



# Cisco PIX Security Appliance Release Notes Version 7.0(4)

---

October 2005

## Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 7](#)
- [Caveats, page 8](#)
- [Obtaining Documentation and Submitting a Service Request, page 15](#)

## Introduction



**Note**

---

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.0.

---

The Cisco PIX 500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability. This release introduces significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high-availability services, and management/monitoring.

For more information on all the new features, see [New Features, page 4](#)



---

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Additionally, the security appliance software supports ASDM. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

## System Requirements

The sections that follow list the system requirements for operating a security appliance.



**Note**

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.0.

## Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you need to upgrade your memory before performing an upgrade to PIX Version 7.0. PIX Version 7.0 requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses. The following security appliance platforms require at least 64 MB of RAM. [Table 1](#) lists Flash memory requirements for Version 7.0.

**Table 1** *Flash Memory Requirements*

security appliance Model	Flash Memory Required in Version 7.0
PIX 515/515E	16 MB
PIX 525	16 MB
PIX 535	16 MB

For more information on minimum memory requirements, see “Minimum Memory Requirements” section in the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*.

## Software Requirements

Version 7.0(4) requires the following:

1. The minimum software version required before performing an upgrade to PIX Version 7.0 is PIX Version 6.2. If you are running a PIX release prior to PIX Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can begin the upgrade to PIX Version 7.0.

To upgrade your PIX software image, go to the following website:

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

2. For information on specific licenses supported on each model of the security appliance, go to the following websites: <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>
3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. See the “[Upgrading to a New Software Release](#)” for new installation requirements.

## Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 7.0(4). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.0(4). If you are using ASDM, we recommend no more than a 500 KB configuration file because larger configuration files can interfere with the performance of ASDM on your workstation.

While configuration files up to 2 MB are 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 the **write terminal** and **show running-config** commands
- Failover (the configuration synchronization time)
- During a system reload

## Cisco VPN Software Interoperability

Cisco VPN Series	Interoperability Comments
Cisco IOS routers	Version 7.0(4) requires Cisco IOS Release 12.3(T)T or higher running on the router when using IKE Mode Configuration on the security appliance.
Cisco VPN 3000 concentrators	Version 7.0(4) requires Cisco VPN 3000 concentrator Version 3.6 or higher for correct VPN interoperability.

## Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco VPN client v3.x/4x (Unified VPN client framework)	Version 7.0(4) supports the Cisco VPN client Version 3.6 or higher that runs on all Microsoft Windows platforms. It also supports the Cisco VPN client Version 3.6 or higher that runs on Linux, Solaris, and Macintosh platforms.

## Cisco Easy VPN Remote Interoperability

Cisco Easy VPN Remote	Interoperability Comments
Cisco PIX Security Appliance Easy VPN Remote v6.3	Version 7.0(4) Cisco Easy VPN server requires the Cisco PIX security appliance Version 6.3 Easy VPN remote that runs on the PIX 501 and PIX 506 platforms.

Cisco Easy VPN Remote	Interoperability Comments
VPN 3000 Easy VPN remote v3.x/4x	Version 7.0(4) Cisco Easy VPN server requires the Version 3.6 or higher of the Easy VPN remote that runs on the VPN 3002 platform.
Cisco IOS Easy VPN remote Release 12.2(16.4)T	Version 7.0(4) Cisco Easy VPN server interoperates with Cisco IOS 806 Easy VPN remote Release (16.4)T.

## Determining the Software Version

Use the **show version** command to verify the software version installed on your security appliance.

## Upgrading to a New Software Release

If you have a Cisco.com (CDC) login, you can obtain software from the following website:

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

## New Features

This section describes the new features in this release. This section includes the following topics:

- [Auto Update Over a VPN Tunnel, page 4](#)
- [Crashinfo Enhancement, page 5](#)
- [Modular Policy Framework Enhancement, page 5](#)
- [Support GTP Load Balancing Across GSNs, page 5](#)
- [Downloadable Access Control Lists Enhancements, page 5](#)
- [Converting Wildcards to Network Mask in Downloadable ACL, page 6](#)
- [IPSec VPN: Add support for Cascading ACLs, page 6](#)
- [Rate limiting of Syslog messages, page 6](#)

## Auto Update Over a VPN Tunnel

With this release, the **auto-update server** command has a new **source interface** argument that lets you specify an interface, such as a VPN tunnel used for management access and specified by the **management-access** command:

```
auto-update server url [source interface] [verify-certificate]
```

```
no auto-update server url [source interface] [verify-certificate]
```

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Crashinfo Enhancement

Output from the **crashinfo** command might contain sensitive information that is inappropriate for viewing by all users connected to the security appliance. The new **crashinfo console disable** command lets you suppress the output from displaying on the console.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Modular Policy Framework Enhancement

The new **set connection timeout** command lets you configure the timeout period, after which an idle TCP connection is disconnected.

For more information, see the “Using Modular Policy Framework” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Support GTP Load Balancing Across GSNs

If the security appliance performs GTP inspection, by default the security appliance drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS. You can enable support for GSN pooling by using the **permit response** command. This command configures the security appliance to allow responses from any of a designated set of GSNs, regardless of the GSN to which a GTP request was sent.

For more information, see the “Enabling and Configuring GTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Downloadable Access Control Lists Enhancements

This feature adds a means of ensuring that downloadable ACL requests sent to a RADIUS server come from a valid source through the Message-Authenticator attribute.

Upon receipt of a RADIUS authentication request that has a username attribute containing the name of a downloadable ACL, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. The presence of the Message-Authenticator attribute prevents malicious use of a downloadable ACL name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions, available at <http://www.ietf.org>.

For more information, see the “Configuring Any RADIUS Server for Downloadable ACLs” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Converting Wildcards to Network Mask in Downloadable ACL

Some Cisco products, for example the VPN 3000 concentrator and Cisco IOS routers, require that downloadable ACLs be configured with wildcards instead of network masks. The adaptive security appliance, on the other hand, requires that downloadable ACLs be configured with network masks. This new feature allows the security appliance to internally convert a wildcard to a netmask. Translation of wildcard netmask expressions means that downloadable ACLs written for Cisco VPN 3000 series concentrators can be used by the security appliance without altering the configuration of the downloadable ACLs on the RADIUS server.

You can configure ACL netmask conversion on a per-server basis, using the **acl-netmask-convert** command, available in the AAA-server configuration mode. For more information about configuring a RADIUS server, see the “Identifying AAA Server Groups and Servers” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## IPSec VPN: Add support for Cascading ACLs

Cascading ACLs involves the insertion of deny ACEs to bypass evaluation against an ACL and resume evaluation against a subsequent ACL in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security. The sequence number assigned to the crypto ACL determines its position in the evaluation sequence within the crypto map set.

For more information, see the “Defining Crypto Maps” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Failover Key Command

The **failover key** command was modified to include the **hex key** keyword and argument. **hex key** specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Rate limiting of Syslog messages

The logging rate limit enables you to limit the rate at which system log messages are generated. You can limit the number of system messages that are generated during a specified time interval.

You can limit the message generation rate for all messages, a single message ID, a range of message IDs, or all messages with a particular severity level. To limit the rate at which system log messages are generated, use the **logging rate-limit** command.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

# Important Notes

## Important Notes in Release 7.0

This section lists important notes related to Version 7.0(4).

### Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in release 7.0(4) for the PIX 535 are 50 tiers. The maximum number of VLANs supported are 150. For more information on the feature support for each platform license, see the “Platform Feature Licenses” section in the *Cisco Security Appliance Command Line Configuration Guide*

### IKE Delete-with-Reason

IKE syslog for Delete-with-Reason will not contain the reason text unless the clients support this feature. Currently the VPN 3002 Version 4.7 and PIX 501 Version 6.3(4) hardware clients do not support this feature.



Note

---

The PIX 501 security appliance is not supported in software Version 7.0.

---

### User Upgrade Guide

Before upgrading to Version 7.0(4), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*. This guide also includes information about deprecated features and other changes in the Cisco PIX Software Version 7.0. For a list of deprecated features, and user upgrade information, go to the following URL:

[http://www.cisco.com/en/US/docs/security/asa/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)



Caution

---

If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Do not upgrade until you have corrected your configuration, as this is not a supported configuration and Version 7.0(4) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.0(4) with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.

---

### Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The security appliance Outbound/Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefits:

- 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.

- Outbound ACLs and Time-based ACLs - Gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling/Disabling of ACL Entries - Provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs, without the need to remove and replace ACL entries.

## Features not Supported in Version 7.0

The following features are not supported in Version 7.0(4) release:

- PPPoE
- L2TP over IPSec
- PPTP

## MIB Supported

For information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.

For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.



### Caution

---

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. Loading a software image from monitor mode, on a PIX security appliance that has a PIX Version 7.0 file system, results in unpredictable behavior and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

---

## Caveats

The following sections describe the caveats for the 7.0(4) release.

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

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

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

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

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

## Open Caveats - Release 7.0(4)

**Table 2** Open Caveats

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCeg57001	No	Packet does not come to inspect after no inspect and inspect
CSCeh15557	No	Assertion in tmatch_compile_proc, all memory is not freed.
CSCeh18115	No	Authentication not triggered sometimes when URL filtering enabled.
CSCeh32087	No	PIM sends Register with untranslated IP when NAT pool exhausted.
CSCeh43554	No	Device may reload if showing and removing config at the same time
CSCeh46345	No	Dynamic L2L could pass clear text traffic when tunnel terminates
CSCeh60845	No	Logginig queue incorrectly registers 8192 256-byte blocks
CSCeh84006	No	Wrong http version number should not be allowed
CSCeh90617	No	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh93834	No	RSA SecurID replica list is lost after reboot
CSCei02273	No	1st log message is not sent by mail in transparent firewall
CSCei43588	No	traceback when trying to match a packet to acl with deny
CSCej04099	No	static xlate breaks management-access inside
CSCsb28708	No	Console traceback using show route command
CSCsb40188	No	SCEP fails if RA cert has 4096 bit key
CSCsb41742	No	P2P/IM/tunneling traffic is only dropped if strict-http action is drop
CSCsb51038	No	Traceback: _snp_sp_create_flow+1937 with outbound ACL and Policy Statics
CSCsb80170	No	Address-pools needed in group-policy - missing functionality from VPN3K
CSCsb81593	No	removing sunrpc-server cli doesnt stop sunrpc traffic from getting thru
CSCsb90046	No	GTP context creation might fail w/ Tunnel Limit xxx exceeded error
CSCsb99385	No	strict-http: with a space before http ver should generate a tcp reset
CSCsc00176	No	clear xlate take 4.5+ mins to clear 60K PAT xlat
CSCsc02485	No	Session Cmd: sendind \036x\r to exit session to ssm causes Traceback
CSCsc07421	No	Traceback in Dispatch Unit - decoding h323 ras message
CSCsc07614	No	Minimum unit poll time causes trouble for failover with 4GE card

**Table 2** Open Caveats (continued)

Software Release 7.0(4)		
ID Number	Corrected	Caveat Title
CSCsc10617	No	GTP: memory leakage after <clear config all> at gtp_init
CSCsc11724	No	Logging: Wrong behavior if syslog is sent to a nonfunctioning tcp server
CSCsc12094	No	AAA fallback authentication does not work with reactivation-mode timed
CSCsc14591	No	xlate and xlate perfmon print graph are all zeros
CSCsc15378	No	Telnet to pix outside interface through IPSEC connection fails
CSCsc15434	No	Assertion violation w/icmp traffic and icmp inspection
CSCsc16041	No	'clear local host' results in memory leak
CSCsc16503	No	Transparent firewall ASR UDP out traffic got errors and inbound failed
CSCsc16607	No	fixup pptp fails with static pat server configuration
CSCsc17051	No	VPNFO: VPN Failover fails to parse P2 SA when IPCOMP is used
CSCsc17428	No	Tracebacks with ci/console with 'clear config all'
CSCsc18324	No	PIX 7.0.2 traceback in Dispatch Unit (Old pc 0x001dbdc6 ebp 0x01212404)
CSCsc18444	No	Tunnel-group for specific peer not created upgrading to 7.0 w/ certs
CSCsc18911	No	PIX does not remove OSPF route for global PAT entry after deleting

## Resolved Caveats - Release 7.0(4)

**Table 3** Resolved Caveats

Software Release 7.0(4)		
ID Number	Corrected	Caveat Title
CSCeh81062	Yes	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh90309	Yes	Checkheaps process crashes while dumping corrupted memory blocks
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh97228	Yes	cTCP: cTCP connection are dropped sporadically when connected F1 Bet
CSCei00497	Yes	PIX 7.0 doesnt encrypt packets if next hop is PIX interface.
CSCei20466	Yes	Increase in CPU utilization when OSPF is enabled
CSCei20682	Yes	FWSM uptime stops at 49 days 17 hours
CSCei23290	Yes	DHCP Relay fails when static specified
CSCei24062	Yes	Some hosts in the network connects to inside intf cannot be reached
CSCei29277	Yes	Performance of Skinny calls through PIX is poor
CSCei31310	Yes	PIX 7.0 sends NAT-T keepalives with wrong UDP pkt length value
CSCei33166	Yes	Crash while pinging through a L2L tunnel w/ 10,000 byte pings
CSCei33782	Yes	Simultaneous TFTP connections are not closed properly
CSCei38012	Yes	DHCP Server should check for correct network upon REQUEST for rebind

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCei38640	Yes	AAA: radius /w expiry does not work when using funk radius server
CSCei38644	Yes	VPN3000 does not properly handle State Attribute
CSCei38647	Yes	IKE SA stuck in MM_DONE state
CSCei38651	Yes	NT auth for VPN clients do not work with domainuser or <u>user@domain</u>
CSCei38657	Yes	P1 rekey may fail when P1/P2 rekeying and retransmit required
CSCei38667	Yes	Can't differentiate between root CA certs that have been re-keyed
CSCei38669	Yes	IPSec rekey causes tunnel to drop
CSCei41326	Yes	AAA: fallback to LOCAL authentication does not work for SSH
CSCei43065	Yes	Traceback - 0x004a21b0 obj-f1/c_crypto_map:_crypto_map_remove_np+80
CSCei43133	Yes	traceback eip 0x006026a4 obj-f1/snp_ha_db in ci/console af cleconfal
CSCei43459	Yes	Cannot pass generic SSH command arguments via SCP in PIX 7.0.1
CSCei44143	Yes	Crash in malloc.c if removing ACE from ACL
CSCei50190	Yes	PIX not accepting 2 ISAKMP policies with different AES types
CSCei50691	Yes	traceback with ASR enabled for session with 2ndary conn in TFW mode
CSCei51783	Yes	Group enumeration possible on Benetton platform
CSCei51867	Yes	Usability - crypto config should be grouped together in CLI output
CSCei52413	Yes	PIX fails to import cert if CA issuer has 4096 bits cert
CSCei52906	Yes	Routes assoc. w/ net ext tunnels fail to get removed after tun drop
CSCei54438	Yes	Inspects that use TCP proxy must enable dual TCP normalizer mode
CSCei56278	Yes	All access-lists removed when removing one
CSCei57279	Yes	Cascading ACL: Deny rules not working after tunnel established
CSCei57980	Yes	c2950/3550/3750 connected to PIX causes RX errors after pix reload
CSCei62347	Yes	acl interval default value not show when inactive parameter used
CSCei64608	Yes	GTP: box reloads when Create Response has 3rd party GSN addr
CSCei65780	Yes	standby PIX may reload during the command replication
CSCei67952	Yes	GTP: PDP Context expires even when data is present in the tunnel
CSCei68679	Yes	Traceback on telnet TACACS+ authentication through the firewall.
CSCei68679	Yes	Traceback on telnet TACACS+ authentication through the firewall.
CSCei69450	Yes	RSH connection done by a cronjob fails through PIX 7.0
CSCei70172	Yes	TCP dynamic proxy doesnt fast retransmit lost packet
CSCei70785	Yes	TCP proxy must send data from retransmit queue when ACK is received
CSCei71868	Yes	Deny message for inbound traffic with no access-list changed
CSCei75013	Yes	config doesnt get copied to admin ctx when changing mode SRM->MRM
CSCei78667	Yes	URL filtering: misc issues related to request exhaustion and cleanup
CSCei81803	Yes	Assert in validate_chunk() during startup

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCei83304	Yes	clear conf sec doesnt clear igmp and ospf param in ifx submode
CSCei83942	Yes	PPTP connection through PIX dropped after 2 min of inactivity
CSCei84925	Yes	traceback obj-f1/snp_tfw:_snpi_tfw_update_l2_entry+75 af apply conf
CSCei87390	Yes	Removing failover group causes traceback with 4GE installed
CSCei87785	Yes	MGCP: Call cannot be placed with IP phone using BTS CA & version 1.0
CSCei92828	Yes	Authentication failing for virtual telnet/http in transparent mode
CSCei93112	Yes	Existing connections not replicated to standby after failover
CSCei93790	Yes	Clear configure all in single transparent mode causes traceback
CSCej08898	Yes	tcpintercept caused trcbck.embconn=0,maxconn!=0,eip:0x00c32dbc
CSCej12123	Yes	OSPF external routes preferred over internal with multiple processes
CSCej24446	Yes	error in processing IKE
CSCsb32565	Yes	Device reboots unexpectedly with traceback
CSCsb36441	Yes	Traceback eip _snp_fp_inspect_ip_options with IP Frag and 10 KB ping
CSCsb36525	Yes	DACL fails intermittently in PIX 7.0 code with ACL can't be found
CSCsb37531	Yes	Traceback after failover if TCP Intercept is triggered.
CSCsb38475	Yes	Port values byte reversed in %PIX-3-620002: Drop CTIQBE syslog message
CSCsb40331	Yes	PIX 7.0(1)2 Assertion Violation w/Multiple Context & VOIP Configuration
CSCsb45373	Yes	Traceback tcp_slow after vpn system test script strtd snd cfg setupUUT
CSCsb45584	Yes	Traceback eip _snp_ids_cleanup_cb with ips promiscuous and 100 byte ping
CSCsb46603	Yes	GTP: Responses that reject Create Requests are dropped
CSCsb46862	Yes	Assertion in ctm_sw_rng_x931.c:update_key
CSCsb47027	Yes	PIX crashed eip 0x00b8773c (image 7.0.2.1)
CSCsb47825	Yes	F1 fails to establish TCP remote access sessions with 3002 HW client
CSCsb49125	Yes	F1 crashes at <show debug> command
CSCsb50946	Yes	High cpu due to shun command
CSCsb52950	Yes	With banner exec command and # as delimiter replication not correct
CSCsb53407	Yes	MFIB: tracebacks when bouncing multicast-routing
CSCsb54545	Yes	Traceback eip _keyword_option_flex_action with show ip local pool
CSCsb55104	Yes	Syslog message 710003 is overloaded; behaves different than in PIX 6.3
CSCsb55282	Yes	sh inventory does not show 4GE module
CSCsb55550	Yes	traceback in pki_ctm:_pki_ctm_verify_signature+164 - 8192 bit certs conn
CSCsb56247	Yes	traceback in crypto_pki:_crypto_pki_poll_crl+52 - with crl opt PKI
CSCsb58364	Yes	VPNFO: tunnels get dropped when fover occurs
CSCsb58364	Yes	VPNFO: tunnels get dropped when fover occurs
CSCsb61027	Yes	mcast: secondary crashes shortly after sync'd with primary

**Table 3 Resolved Caveats (continued)**

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCsb61462	Yes	PIX closes XDMCP/X display connections after some random time
CSCsb61644	Yes	PIX crashes when accessing ASDM over IPSec/TCP-10000 tunnel
CSCsb61832	Yes	HTTP-Proxy functionality (Port Forwarding) not working on Windows ME.
CSCsb62617	Yes	VPN: assertion 0 failed: file malloc.c, line 4570 RA dial/hang test
CSCsb62908	Yes	Closing the Port Forwarding Applet removes existing Proxy configuration
CSCsb63920	Yes	CLI: no ssl trust-point cmd causes traceback, ssl_chain:_ssl_trustpoint
CSCsb64159	Yes	VPNLB: need ability to assign a trustpoint to the vcpip address
CSCsb64985	Yes	4ge module interface stops passing traffic after using QoS and L2L tunn
CSCsb67119	Yes	Inspect ESMTP incorrectly rewrites smtp reply containing 220 in text
CSCsb67166	Yes	Time based ACLs not working properly if object groups are used
CSCsb70268	Yes	'hw-module module 1 reload reloads 4GE module
CSCsb71198	Yes	incorrectly formatted DL ACL causes traceback in IKE daemon
CSCsb72604	Yes	crash in snmp thread after nmap UDP scan of port 161
CSCsb72665	Yes	IX 7 may drop valid TCP segments that carry data in final segment
CSCsb72803	Yes	rash triggered when system is out of memory
CSCsb74050	Yes	F1 crashed when sweep-ping (G-PDU) thru GTP tunnel v0
CSCsb75857	Yes	F1 hit memory corruption crash @ clear conf gtp then clear conf all
CSCsb76268	Yes	Immediately after upgrade to 7.0(1) - interfaces stuck in waitingstate
CSCsb76426	Yes	DACL fails intermittently in PIX 7.0 code with ACL can't be found
CSCsb76995	Yes	%PIX-3-113001: Unable to open AAA session. Session limit [32] reached
CSCsb77332	Yes	traceback in fover_parse on standby unit if config contains webtype acl
CSCsb77397	Yes	Traceback: eip 0x00c3426c strepy:_strepy+12, using deb menu ike commands
CSCsb78230	Yes	hw-module module 1 shut and reset do not bring up the 4ge module
CSCsb79742	Yes	incorrectly formatted downloadable acl causes traceback in emweb/https
CSCsb80196	Yes	DHCP ID String is limited to 50 characters, should be 128
CSCsb81575	Yes	key gen causes an assert if PIX has DES only license
CSCsb82583	Yes	PIX515E with VAC+ fails FIPS validation test and reboots
CSCsb82663	Yes	Out of order TCP packets degrade HTTP inspection performance
CSCsb83962	Yes	F1 OSPF regression scripts hang with removal of router config
CSCsb85239	Yes	PIX running 7.0.(1.5) crash with assert in TCP proxy 'tcp_slow'
CSCsb85767	Yes	URL Filtering with long URLs could cause memory corruption
CSCsb85780	Yes	Malformed HTTP GET request causes URL filtering module to cause a crash.
CSCsb88557	Yes	Traceback at snap:_snap_mini_dump+26 with acl Logging: thread-arp_timer
CSCsb89147	Yes	certificate-to-username mapping broken for some DN attributes
CSCsb91835	Yes	PIX reload in smtp/esmtp inspection {insp_process_smtp_data}

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCsb91837	Yes	vpn-filter incorrectly blocking traffic with echo, echo-response keyword
CSCsb93659	Yes	Local IP doesn't get translated with NAT Exemption
CSCsb94651	Yes	Overlapping static statements should be allowed
CSCsb94689	Yes	4GE card firmware accessing incorrect PHY address
CSCsb95027	Yes	Stadby Betabox rebooted while upgrading to 7.0.3.19
CSCsb95259	Yes	No hits shown on access-list associated to a group-policy vpn-filter
CSCsb97680	Yes	traceback in radpact:_RADPBldHWClientReauth+260 during 3002 New Pin Mode
CSCsb98667	Yes	sunrpc inspection causes memory allocation error on pix 7.0.2
CSCsb99192	Yes	Show access-list   inc xxx causes traffic through device to be delayed
CSCsb99360	Yes	Logging queue 0 is wrongly shown as being unlimited queue
CSCsb99760	Yes	pix 7.0.2 extended split acl reverse of 6.3 format
CSCsb99792	Yes	PATed ICMP conn stops PIX from responding to ICMP Echo-Requests
CSCsc00709	Yes	PIX enable authentication issue
CSCsc02230	Yes	nat entry with outside keyword : ERROR: unable to download policy
CSCsc02485	Yes	Session Cmd: sendind 036xr to exit session to ssm causes Traceback
CSCsc02574	Yes	pki: ID cert signature validation failure allows successful connection
CSCsc05446	Yes	PIX sends ARP for RP address which is few hops away
CSCsc06282	Yes	fover: ip local pool fails to replicate after issuing from grp submode
CSCsc06477	Yes	unable to manage running config with err msg: configuration in progress
CSCsc06702	Yes	VPN: Interface counters are incorrectly incremented on decrypted packets
CSCsc08684	Yes	PIX 7.0.2 built connection number shows up as negative on syslog
CSCsc08843	Yes	DHCP-Relay drops packets when source address is non-zero
CSCsc09527	Yes	VPNFO: cannot establish a vpn tunnel "session limit reached" sa cnt -1
CSCsc09932	Yes	Assertion in file "vf_api.c", line 264, traceback in strdup:_int3+4
CSCsc14837	Yes	ARP fails on the 4GE interfaces in routed firewall mode

## 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/ps2120/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html)

## Software Configuration Tips on the Cisco TAC Home Page

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

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

[http://www.cisco.com/en/US/products/ps6120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html)

## 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. (0502R)

© 2005 Cisco Systems, Inc.  
All rights reserved.