CSCed41138	Yes	PIX crashes in TACACS+ process
CSCed42307	Yes	PIX - TFTP does not work with names longer than 19
CSCed42539	Yes	PIX reload in IPSec timer handler with NAT-T disconnect
CSCed43501	Yes	PIX - PPTP:should continue negotiating MPPE
CSCed49919	Yes	PIX DPD window too small
CSCed50456	Yes	Standby PIX cannot update an arp table
CSCed51833	Yes	H.323 Segmented packet inhibits further processing by fixup
CSCed52666	Yes	fail active on a standby PIX does not produce the
CSCed59187	Yes	PIX drops OSPF Type 10 LSA (Opaque) used for Traffic
CSCed59572	Yes	High CPU utilization with large static list
CSCed69284	Yes	Console connection left at ----more--- prompt causes
CSCed70062	Yes	TCP checks should verify SYN seq number for conns to the

Table 4 Resolved Caveats (continued)

	Software Release 6.3(4)	
ID Number	Corrected	Caveat Title
CSCed73661	Yes	Intermittent DNS doctoring with static
CSCed73761	Yes	SIP:PIX set wrong timer for RTCP port via show xlate
CSCed78642	Yes	DNS doctoring broken with network static
CSCed79836	Yes	PIX - SSH authenticated users appear in the uauth table
CSCed83464	Yes	RIP routes disappear from route table following RIPv2
CSCed84886	Yes	Steady UDP streams develop 7ms hole followed by burst
CSCed93959	Yes	Performance issue when processing large no of SCCP
CSCed94093	Yes	PIX:Nailed option no longer functions after 6.3.3 upgrade
CSCed94713	Yes	ISAKMP NAT-T - peer_attrib not initialized correctly upon
CSCee02990	Yes	PIX receiving two default routes don't use the best metric
CSCee07717	Yes	IKE/VPNC:out of order AM3/TM messages causes tunnel
CSCee09061	Yes	PIX help lacks except arg for filter activex|java, ftp,
CSCee11231	Yes	COSMETIC:PIX-4-407002 does not display global IP address
CSCee11278	Yes	Change DPD algo to be less aggressive in detecting short
CSCee13451	Yes	PIX HW Client IUA:VPN3k user idle timeout of 0 is
CSCee13473	Yes	PIX HW Client IUA:user is reprompted despite passing
CSCee18849	Yes	standby might crash if incorrect LU passed from active
CSCee18998	Yes	AUS:PIX polls AUS with low privilege level, update fails
CSCee24747	Yes	High complexity ACLs may require excessively much memory
CSCee27557	Yes	FTP command traffic may ask for authorization even if not
CSCee33328	Yes	TCP packet with class D source may result in a rst response
CSCee33617	Yes	ssh process may leave unfreed memory
CSCee38484	Yes	PIX 6.3.3.102 & 6.3.3.132 crash with pointers to websense
CSCee45177	Yes	nat0acl + static:need deny for both private and public
CSCee46363	Yes	possible reload with traceback in https_proxy thread under
CSCee49107	Yes	PIX:FTP fixup block PORT response when packet exceeds 60
CSCee50614	Yes	SIP:extra RTCP xlates created
CSCee55244	Yes	SIP:RTP port is sometimes translated to odd global port
CSCee60446	Yes	PIX sends 0.0.0.0 as Remote Address for Command
CSCee61905	Yes	PIX crash when input is invalid for the aaa enable password
CSCee66594	Yes	VPNC:Dropped P2 rekey packets may cause P1 delete too fast
CSCee66760	Yes	MSS values are changing for tacacs+ pass thru
CSCee68864	Yes	SIP:should not NAT Proxy-Auth field
CSCee70374	Yes	PIX - Embedded NetBIOS IP not translated with Outside NAT
CSCee71039	Yes	IKE logging improvements

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
CSCee73793	Yes	Feature:Add the ability for PIX to assign netmask to
CSCee75906	Yes	H.323:Segmented TPKTs not handled by fixup
CSCee93282	Yes	PIX crash at listen/http0
CSCee95572	Yes	VPNC:Outside Management SAs should not come up when NAT-T

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/univercd/cc/td/doc/product/iaabu/pix/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm

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 CCO 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

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_inpck/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 "Related Documentation" section.