



Release Notes for the Cisco PIX Firewall Version 6.1(4)

June 2002

Contents

This document includes the following sections:

- [Introduction](#)
- [System Requirements](#)
- [New and Changed Information](#)
- [Important Notes](#)
- [Caveats](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Introduction

These release notes describe the features, restrictions, and caveats for Cisco PIX Firewall software version 6.1(4).



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

System Requirements

The sections that follow list the system requirements for Cisco PIX Firewall software version 6.1(4).

Memory Requirements



Note

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 have 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 506/506E require 16 MB of Flash memory to boot. (The PIX 501 and PIX 506/506E 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 6.1
PIX 501	8 MB
PIX 506/506E	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

We highly recommend that you use Livengood Gigabit Ethernet cards in systems with a 64-bit/66 MHz PCI bus; for example, in a PIX 535. (If you use the Livengood Gigabit Ethernet cards in a PIX Firewall, the system RAM should be at least 128 MB.) For a PIX Firewall with only a 32-bit/33 MHz bus, such as the PIX 520 and PIX 525, we recommend that you use Wiseman Gigabit Ethernet cards.

Software Requirements

The following are requirements for Cisco PIX Firewall software version 6.1(4):

1. The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, you need to download the Boothelper file from Cisco.com to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from version 4 or earlier and want to use the 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 using PIX Firewall Syslog Server (PFSS), we recommend you install Windows NT Service Pack 6 to fix year 2000 conflicts in Windows NT.

- 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.

Cisco IOS Software Interoperability

Cisco VPN Series	Interoperability
Cisco IOS Routers	If using IKE mode configuration on the PIX Firewall, the router must be running Cisco IOS Release 12.0(6)T or higher.
Cisco VPN 3000 Concentrators	PIX Firewall version 6.1 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 v1.1	PIX Firewall version 6.1 requires Cisco Secure VPN Client version 1.1. Cisco Secure VPN Client version 1.0 and 1.0a are no longer supported.
Cisco VPN 3000 Client v2.5	PIX Firewall version 6.1 requires Cisco VPN 3000 Client version 2.5 or higher. This VPN client can be used with Windows 95, Windows 98, and Windows NT version 4.0. It is not supported on Windows 2000.
Cisco VPN Client v3.x (Unified VPN Client Framework)	PIX Firewall version 6.1 supports the Cisco VPN Client version 3.x. The Cisco VPN Client runs on Linux and all current Microsoft Windows platforms. At this time, the Cisco VPN Client is not supported on other UNIX or Mac platforms.

Determining the Software Version

Use the **show version** command to determine the software version of your PIX Firewall unit.

Upgrading to a New Software Release

If you are a registered cisco.com user, you can obtain software from the following site:

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

To register for a cisco.com login, go to the following site:

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

New and Changed Information

New Features in Release 6.1(4)

This release resolves a number of caveats. The PIX-4FE-66 card is also supported, except for PIX Classic, 10000 and 510 platforms.

New Features in Release 6.1(3)

This release resolves two caveats, CSCdw63021 and CSCdw75833.

New Features in Release 6.1(2)

The PIX 506E and PIX 515E join the PIX Firewall product line. Both the PIX 506E and PIX 515E have faster processors than the PIX 506 and PIX 515. Also, the PIX 506E has a physically different, but functionally equivalent, power supply than the PIX 506.

New Features in Release 6.1(1)

PIX 501

The PIX 501 joins the PIX Firewall product line. The PIX 501 offers consumers affordable, enterprise-strength firewall and VPN capabilities. The PIX 501 works with cable and xDSL modems and, additionally, ships with a default configuration for easier “plug-n-play” installation.

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

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

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

Table 2 Gigabit Ethernet Interface Card Combinations

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



Caution

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



Caution

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



Note

Starting with PIX Firewall software version 6.0(1), and in all subsequent higher versions, the PIX Firewall Classic, PIX10000, and PIX 510 platforms are not supported.

Default Configurations

The PIX 501 ships with a default configuration as of PIX Firewall software version 6.1(1). For more information on the PIX 501 default configuration, please refer to the *Cisco PIX 501 Firewall Quick Start Guide*.

DHCP Server Pool

The DHCP server pool of the PIX 506 has been expanded to 256 addresses.

For information on new features in previous PIX Firewall software versions, refer to the following website:

http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/prod_technical_documentation.html

Maximum 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 higher. For other PIX Firewall platforms and earlier software versions, the maximum configuration file size limit is 1 MB except for the PIX 501, which is limited to a

256 KB configuration file size. However, 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

Cisco Secure Policy Manager may also experience limitations if a PIX Firewall configuration file near 2 MB is used. Please take these considerations into account when planning and implementing your configuration.

Important Notes

AAA Authentication

Configure the access list specified in Attribute 11 (specifies per-user access-list name) on the PIX Firewall. Otherwise, remove Attribute 11 from the AAA RADIUS server configuration if no access list is intended for user authentication. If the access list is not configured on the PIX Firewall when the user attempts to log in, the login will fail. AAA, RADIUS, and Attribute 11 information can be found at the following websites:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007deec.html

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080102925.html



Note

Starting in CAT OS 5.4, a new command was added called **set port host**. Essentially, this is a CLI macro that executes these commands: **set spantree portfast enable**, **set trunk off**, and **set port channel off**. This command provides a quick and convenient way to configure host or access ports to a mode that allows the port to forward traffic in less than one second from linkup.

Downloading PIX Firewall Image

Fast Ethernet cards in 64-bit slots for the PIX 535 are not visible in monitor mode. This problem means that the TFTP server cannot reside on one of these interfaces. The user should use the **copy tftp flash** command to download the PIX Firewall image file via TFTP.

DHCP Server Functionality

The functionality of the DHCP server on the PIX Firewall has been changed to allow users to define a pool of up to 256 DHCP addresses on the PIX 506/506E and larger platforms.

Restrictions

Starting with PIX Firewall software version 6.0(1), FDDI, PL2, and Token Ring interfaces are not supported.

Starting with PIX Firewall software version 6.0(1), PFM is no longer supported; PFM has been replaced by the Cisco PIX Device Manager (PDM).

Caveats

The following sections describe the open caveats for the 6.1(2) 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

Please use Bug Toolkit on [cisco.com](http://www.cisco.com) to view additional caveat information. Bug Toolkit may be accessed at the following website:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Open Caveats - Release 6.1(4)

The caveats in [Table 3](#) are yet to be resolved in this release

Table 3 *Open Caveats*

DDTS Number	Description
CSCds54310	Traceback (ci/console) doing sh map, IPSec tunnel exists.
CSCds80108	Cisco Secure Intrusion Detection System (Cisco Secure IDS) signature number 1101 is not supported by PIX Firewall. When attempted to be accessed, PIX Firewall returns an incorrect error message: Invalid signature number.
CSCdv33495	static PAT and fixup ftp breaks ACTIVE ftp.
CSCdv86755	icmp type is not correctly interpreted with aaa authentication.
CSCdw00291	402103 message for ICMP, although the identities in the message ok.
CSCdw25718	uauth_thread uap->proxy 0 scrolling on console & perf.degraded.
CSCdw34273	Watchdog with overlapping static and dynamic PAT address.
CSCdw37960	VSA in accounting records not defined correctly.
CSCdw81126	PIX sourced UDP traffic to non-existing ip may use many blocks.

Table 3 *Open Caveats (continued)*

DDTS Number	Description
CSCdx17123	Traceback in isakmp receiver while testing xauth aaa rollover, ire.
CSCdx48302	PIX 501 console unable to view debug crypto commands.
CSCdx79285	IKE nego failed with Invalid SPI notification between 501 & 520.
CSCdx80701	H323: H225 channel denied though ACF seen by PIX.
CSCdx81284	PKI: PIX cannot poll CRL after reboot.
CSCdx81692	Write Net sources from wrong interface.
CSCdx83295	DHCPC:DHCP static route not deleted if switch to static ip address.
CSCdx84022	performance degradation with tcp intercept; block depletion.
CSCdx84647	PIX rekeys QM continuously w/ kilobytes lifetime set to certain value.
CSCdx89025	PKI: memory leak when requesting and denying certificate requests.
CSCdx89336	Temporary 1550 byte block exhaustion with udp traffic.
CSCdx89579	PIX 525 Crashes intermittently.
CSCdx90840	Failure Detected - No Block Memory (size 272) in failover.

Resolved Caveats - Release 6.1(4)

The caveats in [Table 4](#) are resolved in this release.

Table 4 *Resolved Caveats*

DDTS Number	Description
CSCds12981	Ssh client disconnected on typing any letter while debug packet on it.
CSCds54310	Traceback (ci/console) doing sh map, IPsec tunnel exists.
CSCdt42853	H225:should create new TPKT & discard original if TPKT.
CSCdt47829	PIX wont learn MAC addresses in range 0008.xxxx.xxxx.
CSCdt85435	UNITY_IOS:ios does not renegotiate ipsec sa when PIX does cl isa sa.
CSCdu59514	PIX syslogs sent with standby rather than active IP.
CSCdu85817	hostobjdb being corrupted.
CSCdv17303	stateful failover show high err count under stress.
CSCdv26953	Skinny:Need to update to version 3.1 code.
CSCdv31029	SIP:maddr= & received= parameters not NATd.
CSCdv32237	Active-X filter does not work correctly.
CSCdv39306	PIX loses ARP entry for HSRP address.
CSCdv40404	IKE mode config bug - causes PIX crash with dump.
CSCdv42836	IKE continuous channel mode does not work with IOS unity version.
CSCdv52820	Memory leak on PIX when verifying peers certs during IKE phase 1.
CSCdv53837	after 1st IPSEC peer down, 60 second delay before switch to 2nd peer.

Table 4 Resolved Caveats (continued)

DDTS Number	Description
CSCdv55044	ESP packets routed basing on encapsulated destination address.
CSCdv56552	Session counts are inconsistent UDP vs. TCP.
CSCdv57122	AAA proxy limit exceeded and out of Tcb_user errors.
CSCdv57570	PIX crashes when vpn client 3.1 connects.
CSCdv60361	H.225:Call fails when newly encoded message is smaller.
CSCdv64039	TCP connection to PIX from token ring client hangs.
CSCdv64435	PIX code space not write protected.
CSCdv65961	1550 byte blocks go to zero, PIX stops passing traffic.
CSCdv69641	PIX can only recognize 2 interfaces in PIX-515E in monitor and image.
CSCdv70291	Traceback triggered by TACACS+ authentication of FTP.
CSCdv71017	PIX reboots with stack trace in isakmp_receiver thread.
CSCdv72013	H323:Inbound call w/ indirect voice due to early removal of data.
CSCdv74412	pptp - non-zero reserved field in header.
CSCdv75812	VoIP fixups drop 1-byte TCP keep-alive.
CSCdv76727	Traceback fover_rep after no fail with failover on serial cable.
CSCdv83025	DNS Flakiness. Some outbound UDP DNS replies being denied by PIX.
CSCdv86755	icmp type is not correctly interpreted with aaa.
CSCdv87789	PIX506E hangs when booting with 64 sector flash.
CSCdw00328	wrap into debug/rate limit invalid hdr.len in isakmp check.
CSCdw00398	Alias with overlapping networks broken.
CSCdw01653	PIX stops prompting for Authentication - out of tcb objects.
CSCdw04410	no failing over should be possible while replicating the config.
CSCdw10863	High DNS query-rate (more than 4000/second) causes memory exhaustion.
CSCdw10880	PIX snmp response on failover status incorrect after PIX failover.
CSCdw11539	PIX dhcp client need to get new addr if current lease.
CSCdw15057	Large DNS query message stops old connection removal.
CSCdw16074	Altiga client cannot connect to PIX with xauth enabled.
CSCdw17097	PIX - DHCP client does not accept dhcp offer with broadcast bit set.
CSCdw18939	executing config floppy, no errors report and config is not restored.
CSCdw24283	Traceback after entering show xlate local command.
CSCdw25026	License not released after 30 seconds in certain scenario.
CSCdw25718	uauth_thread uap->proxy 0 scrolling on console & perf.degraded.
CSCdw27548	PIX is sending wrong authentication type with RIP v2.
CSCdw29965	SSH:Watchdog timeout if receiving huge SSH packets.
CSCdw35460	Traceback when using a ftp connection after disallowing new conns.
CSCdw36415	PIX traceback in ci/console after assertion in limit.c.

Table 4 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdw38189	memory leak with ipsec/certificates + packet loss + delay + bad cert.
CSCdw39040	PIX denies its own ICMP unreachable with PPTP.
CSCdw42039	H323:Should not drop RAS packets if > 1024.
CSCdw45615	standby pix does not return correct MIB-II ipAddrTable.
CSCdw46749	Incorrect processing of ICMP error with nat 0 0 0.
CSCdw49277	RIP2 updates case PIX interface loss of communication and failover.
CSCdw55700	H323:TCP connections incorrectly marked with Fin flag.
CSCdw56153	IKE memory leak w/ PFS enabled crypto map.
CSCdw56480	traceback when trying to copy tftp from 2 telnet session at the same time.
CSCdw57969	static arp entries replying for the arp requests.
CSCdw59655	PPTP:Watchdog timeout followed by traceback in pptp_gre/0 thread.
CSCdw60558	PIX ignores subnet mask when natting using the global command.
CSCdw62717	VPN 3.x Client to PIX - DPD not working correctly.
CSCdw62906	PIX reboots when flooded with aggressive mode proposal requests.
CSCdw63021	PIX crashes upon receiving malformed SNMP packet.
CSCdw63754	Memory leak of 3.7MB when copy tftp pdm-image to flash:image.
CSCdw64258	PIX crash with traceback triggered by uauth.
CSCdw67516	Two PIX535s configured in failover mode keep rebooting.
CSCdw71762	VPN:Unused ISA SAs not used to create IPsec tunnel not deleted.
CSCdw74095	PKI:certificate with serial number 0 gets lost upon reload.
CSCdw74252	PIX crashes when attempting to copy a large PDM file.
CSCdw74985	memory leak with uauth (or xauth) and ftp when conns are pre-allocd.
CSCdw77490	PIX traceback when conf flop.
CSCdw78258	fragmented ICMP replies, data changes across pix using PAT.
CSCdw78269	Authentication stops through pix, must reboot or clear tcp stats.
CSCdw79472	Watchdog timeout thread snmp_ex, PIX keep rebooting after 1 minute.
CSCdw87877	Workaround for checkpoint limitation ftp authentication.
CSCdw90236	CA:cannot use cert after reload.
CSCdw90391	Traceback:lu_rx after generating stateful traffic.
CSCdw94427	sqlnet fixup creates incorrect embryonic for redirect.
CSCdw94583	PIX should use the same radius request ID for the same request.
CSCdx00158	PKI:traceback after type clear config all.
CSCdx00603	PIX does not work with global interface PAT.
CSCdx06796	Traceback in Crypto PKI RECV thread.
CSCdx07927	PKI:Traceback in Cryto CA thread when PIX fails to get CRL.
CSCdx09382	PIX hangs during write net.

Table 4 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdx11660	NIC media and driver type field intermingling.
CSCdx11947	PKI:Memory leak when cert is not granted on CA and PIX.
CSCdx12345	auth-prompt help exists and can be entered in priv exec.
CSCdx12794	PIX send out invalid getcert message.
CSCdx16459	ppp frees a block with free instead of freeb.
CSCdx17242	Instable checksum.
CSCdx25089	PIX intercept bad IPSec packet causing Watchdog timeout.
CSCdx29322	PIX does not send xauth request to aaa after sometime.
CSCdx35340	Assertion lport fport failed in pix/intf1 thread.
CSCdx35823	Unexpected reaction to TACACS+-authenticated HTTP packet.
CSCdx42706	Clear uauth for selected user clears all user.
CSCdx45064	SIP:PIX does not correctly parse <> in the To:and From:
CSCdx47789	PIX Reboots when receiving fragmented SIP INVITE messages.
CSCdx52407	Static route getting overwritten by RIP learnt route.
CSCdx54495	SIP:new content length is incorrect if > 255.
CSCdx57852	ISAKMP Failure with seconds/kilobytes lifetime set to certain values.
CSCdx58065	SIP:named static ip address causes crash or call failure.
CSCdx60754	DHCPC:Address becomes 127.0.0.1 if configure dhcp to static to PPPoE.
CSCdx61012	SIP:200 OK for the BYE not passing thru PIX.

Open Caveats - Release 6.1(3)

The caveats in [Table 5](#) are yet to be resolved in this release.

Table 5 *Open Caveats*

DDTS Number	Description
CSCds10112	Traceback (Crypto PKI RECV) after twice enrolling and getting denied.
CSCds54310	Traceback (ci/console) doing sh map , IPSec tunnel exists.
CSCdt42853	H225: should create new TPKT & discard original if TPKT recvd only.
CSCdt47829	PIX won't learn MAC addresses in range 0008.xxxx.xxxx.
CSCdu31945	The command sysopt route dnat no longer works correctly.
CSCdu35560	netbios does not work with certain IPSec encapsulations.
CSCdu52383	cic_dh_makepair:gen_newpubkey(1) returned 0xd.
CSCdu59514	PIX syslogs sent with standby rather than active IP address.
CSCdu59841	Traceback in hosts conn cleaner thread.
CSCdu85817	hostobjdb being corrupted.

Table 5 *Open Caveats (continued)*

DDTS Number	Description
CSCdv14770	ACL: hitcnt wrong on outbound ACL with tcp permit eq <port#>.
CSCdv21580	Cert enrollments fails with 2048bits sp keys with serial/ip options.
CSCdv24360	PIX rebooted with traceback in qos_metric_deamon thread.
CSCdv24986	Assertion if conf net and command write mem in config file.
CSCdv25850	PIX reboots with stack trace in isakmp_receiver thread (stress).
CSCdv26489	Error in cert validation occurs sometimes when peer changes certs.
CSCdv26934	PIX reboots (isakmp_thread) when negotiating with PIX (revoked cert).
CSCdv30928	SIP: Register messages to remote Proxy dropped.
CSCdv31029	SIP: maddr= & received= parameters not NATd.
CSCdv55044	ESP packets routed based on encapsulated destination address.
CSCdv57731	H323:should drop msgs w/ invalid TPKT & UUIE lengths.
CSCdv60361	H.225: Call fails when newly encoded message is smaller.
CSCdv65760	Denied outbound connections does not get reset by PIX.
CSCdw06216	high CPU usage during PIX SSH session initialization.
CSCdw13876	4-byte blocks leak if remote ipsec peer not responding.
CSCdw18939	executing config floppy, no errors report and config is not restored.
CSCdw24283	Traceback after entering show xlate local command.
CSCdw34273	Watchdog with overlapping static and dynamic PAT address.
CSCdw36415	PIX traceback in ci/console after assertion in limit.c.
CSCdw38189	memory leak with ipsec/certificates + packet loss + delay + bad cert.
CSCdw42509	Telnet session variable NVT does not properly negotiated across PIX.
CSCdw45615	standby pix does not return correct snmp ip table.
CSCdw46749	Incorrect processing of ICMP error with nat 0 0 0.
CSCdw49277	RIP2 updates case PIX interface loss of communication and failover.
CSCdw50388	PIX losing RIP updates.
CSCdw51492	ssh to pix will drop ping packets going across pix.

Resolved Caveats - Release 6.1(3)

The caveats in [Table 6](#) are resolved in this release.

Table 6 *Resolved Caveats*

DDTS Number	Description
CSCdw63021	PIX crashes upon receiving malformed SNMP packet
CSCdw75833	PROTOS-test suite flood the interface will stop PIX to pass traffic

Resolved Caveats - Release 6.1(2)

The caveats in [Table 7](#) are resolved in this release.

Table 7 Resolved Caveats

DDTS Number	Description
CSCdt58805	Watchdog timeout in isakmp_receiver thread.
CSCdt85435	UNITY_IOS:ios does not renegotiate ipsec sa when pix does.
CSCdv00738	Add enhanced platform support for the PIX 506.
CSCdv42836	IKE continuous channel mode does not work with IOS unity.
CSCdv69641	PIX can only recognize 2 interfaces in PIX-515E in monitor.
CSCdv84391	Add OID support for 506E & 515E hardware platforms.
CSCdv87789	PIX 506E hangs when booting with 64 sector flash.
CSCdw20653	PIX 515E cannot load image from monitor mode on PCI slots.
CSCdw29965	SSH:Watchdog timeout if receiving huge SSH packets.
CSCdw53447	Enhancement:Reduce the boot-up time for the PIX-525.

Resolved Caveats - Release 6.1(1)

The caveats in [Table 8](#) are resolved in this release.

Table 8 Resolved Caveats

DDTS Number	Description
CSCds21095	pix pptp stop accepting new connections after sometimes of operation
CSCds71849	dbgtrace_is_debug_trace_on() function need to be optimized
CSCds89340	WDT in dbgtrace thread
CSCdt61216	Naptha (ESTABLISHED) Flooding causes PDM DoS
CSCdt77025	Assertion (IPsec response handler) while running pixIpsecIsakmp.
CSCdt82325	Reload due to exhausted memory while URL filtering heavy traffic.
CSCdt86736	Noticable pause with more than 50000 UDP connections
CSCdt94747	H323: PIX should proxy ACK TPKT if we recvd TPKT only
CSCdu01836	PDM sessions are not released even after closing all the browsers
CSCdu05134	H.323 call does not go thru if calling GW uses slow start
CSCdu10483	PIX doesn't delete its isa sas if the peer doesn't negotiate sa
CSCdu12321	pix fail to do write mem , if a big cmd line exists
CSCdu13760	Perfmon values increase when you do a show perfmon
CSCdu15498	501: have better err msg for write and conf floppy
CSCdu15512	501:VPN LED stays up when there is no VPN traffic/tunnel
CSCdu15537	501: PIX 501 takes 6-ifx license, and show ver lists max 6 supported

Table 8 Resolved Caveats (continued)

DDTS Number	Description
CSCdu20056	Blocks information is empty when PIX crashed.
CSCdu20593	Xauth: With IRE on rekey puts internal addr. entry for uauth.
CSCdu22069	SIP: With Out Proxy & global/nat, xlate created for outside addr
CSCdu22771	PIX is sending Initial Contact during rekey, between PIX-PIX
CSCdu24181	Traceback (IPsec response handler) after L2TP tunnel created.
CSCdu25110	501:mac-addr program in biosburn does not recognize interfaces
CSCdu25260	mcpdm with arg 1.0.1 shows up as 1.0(1)0 in PDM About window
CSCdu25837	Software needs to limit PIX 501 interface speed to 10baseT
CSCdu27169	VoIP: certain embedded IP addr not NATd
CSCdu28566	501: show version display processor speed 100 not 133MHz
CSCdu29410	PIX501: Unit takes failover license which it shouldn't
CSCdu32616	501: The RAM requirement for 501 should be 16M instead of 32M
CSCdu33209	IPSec Antireplay Checking Ineffective 32-64 sequence numbers back
CSCdu33543	pix pptp rejects dial-in req after abnormal termination
CSCdu35041	Assertion crash with lport fport after startup
CSCdu36628	PIX neither uses nor discards CRL if time < last CRL update of CA.
CSCdu38093	PIX crashed in tcp_slow thread when enrolling for certs with sp keys
CSCdu38206	Config lines greater than 255 displayed incorrectly by sh conf
CSCdu38927	PIX failover should try to allocate additional blk if possible
CSCdu39748	H323: generating 50+ calls causes unexpected reload
CSCdu39748	H323: generating 50+ calls causes unexpected reload
CSCdu40845	PIX - Failover does not work with ip verify reverse-path RPF
CSCdu41413	xauth skipped with client 3.0 if inside and outside swapped
CSCdu41525	Netscape error when connecting to PIX with rsa special key
CSCdu41996	Watchdog after interface PAT pool exhausted
CSCdu42112	AAA:when down does not return rejection while using radius
CSCdu42645	Kodiak: some status bits are ignored
CSCdu42656	Kodiak: AH decapsulation requests not setup correctly
CSCdu43284	H323: make use of NELTS & sizeof, remove extern functions
CSCdu47003	Able to pass disallowed SMTP command thru PIX, by sending after mail
CSCdu48184	Nested traceback handling is confusing
CSCdu53473	H225 H245 messages greater than 1024 bytes not inspected
CSCdu53971	misconfigured failover ifc a.b.c.d lines cause flip-flops
CSCdu54443	501:slow performance with mismatched duplex on switch and eth ports
CSCdu54455	501:show version hangs when printing the pix version
CSCdu54495	Unexpected reload when using Websense with TCP4 and url-cache.

Table 8 Resolved Caveats (continued)

DDTS Number	Description
CSCdu55206	Traceback while trying to establish a PPTP tunnel (scripted).
CSCdu55859	URL with arguments are not handled properly
CSCdu57729	max arp number for small memory model should be 256 instead of 16
CSCdu59514	PIX syslog are sent with standby ip address
CSCdu60447	PIX should not initialize COM3 & COM4 serial ports
CSCdu61691	stateful failover doesn't replicate conn for passive ftp using PAT
CSCdu62372	Eliminator Disk does not transfer IP packets properly
CSCdu62647	Kodiak:IPSec encrypt packet introp with IOS is not working in ftp
CSCdu63067	Perfmon command causes interface no buffer
CSCdu63388	SYN-ACK retransmit zeroizes the idle timeout on conn
CSCdu66557	H323 Skinny does not properly open 3rd party IP using nat 0 acl
CSCdu67493	clear int followed by interface number clears all the interfaces
CSCdu67799	IPSEC:pix takes long time to create a 2nd Ipsec tunnel (1 IKE)
CSCdu68118	Write net fails when the first two ethernet int are not in use
CSCdu68124	Intercepted connections timeout prematurely if they are idle
CSCdu70055	PRNG weakness in SSL
CSCdu70175	failing to contact secondary radius server
CSCdu72961	PIX fails to change identity field for RFC 2865
CSCdu73070	Xauth:2 extra prompts for any auth, when a auth request fails radius
CSCdu74672	SMTP Fixup: end-of-data checking incorrect
CSCdu76004	501:continuous reboot if pdm install is not successful
CSCdu78806	SIP: Pingtel phones SIP messages dropped by fixup module
CSCdu80080	SYSLOG: abbreviated logging cmd not replicated on standby PIX
CSCdu80222	Show version: change PIX and PDM product names.
CSCdu80852	Panic: pix/intf0 - init_sip: create_chunk failed
CSCdu83457	extra process_suspend() may cause missing stateful updates
CSCdu88336	IKE delete notify does not delete IPsec SA 60 seconds after setup
CSCdu89190	PIX crashes with multiple ssh aaa authen failures or success
CSCdu89348	PIX reboots with traceback in isakmp_receiver thread when no memory
CSCdu89431	Watchdog timeout failure in ci/console while clearing ipsec sas
CSCdv00692	PIX reboots dumping stack trace in isakmp_time_keeper thread
CSCdv01450	H225: wrong TCP seq if H225v1 re-encoded to H225v2
CSCdv01748	dhcpcd will not work with ip verify reverse path interface inside
CSCdv03096	PIX vulnerable to invalid SIP packets
CSCdv04717	i82550EY devices identified as i82557s
CSCdv06822	501:Watchdog timeout followed by traceback (isakmp_time_keeper)

Table 8 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdv06996	501:PIX is unable to rekey phase1 when the limit reaches to 5 tunnel
CSCdv09731	PIX - AAA failing due to limited number of uauth sessions/source ip
CSCdv10117	Watchdog timeout failure, and hang after reload pri or sec PIX535.
CSCdv11921	501:VPN LED on with no ISA/IPSec SA when SA not deleted thru peer
CSCdv12077	PIX-506: ifx becomes 100full after reload, when configured to auto
CSCdv18119	Skinny: StationRegister message not NATd correctly
CSCdv23491	Cannot load an image on PIX through copy tftp flash command
CSCdv25865	Watchdog timeout in isakmp_receiver thread

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN 3000 Client documentation at the following websites:

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

http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod_technical_documentation.html

Cisco provides PIX Firewall technical tips to registered cisco.com users at the following website:

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

To become a registered cisco.com user, go to this website:

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

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you are a registered cisco.com user, you can visit the following websites for assistance:

TAC Customer top issues for PIX Firewall:

http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/products_installation_guide_chapter09186a008017a424.html

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

To become a registered cisco.com user, go to this website:

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packer*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

Copyright © 2001-2002, Cisco Systems, Inc.
All rights reserved.