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

January 2010

This document contains release information for the following Cisco ASA 5500 Versions:

- 8.2(2)
- 8.2(1)

This document includes the following sections:

Important Notes

- When you upgrade to version 8.2(2), the adaptive security appliance might go into a boot loop if you have an incomplete service policy configuration, such as the following:

  ```
  policy-map global_policy
  service-policy global_policy global
  ```

  The **policy-map** configuration requires the **class** command and associated actions; the **class** command in turn references a **class-map** command. The configuration should be similar to the following default configuration:

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

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

Workaround: Configure a **class-map**, and then add the **class** command to the **policy-map**, and then define actions for the class. Or, remove the incomplete **service** and/or **policy-map** commands (CSCte03164).

- For Smart Call Home Version 3.0(1), full support for the adaptive security appliance on the backend server is not yet available. The following features are *not* available, and will only be available in Cisco Smart Call Home Version 3.1 (not yet released):
  a. Web portal reports related to Threat, Telemetry, and Snapshot messages.
  b. Configuration message parsing to generate a feature list on the web portal.
  c. Diagnostic messages that trigger any action, such as to open an SR case.
- 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 3 for downgrade issues after you upgrade the Phone Proxy and MTA instance, or if you upgrade the activation key with new 8.2 features.
- 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 plugin 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 512 MB 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 does not support custom signatures.

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 AIP SSC or SSM Software, page 4
- Upgrading the Phone Proxy and MTA Instance, page 4
- Activation Key Compatibility When Upgrading, page 4

Downloading Software from Cisco.com

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

http://www.cisco.com/cisco/web/download/index.html

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 AIP SSC or SSM Software

When upgrading the AIP SSC or SSM, do not use the **upgrade** command within the IPS software; instead use the **hw-module 1 recover configure** command within the adaptive security appliance software.

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 6
- 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 Memory (MB)	Default Internal Flash Memory (MB)
5505	256	128
5510	256[1]	512
5520	512	512
5540	1024	512
5550	4096	512
5580	4096	1024

[1] For 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** 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 512 MB 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.

Note On both the ASA 5580-20 and the ASA 5580-40 adaptive security appliances only 4 GB of memory is available for features. The rest are reserved or used by the OS. The **show memory** command will only display values relative to 4 GB.

Memory Upgrade Kits

The ASA 5510 DRAM upgrade kit is available from Cisco with the following part number:

- ASA 5510 DRAM, 512 MB—ASA5510-MEM-512=

256 MB and 512 MB CompactFlash upgrades are avilable from Cisco with the following part numbers:

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

For example:

```
hostname # dir
Directory of disk0:/

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

Table 2 ASDM, SSM, SSC, and VPN Compatibility

Application	Description
ASDM	ASA 5500 Version 8.2 requires ASDM Version 6.2 or later. For information about ASDM requirements for other releases, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
SSM and SSC applications	For information about SSM and SSC application requirements, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

This section includes the following topics:

- New Features in Version 8.2(2), page 7
- New Features in Version 8.2(1), page 10

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

New Features in Version 8.2(2)

Table 3 lists the new features for ASA Version 8.2(2).

Table 3 New Features for ASA Version 8.2(2)

Feature	Description
Remote Access Features	
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. *Also available in Version 8.0(5).*
Application Inspection Features	

Table 3 New Features for ASA Version 8.2(2) (continued)

Feature	Description
Inspection for IP Options	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. **Note** This inspection is enabled by default. The following command is added to the default global service policy: **inspect ip-options**. 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. The following commands were introduced: **policy-map type inspect ip-options**, **inspect ip-options**, **eool**, **nop**.
Enabling Call Set up Between H.323 Endpoints	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. 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. The following command was introduced: **ras-rcf-pinholes enable** (under the **policy-map type inspect h323 > parameters** commands). *Also available in Version 8.0(5).*
Unified Communication Features	
Mobility Proxy application no longer requires Unified Communications Proxy license	The Mobility Proxy no longer requires the UC Proxy license.
Interface Features	
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	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. The MAC addresess are also now persistent accross reloads. 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. The following command was modified: **mac-address auto prefix** *prefix.* *Also available in Version 8.0(5).*
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. The following command was introduced: **flowcontrol**.
Firewall Features	

Table 3 New Features for ASA Version 8.2(2) (continued)

Feature	Description
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. The following commands were introduced or modified: **dynamic-filter ambiguous-is-black**, **dynamic-filter drop blacklist**, **show dynamic-filter statistics**, **show dynamic-filter reports infected-hosts**, and **show dynamic-filter reports top**.
Connection timeouts for all protocols	The idle timeout was changed to apply to all protocols, not just TCP. The following command was modified: **set connection timeout**.
Routing Features	
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. The following command was modified: **dhcp-server** [**subnet-selection** | **link-selection**]. *Also available in Version 8.0(5).*
High Availablility Features	
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. The following commands were modified: **failover interface ip**, **ipv6 address**.
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. *Also available in Version 8.0(5).*
AAA Features	
100 AAA Server Groups	You can now configure up to 100 AAA server groups; the previous limit was 15 server groups. The following command was modified: **aaa-server**.

Table 3 New Features for ASA Version 8.2(2) (continued)

Feature	Description
Monitoring Features	
Smart Call Home	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. **Note** Smart Call Home server Version 3.0(1) has limited support for the adaptive security appliance. See the "Important Notes" for more information. The following commands were introduced: **call-home**, **call-home send alert-group**, **call-home test**, **call-home send**, **service call-home**, **show call-home**, **show call-home registered-module status**.

New Features in Version 8.2(1)

Table 4 lists the new features for Version 8.2(1).

Table 4 New Features for ASA Version 8.2(1)

Feature	Description
Remote Access Features	
One Time Password Support for ASDM Authentication	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. 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. The following commands were introduced: **http server idle-timeout** and **http server session-timeout**. The **http server idle-timeout** default is 20 minutes, and can be increased up to a maximum of 1440 minutes.

Table 4 New Features for ASA Version 8.2(1) (continued)

Feature	Description
Pre-fill Username from Certificate	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 **pre-fill username** and the **username-from-certificate** commands in tunnel-group configuration mode. 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: • **secondary-pre-fill-username**—Enables username extraction for Clientless or AnyConnect client connection. • **secondary-username-from-certificate**—Allows for extraction of a few standard DN fields from a certificate for use as a username.
Double Authentication	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. 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. Double authentication requires the following new tunnel-group general-attributes configuration mode commands: • **secondary-authentication-server-group**—Specifies the secondary AAA server group, which cannot be an SDI server group. • **secondary-username-from-certificate**—Allows for extraction of a few standard DN fields from a certificate for use as a username. • **secondary-pre-fill-username**—Enables username extraction for Clientless or AnyConnect client connection. • **authentication-attr-from-server**—Specifies which authentication server authorization attributes are applied to the connection. • **authenticated-session-username**—Specifies which authentication username is associated with the session. **Note** The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication.

Table 4 New Features for ASA Version 8.2(1) (continued)

Feature	Description
AnyConnect Essentials	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: • No CSD (including HostScan/Vault/Cache Cleaner) • No clientless SSL VPN • Optional Windows Mobile Support 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. To configure AnyConnect Essentials, the administrator uses the following command: **anyconnect-essentials**—Enables the AnyConnect Essentials feature. If this feature is disabled (using the **no** form of this command), the SSL Premium license is used. This feature is enabled by default. **Note** This license cannot be used at the same time as the shared SSL VPN premium license.
Disabling Cisco Secure Desktop per Connection Profile	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. CLI: **[no] without-csd command** **Note** "Connect Profile" in ASDM is also known as "Tunnel Group" in the CLI. Additionally, the **group-url** command is required for this feature. If the SSL VPN session uses connection-alias, this feature will not take effect.
Certificate Authentication Per Connection Profile	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 **ssl certificate authentication** command is no longer needed, but the adaptive security appliance retains it for backward compatibility.
EKU Extensions for Certificate Mapping	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. The following command was introduced: **extended-key-usage**.
SSL VPN SharePoint Support for Win 2007 Server	Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.

Table 4 New Features for ASA Version 8.2(1) (continued)

Feature	Description
Shared license for SSL VPN sessions	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: **license-server** commands (various), **show shared license**. **Note** This license cannot be used at the same time as the AnyConnect Essentials license.
Firewall Features	
TCP state bypass	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: **set connection advanced tcp-state-bypass**.
Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy	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.
Displaying the CTL File for the Phone Proxy	The Cisco Phone Proxy feature includes the **show ctl-file** command, which shows the contents of the CTL file used by the phone proxy. Using the **show ctl-file** command is useful for debugging when configuring the phone proxy instance. This command is not supported in ASDM.
Clearing Secure-phone Entries from the Phone Proxy Database	The Cisco Phone Proxy feature includes the **clear phone-proxy secure-phones** 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 **timeout secure-phones** command). Alternatively, you can use the **clear phone-proxy secure-phones** command to clear the phone proxy database without waiting for the configured timeout. This command is not supported in ASDM.
H.239 Message Support in H.323 Application Inspection	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.

Table 4 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. All IPv6 functionality is supported unless specifically noted.
Botnet Traffic Filter	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." **Note** This feature requires the Botnet Traffic Filter license. See the following licensing document for more information: http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html The following commands were introduced: **dynamic-filter** commands (various), and the **inspect dns dynamic-filter-snoop** keyword.
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: **allow-ssc-mgmt**, **hw-module module ip**, and **hw-module module allow-ip**.
IPv6 support for IPS	You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the **match any** command, and the policy map specifies the **ips** command.
Management Features	

Table 4 New Features for ASA Version 8.2(1) (continued)

Feature	Description
SNMP version 3 and encryption	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). The following commands were introduced: • **show snmp engineid** • **show snmp group** • **show snmp-server group** • **show snmp-server user** • **snmp-server group** • **snmp-server user** The following command was modified: • **snmp-server host**
NetFlow	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.
Routing Features	
Multicast NAT	The adaptive security appliance now offers Multicast NAT support for group addresses.
Troubleshooting Features	
Coredump functionality	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. To enable coredump, use the **coredump enable** command.

Open Caveats

This section contains open caveats in the latest maintenance release.

If you are running an older release, and you need to determine the open caveats for your release, then add the caveats in this section to the resolved caveats from later releases. For example, if you are running Release 8.2(1), then you need to add the caveats in this section to the resolved caveats from 8.2(1) 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:

https://www.cisco.com/authc/forms/CDClogin.fcc?

Table 5 Open Caveats in Version 8.2

Caveat ID	Description
CSCsz73367	Webvpn rewrite not working with ClearTrust SSO
CSCta02877	Traceback in unicorn thread (outway_buffer_i)
CSCta21907	Traceback in arp thread
CSCtb05048	Some syslogs lost when using terminal or trap(UDP)
CSCtb17498	ASA traceback in 'Thread Name: ssh' when working with captures
CSCtb23281	ASA: SIP inspect not opening pinhole for contact header of SIP 183 msg
CSCtb34233	Null0 route installed for EIGRP summary routes is ignored in routing tbl
CSCtb36994	tcp-intercept doesn't start 3WH to inside when configured on xlate
CSCtb37623	police conform-action and exceed-action not displayed in config
CSCtb59109	Traceback seen when match command is configued on asa_dataplane
CSCtb63515	Clientless webvpn on ASA cannot save .html attached file with IE6 OWA
CSCtc10599	traceback when using CLI from ASDM
CSCtc16148	SLA monitor fails to fail back when ip verify reverse is applied
CSCtc25284	cpu hog in dispatch_poll_thread & t_start
CSCtc34281	ASA allows to enable SSH without checking for existing port 22 static
CSCtc37020	Java-trustpoint command when issued from a MS CA server gives an error.
CSCtc40183	8.2.1.11 Webvpn not able to show dropdowns items written in javascripts
CSCtc59391	ASA tracebacks in checkheaps
CSCtc69310	LDAP authentication with Kerberos SASL fails with memory error
CSCtc72997	Traceback in IPsec message handler
CSCtc81874	Nested Traceback in Checkheaps
CSCtc95659	tftp with inspection on fails to go through a lan-2-lan tunnel
CSCtc98145	ASA traceback in thread tmatch compile thread
CSCtc98175	Traceback in thread IPsec message handler
CSCtd21002	Web page does not refresh after initial Citrix client installation

Table 5 Open Caveats in Version 8.2 (continued)

Caveat ID	Description
CSCtd34212	Unexpected ACL recompile failure messages
CSCtd47023	eCrew Application fails to download Java Applet without Smart Tunnel
CSCtd48248	ASA may send truncated HTML page instead of GIF image via WebVPN
CSCtd55121	4GE-SSM will not transmit all fragments
CSCtd57062	Citrix Web Interface SSO fails in first attempt
CSCtd58986	LIC: ASA-5505 with no license crashed when traffic applied to it
CSCtd59046	AAA: ASA-5505 with AAA configured wont execute cmds when heavy traffic
CSCtd62324	ASA tracebacks in Thread Name: pix_flash_config_thread
CSCtd65135	ASA 5580 8.2.1 may traceback at Thread Name: IPsec message handler
CSCtd73605	ASA RIP: "no redistribute static" breaks "default-information originate"
CSCtd73901	Linkdown, Coldstart SNMP Traps not sent with certain snmp-server config
CSCtd83750	SACK requested again however retransmission arrived
CSCtd87194	ASA5580 drops outbound ESP pkt if original pkt needs to be fragmented
CSCtd93250	Traceback : assert+12 at ../finesse/snap_api.h:141
CSCtd94892	8.2.1 traceback at tmatch compile thread:p3_tree_remove assertion
CSCte01475	EIGRP : static route redistribution with distribute-list not working
CSCte03164	eip 0x08a7464d <policymap_attach_action+573 at qos/policymap.c:1399>
CSCte04806	ASA: Application install fails from the clientless portal.
CSCte04866	Customization of Posture Assesment messages with CSD not working
CSCte05534	OWA does not show message pane with rewriter on IE6
CSCte07982	ASA5580 (8.2.1) traceback in Thread Name: DATAPATH-3-464
CSCte08753	Fails to export Local CA Cert after rebooting ASA
CSCte11340	ASA SSL/TLS client sends TLSv1 handshake record in SSLv3 compat mode
CSCte11515	Group-list is displayed to the user even with invalid or no certificate
CSCte15867	ASA 8.2 - EIGRP - route not redistributed properly with distribution lst
CSCte20982	Crash in SNMP thread when out of memory
CSCte21184	Citrix Web App fails to start through rewriter
CSCte23816	Telnet NOOP command sent to ASA cause next character to be dropped
CSCtf63643	Need to remove the FSCK000x.REC from Compact flash after running dosfsck
CSCtf63937	Need use uptodate timestamp when create log/crypto_archive/coredumpinfo

Resolved Caveats in Version 8.2(2)

The caveats listed in Table 6 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:

https://www.cisco.com/authc/forms/CDClogin.fcc?

Table 6 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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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 processe 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'
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 Assement 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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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
CSCsy27547	Using phone-proxy got assertion "ip.ip_version == IP_VERSION_4"
CSCsy28792	ESMTP inspection drops DKIM signatured 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 doesnt seem to work
CSCsy48250	"clear crypto ipsec sa entry" command doesnt work
CSCsy48626	Traceback due to illegal address access in Thread Name: DATAPATH-0-466
CSCsy48816	webvpn cifs unc 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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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]
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	subintefaces 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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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	OCSP 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
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 looses connections following link down
CSCsz67729	IP address in RTSP Reply packet payload not translated
CSCsz70270	ASA: AnyConnect is allowed to connect twice with same assigned IP
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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]
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 csco_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 resetinbound send RST unencrypted when triggered by vpn-filter
CSCta42035	"show conn detail" does not indicate actual timeout
CSCta42455	H323: Disable H323 inspect in one context affects H323 inspect in other
CSCta44073	Group requiring cert-auth not shown in AnyConnect Group-List
CSCta45210	Hang may occur with pre-fill-username feature
CSCta45238	Unable to Download Packet Captures from Admin Context for Other Contexts

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
CSCta45256	WebVPN group-url with a trailing "/" treated differently
CSCta47556	WebVPN: Plugin parameter "csco_sso=1" doesn't work in browser favorites
CSCta47685	WebVPN: Plugin parameter "csco_sso=1" doesn't work with "=" in password
CSCta47769	WebVPN: XML parser and tags with dot.
CSCta49088	"Lost connection to firewall" Message in ASDM with "&" in nameif
CSCta49362	WebVPN: wrong arg count in Flash rewriter
CSCta54837	IPSec over TCP tunnel dropped after launching CIPC
CSCta55072	ASA traceback in Thread Name: Dispatch Unit, Abort: Assert Failure
CSCta55102	WebVPN - PeopleSoft issue
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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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-ing 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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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
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

Table 6 Resolved Caveats in Version 8.2(2) (continued)

Caveat ID	Description
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

For information on the end-user license agreement, go to:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/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

For additional information on IPS, see:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

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

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

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

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

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.