



# Cisco PIX 500 Security Appliance Release Notes Version 7.0(8)

---

June 2008

## 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](#)
- [Related Documentation, page 14](#)
- [Obtaining Documentation and Submitting a Service Request, page 14](#)

## 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: firewall 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(8) 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](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](#)” section on [page 4](#) 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(8). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.0(8). 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(8) requires Cisco IOS Release 12.3(T) or higher running on the router when using IKE Mode Configuration on the security appliance.
Cisco VPN 3000 concentrators	Version 7.0(8) 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(8) 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(8) Cisco Easy VPN server requires Version 3.6 or higher of the Easy VPN remote release that runs on the VPN 3002 platform.
Cisco IOS Easy VPN remote Release 12.2(16.4)T	Version 7.0(8) 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(8) includes several caveat resolutions and the following features:

### Enhancement—capture Command

The **capture asp type asp-drop all** command will capture all packets that the security appliance drops.

### Enhancement—failover timeout Command

The **failover timeout** command no longer requires a failover license for use with the static nailed feature.

### Enhancement—fragment Command

The **fragment** command was enhanced with the **reassemble full** keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled.

### Enhancement—show access-list Output

Expanded access list output is indented to make it easier to read.

### Enhancement—show arp Output

In transparent firewall mode, you might need to know whether an ARP entry is statically configured or dynamically learned. ARP inspection drops ARP replies from a legitimate host if a dynamic ARP entry has already been learned. ARP inspection only works with static ARP entries. The **show arp** command shows each entry with its age if it is dynamic, or no age if it is static.

## Enhancement—show asp drop Output

The **show asp drop** command output includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the **drop reason** keywords next to the description, so you can easily use the **capture asp-drop** command using the keyword.

## Enhancement—show asp table classify Command

An enhancement was made to the **show asp table classify** command to only show rules that have a hits value not equal to zero. The enhanced **show asp table classify hits** command, enables a quick review of which rules are being hit, particularly because since a simple configuration may result in hundreds of entries in the **show asp table classify** command.

## Enhancement—show asp table counters Command

This enhancement adds a timestamp indicating when the **show asp table counters** were cleared. This keeps track of the time that the user executed the command and who executed the command, allowing the user to know how long it had been since the counters were last cleared.

## Enhancement—show conn Command Syntax

The syntax was simplified to use source and destination concepts instead of “local” and “foreign.” In the new syntax, the source address is the first address entered, and the destination is the second address. The old syntax used keywords such as **foreign** and **port** to determine the destination address and port.

## Enhancement—show perfmon Command

This enhancement added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept.

## Enhancement—static Command Error Message

An error message is generated if an actual interface IP address is used instead of the **interface** keyword when configuring static PAT.

## Ethertype ACL MAC Enhancement

EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added.

## Local Address Pool Edit

Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down.

## New—clear asp table Command

The **clear asp table** command has been added to clear the hits output displayed by the **show asp table** commands.

## New—clear conn Command

The **clear conn** command lets you clear connections, including a specific connection between hosts on particular ports. The existing **clear local-host** command clears all connections between two IP addresses (on all ports), so the new **clear conn** command offers greater control.

## New—memory tracking Commands

The following new commands are introduced in this release:

- **memory tracking enable**—This command enables the tracking of heap memory requests.
- **no memory tracking enable**—This command disables the tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system.
- **clear memory tracking**—This command clears all currently gathered information, but continues to track further memory requests.
- **show memory tracking**—This command shows currently allocated memory tracked by the tool, divided by the topmost caller function address.
- **show memory tracking address**—This command shows currently allocated memory divided by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.
- **show memory tracking dump**—This command shows the size, location, partial callstack, and a memory dump of the given memory address.
- **show memory tracking detail**—This command shows various internal details to be used in gaining insight into the internal behavior of the tool.

## Syslog Enhancements

In addition to updated syslogs for failover, SNMP, and IPSec, the following new syslogs were added: syslog for cleared TCP urgent flag, and syslog for aggressive mode aborted when spoofed.

# Important Notes

This section lists important notes related to Version 7.0(8).

## 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(8) 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 messages for Delete-with-Reason do not include 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(8), 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 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, because this configuration is not supported and Version 7.0(8) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.0(8) with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration settings related to the regular traffic interface will be lost after the upgrade. The lost configuration settings 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 the **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(8):

- PPPoE
- L2TP over IPSec
- PPTP

## MIB Supported

For information on MIB Support, go to the following URL:

<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 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 Version 7.0(8).

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 - Version 7.0(8)

Table 2 lists the open caveats for Version 7.0(8).

**Table 2** Open Caveats

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCso76065	No	Traceback when viewing access-list that is simultaneously deleted
CSCsq06129	No	PIX/ASA: Standby unit may reboot without recording a crash file
CSCso98107	No	HTTPS url stuck after large config deployment from CSM
CSCsl55476	No	HT transparent: Secondary gig3/0 port goes orange for sometime after FO
CSCsq43878	No	multi mode A/A failover write standby will see crypto CLI error in stby
CSCsj61214	No	Lower cpu-hog syslog 711002 from Level 7 to Level 4
CSCsm05455	No	Xlate timers for RTP/RTCP in version 7.0 are always 30 seconds
CSCsm20204	No	Extended ping command with no ip specified causes stuck thread
CSCso65837	No	"write mem" from HTTPS adds no monitor-interface CLIs to startup config
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCsd22469	No	DHCP relay and DHCP proxy conflict when both enabled
CSCsq46179	No	Longer timer needed for eToken credential entry

## Resolved Caveats - Version 7.0(8)

Table 3 lists the resolved caveats for Version 7.0(8).

**Table 3** Resolved Caveats

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCeg00330	Yes	DHCP relay: ACK in reply to INFORM may be dropped
CSCsc98412	Yes	Pix console accounting doesn't appear in ACS Logged-In User report
CSCsg61719	Yes	SNMP: Coldstart Trap is not sent
CSCsg96247	Yes	ASA traceback - RSA keypair generation SSH function calls

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsh55107	Yes	DHCP relay fails when static translation for all hosts configured
CSCsh74009	Yes	Show/Clear uauth command will not work for username with spaces
CSCsh91283	Yes	Inspect SunRPC drops segmented packets
CSCsi08317	Yes	PIX using Authentication Proxy and Wildcard causes Certificates error
CSCsi46292	Yes	SNMP coldstart trap not sent in failover scenario
CSCsi49983	Yes	Periodic HW crypto errors 402123 & 402125 see with L2TP/IPSEC
CSCsi53577	Yes	OSPF goes DOWN after reload of VPN Peer
CSCsi65122	Yes	Overlapping static with NAT exemption causes xlate errors on standby
CSCsi68911	Yes	ASA may traceback when pushing rules from SolSoft - corrupted conn_set_t
CSCsi84143	Yes	Mem del-free-poisoner fails to svc alloc requests from the poisoned pool
CSCsj03278	Yes	Traceback in Dispatch Unit thread (page fault)
CSCsj03706	Yes	activex or java filter suppresses the syslog message 304001
CSCsj05830	Yes	Syslog 405001 reports incorrect IP when arp collision detected
CSCsj12938	Yes	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj13797	Yes	SSH connection fails when first server in AAA group is unreachable
CSCsj20942	Yes	ASA stops accepting IP from DHCP when DHCP Scope option is configured
CSCsj31537	Yes	Interface keyword in ACL not permitting traffic
CSCsj37564	Yes	Traceback in Thread Name: IP Thread
CSCsj37760	Yes	h323 inspection does not open RTP pinholes in certain scenarios
CSCsj40295	Yes	Policy NAT not functioning properly after boot
CSCsj43076	Yes	Logging into standby ASA via SSH fails.
CSCsj44098	Yes	traceback caused by gtp inspect handling bad packets
CSCsj46062	Yes	Inconsistent state of failover pair may exist during config sync
CSCsj46729	Yes	ASA: Active and Standby unit have the same MAC address after failover
CSCsj56378	Yes	Traceback in Thread Name: Crypto CA with LDAP CRL query
CSCsj72903	Yes	Additional sanitization needed for syslog message %ASA-5-111008
CSCsj77560	Yes	Traceback in Thread Name: IKE Daemon with CRL checking
CSCsj78675	Yes	HTTP host header not included in PKI requests with terminal enrollment
CSCsj80563	Yes	ASA dynamic VPN match address disconnects some peers as duplicate proxy
CSCsj83531	Yes	Dynamic VPN phase 2 neg with ID_IPV4_ADDR_RANGE accepted as 0.0.0.0/0
CSCsj84405	Yes	Poison route causes default route in ASP routing table to be deleted
CSCsj90479	Yes	IPS and fragments cause Traceback in Thread Name: Dispatch Unit
CSCsj96831	Yes	half-closed tcp connection behaves as an absolute timer on ASA
CSCsj99660	Yes	ASA CONSOLE TIMEOUT does not timeout
CSCsk00547	Yes	Traceback in ci/console when modifying cmap inspection_default

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsk00589	Yes	Traceback in Thread Name: Dispatch Unit
CSCsk03550	Yes	ASA: Route injected through RRI disappear after failover
CSCsk05432	Yes	PKI: Default attribute for an LDAP CRL query should include a binary CRL
CSCsk06996	Yes	Leak in vpnfol_fragdb:vpnfol_fragdb_rebuild on standby
CSCsk10156	Yes	VPN traffic with static PAT to outside ip address denied by outside ACL
CSCsk18083	Yes	nat exemption access-list not checked for protocol or port when applied
CSCsk19065	Yes	Excessive High CPU and packets drops when applying ACL to an interface
CSCsk28972	Yes	Traceback:Thread Name: IKE Daemon when connecting w/ certain certificate
CSCsk39154	Yes	PIX/ASA dynamic l2l vpn does not work in 8.0.2.16
CSCsk41454	Yes	Traceback in thread name: ssh
CSCsk43103	Yes	Traceback in Thread Name emweb/https
CSCsk44832	Yes	Primary does not become active when pri & sec are booted together
CSCsk45943	Yes	PIX: proxy-arps on all interfaces for the vpn-pool
CSCsk59083	Yes	ASA 5505 failover: rebooted unit becomes active after reload
CSCsk59816	Yes	Traceback in the process Crypto CA when retrieving the CRL
CSCsk64117	Yes	CPU Hog seen generating RSA keys during SSH session establishment
CSCsk64428	Yes	High CPU when polling VPN MIBs via SNMP
CSCsk65211	Yes	ASA5505 inside interface w/23bit or smaller subnet mask becomes unstable
CSCsk65940	Yes	crashinfo file corrupted, extra text appended to bottom
CSCsk66924	Yes	ASDM: Monitoring Used memory records different stats history
CSCsk67715	Yes	During Ipsec negotiation, peer ip address is seen reversed in the debugs
CSCsk68658	Yes	ICMP (type 3 code 4) messages generated against ESP flow dropped by ASA
CSCsk68895	Yes	Traceback in thread name Dispatch Unit with IDS packet recv
CSCsk69878	Yes	ASA running 8.0.2 rejects DHCP leases less than 32 seconds
CSCsk71006	Yes	ipv6 acl don't have acl options when using MPF
CSCsk76770	Yes	vpn-filter may prevent renegotiation of the tunnel
CSCsk79728	Yes	ASA5550 7.2.3 traceback with Dispatch Unit
CSCsk80789	Yes	RTSP inspection changes Media Player version to 0.0.0.0
CSCsk81616	Yes	PIX/ASA Traceback in 'dhcp_daemon'
CSCsk85428	Yes	Traceback in scheduler
CSCsk86002	Yes	Memory accounting for aaa chunks is incorrect
CSCsk89639	Yes	Traceback with Thread Name: Checkheaps
CSCsk90689	Yes	telnet to the box and vpn tunnels fail due to 0-byte block depletion
CSCsk96804	Yes	Traceback in Thread Name: Dispatch Unit with inspect h323
CSCsk97671	Yes	VPN client with NULL Encryption L2TP-IPSec behind NAT drops on 71st sec

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCs101053	Yes	ASA doesn't handle the multiple CPS entries in the Issuing CA cert
CSCs112010	Yes	flash memory corruption issues
CSCs112449	Yes	DHCP Client - remove minimum lease time restriction
CSCs117136	Yes	H323: Video breaks with inspection enabled
CSCs119419	Yes	enabling acl-netmask-convert wildcard does not accept acl with host
CSCs123542	Yes	User Certificate mappings against the "whole field" failing
CSCs126604	Yes	Traceback in Dispatch Unit with VPN (not ported to 7.2)
CSCs128306	Yes	PIX/ASA default route redistributed into EIGRP when explicitly disabled
CSCs129315	Yes	Syslog 713902 appears on standby unit when disconnecting VPN connection
CSCs130307	Yes	PIX/ASA fails to install cert with an empty subject/issuer alt name ext
CSCs133600	Yes	Traceback when show service after removing global policy with police
CSCs137767	Yes	Traceback when timeout with L2TP and delay-free-poisoner enabled
CSCs138314	Yes	HA: SNMP trap authentication replicated to standby improperly
CSCs155623	Yes	SNMP link trap varbind list missing values
CSCs156635	Yes	Input errors remains 0 even when CRC counts up
CSCs157533	Yes	setting privilege for capture does not affect "no capture"
CSCs159247	Yes	Unable to request CRL for trustpoint with only ID certificate
CSCs159266	Yes	PKI: export/import of pkcs12 containing only ID cert fails
CSCs166758	Yes	TCP intercept comes before ACL checks. All TCP ports appear open
CSCs168785	Yes	Confusing Error message when Interfaces have overlapping networks
CSCs170685	Yes	Traceback in Thread Name: accept/http
CSCs173850	Yes	Traceback occurs when SIP session is active and switchover occurs twice
CSCs174327	Yes	Traceback in fover_parse when editing ACL config
CSCs175006	Yes	Traceback on entering command "vpnclient nem-st-autoconnect"
CSCs178638	Yes	stateful subinterface would not become Up, remains Failed
CSCs179211	Yes	Traceback: AAA task overflow when object-group acls and virtual telnet
CSCs182200	Yes	IPSec not encrypting after failover
CSCs184179	Yes	Traceback at ssh thread when working with 'capture'
CSCs187918	Yes	IPSec: RESPONDER-LIFETIME not properly created
CSCs193003	Yes	TACACS+ allow enable command but output has "Command authorization fail"
CSCs195244	Yes	Traceback in Dispatch Unit caused by rapid connection successions
CSCs195856	Yes	DHCP learned default route not in route table if other DHCP interfaces
CSCs197161	Yes	RTSP connections failing when RTSP inspection enabled
CSCs199322	Yes	Traceback at ids_put in Thread Name: Dispatch Unit
CSCsm00894	Yes	LDAP map fails for IETF-Radius-Framed-IP-Address

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsm05055	Yes	PIX traceback occurs when 'established udp 0 0' is enabled
CSCsm07888	Yes	Authenticator value on retransmitted RADIUS request pkt changed
CSCsm17247	Yes	H323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT
CSCsm18437	Yes	clear interface doesn't clear max queue counter
CSCsm22002	Yes	Traceback in qos/qos_rate_limiter while processing pakt with TCP flow
CSCsm28529	Yes	page fault in fover_parse - eip og_rem_objgrp with DFP
CSCsm29337	Yes	Dest unicast address to multicast address NAT not working in 7.x
CSCsm30926	Yes	ASA: Traceback with high voice traffic and voice inspection
CSCsm31973	Yes	SNMP walk on cefcMIBEnableStatusNotification : value returned : 2
CSCsm32972	Yes	SNMP Counters Get Stuck on Repeated Polls
CSCsm36660	Yes	DHCP Server: Must send DHCP decline if DHCP proposes in-use address
CSCsm41986	Yes	Need to handle fragmented IP packets with 8-byte first frag
CSCsm50135	Yes	Memory leakage caused by catcher_recv_packet_have_sa
CSCsm50494	Yes	Device is not able to process CRL with extension CRL number > 65535
CSCsm56957	Yes	Traceback occurs in Dispatch Unit with QoS
CSCsm57920	Yes	H323: inspection on video call may cause traceback within 5 min
CSCsm68097	Yes	SSH resource exhausted preventing further sessions
CSCsm70860	Yes	Difference of total vpn session via OID SNMP and vpn-sessiondb summary
CSCsm73565	Yes	Traceback in Thread Name Dispatch Unit during network scan
CSCsm91261	Yes	Traceback in 'ssh' thread
CSCsm92266	Yes	Traceback may occur when AAA command authorization is enabled
CSCsm93083	Yes	Syslog 713254 does not get generated for 7.0 and 7.1
CSCso08335	Yes	ISAKMP: Add syslog when Aggressive mode aborted when Spoof Protection
CSCso15583	Yes	Traceback when many remote peers try to establish ipsec L2L tunnels
CSCso17900	Yes	DFP may not background free due to memory calculation
CSCso24494	Yes	PIX/ASA: DHCP server fails to respond to Vista DHCPINFORM request
CSCso35351	Yes	Firewall may crash in thread vpnfol_thread_msg while viewing config
CSCso36070	Yes	Value returned by sysServices MIB is incorrect
CSCso40008	Yes	PIX is sending DN during rekey instead of FQDN
CSCso50996	Yes	ASA dropping the packet instead of encrypting it.
CSCso64731	Yes	security-association lifetime cannot be removed with no crypto map ...
CSCso81153	Yes	Traceback in dispatch unit with MGCP inspection
CSCso82264	Yes	ASA: icmp inspection may drop icmp error packets
CSCso84996	Yes	ASA truncates CN field at 11 characters if CN contains '@' (W2K CA)

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCso85452	Yes	h323 messages on console; performance degrade
CSCso87435	Yes	NAT-T not working when client source port not 4500 with ACL match

## 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/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)

## 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0805R)

© 2008 Cisco Systems, Inc.

All rights reserved.