



Cisco PIX 500 Security Appliance Release Notes Version 7.0(7)

July 2007

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 4](#)
- [Caveats, page 6](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 13](#)

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](#).



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

© 2007 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 the system 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 the “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(7) 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 website:

http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html

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(7). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.0(7). 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(7) 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(7) 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(7) 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
VPN 3000 Easy VPN remote v3.x/4x	Version 7.0(7) 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(7) 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

Version 7.0(7) includes several caveat resolutions.

Important Notes

This section lists important notes related to Version 7.0(7).

Common Criteria EAL4+

For information about common criteria EAL4+, see the *Installation and Configuration for Common Criteria EAL4 Evaluated Cisco Adaptive Security Appliance, Version 7.0(6)* document.

Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in release Version 7.0(7) 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 system log messages for Delete-with-Reason do 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(7), 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

**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(7) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.0(7) 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(7):

- 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 Version 7.0(7).

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

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

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

Open Caveats - Version 7.0(7)

Table 2 lists the open caveats for Version 7.0(7).

Table 2 Open Caveats

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCej04099	No	static xlate breaks management-access inside
CSCek21850	No	SIP: Stanby PIX shows the wrong value of xlate timeout for sip media.
CSCsh91283	No	ASA/PIX: SunRPC inspect dropping packets on 7.0.6
CSCsi08317	No	PIX using Authentication Proxy and Wildcard causes Certificates error
CSCsi41045	No	OSPF: default-info originate with route-map fails with next hop or source
CSCsi98617	No	VPNFO: Standby stale sessions not removed
CSCsi98637	No	VPN: Traceback in Thread Name: tmatch compile thread

Table 2 **Open Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsj03706	No	activex or java filter suppresses the syslog message 304001
CSCsj12938	No	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj13797	No	SSH connection fails when first server in AAA group is unreachable
CSCsj32989	No	ASA traceback when running 100 user Avalanche webvpn goodput test
CSCsj37890	No	Traceback in Thread Name: tmatch compile thread
CSCsj43778	No	ASA may slowly lose free memory to SNP Conn chunk
CSCsj44098	No	traceback caused by gtp inspect handling bad packets

Resolved Caveats - Version 7.0(7)

Table 3 lists the resolved caveats for Version 7.0(7).

Table 3 **Resolved Caveats**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsb45561	Yes	standby instead of active keeps sending register to RP after failover
CSCsd43563	Yes	Crypto accelerator errors seen - connections failing
CSCsd81262	Yes	CA cert with spaces could fail to install
CSCsd81294	Yes	'crypto ca import' of SSL cert may traceback in Thread Name: accept/http
CSCse09503	Yes	Syslog 304001 not generated when strict-http action allow log configured
CSCse14419	Yes	ASA 7.0(4) : not randomizing TCP SACK sequence numbers
CSCse20538	Yes	IKE Syslogs 713041 713042 should specify interface name
CSCse22330	Yes	Traceback in Thread Name: Dispatch Unit
CSCse30102	Yes	VPN dynamic ACL can be deleted from the CLI
CSCse30616	Yes	ASA VPN load balancing cannot ping cluster ip address
CSCse36112	Yes	PIX/ASA never processes huge access-list if it runs short of memory
CSCse37733	Yes	Traceback with both interface nameif 0 and nat ID 0
CSCse42413	Yes	Traceback after WebVPN authentication with FreeRadius
CSCse44258	Yes	Modifying vpn-filter acl blocks normal traffic from inside to outside
CSCse45327	Yes	VPN stateful failover gets out of sync
CSCse49440	Yes	SNMP: incorrect cpu usage sent for CISCO-PROCESS-MIB
CSCse52050	Yes	Very large ACL applied to NAT or Crypto may traceback in Checkheaps
CSCse55931	Yes	1550 byte block depletion prohibits websense communication
CSCse66133	Yes	Traceback in Thread Name: ssh when ACLs are displayed in SSH or ASDM
CSCse66490	Yes	Traceback with 'Thread Name: accept/http' after editing time-based ACLs

Table 3 **Resolved Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCse76150	Yes	No TACACS+ authorization request sent for show run command
CSCse86968	Yes	Standby unit sends accounting records for replicated DACL commands
CSCse89013	Yes	debug radius decode does not show all attributes in Radius requests
CSCse96559	Yes	vpn-filter does not work when used with IOS ESVPN client
CSCsf02349	Yes	Traceback in ThreadName: ci/console when add certificate in wrong format
CSCsf02716	Yes	ASA doesn't send failover syslog via SNMP TRAP
CSCsf05931	Yes	AAA: group-lock does not handle tunnel-group names with spaces
CSCsf08950	Yes	AAA: Memory leak with ACL in cut-through-proxy
CSCsf10663	Yes	High CPU / System locks up when adding a network object entry
CSCsf11095	Yes	show conn display problems for secondary conns with static network
CSCsf16622	Yes	Firewall should log syslog when IGMP report denied by IGMP ACL
CSCsf16633	Yes	ASA - OSPF over VPN tunnel not working correctly
CSCsf21159	Yes	CRL checking fails when using Entrust CA on ASA
CSCsf21882	Yes	Traceback in Thread: Dispatch Unit with QOS police configuration
CSCsf22966	Yes	TCP proxy doesn't support window-scale - SIP packet not fwded
CSCsf23020	Yes	SIP: SIP Fixup cannot process multiple SIP packets in one TCP segment
CSCsf23145	Yes	Unable to complete large uploads through VPN if packet loss occurs
CSCsf24272	Yes	IPv6: ACL corruption with service object-group
CSCsf28690	Yes	L2TP/IPsec ASA rejects clients certificate
CSCsf30287	Yes	VPN: Traceback in Thread Name: PIX Garbage Collector
CSCsf30571	Yes	Traceback in ssh_init
CSCsf31767	Yes	comma cannot be used in Subject DN in certificate parameters of ASA
CSCsf98804	Yes	Wrong TCP sequence numbers in ICMP Unreachable when sent through ASA
CSCsf99335	Yes	Traceback in Thread Name: IKE Daemon and Checkheaps memory corruption
CSCsf99833	Yes	Traceback in fover_FSM_thread w/deb fover switch and stateful link down
CSCsg00066	Yes	Traceback in accept/http with ASDM 'clear configure crypto dynamic-map'
CSCsg00914	Yes	OSPF neighbors don't form due to corrupted arp entry
CSCsg04324	Yes	VPN: high cpu usage with DHCP assigned IP addresses
CSCsg08640	Yes	access-list damaged and frozen, clear config acl has no effect
CSCsg08799	Yes	Traceback in Dispatch Unit and assertion flow->vpn_handle == NULL
CSCsg10605	Yes	ASA: TCP normalizer spoofs an ACK with all zeroes src MAC address
CSCsg16149	Yes	data sent with Active MAC after switchover to standby
CSCsg17150	Yes	Traceback in Thread Name: Dispatch Unit with Large Multicast Packets
CSCsg19285	Yes	Traceback in Thread Name: telnet/ci with shun of loopback address
CSCsg21230	Yes	EASTERN is hardcoded as SMTP date timezone

Table 3 **Resolved Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsg21242	Yes	ASA: Outbound ESP blocked by VPN-Filter when using Originate-Only
CSCsg23233	Yes	VPN: 'show isa sa' may cause traceback in Thread Name: telnet/ci
CSCsg23270	Yes	Traceback in Thread Name: telnet/ci with 'show local grep 1.1.1.1'
CSCsg27124	Yes	PIX 7.x does not allow RST pkt to pass from srv to client after failover
CSCsg30214	Yes	ISAKMP threshold value in primary and secondary not the same
CSCsg31948	Yes	Trace back in Thread Name: snmp (Old pc 0x009fa5a0 ebp 0x0202cfcc)
CSCsg31956	Yes	VPN: Traceback in Thread Name: IKE Daemon
CSCsg35215	Yes	Syslog server down causes ICMP flood if ICMP is denied at interface
CSCsg39502	Yes	ASA 7.0.6 Traceback in tmatch compile
CSCsg39762	Yes	5510 show ver misleadingly indicates backplane FE as Not license
CSCsg39936	Yes	Pix/ASA: Disabling pim on subinterface causes other interface mcast fail
CSCsg40572	Yes	Traceback in Thread Name: IKE Daemon
CSCsg40894	Yes	ASA traceback due to memory mem_get_owner
CSCsg41593	Yes	If 2 DHCP servers for VPN clients, failover for DHCP not successful
CSCsg43591	Yes	SCP connection to PIX fails
CSCsg43844	Yes	In failover pair standby ASA used memory is higher than in active
CSCsg48997	Yes	RST-ACK sent by service resetoutbound uses wrong sequence number
CSCsg50757	Yes	Memory corruption of dispatch_ctxt_t in checkheaps
CSCsg52106	Yes	Embryonic value -1 under syslog and count to host = 42949672
CSCsg52108	Yes	The uauth timeout is not enforced via TACACS+
CSCsg58837	Yes	ASA traceback in Dispatch Unit during configuration replication
CSCsg60095	Yes	VPN traffic permitted by vpn-filter is denied
CSCsg63297	Yes	CPU hog when update large object group in policy nat
CSCsg68186	Yes	Malformed Regex causes traceback on ASA/PIX
CSCsg69149	Yes	Policy NAT with large ACL and HA may traceback in tmatch compile thread.
CSCsg69408	Yes	Need warning when using time based ACLs with policy NAT/PAT
CSCsg83130	Yes	Device reload with no crashinfo file
CSCsg86538	Yes	Dynamic L2L tunnel fails if the remote peer ip is changed
CSCsg89271	Yes	PIX 7.2.1 corrupting SDP media attributes in RTSP
CSCsg90455	Yes	VPN:Traceback in Thread Name: Dispatch Unit with fragmented cTCP packets
CSCsg92979	Yes	copy ftp from firewall fails when default passive mode is used
CSCsg94167	Yes	Kerberos SASL uses the wrong name-type for TGS request
CSCsg94762	Yes	URL caching leads to invalid filter server status on PIX/ASA
CSCsg96150	Yes	dependence between sysopt connection permit-vpn and management commands
CSCsg96701	Yes	traceback at Thread PIM IPv4

Table 3 **Resolved Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsg97348	Yes	FW replying to port application requests that are not active using VPN.
CSCsh01646	Yes	pptp inspect does not alter Call ID in some packets
CSCsh06232	Yes	PIX does not open RTP connections for H323 calls
CSCsh12413	Yes	FO: Syslog 111111: Memory requested from Null Chunk seen every min.
CSCsh14023	Yes	TACACS+ CMD Accounting packets have a Caller-ID field of 0.0.0.0
CSCsh15587	Yes	Garbage characters printed on console at end of long show cmd
CSCsh19536	Yes	VPN-FO: Sessions not cleaned up correctly on Standby
CSCsh20558	Yes	PIX/ASA traceback in dhcp_daemon
CSCsh20618	Yes	80-byte block memory leak with asn1 decoding
CSCsh21984	Yes	When out of available URL requests, future HTTP GETs dropped silently
CSCsh22262	Yes	FTP authen fails if trailing <cr> exists in banner & aaa proxy enabled
CSCsh23012	Yes	data received after static pat is removed causes traceback
CSCsh23318	Yes	When a pending URL request times out the Buffered traffic is lost
CSCsh23865	Yes	Nailed Static configuration doesn't appear in config
CSCsh25317	Yes	TCP Norm: simultaneous close specific FIN sequence problem
CSCsh25337	Yes	LSA Flush Update from IBM mainframe running OSPF are being ignored
CSCsh27267	Yes	Traceback in Thread Name: dns_process
CSCsh29038	Yes	syslog 302020 missing {in out}bound
CSCsh29233	Yes	Device reload with no saved traceback - no crashinfo file present
CSCsh29621	Yes	new url-server requests are inserted into queue in wrong order
CSCsh30022	Yes	Traceback at IKE Receiver while applying initial config with ASDM
CSCsh32241	Yes	Block size 256 depletion causing failover issues
CSCsh33290	Yes	Transparent FW passes arp requests from standby, causing arp problems
CSCsh37533	Yes	VPN Filter not applied to IOS EZVPN client with secondary inside address
CSCsh37889	Yes	Cannot use certain Verisign certificates as from 7.1(2.5)
CSCsh38298	Yes	crashinfo file only captures 4KB of console history, lose important info
CSCsh38415	Yes	ASA5500 GE NIC flatlining on bootup when connected to Cat3750
CSCsh44467	Yes	Static ARP Entry Removed From the Configuration and ARP Table
CSCsh45414	Yes	ASA Radius state machine reuses state attribute from failed auth
CSCsh47255	Yes	PIX 7.2.2 vpnfol_thread_timer traceback
CSCsh50673	Yes	OSPF: redistributed default route not installed after route flap
CSCsh53246	Yes	Traceback when specifying ldap port.
CSCsh53299	Yes	routes inherited from RRI not redistributed into OSPF after failover
CSCsh53603	Yes	Unable to resolve ARP entry for a directly connected host
CSCsh58930	Yes	TFW: Static needs route for traffic

Table 3 **Resolved Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsh60180	Yes	Traceback in snp flow bulk sync thread
CSCsh62358	Yes	CTIQBE Fixup does not work with Call Manager 4.2.1
CSCsh65168	Yes	group policy name cannot contain spaces
CSCsh66223	Yes	enhanced debug and behavior change for 'LU allocate xlate failed' syslog
CSCsh66814	Yes	SIP pinhole for inbound INVITE timesout before expires in outbound REGIS
CSCsh68174	Yes	Print warning when logging ftp-bufferwrap CLI is configured
CSCsh72961	Yes	connections matching nailed xlate never time out
CSCsh74009	Yes	Show/Clear uauth command will not work for username with spaces.
CSCsh74885	Yes	Traceback in thread accept/ssh_131071
CSCsh80069	Yes	Traceback in Thread name: vpnfol_thread_sync
CSCsh80740	Yes	ifAdminStatus stays down when no shutdown is configured
CSCsh80889	Yes	LU allocate connection failed msg due to failed VPN flow replication
CSCsh80968	Yes	ASA traceback through memory corruption
CSCsh81111	Yes	Denial-of-Service in VPNs with password expiry
CSCsh82130	Yes	Command authorization for clear fails for priv level lower than 15
CSCsh83148	Yes	Tcp Timestamp unexpectedly set to 0 for flows reordered by the firewall
CSCsh84639	Yes	cardmanager detects failover when SSM module is updated.
CSCsh86334	Yes	Syslog 199002 not sent to external syslog server on bootup
CSCsh86444	Yes	VPN: TCP traffic allowed on any port with management-access enabled.
CSCsh86796	Yes	Process qos_metric_daemon hogging CPU
CSCsh89816	Yes	ASA in transparent mode: answer-only vpn, but can still initiate VPN
CSCsh90659	Yes	Traceback: Thread Name:vpnlb_thread in standby after taking active role
CSCsh93864	Yes	sdi_work process causes high cpu in 7.1
CSCsh96805	Yes	ASA traceback in Dispatch Unit
CSCsh97976	Yes	show int ip brief shows incorrect line protocol status
CSCsi05768	Yes	ASA: DPD thresholds over 300 are not accepted for remote access
CSCsi10874	Yes	Change priority of shun command
CSCsi11941	Yes	When URL filtering is enabled Streaming Media loads slowly
CSCsi12437	Yes	Traceback in Thread Name: IPsec message handler when under heavy load
CSCsi12878	Yes	Standby traceback with mysterious 4 bytes
CSCsi17946	Yes	Traceback in Thread Name: accept/http while doing 'wr mem' in ASDM
CSCsi18097	Yes	Deleted SNMP command reappear after failover
CSCsi25877	Yes	Syslog 111008 not generated on Active when no failover active cmd issued
CSCsi31386	Yes	ASA OSPF router-id swap between multiple process after reboot
CSCsi39655	Yes	SIP: Pinhole timeout for INVITE different from REGISTER expires value

Table 3 **Resolved Caveats (continued)**

ID Number	Software Version 7.0(7)	
	Corrected	Caveat Title
CSCsi39924	Yes	standby unit reloads when 'show access-list' is issued
CSCsi41717	Yes	PIX/ASA Cannot Parse Large URI in SIP message
CSCsi43521	Yes	ASA does not include http host header in CRL request
CSCsi43722	Yes	ASA - MGCP inspection drops part of piggybacked MGCP messages
CSCsi46497	Yes	Verisign certificate lost after ASA is reloaded.
CSCsi46950	Yes	npdisk password recovery does not work with multicontext mode
CSCsi48208	Yes	assertion hdr->dispatch_last < NELTS(hdr->dispatch)
CSCsi48221	Yes	FO status switches back and forth between Standby ready and Failed
CSCsi48812	Yes	multicast: assert new_flow->conn->conn_set == NULL file snp_mcast.c
CSCsi51423	Yes	global cmd may fail using names with '-' and w/ name string overlap
CSCsi52538	Yes	wildcard mask accepted for ip local pool
CSCsi56605	Yes	TCP connection opened for WebVPN on non WebVPN enabled interfaces.
CSCsi62588	Yes	Traceback in Thread Name: aaa
CSCsi68946	Yes	Inbound traffic is being dropped due to NAT-EXEMPT rpf-check
CSCsi70522	Yes	Traceback in Thread Name: Crypto CA
CSCsi72224	Yes	SSH connection allowed to be built from inside host to outside int
CSCsi73804	Yes	IPSec over UDP port could be 4500 as auth server pushed down attr
CSCsi78808	Yes	Unable to convert dynamic ACL back to extended ACL
CSCsi83395	Yes	show interface input hardware queue counters incorrect
CSCsi84498	Yes	Traceback in Thread Name: IKE Daemon
CSCsi85823	Yes	PIX/ASA 7.X should accept RIP V1 updates like 6.X
CSCsi85856	Yes	Syslog not sent when AAA server is marked as FAILED
CSCsi89345	Yes	Failover: Standby Restart - 1550 block memory depletion
CSCsi89641	Yes	Invalid interface DHCP relay status after removing relay server entry
CSCsi89890	Yes	nat-exempt failed on non-outside interface
CSCsi91487	Yes	HTTP inspection evasion using Unicode encoding for HTTP-based attacks
CSCsi96469	Yes	asa 7.2.2 not using port specified in X509v3 CRL DP url
CSCsi98617	Yes	VPNFO: Standby stale sessions not removed
CSCsj01692	Yes	PKI: error installing Intermediate CA cert with 76 char CN
CSCsj06153	Yes	TCP sessions to the box deny issue
CSCsj16732	Yes	default-originate w/ route-map w/ acl permit host 0.0.0.0 doesn't work
CSCsj24810	Yes	vpn clients unable to connect due to DHCP Proxy processing
CSCsj32011	Yes	HTTP Apache evasion using other white space

Related Documentation

Use this document in conjunction with the security appliance 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

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 the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

© 2007 Cisco Systems, Inc.
All rights reserved.