Cisco ASA 5500 Series Release Notes Version 8.0(3)

26 December 2008

Contents

This document includes the following sections:

Introduction

This version supports the following products:

- Cisco ASA 5500 series adaptive security appliance, Version 8.0(3)
- ASDM, Version 6.0(3)
- Cisco AnyConnect VPN client, Version 2.1
- Cisco Secure Desktop, Version 3.2(1)
- Cisco Intrusion Prevention System, Version 6.0

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

Cisco ASA 5500 Series Adaptive Security Appliance

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.

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. For more information on ASDM, see the *Cisco ASDM Release Notes Version 6.0(3).*

Cisco AnyConnect VPN Client

The Cisco AnyConnect VPN client is also supported in this version. It works with the adaptive security appliance to connect remote users running Microsoft Windows Vista, Windows XP, Windows 2000, Linux, or Macintosh OS X with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. For more information, see the *Release Notes for Cisco AnyConnect VPN Client, Version 2.0*.

Cisco Intrusion Prevention System

IPS is also supported in this version. For more information, go to the following URL:

www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

System Requirements

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

Memory Requirements

Table 1 lists the DRAM memory requirements for the adaptive security appliance. The memory listed in this table is the default value that ships with each adaptive security appliance.

Table 1 DRAM Memory Requirements

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

All adaptive security appliances require a minimum of 64 MB of internal CompactFlash, and they all ship with a minimum of 128 MB of internal CompactFlash.

If your adaptive security appliance has only 64 MB of internal CompactFlash, you should not store multiple system images, or multiple images of the new AnyConnect VPN client components, client/server plugins, or Cisco Secure Desktop.

We recommend that you purchase a 256 MB or 512 MB CompactFlash upgrade from Cisco, choosing from the following part numbers:

- ASA5500-CF-256 MB = ASA 5500 Series CompactFlash, 256 MB
- ASA5500-CF-512 MB = ASA 5500 Series CompactFlash, 512 MB

You can check the size of internal flash and the amount of free flash memory on the adaptive security appliance by doing the following:

- ASDM—Click **Tools > File Management**. The amounts of total and available flash memory appear on the bottom left in the pane.
- CLI—In Privileged EXEC mode, enter the **dir** command. The amounts of total and available flash memory appear on the bottom of the output.

For example:

```
hostname # dir
Directory of disk0:/

2      drwx  4096        11:22:00 Dec 01 2006  csco_config
43     -rwx  14358528    08:46:02 Feb 19 2007  cdisk.bin
44     -rwx  4634        14:32:48 Sep 17 2004  first-backup
45     -rwx  4096        09:55:02 Sep 21 2004  fsck-2451
46     -rwx  4096        09:55:02 Sep 21 2004  fsck-2505
47     -rwx  774         10:48:04 Nov 21 2006  profile.tmpl
48     -rwx  406963      12:45:34 Feb 06 2007  svc
3      drwx  8192        03:35:24 Feb 02 2007  log
49     drwx  4096        07:10:54 Aug 09 2006  1
50     -rwx  21601       14:20:40 Dec 17 2004  tftp
51     -rwx  17489       06:36:40 Dec 06 2006  custom.xml
136    -rwx  12456368    10:25:08 Feb 20 2007  asdmfile
53     -rwx  20498       13:04:54 Feb 12 2007  tomm_english
54     drwx  4096        14:18:56 Jan 14 2007  sdesktop
56     -rwx  14358528    08:32:30 Feb 19 2007  asa800-215-k8.bin
57     -rwx  10971       09:38:54 Apr 20 2006  cli.lua
58     -rwx  6342320     08:44:54 Feb 19 2007  asdm-600110.bin
```

```
59      -rwx  0           04:38:52 Feb 12 2007  LOCAL-CA-SERVER.udb
60      -rwx  322         15:47:42 Nov 29 2006  tmpAsdmCustomization1848612400
8       -rwx  65111       10:27:48 Feb 20 2007  tomm_backup.cfg
61      -rwx  416354      11:50:58 Feb 07 2007  sslclient-win-1.1.3.173.pkg
62      -rwx  23689       08:48:04 Jan 30 2007  asa1_backup.cfg
63      -rwx  45106       07:19:18 Feb 12 2007  securedesktop_asa_3_2_0_54.pkg
64      -rwx  224         01:22:44 Oct 02 2006  LOCAL-CA-SERVER.crl
65      drwx  4096        12:37:24 Feb 20 2007  LOCAL-CA-SERVER
66      -rwx  425         11:45:52 Dec 05 2006  anyconnect
67      -rwx  1555        10:18:04 Sep 29 2006  LOCAL-CA-SERVER_00001.p12
68      -rwx  0           12:33:54 Oct 01 2006  LOCAL-CA-SERVER.cdb
69      -rwx  3384309     07:21:46 Feb 12 2007  securedesktop_asa_3_2_0_57.pkg
70      -rwx  774         05:57:48 Nov 22 2006  cvcprofile.xml
71      -rwx  338         15:48:40 Nov 29 2006  tmpAsdmCustomization430406526
72      -rwx  32          09:35:40 Dec 08 2006  LOCAL-CA-SERVER.ser
73      -rwx  2205678     07:19:22 Jan 05 2007  vpn-win32-Release-2.0.0156-k9.pkg
74      -rwx  3380111     11:39:36 Feb 12 2007  securedesktop_asa_3_2_0_56.pkg

62881792 bytes total (3854336 bytes free)

hostname #
```

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

Note If you use 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.

Operating System and Browser Requirements

We have tested clientless SSL VPN on the following operating systems and browsers, however it may work on others:

- Microsoft Windows XP with Internet Explorer 6.0 or 7.0, or Firefox 1.5 or 2.0
- Microsoft Windows Vista with Internet Explorer 7.0 or Firefox 2.0
- Macintosh OS X with Safari 2.0 or Firefox 2.0
- Linux with Firefox 1.5 or 2.0

For information on the requirements and restrictions of the individual features of clientless SSL VPN (such as plug-ins, smart tunnels, and port forwarding), see the documentation on those features in the *Cisco Security Appliance Command Line Configuration Guide*.

The release notes for ASDM, Cisco AnyConnect Client, and VPN Client list the browsers these products support. The *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators* lists the browsers Secure Session (also called Vault) and Cache Cleaner support.

Determining the Software Version

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

Upgrading to a New Software Version

ASA Version 8.0(3) delivers major enhancements to SSL VPN Remote Access services providing advanced capabilities that simplify the management and deployment of SSL VPNs while enhancing end-user services and ease-of-use. Highlights of Version 8.0(3) for Remote Access include:

- Secure access anywhere, even unmanaged endpoints, through customizable, localizable clientless access
- Flexible access policies on a per-user, per-session, per-machine basis, enabling appropriate access for employees and partners based on their identity and the posture of their endpoints
- Always up-to-date full-tunnel access through the new AnyConnect client, including Dynamic Transport Layer Security support for latency-sensitive applications like VoIP
- Microsoft Windows Vista (32- and 64-bit) and MacOS X support

SSL VPN customers are encouraged to upgrade to Version 8.0(3).

ASA Version 8.0(3) also provides new functionality for firewall customers, as listed below. However, given this release is primarily targeted towards our SSL VPN customers, customers who remain satisfied with the firewall feature content of the ASA Version 7.x series are encouraged to remain on 7.x until such time as they have a business requirement for Version 8.0(3). To support customers choosing to remain on 7.x versions, release updates across all 7.x have been made available.

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

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

You must upgrade from Version 7.2.(x) to Version 8.0(3) and vice versa, because older versions of the ASA images do not recognize new ASDM images, and new ASA images do not recognize old ASDM images.

You can also use the CLI to download the image. For more information, see the "Downloading Software or Configuration Files to Flash Memory" section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.2.(x) to Version 8.0(3), perform the following steps:

Step 1 Make a backup copy of your current configuration file.

Step 2 To retain and use an existing portal customization or URL list, make sure that clientless SSL VPN is enabled on the adaptive security appliance by doing the following:

- ASDM—Choose **Configuration > Remote Access VPN > Clientless SSL VPN** to enable clientless SSL VPN connections on the appropriate interface.
- CLI—Enter the **webvpn enable** command in global configuration mode to enable clientless SSL VPN connections on the appropriate interface.

Step 3 Load the new Version 8.0(3) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 4 Restart the device to load the Version 8.0(3) image.

Step 5 Load the new ASDM 6.0 image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 6 Enter the following command to tell the adaptive security appliance where to find the ASDM image:

```
hostname(config)# asdm image disk0:/asdmfilename (no spaces after the / character, or
within the filename itself)
```

Upgrading to Version 8.0 for Portal Customization and URL Lists

Version 8.0 extends the functionality for configuring customization and URL lists, and the new process is incompatible with previous versions. During the software upgrade to 8.0, the adaptive security appliance preserves your current configuration by using old settings to generate new customization objects and URL lists. This process occurs only once, and is more than a simple transformation from the old format to the new one, because the old values are only a partial subset of the new ones.

Note Version 7.2 portal customizations and URL lists work only if clientless SSL VPN (WebVPN) configuration is enabled on the appropriate interface in the Version 7.2(x) configuration file *before* you upgrade to Version 8.0(3).

To make any changes to existing URL lists or customizations, after you upgrade to Version 8.0(3), you must use the new **export/import webvpn url-list** commands that replace the 7.2 **url-list** commands in webvpn mode.

Similarly, to make changes to the portal customization, use the new **export/import webvpn customization** commands. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

The group policy, username, and tunnel group still enforce the url-list and customization objects.

Downgrading to Version 7.2(x) Software

To downgrade from Version 8.0(3) to 7.2(x), perform the following steps:

Step 1 Load the 7.2(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 2 Restart the device to load the 7.2(x) image.

Step 3 Load the ASDM 5.2(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 4 Enter the following command to tell the adaptive security appliance where to find the ASDM image:

```
hostname(config)# asdm image disk0:/asdmfilename (no spaces after the / character, or
within the filename itself)
```

Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2 requires ASA Version 8.0(3). You do not need to restart the adaptive security appliance after you install or upgrade Cisco Secure Desktop.

Note Archive and delete the Secure Desktop desktop/data.xml configuration file before upgrading to Cisco Secure Desktop 3.2. To create a clean configuration file, uninstall Cisco Secure Desktop before reinstalling it.

The expanded flexibility provided by a prelogin assessment sequence editor, and replacement of the Cisco Secure Desktop feature policies with a dynamic access policy (DAP) configured on the adaptive security appliance, are incompatible with Cisco Secure Desktop 3.1.1 configurations. Cisco Secure Desktop automatically inserts a new, default configuration file when it detects that one is not present.

For consistency with the previous release notes, these instructions provide the CLI commands needed to install Secure Desktop. You may, however, prefer to use ASDM. To do so, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup** and click **Help**.

To install or upgrade the Cisco Secure Desktop software, perform the following steps:

Step 1 Retrieve the securedesktop_asa_3_2_0_*build*.pkg file from the following website and install it on the flash memory card of the adaptive security appliance:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 2 Enter the following commands to access webvpn configuration mode:

```
hostname# config terminal
hostname(config)# webvpn
hostname(config-webvpn)#
```

Step 3 To validate the Cisco Secure Desktop distribution package and add it to the running configuration, enter the following command in webvpn configuration mode:

```
hostname(config-webvpn)# csd image disk0:/securedesktop_asa_3_2_0_build.pkg
hostname(config-webvpn)#
```

Step 4 To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in webvpn configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.

```
hostname(config-webvpn)# csd enable
hostname(config-webvpn)#
```

New Features

Released: November 7, 2007

Table 2 lists the new features forASA and PIX Version 8.0(3).

Table 2 New Features for ASA and PIX Version 8.0(3)

Feature	Description
VPN Features	
AnyConnect RSA SoftID API Integration	Provides support for AnyConnect VPN clients to communicate directly with RSA SoftID for obtaining user token codes. It also provides the ability to specify SoftID message support for a connection profile (tunnel group), and the ability to configure SDI messages on the security appliance that match SDI messages received through a RADIUS proxy. This feature ensures the prompts displayed to the remote client user are appropriate for the action required during authentication and the AnyConnect client responds successfully to authentication challenges.

Table 2 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
IP Address Reuse Delay	Delays the reuse of an IP address after it has been returned to the IP address pool. Increasing the delay prevents problems the security appliance may experience when an IP address is returned to the pool and reassigned quickly.
Clientless SSL VPN Caching Static Content Enhancement	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 adaptive 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 **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) #` *Also available in Version 7.2(3).*
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: **smartcard-removal-disconnect** {**enable** | **disable**}. This option is enabled by default. *Also available in Version 7.2(3).*
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: **redirect-fqdn** {**enable** | **disable**}. *Also available in Version 7.2(3).*
Application Inspection Features	

Table 2 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
WAAS and ASA Interoperability	The **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. *Also available in Version 7.2(3).*
DNS Guard Enhancement	Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request. *Also available in Version 7.2(3).*

Table 2 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
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 syslog 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 the 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*> *Also available in Version 7.2(3).*
High Availability Features	
Added Dataplane Keepalive Mechanism	You can now configure the adaptive security appliance so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two adaptive security appliances with AIP SSMs are configured in failover and the AIP SSM software is updated, the adaptive security appliance triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect. *Also available in Version 7.0(7) and 7.2(3)*
Fully Qualified Domain Name Support Enhancement	Added option in the **redirect-fqdn** command to send either the fully qualified domain name (FQDN) or the IP address to the client in a VPN load balancing cluster.
DHCP Features	
DHCP client ID enhancement	If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use this new command to include the interface MAC address for option 61. If you do not configure this command, the client ID is as follows: cisco-<MAC>-<interface>-<hostname>. We introduced the following command: **dhcp-client client-id interface** *interface_name* *Also available in Version 7.2(3).*

Table 2 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
DHCP client broadcast flag	If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1. If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address. The DHCP client can receive both broadcast and unicast offers from the DHCP server. We introduced the following command: **dhcp-client broadcast-flag**
Platform Features	
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. *Also available in Version 7.2(3).*
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. *Also available in Version 7.2(3).*
Troubleshooting Features	
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 five-tupple **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*]] *Also available in Version 7.2(3).*

Table 2 New Features for ASA and PIX Version 8.0(3) (continued)

Feature	Description
ASDM Features	
ASDM banner enhancement	The adaptive security appliance 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* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** *Also available in Version 7.2(3).*

Important Notes

Observe the following upgrade and operational limitations.

ASA Compatible with EIGRP Version 3

EIGRP support was added in Version 8.0(2). However, due to a packet format change, Version 8.0(3) and later are not compatible with Version 8.0(2). Therefore, if you upgrade an adaptive security appliance to Version 8.0(3) or later, and it is peering with another adaptive security appliance running Version 8.0(2), then the peer must also be upgraded, or EIGRP will not operate correctly.

No .NET over Clientless

Clientless sessions do not support .NET framework applications (CSCsv29942).

Caveats

The following sections describe the caveats for Version 8.0(3).

For your convenience in locating caveats in the Cisco 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 8.0(3)

Table 3 Open Caveats

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsf25418	No	Traceback in Thread Name: tmatch compile after assert
CSCsg71579	No	Programming assertion malloc.c:3822 on secondary after failover from pri
CSCsg99492	No	SASL GSSAPI-Kerberos authentication not happening with Sunone Server
CSCsh91747	No	SSL VPN stress cause SSL lib error. Function: DO_SSL3_WRITE
CSCsj08209	No	clear ospf process causes traceback
CSCsj25672	No	1550 block leak when running multiple tls codenomicon suites.
CSCsj28099	No	ASA can hang on certain tasks if disk is corrupt.
CSCsj32989	No	ASA traceback when running 100 user Avalanche webvpn goodput test
CSCsj83081	No	traceback after clear conf filter. eip 0x00beb377.
CSCsj84640	No	Memory leak on CRYPTO_malloc
CSCsk08454	No	ASA 8.0 fails to send TACACS request over L2L tunnel
CSCsk19065	No	Excessive High CPU and packets drops when applying ACL to an interface
CSCsk21548	No	2048 byte Block depletion related to Fragmented multicast traffic
CSCsk21641	No	Traceback in Dispatch unit related to fragmented multicast traffic
CSCsk36399	No	Traceback in PIX Garbage Collector (Old pc 0x008b619d ebp 0x0261ed60)
CSCsk36703	No	Traceback in thread name IP Thread
CSCsk36952	No	Traceback in Thread: accept/http when changing DHCP config via ASDM
CSCsk37533	No	SIP: Traceback in 7.0(7) with segmented SIP packets
CSCsk38848	No	ASA crashes in Active/Standby Routed Mode causing voice failures
CSCsk40743	No	system miss ticks when cpu-hog is present
CSCsk42958	No	Traceback in thread https_proxy
CSCsk45220	No	Regex used in CLI command filtering causes device reload

Table 3 Open Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsk48344	No	Inspect http is not matching server response fields
CSCsk48629	No	ASA crashes with Unicorn Proxy Thread
CSCsk55665	No	reload with panic: route_process inconsistent annotation
CSCsk60581	No	Device reload when the SIP PROTOS Suite is launched
CSCsk69537	No	Traceback in Dispatch Unit during ASDM access
CSCsk70941	No	Traceback in Thread Name: Dispatch Unit
CSCsk78634	No	ASA Traceback in thread MFIB
CSCsk84529	No	Reload with Thread Name: ssh
CSCsk88517	No	ASA stops servicing WebVPN login page
CSCsk89022	No	ASA dhcp server crashed while removing dhcpd configuration.
CSCsk89600	No	Reload in Dispatch Unit thread with ESMTP inspection enabled
CSCsk89639	No	Reload with Thread Name: Checkheaps
CSCsk90689	No	telnet to the box and vpn tunnels fail due to 0-byte block depletion
CSCsk95246	No	no router rip, followed by router rip & network cause vPifnum & tracebac
CSCsk96804	No	Traceback in Thread Name: Dispatch Unit with inspect h323
CSCsk97830	No	Traceback in thread name Dispatch Unit
CSCsl01792	No	ASA traceback in Thread Name: Dispatch Unit
CSCsl02630	No	WebVPN: Traceback in Thread Name: emweb/https
CSCsl04124	No	ASA 8.0.2 - SIP call from outside w/o sound : SIP::Error - fail to NAT
CSCsl04893	No	ASA: Traceback with threadname Dispatch Unit
CSCsl04953	No	Need to add additional support for DECNET multicast in Transparent mode
CSCsl05707	No	ASA: crash when removing h323 h225 inspection
CSCsl06247	No	ASA-0-716507: Fiber scheduler has reached unreachable code causes outage
CSCsl07386	No	WebVPN: Traceback in Thread Name: vpnfol_thread_sync at failover sync
CSCsl08970	No	Downgrade from 8.0.2 to 7.2.3.5 can cause traceback
CSCsl10562	No	DAP_TRACE: Username: fatemeh, Selected DAPs: <error>
CSCsl11435	No	telnet over VPN hangs when ASA failover occurs
CSCsl11572	No	Traceback - emweb/https - Watchdog Timeout in 0x00909c3d:_vpn_put_uauth
CSCsl12010	No	flash memory corruption issues
CSCsl17136	No	ASA-PIX: H323 Video breaks with inspection enabled.
CSCsl17381	No	ASA crashes with Thread Name: CTM message handler
CSCsl18071	No	Windows Media Player can not play media file with/without L-2-L Ipsec
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCsf07135	No	ASDM connection may cause packet loss

Table 3 Open Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsh78681	No	In use memory count displayed incorrectly
CSCsh79097	No	Syslog message displaying reason why flow is closed by ESMTP inspection
CSCsi49983	No	Periodic HW crypto errors 402123 & 402125 see with L2TP/IPSEC
CSCsi79159	No	admin connections via management-access fail
CSCsi94163	No	PPPOE connection does not renegotiate immediatly after short disconnect
CSCsj02948	No	%ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error
CSCsj07428	No	Idle IPSEC connections not closing out
CSCsj61214	No	Lower cpu-hog syslog 711002 from Level 7 to Level 4
CSCsj71788	No	Slow response when entering commands via Telnet
CSCsk00089	No	ASA 7.2 : Firewall-MIB : no snmp object for failover lan int status
CSCsk10088	No	LDAPS / LDAP over SSL suddenly stops working
CSCsk14532	No	ASA - FTP Type Mount remains inaccessible if FTP server goes offline
CSCsk14695	No	WebVPN with SDI in new pin mode does not prompt user
CSCsk18083	No	nat exemption access-list not checked for protocol or port when applied
CSCsk18084	No	cikeTunnelTable does not populate for some of the ISAKMP SA's.
CSCsk19485	No	syslog TCP_CONN_END shows Reset-O for ASA generated TCP RST
CSCsk29306	No	ASA 8.0 - Error Contacting Host error when accessing CIFS Shares
CSCsk30698	No	PIX/ASA may stop generating syslogs all together
CSCsk33310	No	PIX SIP fixup does not correctly open RTP conns using NAT 0
CSCsk34404	No	Multicontext mode: static nat overlap check not valid when no classifier
CSCsk40210	No	Auth-Proxy DACLs may become stale and impossible to delete
CSCsk42595	No	ASA:: 2 Factor Authentication with Password-Management Fails for SSL VPN
CSCsk47949	No	ASDM hangs at 47% if packet losses on the network
CSCsk47999	No	TCP session stays half-open when FIN sequence problem.
CSCsk48355	No	ISAKMP SA stuck in AM_WAIT_DELETE after ASA upgrade
CSCsk48377	No	Clear Xlate doesn't clear for a host in a static entry
CSCsk49506	No	Local-host for u-turn traffic on lowest sec level used for license limit
CSCsk50537	No	ASA Javascript error with webvpn and mail server (SUN iPlanet)
CSCsk54728	No	Citrix applications do not close automatically when Logging off WebVPN
CSCsk64428	No	High CPU when polling VPN MIBs via SNMP
CSCsk65211	No	ASA5505 inside interface w/23bit or smaller subnet mask becomes unstable
CSCsk65788	No	FO: Webvpn customization import not replicated to Standby device
CSCsk65940	No	crashinfo file corrupted, extra text appended to bottom
CSCsk71006	No	ipv6 acl don't have acl options when using MPF

Table 3 Open Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsk71413	No	Traceback: chunk memory corruption with caller occam_arena__get_block.
CSCsk73047	No	Crash in Thread Name: IKE Receiver
CSCsk75944	No	ASA configuration of NTP - NTP process fails to initialise
CSCsk80789	No	RTSP inspection changes Media Player version to 0.0.0.0
CSCsk84107	No	Standby uses active sub-interface ip address after enabling monitoring
CSCsk88563	No	Answers to DHCPINFORM packets use wrong destination MAC address
CSCsk89474	No	URL filtering not performed for u-turn vpn traffic
CSCsk91598	No	Sip inspection on ASA fails to NAT record-route entries in invite packet
CSCsk93067	No	no management-access Inside still allows telnet over IPSec tunnel
CSCsk94835	No	UDP SIP not being inspected by default-inspection-class
CSCsk97671	No	VPN client with NULL Encryption L2TP-IPSec behind NAT drops on 71st sec
CSCsl02675	No	ASDM>Tools> ping fails when entering hostname in IP address field
CSCsl02821	No	VPN tunnel might not reestablish after failover
CSCsl03839	No	WebVPN does not modify URLs in Sharepoint .iqy files
CSCsl04448	No	Cannot remove url-server despite having removed url-block cmd in 7.2.3
CSCsl04900	No	SIP invite fixup'd with name rather than IP address
CSCsl05751	No	Citrix with Client Detection is not working
CSCsl05777	No	Citrix Apps hanging when opening multiple Apps
CSCsl08857	No	warning message with certificate based authentication
CSCsl10052	No	new L2TP sessions are denied after %ASA-4-403103 is seen in the logs
CSCsl11321	No	ASA doesn't send coldStart trap when speed/duplex is fixed as 100/full
CSCsl14914	No	webvpn rewriter causing webpage to fail with Cisco clientless webvpn
CSCsl15013	No	DHCPrelay broken with 2 DHCPrelay servers when second one out of service
CSCsl16873	No	CSD version 3.2 installed on ASA shows some unwanted garbage characters
CSCsl17191	No	PIX/ASA PMTUD: ICMP type 3 code 4 uses wrong source interface
CSCsl18668	No	last configured dhcprelay server shows up first in configuration

Resolved Caveats - Version 8.0(3)

Table 4 Resolved Caveats

DDTS Number	Software Version 8.0(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
CSCsc98412	Yes	Pix console accounting doesn't appear in ACS Logged-In User report
CSCsd51407	Yes	Dual ISP fails after failover, routing table have stale routes
CSCsd65922	Yes	webvpn acls should allow wilcard * hostnames
CSCse31519	Yes	OCSP: CRL checking of externally signed responder cert fails
CSCse99033	Yes	tracked route removed from Standby firewall after failover
CSCsf30571	Yes	Traceback in ssh_init
CSCsg16149	Yes	data sent with Active MAC after switchover to standby
CSCsg25616	Yes	ASA put PATed src port in ICMP (type3, code4)
CSCsg43591	Yes	SCP connection to PIX fails
CSCsg52106	Yes	Embryonic value -1 under syslog and count to host = 42949672
CSCsg61719	Yes	SNMP: Coldstart Trap is not sent
CSCsg78524	Yes	NT Authentication (NTLM) is attempted three times with a bad password
CSCsg93050	Yes	Inspect DCERPC failure. Packet too small error
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:\/\/
CSCsg99807	Yes	ICMP (type3, code4) is not sent after learning PMTU
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 doesnt appear in config
CSCsh26607	Yes	'inspect skinny' drops/corrupts packets with high network latency
CSCsh32241	Yes	Block size 256 depletion causing failover issues
CSCsh33290	Yes	Transparent FW passes arp requests from standby, causing arp problems
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
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

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsh44467	Yes	Static ARP Entry Removed From the Configuration and ARP Table
CSCsh45414	Yes	ASA Radius state machine reuses state attribute from failed auth
CSCsh46436	Yes	Radius NAS-Port-Type not sent in SSH authentication request
CSCsh48962	Yes	Duplicate ASP table entry causes FW to encrypt traffic with invalid SPI
CSCsh53246	Yes	Traceback when specifying ldap port.
CSCsh53603	Yes	Unable to resolve ARP entry for a directly connected host
CSCsh54016	Yes	PIX 7.2.2 memory degradation
CSCsh55107	Yes	DHCP relay fails when static translation for all hosts configured
CSCsh56084	Yes	ASA CIFS over WebVPN : file created on server but write operation fails
CSCsh56439	Yes	Multicast: Crash in Thread Name: MFIB
CSCsh58003	Yes	IPCP not coming up when using 'ip address pppoe'
CSCsh59098	Yes	Traceback at ThreadName:Unicorn Proxy Thread(pc 0x00c5a9a4 ebp 0x0dd71cc
CSCsh60896	Yes	ESMTP inspection hogging CPU
CSCsh62358	Yes	CTIQBE Fixup does not work with Call Manager 4.2.1
CSCsh65168	Yes	group policy name cannot contain spaces
CSCsh66209	Yes	Traceback at Thread Name: Dispatch Unit(Old pc 0x00218f77 ebp 0x018724a8
CSCsh66576	Yes	L2TP: Connectivity issues with 1500 established sessions
CSCsh66814	Yes	SIP pinhole for inbound INVITE timesout 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
CSCsh74009	Yes	Show/Clear uauth command will not work for username with spaces.
CSCsh74885	Yes	Traceback in thread accept/ssh_131071
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
CSCsh83925	Yes	ASA traceback in Thread Name: EAPoUDP
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 intiate VPN
CSCsh90659	Yes	Traceback: Thread Name:vpnlb_thread in standby after taking active role
CSCsh91283	Yes	Inspect SunRPC drops segmented packets
CSCsh96817	Yes	L2TP: Can not connect more than one Vista client at the same time

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
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
CSCsh98791	Yes	OCSP with CA signed responder cert failing verification check
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
CSCsi07349	Yes	SAA/tracking traceback under specific CLI sequence
CSCsi08103	Yes	command author does not mark aaa-server dead when TACACS unavailable
CSCsi08317	Yes	PIX using Authentication Proxy and Wildcard causes Certificates error
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
CSCsi10466	Yes	SIP inspect fails for INVITE where display name contains string 'tel'
CSCsi11941	Yes	When URL filtering is enabled Streaming Media loads slowly
CSCsi13865	Yes	SNMP in multi-mode creates message vPif_getVpif: bad vPifNum
CSCsi15805	Yes	SNMP interface counters incorrect on ASA-5505
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
CSCsi21431	Yes	Traceback in Thread Name: IP Address Assign
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
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
CSCsi34289	Yes	Traceback in Thread Name: ddns_update_process with DDNS update
CSCsi35603	Yes	L2TP/IPSec sessions hanging when authenticating with EAP
CSCsi35943	Yes	FO: WebVPN Customization/webcontent fails when Failover is initiated
CSCsi35953	Yes	Asa 7.2 webvpn session with certif cannot establish when CN contains /
CSCsi36169	Yes	WebVPN: Aware server becomes unresponsive

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
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
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
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
CSCsi48208	Yes	assertion hdr->dispatch_last < NELTS(hdr->dispatch)
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
CSCsi53577	Yes	OSPF goes DOWN after reload of VPN Peer
CSCsi54132	Yes	Not getting syslog 302010 message
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
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
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
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
CSCsi74352	Yes	ESMTP blocking emails with nested MIME headers
CSCsi78808	Yes	Unable to convert dynamic ACL back to extended ACL
CSCsi81504	Yes	RDP plug-in Connection Failed due to host name sent to ASA instead of IP
CSCsi84498	Yes	Traceback in Thread Name: IKE Daemon

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
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
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
CSCsi98616	Yes	The TCP connections in SVC won't survive after consecutive failovers.
CSCsj01643	Yes	IPSec VPN first auth fails when SDI SoftID is in Cleared PIN Mode
CSCsj01692	Yes	PKI: error installing Intermediate CA cert with 76 char CN
CSCsj02842	Yes	AnyConnect failed to establish:syslog 716023 even with 0 vpn sessions
CSCsj03278	Yes	Traceback in Dispatch Unit thread (page fault)
CSCsj03437	Yes	WebVPN: RDP Icon fails after a redirect action to a Citrix Presentation
CSCsj03706	Yes	activex or java filter suppresses the syslog message 304001
CSCsj05830	Yes	Syslog 405001 reports incorrect IP when arp collision detected
CSCsj06868	Yes	ASA port of pix CSCsi95902 ppp freed memory access on session close
CSCsj10082	Yes	ASA - Traceback in tcp_send_pending
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
CSCsj19829	Yes	WebVPN: http-proxy interferes with port-forward
CSCsj20475	Yes	WebVPN: Group-URL fails without a /
CSCsj20942	Yes	ASA stops accetping 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
CSCsj25910	Yes	http admin access broken for if access rule matches inside network
CSCsj28634	Yes	WebVPN: BAAN ERP application with SSA Webtop fails
CSCsj31537	Yes	Interface keyword in ACL not permitting traffic
CSCsj33267	Yes	traceback in SSH/console with show runn access-list <webtype-CL-name>
CSCsj34537	Yes	ASA 8.0 show vpn-sessiondb detail remote does not show client version
CSCsj36241	Yes	%ASA-1-111111: Invalid function called in NVGEN of 'port-forward'
CSCsj36700	Yes	Assert in ctm_utils after term mon in ssh vty session
CSCsj37564	Yes	Traceback in Thread Name: IP Thread
CSCsj37760	Yes	h323 inspection does not open RTP pinholes in certain scenarios
CSCsj38269	Yes	webvpn load balancing wrong certificate is send to browser
CSCsj38362	Yes	Traceback in Thread Name: fover_parse
CSCsj40295	Yes	Policy NAT not functioning properly after boot

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsj40648	Yes	Traceback in Thread Name: emweb/https
CSCsj41977	Yes	cert handling inconsistent between physical and LB interfaces
CSCsj42456	Yes	ASA 8.0: CSCOPF.CAB has expired Code Signing cert
CSCsj43076	Yes	Logging into standby ASA via SSH fails.
CSCsj43454	Yes	New l2tp over ipsec sessions blocked due to AAA session limit
CSCsj44098	Yes	traceback caused by gtp inspect handling bad packets
CSCsj44460	Yes	UDP/500 not removed from global PAT pool when crypto map is applied
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
CSCsj47652	Yes	clear config all command does not remove the aaa-server config
CSCsj49481	Yes	WebVPN: HTTPS Page not rendered correctly while HTTP works fine
CSCsj50691	Yes	traceback in Thread Name: Crypto CA (Old pc 0x009dcd56 ebp 0x041b7c18)
CSCsj50913	Yes	ASA : Copying file to OnStor Server via WebVPN fails.
CSCsj51849	Yes	cpu-hog observed in process nic status poll thread
CSCsj52557	Yes	WebVPN: Traceback in Thread Name: emweb/https
CSCsj52581	Yes	no crypto isakmp nat-traversal inconsistent configuration after reboot
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
CSCsj56692	Yes	WebVPN CIFS file dates are incorrect when using Firefox 2
CSCsj59397	Yes	memory leak with sysopt connection reclassify-vpn
CSCsj60659	Yes	emweb/https traceback when portscanned on tcp/443
CSCsj62895	Yes	traceback in Crypto CA - eip crypto_pki_poll_crl+149
CSCsj63345	Yes	DAP radius.25(Class) selection attribute doesn't trigger DAP selection
CSCsj64247	Yes	Traceback in Thread Name: Unicorn Admin Thread
CSCsj64523	Yes	WebVPN Webtop to be fixed in 8.0.2
CSCsj64760	Yes	WebVPN: Traceback in Thread Name: Unicorn Proxy Thread
CSCsj66077	Yes	Watchdog: traceback in Thread Name: ssh
CSCsj66185	Yes	ASA: Switching primary and secondary unit can cause duplicate MAC
CSCsj66667	Yes	group-url hostname should not be case-sensitive
CSCsj66819	Yes	ASA - Citrix Client not connecting through WebVPN - SSL Error 35
CSCsj72903	Yes	Additional sanitization needed for syslog message %ASA-5-111008
CSCsj77560	Yes	ASA crash while CRL checking CRL_CheckCertRevocation pki_verify_certific

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsj77765	Yes	ASA crash at emweb/https thread
CSCsj78551	Yes	WebVPN - smart-tunnel doesn't enforce ACLs
CSCsj78675	Yes	HTTP host header not included in PKI requests with terminal enrollment
CSCsj78831	Yes	WebFO: Disconnecting clientless deletes local ACL from standby
CSCsj80196	Yes	Clientless WebVPN traffic not sent when matching crypto dynamic map ACL
CSCsj80563	Yes	ASA dynamic VPN match address disconnects some peers as duplicate proxy
CSCsj82370	Yes	WebVPN: OWA left pane unresponsive when trying to access the folders
CSCsj83531	Yes	Dynamic VPN phase 2 neg with ID_IPV4_ADDR_RANGE accepted as 0.0.0.0/0
CSCsj87980	Yes	Traceback in Thread Name: Checkheaps when applying ips command
CSCsj89976	Yes	WEBVPN: Traceback in Thread Session Manager
CSCsj90479	Yes	IPS and fragments cause Traceback in Thread Name: Dispatch Unit
CSCsj92194	Yes	Implicit ACL 'Deny IP Any Any' Ignored on EasyVPN Client
CSCsj93677	Yes	ASA cache not overwritten when anyconnect profile is updated
CSCsj96065	Yes	TunnelGroup not showing in DAP attributes
CSCsj96831	Yes	half-closed tcp connection behaves as an absolute timer on ASA
CSCsj97241	Yes	80 byte block depletion with stateful failover enabled
CSCsj98072	Yes	Unable to configure http access to management interface for ASDM
CSCsj98458	Yes	LDAP CRL checking failure for Cert Chain
CSCsj98622	Yes	SIP: Not translate c= address if first m= has port 0 in SDP body.
CSCsj99242	Yes	Assert: Traceback in Thread Name: Dispatch Unit
CSCsj99660	Yes	ASA CONSOLE TIMEOUT does not timeout
CSCsk00547	Yes	Traceback in ci/console when modifying cmap inspection_default
CSCsk03033	Yes	ASA, Issues with Local CA Server/Certificate Backup/Restore Procedures
CSCsk03550	Yes	ASA: Route injected through RRI disappear after failover
CSCsk05252	Yes	WebVPN: RDP Plug-in Rendering Issues..screen partially-cutoff
CSCsk05432	Yes	PKI: Default attribute for an LDAP CRL query should include a binary CRL
CSCsk05689	Yes	RDP Layout Manager Incompatible with some JDK versions
CSCsk06996	Yes	Leak in vpnfol_fragdb:vpnfol_fragdb_rebuild on standby
CSCsk08556	Yes	Frames offset incorrect in automation
CSCsk10156	Yes	VPN traffic with static PAT to outside ip address denied by outside ACL
CSCsk12859	Yes	ASA 8.0.2 Traceback under heavy loads of traffic
CSCsk14556	Yes	Local CA - Invalid user cert generated when using FTP Mount DB Store
CSCsk17475	Yes	Smart Tunnel may cause applications to crash
CSCsk19882	Yes	Memory leak in ASA due to WEBVPN compression

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsk25164	Yes	IPSec VPN Client Update not working for mac-> headend issue
CSCsk26830	Yes	Certificate authorization broken when using all DN fields as username
CSCsk27085	Yes	ASA 5505 switch stops forwarding arp packets to ASA
CSCsk27950	Yes	WebVPN: JNLP files are not rewritten
CSCsk28847	Yes	ASA only sends six (6) Radius IETF class 25 attributes for accounting
CSCsk28972	Yes	Traceback:Thread Name: IKE Daemon when connecting w/ certain certificate
CSCsk30589	Yes	Memory leak in snp_mp_ssl_new_conn
CSCsk30787	Yes	Syslogs 605004 and 605005 list IPs as 0.0.0.0 for ASDM connections
CSCsk31007	Yes	SIP: traceback in Thread Name: Dispatch Unit
CSCsk31129	Yes	SIP inspection breaks SIP authentication
CSCsk31414	Yes	WebVPN-CIFS: wrong error message: ...blocked for security reasons!
CSCsk33293	Yes	Traceback in IKE daemon when vlan configured under group-policy
CSCsk33563	Yes	ASA webvpn- CIFS browsing fails when using French language
CSCsk33925	Yes	WebVPN: Regression with OWA as a result of CSCsj82370
CSCsk34125	Yes	debug webvpn javascript trace user does not show up in show debug
CSCsk36854	Yes	DAP: Lua runtime error for strings embedded with double quotes
CSCsk38046	Yes	WebVPN: customization within the tunnel group
CSCsk38962	Yes	memory leak in webvpn failover
CSCsk39154	Yes	PIX/ASA dynamic l2l vpn does not work in 8.0.2.16
CSCsk39286	Yes	ASA5505:Setting Duplex causes a 5 or 6 second outage on the interface.
CSCsk41405	Yes	Traceback in Private Build: Thread Name: Unicorn Proxy Thread
CSCsk41454	Yes	Traceback in thread name: ssh
CSCsk42468	Yes	Transparent firewall allows Telnet access via outside interface
CSCsk42683	Yes	FT: Crash while FTP'ing new ASA image
CSCsk43103	Yes	Traceback in Thread Name emweb/https
CSCsk43257	Yes	ASA - AAA Authorization hang at login when authentication server is down
CSCsk45117	Yes	Traceback in webvpn_url_mangle.c
CSCsk45943	Yes	PIX: proxy-arps on all interfaces for the vpn-pool
CSCsk46821	Yes	ASDM configuration window is blank on initial connect
CSCsk48199	Yes	Traceback in Dispatch Unit thread (page fault)
CSCsk48794	Yes	CSD: SecureDesktopSpace click on clientless link goes to logon page
CSCsk49149	Yes	mem leak with inspect esmtp
CSCsk50639	Yes	WebVPN Thread Name: netfs_thread_init when browsing with cifs
CSCsk55097	Yes	WebVPN: OWA new contact functionality not working

Table 4 Resolved Caveats (continued)

DDTS Number	Software Version 8.0(3)	
	Corrected	**Caveat**
CSCsk59029	Yes	Webvpn: terminal service client6 failed with smart tunnel when name used
CSCsk59816	Yes	Traceback in the process Crypto CA when retrieving the CRL
CSCsk60110	Yes	ASA webvpn APCF command is accepted but not seen in the config
CSCsk61945	Yes	ASA incompatible with routers using EIGRP version 3
CSCsk63982	Yes	ASA with EzVPN client does not send DHCP renew packets, tunnel flaps
CSCsk64111	Yes	Memory Leak in WebVPN Subsystem (1782 & 1856 byte segments)
CSCsk65425	Yes	failing to verify OCSP for RemoteAccess VPN - EJBCA CA infrastructure
CSCsk65863	Yes	traceback in ppp_timer_thread
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
CSCsk70716	Yes	ASDM issuer address changes after failover
CSCsk71135	Yes	ASA 7.2.3 - Traceback in Unicorn Proxy Thread
CSCsk73724	Yes	ASA 5505 default route via dhcp setroute goes away after link flap
CSCsk76401	Yes	set connection decrement-ttl does not work for traceroute
CSCsk77197	Yes	RDP and citrix plugins fail with java error when ACL applied in DAP
CSCsk77613	Yes	webvpn: 3 MB/day mem leak with 76288 byte frag on lightly used device
CSCsk79263	Yes	On link flap, DHCP REQUEST sent only once
CSCsk79728	Yes	ASA5550 7.2.3 crash with Dispatch Unit (Old pc 0x00223a67 ebp 0x018b1318
CSCsk81616	Yes	PIX/ASA Crashes in 'dhcp_daemon'
CSCsk83113	Yes	emweb memory accounting is incorrect.
CSCsk84808	Yes	Unable to remove WebVPN capture CLI, ERROR:Unable to get real-time
CSCsk85428	Yes	Crash in Thread name: snmp
CSCsk85441	Yes	Traceback in thread https_proxy
CSCsk86002	Yes	Memory accounting for aaa chunks is incorrect.
CSCsk87093	Yes	L2TP /EAP-TLS sessions disconnect with 734 error the first time
CSCsk93628	Yes	Packet dropped when mss-exceed is configured to allow
CSCsk95133	Yes	Traceback in Thread Unicorn Proxy related to WebVPN page rewrite
CSCsk96050	Yes	ASA - traceback in Thread Name: ssh

Related Documentation

For additional information on the adaptive security appliance, go to:

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.