



Release Notes for the Cisco ASA 5500 Series, Version 8.2(x)

August 2010

This document contains release information for Cisco ASA 5500 Versions 8.2(1) through 8.2(3).

This document includes the following sections:

- [Important Notes, page 1](#)
- [Limitations and Restrictions, page 2](#)
- [Upgrading the Software, page 2](#)
- [System Requirements, page 4](#)
- [New Features, page 8](#)
- [Open Caveats, page 17](#)
- [Resolved Caveats, page 22](#)
- [End-User License Agreement, page 55](#)
- [Related Documentation, page 55](#)
- [Important Notes, page 1](#)
- [Obtaining Documentation and Submitting a Service Request, page 55](#)

Important Notes

- Pause frame transmission can be enabled on every customer data port using the existing **flow control** command mechanism. Pause frame reception is not supported.
- 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.
- See the [“Upgrading the Software” section on page 2](#) for downgrade issues after you upgrade the Phone Proxy and MTA instance, or if you upgrade the activation key with new 8.2 features.



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

© 2010 Cisco Systems, Inc. All rights reserved.

- For detailed information and FAQs about feature licenses, including shared licenses and temporary licenses, see *Managing Feature Licenses for Cisco ASA 5500 Version 8.2* at <http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html>.
- When using Clientless SSL VPN Post-SSO parameters for the Citrix Web interface bookmark, Single Sign On (SSO) works, but the Citrix portal is missing the Reconnect and Disconnect buttons. Only the Log Off button appears. When not using SSO over Clientless, all three buttons show up correctly.
Workaround: Use the Cisco HTTP-POST plug-in to provide SSO and correct Citrix portal behavior.
- On the ASA 5510, Version 8.2 uses more base memory than previous releases. This might cause problems for some ASA 5510 users who are currently running low on free memory (as indicated in the **show memory** command output). If your current **show memory** command output displays less than 20% free, we recommend upgrading the memory on the ASA 5510 from 256 MB to 1 GB before proceeding with the Version 8.2 upgrade. See the “[Memory Requirements](#)” section on page 5.
- 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 the 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

- 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.
- No .NET over Clientless sessions—Clientless sessions do not support .NET framework applications (CSCsv29942).
- The adaptive security appliance does not support phone proxy and 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.

Upgrading the Software

To upgrade to 8.2, see the “Managing Software and Configurations” chapter in *Cisco ASA 5500 Series Configuration Guide using the CLI*. Be sure to back up your configuration before upgrading.

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

This section includes the following topics:

- [Downloading Software from Cisco.com, page 3](#)
- [Upgrading Between Major Releases, page 3](#)
- [Upgrading the Phone Proxy and MTA Instance, page 3](#)
- [Activation Key Compatibility When Upgrading, page 3](#)

Downloading Software from Cisco.com

If you have a Cisco service contract, you can obtain software from the following website:

<http://www.cisco.com/go/asa-software>

Upgrading Between Major Releases

To ensure that your configuration updates correctly, you must upgrade to each major release in turn. Therefore, to upgrade from Version 7.0 to Version 8.2, first upgrade from 7.0 to 7.1, then from 7.1 to 7.2, and finally from Version 7.2 to Version 8.2 (8.1 was only available on the ASA 5580).

Upgrading the Phone Proxy and MTA Instance

In Version 8.0(4), you configured a global media-termination address (MTA) on the adaptive security appliance. In Version 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTAs). As a result of this enhancement, the old CLI has been deprecated. You can continue to use the old configuration if desired. However, if you need to change the configuration at all, only the new configuration method is accepted; you cannot later restore the old configuration.



Note

If you need to maintain downgrade compatibility, you should keep the old configuration as is.

To upgrade the Phone Proxy, perform the following steps:

-
- Step 1** Create the MTA instance to apply to the phone proxy instance for this release. See “Creating the Media Termination Instance” section in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.
- Step 2** To modify the existing Phone Proxy, enter the following command:
- ```
hostname(config)# phone-proxy phone_proxy_name
```
- Where *phone\_proxy\_name* is the name of the existing Phone Proxy.
- Step 3** To remove the configured MTA on the phone proxy, enter the following command:
- ```
hostname(config)# no media-termination address ip_address
```
- Step 4** Apply the new MTA instance to the phone proxy by entering the following command:
- ```
hostname(config)# media-termination instance_name
```
- Where *instance\_name* is the name of the MTA that you created in [Step 1](#).
- 

## Activation Key Compatibility When Upgrading

Your activation key remains compatible if you upgrade to Version 8.2 or later, and also if you later downgrade. After you upgrade, if you activate additional feature licenses that were introduced before 8.2, then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were introduced in 8.2 or later, then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:

- If you previously entered an activation key in an earlier version, then the adaptive security appliance uses that key (without any of the new licenses you activated in Version 8.2 or later).
- If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.

## System Requirements

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

- [Memory Requirements, page 5](#)
- [ASDM, SSM, SSC, and VPN Compatibility, page 7](#)

## Memory Requirements

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

- [Standard DRAM and Internal Flash Memory, page 5](#)
- [Memory Upgrade Kits, page 5](#)
- [Viewing Flash Memory, page 6](#)
- [DRAM, Flash Memory, and Failover, page 6](#)

### Standard DRAM and Internal Flash Memory

[Table 1](#) lists the standard memory shipped with the adaptive security appliance.

**Table 1**      **Standard Memory**

| ASA Model | Default DRAM Before Feb. 2010 | Default DRAM After Feb. 2010 |
|-----------|-------------------------------|------------------------------|
| 5505      | 256                           | 512                          |
| 5510      | 256 <sup>1</sup>              | 1 GB                         |
| 5520      | 512                           | 2 GB                         |
| 5540      | 1024                          | 2 GB                         |
| 5550      | 4096                          | 4 GB                         |
| 5580      | 4096                          | 8 GB                         |

1. For the ASA 5510—Version 8.2 uses more base memory than previous releases, which might cause problems for some ASA 5510 users who are currently running low on free memory (as indicated in the **show memory** output). If your current **show memory** output displays less than 20% free, we recommend upgrading the memory on the ASA 5510 from 256 MB to 1 GB before proceeding with the release 8.2 upgrade.



**Note**

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

### Memory Upgrade Kits

With Version 8.2(3), new memory upgrade kits are available for existing ASA platforms. [Table 2](#) shows the upgrade kits that are available from Cisco with their corresponding part numbers.

**Table 2**      **Cisco ASA Memory Upgrade Kits**

| Cisco ASA Memory Upgrades Available | Product Identification Number |
|-------------------------------------|-------------------------------|
| Cisco ASA 5505 upgrade, 512 MB      | ASA5505-MEM-512=              |
| Cisco ASA 5510 upgrade, 1 GB        | ASA5510-MEM-1GB=              |
| Cisco ASA 5520 upgrade, 2 GB        | ASA5520-MEM-2GB               |
| Cisco ASA 5540 upgrade, 2 GB        | ASA5540-MEM-2GB=              |

Table 3 shows the CompactFlash upgrades that are available from Cisco with their corresponding part numbers.

**Table 3 CompactFlash Upgrades**

| CompactFlash Upgrades Available      | Product Identification Number |
|--------------------------------------|-------------------------------|
| ASA 5500 Series CompactFlash, 256 MB | ASA5500-CF-256MB=             |
| ASA 5500 Series CompactFlash, 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 hardware configuration, must be the same model, must have the same number and types of interfaces, must have the same feature licenses, and 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                     | <p>The following list shows the ASA and ASDM compatibility:</p> <ul style="list-style-type: none"> <li>• ASA 8.2(1) requires ASDM 6.2(1) or later</li> <li>• ASA 8.2(2) requires ASDM 6.2(5) or later</li> <li>• ASA 8.2(3) requires ASDM 6.3(3) or later</li> </ul> <p>For information about ASDM requirements for other releases, see <i>Cisco ASA 5500 Series Hardware and Software Compatibility</i>:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html</a></p> |
| VPN                      | <p>For the latest OS and browser test results, see the <i>Supported VPN Platforms, Cisco ASA 5500 Series</i>:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html</a></p>                                                                                                                                                                                                                                                                     |
| SSM and SSC applications | <p>For information about SSM and SSC application requirements, see <i>Cisco ASA 5500 Series Hardware and Software Compatibility</i>:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html</a></p>                                                                                                                                                                                                                                                                      |

# New Features



## Note

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

This section includes the following topics:

- [New Features in Version 8.2\(3\), page 8](#)
- [New Features in Version 8.2\(2\), page 8](#)
- [New Features in Version 8.2\(1\), page 11](#)

## New Features in Version 8.2(3)

[Table 5](#) lists the new features for ASA Version 8.2(3).

**Table 5**      **New Features for ASA Version 8.2(3)**

| Feature                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Access Features</b>                           |                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Diffie-Hellman 5 and 2K certificate support in hardware | Hardware processing for large modulus operations (Diffie-Hellman 5 (DH5) and 2K cert RSA). This feature enables you to switch operations such as DH5 and 2K cert RSA from software to hardware. Enable this feature only if it is necessary to improve the connection rate. It applies to the ASA 5510, 5520, 5540, and 5550 only.<br><br>The following command was introduced: <b>crypto engine large-mod-accel</b> . |
| Microsoft Internet Explorer proxy lockdown control      | Lets you show or hide the Internet Explorer Connections tab for the duration of an AnyConnect session.<br><br>The following command was introduced: <b>msie-proxy lockdown</b> .<br><i>Also available in Version 8.2(3).</i>                                                                                                                                                                                           |
| Trusted Network Detection Pause and Resume              | This feature enables the AnyConnect client to retain its session information and cookie so that it can seamlessly restore connectivity after the user leaves the office, as long as the session does not exceed the idle timer setting. This feature requires an AnyConnect release that supports TND pause and resume.                                                                                                |

[Table 6](#) lists the new features for ASA Version 8.2(2).

**Table 6**      **New Features for ASA Version 8.2(2)**

| Feature                                               | Description                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Access Features</b>                         |                                                                                                                                                                                                                                                                                                                                                  |
| Scalable Solutions for Waiting-to-Resume VPN Sessions | An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in.<br><br><i>Also available in Version 8.0(5).</i> |



Table 6 New Features for ASA Version 8.2(2) (continued)

| Feature                                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Inspection Features</b>                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Inspection for IP Options                                                                                         | <p>You can now control which IP packets with specific IP options should be allowed through the adaptive security appliance. You can also clear IP options from an IP packet, and then allow it through the adaptive security appliance. Previously, all IP options were denied by default, except for some special cases.</p> <p><b>Note</b> This inspection is enabled by default. The following command is added to the default global service policy: <b>inspect ip-options</b>. Therefore, the adaptive security appliance allows RSVP traffic that contains packets with the Router Alert option (option 20) when the adaptive security appliance is in routed mode.</p> <p>The following commands were introduced: <b>policy-map type inspect ip-options, inspect ip-options, eool, nop</b>.</p> |
| Enabling Call Set up Between H.323 Endpoints                                                                      | <p>You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The adaptive security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages.</p> <p>Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint IP address is unknown and the adaptive security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled.</p> <p>The following command was introduced: <b>ras-rcf-pinholes enable</b> (under the <b>policy-map type inspect h323 &gt; parameters</b> commands).</p> <p><i>Also available in Version 8.0(5).</i></p>                                                                                      |
| <b>Unified Communication Features</b>                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Mobility Proxy application no longer requires Unified Communications Proxy license                                | The Mobility Proxy no longer requires the UC Proxy license.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Interface Features</b>                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements | <p>The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair.</p> <p>The MAC addresses are also now persistent accross reloads.</p> <p>The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.</p> <p>The following command was modified: <b>mac-address auto prefix prefix</b>.</p> <p><i>Also available in Version 8.0(5).</i></p>                                                                                                                                                                                                                 |

**Table 6**      **New Features for ASA Version 8.2(2) (continued)**

| Feature                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support for Pause Frames for Flow Control on the ASA 5580 10 Gigabit Ethernet Interfaces  | You can now enable pause (XOFF) frames for flow control.<br>The following command was introduced: <b>flowcontrol</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Firewall Features</b>                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Botnet Traffic Filter Enhancements                                                        | The Botnet Traffic Filter now supports automatic blocking of blacklisted traffic based on the threat level. You can also view the category and threat level of malware sites in statistics and reports. Reporting was enhanced to show infected hosts. The 1 hour timeout for reports for top hosts was removed; there is now no timeout.<br><br>The following commands were introduced or modified: <b>dynamic-filter ambiguous-is-black</b> , <b>dynamic-filter drop blacklist</b> , <b>show dynamic-filter statistics</b> , <b>show dynamic-filter reports infected-hosts</b> , and <b>show dynamic-filter reports top</b> . |
| Connection timeouts for all protocols                                                     | The idle timeout was changed to apply to all protocols, not just TCP.<br>The following command was modified: <b>set connection timeout</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Routing Features</b>                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues                       | This enhancement introduces adaptive security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server configured for VPN clients, you can now configure the adaptive security appliance to send the Subnet Selection option or the Link Selection option.<br><br>The following command was modified: <b>dhcp-server [subnet-selection   link-selection]</b> .<br><br><i>Also available in Version 8.0(5).</i>                                                                                                 |
| <b>High Availability Features</b>                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IPv6 Support in Failover Configurations                                                   | IPv6 is now supported in failover configurations. You can assign active and standby IPv6 addresses to interfaces and use IPv6 addresses for the failover and Stateful Failover interfaces.<br><br>The following commands were modified: <b>failover interface ip</b> , <b>ipv6 address</b> .                                                                                                                                                                                                                                                                                                                                    |
| No notifications when interfaces are brought up or brought down during a switchover event | To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent.<br><br><i>Also available in Version 8.0(5).</i>                                                                                                                                                                                                                                                                                                                 |
| <b>AAA Features</b>                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 100 AAA Server Groups                                                                     | You can now configure up to 100 AAA server groups; the previous limit was 15 server groups.<br>The following command was modified: <b>aaa-server</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 6**      *New Features for ASA Version 8.2(2) (continued)*

| Feature                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Monitoring Features</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Smart Call Home            | <p>Smart Call Home offers proactive diagnostics and real-time alerts on the adaptive security appliance and provides higher network availability and increased operational efficiency. Customers and TAC engineers get what they need to resolve problems quickly when an issue is detected.</p> <p><b>Note</b> Smart Call Home server Version 3.0(1) has limited support for the adaptive security appliance. See the “Important Notes” for more information.</p> <p>The following commands were introduced: <b>call-home</b>, <b>call-home send alert-group</b>, <b>call-home test</b>, <b>call-home send</b>, <b>service call-home</b>, <b>show call-home</b>, <b>show call-home registered-module status</b>.</p> |

## New Features in Version 8.2(1)

[Table 7](#) lists the new features for Version 8.2(1).

**Table 7**      *New Features for ASA Version 8.2(1)*

| Feature                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Access Features</b>                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| One Time Password Support for ASDM Authentication | <p>ASDM now supports administrator authentication using one time passwords (OTPs) supported by RSA SecurID (SDI). This feature addresses security concerns about administrators authenticating with static passwords.</p> <p>New session controls for ASDM users include the ability to limit the session time and the idle time. When the password used by the ASDM administrator times out, ASDM prompts the administrator to re-authenticate.</p> <p>The following commands were introduced: <b>http server idle-timeout</b> and <b>http server session-timeout</b>. The <b>http server idle-timeout</b> default is 20 minutes, and can be increased up to a maximum of 1440 minutes.</p> |

**Table 7**      ***New Features for ASA Version 8.2(1) (continued)***

| Feature                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pre-fill Username from Certificate | <p>The pre-fill username feature enables the use of a username extracted from a certificate for username/password authentication. With this feature enabled, the username is “pre-filled” on the login screen, with the user being prompted only for the password. To use this feature, you must configure both the <b>pre-fill username</b> and the <b>username-from-certificate</b> commands in tunnel-group configuration mode.</p> <p>The double-authentication feature is compatible with the pre-fill username feature, as the pre-fill username feature can support extracting a primary username and a secondary username from the certificate to serve as the usernames for double authentication when two usernames are required. When configuring the pre-fill username feature for double authentication, the administrator uses the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Double Authentication              | <p>The double authentication feature implements two-factor authentication for remote access to the network, in accordance with the Payment Card Industry Standards Council Data Security Standard. This feature requires that the user enter two separate sets of login credentials at the login page. For example, the primary authentication might be a one-time password, and the secondary authentication might be a domain (Active Directory) credential. If either authentication fails, the connection is denied.</p> <p>Both the AnyConnect VPN client and Clientless SSL VPN support double authentication. The AnyConnect client supports double authentication on Windows computers (including supported Windows Mobile devices and Start Before Logon), Mac computers, and Linux computers. The IPsec VPN client, SVC client, cut-through-proxy authentication, hardware client authentication, and management authentication do not support double authentication.</p> <p>Double authentication requires the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-authentication-server-group</b>—Specifies the secondary AAA server group, which cannot be an SDI server group.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>authentication-attr-from-server</b>—Specifies which authentication server authorization attributes are applied to the connection.</li> <li>• <b>authenticated-session-username</b>—Specifies which authentication username is associated with the session.</li> </ul> <p><b>Note</b>    The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication.</p> |

**Table 7**      **New Features for ASA Version 8.2(1) (continued)**

| Feature                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AnyConnect Essentials                                 | <p>AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the adaptive security appliance, that provides the full AnyConnect capability, with the following exceptions:</p> <ul style="list-style-type: none"> <li>• No CSD (including HostScan/Vault/Cache Cleaner)</li> <li>• No clientless SSL VPN</li> <li>• Optional Windows Mobile Support</li> </ul> <p>The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client.</p> <p>To configure AnyConnect Essentials, the administrator uses the following command:</p> <p><b>anyconnect-essentials</b>—Enables the AnyConnect Essentials feature. If this feature is disabled (using the <b>no</b> form of this command), the SSL Premium license is used. This feature is enabled by default.</p> <p><b>Note</b> This license cannot be used at the same time as the shared SSL VPN premium license.</p> |
| Disabling Cisco Secure Desktop per Connection Profile | <p>When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN connections to the adaptive security appliance. This new feature lets you exempt certain users from running Cisco Secure Desktop on a per connection profile basis. It prevents the detection of endpoint attributes for these sessions, so you might need to adjust the Dynamic Access Policy (DAP) configuration.</p> <p>CLI: <b>[no] without-csd command</b></p> <p><b>Note</b> “Connect Profile” in ASDM is also known as “Tunnel Group” in the CLI. Additionally, the <b>group-url</b> command is required for this feature. If the SSL VPN session uses connection-alias, this feature will not take effect.</p>                                                                                                                                                                                                                                                                                                                           |
| Certificate Authentication Per Connection Profile     | <p>Previous versions supported certificate authentication for each adaptive security appliance interface, so users received certificate prompts even if they did not need a certificate. With this new feature, users receive a certificate prompt only if the connection profile configuration requires a certificate. This feature is automatic; the <b>ssl certificate authentication</b> command is no longer needed, but the adaptive security appliance retains it for backward compatibility.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| EKU Extensions for Certificate Mapping                | <p>This feature adds the ability to create certificate maps that look at the Extended Key Usage extension of a client certificate and use these values in determining what connection profile the client should use. If the client does not match that profile, it uses the default group. The outcome of the connection then depends on whether or not the certificate is valid and the authentication settings of the connection profile.</p> <p>The following command was introduced: <b>extended-key-usage</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SSL VPN SharePoint Support for Win 2007 Server        | <p>Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Table 7**      ***New Features for ASA Version 8.2(1) (continued)***

| <b>Feature</b>                                                                        | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared license for SSL VPN sessions                                                   | <p>You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the adaptive security appliances as a shared license server, and the rest as clients. The following commands were introduced: <b>license-server</b> commands (various), <b>show shared license</b>.</p> <p><b>Note</b> This license cannot be used at the same time as the AnyConnect Essentials license.</p>                                                                                                                                                                                                                                                                                                     |
| <b>Firewall Features</b>                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| TCP state bypass                                                                      | <p>If you have asymmetric routing configured on upstream routers, and traffic alternates between two adaptive security appliances, then you can configure TCP state bypass for specific traffic. The following command was introduced: <b>set connection advanced tcp-state-bypass</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy | <p>In Version 8.0(4), you configured a global media-termination address (MTA) on the adaptive security appliance. In Version 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTAs). As a result of this enhancement, the old CLI has been deprecated. You can continue to use the old configuration if desired. However, if you need to change the configuration at all, only the new configuration method is accepted; you cannot later restore the old configuration.</p>                                                                                                                                                                                                                                                                                        |
| Displaying the CTL File for the Phone Proxy                                           | <p>The Cisco Phone Proxy feature includes the <b>show ctl-file</b> command, which shows the contents of the CTL file used by the phone proxy. Using the <b>show ctl-file</b> command is useful for debugging when configuring the phone proxy instance.</p> <p>This command is not supported in ASDM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Clearing Secure-phone Entries from the Phone Proxy Database                           | <p>The Cisco Phone Proxy feature includes the <b>clear phone-proxy secure-phones</b> command, which clears the secure-phone entries in the phone proxy database. Because secure IP phones always request a CTL file upon bootup, the phone proxy creates a database that marks the IP phones as secure. The entries in the secure phone database are removed after a specified configured timeout (via the <b>timeout secure-phones</b> command). Alternatively, you can use the <b>clear phone-proxy secure-phones</b> command to clear the phone proxy database without waiting for the configured timeout.</p> <p>This command is not supported in ASDM.</p>                                                                                                                                     |
| H.239 Message Support in H.323 Application Inspection                                 | <p>In this release, the adaptive security appliance supports the H.239 standard as part of H.323 application inspection. H.239 is a standard that provides the ability for H.300 series endpoints to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel. The adaptive security appliance opens a pinhole for the additional media channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13. The decoding and encoding of the telepresentation session is enabled by default. H.239 encoding and decoding is preformed by ASN.1 coder.</p> |

**Table 7**      **New Features for ASA Version 8.2(1) (continued)**

| Feature                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck | H.323 application inspection has been enhanced to process common H.323 endpoints. The enhancement affects endpoints using the extendedVideoCapability OLC with the H.239 protocol identifier. Even when an H.323 endpoint does not send OLCAck after receiving an OLC message from a peer, the adaptive security appliance propagates OLC media proposal information into the media array and opens a pinhole for the media channel (extendedVideoCapability).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IPv6 in transparent firewall mode                                | Transparent firewall mode now participates in IPv6 routing. Prior to this release, the adaptive security appliance could not pass IPv6 traffic in transparent mode. You can now configure an IPv6 management address in transparent mode, create IPv6 access lists, and configure other IPv6 features; the adaptive security appliance recognizes and passes IPv6 packets.<br><br>All IPv6 functionality is supported unless specifically noted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Botnet Traffic Filter                                            | <p>Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.”</p> <p><b>Note</b>    This feature requires the Botnet Traffic Filter license. See the following licensing document for more information:</p> <p style="text-align: center;"><a href="http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html">http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html</a></p> <p>The following commands were introduced: <b>dynamic-filter</b> commands (various), and the <b>inspect dns dynamic-filter-snoop</b> keyword.</p> |
| AIP SSC card for the ASA 5505                                    | The AIP SSC offers IPS for the ASA 5505 adaptive security appliance. Note that the AIP SSM does not support virtual sensors. The following commands were introduced: <b>allow-ssc-mgmt</b> , <b>hw-module module ip</b> , and <b>hw-module module allow-ip</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IPv6 support for IPS                                             | You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the <b>match any</b> command, and the policy map specifies the <b>ips</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 7**      ***New Features for ASA Version 8.2(1) (continued)***

| <b>Feature</b>                  | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Management Features</b>      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SNMP version 3 and encryption   | <p>This release provides DES, 3DES, or AES encryption and support for SNMP Version 3, the most secure form of the supported security models. This version allows you to configure authentication characteristics by using the User-based Security Model (USM).</p> <p>The following commands were introduced:</p> <ul style="list-style-type: none"> <li>• <b>show snmp engineid</b></li> <li>• <b>show snmp group</b></li> <li>• <b>show snmp-server group</b></li> <li>• <b>show snmp-server user</b></li> <li>• <b>snmp-server group</b></li> <li>• <b>snmp-server user</b></li> </ul> <p>The following command was modified:</p> <ul style="list-style-type: none"> <li>• <b>snmp-server host</b></li> </ul> |
| NetFlow                         | <p>This feature was introduced in Version 8.1(1) for the ASA 5580; this version introduces the feature to the other platforms. The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Routing Features</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Multicast NAT                   | The adaptive security appliance now offers Multicast NAT support for group addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Troubleshooting Features</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Coredump functionality          | <p>A coredump is a snapshot of the running program when the program has terminated abnormally. Coredumps are used to diagnose or debug errors and save a crash for later or off-site analysis. Cisco TAC may request that users enable the coredump feature to troubleshoot application or system crashes on the adaptive security appliance.</p> <p>To enable coredump, use the <b>coredump enable</b> command.</p>                                                                                                                                                                                                                                                                                             |



# 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 these sections to the resolved caveats from later releases. For example, if you are running Release 8.2(1), then you need to add the caveats in this section to the resolved caveats from 8.2(2) and above 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://www.cisco.com/support/bugtools>

**Table 8** *Open Caveats in Version 8.2*

| Caveat ID  | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCsu02296 | ASA - show parser dump all crashes ASA                                   |
| CSCsv69723 | sharepoint 2007: cannot download picture                                 |
| CSCsw51998 | Traceback in Thread Name: DHCP Receiver                                  |
| CSCsw63541 | Titan Performance drop of more than 13% in conns/sec test.               |
| CSCsy15575 | asa locks up during boot process                                         |
| CSCsz44017 | Crash when pinging public interface over tunnel using proxy              |
| CSCsz78203 | ASA STI 8.0 flash console hang while booting up Titan 8.2.1 release      |
| CSCtb04908 | traceback Unicorn Proxy Thread Page fault: Address not mapped            |
| CSCtb14102 | Crash occurs when cplan of CSC-SSM card configured for ether-type pppoe  |
| CSCtb37623 | police conform-action and exceed-action not displayed in config          |
| CSCtb59109 | Traceback seen when match command is configured on asa_dataplane         |
| CSCtb63515 | Clientless webvpn on ASA cannot save .html attached file with IE6 OWA    |
| CSCtb83798 | ASA 8.2.1 crash at fover_parse                                           |
| CSCtc10599 | traceback when using CLI from ASDM                                       |
| CSCtc12240 | Webvpn- rewrite : ASA inserts lang=VBScript incorrectly                  |
| CSCtc14782 | IPSec Client u-turn with nat fails to look up correct route.             |
| CSCtc32031 | ASA may reload with traceback in thread name CTM message handler         |
| CSCtc32872 | TFW ENH: Management interface should operate in routed mode              |
| CSCtc59462 | traceback Thread Name: ssh (Old pc 0x08b4465b <npshim_read+187 at tcp/np |
| CSCtc65904 | OSPF L2L tunnel neighbors are DOWN after del/add of configuration        |
| CSCtc79873 | ASA 8.2 may calculate memory usage incorrectly                           |
| CSCtc84814 | infinite prompts of cert validation failure during AnyConnect cert auth. |
| CSCtc95659 | tftp with inspection on fails to go through a lan-2-lan tunnel           |
| CSCtd21002 | Web page does not refresh after initial Citrix client installation       |
| CSCtd22166 | ASA grinding VPN Client download performance to a halt (<1Mb/s)          |

**Table 8**      **Open Caveats in Version 8.2 (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtd34212       | Unexpected ACL recompile failure messages                                |
| CSCtd56497       | Traceback with scp after failed download                                 |
| CSCtd58338       | dsh_alloc_handle fails when there are free handles in other core's pools |
| CSCtd59046       | AAA: ASA-5505 with AAA configured wont execute cmds when heavy traffic   |
| CSCtd73605       | ASA RIP: "no redistribute static" breaks "default-information originate" |
| CSCtd73901       | Linkdown, Coldstart SNMP Traps not sent with certain snmp-server config  |
| CSCtd93250       | Traceback : assert+12 at ../finesse/snap_api.h:141                       |
| CSCtd94634       | Suspected memory allocation with logging causes crash                    |
| CSCte01475       | EIGRP : static route redistribution with distribute-list not working     |
| CSCte04806       | ASA: Application install fails from the clientless portal.               |
| CSCte08816       | ASA NAT: LU allocate xlate failed error                                  |
| CSCte15867       | ASA 8.2 - EIGRP - route not redistributed properly with distribution lst |
| CSCte21184       | Citrix Web App fails to start through rewriter                           |
| CSCte64052       | ASA 5505 - 10 user version VPN sessions impact FW restricted license     |
| CSCte66535       | console hangs w/ sys load after bouncing webvpn on private interface     |
| CSCte66723       | Traceback thread ci/console - Invalid permission after bouncing webvpn   |
| CSCte67462       | ASA shows duplicate header when a webserver is accessed via WebVPN       |
| CSCte69307       | asp encrypt rule disappears after toggling answer-only crypto-map        |
| CSCte69623       | df election in pim bidir mode fails after failover to secondary unit     |
| CSCte78884       | without-csd should only work with group-url                              |
| CSCte81296       | Camera software not accessible via Clientless SSL VPN                    |
| CSCte90946       | Multi-context ASA Resets a connection from Flooded packet                |
| CSCtf01287       | SSH to the ASA may fail - ASA may send Reset                             |
| CSCtf02759       | webvpn rewriter fails to parse </object> java tag correctly              |
| CSCtf08776       | parser ambiguity when host token is associated to an ip address          |
| CSCtf20269       | 1550 block exhaustion due to EIGRP multicast storm                       |
| CSCtf23503       | Unable to access custom medical appli through Clientless VPN             |
| CSCtf25227       | 5505 Assertion when reset device to factory default config               |
| CSCtf29640       | Certificate authentication fails intermittently                          |
| CSCtf33314       | WebVPN CIFS browsing not working on Windows Mobile 6.1/6.5               |
| CSCtf42361       | show memory output incorrect after memory install and upgrade to 8.2.2   |
| CSCtf42689       | CIFS, "dir cifsSharedAuth:" causing traceback                            |
| CSCtf51799       | "No failover active" on active unit triggers the reload of the standby.  |
| CSCtf54075       | Free memory in show memory and show memory detail is not same            |
| CSCtf66116       | ASA: May crash in Thread Name: Dispatch Unit                             |
| CSCtf76330       | Standby memory leak in chunk_create via SNP Conn Core                    |

**Table 8**      **Open Caveats in Version 8.2 (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtf79704       | ASA -- crasActGrNumUsers does not update after upgrade                   |
| CSCtf88764       | Failover should not allow broadcast failover address                     |
| CSCtf88768       | Traceback with assert in fover_parse on secondary when syncing config    |
| CSCtf91234       | Traceback in thread name: accept/http                                    |
| CSCtf99449       | Traceback in thread name Dispatch Unit                                   |
| CSCtg06316       | Insufficient performance during the packet flood                         |
| CSCtg06320       | DHCP ACK not sent by the firewall.                                       |
| CSCtg17455       | Unable to access Remedy 7 with WebVPN                                    |
| CSCtg22656       | ASA local CA: not redirected to cert download page when user first login |
| CSCtg31015       | EIGRP bandwidth value listed incorrectly for SFP gig link on SSM-4GE     |
| CSCtg33991       | ASR is still working after stateful link is disabled                     |
| CSCtg39093       | ASA hardware accelerator may report 402124 and write crypto_arch files   |
| CSCtg43426       | Orhtrus ATA 187: Cannot dial out call from ATA 187 with Phone Proxy      |
| CSCtg50770       | Mngt-access (ASDM,SSH) to inside intf of 5580 fails over RA VPN session  |
| CSCtg54999       | ASA - traceback in Thread Name: websns_snd                               |
| CSCtg58074       | ASA CRYPTO: Hardware Accelerator Archive File Created                    |
| CSCtg60825       | tcp normalizer: Incorrect Proxy ACK's seen with inspect esmtp enabled    |
| CSCtg61106       | ASA GUI Text and Messages customization not working.                     |
| CSCtg63992       | standby running out of 1550 blocks after multicast traffic               |
| CSCtg64034       | config sync does not complete and secondary keeps going to no failover   |
| CSCtg64391       | ASA5580 8.2.1 crashes with thread name: dhcp_daemon                      |
| CSCtg68013       | AC can't handle pre-login banner from ASA containing Japanese characters |
| CSCtg68791       | traceback _fiber_setup_for_jumpstart+37 at unicorn/ak47/fibers/fibers-ju |
| CSCtg71327       | Spyker: Root cause issue where Cavium chip fails reset                   |
| CSCtg71534       | Localization fails when using CSD with ASA v8.2.2.x and 8.3.x            |
| CSCtg71572       | vpn-simultaneous-logins configuration does not work for certification    |
| CSCtg74172       | Can get around dynamic-filter by using caps in domain name               |
| CSCtg76404       | Traceback in Thread Name: Checkheaps due to logging                      |
| CSCtg76698       | ASA: Manual Installation link for AnyConnect doesn't work                |
| CSCtg78775       | asa passes the first packet but denies the rest in pim bidir mode        |
| CSCtg82062       | Secondary tracebacks after removing large unused ACLs (3000 lines)       |
| CSCtg83750       | ASA: New ASDM/WEBVPN/SVC login sessions fail after some time             |
| CSCtg86381       | Error when addressing management interface with IPv6                     |
| CSCtg86810       | show run all command causes SSH session hang                             |
| CSCtg86983       | OSPF route remains on Standby ASA after failover                         |
| CSCtg87046       | WebVPN: unmangled POST requests from SAP webinterface                    |

**Table 8**      **Open Caveats in Version 8.2 (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtg88242       | HT box crashed @ fl_parse_cmd when running HTTP/SIP/FTP/RTSP/SCCP traffi |
| CSCtg88576       | asa standby unit crashes with assertion in snp_sp_action.c               |
| CSCtg89906       | Config locked due to snmp trap syslog config and ICMP port unreachable   |
| CSCtg93137       | Crash in capture_core_local_block when running SCCP PP calls & SIP calls |
| CSCtg94337       | assert failure in unicorn proxy thread using checked build.              |
| CSCtg97450       | clear config all causes crash in fover_health_monitoring_thread          |
| CSCtg99650       | HA: active goes to standby for no apparent reason...sync's empty cfg     |
| CSCth05467       | WebVPN: Any email can't be send in OWA 2010 with S/MIME installed        |
| CSCth05550       | Skinny TCP Proxy sends TCP Ack before receiving TCP Ack from destination |
| CSCth05564       | ASA traceback in Thread Name: Unicorn Admin Handler                      |
| CSCth07710       | Camera page does not load correctly                                      |
| CSCth11492       | Crash seen after Primary ASA reloads and is switched to active role      |
| CSCth12612       | ASA - VPN load balancing is disabled after failover                      |
| CSCth13865       | ASA CPU Hog causes interface overruns when Gig interface is 100Mbps.     |
| CSCth14248       | ASA not sending all logging messages via TCP logging                     |
| CSCth16122       | Interface overruns upon SSH                                              |
| CSCth20293       | Cannot access Kronos application using Clientless SSL VPN                |
| CSCth23673       | WebVPN: All control(ribbon) elements don't work for SharePoint 2010      |
| CSCth26429       | WebVPN: "Add new..." button doesn't work properly for SharePoint 2010    |
| CSCth26474       | 1550 blocks get depleted                                                 |
| CSCth26636       | Page fault in unicorn proxy on memory exhaustion with system tests       |
| CSCth27045       | Spyker single-routed mode memory leaks in PSI system tests               |
| CSCth31814       | Changing interface config to dhcp will add AAA cmd and break EasyVPN     |
| CSCth31999       | IPSec RA cps at 181 is below 200 cps requirement.                        |
| CSCth34278       | Clientless WebVPN Memory Leak Causes Blank Page after Authentication     |
| CSCth35961       | WebVPN: Preview mode for emails works improperly for DWA 8.5.1           |
| CSCth36061       | WebVPN: Send (save, ...) actions don't work for DWA 8.5.1 in Firefox     |
| CSCth38998       | Unable to edit WebVPN configuration due to file corruption               |
| CSCth43126       | Access-list log interval not taking effect                               |
| CSCth48178       | ha :Watchdog fover_FSM_thread during failover IPv6 on SSM-4GE-INC        |
| CSCth48476       | ASA WebVPN doesnt rewrite URL Encoded Data in Location Response Header   |
| CSCth53036       | Memory corruption when using dfp in system test                          |
| CSCth58048       | Assert Failure caused Traceback in Thread Name: Dispatch Unit            |
| CSCth60145       | RRI not removed after user disconnects - impacting load-balancing        |
| CSCth61141       | ASA opens interactive shell over ssh with plink                          |
| CSCth66117       | IPv6 traffic may fail because ASA chooses wrong source address           |

**Table 8**      **Open Caveats in Version 8.2 (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCth66959       | ASA WebVPN : VMware apps fail when server uses certs                     |
| CSCth70023       | ASA crash in Thread Name:License Thread                                  |
| CSCth72997       | 'Authentication Error' When Trying to Browse Domain-Based DFS            |
| CSCth81252       | Spyker: Thread Name: vfw_init_thread Page fault: Address not mapped      |
| CSCth81601       | ASA tracebacks in Thread Name: Dispatch Unit                             |
| CSCth82011       | CA certificate installation without optional extension fails on ASA      |
| CSCth83588       | cut-through proxy authentication prompt does not show up                 |
| CSCth84519       | PIM packet with own source address seen after failover on standby peer   |
| CSCth86217       | access-list line number not properly checked when a remark is removed    |
| CSCth86507       | Heap memory tail magic verification failed                               |
| CSCth87757       | ASA WebVPN Citrix Xenapp applications fail after upgrade from v5 to v9   |
| CSCth88759       | show vpn-sessiondb remote command missing group-policy & corrupted text  |
| CSCth90087       | WebVPN:sharepoint 07/word 07/excel 07 Create/Edit documents doesn't work |
| CSCth90235       | IPsec VPN with certificate auth fails to establish after some time       |
| CSCth92293       | ASA not syncing failover state                                           |
| CSCth93290       | Active unit tracebacks in Thread Name: IKE Daemon                        |
| CSCth95897       | P2 Spyker C crash with Panic at EDVT cold power cycle corner             |
| CSCth97195       | Search list with 5k elements times out/loads incompletely across WebVPN  |
| CSCth97257       | Icons (links) missing after running recalculate function                 |
| CSCti03135       | Search using Dojo Toolkit fails across WebVPN with 404 Error             |
| CSCti04034       | ASA fails to rewrite 'form["action"]' javascript construct               |
| CSCti06240       | Ipsec L2L performace is down about 50% with 64 byte pkts                 |
| CSCti07641       | APCF code does not interpret HTTP 304 response code correctly            |
| CSCti11757       | SNMP: ASA responds after two SNMP requests                               |
| CSCti12613       | Unable to launch ASDM, sslv3 alert bad certificate                       |
| CSCti13111       | ASA 8.2.(2)15 crash in Thread Name: IKE Daemon                           |
| CSCti13871       | Spyker: Reloads when Midland B is reset or when loading image            |
| CSCti14000       | snmp: Traceback in SNMP Notify Thread                                    |
| CSCti14272       | timebased license expired pre-maturely                                   |
| CSCti16381       | Interfaces in failed mode after zero-downtime downgrade procedure        |
| CSCti16586       | ASA 8.2(1)11 failed to return MIB data for SNMPV3 GetBulk request        |
| CSCti16694       | ASA 8.2(1)11 SNMP v3 - not able to set SNMP write view                   |
| CSCti17266       | IPSEC: ASA generates 'The ASA hardware accelerator Ipsec ring timed out' |
| CSCti20650       | Cannot assign MSIE PAC-URL to VPN users from RADIUS AV pairs             |
| CSCti20726       | ASA: ICMP error may be dropped due to rpf-check                          |
| CSCti21616       | Nameif a redundant intf with failover triggers consistent bogus warnings |

**Table 8**      *Open Caveats in Version 8.2 (continued)*

| Caveat ID  | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCti22636 | "failover exec standby" TACACS+ authorization failure                    |
| CSCti23723 | ASA does not handle HTTP HEAD requests for pages served on its Aware web |
| CSCti24271 | Unable to ssh to the ASA (8.2.2)                                         |
| CSCti24526 | Flood of random IPv6 router advertisements causes high CPU and DoS       |
| CSCti24552 | "no ipv6 address autoconfig" causes crash after ICMPv6 flood             |
| CSCti24787 | ASA version 8.2.2 crash in ThreadName:Tmatch compile                     |

## Resolved Caveats

This section includes the following topics:

- [Resolved Caveats in Version 8.2\(3\), page 22](#)
- [Resolved Caveats in Version 8.2\(2\), page 42](#)

## Resolved Caveats in Version 8.2(3)

The caveats listed in [Table 9](#) were resolved in software Version 8.2(3). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

<http://www.cisco.com/support/bugtools>

**Table 9**      *Resolved Caveats in Version 8.2(3)*

| Caveat ID  | Description                                                            |
|------------|------------------------------------------------------------------------|
| CSCei47856 | VPN: Need to add NAT-T support for RFC3947                             |
| CSCsi27903 | L2TP & NAC -> Default NAC policy prevents data from passing            |
| CSCsj40174 | SIP CRLF keepalives stall TCP-based SIP connections                    |
| CSCsj43055 | Increase CPU-hog syslog 711002 back to 100 ms by default               |
| CSCsj43068 | Make CPU hog more configurable (8.x)                                   |
| CSCsk03602 | FT: workaround for read-only flashes                                   |
| CSCsk40907 | DAP: Increase DAP aggregation max lists lengths and make them dynamic  |
| CSCsl04124 | SIP does not support 'early RTCP'                                      |
| CSCsl41515 | ASA traceback in Dispatch Unit (Old pc 0x00223a67 ebp 0x018b12f8)      |
| CSCsl95928 | High CPU utilization due to OSPF                                       |
| CSCsm11264 | When long url triggers syslog 304001 ASA stops sending syslogs to ASDM |
| CSCsm39914 | match resp body length for http class-map doesnt take correct value    |
| CSCsm40830 | traceback netfs_thread_init                                            |
| CSCsm98354 | No accounting packet for some commands                                 |
| CSCso33982 | Change or replace CPU Hog syslog message                               |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCso65967       | SIP builds many secondary conns with register msg but no registrar       |
| CSCsq34317       | Without authproxy currently configured, authproxy DACLs may become stale |
| CSCsq34336       | ASA: rate-limiting for encrypted s2s traffic not consistently handled    |
| CSCsq53127       | DACL remain stale when when used with EzVPN NEM                          |
| CSCsq61081       | Intf monitoring table for ASDM history stats shows the wrong timestamp   |
| CSCsr39880       | Insert and removal of compact flash may result in system hang            |
| CSCsr66402       | Tracebacks on standby unit (Thread Name: lu_rx)                          |
| CSCsr96463       | ASA denial of service on dhcp server                                     |
| CSCsu27158       | Traceback in Unicorn Proxy Thread (Old pc <fiber_yield+92 )              |
| CSCsu27257       | "show asp table classify" doesn't show WCCP domain                       |
| CSCsu48860       | traceback eip 0x08c4cab2 log_to_servers+1426 at /slib/include/channel.h  |
| CSCsu56483       | Extend show ak47 to display per pool and per block information           |
| CSCsu77600       | WEBVPN RDP plugin window keys are incorrect. Shift (key) .jar            |
| CSCsv16326       | 'mac-address auto' causes interfaces to fail                             |
| CSCsv36948       | CIFS access to Win2008 server via IP address is not working.             |
| CSCsv37979       | Changing interface IP Address does not clear existing connections        |
| CSCsv40504       | Telnet connection permitted to lowest security level interface           |
| CSCsv52169       | Traceback at thread name PIX Garbage Collector                           |
| CSCsv65768       | Webvpn memory leak in ramfs-blocks                                       |
| CSCsv66510       | Smart Tunnel on Mac Leopard 10.5.x failing                               |
| CSCsv71282       | Numerous CPU-hogs in vpnfol_thread_timer                                 |
| CSCsv71555       | Traceback on ASA during configuration of h323 inspection                 |
| CSCsv73764       | Unable to Browse to Domain Based DFS Namespaces                          |
| CSCsv86200       | ASA 8.0.4.7 Traceback in Thread Name: tmatch compile thread              |
| CSCsv89645       | ASA 8.04 - certificate chain not being sent when configured w/ IPSEC RA  |
| CSCsv91391       | L2TP with EAP auth stuck [%ASA-4-403102 - authentication pending]        |
| CSCsv91564       | Multiple certificates are installed to one trustpoint when importing.    |
| CSCsv92337       | Assert in syslog.c when called from the CTM data path.                   |
| CSCsv94599       | ASA5550 reloads in tmatch_compile thread on tmatch_element_release       |
| CSCsv96545       | ASA is dropping arp on SSM-4GE                                           |
| CSCsv98614       | Crash in ASA when CIPC phones registers from DMZ                         |
| CSCsw19588       | Standby console freezes if user logs in prior to detecting mate          |
| CSCsw25253       | ssl vpn related memory corruption causes traceback                       |
| CSCsw37504       | ISAKMP delayed when processing large CRL files                           |
| CSCsw41161       | PMTUD - ICMP type 3 code 4 generated for GRE flow is dropped 313005      |
| CSCsw47441       | Java Applet Signing Error..plugins still use old expired certificate     |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsw48687       | Telnet and SSH bookmarks greyed out                                      |
| CSCsw49953       | custom dns group is ignored in WebVPN searches - error contacting host   |
| CSCsw51809       | sqlnet traffic causes traceback with inspection configured               |
| CSCsw63453       | "Error Contacting Host" when accessing CIFS shares with spaces           |
| CSCsw70329       | Remote access vpn unable to est after failover with DHCP assigned addr   |
| CSCsw70786       | SACK is dropped when TCP inspection engines are used                     |
| CSCsw70793       | L4TM: Memory leak with l4tm use-dynamic-data                             |
| CSCsw76595       | PP: phone cannot register when configured as Authenticated on UCM        |
| CSCsw77033       | SSL VPN: Java-rewriter: memory leak implicating WebVPN                   |
| CSCsw79486       | ASA SDI auth is not responding in time when wrong credentials is entered |
| CSCsw83282       | Watchdog failure in fover_FSM_thread                                     |
| CSCsw85251       | dhcp-network-scope ip that matches interface can cause route deletion    |
| CSCsw88037       | Traceback in IKE Daemon (Old pc 0x080f3c55 <ctm_wait_for_synchronous_com |
| CSCsw90161       | Traceback on Standby after excuting "show vpn session remote"            |
| CSCsw90717       | ASA phone Proxy reboots unexpectedly                                     |
| CSCsw91072       | Identity cert being imported without errors, if conflicting with CA cert |
| CSCsx03234       | ASA automatically restarting after receiving OCSP response               |
| CSCsx03294       | 1550 block leaks leading active ASA to reload                            |
| CSCsx03473       | ASA traceback in Thread Name: netfs_thread_init                          |
| CSCsx03746       | "threat-detection statistics host" disappears                            |
| CSCsx07091       | PIX/ASA LDAP authentication doesn't work over tunnel                     |
| CSCsx07862       | Traffic shaping with priority queueing causes packet delay and drops     |
| CSCsx08270       | PP: Explicit ACL deny will cause secure phones to fail registration      |
| CSCsx15055       | set nat-t-disable in crypto map does not override global nat-t config    |
| CSCsx15589       | "revocation check ocsp none" does not reject revoked certificates        |
| CSCsx16147       | Traceback in Thread Name: fover_parse                                    |
| CSCsx19947       | IGMP Join fails on subinterface after upgrade to 8.1(2)                  |
| CSCsx20038       | Wrong counters in "show int" for Redundant interface                     |
| CSCsx23797       | SSL decrypt error using NULL-SHA1                                        |
| CSCsx25628       | %PIX ASA-3-713128 should be logged as a lower level message              |
| CSCsx27609       | 5580 traceback implicating snp_nat_find_portlist w/ stress test          |
| CSCsx27851       | Entering interface ? from cmd specific config mode returns to global cfg |
| CSCsx27861       | Both ASAs are active when FO interfaces are directly connected           |
| CSCsx29872       | SSL VPN: Script Errors When Accessing DWA 8.0.2                          |
| CSCsx30193       | Failover slow to switchover when LAN interface connected with crossover  |
| CSCsx31333       | Spaces in DAP record name should be allowed                              |



**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsx34892       | SNMP traps for certain contexts not generated                            |
| CSCsx35351       | ASA 5505 ezvpn may leak memory due to startup errors                     |
| CSCsx41170       | uauth inactivity timer not taking effect                                 |
| CSCsx42122       | ASA/CSD - certificate mapping does not work if CSD is enabled            |
| CSCsx42142       | static route: ASA should not accept static multicast routes              |
| CSCsx43658       | WebVPN CIFS: uploading files fails sometimes to HomeServer               |
| CSCsx44083       | Traceback during large ACL Compilation - driver ioctl call               |
| CSCsx50318       | OCSF revocation stops working after some time on Cisco ASA               |
| CSCsx50721       | Anyconnect unable to establish DTLS tunnel if ASA IP address change      |
| CSCsx50884       | Adding shared interface to second context stops traffic to 1st context   |
| CSCsx52598       | No focus on 'More information required' radius challenge/response page   |
| CSCsx52748       | ASA may crash under high IPSEC load                                      |
| CSCsx53529       | Traceback on telnet/ci from "show nat" command                           |
| CSCsx54449       | ASA may process LDAP password policy with no password-management         |
| CSCsx54893       | CSD: Unable to run smart-tunnel inside "browser only" vault              |
| CSCsx57142       | SIP Inspection Doesn't NAT Call-info field in SIP Notify message         |
| CSCsx58682       | ASA Local CA and caSe SenSiTiviTy - p12 file vs. username conflict       |
| CSCsx59014       | ASA allows VPN user although Zonelabs Integrity firewall rejects         |
| CSCsx59403       | Automatically added AAA command break ASA5505EasyVPN client after reboot |
| CSCsx59746       | Tacacs Command Accounting does not send packet for 'nat-control'         |
| CSCsx61755       | aaa Page fault: Invalid permission when box is under moderate stress     |
| CSCsx64741       | Page fault: Address not mapped with telnet traffic. eip and cr2 = 0      |
| CSCsx64804       | CIFS URI cutoff after 15 characters                                      |
| CSCsx65702       | ASA traceback upon failover with interface monitor enabled               |
| CSCsx65945       | High memory usage in chunk_create                                        |
| CSCsx67543       | Change default username from pix to asa, or remove all together          |
| CSCsx68049       | ASA - High CPU by function "branch_height" from CPU profile              |
| CSCsx68765       | VMWARE web applications (view/vdm) do not work with smart-tunnel         |
| CSCsx70559       | TCP Proxy drops the keepalives ACK sent on H225 conn, call gets dropped  |
| CSCsx73295       | CSF-MOC clients can not register with OCS with ASA SIP-INSPECT           |
| CSCsx73547       | Stateful Conns Disappear From Standby During Failover                    |
| CSCsx76473       | CSD: Group-url fails in Vault.                                           |
| CSCsx77780       | Adding shared interface to second context stops traffic to 1st context   |
| CSCsx79918       | Crypto CA limited to 65536 requests                                      |
| CSCsx80024       | spin_lock_release_actual:lock->owner=bcc20000,process_self=7b3d000,lock_ |
| CSCsx81472       | ASA might automatically restart after issuing 'show vpdn'                |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsx81722       | ASA 8.0.4 traceback in Thread Name: IKE Daemon                           |
| CSCsx83353       | WCCP Service Ports Missing in ASP Table when Adding Redirect ACL Entry   |
| CSCsx94330       | AC with CSD and DAP for Posture Assessment matches wrong DAP Policy      |
| CSCsx94849       | Unpredictable behavior after failover w/shortest timeout conf.           |
| CSCsx95377       | Adding host to http access results in Could not start Admin error        |
| CSCsx95461       | ifHighSpeed and ifSpeed values are zero for 10G operational interfaces   |
| CSCsx95785       | ifType values returns as other (1) for 10G interfaces                    |
| CSCsx97569       | PIX/ASA traceback with Thread Name: CMGR Server Process                  |
| CSCsx99960       | ASA5580-20 traceback in CP Processing                                    |
| CSCsy01000       | Cannot start ASDM session - ssl lib error                                |
| CSCsy03579       | Standby ASA traceback after becoming active, EIP snp_fp_inspect_dns+42   |
| CSCsy04974       | Syslog 113019 Disconnect reason not working                              |
| CSCsy08416       | emWEB crashes on requests to filenames with white spaces                 |
| CSCsy08905       | process_create corrupt ListQ memory when MAX_THREAD is exceeded          |
| CSCsy10473       | ASA Improve RADIUS accounting disconnect codes for vpn client            |
| CSCsy13488       | DDNS: A RR update fails if cache entry exists in show dns-host           |
| CSCsy14672       | ASA might automatically restart in Thread Name: ppp_timer_thread         |
| CSCsy16595       | The ASA traceback intermittent in IPSec                                  |
| CSCsy17783       | Large CRLs freeze processing on the ASA for extended time periods        |
| CSCsy20002       | File upload causes hang without recovery                                 |
| CSCsy21333       | Traceback in Thread Name: aaa when using Anyconnect with certificate     |
| CSCsy21727       | Failover pair is not able to sync config and stuck in Sync Config state  |
| CSCsy22484       | Cisco ASA may traceback after processing certain TCP packets             |
| CSCsy23275       | Smart Tunnels and POST parameters should be interoperable                |
| CSCsy26775       | Traceback while refreshing CRL                                           |
| CSCsy27395       | qos: traceback in thread name: ssh, eip mqc_get_blt_def                  |
| CSCsy27547       | Using phone-proxy got assertion "ip.ip_version == IP_VERSION_4"          |
| CSCsy28792       | ESMTP inspection drops DKIM signed emails with content-type              |
| CSCsy28853       | inspect-mgcp: call-agent name and gateway name disappears after a reboot |
| CSCsy29949       | WebVPN: slow response with CGI scripts                                   |
| CSCsy30717       | Keepalive not processed correctly thru TCP Proxy                         |
| CSCsy31955       | Incorrect severity for ASA syslog message 106102                         |
| CSCsy32767       | WebVPN OWA 2007 + AttachView Freezes IE6 and will not close              |
| CSCsy47993       | Names not supported in EIGRP summary-address command                     |
| CSCsy48107       | "clear crypto ipsec sa entry" command doesnt seem to work                |
| CSCsy48250       | "clear crypto ipsec sa entry" command doesnt work                        |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsy48626       | Traceback due to illegal address access in Thread Name: DATAPATH-0-466   |
| CSCsy48816       | webvpn cifs unc url doesn't work                                         |
| CSCsy49823       | Interface fails to pass traffic because soft-np shows interface as down  |
| CSCsy49841       | ASA Traceback in Thread fover_FSM_thread with A/A FO testing             |
| CSCsy50018       | Lua recovery errors observed during boot in multiple-context mode        |
| CSCsy50113       | traceback in Dispatch Unit: Page fault: Address not mapped               |
| CSCsy50428       | page fault while adding/enrolling users to Local CA w/script             |
| CSCsy53263       | Tacacs connection match accounting does not display port information     |
| CSCsy53387       | " crypto map does not hole match" message pops up during conditon debug  |
| CSCsy55762       | Memory leak in 72 / 80 / 192 bytes memory blocks [ tmatch]               |
| CSCsy56403       | ASA stops accepting IP from DHCP when DHCP Scope option is configured    |
| CSCsy56570       | Redundant interface as failover link lose peer route after reload        |
| CSCsy56739       | Traceback on standby while processing write memory if context is removed |
| CSCsy57590       | AC asks for Username/Password after certs fail with group-url cert only  |
| CSCsy57872       | Unable to SSH over remote access VPN (telnet, asdm working)              |
| CSCsy58218       | WebVPN: hide internal password in customization doesn't work             |
| CSCsy59225       | FW sends rst ack for tcp packet with L2 multicast mac not destined to it |
| CSCsy60403       | SSL rekey fails for AnyConnect when using client-cert authentication     |
| CSCsy64028       | WebVPN: NTLM authentication does not work on a cu server                 |
| CSCsy65734       | ASA: traceback with thread name "email client"                           |
| CSCsy68961       | ASA 5580 reboots with traceback in threat detection                      |
| CSCsy71401       | Traceback when editing object-group                                      |
| CSCsy72423       | WebVPN: ASA sends a bad If-Modified-Since header                         |
| CSCsy74773       | page fault in fover _parse on a/s stress with 240 vlan on 2 red ifaces   |
| CSCsy75345       | subintefaces on 4ge-ssm ports fail with mac-address auto and failover    |
| CSCsy75401       | "Failover act l group #" not working with SSM 4GE as failover connection |
| CSCsy75684       | Traceback from thread DATAPATH-0-483 on failover                         |
| CSCsy75720       | asdm does not connect to secondary on failover                           |
| CSCsy75800       | Shared int Mac add auto reload primary there will be some packet loss    |
| CSCsy76163       | Not able utilize search engine via webvpn                                |
| CSCsy76537       | Issue with RTP Pinhole timeout                                           |
| CSCsy77628       | the procedure of copying a file from ramfs to flash should be atomic     |
| CSCsy78105       | CPOC: Watchdog Traceback in snp_flow_free / snp_conn_release             |
| CSCsy80242       | ASA: LDAP Password-expiry with Group-Lock locks users out                |
| CSCsy80565       | Mfw-routed sub-sec fover A/S setup re-syncs on context add               |
| CSCsy80716       | WebVPN: full customization disables dap message                          |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsy81426       | Sip inspection is dropping ftp secondary connection on port 5060         |
| CSCsy81475       | Traceback due to assert in Thread Name: DATAPATH-0-466                   |
| CSCsy82188       | WebVPN: ASA can't support IP/mask based NTLM SSO consistently            |
| CSCsy82260       | ASA fails to redirect traffic to WCCP cache server                       |
| CSCsy83043       | Redundant interface is down if any member is down at boot                |
| CSCsy83106       | Unable to add member interface to Redundant Interface                    |
| CSCsy84268       | AIP-SSM stays in Unresponsive state after momentary voltage drop         |
| CSCsy85642       | websense restriction access page does not display                        |
| CSCsy85759       | Remove "Server:" directive from SSL replies when CSD enabled             |
| CSCsy86769       | ASA5505 should not allow pkts to go thru prior to loading config         |
| CSCsy86795       | ASA - Log messages for all subinterfaces seen when adding just one vlan  |
| CSCsy87867       | ASA inspect pptp does not alter Call ID in inbound Set-Link-info packets |
| CSCsy88084       | Smart Tunnel failing on MAC 10.5.6 with Firefox 2 and Safari             |
| CSCsy88174       | ESMTP inspection "match MIME filetype" matches on file content as well   |
| CSCsy88238       | Memory leak in Webvpn related to CIFS                                    |
| CSCsy90150       | ASA doesn't properly handle large SubjectAltName field - UPN parse fails |
| CSCsy91142       | Using name aliases for the interface will cause vpn lb to break          |
| CSCsy92661       | Traceback in Thread Name: Dispatch Unit (Old pc 0x081727e4 ebp 0xaad3cd1 |
| CSCsy93180       | DWA 8.5: Unable to send an e-mail with attachment.                       |
| CSCsy94410       | asa in tfw mode reboots on ping to ipv6 addr with no ipv6 addr on box    |
| CSCsy96753       | WebVPN Flash rewriter may not clean up all temporary files               |
| CSCsy97437       | SNMP community string not hidden in 'show startup' or 'show conf'        |
| CSCsy98446       | Memory leaked when matching tunnel group based on URL                    |
| CSCsy98584       | Traceback on Thread Name: AAA due to downloadable ACL processing         |
| CSCsy98662       | Access-list allows port ranges with start-port greater than end-port     |
| CSCsy99063       | traceback Thread Name: fover_tx after multiple SSH to active unit        |
| CSCsz01314       | Traceback in ci/console after sh crypto ipsec sa                         |
| CSCsz02807       | Logging standby can create logging loop with syslogs 418001 and 106016   |
| CSCsz02849       | Long delay before standby becomes active if unit holdtime misconfigured  |
| CSCsz06329       | Unexpect Syslog: No SPI to identify Phase 2 SA                           |
| CSCsz10339       | console hangs for extended period of time when config-url is applied     |
| CSCsz10924       | Management port in promiscuous mode processes packets not destined to it |
| CSCsz11180       | TCP Proxy mis-calculates TCP window causing connectivity problems        |
| CSCsz11835       | ASA intermittently drops traffic for authenticated users w/auth-proxy    |
| CSCsz17027       | L2TP: DACL w/ Wildcard Mask not applied to L2TP over IPSec Clients       |
| CSCsz18759       | Certificate mapping does not override the group chosen by URL            |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsz19296       | IPSEC NAT-T - block may get dropped due to VPN handle mismatch           |
| CSCsz20830       | webpage showing missing content.                                         |
| CSCsz22256       | ASA disconnects IPSec VPN client at P2 rekey with vlan mapping in grppol |
| CSCsz24401       | Stuck EIGRP ASP entry prevents neighbor from coming up                   |
| CSCsz26471       | CRL request failure for Local CA server after exporting and importing    |
| CSCsz29041       | ASA: If CA cert import fails will delete id cert under same trustpoint   |
| CSCsz32125       | Remove ability to add WebVPN group-alias with non-English chars via CLI  |
| CSCsz32354       | Traceback in thread SSH related to using help in policy-map config mode  |
| CSCsz33854       | Report the following error immediately "Your certificate is invalid"     |
| 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  |
| CSCsz34300       | acl-netmask-convert auto-detect cannot convert wildcard mask of 0.0.0.0  |
| CSCsz34811       | Session MIB to mirror sh vpn-sessiondb summary doesn't show proper info  |
| CSCsz35484       | Failover pair with CSC-SSM: High CPU usage by SSM Accounting Thread      |
| CSCsz36816       | OCSF connection failures leaks tcp socket causing sockets to fail        |
| CSCsz37495       | Customization editor: wrong URL of Save icon (text link is OK)           |
| CSCsz38884       | ASA SSLVPN: Error contacting hosts when auto-signon configured           |
| CSCsz39438       | Floating toolbar missing for ARWeb (Remedy) via clientless WebVPN        |
| CSCsz40743       | Resetting the AIP module may cause the ASA to reload with a traceback    |
| CSCsz42003       | ASA 5510 traceback with skinny inspection and phone proxy                |
| CSCsz43374       | AC re-directed to IP address instead of hostname causes cert error       |
| CSCsz43608       | Anyconnect fails to launch if interface ip address is mapped to a name   |
| CSCsz43748       | Port Forwarding creates memory leak                                      |
| CSCsz44078       | Traceback in capture when adding a dataplane match command               |
| CSCsz48558       | PIX/ASA: L2L RRI routes removed after failover when using originate-only |
| CSCsz48653       | WARNING: The vlan id entered is not currently configured under any int   |
| 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                        |
| CSCsz54501       | ASA 5580 traceback in failover with DATAPATH-3-555 thread                |
| CSCsz55620       | WebVPN: Specific RSS feed give blank page                                |
| CSCsz58391       | Burst Traffic causes underrun when QoS shaping is enabled on ASA         |
| CSCsz58862       | Crash when accessing non-allocated memory for default domainname.        |
| CSCsz59196       | Webvpn ACL that permits on tcp with no range does not work using DAP     |
| CSCsz59368       | AAA: Ability to hide Radius key and password in configuration            |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsz61074       | ASA should reject unuseable ip pool config                               |
| CSCsz62364       | ASA5580 snmpget will not provide output for certain OIDs                 |
| CSCsz62566       | ASA 8.0(4) traceback in Dispatch Unit due to stack corruption            |
| CSCsz63008       | Memory leak in 72 / 80 bytes memory blocks [ tmatch]                     |
| CSCsz63217       | Stateful Failover loses 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       | Incorrectly 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        |
| 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     |
| 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                  |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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                          |
| CSCta02877       | Traceback in unicorn thread (outway_buffer_i)                            |
| 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              |
| 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    |
| 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                     |
| CSCta23995       | The logic for tunnel group list to anyconnect is incorrect               |
| CSCta24704       | Syslog id 302014 shows TCP Reset-O for RESET generated by ASA            |
| 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                         |
| CSCta28493       | Traceback in fover_parse on secondary FO unit                            |
| CSCta28795       | WebVPN: SAP Adobe Acrobat form does not send POST                        |
| CSCta31285       | ASA assigns user to DfltGrpPolicy when cancelling change password option |
| CSCta32954       | Traceback in Thread Name: aaa                                            |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCta33092       | "show service-policy" output for policing shows wrong "actions: drop"    |
| CSCta33419       | ASA VPN dropping self-sourced ICMP packets (PMTUD)                       |
| CSCta35443       | Traceback with block allocation failure                                  |
| CSCta36043       | POST plugin uses Port 80 by default even when cisco_proto=https          |
| CSCta38452       | ICMP unreachable dropped with unique Nat configuration                   |
| CSCta38552       | Smart tunnel bookmark failed with firefox browser                        |
| CSCta39633       | Strip-realm is not working with L2TP-IPSEC connection type               |
| CSCta39767       | Service reset inbound 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 "cisco_sso=1" doesn't work in browser favorites |
| CSCta47685       | WebVPN: Plugin parameter "cisco_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           |
| 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 |



**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCta94184       | Cannot open DfltCustomization profile after downgrade from 8.2(1) to 8.0 |
| CSCta95693       | Traceback eip 0x093478ab <_udivdi3+363 at /tmp/vmurphy                   |
| 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"            |
| CSCtb17123       | Policy NAT ignored if source port used in access-list                    |
| CSCtb17498       | ASA traceback in 'Thread Name: ssh' when working with captures           |
| CSCtb17539       | Secondary language characters displayed on Web Portal                    |
| CSCtb18378       | WebVPN: RDP plug-in 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 |
| CSCtb23281       | ASA: SIP inspect not opening pinhole for contact header of SIP 183 msg   |
| CSCtb25740       | Trustpoint certificate will not be updated after re-enrollment           |
| CSCtb27147       | ASA traceback in Thread Name: snmp                                       |
| 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 |
| CSCtb35842       | traceback eip:lavg_dp_work+1 at slib/loadavg.c:241 with vpn & failover   |
| CSCtb36994       | tcp-intercept doesn't start 3WH to inside                                |
| CSCtb37219       | Traceback in Dispatch Unit AIP-SSM Inline and nailed option on static    |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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                          |
| 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  |
| CSCtb53377       | WebVPN: Rewrite issues with Spartan Stores application/portal            |
| CSCtb56128       | CIFS 'file-browsing disable' blocks access to share if '/' at end of url |
| CSCtb57172       | LDAP CRL Download Fails due to empty attribute                           |
| CSCtb58989       | ASDM fails to load due to out of DMA memory when logging is configured   |
| 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           |
| CSCtb64885       | webvpn-cifs: Not able to browsing CIFS shared on server 2008             |
| CSCtb64913       | WEBVPN: page fault in thread name dispatch 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                        |
| CSCtb83645       | Hang may occur with webvpn certificate authentication                    |
| 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                |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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                                   |
| CSCtc02642       | QOS policy-map with match tunnel-group is not applied after reload       |
| CSCtc03206       | asdm fails to launch through smart tunnels                               |
| 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 |
| CSCtc15442       | IXGBE: interface rx queue low count at 0                                 |
| CSCtc16148       | SLA monitor fails to fail back when ip verify reverse is applied         |
| CSCtc18516       | Dynamic NAT Idle Timeout not Reset on Connection Activity                |
| CSCtc20079       | child flows created via established cmd torn down when parent is removed |
| CSCtc22965       | FIPS ASA will not pass FIPS POST in 8.2                                  |
| CSCtc23007       | Sip inspection drops 200 OK packet with early RTP/RTCP                   |
| CSCtc25115       | RDP SSO doesn't send pass                                                |
| CSCtc25147       | Anyconnect certificate validation fails with tunnel-group w/aaa auth     |
| CSCtc27448       | ASA failovers when Management interface resets                           |
| CSCtc29220       | On boot, TACACS server is marked FAILED if defined by DNS name           |
| CSCtc30025       | PP: Incorrect Entry Installed in ASP Table for proxy-server command      |
| CSCtc30413       | Traceback with SIP pinhole replication Thread Name: Dispatch Unit        |
| CSCtc32826       | ASA 8.0.4 Smarttunnel Relay.dll crashes browser if proxy is configured   |
| CSCtc34281       | High CPU due to multiple applications listening on a share port          |
| CSCtc34355       | 4GE interfaces with OSPF is broken starting from 100.5.0.37              |
| 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               |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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          |
| CSCtc81874       | Traceback: CTM message handler - L2TP and crypto reset - stack overflow  |
| 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                  |
| CSCtc90935       | WebVPN Configuration: ASA 5505 crash during config restoration from ASDM |
| 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                                        |
| CSCtd02193       | Heap memory head magic verification failed on asdm access                |
| CSCtd03464       | show vpn-sessiondb remote command outputs wrong Group Policy             |
| CSCtd13971       | Page fault: Address not mapped crash in system test                      |
| 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   |
| CSCtd26388       | Traceback in IKE daemon                                                  |
| 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                           |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtd28887       | ASA: Webvpn CIFs does not refresh updated files                          |
| CSCtd29154       | Traceback when CSR is generated                                          |
| CSCtd29482       | Traceback with Logging flash-bufferwrap configured and heavy logging     |
| CSCtd30953       | LDAP CRL Download Fails due to empty attribute pki-cro                   |
| CSCtd31831       | ASA traceback in Thread Name: Checkheaps                                 |
| CSCtd34024       | ASA not getting IPv6 ND solicitation on subinterfaces                    |
| CSCtd34106       | pim spt infinity can cause dp-cp queue overload and affect eigrp, pim, . |
| CSCtd34592       | changing from SRFW to MRFW with max vlan config results in boot-loop     |
| CSCtd35450       | Excessive memory allocation for large routing tables                     |
| 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               |
| CSCtd40491       | Add new syslog for vpn-filters - Missing post 8.0.                       |
| 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       |
| CSCtd54252       | traceback in checkheaps during backup of asa with smartcare appliance    |
| CSCtd55032       | ASA running 8.0.4.32 traceback in Thread Name: Dispatch Unit             |
| CSCtd55121       | 4GE-SSM will not transmit all fragments                                  |
| CSCtd55346       | Remove uninformative Peer Tbl remove messages                            |
| CSCtd56249       | CTA does not respond for EAP from ASA 8.0.5 with NAC                     |
| CSCtd60720       | Error event causes Syslog 199011 "Close on bad channel in process/fiber" |
| CSCtd61244       | isakmp policy fails to load when isakmp is enabled on multiple interface |
| CSCtd67406       | WebVPN: JS rewriter error when processing IN statement                   |
| CSCtd71913       | WebVPN Application Access page not displayed if AES chosen               |
| CSCtd74691       | VPN session not replicate to Standby after Failover State Link failure   |
| CSCtd79084       | checkheaps causes nested traceback                                       |
| CSCtd81305       | WebVPN: Plugin SSO not working with special characters in username or pw |
| CSCtd86141       | Page Fault :fiber_cancel+15 at unicorn/ak47/fibers/fibers.c:1153         |
| 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    |
| CSCtd93962       | NAT with ACL statements causing long time to reboot.                     |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtd94385       | ASA: Unable to pass traffic through an Airlink router w DTLS enabled     |
| CSCte00896       | Beta Box Assertion in udpmod_user_put                                    |
| CSCte01345       | Error while trying to load rewritten webpage of CarnegieMellon Univ Libr |
| CSCte03164       | eip 0x08a7464d <polycmap_attach_action+573 at qos/polycmap.c:1399>       |
| 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     |
| CSCte14901       | Prepending a space bypasses SMTP inspection                              |
| CSCte15462       | Disable URL entry should only disable http/https                         |
| CSCte15729       | 5580 traceback at CP process while running 600 calls on 2 trunks         |
| CSCte18319       | ASA 8.0.5 snmp-server re-configuration can cause socket used messages    |
| 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                       |
| CSCte29198       | mcast pkts can interfere w/ other punts on the DP-to-CP queue            |
| 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   |
| CSCte43903       | ASA5580 traceback in thread DATAPATH-2-476, eip rt_timer_cancel_callback |
| CSCte45632       | Standby ASA shows ready when its has no communication to active ASA      |
| CSCte46074       | assertion "*cntp != 0" failed: file "mp-datastruct/mp_mutex_rw_lock.h"   |
| CSCte46239       | Cookie being set improperly due to webvpn misreading firefox flags       |
| CSCte51194       | IPv6: Multiple equal cost routes not working                             |
| CSCte55194       | "possible channel leak" when loading with large configuration            |
| CSCte55199       | WebVPN Smart Tunnel failing for ProPalms Application                     |
| CSCte55474       | https/ssh connections to the ASA produce fiber scheduler error syslog    |
| CSCte55571       | ASA names the destination file "scp_fX" if not specified during SCP      |
| 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          |
| CSCte58507       | AC Essentials not enabled w/ active ssl session should provide msg       |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCte62729       | ASA5580 traceback in Thread Name: fover_FSM_thread                       |
| CSCte64811       | ASA 8.04 - certificate chain not being sent during rekey w/ IPSEC RA     |
| 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. |
| CSCte69935       | Beta Box assertion: snp_tcp_timeout_cb+0 at np/soft-np/snp_tcp_norm.c:82 |
| 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   |
| CSCte80027       | ASA 8.0(5) - "LU allocate connection failed"                             |
| CSCte80609       | Actions attached to class class-default don't apply to traffic           |
| CSCte81368       | Sip inspection fails to nat embedded media port                          |
| CSCte85803       | After failover, skinny message are decoded as SCCPv0 instead of SCCPv17  |
| CSCte87293       | ISAKMP SA stuck in AM_FREE state                                         |
| CSCte91045       | Dhcpd incorrectly sends DHCPNAK                                          |
| CSCte92557       | ASA HW client: deny rule for DHCP should account for remote subnets      |
| CSCte94184       | FO: "service resetoutside" exists only in standby unit after failover    |
| CSCte98818       | LDAP authentication stops operating to Win2008 srvr after sometime       |
| CSCtf02322       | ASA - Memory depleting 1% per day due to snmp-server ipsec configuration |
| CSCtf02712       | Traceback in Dispatch Unit (Old pc 0x08180444 ebp 0xc793d980)            |
| CSCtf06292       | ASA doesn't handle chunk encoding correctly                              |
| CSCtf09477       | port openssl patch                                                       |
| CSCtf11646       | WebVPN: RDP is crashing through Smart Tunnels on Mac                     |
| CSCtf13556       | Slow memory leak in WebVPN related to CIFS cache                         |
| CSCtf13801       | ASA PPTP inspection not overwriting Call ID in Call-Clear-Request        |
| CSCtf22332       | Thread Name: netfs_thread_init                                           |
| CSCtf23469       | ASA 8.0.5+ webvpn FTP bookmarks no longer will pass embedded user/pass   |
| CSCtf24681       | SNAP frames are sent from Management interface in Transparent mode ASA   |
| CSCtf25180       | ASA: Discrepancy seen between SNMP MIB and sh vpn-sessiondb output       |
| CSCtf25808       | ICMP error messages dropped in multi-context asymmetric routing mode     |
| CSCtf28464       | Memory Leak In CIFS can casue memory depletion                           |
| CSCtf28466       | ASA Fails to assign available addresses from local pool                  |
| CSCtf28467       | Copy to disk0 without ":", prefills dest as disk0, cant delete/view file |
| CSCtf29867       | Memory leak happens due to huge number of LDAP authentication failure    |
| CSCtf30557       | show failover command authorization not available                        |
| CSCtf31220       | Reload command "hangs" on ASA                                            |
| CSCtf33469       | ASA 8.0.5 1550 block depletion with ASDM open                            |
| CSCtf39296       | Webvpn with challenge/response: password field should have focus         |

**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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          |
| 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                                 |
| 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                        |
| CSCtf50185       | when doing DTLS rekey, AC may get disconnected with reason idle-timeout  |
| CSCtf52703       | ASA/w 4-GE-SSM shows module status unresponsive after power surge        |
| CSCtf52903       | Wrong url message is generated when access to group-url ended with "/"   |
| 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           |
| CSCtf56913       | ASA crash on thread name snmp, eip getstats on redundant interface       |
| 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                             |
| CSCtf67122       | Traceback when trying to print syslog 444110 in Thread Name: ms-client   |
| CSCtf68934       | Standby Unit not getting session replicated, rerr TCP and UDP increasing |
| CSCtf69301       | Copy /pcap capture fails when packet larger than 2k                      |
| CSCtf73359       | ASA uses different source IP for data traffic of passive FTP connection  |
| CSCtf81534       | Received unexpected event EV_TERMINATE in state MM_SND_MSG6_H            |
| CSCtf85135       | Add nano sleep to cp process suspend handling                            |
| CSCtf91831       | call-home send CMD email - may fail with Lone CR or LF in headers        |
| CSCtf96635       | Removing HTTP server caused page fault traceback                         |
| CSCtf99907       | mcast: fix smp locking issues                                            |
| CSCtg11699       | ASA high CPU in DHCP Proxy thread                                        |
| CSCtg13981       | ASA doesn't set correct MIME type for CSS files                          |
| CSCtg14750       | Dynamic-filter syslogs 338004 and 338008 show '0' for src and dest ports |
| CSCtg17779       | Flows torndown over VPN tunnel log 302014 with Flow closed by inspection |
| CSCtg18674       | RSA Crossrealm Authentication fails to authenticate for vpn users        |
| CSCtg20177       | Clientless WebVPN not working with SAP Release 3 adobe forms             |



**Table 9**      **Resolved Caveats in Version 8.2(3) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                      |
|------------------|-------------------------------------------------------------------------|
| CSCtg21370       | %ASA-5-711005 generated when a L2TP client connects                     |
| 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                  |
| CSCtg36637       | HEAD requests blocked from a web folder handler processing              |
| CSCtg39859       | ASA MAC Smart tunnel file upload fails after about 200 KB               |
| CSCtg41163       | ASA:high memory usage seen on ASA version 8.0.x onwards                 |
| CSCtg45489       | Access List for L2L "show crypt ipsec sa" blank after FO and rekey      |
| CSCtg45916       | Don't do DAP re-validation at svc re-key and new tunnel generation      |
| CSCtg46175       | Xlate Idle Timer Incorrectly Refreshed by Dropped Packets               |
| CSCtg48603       | ASA traceback in Thread Name: Dispatch Unit                             |
| CSCtg51135       | external appl unable to make connection via proxy server-smart tunnel   |
| CSCtg63818       | Memory leak when using certs for SSL AAA                                |
| CSCtg65421       | CIFS SSO fails with non-ASCII characters in username or password        |
| CSCtg67798       | DAP errors when certain special strings present in the ldap value field |
| CSCtg68689       | Can't add policy static PAT bk if it was deleted by "clear conf static" |
| CSCtg74608       | WEBVPN: PDF form button doesn't work with secure link                   |
| CSCtg79235       | OCSP: Need allow some slop on time check for OCSP response              |
| CSCtg81514       | Webvpn with Citrix - Xenapp upgrade from 11.2 to 12.0 breaks app access |
| CSCtg84635       | PP: signaling sessions are not removed after phone disconnects          |
| CSCtg90646       | ASA - webtype ACLs are not replicated to the standby                    |
| CSCtg96403       | ICMP traceroute does not work even after the CSCtf25808 fix             |
| CSCtg97145       | Interface overruns upon IPSEC rekey with PFS and DH5                    |
| CSCth03659       | clear conf all with syslog without any traffic causes a crash.          |
| CSCth05572       | asa page fault traceback in thread name: netfs_thread_init              |
| CSCth09682       | ASA5580-40: Unable to remove SNMP entry from context config             |
| CSCth11779       | ASA sends invalid XML when group-alias contains &                       |
| 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                              |
| CSCth25402       | Implement MSIE proxy lockdown knob on the ASA                           |
| CSCth26439       | Traceback panic spin_lock_fair_mode_enqueue: Lock (ctm_ipsec_sa_lock_t) |
| CSCth26462       | WebVPN proxy-bypass with 'rewrite link' does not rewrite HTTPS links    |
| CSCth38713       | Jumbo frame configuration: Requires warning message                     |
| CSCth38721       | Timer error on console not useful: init with uninitialized master       |

**Table 9** *Resolved Caveats in Version 8.2(3) (continued)*

| Caveat ID  | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCth42526 | ASA:vpn-sessiondb logoff ipaddress <peer> does not clear tunnelled flows |
| CSCth42839 | show conn port functionality change                                      |
| CSCth43128 | ASA WebVPN : Forms don't get saved in CRM due to no pop-up               |
| CSCth46161 | Transparent mode ASA does not pass IPv6 Router Advertisement packet      |
| CSCth56065 | DAP_ERROR:...dap_add_csd_data_to_lua: Unable to load Host Scan data:     |
| CSCth67419 | WebVPN - rewriter interprets "application/pdf" as generic link           |
| CSCth68948 | Memory not released after EZVPN client with cert fails authentication    |
| CSCth80945 | ASA 8.3.1: Traceback with snp_fp_punt_block_free_cleanup                 |

## Resolved Caveats in Version 8.2(2)

The caveats listed in [Table 10](#) were resolved in software Version 8.2(2). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

<http://www.cisco.com/support/bugtools>

**Table 10** *Resolved Caveats in Version 8.2(2)*

| Caveat ID  | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCsi27903 | L2TP & NAC -> Default NAC policy prevents data from passing              |
| 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    |
| CSCsl04124 | SIP does not support 'early RTCP'                                        |
| CSCsm39914 | match resp body length for http class-map doesnt take correct value      |
| CSCsm40830 | traceback netfs_thread_init                                              |
| CSCso80611 | context using SSM app in promiscuous mode shows incorrect memory usage   |
| CSCsq34317 | Without authproxy currently configured, authproxy DACLs may become stale |
| CSCsq34336 | ASA: rate-limiting for encrypted s2s traffic not consistently handled    |
| CSCsu27257 | "show asp table classify" doesn't show WCCP domain                       |
| CSCsu48860 | traceback eip 0x08c4cab2 log_to_servers+1426 at /slib/include/channel.h  |
| CSCsu56483 | Extend show ak47 to display per pool and per block information           |
| CSCsv36948 | CIFS access to Win2008 server via IP address is not working.             |
| CSCsv40504 | Telnet connection permitted to lowest security level interface           |
| CSCsv43552 | Radius accounting request fails on ASA if we have many radius attributes |
| CSCsv52169 | Traceback at thread name PIX Garbage Collector                           |
| CSCsv73764 | Unable to Browse to Domain Based DFS Namespaces                          |
| CSCsv86200 | ASA 8.0.4.7 Traceback in Thread Name: tmatch compile thread              |
| CSCsv89645 | ASA 8.04 - certificate chain not being sent when configured w/ IPSEC RA  |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsv91391       | L2TP with EAP auth stuck [%ASA-4-403102 - authentication pending]        |
| CSCsv91564       | Multiple certificates are installed to one trustpoint when importing.    |
| CSCsv96545       | ASA is dropping arp on SSM-4GE                                           |
| CSCsw19588       | Standby console freezes if user logs in prior to detecting mate          |
| CSCsw25253       | ssl vpn related memory corruption causes traceback                       |
| CSCsw37504       | ISAKMP delayed when processing large CRL files                           |
| CSCsw41161       | PMTUD - ICMP type 3 code 4 generated for GRE flow is dropped 313005      |
| CSCsw47441       | Java Applet Signing Error..plugins still use old expired certificate     |
| CSCsw51809       | sqlnet traffic causes traceback with inspection configured               |
| CSCsw70786       | SACK is dropped when TCP inspection engines are used                     |
| CSCsw76595       | PP: phone cannot register when configured as Authenticated on UCM        |
| CSCsw77033       | SSL VPN: Java-rewriter: memory leak implicating WebVPN                   |
| CSCsw91072       | Identity cert being imported without errors, if conflicting with CA cert |
| CSCsx03294       | 1550 block leaks leading active ASA to reload                            |
| CSCsx07862       | Traffic shaping with priority queueing causes packet delay and drops     |
| CSCsx15055       | set nat-t-disable in crypto map does not override global nat-t config    |
| CSCsx19947       | IGMP Join fails on subinterface after upgrade to 8.1(2)                  |
| CSCsx20038       | Wrong counters in "show int" for Redundant interface                     |
| CSCsx23611       | VPN: TCP traffic allowed on any port with management-access enabled.     |
| CSCsx25628       | %PIX ASA-3-713128 should be logged as a lower level message              |
| CSCsx27609       | 5580 traceback implicating snp_nat_find_portlist w/ stress test          |
| CSCsx27851       | Entering interface ? from cmd specific config mode returns to global cfg |
| CSCsx41170       | uauth inactivity timer not taking effect                                 |
| CSCsx49794       | WebVPN: RDP Plugin does not work with ActiveX with large cert chain      |
| CSCsx50318       | OCSP revocation stops working after some time on Cisco ASA               |
| CSCsx50721       | Anyconnect unable to establish DTLS tunnel if ASA IP address change      |
| CSCsx52598       | No focus on 'More information required' radius challenge/response page   |
| CSCsx54449       | ASA may process LDAP password policy with no password-management         |
| CSCsx54893       | CSD: Unable to run smart-tunnel inside "browser only" vault              |
| CSCsx57142       | SIP Inspection Doesn't NAT Call-info field in SIP Notify message         |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsx58682       | ASA Local CA and caSe SenSiTiviTy - p12 file vs. username conflict       |
| CSCsx59014       | ASA allows VPN user although Zonelabs Integrity firewall rejects         |
| CSCsx59403       | Automatically added AAA command break ASA5505EasyVPN client after reboot |
| CSCsx59746       | Tacacs Command Accounting does not send packet for 'nat-control'         |
| CSCsx65702       | ASA traceback upon failover with interface monitor enabled               |
| CSCsx65945       | High memory usage in chunk_create                                        |
| CSCsx68765       | VMWARE web applications (view/vdm) do not work with smart-tunnel         |
| CSCsx73547       | Stateful Conns Disappear From Standby During Failover                    |
| CSCsx76473       | CSD: Group-url fails in Vault.                                           |
| CSCsx79918       | Crypto CA limited to 65536 requests                                      |
| CSCsx81472       | ASA might automatically restart after issuing 'show vpdn'                |
| CSCsx83353       | WCCP Service Ports Missing in ASP Table when Adding Redirect ACL Entry   |
| CSCsx94330       | AC with CSD and DAP for Posture Assessment matches wrong DAP Policy      |
| CSCsx94849       | Unpredictable behavior after failover w/shortest timeout conf.           |
| CSCsx95377       | Adding host to http access results in Could not start Admin error        |
| CSCsx95461       | ifHighSpeed and ifSpeed values are zero for 10G operational interfaces   |
| CSCsx95785       | ifType values returns as other (1) for 10G interfaces                    |
| CSCsx97569       | PIX/ASA traceback with Thread Name: CMGR Server Process                  |
| CSCsx99960       | ASA5580-20 traceback in CP Processing                                    |
| CSCsy03579       | Standby ASA traceback after becoming active, EIP snp_fp_inspect_dns+42   |
| CSCsy04974       | Syslog 113019 Disconnect reason not working                              |
| CSCsy07794       | Webvpn error recovery events caused by improper error handling           |
| CSCsy08778       | no pim on one subif disables eigrp on same physical of 4 ge module       |
| CSCsy08905       | process_create corrupt ListQ memory when MAX_THREAD is exceeded          |
| CSCsy10473       | ASA Improve RADIUS accounting disconnect codes for vpn client            |
| CSCsy13488       | DDNS: A RR update fails if cache entry exists in show dns-host           |
| CSCsy14672       | ASA might automatically restart in Thread Name: ppp_timer_thread         |
| CSCsy16595       | The ASA traceback intermittent in IPSec                                  |
| CSCsy17783       | Large CRLs freeze processing on the ASA for extended time periods        |
| CSCsy20002       | File upload causes hang without recovery                                 |
| CSCsy21333       | Traceback in Thread Name: aaa when using Anyconnect with certificate     |
| CSCsy21727       | Failover pair is not able to sync config and stuck in Sync Config state  |
| CSCsy23275       | Smart Tunnels and POST parameters should be interoperable                |
| CSCsy25908       | ASA 8.2 Beta does not work with /31 subnet on failover interface config  |
| CSCsy26775       | Traceback while refreshing CRL                                           |
| CSCsy27395       | qos: traceback in thread name: ssh, eip mqc_get_blt_def                  |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsy27547       | Using phone-proxy got assertion "ip.ip_version == IP_VERSION_4"          |
| CSCsy28792       | ESMTP inspection drops DKIM signed emails with content-type              |
| CSCsy28853       | inspect-mgcp: call-agent name and gateway name disappears after a reboot |
| CSCsy29949       | WebVPN: slow response with CGI scripts                                   |
| CSCsy30717       | Keepalive not processed correctly thru TCP Proxy                         |
| CSCsy31955       | Incorrect severity for ASA syslog message 106102                         |
| CSCsy32767       | WebVPN OWA 2007 + AttachView Freezes IE6 and will not close              |
| CSCsy44823       | WebVPN: Smart Tunneled bookmark on Mac with Safari fails with ACL        |
| CSCsy47819       | Traceback occurs when 5505 HwClient connects - password-management used  |
| CSCsy47993       | Names not supported in EIGRP summary-address command                     |
| CSCsy48107       | "clear crypto ipsec sa entry" command doesn't seem to work               |
| CSCsy48250       | "clear crypto ipsec sa entry" command doesn't work                       |
| CSCsy48626       | Traceback due to illegal address access in Thread Name: DATAPATH-0-466   |
| CSCsy48816       | webvpn cifs url doesn't work                                             |
| CSCsy49841       | ASA Traceback in Thread fover_FSM_thread with A/A FO testing             |
| CSCsy50018       | Lua recovery errors observed during boot in multiple-context mode        |
| CSCsy50113       | traceback in Dispatch Unit: Page fault: Address not mapped               |
| CSCsy50428       | page fault while adding/enrolling users to Local CA w/script             |
| CSCsy53263       | Tacacs connection match accounting does not display port information     |
| CSCsy53387       | "crypto map does not hole match" message pops up during condition debug  |
| CSCsy55762       | Memory leak in 72 / 80 / 192 bytes memory blocks [tmatch]                |
| CSCsy56570       | Redundant interface as failover link lose peer route after reload        |
| CSCsy56739       | Traceback on standby while processing write memory if context is removed |
| CSCsy57590       | AC asks for Username/Password after certs fail with group-url cert only  |
| CSCsy57872       | Unable to SSH over remote access VPN (telnet, asdm working)              |
| CSCsy58218       | WebVPN: hide internal password in customization doesn't work             |
| CSCsy59225       | FW sends rst ack for tcp packet with L2 multicast mac not destined to it |
| CSCsy60403       | SSL rekey fails for AnyConnect when using client-cert authentication     |
| CSCsy64028       | WebVPN: NTLM authentication does not work on a cu server                 |
| CSCsy65734       | ASA: traceback with thread name "email client"                           |
| CSCsy68961       | ASA 5580 reboots with traceback in threat detection                      |
| CSCsy71401       | Traceback when editing object-group                                      |
| CSCsy72423       | WebVPN: ASA sends a bad If-Modified-Since header                         |
| CSCsy75345       | subinterfaces on 4ge-ssm ports fail with mac-address auto and failover   |
| CSCsy75684       | Traceback from thread DATAPATH-0-483 on failover                         |
| CSCsy75720       | asdm does not connect to secondary on failover                           |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsy75800       | Shared int Mac add auto reload primary there will be some packet loss    |
| CSCsy76163       | Not able utilize search engine via webvpn                                |
| CSCsy77628       | the procedure of copying a file from ramfs to flash should be atomic     |
| CSCsy78105       | CPOC: Watchdog Traceback in snp_flow_free / snp_conn_release             |
| CSCsy80242       | ASA: LDAP Password-expiry with Group-Lock locks users out                |
| CSCsy80694       | ASA's DOM wrapper issue- Clientless XSS                                  |
| CSCsy80705       | ASA WebVPN HTTP server issue-XSS                                         |
| CSCsy80709       | WebVPN FTP and CIFS issue                                                |
| CSCsy80716       | WebVPN: full customization disables dap message                          |
| CSCsy81475       | Traceback due to assert in Thread Name: DATAPATH-0-466                   |
| CSCsy82093       | XSS via Host: header in WebVPN Request.                                  |
| CSCsy82188       | WebVPN: ASA can't support IP/mask based NTLM SSO consistently            |
| CSCsy82260       | ASA fails to redirect traffic to WCCP cache server                       |
| CSCsy83043       | Redundant interface is down if any member is down at boot                |
| CSCsy83106       | Unable to add member interface to Redundant Interface                    |
| CSCsy84268       | AIP-SSM stays in Unresponsive state after momentary voltage drop         |
| CSCsy85759       | Remove "Server:" directive from SSL replies when CSD enabled             |
| CSCsy86769       | ASA5505 should not allow pkts to go thru prior to loading config         |
| CSCsy86795       | ASA - Log messages for all subinterfaces seen when adding just one vlan  |
| CSCsy87867       | ASA inspect pptp does not alter Call ID in inbound Set-Link-info packets |
| CSCsy88084       | Smart Tunnel failing on MAC 10.5.6 with Firefox 2 and Safari             |
| CSCsy88174       | ESMTP inspection "match MIME filetype" matches on file content as well   |
| CSCsy88238       | Memory leak in Webvpn related to CIFS                                    |
| CSCsy90150       | ASA doesn't properly handle large SubjectAltName field - UPN parse fails |
| CSCsy91142       | Using name aliases for the interface will cause vpn lb to break          |
| CSCsy92661       | Traceback in Thread Name: Dispatch Unit (Old pc 0x081727e4 ebp 0xaad3cd1 |
| CSCsy94410       | asa in tfw mode reboots on ping to ipv6 addr with no ipv6 addr on box    |
| CSCsy96753       | WebVPN Flash rewriter may not clean up all temporary files               |
| CSCsy97437       | SNMP community string not hidden in 'show startup' or 'show conf'        |
| CSCsy98446       | Memory leaked when matching tunnel group based on URL                    |
| CSCsy98584       | Traceback on Thread Name: AAA due to downloadable ACL processing         |
| CSCsy98662       | Access-list allows port ranges with start-port greater than end-port     |
| CSCsy99063       | traceback Thread Name: fover_tx after multiple SSH to active unit        |
| CSCsz01314       | Traceback in ci/console after sh crypto ipsec sa                         |
| CSCsz02807       | Logging standby can create logging loop with syslogs 418001 and 106016   |
| CSCsz02849       | Long delay before standby becomes active if unit holdtime misconfigured  |

**Table 10** *Resolved Caveats in Version 8.2(2) (continued)*

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsz06329       | Unexpect Syslog: No SPI to identify Phase 2 SA                           |
| CSCsz06748       | ASA traceback in inspect Skinny                                          |
| CSCsz10339       | console hangs for extended period of time when config-url is applied     |
| CSCsz10924       | Management port in promiscuous mode processes packets not destined to it |
| CSCsz11180       | TCP Proxy mis-calculates TCP window causing connectivity problems        |
| CSCsz11835       | ASA intermittently drops traffic for authenticated users w/auth-proxy    |
| CSCsz17027       | L2TP: DACL w/ Wildcard Mask not applied to L2TP over IPsec Clients       |
| CSCsz18759       | Certificate mapping does not override the group chosen by URL            |
| CSCsz19296       | IPSEC NAT-T - block may get dropped due to VPN handle mismatch           |
| CSCsz20830       | webpage showing missing content.                                         |
| CSCsz22256       | ASA disconnects IPsec VPN client at P2 rekey with vlan mapping in grppol |
| CSCsz24401       | Stuck EIGRP ASP entry prevents neighbor from coming up                   |
| CSCsz24748       | Assert violation in TCP channel during tcp_open_connect                  |
| CSCsz24793       | no credentials for AnyConnect:cert validation error for TG with AAA only |
| CSCsz26471       | CRL request failure for Local CA server after exporting and importing    |
| CSCsz29041       | ASA: If CA cert import fails will delete id cert under same trustpoint   |
| CSCsz32125       | Remove ability to add WebVPN group-alias with non-English chars via CLI  |
| CSCsz32354       | Traceback in thread SSH related to using help in policy-map config mode  |
| CSCsz33131       | ASA 5580-40: significant performance drop in CPS and PPS in TFW mode     |
| CSCsz33877       | traceback in schedctl_start - clientless/FO/LOCAL aaa                    |
| CSCsz34273       | PIX/ASA don't generate syslog 305005 on nat-rpf-failed counter increase  |
| CSCsz34300       | acl-netmask-convert auto-detect cannot convert wildcard mask of 0.0.0.0  |
| CSCsz34811       | Session MIB to mirror sh vpn-sessiondb summary doesn't show proper info  |
| CSCsz35484       | Failover pair with CSC-SSM: High CPU usage by SSM Accounting Thread      |
| CSCsz36816       | OCSF connection failures leaks tcp socket causing sockets to fail        |
| CSCsz37164       | "vpn-simultaneous-logins 0" does not prevent user access in all cases    |
| CSCsz37492       | traceback eip 0x09307337 <mem_get_owner+55 at slib/malloc.c:5785>        |
| CSCsz37495       | Customization editor: wrong URL of Save icon (text link is OK)           |
| CSCsz38884       | ASA SSLVPN: Error contacting hosts when auto-signon configured           |
| CSCsz39438       | Floating toolbar missing for ARWeb (Remedy) via clientless WebVPN        |
| CSCsz40743       | Reseting the AIP module may cause the ASA to reload with a traceback     |
| CSCsz42003       | ASA 5510 traceback with skinny inspection and phone proxy                |
| CSCsz43374       | AC re-directed to IP address instead of hostname causes cert error       |
| CSCsz43608       | Anyconnect fails to launch if interface ip address is mapped to a name   |
| CSCsz43748       | Port Forwarding creates memory leak                                      |
| CSCsz44078       | Traceback in capture when adding a dataplane match command               |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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                        |
| CSCsz54501       | ASA 5580 traceback in failover with DATAPATH-3-555 thread                |
| 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 loses 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        |
| CSCsz70401       | ldap-attrib-map for Group set fails to include Class in Radius Accting   |
| 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                               |
| 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       |
| CSCsz78701       | dhcprelay issue after configuration changes in multi context mode        |
| 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     |
| CSCsz85299       | Syslogs are incorrectly logged at level 0 - emergencies                  |



**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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                     |
| CSCta08559       | Clientless Webvpn is not working with SAP adobe/acrobat forms            |
| 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              |
| CSCta15956       | Coredump will be truncated & not completed                               |
| 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    |
| CSCta23184       | Traceback in Datapath-1-480                                              |
| CSCta23935       | Active/Active FO fails when using a shared interface with the same name  |
| CSCta25498       | L2TP still has auth stuck [%ASA-4-403102 - authentication pending]       |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCta26626       | PAT Replication failures on ASA failover                                 |
| CSCta27739       | Standby ASA leaking memory in webvpn environment                         |
| CSCta28795       | WebVPN: SAP Adobe Acrobat form does not send POST                        |
| 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 cisco_proto=https          |
| CSCta38452       | ICMP unreachable dropped with unique Nat configuration                   |
| CSCta38552       | Smart tunnel bookmark failed with firefox browser                        |
| CSCta39633       | Strip-realm is not working with L2TP-IPSEC connection type               |
| CSCta39767       | Service reset inbound 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 "cisco_sso=1" doesn't work in browser favorites |
| CSCta47685       | WebVPN: Plugin parameter "cisco_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                                                |
| CSCta55277       | traceback seen with assertion "0" failed: file "block.c", line 2716      |
| 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           |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCta86483       | Group Alias no longer accepts spaces - Broadview                         |
| CSCta88732       | WebVPN Traceback in Unicorn Proxy while rewriting Java applets           |
| 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                            |
| CSCtb01729       | ASA traceback in Thread Name: tmatch compile thread                      |
| 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"            |
| CSCtb17123       | Policy NAT ignored if source port used in access-list                    |
| CSCtb17539       | Secondary language characters displayed on Web Portal                    |
| CSCtb18378       | WebVPN: RDP plug-in SSO fails when username contains space               |
| 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                 |
| CSCtb37395       | traceback: <netfs_init_ctx+65 at netfs/netfs_api.c:399>                  |
| CSCtb38075       | Phone Proxy Dropping RTP Packets After Prolonged Inactivity from Inside  |
| CSCtb38344       | ASA tracebacks in Thread Name: vPif_stats_cleaner                        |
| CSCtb39300       | IPv6 VPN traffic fails when more than 1 sub interface is configured.     |
| CSCtb42847       | "clear cry isakmp sa <ip>" doesnt work if there's no corresponding P2 SA |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtb42871       | Traceback in Thread Name: PIX Garbage Collector                          |
| 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     |
| CSCtb50486       | failover link restored while replication causes failover off             |
| CSCtb52929       | Show service-policy output needs to be present in show tech              |
| CSCtb52935       | tmatch: Traceback while passing traffic in certain configuration         |
| 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                        |
| CSCtb83645       | Hang may occur with webvpn certificate authentication                    |
| 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                    |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCtc00929       | ASA WebVPN CIFS tries to connect to type GROUP name                      |
| CSCtc01815       | Mem leak in Radius_Coalesce_AVpairs                                      |
| CSCtc01864       | Memory leak in CRL_CheckCertRevocation                                   |
| 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                        |
| CSCtc05405       | Port-Forwarding applet not operational with certain OS/Java versions     |
| CSCtc13966       | tmatch_compile_thread traceback w/ low mem condition due to huge vpn acl |
| CSCtc17075       | Memory leaks found when pushing msie-proxy info to Ipsec client.         |
| CSCtc18516       | Dynamic NAT Idle Timeout not Reset on Connection Activity                |
| CSCtc20079       | child flows created via established cmd torn down when parent is removed |
| CSCtc22965       | FIPS ASA will not pass FIPS POST in 8.2                                  |
| CSCtc23007       | Sip inspection drops 200 OK packet with early RTP/RTCP                   |
| CSCtc25115       | RDP SSO doesn't send pass                                                |
| CSCtc25147       | Anyconnect certificate validation fails with tunnel-group w/aaa auth     |
| 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        |
| CSCtc32826       | ASA 8.0.4 Smarttunnel Relay.dll crashes browser if proxy is configured   |
| 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                    |
| CSCtc43209       | ASA traceback: Thread Name: IKE Daemon                                   |
| CSCtc43396       | Coredump from emweb/https when connecting phone VPN client               |
| CSCtc46138       | Traceback on changing snmp-server port                                   |
| CSCtc46309       | CIFS : Authentication Error with percentage symbol in password           |
| CSCtc48310       | ASA: Traceback during NTLM authentication                                |
| CSCtc52217       | Clientless WebVPN: Errors with DWA 8.5 (Domino Web Access / Notes)       |
| CSCtc52953       | Traceback with panic message: Lock (snp_conn_t) is held for a long time  |
| CSCtc58632       | SSM IPS sends TCP RST to wrong TCP seq number                            |

**Table 10**      **Resolved Caveats in Version 8.2(2) (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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  |
| 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          |
| CSCtc82010       | vpnlb_thread traceback under low mem condition due to huge vpn acl       |
| CSCtc82025       | emweb/https traceback under low memory condition                         |
| CSCtc85647       | snmpwalk on user context does not work                                   |
| CSCtc87596       | High cpu and memory tilization in asa with tls proxy inspection          |
| CSCtc90093       | WebVPN: Firefox users have issues searching with google                  |
| CSCtc93523       | Traceback in Thread Name: SiteMinder SSO Request                         |
| 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                           |
| CSCtd25685       | New active member should send SNAP frames for MAC address table update   |
| CSCtd26388       | Traceback in IKE daemon                                                  |
| 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                           |
| CSCtd29154       | Traceback when CSR is generated                                          |
| CSCtd34106       | pim spt infinity can cause dp-cp queue overload and affect eigrp, pim, . |
| CSCtd35450       | Excessive memory allocation for large routing tables                     |
| CSCtd37269       | Traceback when deleting an rsa key with special characters               |
| CSCtd42963       | threshold checking for average rate not working in threat-detection      |
| CSCtd43980       | traceback while doing ASDM certificate only backup                       |
| CSCtd44244       | Traceback seen at thread: Dynamic Filter VC Housekeeper                  |
| CSCtd52211       | ASA assert "new_flow->conn->conn_set == NULL" failed: file "snp_mcast.c" |
| CSCtd54025       | Connection once entered into discard state and remains in discard state  |
| CSCtd55346       | Remove uninformative Peer Tbl remove messages                            |
| CSCtd86141       | Page Fault :fiber_cancel+15 at unicorn/ak47/fibers/fibers.c:1153         |

# End-User License Agreement

Information about the end-user license agreement is available at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/eu1jen\\_\\_\\_\\_.pdf](http://www.cisco.com/univercd/cc/td/doc/es_inpk/eu1jen____.pdf)

## 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 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

©2010 Cisco Systems, Inc. All rights reserved.

