Cisco PIX Firewall Release Notes Version 6.3(5)

February 2008

Contents

This document includes the following sections:

Introduction

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

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

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

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

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/public/sw-center/index.shtml

New and Changed Information

Version 6.3(5) is a maintenance release which includes several caveat resolutions.

Important Notes in Release 6.3

This section describes important notes for Version 6.3.

Simultaneous PPTP Connection Limitation

There is a hardware limitation of 128 concurrent sessions in PIX 6.x. If you subtract one for the PPTP listening socket, the maximum number of simultaneous PPTP connections is127.

Attempts to connect more than 127 connections with PIX 6.x generates the following error message:

```
%PIX-3-213001: PPTP control daemon socket io accept error, errno = 5
```

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(5)

Table 3 Open Caveats

	Software Release 6.3(5)	
ID Number	**Corrected**	**Caveat Title**
CSCec44081	No	No address translation if multiple ILS messages in one TCP segment
CSCee92806	No	Tunnel not established with NAT-T and certs when MTU > 1500
CSCeg13784	No	PIX tracebacks in turboacl_process when compiling access-list
CSCeg13789	No	PIX - compiled ACLs become corrupted over time
CSCeg54777	No	Throughput drop for combined FW and multi-tunnel VPN traffic
CSCeg83890	No	PIX 501 sends extra byte in passw attr during IUA challenge process
CSCeh40145	No	Assertion getting statistics via PDM while PIX in NEM and reloading
CSCei07402	No	PIX failed over with SSH thread
CSCei47019	No	Logger thread priority too low to allow proper logging queue drain
CSCei47678	No	PIX not following SNMP packet size standard in RFC 3417
CSCei62031	No	Traceback in malloc:_free+17 on executing no capture
CSCei63244	No	Traceback with lu_rx thread name in failover mode
CSCei74718	No	Traceback seen at ssh_init when testing capture
CSCsb34758	No	Connection to DMZ fails after PIX authentication session
CSCsb45070	No	Assertion bp->rptr >= bp->base && bp->wptr <= bp->limit failed: file

Table 3 Open Caveats (continued)

ID Number	Software Release 6.3(5)	
	Corrected	Caveat Title
CSCsb48916	No	Manual ipsec fail when esp-aes-256 specified with auth
CSCsb53549	No	VAC+ may cause interface to stop passing all traffic
CSCsb53760	No	Port redirection for DNS traffic does not work correctly
CSCsb54610	No	Reload in fover_parse when synchronizing very large access-list

Resolved Caveats - Release 6.3(5)

Table 4 Resolved Caveats

ID Number	Software Release 6.3(5)	
	Corrected	Caveat Title
CSCdu79031	Yes	Latency through PIX when issuing **write mem** command
CSCea40885	Yes	PIX - Capture sometimes records wrong MAC addr for PIXs
CSCec86400	Yes	PIX traceback after issuing show isakmp sa detail
CSCec89275	Yes	Reboot with traceback after modifying access-list
CSCef10485	Yes	PIX assigns the first time wrong IP address to VPNclient
CSCef15146	Yes	RIP may put the routes with bigger metric into the routing
CSCef16218	Yes	Active FTP failed with outside NAT and retransmit PORT
CSCef16873	Yes	No Audio During SIP Gateway Call
CSCef17488	Yes	PIX SIP fixup does not correctly open RTP conns using NAT
CSCef17703	Yes	Premature invalid SPI with dynamic crypto map
CSCef22894	Yes	Increase amount of memory allowed for the PDM history
CSCef24632	Yes	PIX might reload when clearing the config with pdm history
CSCef26256	Yes	PIX crash while doing write standby
CSCef27344	Yes	DHCP relay does not work with BOOTP
CSCef39526	Yes	Alias command may cause High CPU on Secondary PIX
CSCef47155	Yes	PPTP passthru fails after upgrading to 6.3.4
CSCef47529	Yes	PIX crash in radius_snd thread
CSCef57566	Yes	PIX PMTUD implementation for IPSec vulnerable to spoofed
CSCef61702	Yes	4-byte block leak when sending TCP RST in some
CSCef66863	Yes	OSPF redistribute connected vlan fails on physical
CSCef75987	Yes	Packets corrupted and spurious invalid SPI with VAC under
CSCef80869	Yes	arp-response received on a wrong interface causes crash
CSCef81257	Yes	Inbound SYN Packet has ACK changed from 0 to some random
CSCef82742	Yes	Presence of extra lf in uauth FTP answer

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(5)	
	Corrected	Caveat Title
CSCef84827	Yes	Write Standby is causing http server disabled on standby
CSCef86106	Yes	Mishandling of syslog message 106013
CSCef91771	Yes	Identity NAT norandomseq broken with stateful failover
CSCef93994	Yes	SIP:Large # of SIP conns from REGISTER xactions cause
CSCef94622	Yes	On receiving invalid ACK, RST should be allowed through
CSCef98132	Yes	aaa auth match statement not working correctly with
CSCeg02725	Yes	Crash when removing aaa serve
CSCeg04006	Yes	SEQ number in the outbound RST packet gets randomized
CSCeg05291	Yes	SIP: PIX does not reset xlate timer for RTP in certain
CSCeg07701	Yes	pptp stops accepting new connections: tcp listening socked
CSCeg07744	Yes	Linkdown trap does not contain ifIndex variable
CSCeg20248	Yes	PIX 501 crashes when VPN to VPN 3030 concentrator using
CSCeg22626	Yes	SIP: PIX add extra white space when IP Address Privacy is
CSCeg24504	Yes	Embryonic xlate gets consumed instead of using PAT xlate
CSCeg31510	Yes	PIX sets wrong content-length in SIP header
CSCeg38460	Yes	SIP: Signalling secondary connection not timing out as
CSCeg40538	Yes	SIP:2ndary conns for INVITE should stay up for duration of
CSCeg41622	Yes	SIP: Source UDP port of Register are not translated in
CSCeg48656	Yes	Potential SYN, ACK, RST loop on TCP recovery mechanism
CSCeg52090	Yes	PIX resetting ftp connection
CSCeg54523	Yes	PIX reboots continuously with overlapping/redundant statics
CSCeg56154	Yes	PIX crash with wrong clear ospf syntax
CSCeg58814	Yes	PIX crash stack overflow when show crypto ipsec identity
CSCeg61351	Yes	PIX 6.3(4) crashes with thread tacplus_snd similar to
CSCeg71881	Yes	Conversion from dhcpd to dhcprelay requires reboot
CSCeh10239	Yes	SIP: RTP session is closed/disconnected when receive
CSCeh21989	Yes	PIX 6.3 translates aaa accounting cmd automatically and
CSCeh22724	Yes	Incorrect xlate can be created by SIP fixup
CSCeh28734	Yes	Standby PIX takes active unit MAC for a few sec after boot
CSCeh33341	Yes	FastEthernet driver might corrupt packets under extreme
CSCeh42211	Yes	TurboACL with more than 65535 elements may compile wrong
CSCeh42901	Yes	SIP: CSeq No parsed incorrectly if CSeq no length is 10
CSCeh47107	Yes	SIP: SIP URI Parse error happens when receiving SIP
CSCeh52176	Yes	DNS guard disconnects conn on one response
CSCeh62359	Yes	SIP: sip-disconnect timeout for SIP sessions

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.3(5)	
	Corrected	Caveat Title
CSCeh62642	Yes	SIP: sip-invite timeout for SIP sessions
CSCeh71223	Yes	PIX stops forwarding the failover hello packet while write
CSCeh71254	Yes	Active FTP failed with cut-through proxy for FTP
CSCeh73510	Yes	PIX adds <16> in DC field for LDAP CRL request
CSCeh74381	Yes	On receiving invalid ACK, RST should be allowed through
CSCeh78170	Yes	Many SA requests at once cause unpredictable failover
CSCeh92328	Yes	OSPF external routes preferred over internal with multiple processes
CSCeh94584	Yes	Object group search for acl can be enabled after acl is used in nat
CSCeh96286	Yes	Deadlock of vac poll and interface threads with VAC card
CSCeh96556	Yes	4 byte block exhaustion may cause failover or dropped connections
CSCei09184	Yes	L2TP over IPSEC NAT-T not working with WindowsXP
CSCei10683	Yes	SIP: fail to open a conn for Record route in NOTIFY
CSCei17398	Yes	Excessive TCP retransmissions for connections to the PIX
CSCei22149	Yes	URL filtering: misc issues related to request exhaustion and cleanup
CSCei24710	Yes	ffs: loading PDM from mozilla causes assert
CSCei29707	Yes	RTSP fixup does not recognise server ports
CSCei41295	Yes	Two dynamic maps configured and the correct one not picked up
CSCei46448	Yes	Port F1 fix (CSCeh38022) to 6.3. This is the GigE driver tx ring fix
CSCei58383	Yes	PIX crashes when -v option used without parameter in piping
CSCei64471	Yes	PIX crashes when entering CA SAVE ALL
CSCsb33373	Yes	SIP: Not translate c= address if first m= has port 0 in SDP body
CSCsb37529	Yes	PIX 6.3.3 crashes with traceback dbgtrace:_dbg_output+135

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.