



Cisco ASA 5500 Series Release Notes Version 7.2(3)

August 2007

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Supported Platforms and Feature Licenses, page 4](#)
- [New Features, page 7](#)
- [Important Notes, page 10](#)
- [Caveats, page 10](#)
- [Related Documentation, page 22](#)
- [Obtaining Documentation and Submitting a Service Request, page 22](#)

Introduction

The Cisco ASA 5500 series adaptive security appliances are purpose-built solutions that combine the most effective security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the adaptive security appliance provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network adaptive security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

For more information on all of the new features, see [New Features, page 7](#).



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

© 2007 Cisco Systems, Inc. All rights reserved.

Additionally, the adaptive security appliance software supports Cisco Adaptive Security Device Manager (ASDM). ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use web-based management interface. Bundled with the adaptive security appliance, ASDM accelerates adaptive security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of the adaptive security appliance. Its secure, web-based design enables anytime, anywhere access to adaptive security appliances.

System Requirements

The sections that follow list the system requirements for operating an adaptive security appliance. This section includes the following topics:

- [Memory Requirements, page 2](#)
- [Determining the Software Version, page 2](#)
- [Upgrading to a New Software Version, page 3](#)

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the adaptive security appliance.

Table 1 **DRAM Memory Requirements**

ASA Model	DRAM Memory
ASA 5505	256 MB
ASA 5510	256 MB
ASA 5520	512 MB
ASA 5540	1024 MB
ASA 5550	4096 MB

All adaptive security appliances require a minimum of 64 MB of internal CompactFlash.

In a failover configuration, the two units must have the same hardware configuration. They must be the same model, have the same number and types of interfaces, and the same amount of RAM. For more information, see the “Configuring Failover” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.



Note

If using two units with different flash memory sizes, make sure that the unit with the smaller flash memory has enough space for the software images and configuration files.

Determining the Software Version

Use the **show version** command to verify the software version of your adaptive security appliance. Alternatively, you can see the software version, on the Cisco ASDM home page.

Upgrading to a New Software Version

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

<http://www.cisco.com/cisco/software/navigator.html>



Note

ASA and ASDM images must be compatible, for example ASA Version 7.2(3) is compatible to ASDM Version 5.2(3). ASDM will not work with an incompatible platform version. You will get an error message and ASDM will close.

You can also use the command-line interface to download the image, see the “Downloading Software or Configuration Files to Flash Memory” section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.1.(x) to 7.2(3), you must perform the following steps:

-
- Step 1** Load the new 7.2(3) image from the following website:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 2** Reload the device so that it uses the 7.2(3) image.
 - Step 3** Load the new ASDM 5.2.(x) image from the following website:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 4** Enter the following command; this will tell the adaptive security appliance where to find the ASDM image:
hostname(config)# **asdm image disk0:/ asdm file**
-

To downgrade from Version 7.2(3) to 7.1.(x), you must perform the following steps:

-
- Step 1** Load the 7.1(x) image from the following website:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 2** Reload the device so that it uses the 7.1(x) image.
 - Step 3** Load the ASDM 5.1(x) image from the following website:
<http://www.cisco.com/cisco/software/navigator.html>
 - Step 4** Enter the following command; this will tell the adaptive security appliance where to find the ASDM image:
hostname(config)# **asdm image disk0:/ asdm file**
-

Supported Platforms and Feature Licenses

This software version supports the following platforms; see the associated tables for the feature support for each model:

- ASA 5505, [Table 2](#)
- ASA 5510, [Table 3](#)
- ASA 5520, [Table 4](#)
- ASA 5540, [Table 5](#)
- ASA 5550, [Table 6](#)



Note

Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

Table 2 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Users, concurrent ¹	10	<i>Optional Licenses:</i>	10	<i>Optional Licenses:</i>
		50 Unlimited		50 Unlimited
Security Contexts	No support		No support	
VPN Sessions ²	10 combined IPSec and WebVPN		25 combined IPSec and WebVPN	
Max. IPSec Sessions	10		25	
Max. WebVPN Sessions	2	<i>Optional License: 10</i>	2	<i>Optional License: 10</i>
VPN Load Balancing	No support		No support	
Failover	None		Active/Standby (no stateful failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns ³	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Minimum RAM	256 MB		256 MB	

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit only when they communicate with the outside (Internet VLAN). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host command** to view the host limits.
2. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
3. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table 3 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License						Security Plus					
Users, concurrent	Unlimited						Unlimited					
Security Contexts	No support						2	Optional Licenses:				
								5				
VPN Sessions ¹	250 combined IPSec and WebVPN						250 combined IPSec and WebVPN					
Max. IPSec Sessions	250						250					
Max. WebVPN Sessions	2	Optional Licenses:					2	Optional Licenses:				
		10	25	50	100	250		10	25	50	100	250
VPN Load Balancing	No support						No support					
Failover	None						Active/Standby or Active/Active					
GTP/GPRS	No support						No support					
Max. VLANs	50						100					
Concurrent Firewall Conns ²	50 K						130 K					
Max. Physical Interfaces	Unlimited						Unlimited					
Encryption	Base (DES)		Optional license: Strong (3DES/AES)				Base (DES)		Optional license: Strong (3DES/AES)			
Min. RAM	256 MB						256 MB					

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 4 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License							
Users, concurrent	Unlimited					Unlimited		
Security Contexts	2	Optional Licenses:						
		5	10	20				
VPN Sessions ¹	750 combined IPSec and WebVPN							
Max. IPSec Sessions	750							
Max. WebVPN Sessions	2	Optional Licenses:						
		10	25	50	100	250	500	750
VPN Load Balancing	Supported							
Failover	Active/Standby or Active/Active							
GTP/GPRS	None		Optional license: Enabled					
Max. VLANs	150							
Concurrent Firewall Conns ²	280 K							
Max. Physical Interfaces	Unlimited							

Table 4 ASA 5520 Adaptive Security Appliance License Features (continued)

ASA 5520	Base License	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Min. RAM	512 MB	

- Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 5 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License									
Users, concurrent	Unlimited						Unlimited			
Security Contexts	2	Optional licenses:								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None		Optional license: Enabled							
Max. VLANs	200									
Concurrent Firewall Conns ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		Optional license: Strong (3DES/AES)							
Min. RAM	1 GB									

- Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 6 ASA 5550 Adaptive Security Appliance License Features

ASA 5550	Base License										
Users, concurrent	Unlimited										
Security Contexts	2	Optional licenses:									
		5	10	20	50						
VPN Sessions ¹	5000 combined IPSec and WebVPN										
Max. IPSec Sessions	5000										
Max. WebVPN Sessions	2	Optional Licenses:									
		10	25	50	100	250	500	750	1000	2500	5000

Table 6 **ASA 5550 Adaptive Security Appliance License Features (continued)**

ASA 5550	Base License	
VPN Load Balancing	Supported	
Failover	Active/Standby or Active/Active	
GTP/GPRS	None	<i>Optional license: Enabled</i>
Max. VLANs	250	
Concurrent Firewall Conns ²	650 K	
Max. Physical Interfaces	Unlimited	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Min. RAM	4 GB	

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

New Features

This section lists the new features for Version 7.2(3). All new features are supported in ASDM 5.2(3).

ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1

The ASA 5510 adaptive security appliance now has the security plus license to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from base to security plus, the capacity of the external port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface

ASA 5505 Increased VLAN range

The ASA 5505 adaptive security appliance now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported.

Smart Card Removal Disconnect

This feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clients (both IPSec and SSL) will, by default, tear down existing VPN tunnels when the user removes the Smart Card used for authentication. The following cli command disconnects existing VPN tunnels when a smart card is removed. This option is enabled by default.

```
smartcard-removal-disconnect {enable|disable}
```

capture Command Enhancement

The enhancement to the **capture** command allows the user to capture traffic and display it in real time. It also allows the user to specify command line options to filter traffic without having to configure a separate access list. This enhancement adds the [real-time] and a five-tuple [match] options.

```
capture <cap_name> [[real-time] [dump] [detail [trace]] [match <prot> {host <ip> | <ip>
<mask> | any} [eq | lt | gt <port>] {host <ip> | <ip> <mask> | any} [eq | lt | gt
<port>]]
```

Support for ESMTP over TLS

This enhancement adds the configuration parameter allow-tls [action log] in the esmtp policy-map. By default, this parameter is not enabled. When it is enabled, ESMTP inspection would not mask the 250-STARTTLS echo reply from the server nor the **STARTTLS** command from the client. After the server replies with the 220 reply code, the ESMTP inspection turns off by itself— the ESMTP traffic on that session is no longer inspected. If the allow-tls action log parameter is configured, the system log message ASA-6-108007 is generated when TLS is started on an ESMTP session.

```
policy-map type inspect esmtp esmtp_map
parameters
allow-tls [action log]
```

A new line for displaying counters associated with the allow-tls parameter is added to the **show service-policy inspect esmtp** command. It is only present if allow-tls is configured in policy map. By default, this parameter is not enabled.

```
show service-policy inspect esmtp
allow-tls, count 0, log 0
```

This enhancement adds a new system log message for the allow-tls parameter. It indicates on an esmtp session the server has responded with a 220 reply code to the client **STARTTLS** command. The ESMTP inspection engine will no longer inspect the traffic on this connection.

System log Number and Format:

```
%ASA-6-108007: TLS started on ESMTP session between client <client-side interface-name>:<client
IP address>/<client port> and server <server-side interface-name>:<server IP address>/<server port>
```

DHCP Client

The **dhcp-client client-id interface <interface name>** command forces a MAC address to be stored inside a DHCP request packet instead of the default internally generated unique string. This CLI allows the adaptive security appliance to obtain a DHCP address from the ISP with this special requirement.

WAAS and ASA Interoperability

The **[no] inspect waas** command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The **[no] inspect waas** command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default.

The keyword option waas is added to the **show service-policy inspect** command to display WAAS statistics.


```
show service-policy inspect waas
```

A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections.

System Log Number and Format:

```
%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to
out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.
```

A new connection flag "W" is added in the WAAS connection. The **show conn detail** command is updated to reflect the new flag.

ASDM Banner Enhancement

The adaptive security appliance Version 7.2(3) software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog box with the option to continue or disconnect. The Continue option dismisses the banner and completes login as usual whereas, the Disconnect option dismisses the banner and terminates the connection. This enhancement requires the customer to accept the terms of a written policy before connecting. Following is the new CLI associated with this enhancement:

```
banner {exec | login | motd | asdm} <text>
no banner {exec | login | motd | asdm} [<text>]
show banner [{exec | login | motd | asdm}]
clear banner
```

WebVPN load Balancing

The adaptive security appliance now supports the use of FQDNs for load balancing. To perform WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balancing, enter the **redirect-fqdn enable** command. Then add an entry for each of your adaptive security appliance outside interfaces into your DNS server if not already present. Each adaptive security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup. Enable DNS lookups on your adaptive security appliance with the **dns domain-lookup inside** command (or whichever interface has a route to your DNS server). Finally, you must define the ip address, of your DNS server on the adaptive security appliance. Following is the new CLI associated with this enhancement:

```
[no] redirect-fqdn {enable | disable}
default: disable
```

cache Command Changes

There are two changes to the clientless SSL VPN caching commands:

The **cache-compressed** command is deprecated.

The new **cache-static-content** command configures the security appliance to cache all static content, which means all cacheable Web objects that are not subject to SSL VPN rewriting. This includes content such as images and PDF files.

The syntax of the command is **(no) cache-static-content enable | disable**. By default, static content caching is disabled.

Example:

```
hostname (config) # webvpn
hostname (config-webvpn) # cache
hostname (config-webvpn-cache) # cache-static-content enable
hostname (config-webvpn-cache) #
```

Important Notes

This section lists important notes.

sysopt uauth allow-http-cache Command

The **sysopt uauth allow-http-cache** command is deprecated as this command isn't needed for compatibility with current browsers.

Features not Supported

The PPTP feature is not supported.

Caveats

The following sections describe the caveats for the Version 7.2(3).

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://tools.cisco.com/Support/BugToolKit/>

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

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

Open Caveats - Version 7.2(3)

[Table 7](#) lists open caveats for Version 7.2(3).

Table 7 **Open Caveats**

DDTS Number	Software Version 7.2(3)	
	Corrected	Caveat
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCej04099	No	static xlate breaks management-access inside
CSCsc98412	No	PIX console accounting doesn't appear in ACS Logged-In User report
CSCse29407	No	pim accept-register list documentation issue
CSCse93941	No	add acl logging capability to vpn-filter
CSCsf25418	No	Traceback in Thread Name: tmatch compile after assert
CSCsg47023	No	L2TP Connections with Certificates to ASA Fail to Connect
CSCsg63145	No	Traceback with Thread Name: PIX Garbage Collector
CSCsg65434	No	Multiple ipsec peers : PIX/ASA stops processing the IPSEC peers list
CSCsg71579	No	Programming assertion malloc.c:3822 on secondary after failover from pri
CSCsg99492	No	SASL GSSAPI-Kerberos authentication not happening with Sunone Server
CSCsh48208	No	Directly connected network missing in route table
CSCsh78681	No	In use memory count displayed incorrectly
CSCsh91283	No	ASA/PIX: SunRPC inspect dropping packets on 7.0.6
CSCsi00074	No	Incorrect values returned by SSL VPN OIDs
CSCsi04673	No	FW may drop packets when VPN address pool overlaps with interface subnet
CSCsi32502	No	packet/byte counters are not populated for the session table of CRAS MIB
CSCsi35603	No	L2TP/IPSec sessions hanging when authenticating with EAP
CSCsi40796	No	ASA fails rekey with Checkpoint
CSCsi45911	No	ASA cpu approaches 100%, 80 byte blocks are leaked and mem>0 w/ssl str
CSCsi52176	No	TCP Normalizer Traceback in Thread Name: Dispatch Unit
CSCsi53577	No	OSPF goes DOWN after reload of VPN Peer
CSCsi68911	No	ASA may traceback when pushing rules from SolSoft - corrupted conn_set_t
CSCsi80155	No	memory leak found during batch test of malformed HTTP messages
CSCsi94163	No	PPPOE connection does not renegotiate immediatly after short disconnect
CSCsi98617	No	VPNFO: Standby stale sessions not removed
CSCsj01620	No	Type 0 Client-ID for RA clients not supported by some DHCP servers
CSCsj01643	No	IPSec VPN first auth fails when SDI SoftID is in Cleared PIN Mode
CSCsj02948	No	%ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error
CSCsj03437	No	WebVPN: RDP Icon fails after a redirect action to a Citrix Presentation
CSCsj07428	No	Idle IPSEC connections not closing out
CSCsj10151	No	Traceback in Dispatch Unit (possible double-free)
CSCsj12938	No	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj18055	No	Traceroute fails through ASA if outside interface is pppoe and doing PAT

Table 7 **Open Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsj19607	No	Traceback in Checkheaps - mem corruption PC on stride_list_node
CSCsj19904	No	Traceback in Thread Name: OSPF Router
CSCsj29444	No	VPN Client authentication fails with Novell Radius and Active Card
CSCsj32989	No	ASA traceback when running 100 user Avalanche webvpn goodput test
CSCsj42343	No	PIX 525 - bad vpif msgs are from the vpnfo module
CSCsj43076	No	Logging into standby ASA via SSH fails.
CSCsj43703	No	ASA mem leak on CRYPTO_malloc
CSCsj49481	No	WebVPN: HTTPS Page not rendered correctly while HTTP works fine
CSCsj56287	No	Traceback in Thread Name: ssh/timer
CSCsj61214	No	Lower cpu-hog syslog 711002 from Level 7 to Level 4
CSCsj66655	No	Duplicate ASP crypto table entry forwards VPN traffic using invalid SPI
CSCsj68874	No	Inspect HTTP invokes multiple times with interface service-policy
CSCsj74539	No	Traceback on Standby in Thread Name: fover_FSM_thread
CSCsj77641	No	Viewing QoS policing statistics may create traceback
CSCsj80196	No	Clientless WebVPN traffic not sent when matching crypto dynamic map ACL
CSCsj80563	No	ASA dynamic VPN match address disconnects some peers as duplicate proxy
CSCsj82413	No	QoS: class-map : match tunnel-group <tgrp-name> errors on reboot
CSCsj84640	No	Memory leak on CRYPTO_malloc
CSCsj87886	No	Failover conn replication fails while doing bidirectional NAT
CSCsj90274	No	Citrix sessions randomly disconnect
CSCsj90479	No	Traceback in Thread Name: Dispatch Unit
CSCsj92194	No	Implicit ACL 'Deny IP Any Any' Ignored on EasyVPN Client
CSCsj96159	No	Traceback when freeing a packet from TCP_MOD function
CSCsj96831	No	half-closed tcp connection behaves as an absolute timer on ASA
CSCsj97241	No	80 byte block depletion with stateful failover enabled
CSCsj98622	No	SIP: Not translate c= address if first m= has port 0 in SDP body.
CSCsj99182	No	Traceback on Standby box in Thread IPsec message handler
CSCsj99242	No	Assert: Traceback in Thread Name: Dispatch Unit
CSCsj99660	No	ASA CONSOLE TIMEOUT does not timeout
CSCsk00072	No	ASA 7.2 Firewall-MIB : no snmp object for failover lan int status
CSCsk00089	No	ASA 7.2 : Firewall-MIB : no snmp object for failover lan int status
CSCsk00589	No	Traceback in Thread Name: Dispatch Unit
CSCsk03550	No	ASA: Route injected through RRI disappear after failover
CSCsk04594	No	traceback: watchdog crash in uauth thread

Table 7 **Open Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsk05453	No	Programming assertion while configuring http inspection policy
CSCsk06996	No	Leak in vpnfol_fragdb:vpnfol_fragdb_rebuild on standby

Resolved Caveats - Version 7.2(3)

[Table 8](#) lists resolved caveats for Version 7.2(3).

Table 8 **Resolved Caveats**

DDTS Number	Software Version 7.2(3)	
	Corrected	Caveat
CSCeg00330	Yes	DHCP relay: ACK in reply to INFORM may be dropped
CSCsb45561	Yes	standby instead of active keeps sending register to RP after failover
CSCsd43563	Yes	Crypto accelerator errors seen - connections failing
CSCsd51407	Yes	Dual ISP fails after failover, routing table have stale routes
CSCse14419	Yes	ASA 7.0(4) : not randomizing TCP SACK sequence numbers
CSCse21181	Yes	Decouple Passwd-Mngt checks from LDAP Authentication-Search
CSCse49440	Yes	SNMP: incorrect cpu usage sent for CISCO-PROCESS-MIB
CSCse88291	Yes	Traceback with WEBVPN user login when memory is running low.
CSCsf30571	Yes	Traceback in ssh_init
CSCsg08640	Yes	access-list damaged and frozen, clear config acl has no effect
CSCsg09071	Yes	L2TP over IPSEC disconnections syslog are always-'User requested'
CSCsg16149	Yes	data sent with Active MAC after switchover to standby
CSCsg39936	Yes	Pix/ASA: Disabling pim on subinterface causes other interface mcast fail
CSCsg43591	Yes	SCP connection to PIX fails
CSCsg52106	Yes	Embryonic value -1 under syslog and count to host = 42949672
CSCsg53120	Yes	ASA WebVPN Time-out on Database Requests
CSCsg56876	Yes	WebVPN: traceback after applying http or IM deep inspection
CSCsg60095	Yes	VPN traffic permitted by vpn-filter is denied
CSCsg61719	Yes	SNMP: Coldstart Trap is not sent
CSCsg68181	Yes	WebVpnPortForward Java applet Certificate Expired
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
CSCsg70698	Yes	Session timer is not reset during WebVPN ActiveX and Java tunneling

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsg76777	Yes	7.2 transparent / change of behavior : ASA does not retain the src mac
CSCsg77099	Yes	WebVPN Java archives with uncompressed entries fail through rewriter
CSCsg78524	Yes	NT Authentication (NTLM) is attempted three times with a bad password
CSCsg80370	Yes	memory leak in ftp inspection causes high cpu
CSCsg81621	Yes	Cannot authenticate user on first attempt with Unite application.
CSCsg83130	Yes	Device reload with no crashinfo file
CSCsg86020	Yes	web terminal services through webvpn on ASA might not work.
CSCsg86507	Yes	Standby traceback in dispatch unit when enabling 'per-client-max' MPF
CSCsg86538	Yes	Dynamic L2L tunnel fails if the remote peer ip is changed
CSCsg86583	Yes	JavaScript rewriting of typeof followed by src
CSCsg87808	Yes	'wr mem' fails due to snmp config; Error: (Configuration line too long)
CSCsg87815	Yes	sync config with long snmp configuration causes traceback on active unit
CSCsg87891	Yes	WebVPN: Homepage is not accessible when url-entry is disabled.
CSCsg88048	Yes	WebVPN Terminal Server ActiveX control not installed when using WebVPN
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
CSCsg93050	Yes	Inspect DCERPC failure. Packet too small error
CSCsg94165	Yes	Device reload when quit (hit q) from <more> console paged display
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
CSCsg96247	Yes	ASA traceback - RSA keypair generation SSH function calls
CSCsg96351	Yes	http regex matching fails to match http://
CSCsg96701	Yes	traceback at Thread PIM IPv4
CSCsg96891	Yes	ASA 7.2.2.1 Traceback: Unicorn Proxy Thread
CSCsg97348	Yes	FW replying to port application requests that are not active using VPN.
CSCsg99807	Yes	ICMP (type3, code4) is not sent after learning PMTU
CSCsh01646	Yes	pptp inspect does not alter Call ID in some packets
CSCsh05517	Yes	EAP state engine triggers retransmission. Clients reply terminates LCP
CSCsh05888	Yes	Standby traceback in vpnfol_thread_msg
CSCsh06232	Yes	PIX does not open RTP connections for H323 calls
CSCsh12413	Yes	FO: Syslog 111111: Memory requested from Null Chunk seen every min.
CSCsh12711	Yes	Traceback in TCP Normalizer
CSCsh14023	Yes	TACACS+ CMD Accounting packets have a Caller-ID field of 0.0.0.0

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsh15587	Yes	Garbage characters printed on console at end of long show cmd
CSCsh16767	Yes	WebVPN: DWA problem with sending attachments
CSCsh17164	Yes	ping command within CONTEXT causes SSH session to hang.
CSCsh18659	Yes	ASA-WebVPN: Java Applet for Cisco Unix ACS management doesn't load
CSCsh19536	Yes	VPN-FO: Sessions not cleaned up correctly on Standby
CSCsh20618	Yes	80-byte block memory leak with asn1 decoding
CSCsh21446	Yes	Req Method HEAD is dropped when proto-violation is on at inspect HTTP
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
CSCsh22531	Yes	ASA: Qos Policing only works when in input direction
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 doesnt appear in config
CSCsh23910	Yes	ASDM Shows no IP & Line Down for all interfaces
CSCsh25317	Yes	TCP Norm: simultaneous close specific FIN sequence problem
CSCsh25337	Yes	LSA Flush Update from IBM mainframe running OSPF are being ignored
CSCsh26607	Yes	'inspect skinny' drops/corrupts packets with high network latency
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
CSCsh33287	Yes	Users with priv 0 can get to level 15 when authen. ena. LOCAL configured
CSCsh33290	Yes	Transparent FW passes arp requests from standby, causing arp problems
CSCsh33982	Yes	(E)SMTP Multiple Content-Type headers check is wrong
CSCsh35400	Yes	Not able to login to a server through webvpn
CSCsh35548	Yes	Catalyst EEPROM in ASA5505 failed mfg testing.
CSCsh35715	Yes	ESMTP inspection drops emails with special characters in the email addr
CSCsh36387	Yes	ASA 5510 7.2.2 / traceback in Thread Name: IKE Daemon
CSCsh36559	Yes	SVC session not replicated to stdby when addr pool defined in grp policy
CSCsh37533	Yes	VPN Filter not applied to IOS EZVPN client with secondary inside address
CSCsh37755	Yes	Certificate installation fails if 2 CA certs have same issuer name
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

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsh38415	Yes	ASA5500 GE NIC flatlining on bootup when connected to Cat3750
CSCsh40829	Yes	LDAP: multiple Cisco-AV-Pair need to be enforced on vpn-session
CSCsh41155	Yes	ASA h323 inspect corrupts q931 packet
CSCsh41496	Yes	ldap-login-dn requires full path name of admin user
CSCsh42793	Yes	LDAP Authentication bypass Vulnerability
CSCsh43698	Yes	Audio and Video doesnot flow thru SIP Trunk after MOH and Resume
CSCsh44239	Yes	Tunnel might not establish with AO and OO connection types configured
CSCsh44467	Yes	Static ARP Entry Removed From the Configuration and ARP Table
CSCsh45169	Yes	ASA uses tunneled route to contact LDAP server instead of default GW
CSCsh45414	Yes	ASA Radius state machine reuses state attribute from failed auth
CSCsh46436	Yes	Radius NAS-Port-Type not sent in SSH authentication request
CSCsh47255	Yes	PIX 7.2.2 vpnfol_thread_timer traceback
CSCsh48962	Yes	Duplicate ASP table entry causes FW to encrypt traffic with invalid SPI
CSCsh49714	Yes	Traceback in Thread Name: emweb/cifs at Failover
CSCsh50277	Yes	Multiple DHCP ACKs to an INFORM message may cause 1550 block leak
CSCsh50399	Yes	Inspect FTP hold 254 MB memory after 12+ hr real world FTP test load
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
CSCsh53409	Yes	ASDM sessions authenticated using RADIUS have incorrect privilege level
CSCsh53603	Yes	Unable to resolve ARP entry for a directly connected host
CSCsh53681	Yes	ASA OCSP RESP CERT verification fails if response has no responder CERT
CSCsh54016	Yes	PIX 7.2.2 memory degradation
CSCsh56084	Yes	ASA CIFS over WebVPN : file created on server but write operation fails
CSCsh56439	Yes	Multicast: Crash in Thread Name: MFIB
CSCsh57791	Yes	Webvpn shows aspx file as blank pop-up page
CSCsh58003	Yes	IPCP not coming up when using 'ip address pppoe'
CSCsh58930	Yes	TFW: Static needs route for traffic
CSCsh59098	Yes	Traceback at ThreadName: Unicorn Proxy Thread(pc 0x00c5a9a4 ebp 0x0dd71cc
CSCsh60180	Yes	Traceback in snp flow bulk sync thread
CSCsh60848	Yes	Traceback in regex_nvclr() from fover_parse thread
CSCsh60896	Yes	ESMTP inspection hogging CPU
CSCsh61351	Yes	ASA DNS load balancing http redirect sends wrong ip if reverse DNS fails
CSCsh61431	Yes	VPNLB: http redirect does not work when using non-default webvpn port
CSCsh62358	Yes	CTIQBE Fixup does not work with Call Manager 4.2.1

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsh62362	Yes	Default for WebVPN Cache on 7.1/7.2 should be 'disabled'
CSCsh63333	Yes	Memory leak with CIFS share access via WebVPN
CSCsh65168	Yes	group policy name cannot contain spaces
CSCsh66209	Yes	Traceback at Thread Name: Dispatch Unit(Old pc 0x00218f77 ebp 0x018724a8
CSCsh66223	Yes	enhanced debug and behavior change for 'LU allocate xlate failed' syslog
CSCsh66576	Yes	L2TP: Connectivity issues with 1500 established sessions
CSCsh66814	Yes	SIP pinhole for inbound INVITE timeout before expires in outbound REGIS
CSCsh67105	Yes	ASA 7.2(2): high cpu usage with DHCP assigned IP addresses
CSCsh68174	Yes	Print warning when logging ftp-bufferwrap CLI is configured
CSCsh71039	Yes	PIX 7.2.2: L2TP client receives ip 255.255.255.255 from RADIUS server
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
CSCsh75977	Yes	Automatically added AAA commands break Easy VPN client after reboot
CSCsh78219	Yes	7.1.2.5 or later sw Will Not work in Fover with 7.1.1-7.1.2.4 on ASA/SSM
CSCsh78335	Yes	Webvpn - Non-standard JAR manifest digests
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
CSCsh82286	Yes	tcp transfers through firewall fail with inspect im enabled
CSCsh83148	Yes	Tcp Timestamp unexpectedly set to 0 for flows reordered by the firewall
CSCsh83925	Yes	ASA traceback in Thread Name: EAPoUDP
CSCsh84380	Yes	Traceback in Thread Name: fover_parse when reloading primary w/syst
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
CSCsh89784	Yes	PIX/ASA Packet capture w/ ACL does not work for locally generated packet
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
CSCsh92960	Yes	broadcast flag set on dhcp request but not discover
CSCsh96805	Yes	ASA traceback in Dispatch Unit
CSCsh96817	Yes	L2TP: Can not connect more than one Vista client at the same time

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsh97584	Yes	video connection through ASA fails
CSCsh97976	Yes	show int ip brief shows incorrect line protocol status
CSCsh98679	Yes	ASA: WCCP packets redirected stops incrementing after 2-3 mins
CSCsh98826	Yes	WebVPN: Check CLSID in CSCO_is_java_obj
CSCsi00177	Yes	HTTP inspection does not properly support chunked transfer encoding
CSCsi01498	Yes	ESMTP inspect cannot handle content-type string in DKIM headers
CSCsi03576	Yes	Webvpn: OWA 2000 replies/forwards fail after upgrading to latest hotfix
CSCsi05471	Yes	webvpn crash with citrix
CSCsi05768	Yes	ASA: DPD thresholds over 300 are not accepted for remote access
CSCsi06469	Yes	Inactiviting then reactivating nat 0 multiple access-lists breaks nat 0
CSCsi08103	Yes	command author does not mark aaa-server dead when TACACS unavailable
CSCsi08957	Yes	SNMPv2-SMI enterprises.3076.2.1.2.26.1.2.0 not showing actual connection
CSCsi10396	Yes	ASA crashes at Thread Name: emweb/https while file uploading >1MB
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
CSCsi13865	Yes	SNMP in multi-mode creates message vPif_getVpif: bad vPifNum
CSCsi15805	Yes	SNMP interface counters incorrect on ASA-5505
CSCsi15853	Yes	SiteMinder SSO not sending cookie after authentication
CSCsi16248	Yes	Denial of Service in SSL VPNs
CSCsi17946	Yes	Traceback in Thread Name: accept/http while doing 'wr mem' in ASDM
CSCsi18097	Yes	Deleted SNMP command reappear after failover
CSCsi18736	Yes	IPSec RA session not replicated to standby if addr pool in group policy
CSCsi20384	Yes	ASDM: 5.2 and 6.0 does not display historic graphs for Blocks
CSCsi21160	Yes	ASA NAC revalidation timer triggers frequently under some conditions
CSCsi21431	Yes	Traceback in Thread Name: IP Address Assign
CSCsi21488	Yes	WebVPN: Traceback in Thread Name: vpnfol_thread_msg on Standby
CSCsi21595	Yes	Watch dog timeout crash due to large# of vlans cfgd on the 4GE port
CSCsi23369	Yes	VPNLB master may lose communication with cluster member
CSCsi23740	Yes	ESMTP inspect does not match content-type properly in mail headers
CSCsi24458	Yes	DHCP Client unable to obtain IP address because of Client-ID
CSCsi25877	Yes	Syslog 111008 not generated on Active when no failover active cmd issued
CSCsi27609	Yes	ASA may drop subsequent requests on INVITE dialog
CSCsi27755	Yes	ASA 7.2.2.16 Traceback in Thread Name: emweb/https
CSCsi31386	Yes	ASA OSPF router-id swap between multiple process after reboot

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsi34289	Yes	Traceback in Thread Name: ddns_update_process with DDNS update
CSCsi34789	Yes	ASA: Cut-Through Proxy fails over L2L tunnel with http error
CSCsi35953	Yes	Asa 7.2 webvpn session with certif cannot establish when CN contains /
CSCsi39655	Yes	SIP: Pinhole timeout for INVITE different from REGISTER expires value
CSCsi39669	Yes	Traceback in Thread Name: Dispatch Unit with app-fw
CSCsi39924	Yes	standby unit reloads when 'show access-list' is issued
CSCsi40553	Yes	Asa 7.2.2 Failover : the secondary gets a modified config from the prima
CSCsi41717	Yes	PIX/ASA Cannot Parse Large URI in SIP message
CSCsi41976	Yes	Jitter for established connection when compiling ACE's
CSCsi42073	Yes	ASA boot time around 4 hours when ACE config is very long
CSCsi42140	Yes	WebVPN: JavaScript menu is not expandable
CSCsi42338	Yes	PIX/ASA aaa authentication does not work over VPN tunnel : NT,LDAP,SDI
CSCsi43521	Yes	ASA does not include http host header in CRL request
CSCsi43722	Yes	ASA - MGCP inspection drops part of piggybacked MGCP messages
CSCsi43813	Yes	SVC clients are unable to connect to the standby after ASA failover
CSCsi44506	Yes	Traceback in Dispatch thread - softnp sending garbage to sal layer
CSCsi46292	Yes	SNMP coldstart trap not sent in failover scenario
CSCsi46497	Yes	Verisign certificate lost after ASA is reloaded.
CSCsi46950	Yes	npdisk password recovery does not work with multicontext mode
CSCsi47110	Yes	vpn-simultaneous-logins 0 denies management access to the ASA
CSCsi47957	Yes	WebVPN: Traceback in Thread Name: Unicorn Proxy Thread
CSCsi48208	Yes	assertion hdr->dispatch_last < NELTS(hdr->dispatch)
CSCsi48812	Yes	multicast: assert new_flow->conn->conn_set == NULL file snp_mcast.c
CSCsi50632	Yes	NAT: Exempt causing 5505 to crash in <nat_rule_to_cli+293 at pix/cmd/c_n
CSCsi51423	Yes	global cmd may fail using names with '-' and w/ name string overlap
CSCsi51600	Yes	Misleading prompt with radius/sdi authentication on 7.2.2
CSCsi52370	Yes	WCCP may result in 1550 block depletion & sends GRE packets >1500
CSCsi52538	Yes	wildcard mask accepted for ip local pool
CSCsi54132	Yes	Not getting syslog 302010 message
CSCsi54517	Yes	Traceroute not working using l2tp/ipsec client to the outside network
CSCsi55798	Yes	assert in webvpn functionality as CRLF not detected where expected
CSCsi56605	Yes	TCP connection opened for WebVPN on non WebVPN enabled interfaces.
CSCsi57504	Yes	Traceback in Dispatch Unit when no route for nat traffic from SSM
CSCsi58109	Yes	ASA requests username/password until next available aaa server found
CSCsi59403	Yes	Standby: Traceback Thread Name: fover_parse with fover and ifc mac cfgd

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsi60580	Yes	WebVPN: Incorrect rewriting of VBScript's parent.window.location.hr
CSCsi62588	Yes	Traceback in Thread Name: aaa
CSCsi63099	Yes	ASA traceback w/ Thread Name: Unicorn Proxy Thread
CSCsi67016	Yes	Traceback in Thread Name: Dispatch Unit
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
CSCsi73181	Yes	vpn-simultaneous-logins/access hrs controls the admin sessions SSH,ASDM
CSCsi73804	Yes	IPSec over UDP port could be 4500 as auth server pushed down attr
CSCsi74352	Yes	ESMTP blocking emails with nested MIME headers
CSCsi74710	Yes	WEBVPN: port-forwarding converts names to IP addresses
CSCsi75355	Yes	5505 WebVPN: hw accelerator errors with >1024 bit cert
CSCsi78808	Yes	Unable to convert dynamic ACL back to extended ACL
CSCsi79393	Yes	Standby ASA reloads in thread vpnfol_thread_msg
CSCsi83144	Yes	Need to mask password in debug aaa common output
CSCsi83395	Yes	show interface input hardware queue counters incorrect
CSCsi84498	Yes	Traceback in Thread Name: IKE Daemon
CSCsi85790	Yes	Traceback in Thread Name: IP Thread when configuring PPPoE
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
CSCsi88508	Yes	WebVPN shows Blank Page
CSCsi89345	Yes	Failover: Standby Restart - 1550 block memory depletion
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
CSCsi98464	Yes	ASA injects another 'BrowserProtocol' keyword in ICA file
CSCsi99518	Yes	show asdm history does not show interface statistics
CSCsj01692	Yes	PKI: error installing Intermediate CA cert with 76 char CN
CSCsj03278	Yes	Traceback in Dispatch Unit thread (page fault)
CSCsj03706	Yes	activex or java filter suppresses the syslog message 304001
CSCsj05188	Yes	WEBVPN TSWeb fails: connect button is grayed out
CSCsj05830	Yes	Syslog 405001 reports incorrect IP when arp collision detected
CSCsj06153	Yes	TCP sessions to the box deny issue
CSCsj06868	Yes	ASA port of pix CSCsi95902 ppp freed memory access on session close
CSCsj10082	Yes	ASA - Traceback in tcp_send_pending

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(3)	
CSCsj10869	Yes	SNMP interface counters incorrect on PIX/ASA 7.2.2.22
CSCsj12843	Yes	SVC disconnects after idle-timeout even if traffic is passing
CSCsj16732	Yes	default-originate w/ route-map w/ acl permit host 0.0.0.0 doesn't work
CSCsj18218	Yes	ASA hangs when processing Citrix data
CSCsj19829	Yes	WebVPN: http-proxy interferes with port-forward
CSCsj20254	Yes	syslog 716046 on standby causing traceback
CSCsj20403	Yes	WebVPN: port-forward command shows up twice in the config
CSCsj20438	Yes	SSL VPN's logged off are not removed from standby sessiondb
CSCsj20942	Yes	ASA stops accepting IP from DHCP when DHCP Scope option is configured
CSCsj24810	Yes	vpn clients unable to connect due to DHCP Proxy processing
CSCsj24914	Yes	vpn-simultaneous-logins does not work when configuring PKI and no-xauth
CSCsj28634	Yes	WebVPN: BAAN ERP application with SSA Webtop fails
CSCsj31537	Yes	Interface keyword in ACL not permitting traffic
CSCsj36241	Yes	%ASA-1-111111: Invalid function called in NVGEN of 'port-forward'
CSCsj36655	Yes	ASA 5505 and 5550 continuous crash on startup
CSCsj37564	Yes	Traceback in Thread Name: IP Thread
CSCsj38362	Yes	Traceback in Thread Name: fover_parse
CSCsj40248	Yes	ASA cifs: no error indication when file upload fails due to emweb server
CSCsj40295	Yes	Policy NAT not functioning properly after boot
CSCsj40648	Yes	Traceback in Thread Name: emweb/https
CSCsj42456	Yes	ASA 8.0: CSCOPF.CAB has expired Code Signing cert
CSCsj43454	Yes	New l2tp over ipsec sessions blocked due to AAA session limit
CSCsj44098	Yes	traceback caused by gtp inspect handling bad packets
CSCsj46729	Yes	ASA: Active and Standby unit have the same MAC address after failover
CSCsj47652	Yes	clear config all command does not remove the aaa-server config
CSCsj50691	Yes	traceback in Thread Name: Crypto CA (Old pc 0x009dcd56 ebp 0x041b7c18)
CSCsj50913	Yes	ASA : Copying file to OnStor Server via WebVPN fails.
CSCsj53102	Yes	SSH access through VPN tunnel to management interface not working
CSCsj53566	Yes	Traceback in Thread Name: Dispatch Unit continuously on upgrade to 8.0.2
CSCsj56051	Yes	AAA authorization commands LOCAL fallback broken
CSCsj56378	Yes	Traceback in Thread Name: Crypto CA with LDAP CRL query
CSCsj77560	Yes	ASA crash while CRL checking CRL_CheckCertRevocation pki_verify_certific
CSCsj77765	Yes	ASA crash at emweb/https thread
CSCsj78831	Yes	WebFO: Disconnecting clientless deletes local ACL from standby

Related Documentation

For additional information on the Cisco ASA 5500 series adaptive security appliances, see the following URL on Cisco.com:

<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.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 an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2009 Cisco Systems, Inc. All rights reserved.