Release Notes for the Cisco ASA 5500 Series, Version 8.3(x)

Released: August 2010

Updated: July 12, 2016

This document contains release information for Cisco ASA 5500 Versions 8.3(1) and 8.3(2).

This document includes the following sections:

Note Before you upgrade to 8.3(x), be sure to see the *Cisco ASA 5500 Migration Guide for Version 8.3*. The following major changes require configuration migration:

- NAT redesign.
- Real IP addresses in access rules instead of mapped addresses.
- Named network objects and service objects.

See also the "Important Notes" section on page 2.

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

Important Notes

- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.
- (For upgrading from Version 8.2 and earlier to Version 8.3(2) and later) NAT exemption (the **nat 0 access-list** command) is migrated to a twice NAT rule with the **unidirectional** keyword. The **unidirectional** keyword only allows traffic on the source network to initiate connections. This migration change was made to fix CSCtf89372. Upgrading to Version 8.3(1) does not add the **unidirectional** keyword.

  Note Because NAT exemption is normally bidirectional, you might need to remove the **unidirectional** keyword to restore the original function. Specifically, this change adversely affects many VPN configurations that include NAT exemption rules (see CSCti36048 for this new issue). To avoid manual intervention, we recommend upgrading to 8.3(1) first, and then upgrade to a later release.

  If you are impacted by this issue, you will see a syslog message like the following:

  ```
  %ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
  Connection for icmp src Outside:192.168.1.5 dst inside:10.10.5.20 (type 8, code
  0) denied due to NAT reverse path failure
  ```

- To run Version 8.3 in a production environment, you need to upgrade the memory on the Cisco ASA 5505, 5510, 5520, or 5540. See the "Memory Information" section on page 4 for more information. If you do not install a memory upgrade, you receive the following message upon logging in:

```
**************************************************************************
**
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***
**
**          ----> Minimum Memory Requirements NOT Met! <----
**
**  Installed RAM:  512 MB
**  Required  RAM: 2048 MB
**  Upgrade part#: ASA5520-MEM-2GB=
**
**  This ASA does not meet the minimum memory requirements needed to
**  run this image. Please install additional memory (part number
**  listed above) or downgrade to ASA version 8.2 or earlier.
**  Continuing to run without a memory upgrade is unsupported, and
**  critical system features will not function properly.
**
**************************************************************************
*
```

- The Advanced Inspection and Prevention Security Services Card (AIP SSC) can take up to 20 minutes to initialize the first time it boots after a new image is applied. This initialization process must complete before configuration changes can be made to the sensor. Attempts to modify and save configuration changes before the initialization completes will result in an error.
- If you are upgrading from a pre-8.2 release, see the 8.2 release notes for downgrade issues after you upgrade the Phone Proxy and MTA instance, or for downgrade issues if you upgrade the activation key with new 8.2 features.
- When using Clientless SSL VPN Post-SSO parameters for the Citrix Web interface bookmark, Single-Signon (SSO) works, but the Citrix portal is missing the Reconnect and Disconnect buttons. Only the Log Off button shows. When not using SSO over Clientless, all three buttons show up correctly.

  Workaround: Use the Cisco HTTP-POST plugin to provide single signon and correct Citrix portal behavior.
- Connection Profile/Tunnel Group terminology in CLI vs. ASDM—The adaptive security appliance tunnel groups define the initial connection parameters and attributes (such as AAA, client address assignment, and connection alias/group-url) for a remote access VPN session. In CLI they are referred to as *tunnel groups*, whereas in ASDM they are referred to as *Connection Profiles*. A VPN policy is an aggregation of Connection Profile, Group Policy, and Dynamic Access Policy authorization attributes.

Limitations and Restrictions

- The SSL SHA-2 digital signature capability for authentication of AnyConnect SSL VPN sessions (Versions 2.5.1 and above) is not currently supported on ASA Version 8.3.x. The feature was introduced in ASA interim Version 8.2.3.9.
- Stateful Failover with Phone Proxy—When using Stateful Failover with phone proxy, information is not passed to the standby unit; when the active unit goes down, the call fails, media stops flowing, and the call must be re-established.
- Clientless SSL VPN .NET limitation—Clientless SSL sessions might not properly support .NET framework applications. In some cases you need to enable the application for use with Smart Tunnels; however, there is a chance it could still fail. For example, it might fail when an executable binary (.exe) is created using the .NET framework (CSCsv29942).
- The adaptive security appliance does not support phone proxy with CIPC for remote access.
- The AIP SSC-5 does not support virtualization, unretiring default retired signatures, creating custom signatures, adding signatures, cloning signatures, or anomaly detection.
- An IPv6 Site-to-Site tunnel between an adaptive security appliance and an IOS router will fail during phase 2 negotiation. (CSCtd38078)
- ASA cannot fully support domain based DFS. To support this, the ASA would need to join the Active Directory and query the Active Directory server for DFS referral. Instead the ASA sends the DFS referral to the DNS servers configured for the users. Since the AD server is the DNS server in most cases, the majority of customer configurations are covered.

System Requirements

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

Memory Information

The adaptive security appliance includes DRAM and an internal CompactFlash card. On some models, you can optionally use an external CompactFlash card as well. This section includes the following topics:

Memory Requirements

Table 1 lists the standard and recommended flash memory and DRAM. Note that the shipping DRAM increased after February 2010; the DRAM requirements for 8.3 and higher match the newer default shipping sizes. See the "Memory Upgrade Kits" section on page 5 to order an upgrade kit.

Note If a memory upgrade might be required, the required memory is in **bold**. See the "Memory Upgrade Kits" section on page 5.

ASA 5520 and ASA 5540 adaptive security appliances that were manufactured before August 2011 have 4 DIMM sockets. ASA 5520 and ASA 5540 adaptive security appliances manufactured after this date have 2 DIMM sockets.

Table 1 Standard Memory and Memory Requirements for the Cisco ASA 5500 Series

ASA Model	Internal Flash Memory (Default Shipping)[1,2]	DRAM (Default Shipping)	
		Before Feb. 2010	After Feb. 2010 (Required for 8.3 and Higher)
5505	128 MB	256 MB	**512 MB**[3]
5510	256 MB	256 MB	**1 GB**
5520	256 MB	512 MB	**2 GB**
5540	256 MB	1 GB	**2 GB**
5550	256 MB	4 GB	4GB
5580-20	1 GB	8 GB	8GB
5580-40	1 GB	12 GB	12 GB
5585-X wih SSP-10	2 GB	N/A	6 GB
5585-X wih SSP-20	2 GB	N/A	12 GB

Table 1 Standard Memory and Memory Requirements (continued) for the Cisco ASA 5500 Series

ASA Model	Internal Flash Memory (Default Shipping)[1,2]	DRAM (Default Shipping)	
		Before Feb. 2010	After Feb. 2010 (Required for 8.3 and Higher)
5585-X wih SSP-40	2 GB	N/A	12 GB
5585-X wih SSP-60	2 GB	N/A	24 GB

1. For the ASA 5510 through 5550, you might need to upgrade the internal flash memory to 512 MB or add external flash memory if you load multiple images of the AnyConnect client along with one or more images of the ASA software, ASDM, client/server plugins, or Cisco Secure Desktop. In particular, you might need to upgrade for multiple AnyConnect 3.0 and higher clients with optional modules. The ASA 5505 does not have a flash memory upgrade available.
2. The default internal flash memory for some models was 64 MB in the past; if you have one of these early units, we recommend upgrading your flash memory to at least the new shipping default.
3. For the ASA 5505, only the Unlimited Hosts license and the Security Plus license with failover enabled require 512 MB; other licenses can use 256 MB.

Memory Upgrade Kits

Table 2 lists the DRAM upgrade kits.

Table 2 DRAM Upgrade Kits

Model	Size	Part Number
ASA 5505	512 MB	ASA5505-MEM-512=
ASA 5510[1]	1 GB	ASA5510-MEM-1GB=
ASA 5520	2 GB	ASA5520-MEM-2GB=
ASA 5540	2 GB	ASA5540-MEM-2GB=

1. If you previously purchased the 512 MB upgrade kit for the ASA 5510 (ASA5510-MEM-512=), you must upgrade to the 1 GB memory upgrade kit to run Version 8.3.

Table 3 lists the CompactFlash upgrade kits available for the ASA 5510 through ASA 5550, for use as internal or external flash memory.

Table 3 CompactFlash Upgrade Kits

Model	Size	Part Number
ASA 5510 through ASA 5550	256 MB	ASA5500-CF-256MB=
ASA 5510 through ASA 5550	512 MB	ASA5500-CF-512MB=

Viewing Flash Memory

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—Choose **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:/

43      -rwx  14358528    08:46:02 Feb 19 2007  cdisk.bin
136     -rwx  12456368    10:25:08 Feb 20 2007  asdmfile
58      -rwx  6342320     08:44:54 Feb 19 2007  asdm-600110.bin
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
66      -rwx  425         11:45:52 Dec 05 2006  anyconnect
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 #
```

DRAM, Flash Memory, and Failover

In a failover configuration, the two units must have the same amount of DRAM. You do not have to have the same amount of flash memory. For more information, see the failover chapters in *Cisco ASA 5500 Series Configuration Guide using the CLI*.

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.

ASDM, SSM, SSC, and VPN Compatibility

Table 4 lists information about ASDM, SSM, SSC, and VPN compatibility with the ASA 5500 series.

Table 4 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA 5500 Version 8.3 requires ASDM Version 6.3 or later. For information about ASDM requirements for other releases, see *Cisco ASA 5500 Series Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
SSM and SSC applications	For information about SSM and SSC application requirements, see *Cisco ASA 5500 Series Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

This section lists new features for each maintenance release, and includes the following topics:

- New Features in Version 8.3(2.25), page 7
- New Features in Version 8.3(2), page 8
- New Features in Version 8.3(1), page 10

Note New, changed, and deprecated syslog messages are listed in *Cisco ASA 5500 Series System Log Messages*.

New Features in Version 8.3(2.25)

Released: August 31, 2011

Table 5 lists the new features for ASA interim Version 8.3(2.25).

Note We recommend that you upgrade to a Cisco.com-posted ASA interim release only if you have a specific problem that it resolves. If you decide to run an interim release in a production environment, keep in mind that only targeted testing is performed on interim releases. Interim releases are fully supported by Cisco TAC and will usually remain on the download site only until the next maintenance release is available. If you choose to run an interim release, we strongly encourage you to upgrade to a fully-tested maintenance or feature release when it becomes available.

We will document interim release features at the time of the next maintenance or feature release. For a list of resolved caveats for each ASA interim release, see the interim release notes available on the Cisco.com software download site.

Table 5 New Features for ASA Interim Version 8.3(2.25)

Feature	Description
Remote Access Features	
Clientless SSL VPN browser support	The ASA now supports clientless SSL VPN with Microsoft Internet Explorer 9 and Firefox 4. *Also available in Version 8.2(5.13) and 8.4.2(8).*
Compression for DTLS and TLS	To improve throughput, Cisco now supports compression for DTLS and TLS on AnyConnect 3.0 or later. Each tunneling method configures compression separately, and the preferred configuration is to have both SSL and DTLS compression as LZS. This feature enhances migration from legacy VPN clients. **Note** Using data compression on high speed remote access connections passing highly compressible data requires significant processing power on the ASA. With other activity and traffic on the ASA, the number of sessions that can be supported on the platform is reduced. We introduced or modified the following commands: **anyconnect dtls compression** [**lzs** | **none**] and **anyconnect ssl compression** [**deflate** | **lzs** | **none**]. *Also available in Version 8.2(5.13) and 8.4.2(8).*
Troubleshooting Features	
Regular expression matching for the **show asp table classifier** and **show asp table filter** commands	You can now enter the **show asp table classifier** and **show asp table filter** commands with a regular expression to filter output. We modified the following commands: **show asp table classifier match** *regex*, **show asp table filter match** *regex*. *Also available in Version 8.2(5.13) and 8.4.2(8).*

New Features in Version 8.3(2)

Released: August 2, 2010

Table 6 lists the new features forASA Version 8.3(2).

Table 6 New Features for ASA Version 8.3(2)

Feature	Description
Monitoring Features	
Enhanced logging and connection blocking	When you configure a syslog server to use TCP, and the syslog server is unavailable, the adaptive security appliance blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the adaptive security appliance is full; connections resume when the logging queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommend allowing new connections when syslog messages cannot be sent. To allow new connections, configure the syslog server to use UDP or use the **logging permit-hostdown** command. The following commands were modified: **show logging**. The following syslog messages were introduced: 414005, 414006, 414007, and 414008
Remote Access Features	
2048-bit RSA certificate and Diffie-Hellman Group 5 (DH5) performance improvement	(ASA 5510, ASA 5520, ASA 5540, and ASA 5550 only) We strongly recommend that you enable hardware processing instead of software for large modulus operations such as 2048-bit certificates and DH5 keys. If you continue to use software processing for large keys, you could experience significant performance degradation due to slow session establishment for IPsec and SSL VPN connections. We recommend that you initially enable hardware processing during a low-use or maintenance period to minimize a temporary packet loss that can occur during the transition of processing from software to hardware. **Note** For the ASA 5540 and ASA 5550 using SSL VPN, in specific load conditions, you may want to continue to use software processing for large keys. If VPN sessions are added very slowly and the ASA runs at capacity, then the negative impact to data throughput is larger than the positive impact for session establishment. The following commands were introduced or modified: **crypto engine large-mod-accel**, **clear configure crypto engine**, **show running-config crypto engine**, and **show running-config crypto**. *Also available in Version 8.2(3).*
Microsoft Internet Explorer proxy lockdown control	Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged; the default setting for the tab can be shown or hidden, depending on the user registry settings. The following command was introduced: **msie-proxy lockdown**. *Also available in Version 8.2(3).*
Secondary password enhancement	You can now configure SSL VPN support for a common secondary password for all authentications or use the primary password as the secondary password. The following command was modified: **secondary-pre-fill-username** [**use-primary-password** | **use-common-password**]]

Table 6 New Features for ASA Version 8.3(2) (continued)

Feature	Description
General Features	
No Payload Encryption image for export	For export to some countries, payload encryption cannot be enabled on the Cisco ASA 5500 series. For version 8.3(2), you can now install a No Payload Encryption image (asa832-npe-k8.bin) on the following models: • ASA 5505 • ASA 5510 • ASA 5520 • ASA 5540 • ASA 5550 Features that are disabled in the No Payload Encryption image include: • Unified Communications. • Strong encryption for VPN (DES encryption is still available for VPN). • VPN load balancing (note that the CLI is still present; the feature will not function, however). • Downloading of the dynamic database for the Botnet Traffic Filer (Static black and whitelists are still supported. Note that the CLI is still present; the feature will not function, however.). • Management protocols requiring strong encryption, including SSL, SSHv2, and SNMPv3. You can, however, use SSL or SNMPv3 using base encryption (DES). Also, SSHv1 and SNMPv1 and v2 are still available. If you attempt to install a Strong Encryption (3DES/AES) license, you see the following warning: `WARNING: Strong encryption types have been disabled in this image; the VPN-3DES-AES license option has been ignored.`

New Features in Version 8.3(1)

Released: March 8, 2010

Table 7 lists the new features forASA Version 8.3(1).

Table 7 New Features for ASA Version 8.3(1)

Feature	Description
Remote Access Features	
Smart Tunnel Enhancements	Logoff enhancement—Smart tunnel can now be logged off when all browser windows have been closed (parent affinity), or you can right click the notification icon in the system tray and confirm log out. Tunnel Policy—An administrator can dictate which connections go through the VPN gateway and which do not. An end user can browse the Internet directly while accessing company internal resources with smart tunnel if the administrator chooses. Simplified configuration of which applications to tunnel—When a smart tunnel is required, a user no longer needs to configure a list of processes that can access smart tunnel and in turn access certain web pages. An “enable smart tunnel” check box for either a bookmark or standalone application allows for an easier configuration process. Group policy home page—Using a check box in ASDM, administrators can now specify their home page in group policy in order to connect via smart tunnel. The following commands were introduced: **smart-tunnel network**, **smart-tunnel tunnel-policy**.
Newly Supported Platforms for Browser-based VPN	Release 8.3(1) provides browser-based (clientless) VPN access from the following newly supported platforms: • Windows 7 x86 (32-bit) and x64 (64-bit) via Internet Explorer 8.x and Firefox 3.x • Windows Vista x64 via Internet Explorer 7.x/8.x, or Firefox 3.x. • Windows XP x64 via Internet Explorer 6.x/7.x/8.x and Firefox 3.x • Mac OS 10.6.x 32- and 64-bit via Safari 4.x and Firefox 3.x. Firefox 2.x is likely to work, although we no longer test it. Release 8.3(1) introduces browser-based support for 64-bit applications on Mac OS 10.5. Release 8.3(1) now supports smart tunnel access on all 32-bit and 64-bit Windows OSs supported for browser-based VPN access, Mac OS 10.5 running on an Intel processor only, and Mac OS 10.6.x. The adaptive security appliance does not support port forwarding on 64-bit OSs. Browser-based VPN access does not support Web Folders on Windows 7, Vista, and Internet Explorer 8. An ActiveX version of the RDP plug-in is not available for 64-bit browsers. **Note** Windows 2000 and Mac OS X 10.4 are no longer supported for browser-based access.

Table 7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
IPv6 support for IKEv1 LAN-to-LAN VPN connections	For LAN-to-LAN connections using mixed IPv4 and IPv6 addressing, or all IPv6 addressing, the adaptive security appliance supports VPN tunnels if both peers are Cisco ASA 5500 series adaptive security appliances, and if both inside networks have matching addressing schemes (both IPv4 or both IPv6). Specifically, the following topologies are supported when both peers are Cisco ASA 5500 series adaptive security appliances: • The adaptive security appliances have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interface and IPv4 addresses on the outside interfaces). • The adaptive security appliances have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces). **Note** The defect CSCtd38078 currently prevents the Cisco ASA 5500 series from connecting to a Cisco IOS device as the peer device of a LAN-to-LAN connection. The following commands were modified or introduced: **isakmp enable**, **crypto map**, **crypto dynamic-map**, **tunnel-group**, **ipv6-vpn-filter**, **vpn-sessiondb**, **show crypto isakmp sa**, **show crypto ipsec sa**, **show crypto debug-condition**, **show debug crypto**, **show vpn-sessiondb**, **debug crypto condition**, **debug menu ike**.
Firewall Features	
Interface-Independent Access Policies	You can now configure access rules that are applied globally, as well as access rules that are applied to an interface. If the configuration specifies both a global access policy and interface-specific access policies, the interface-specific policies are evaluated before the global policy. The following command was modified: **access-group global**.
Network and Service Objects	You can now create named network objects that you can use in place of a host, a subnet, or a range of IP addresses in your configuration and named service objects that you can use in place of a protocol and port in your configuration. You can then change the object definition in one place, without having to change any other part of your configuration. This release introduces support for network and service objects in the following features: • NAT • Access lists • Network object groups The following commands were introduced or modified: **object network**, **object service**, **show running-config object**, **clear configure object**, **access-list extended**, **object-group network**.

Table 7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Object-group Expansion Rule Reduction	Significantly reduces the network object-group expansion while maintaining a satisfactory level of packet classification performance. The following commands were modified: **show object-group**, **clear object-group**, **show access-list**.
NAT Simplification	The NAT configuration was completely redesigned to allow greater flexibility and ease of use. You can now configure NAT using auto NAT, where you configure NAT as part of the attributes of a network object, and manual NAT, where you can configure more advanced NAT options. The following commands were introduced or modified: **nat** (in global and object network configuration mode), **show nat**, **show nat pool**, **show xlate**, **show running-config nat**. The following commands were removed: **global**, **static**, **nat-control**, **alias**.
Use of Real IP addresses in access lists instead of translated addresses	When using NAT, mapped addresses are no longer required in an access list for many features. You should always use the real, untranslated addresses when configuring these features. Using the real address means that if the NAT configuration changes, you do not need to change the access lists. The following commands and features that use access lists now use real IP addresses. These features are automatically migrated to use real IP addresses when you upgrade to 8.3, unless otherwise noted. • **access-group** command • Modular Policy Framework **match access-list** command • Botnet Traffic Filter **dynamic-filter enable classify-list** command • AAA **aaa ... match** commands • WCCP **wccp redirect-list group-list** command **Note** WCCP is not automatically migrated when you upgrade to 8.3.
Threat Detection Enhancements	You can now customize the number of rate intervals for which advanced statistics are collected. The default number of rates was changed from 3 to 1. For basic statistics, advanced statistics, and scanning threat detection, the memory usage was improved. The following commands were modified: **threat-detection statistics port number-of-rates**, **threat-detection statistics protocol number-of-rates**, **show threat-detection memory**.
Unified Communication Features	
SCCP v19 support	The IP phone support in the Cisco Phone Proxy feature was enhanced to include support for version 19 of the SCCP protocol on the list of supported IP phones.

Table 7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Cisco Intercompany Media Engine Proxy	Cisco Intercompany Media Engine (UC-IME) enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them. The following commands were modified or introduced: **uc-ime**, **fallback hold-down**, **fallback monitoring**, **fallback sensitivity-file**, **mapping-service listening-interface**, **media-termination**, **ticket epoch**, **ucm address**, **clear configure uc-ime**, **debug uc-ime**, **show running-config uc-ime**, **inspect sip**.
SIP Inspection Support for IME	SIP inspection has been enhance to support the new Cisco Intercompany Media Engine (UC-IME) Proxy. The following command was modified: **inspect sip**.
Monitoring Features	
Time Stamps for Access List Hit Counts	Displays the timestamp, along with the hash value and hit count, for a specified access list. The following command was modified: **show access-list**.
High Performance Monitoring for ASDM	You can now enable high performance monitoring for ASDM to show the top 200 hosts connected through the adaptive security appliance. Each entry of a host contains the IP address of the host and the number of connections initiated by the host, and is updated every 120 seconds. The following commands were introduced: **hpm topn enable**, **clear configure hpm**, **show running-config hpm**.
Licensing Features	
Non-identical failover licenses	Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. **Note** For the ASA 5505 and 5510 adaptive security appliances, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license. The following commands were modified: **show activation-key** and **show version**.

Table 7 New Features for ASA Version 8.3(1) (continued)

Feature	Description
Stackable time-based licenses	Time-based licenses are now stackable. In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The adaptive security appliance allows you to *stack* time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early. For licenses with numerical tiers, stacking is only supported for licenses with the same capacity, for example, two 1000-session SSL VPN licenses. You can view the state of the licenses using the show activation-key command.
Intercompany Media Engine License	The IME license was introduced.
Time-based licenses based on Uptime	Time-based licenses now count down according to the total uptime of the ASA; the system clock does not affect the license.
Multiple time-based licenses active at the same time	You can now install multiple time-based licenses, and have one license per feature active at a time. The following commands were modified: **show activation-key** and **show version**.
Discrete activation and deactivation of time-based licenses.	You can now activate or deactivate time-based licenses using a command. The following command was modified: **activation-key** [**activate** | **deactivate**].
General Features	
Master Passphrase	The master passphrase feature allows you to securely store plain text passwords in encrypted format. It provides a master key that is used to universally encrypt or mask all passwords, without changing any functionality. The following commands were introduced: **key config-key password-encryption**, **password encryption aes**.

Upgrading the Software

See the following table for the upgrade path for your version.

Note There are no special requirements for Zero Downtime Upgrades for failover.

Current ASA Version	Upgrade to:
8.2(x) and earlier	8.3(1) or later

For detailed steps about upgrading, see the 8.3 upgrade guide.

Open Caveats

Table 8 contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from later releases. For example, if you are running Release 8.3(1), then you need to add the caveats in this section to the resolved caveats from 8.3(2) and later to determine the complete list of open caveats.

If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 8 Open Caveats in Version 8.3

Caveat ID	Description
CSCth38885	5550 failing 375 session rate test with too many Client Unsuccesful txs
CSCth44056	5580-40 1000 uni-directional flows max PPS drop around 20% from 8.3.1.3
CSCth52685	ASDM:syslog messages are not getting generated in ASDM in transparent md
CSCth73056	EAL4: New UDP flows blocked for established clients when tcp syslog down
CSCth81168	ASDM Real-Time LogViewer unable to auto resume after AAA timeout
CSCth81765	EAL4:show runn all http doesn't show idle and session timeouts
CSCth87386	EAL4:ASA remains in HostDown blocking after "no logging enabled" command
CSCth95631	EAL4: Syslog 'not connected time' improperly updates
CSCti36048	ASA upgrade to 8.3(2) adds unidirectional keyword to manual nat lines

Resolved Caveats

This section includes the following topics:

Resolved Caveats in Version 8.3(2)

Table 9 lists the resolved caveats for Version 8.3(2). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 9 Resolved Caveats in Version 8.3(2)

Caveat ID	Description
CSCsd99542	Configure fail state link without IP addr causes LAND attack syslogs
CSCsm98354	No accounting packet for some commands
CSCso65967	SIP builds many secondary conns with register msg but no registrar

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCso96413	telnet connections to the box hang after telnet timeout expires
CSCsv55629	The ability to use a cert DN field for author with aaa&cert authentic
CSCsv96545	ASA is dropping arp on SSM-4GE
CSCsw85251	dhcp-network-scope ip that matches interface can cause route deletion
CSCsy50676	Memory corruption and traceback in Thread Name: radius_rcv_auth (VPN)
CSCsy57838	5505 HWclient/LB - auth fail results in never ending connection attmpt
CSCsz48653	WARNING: The vlan id entered is not currently configured under any int
CSCsz62566	ASA 8.0(4) traceback in Dispatch Unit due to stack corruption
CSCta02877	Traceback in unicorn thread (outway_buffer_i)
CSCtb10530	Remove "sysopt nat-convert enable | start" support for broadview/main
CSCtb17498	ASA traceback in 'Thread Name: ssh' when working with captures
CSCtb20340	Removed ACL permits inbound packets
CSCtb23281	ASA: SIP inspect not opening pinhole for contact header of SIP 183 msg
CSCtb34233	Null0 route installed for EIGRP summary routes is ignored in routing tbl
CSCtb36994	tcp-intercept doesn't start 3WH to inside
CSCtb45354	ASA traceback thread name dispatch unit, assertion calendar_queue.h
CSCtb58989	ASDM fails to load due to out of DMA memory when logging is configured
CSCtb83271	TFW: clear conf access-group clears the time stamp of ACE
CSCtc13200	ASA 5510 mount flash failed after load BV image.
CSCtc16148	SLA monitor fails to fail back when ip verify reverse is applied
CSCtc22965	FIPS ASA will not pass FIPS POST in 8.2
CSCtc30025	PP: Incorrect Entry Installed in ASP Table for proxy-server command
CSCtc38762	Traceback eip 0x08065626 <wakeup+166 at finesse/thread.c:378>
CSCtc73402	Upgrading from 8.2.1 to Broadview causes license mismatch
CSCtc81874	Traceback: CTM message handler - L2TP and crypto reset - stack overflow
CSCtc91086	Hangs, CPU hogs, & other performance degradation with 2k Certs
CSCtd23607	hold/resume issue after transfer PSTN call across IME
CSCtd29482	Traceback with Logging flash-bufferwrap configured and heavy logging
CSCtd32984	SNAP frame with MAC address learned on management-only interface is sent
CSCtd36422	TCP proxy in SIP inspection causing 1550 block deplete temporarily
CSCtd36473	IPsec: Outbound context may be deleted prematurely
CSCtd37097	AnyConnect 2.4 can't connect but both auths are successful
CSCtd42601	License: Perm license may be inserted as temp license as well
CSCtd44433	ASA - 1550 block leaking due to email proxy
CSCtd45384	Downgrade BV license: expired (temp keys) reappears after upgrade to BV
CSCtd50421	re-adding class in policy-map causes undesired behavior-see CSCte80609

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCtd51393	UC-IME: Calls attempted above 450 has drop and fallback notification sen
CSCtd52211	ASA assert "new_flow->conn->conn_set == NULL" failed: file "snp_mcast.c"
CSCtd53133	eip 0x090a9de7 <pStorageAsyncProcessor+2371 at unicorn/cte/common/pstora
CSCtd53313	IPv6 Failover: SSH to the standby active fails when no standby address
CSCtd53356	ASA traceback when new DHCPD commands entered
CSCtd54025	Connection once entered into discard state and remains in discard state
CSCtd55032	ASA running 8.0.4.32 traceback in Thread Name: Dispatch Unit
CSCtd55121	4GE-SSM will not transmit all fragments
CSCtd56249	CTA does not respond for EAP from ASA 8.0.5 with NAC
CSCtd57667	MUS: ASA does not changes the etag in subsequent responses to wsa
CSCtd60720	Error event causes Syslog 199011 "Close on bad channel in process/fiber"
CSCtd62371	Duplicate warning appears when capture is enabled on optimized ACL
CSCtd62379	class-map command accepts Optimized ACL
CSCtd63395	Periodic unsuccessfuls during top rate 90B measurement
CSCtd64133	Broadview WEBVPN ST notification icon should have a description
CSCtd67081	traceback DATAPATH-0-1312 after combined vpn system test
CSCtd70378	Broadview: Migration of configuration leaves zero free memory
CSCtd70867	multicast packet latency time increase comparing with 8.1.2
CSCtd71498	NAT: optimize dynamic nat migration based on security-level (beta 384)
CSCtd74691	VPN session not replicate to Standby after Failover State Link failure
CSCtd75798	IME Fallback intermittently triggered, RT/TNP conference zip tone
CSCtd78734	The 4GE SSM Module reset due to stuck Bcast when 5550 became FO active
CSCtd80881	NAT: syntax mismatch in object names created while NAT migration
CSCtd86077	MUS host command problem
CSCtd86141	Page Fault :fiber_cancel+15 at unicorn/ak47/fibers/fibers.c:1153
CSCtd86202	MUS: unreadable characters and unexpected username in debug output
CSCtd86281	FTP download for files larger than 2GB doesn't work properly
CSCtd87194	ASA5580 drops outbound ESP pkt if original pkt needs to be fragmented
CSCtd91710	'show run access-list' doesnt display object name after migration
CSCtd93018	Wrong processing of {a:b?c:d, src:xyz} : discovered wwo CSCtb83100
CSCtd93397	The IP address logged in sysog 106100 for Broadview is not same as ACL
CSCtd93962	NAT with ACL statements causing long time to reboot.
CSCtd94385	ASA: Unable to pass traffic through an Airlink router w DTLS enabled
CSCtd97103	IME: MOH not working
CSCte00896	Beta Box Assertion in udpmod_user_put
CSCte00970	Encrypted passwords are not decrypted correctly

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCte01345	Error while trying to load rewritten webpage of CarnegieMellon Univ Libr
CSCte03164	eip 0x08a7464d <policymap_attach_action+573 at qos/policymap.c:1399>
CSCte04794	PSIRT change-FCAdB timeout causing problems with test/automation
CSCte05494	Failover does not happen with interface shut with sub-second polltime
CSCte05514	CA ServiceDesk hidden frame not showing
CSCte05741	Syslog 113004 doesn't display servername for the user when names gt 16
CSCte07907	SSLVPN: Anyconnect Client cannot establish tunnel to ASA
CSCte08022	Active ASA tracebacks in Thread Name: Dispatch Unit
CSCte08753	Fails to export Local CA Cert after rebooting ASA
CSCte11340	ASA SSL/TLS client sends TLSv1 handshake record in SSLv3 compat mode
CSCte14047	Traceback: "bp" failed: file "ctm_nlite_ipsec.c : 2755 w/ vpn sys test
CSCte14517	Assertion "!hash_entry_hashed(entry)" fail:file "mps_hash_table_simple.c
CSCte14901	Prepending a space bypasses SMTP inspection
CSCte15444	hwclient cannot create ACL when names used in vpnclient CLI
CSCte15462	Disable URL entry should only disable http/https
CSCte15552	HA: config syncing failure when failover link using ipv6 address.
CSCte15729	5580 traceback at CP process while running 600 calls on 2 trunks
CSCte15847	Unable to migrate to ip-options config after CSCte03164
CSCte17614	call-home syslog msg may not be sent after ASA is up over 50 days
CSCte18089	BV: Error while creating ACL with diffrent object name with same content
CSCte18273	ASA continuously reboots when fips is enabled
CSCte18319	ASA 8.0.5 snmp-server re-configuration can cause socket used messages
CSCte19942	BTF: 'show dynamic-filter reports top malware-ports' report empty
CSCte20030	5580 crashes at inspect_sip on running more than 600 calls
CSCte20982	Traceback in SNMP thread when out of memory
CSCte21219	Certificate authentication failing on ASA: incorrect key for validation
CSCte21953	ASA may allow authentication of an invalid username for NT auth
CSCte23816	Telnet NOOP command sent to ASA cause next character to be dropped
CSCte25727	ASA unable to assign users policy when cancelling change password option
CSCte25741	ASA doesn't allow username length of <4 characters
CSCte26480	NAT: Inactive rules with empty object-groups should be disallowed
CSCte29198	mcast pkts can interfere w/ other punts on the DP-to-CP queue
CSCte31040	UC-IME: rtp-min/max port configs for mta not applied to IME media
CSCte33606	NAT: dynamic auto NAT with subnet 0.0.0.0/0 should be restricted
CSCte35887	show running obj<tab completion> behaves incorrectly
CSCte36309	Traceback on active unit when start config sync to standby

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCte38651	ASA fails to establish tunnel (ipsec-ra) with 5505 vpnclient
CSCte38909	msgid in Language Localization are not synchronized
CSCte38942	SSL sockets stuck in CLOSE_WAIT status using webvpn
CSCte39982	Standby ASA tracebacks in Thread Name: vpnfol_thread_msg
CSCte40264	ASA5580 syslog does not work properly with management-access feature
CSCte41930	Assert in access_list.c when viewing v4 ACL with v6 addresses configured
CSCte42788	ASA anyconnect DTLS CONN is torn down when tftp error MSG is rvd- CIPC
CSCte43619	deleting and adding a remark doesn't reflect in show run output
CSCte43903	ASA5580 traceback in thread DATAPATH-2-476, eip rt_timer_cancel_callback
CSCte43926	Thruput Performance Drop of 5%+ in BV when compared with Titan.
CSCte44055	Failed TACACS authentications connections immediately disconnect
CSCte44112	" icmp-type" object groups can be erroneously used with the IPv6 ACL
CSCte44256	UC-IME: Mid-Call Key Change leads to License mismatch for K8 License
CSCte44352	Critical temp for ASA5580 processors needs to be increased
CSCte45632	Standby ASA shows ready when its has no communication to active ASA
CSCte45872	CIFS URL with Macro substition prevents login to a users home share.
CSCte46074	assertion "*cntp != 0" failed: file "mp-datastruct/mp_mutex_rw_lock.h"
CSCte46239	Cookie being set improperly due to webvpn misreading firefox flags
CSCte46460	Post migration ACL allows traffic that was denied prior
CSCte47033	MUS: Client FW rules should work independently of MUS
CSCte47509	Inspect SIP: Segmented SIP message failed version check
CSCte48186	NAT: Warning being issued for undirectional option usage not required
CSCte51127	"sh crypto protocol statistics srtp" ouput incorrect
CSCte51194	IPv6: Multiple equal cost routes not working
CSCte51349	Traceback with Thread Name: DATAPATH-5-1386
CSCte52578	NAT: disallow invalid service objects in manual NAT
CSCte52922	DSCP Field not copied from inner to outer IP header for IPSec Tunnel
CSCte53635	MUS: ASA does not authenticate HTTP HEAD request from WSA
CSCte55149	IPsec IPv6 in IPv6 tunnel, ESP packets dropped by RPF
CSCte55194	"possible channel leak" when loading with large configuration
CSCte55571	ASA names the destination file "scp_fX" if not specified during SCP
CSCte55759	Some segmented SIP messages not reassembled
CSCte56059	Packettracer output doesn't show configured NAT command
CSCte56810	UC-IME: update inspect SRTP debugs
CSCte57663	VPN user cannot ping to inside interface with management-access config
CSCte58070	ASA 8.2 webvpn custom login page shows Javascript error with IE

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCte58126	Nat-migration misleading "INFO message" during hitless upgrade
CSCte58507	AC Essentials not enabled w/ active ssl session should provide msg
CSCte58660	RTP packets dropped by ASA resulting in one-way audio
CSCte58781	ASA558040 console hang with 24 interfaces and jumbo frame
CSCte60159	HA licenses in two 5505s aggregate incorrect
CSCte62519	email mail proxy not intended to be an AC Essentials feature
CSCte62729	ASA5580 traceback in Thread Name: fover_FSM_thread
CSCte64609	VPN Filter Dynamic ACLs not removed after VPN Client phase 1 rekey
CSCte64715	License :FullT with perm keys, erased disk, not prompted for act keys
CSCte64811	ASA 8.04 - certificate chain not being sent during rekey w/ IPSEC RA
CSCte64861	Call-home XML schema incorrect
CSCte65315	WebVPN user-storage does not work if user logon as DOMAIN\Username
CSCte66568	Double authentication broken in 8.2.2 when use-primary-username is conf.
CSCte66849	VPN nat blocks non-VPN inbound traffic by matching vpn acl
CSCte67838	UC-IME: DES and AES SSL encryption keys not allowed for K8 license
CSCte69935	Beta Box assertion: snp_tcp_timeout_cb+0 at np/soft-np/snp_tcp_norm.c:82
CSCte70187	Real IP logs show successful ACL migration even if ACL is deleted
CSCte70201	ACL numbers changed if some ACLs are deleted, no match betw orig/newACL
CSCte70246	ACL/Access group not removed if ACL with Obj Grp fails migration
CSCte71026	NAT: Traceback seen while configuring dynamic NAT
CSCte72114	SSH process may exist after being orphaned from SSH session
CSCte72846	OWA 2003 To, CC, BCC buttons in address book does not work with webvpn
CSCte73170	ACL migr. fails if global pool is shared w/mult. NAT nets if one is 0 0
CSCte73527	ASA5580 license recovery failed.
CSCte74686	NAT: Migration for Twice NAT is failing
CSCte74866	NAT: Wrong Migration logs for identity NAT.
CSCte75201	Nat: Nat migration with Connection limits is not complete
CSCte78445	Titan: Interface setup causes crash
CSCte78820	Double auth: OTP challenge succeeds but new password/verify is rejected.
CSCte79778	dns_process crashed with assertion failure
CSCte80027	ASA 8.0(5) - "LU allocate connection failed"
CSCte80482	"show uc media call-id/session-id <id>" does not work and causes a crash
CSCte80609	Actions attached to class class-default don't apply to traffic
CSCte80973	Enhancement: Broadview insufficient memory warning
CSCte81300	disable console clear function when boot up.
CSCte81335	Remove "port-forwarding" CLI

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCte81368	Sip inspection fails to nat embedded media port
CSCte81860	TCP reset action does not reset connection
CSCte82378	Auto NAT order dependency while syncing config from ASDM
CSCte83714	NAT Migration: Inbound traffic blocked with easy vpn NEM modeconnection
CSCte85038	INFO about migration of over lapping networks should be given to cust
CSCte85803	After failover, skinny message are decoded as SCCPv0 instead of SCCPv17
CSCte87148	Memory tracking indicates false positives when used in dev test & field
CSCte87293	ISAKMP SA stuck in AM_FREE state
CSCte87518	No traffic passes after fail-open inline SSE sensorApp dies
CSCte90623	BTF: drop syslog messages are wrong (level 3 instead of level 4)
CSCte91045	Dhcpd incorrectly sends DHCPNAK
CSCte91279	5575: With 10000 TLS sessions the system tracebacks
CSCte92557	ASA HW client: deny rule for DHCP should account for remote subnets
CSCte92758	NAT: Migration failed for DNS re-write with static PAT.
CSCte94006	BV license: FullT License recovery - perm license is set to default
CSCte94184	FO: "service resetoutside" exists only in standby unit after failover
CSCte95091	Nat:Observing same nat lines in huge number of times after migration
CSCte95175	manual NAT should adopt origin-translated scheme for service objects
CSCte96408	Real IP migration for multiple static NAT/PAT broken with .24 build
CSCte96800	IPSec L2L traffic failing through the tunnel
CSCte98818	LDAP authentication stops operating to Win2008 srvr after sometime
CSCtf00775	Stale WSA registration with ASA failover setup after failover active
CSCtf02322	ASA - Memory depleting 1% per day due to snmp-server ipsec configuration
CSCtf02712	Traceback in Dispatch Unit (Old pc 0x08180444 ebp 0xc793d980)
CSCtf03113	Traceback with L4TM enabled
CSCtf04472	on-line help Typo - Activation-key CLI
CSCtf06292	ASA doesn't handle chunk encoding correctly
CSCtf07633	Crash assertion "0" failed: file "snp_nat_xlate.c", on upgrade to Bview
CSCtf08599	NAT Migration 2000+Static NAT w/o mem upgrade leads to unpredictable ASA
CSCtf09477	port openssl patch
CSCtf11646	WebVPN: RDP is crashing through Smart Tunnels on Mac
CSCtf12679	ASA reboots on issuing "do show run" command.
CSCtf12732	unix-proxy doesn't build
CSCtf13328	Help for NAT, Object, Object-Group, Access-list, Acc.Group not available
CSCtf13368	call-home cpu usage normal notification is not triggered
CSCtf13556	Slow memory leak in WebVPN related to CIFS cache

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCtf13801	ASA PPTP inspection not overwriting Call ID in Call-Clear-Request
CSCtf17718	CSD Token Times out too early - prevents connection
CSCtf17734	Crash with "show uc-ime signalling"
CSCtf18754	BTF: a l4tm_main_process per context introduces too much overhead
CSCtf19753	After upgrade to 8.3 traffic no longer forwarded to tunnel default gw
CSCtf22332	Thread Name: netfs_thread_init
CSCtf23029	mac smart tunnels fails to launch firefox
CSCtf23251	WebVPN: Rewrite issues with Ironport ESA management UI
CSCtf23469	ASA 8.0.5+ webvpn FTP bookmarks no longer will pass embedded user/pass
CSCtf23544	UC-IME: K8 Lic limits SRTP sessions to be 249
CSCtf23906	Factory-Default: ASA5505 nat policy
CSCtf24681	SNAP frames are sent from Management interface in Transparent mode ASA
CSCtf25180	ASA: Discrepency seen between SNMP MIB and sh vpn-sessiondb output
CSCtf25542	Traceback soon after boot-up
CSCtf25808	ICMP error messages dropped in multi-context asymmetric routing mode
CSCtf28464	Memory Leak In CIFS can casue memory depletion
CSCtf28467	Copy to disk0 without ":", prefills dest as disk0, cant delete/view file
CSCtf29077	BTF: top malware-sites report 'dropped conns' not cleared properly
CSCtf29867	Memory leak happens due to huge number of LDAP authentication failure
CSCtf30557	show failover command authorization not available
CSCtf31173	Show version displays UC IME feature in multimode
CSCtf31220	Reload command "hangs" on ASA
CSCtf33469	ASA 8.0.5 1550 block depletion with ASDM open
CSCtf37587	5585: Phone Proxy 5000 SRTPtoSRTP sessions system tracebacks
CSCtf39296	Webvpn with challenge/response: password field should have focus
CSCtf39422	NAT Config migration to 8.3 allowed a Conn which should be deny NAT RPF
CSCtf39875	DHCP renewals after FO switch block new vpn sessions
CSCtf42412	Saving files in microsoft word on sharepoint through webvpn fails
CSCtf42516	ASA 5580 8.2(2) traceback with traffic across 10 Gig interfaces
CSCtf45762	VPN-Filter: Logging not working on SMP platform
CSCtf45794	Removing authentication-server-group from tun-grp not going to LOCAL
CSCtf46141	Insertion of external CF fails.
CSCtf46175	Traceback vpnfol_thread_sync after webvpn stress test with DFP enabled
CSCtf46612	Option to change Pane Title missing from customization editor
CSCtf47041	Active ASA unit tracebacks in Thread Name: ssh
CSCtf48558	IPSec traffic not working after failover

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCtf49095	ldap-dn password is in the clear within running config
CSCtf49620	IKE not passing Cert attr to LDAP server causing Authorization failure
CSCtf49636	asa standby unit reboots after acl config changes
CSCtf52703	ASA/w 4-GE-SSM shows module status unresponsive after power surge
CSCtf54034	DHCP learned route may not be removed at end of lease time
CSCtf54627	Certificate map fails to match with case sensitive SAN
CSCtf55116	quiting "show controller" command with 'q' key triggers failover
CSCtf55261	ASA5580 high frequency tracebacks after upgrade 8.1.2 to 8.2.2
CSCtf55266	call-home: call-home crashed with XML messages on 64bit platform
CSCtf56913	ASA crash on thread name snmp, eip getstats on redundant interface
CSCtf57830	Incorrect real ip translation of ACE after 8.3.1 upgrade
CSCtf59177	Rule ordering incorrect when undirectional twice NAT rules are present
CSCtf60571	ASA 8.2.2 memory leak in inspect
CSCtf62302	RST sent over L2L is dropped by peer due to tcp-rstfin-ooo
CSCtf63794	ASA traceback when adding static nat command
CSCtf66233	FSCK fails when coredump dir exists but coredumps aren't configured
CSCtf67122	Traceback when trying to print syslog 444110 in Thread Name: ms-client
CSCtf67172	Links using macro substitution in portal bookmarks greyed out in 8.3.1
CSCtf68934	Standby Unit not getting session replicated, rerr TCP and UDP increasing
CSCtf69301	Copy /pcap capture fails when packet larger than 2k
CSCtf69322	ISAKMP Packet decode for IKE-Frag shows incorrect Frag ID (byte-swap)
CSCtf72448	HA - unexpected bulk sync triggered after failover
CSCtf72654	timebased license of shared license participant feature is broken
CSCtf73343	3DES Known Answer Test: Failure
CSCtf73359	ASA uses different source IP for data traffic of passive FTP connection
CSCtf73728	ASA PKI: OCSP request does not contain host header
CSCtf78359	Fix for CSCtd86281 has some type casting issues with offset_t
CSCtf81316	IME Calls Fail to MP and UCCX with End to End Secure SIP Trunks
CSCtf81534	Received unexpected event EV_TERMINATE in state MM_SND_MSG6_H
CSCtf84397	Spyker fails to establish AC sessions after block depletion from DH test
CSCtf85135	Add nano sleep to cp process suspend handling
CSCtf86818	Outbound VPN-Filter rule not being removed when last user gone
CSCtf87344	Telnet NOOP command sent to ASA cause next character to be dropped
CSCtf89372	Manual NAT rule (inside,any) source static always takes precedence
CSCtf90588	WebVPN: DWA 8.5 gives exception for the 'Insert Link' action
CSCtf90617	WebVPN: 593 error code in DWA 8.5 for 'Insert image' action

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCtf91831	call-home send CMD email - may fail with Lone CR or LF in headers
CSCtf99056	call-home Timestamp misspelled in e-mail messages
CSCtf99907	mcast: fix smp locking issues
CSCtg01286	ASA 8.3 fails to connect L2TP IPSec client with NAT-T
CSCtg07755	Spyker: Crash in PTHREAD with Midland-B running IPS version 212
CSCtg11699	ASA high CPU in DHCP Proxy thread
CSCtg13981	ASA doesn't set correct MIME type for CSS files
CSCtg14125	ASA: cannot create _vpn object-group
CSCtg14368	ASA crashes when phone proxy debugging is enabled.
CSCtg14750	Dynamic-filter syslogs 338004 and 338008 show '0' for src and dest ports
CSCtg16216	Both the prmary and secondary ASAs assume active role simultaneously
CSCtg17779	Flows torndown over VPN tunnel log 302014 with Flow closed by inspection
CSCtg18674	RSA Crossrealm Authentication fails to authenticate for vpn users
CSCtg18908	standalone webvpn rewriter build fails in titan branch (8.2)
CSCtg20177	Clientless WebVPN not working with SAP Release 3 adobe forms
CSCtg21370	%ASA-5-711005 generated when a L2TP client connects
CSCtg24763	Packet-tracer shows inconsistent results simulating VPN traffic
CSCtg25510	ASA tracebacks in Thread Name: IPsec message handler
CSCtg28821	ASA: AAA Session limit [2048] reached when xauth is disabled for vpn
CSCtg29897	ASDM is not able to upload DAP selection configuration
CSCtg31777	cl conn or timeout can crash DP if same flow is accessed concurrently
CSCtg33169	NAT: overlapping source networks in ACL only creates one object
CSCtg35615	IKEv1: SNMP MIB Tunnel Types need update IPv6 value
CSCtg36637	HEAD requests blocked from a web folder handler processing
CSCtg38272	service resetinbound thru VPN fails without intrainterface same-security
CSCtg39859	ASA MAC Smart tunnel file upload fails after about 200 KB
CSCtg42154	traceback in CERT API when invoking "failover active"
CSCtg45829	ASA crash in thread name: IPv6 input
CSCtg45851	Traceback: CP Processing
CSCtg45916	Don't do DAP re-validation at svc re-key and new tunnel generation
CSCtg46175	Xlate Idle Timer Incorrectly Refreshed by Dropped Packets
CSCtg46276	PP:sh asp table installs Natted IP addr of proxy server instead of Real
CSCtg48603	ASA traceback in Thread Name: Dispatch Unit
CSCtg51135	external appl unable to make connection via proxy server-smart tunnel
CSCtg52476	Implement secondary common password support
CSCtg52478	PIM nbr jp_buffer can be corrupted under stress

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCtg53945	Macros in portal bookmarks not working, OK in homepage-url..ASA 8.3.1
CSCtg58527	Titan: IPSEC handler causes 5505 traceback
CSCtg58757	active unit console becomes unresponsive after traffic and config change
CSCtg60913	Traceback with assertion 'ERROR: accesing without lock"
CSCtg60981	Rapid memory leak after Anyconnect dtls test load set to monitor and rec
CSCtg61032	RDP ActiveX Plugins fails with 8.3.1 when ASA has CA Heirarchy
CSCtg61810	standby unit crashes under multicast traffic
CSCtg63818	Memory leak when using certs for SSL AAA
CSCtg65862	device-mgr: cpu-hog traceback with host stat reporting
CSCtg66953	Standby unit goes into endless message loop while trying to sync config
CSCtg67798	DAP errors when certain special strings present in the ldap value field
CSCtg67898	ACM: Unable to delete object error while "clear conf all" in context
CSCtg68480	Spyker: Traceback in 5565 all phones outside with Phone proxy long run
CSCtg68689	Can't add policy static PAT bk if it was deleted by "clear conf static"
CSCtg68691	Apps with high volume of lookup may experience lock up with smart tunnel
CSCtg69742	standby unit crashes under heavy multicast traffic and continuous script
CSCtg71735	Watchdog failure in vpnfol_thread_msg
CSCtg73255	Some acl remarks not removable after migration to 8.3.1
CSCtg74237	Assert in thread.c on VLAN scaling test
CSCtg74631	Appfault related to MUS/ASA functionality fails
CSCtg76207	standby unit crashes at show failover with active traffic
CSCtg78988	call-home: threat message description incorrect
CSCtg78994	call-home: support environment monitoring in spyker
CSCtg79235	OCSP: Need allow some slop on time check for OCSP response
CSCtg81359	Traceback in Unicorn Admin Handler
CSCtg81514	Webvpn with Citrix - Xenapp upgrade from 11.2 to 12.0 breaks app access
CSCtg83665	standby unit crashes at snp_sp_main.c
CSCtg84635	PP: signaling sessions are not removed after phone disconnects
CSCtg87798	Smart tunnel notification does not pop for home page on Mac
CSCtg94352	Windows Vista / 7 L2TP client behind nat does not connect to ASA 8.3
CSCtg95077	ASDM ASA fails to display hitcounts on Access Rules page
CSCtg96403	ICMP traceroute does not work even after the CSCtf25808 fix
CSCtg96792	Traceback: <meth_frame_decode+347 at media/media_ethernet.c:118>
CSCtg97145	Interface overruns upon IPSEC rekey with PFS and DH5
CSCth00546	Obj:Inconsistency between object and object-group behavior for IPv6.
CSCth02826	IP Version mismatch with object group network with IPv4 and IPv6 address

Table 9 Resolved Caveats in Version 8.3(2) (continued)

Caveat ID	Description
CSCth03659	clear conf all with syslog without any traffic causes a crash.
CSCth04487	WEBVPN:wwwin secondary links do not work in any version
CSCth05572	asa page fault traceback in thread name: netfs_thread_init
CSCth11642	ci/console page fault: pmeminfo_upd_free+54 at resmgr/res_mgr_api.c:2773
CSCth13701	traceback: debug menu webvpn 9
CSCth15152	Traceback typing "import webvpn webcontent /+CSCOU+/logon.inc stdin"
CSCth15736	tcp-norm: page fault crash thread name: dispatch unit
CSCth18720	Thread Name: lu_rx Page fault: Address not mapped
CSCth19342	ASA drops SYN-ACK packets with EOOL option
CSCth22144	CCB: Add EAL4 Logging Enhancements
CSCth22576	Memory leak for mp_percore_alloc during increased security context test
CSCth25402	Implement MSIE proxy lockdown knob on the ASA
CSCth26462	WebVPN proxy-bypass with 'rewrite link' does not rewrite HTTPS links
CSCth28742	CCB EAL4: Update syslogs per review comments
CSCth32416	SIP HA stoppage update problem with large SIP sessions
CSCth36592	5580-20 crash after running 10000 session ipsec L2L test.
CSCth45953	EAL4:SSH management fails with AuditBLock ON/OFF
CSCth59064	EAL4:Display Login failed to VPN users when TCP-Sylog blocking ON
CSCth59623	ACM: Enabling TopN reports getting traceback.
CSCth60265	EAL4: High-water mark blocking not being triggered with log queue @90%
CSCth60669	EAL4: ASA takes minutes to detect TCP syslog server unreachable
CSCth63690	EAL4: Incorrect syslog message when removing TCP logging host
CSCth78205	EAL4: QueueFull blocking mode entered when no TCP syslog configured
CSCth80608	EAL4: QueueFull blocking remains after removing TCP syslog server config
CSCth80902	EAL4: "logging queue 1 or 2" cmmd causes ASA traceback
CSCth80945	ASA 8.3.1: Traceback with snp_fp_punt_block_free_cleanup
CSCth83098	EAL4: Temporary incorrect 'permit hostdown' tcp syslog function
CSCth90489	DH5 should be generate in hw when cache is empty with large mod accel on

Resolved Caveats in Version 8.3(1)

Table 10 lists the resolved caveats for Version 8.3(1). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 10 Resolved Caveats in Version 8.3(1)

Caveat ID	Description
CSCeh98117	Passwords in ASA are displayed in cleartext when viewed with more cmd
CSCsf30287	VPN: Traceback in Thread Name: PIX Garbage Collector
CSCsj40174	SIP CRLF keepalives stall TCP-based SIP connections
CSCsk03602	FT: workaround for read-only flashes
CSCsk40907	DAP: Increase DAP aggregation max lists lengths and make them dynamic
CSCsq53127	DACL remain stale when when used with EzVPN NEM
CSCsv52169	Traceback at thread name PIX Garbage Collector
CSCsv71282	Numerous CPU-hogs in vpnfol_thread_timer
CSCsv73764	Unable to Browse to Domain Based DFS Namespaces
CSCsv86200	ASA 8.0.4.7 Traceback in Thread Name: tmatch compile thread
CSCsv96545	ASA is dropping arp on SSM-4GE
CSCsw37504	ISAKMP delayed when processing large CRL files
CSCsx49794	WebVPN: RDP Plugin does not work with ActiveX with large cert chain
CSCsx83353	WCCP Service Ports Missing in ASP Table when Adding Redirect ACL Entry
CSCsy26775	Traceback while refreshing CRL
CSCsy30717	Keepalive not processed correctly thru TCP Proxy
CSCsy56403	ASA stops accepting IP from DHCP when DHCP Scope option is configured
CSCsy57872	Unable to SSH over remote access VPN (telnet, asdm working)
CSCsy82260	ASA fails to redirect traffic to WCCP cache server
CSCsy91157	Watchdog when inspecting malformed SIP traffic
CSCsy97437	SNMP community string not hidden in 'show startup' or 'show conf'
CSCsy98584	Traceback on Thread Name: AAA due to downloadable ACL processing
CSCsz01314	Traceback in ci/console after sh crypto ipsec sa
CSCsz19296	IPSEC NAT-T - block may get dropped due to VPN handle mismatch
CSCsz32354	Traceback in thread SSH related to using help in policy-map config mode
CSCsz34006	AnyConnect presents Smart Card PIN when using only AAA-non certificates
CSCsz34273	PIX/ASA don't generate syslog 305005 on nat-rpf-failed counter increase
CSCsz36816	OCSP connection failures leaks tcp socket causing sockets to fail
CSCsz39438	Floating toolbar missing for ARWeb (Remedy) via clientless WebVPN
CSCsz42003	ASA 5510 traceback with skinny inspection and phone proxy
CSCsz44078	Traceback in capture when adding a dataplane match command

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCsz48558	PIX/ASA: L2L RRI routes removed after failover when using originate-only
CSCsz49463	PP: One way audio between out-phones when they are behind a Nat router
CSCsz52448	WebVPN: RDP plug-in SSO fails.
CSCsz52937	ASA traceback in Thread Name: Dispatch Unit with TCP intercept
CSCsz53474	1550 Block Depletions leading to unresponsiveness
CSCsz55620	WebVPN: Specific RSS feed give blank page
CSCsz58391	Burst Traffic causes underrun when QoS shaping is enabled on ASA
CSCsz59196	Webvpn ACL that permits on tcp with no range does not work using DAP
CSCsz61074	ASA should reject unuseable ip pool config
CSCsz62364	ASA5580 snmpget will not provide output for certain OIDs
CSCsz63008	Memory leak in 72 / 80 bytes memory blocks [tmatch]
CSCsz63217	Stateful Failover looses connections following link down
CSCsz67729	IP address in RTSP Reply packet payload not translated
CSCsz70270	ASA: AnyConnect is allowed to connect twice with same assigned IP
CSCsz70541	Smart Tunnels and POST params should support "\" in the username
CSCsz70555	WebVPN: ST on Mac should popup the tunneled application when started
CSCsz70846	Strip Realm for WebVPN broken in 8.2, also implement strip-group
CSCsz70906	IPsec/TCP fails due to corrupt SYN+ACK from ASA when SYN has TCP options
CSCsz72175	CSD: flash:/sdesktop/data.xml file gets truncated when it is > 64kB
CSCsz72351	L2TP with EAP auth stuck [%ASA-4-403102 - authentication pending]
CSCsz72684	Traceback on Standby unit during configuration sync
CSCsz72810	InCorectly added "Host Scan File Check e.g 'C:\' " breaks DAP Policies
CSCsz73096	vpn-sessiondb : Address sorting is incorrect
CSCsz73284	access-list logging prints 106100 syslog always at informational level
CSCsz73387	DAP dap.xml file corrupt after replication
CSCsz73955	MAC OSX: Smarttunnel applications don't use name resolution
CSCsz75451	ASA 8.2.1 reloads in "ldap_client_thread" on "Get AD Groups" via ASDM
CSCsz76191	WebVPN: IE shows secure/unsecure items messages
CSCsz77705	sh vpn-sessiondb displays incorrect peer for dynamic to static l2l
CSCsz77717	TCP sessions remain in CLOSEWAIT indefinitely
CSCsz78701	dhcprelay issue after configuration changes in multi context mode
CSCsz79757	Traceback - Thread Name: Dispatch Unit with skinny inspect enabled
CSCsz80366	Citrix ICA on Macintosh over Smart Tunnel fails
CSCsz80777	WebVPN: Disabling CIFS file-browsing still allows shares to be viewed.
CSCsz83417	Clientless WebVPN memory leak in rewriter while compressing/decompressin
CSCsz83798	ASA5580 interfaces does not come up when interfaces are shut/no shut

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCsz85299	Syslogs are incorrectly logged at level 0 - emergencies
CSCsz85597	coredump.cfg file gets rewritten every time show run is executed
CSCsz86120	Traceback when threat detection is disabled and using jumbo frames
CSCsz86143	ASA - traceback in datapath
CSCsz86891	Traceback in Thread Name: Dispatch Unit, Page fault
CSCsz87577	Duplicate shun exemption lines allowed in configuration
CSCsz92485	Traceback in ak47 debug command.
CSCsz92650	Clientless SSL VPN Script Errors when accessing DWA 8.5
CSCsz92808	ASA: Memory leak when secure desktop is enabled
CSCsz93229	WebVPN: Silverlight player does not appear
CSCsz93231	WebVPN: Flash does not play video
CSCsz93235	WebVPN:Silverlight player does not play
CSCsz95464	Anyconnect fails to connect with special character password "<>"
CSCsz97334	Memory leak associated with WebVPN inflate sessions
CSCsz99458	MAC Smart Tunnel fails for certain Java web-applications
CSCta00078	webvpn: Issue w/ processing cookie with quoted value of expire attribute
CSCta01745	IGMP Join From Second Interface Fails to Be Processed
CSCta02170	Traceback in Thread Name: Unicorn Admin Handler
CSCta03382	SQLNET query via inspection cause communication errors
CSCta06294	ASA traceback in Thread Name: Unicorn Proxy Thread
CSCta06806	traceback: netfs_request+289 at netfs/netfs_api.c:89
CSCta10301	ASA 5580 traceback in thread name DATAPATH-0-550
CSCta10530	ASA - management sockets are not functional after failover via vpn
CSCta12118	Exhaustion of 256 byte blocks and traceback in fover_serial_rx
CSCta13245	WEBVPN - CIFS needs to be able to ask IPV4 address from DNS
CSCta16152	ASA WEBVPN causes javascript error when using a ASP.NET application
CSCta16164	n2h2 Redirect Page Fails To Forward Under Load
CSCta16720	vpn-framed-ip-address does not accept /32 netmask
CSCta18361	Traceback in Thread Name: DATAPATH-2-567
CSCta18472	CPU Hog in IKE Daemon
CSCta18623	'Per-User-Override' Keyword Removed from an 'Access-Group' Line
CSCta18741	PIX/ASA: IOS ezvpn ipsec decompression fails with ASA as ezvpn server
CSCta20344	DH group 5 freezes IKE processing for about 80ms
CSCta21219	Clientless SSL: Citrix Web Interface XenApps 5.1 client detection fails
CSCta23184	Traceback in Datapath-1-480
CSCta23935	Active/Active FO fails when using a shared interface with the same name

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCta25498	L2TP still has auth stuck [%ASA-4-403102 - authentication pending]
CSCta26626	PAT Replication failures on ASA failover
CSCta27739	Standby ASA leaking memory in webvpn environment
CSCta31285	ASA assigns user to DfltGrpPolicy when cancelling change password option
CSCta32954	Traceback in Thread Name: aaa
CSCta33092	"show service-policy" output for policing shows wrong "actions: drop"
CSCta33419	ASA VPN dropping self-sourced ICMP packets (PMTUD)
CSCta36043	POST plugin uses Port 80 by default even when csco_proto=https
CSCta38452	ICMP unreachable dropped with unique Nat configuration
CSCta39633	Strip-realm is not working with L2TP-IPSEC connection type
CSCta39767	Service resetinbound send RST unencrypted when triggered by vpn-filter
CSCta42035	"show conn detail" does not indicate actual timeout
CSCta42455	H323: Disable H323 inspect in one context affects H323 inspect in other
CSCta44073	Group requiring cert-auth not shown in AnyConnect Group-List
CSCta45210	Hang may occur with pre-fill-username feature
CSCta45238	Unable to Download Packet Captures from Admin Context for Other Contexts
CSCta45256	WebVPN group-url with a trailing "/" treated differently
CSCta47556	WebVPN: Plugin parameter "csco_sso=1" doesn't work in browser favorites
CSCta47685	WebVPN: Plugin parameter "csco_sso=1" doesn't work with "=" in password
CSCta47769	WebVPN: XML parser and tags with dot.
CSCta49088	"Lost connection to firewall" Message in ASDM with "&" in nameif
CSCta49362	WebVPN: wrong arg count in Flash rewriter
CSCta54837	IPSec over TCP tunnel dropped after launching CIPC
CSCta55072	ASA traceback in Thread Name: Dispatch Unit, Abort: Assert Failure
CSCta55102	WebVPN - PeopleSoft issue
CSCta55567	Traceback when adding "crypto ca server user-db email-otp"
CSCta56375	ASA5580 8.1.2 without NAT RTSP inspection changes video server's IP
CSCta56895	ASA WEBVPN page rendering issue with forms and Modal dialog
CSCta57915	IKE phase 2 for secondary peer fails with connection-type originate-only
CSCta58656	SIP: Filtering by calling/called party should apply to ALL SIP messages
CSCta62631	H323 inspection fails when multiple TPKT messages in IP packet
CSCta73035	ASA: Threat Detection may not release all TD hosts upon disabling
CSCta78657	FTP transfers fail thru OSPF-enabled interfaces when failover occurs
CSCta79938	Standby ASA reloading because unable to allocate ha msg buffer
CSCta86483	Group Alias no longer accepts spaces - Broadview
CSCta88732	WebVPN Traceback in Unicorn Proxy while rewriting Java applets

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCta90855	Netflow does not make use of management-access feature
CSCta92056	Url filter: Need to disable TCP CP stack Nagles algorithm
CSCta93567	Need better error message for VLAN Mapping for NEM Clients not supported
CSCta94184	Cannot open DfltCustomization profile after downgrade from 8.2(1) to 8.0
CSCta98269	ASA SMP traceback in CP Midpath Processing
CSCta99081	ASA traceback has affected failover operation
CSCtb01577	ASA unable to assign IP address for VPN client from DHCP intermittently
CSCtb01729	ASA traceback in tmatch compile thread on tmatch_element_release
CSCtb04058	ASA sends link state traps when doing a failover
CSCtb04171	TD reporting negative session count
CSCtb04188	TD may report attackers as targets and vice versa
CSCtb05806	assert in thread DATAPATH-1-467 on ASA5580
CSCtb05956	ASA memory leak one-time ntlm authentication
CSCtb06293	Upgrade to 8.2.1 causes boot loop
CSCtb07020	Inspection with Messenger causes a traceback
CSCtb07060	ASA bootloops with 24 or more VLANs in multimode
CSCtb12123	show chunkstat should not output empty sibling chunks
CSCtb12184	Unable to reload appliance when out of memory
CSCtb12225	memory leak in SNP Conn Core exhausts all memory via chunk_create
CSCtb16769	When CRL cache is empty revocation check falls back to "NONE"
CSCtb17498	ASA traceback in 'Thread Name: ssh' when working with captures
CSCtb17539	Secondary language characters displayed on Web Portal
CSCtb18378	WebVPN: RDP plug-ing SSO fails when username contains space
CSCtb18901	enable_15 user can execute some commands on fallback to LOCAL db.
CSCtb18940	8.2 Auto Signon domain parameter does not work with CIFS
CSCtb20340	Removed ACL permits inbound packets
CSCtb20506	Deleting group-policy removes auto-signon config in other group-policies
CSCtb25740	Trustpoint certificate will not be updated after re-enrollment
CSCtb27753	Unable to use the search on a webpage through Webvpn
CSCtb31899	Memory leak in the WebVPN memory pools
CSCtb32114	WebVPN: rewriter adds port 80 to server without checking
CSCtb34233	Null0 route installed for EIGRP summary routes is ignored in routing tbl
CSCtb38075	Phone Proxy Dropping RTP Packets After Prolonged Inactivity from Inside
CSCtb38344	ASA tracebacks in Thread Name: vPif_stats_cleaner
CSCtb42847	"clear cry isakmp sa <ip>" doesnt work if there's no corresponding P2 SA
CSCtb42871	Traceback in Thread Name: PIX Garbage Collector

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCtb45354	ASA traceback thread name dispatch unit, assertion calendar_queue.h
CSCtb45571	MAC OS VMWARE web applications VDI do not work with smart-tunnel
CSCtb48049	Reload with traceback in Thread Name: CP Midpath Processing
CSCtb49797	Unnecessary SNAP frame is sent when redundant intf switchover occurs
CSCtb52929	Show service-policy output needs to be present in show tech
CSCtb52943	ifSpeed for redundant interfaces show zero values
CSCtb53186	Duplicate ASP crypto table entry causes firewall to not encrypt traffic
CSCtb56128	CIFS 'file-browsing disable' blocks access to share if '/' at end of url
CSCtb57172	LDAP CRL Download Fails due to empty attribute
CSCtb60778	Traceback in 'ci/console' when Failing Over with Phone Proxy Configured
CSCtb61326	Problem with cp conn's c_ref_cnt while release cp_flow in tcp_proxy_pto
CSCtb62670	ASA source port is reused immediately after closing
CSCtb63825	NetFlow references IDB Interface Value instead of SNMP ifIndex
CSCtb64480	Automatically added AAA command break ASA5505EasyVPN client
CSCtb64885	webvpn-cifs: Not able to browsing CIFS shared on server 2008
CSCtb64913	WEBVPN: page fault in thread name dispath unit, eip udpmod_user_put
CSCtb65464	ASA (8.2.1) traceback in dhcp_daemon
CSCtb65722	Javascript: Mouseover not working through WebVPN
CSCtb69216	LOCAL CA enrolled user is sent enrollment reminder after expiration
CSCtb69486	AAA session limit reached with cert-only authentication
CSCtb77128	Unknown interface '0' returned in snmpwalk on ASA
CSCtb83786	SSM-4GE sees multicast traffic when built-in interfaces do not
CSCtb86463	Traceback: DATAPATH w/ asp-drop circular-buffer capture
CSCtb86570	ASA:assert 0 file:"match_tunnelgrp_chain.c" when altering service policy
CSCtb88338	Ping loss occurs after SSH session is terminated
CSCtb89824	System hang after reload quick when out of memory
CSCtb92911	ASDM logging freezes when a long URL is accessed
CSCtb95067	Certificate mapping only partially overrides the group chosen by URL
CSCtb95326	Traceback: cppoll
CSCtb98328	Trustpoint enrollment password replaced by * after reboot
CSCtb98621	WEBVPN: ASP.NET file link with backslash is modified to a forward slash
CSCtb99389	Standby unit traceback when active reloads
CSCtc00487	Traceback: Unicorn Proxy Thread With Forms Based Auth
CSCtc00929	ASA WebVPN CIFS tries to connect to type GROUP name
CSCtc01815	Mem leak in Radius_Coalesce_AVpairs
CSCtc01864	Memory leak in CRL_CheckCertRevocation

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCtc02642	QOS policy-map with match tunnel-group is not applied after reload
CSCtc03451	TCP SIP Call Dropped When Resuming from Hold Due to Incorrect Timeout
CSCtc03654	npshim: memory leak denies SSL access to/from ASA
CSCtc13966	tmatch_compile_thread traceback w/ low mem condition due to huge vpn acl
CSCtc18516	Dynamic NAT Idle Timeout not Reset on Connection Activity
CSCtc20079	child flows created via established cmd torn down when parent is removed
CSCtc23007	Sip inspection drops 200 OK packet with early RTP/RTCP
CSCtc25115	RDP SSO doesn't send pass
CSCtc27448	ASA failovers when Management interface resets
CSCtc29220	On boot, TACACS server is marked FAILED if defined by DNS name
CSCtc30413	Traceback with SIP pinhole replication Thread Name: Dispatch Unit
CSCtc34355	4GE interfaces with OSPF is broken starting from 100.5.0.37
CSCtc35051	ASA 5580 hangs with only 200 concurrent users due to 2048-bit keys
CSCtc35058	Console hangs when trying to write mem or view config
CSCtc35096	Personalized Bookmarks do not account for authentication realms
CSCtc35404	0 size block depletion may cause failover mate not detected
CSCtc37653	Cable-based failover does not work
CSCtc40891	memory leaks after anyconnect test with packet drops
CSCtc41374	ASA: standby unit traceback during failover replication
CSCtc42064	ASA passes reset packets after a connection is closed
CSCtc42215	ASA 8.2.1.4 Crash when webvpn capture is configured
CSCtc43209	ASA traceback: Thread Name: IKE Daemon
CSCtc43396	Coredump from emweb/https when connecting phone VPN client
CSCtc46309	CIFS : Authentication Error with percentage symbol in password
CSCtc47782	Malformed IKE traffic causes rekey to fail
CSCtc48310	ASA: Traceback during NTLM authentication
CSCtc52217	Clientless WebVPN: Errors with DWA 8.5 (Domino Web Access / Notes)
CSCtc58632	SSM IPS sends TCP RST to wrong TCP seq number
CSCtc62281	When SAPI tcp-proxy buffer exceeding limit generates misleading syslog
CSCtc69318	Active/Active - Failover status flaps when shared interface link is down
CSCtc70548	WebVPN: Cisco Port Forwarder ActiveX does not get updated automatically
CSCtc71135	SSL lib error. Function: DO_SSL3_WRITE while making cert only SSLVPN
CSCtc73117	DHCP Proxy -2s delay between consecutive DHCP lease renew after failover
CSCtc73833	Radius authentication fails after SDI new-pin or next-code challenge
CSCtc74064	Soft-np doesn't correctly set port to promiscuous mode
CSCtc78636	asa https authentication (with/without listener) doesn't prompt

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCtc82010	vpnlb_thread traceback under low mem condition due to huge vpn acl
CSCtc82025	emweb/https traceback under low memory condition
CSCtc90093	WebVPN: Firefox users have issues searching with google
CSCtc91042	ASA does not handle HTTP HEAD requests for pages served on its Aware web
CSCtc93523	Traceback in Thread Name: SiteMinder SSO Request
CSCtc96018	ASA watchdog when inspecting malformed SIP traffic
CSCtc98097	Cable modem drops 5505/SSC packets due to invalid source MAC address..
CSCtc99553	Personal Bookmark using plugins won't use parameters other than the 1st
CSCtd00457	Sharepoint: WebFolders Fails to Copy Files
CSCtd00697	IMPORTANT TLS/SSL SECURITY UPDATE
CSCtd03464	show vpn-sessiondb remote command outputs wrong Group Policy
CSCtd14917	Launching ASDM triggers ASA software traceback
CSCtd15605	assertion "t->stack[0] == STKINIT" failed: file "thread.c", line 743
CSCtd21034	vpn-session-db shows incorrect group-policy for failed memberOf ldap-map
CSCtd25685	New active member should send SNAP frames for MAC address table update
CSCtd27345	Failover replicated conns failed if failover lan/stateful link down
CSCtd27888	1-hour threat-detection enabled by "clear threat-detection rate"
CSCtd28327	ASA not displaying pictures on the portal page
CSCtd28887	ASA: Webvpn CIFs does not refresh updated files
CSCtd29154	Traceback when CSR is generated
CSCtd30953	LDAP CRL Download Fails due to empty attribute pki-cro
CSCtd31831	ASA traceback in Thread Name: Checkheaps
CSCtd34106	pim spt infinity can cause dp-cp queue overload and affect eigrp, pim, .
CSCtd35450	Excessive memory allocation for large routing tables
CSCtd42963	threshold checking for average rate not working in threat-detection
CSCtd43241	Traceback on secondary with SIP connection replication
CSCtd44433	ASA - 1550 block leaking due to email proxy
CSCtd50421	re-adding class in policy-map causes undesired behavior-see CSCte80609
CSCtd51042	ASA: ip IPSec SA not brought up if similar icmp SA is up
CSCtd52211	ASA assert "new_flow->conn->conn_set == NULL" failed: file "snp_mcast.c"
CSCtd53390	TCP RSTs returned from inline IPS are dropped on multi-context ASA
CSCtd54025	Connection once entered into discard state and remains in discard state
CSCtd54252	traceback in checkheaps during backup of asa with smartcare appliance
CSCtd55346	Remove uninformative Peer Tbl remove messages
CSCtd79084	checkheaps causes nested traceback
CSCtd81305	WebVPN: Plugin SSO not working with special characters in username or pw

Table 10 Resolved Caveats in Version 8.3(1) (continued)

Caveat ID	Description
CSCtd86141	Page Fault :fiber_cancel+15 at unicorn/ak47/fibers/fibers.c:1153
CSCte03164	eip 0x08a7464d <policymap_attach_action+573 at qos/policymap.c:1399>
CSCte08022	Active ASA tracebacks in Thread Name: Dispatch Unit
CSCte18319	ASA 8.0.5 snmp-server re-configuration can cause socket used messages
CSCte21953	ASA may allow authentication of an invalid username for NT auth
CSCte39708	Encoded error message issue in /+CSCOE+/logon.html
CSCte39982	Standby ASA tracebacks in Thread Name: vpnfol_thread_msg
CSCte42788	ASA anyconnect DTLS CONN is torn down when tftp error MSG is rvd- CIPC
CSCte46074	assertion "*cntp != 0" failed: file "mp-datastruct/mp_mutex_rw_lock.h"
CSCte46239	Cookie being set improperly due to webvpn misreading firefox flags
CSCte64861	Call-home XML schema incorrect
CSCte66568	Double authentication broken in 8.2.2 when use-primary-username is conf.
CSCte80027	ASA 8.0(5) - "LU allocate connection failed"

Related Documentation

For additional information on the adaptive security appliance, see *Navigating the Cisco ASA 5500 Series Documentation*:

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.