



Cisco PIX Firewall Release Notes Version 6.3(4)

July 2004

Contents

This release 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, page 1](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [Important Notes, page 7](#)
- [Caveats, page 10](#)
- [Related Documentation, page 15](#)
- [Obtaining Documentation and Submitting a Service Request, page 15](#)

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



Corporate Headquarters:

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

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

- 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>

- 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/public/sw-center/index.shtml>

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, page 5](#)

[AAA Fallback for Administrative Access, page 5](#)

[SNMP Fixup, page 6](#)

[IKE Syslog Support Improved, page 6](#)

[New Syslog Messaging for AAA authentication, page 6](#)

[SIP IP Address Privacy Enhancement, page 6](#)

[New Ability to Assign Netmasks with Address Pools, page 6](#)

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 three logical interfaces may be configured on the 506/506E. For more information on the maximum number of interfaces supported on the PIX Firewall models, refer to “Using Logical Interfaces” in the *Cisco PIX Firewall and VPN Configuration Guide*.
- 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_Address/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.

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:

<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(4)

Table 3 Open Caveats

ID Number	Software Release 6.3(4)	
	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
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
CSCeb81267	Yes	RIPv2 mcast update sent out on a no RIP configure interface
CSCec03849	Yes	SIP: PIX sometimes add extra CRLF at the end of SDP body
CSCec04989	Yes	SIP: PIX does not translate via address in 200 and 401
CSCec09043	Yes	H.323 ACF/LCF data not changed with fixup
CSCec12942	Yes	PIX might reboot in ci/console thread while doing show cry
CSCec13051	Yes	ICMP type 3 code 4 not sent back to inside with IPSEC +
CSCec15510	Yes	Non-existing hosts counted towards the license on PIX 501
CSCec19113	Yes	PIX crash in thread PIX Garbage Collector in pix_gc
CSCec20284	Yes	H323 issue when rtp endpoints are diff to call control
CSCec20686	Yes	isakmp_time_keeper crash
CSCec20807	Yes	traceback in riprx/1 when enabling rip default inside
CSCec24103	Yes	LCP is not dropped after Authenticate-Request retry
CSCec27881	Yes	[SIP] PIX drops rtp packets for inside to outside calls
CSCec30203	Yes	PIX crash in turboacl_process issuing access-list compiled
CSCec31274	Yes	Vulnerability Issues in SSL
CSCec31498	Yes	One way voice occur after PIX failover during call
CSCec35886	Yes	PPPoE: can not add default route if OSPF-sourced default
CSCec42006	Yes	PPPoE: session doesnt recover from lost PADS packets
CSCec42449	Yes	Stateful FO does not replicate Conn for active FTP with
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

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
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 doesnt 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	SIP: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
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 doesnt handle multiline banners correctly
CSCed12881	Yes	sysName does not return FQDN. Violates RFC spec

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
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
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

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(4)	
	Corrected	Caveat Title
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 dont 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 activexljava, 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
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/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 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 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.

CCSP, the Cisco Square Bridge logo, 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, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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 United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0406R)

Copyright © 2004 Cisco Systems, Inc.
All rights reserved.