



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

---

**June 15, 2009**

This document contains release information for Cisco ASA 5500 Version 8.2(1).

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 6](#)
- [Open Caveats in Software Version 8.2, page 13](#)
- [End-User License Agreement, page 17](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 17](#)

## Important Notes

- 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.
- 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://preview.cisco.com/en/US/docs/security/asa/asa82/license/license82.html>.



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

- When using Clientless SSL VPN Post-SSO parameters for the Citrix Web interface bookmark, Single-Signon (SSO) works, but the Citrix portal is missing the Reconnect and Disconnect buttons. Only the Log Off button shows. When not using SSO over Clientless, all three buttons show up correctly.

**Workaround:** Use the Cisco HTTP-POST plugin to provide single signon and correct Citrix portal behavior.

- 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. See the “[Memory Requirements](#)” section on page 4.
- Connection Profile/Tunnel Group terminology in CLI vs. ASDM—The adaptive security appliance tunnel groups define the initial connection parameters and attributes (such as AAA, client address assignment, and connection alias/group-url) for a remote access VPN session. In CLI they are referred to as *tunnel groups*, whereas in ASDM they are referred to as *Connection Profiles*. A VPN policy is an aggregation of Connection Profile, Group Policy, and Dynamic Access Policy authorization attributes.

## Limitations and Restrictions

- 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 3](#)
- [Upgrading the Phone Proxy and MTA Instance, page 3](#)
- [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/cgi-bin/tablebuild.pl/asa>

## 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 4](#)
- [ASDM, SSM, SSC, and VPN Compatibility, page 6](#)

## 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 4](#)
- [Memory Upgrade Kits, page 5](#)
- [Viewing Flash Memory, page 5](#)
- [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 <sup>1</sup>         | 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 4GB 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 4GB.

## 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 available 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.<br>For information about ASDM requirements for other releases, see <i>Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility</i> :<br><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> |
| VPN                      | For the latest OS and browser test results, see the <i>Cisco ASA 5500 Series—Supported VPN Platforms, Version 8.2(1)</i> :<br><a href="http://www.cisco.com/en/US/docs/security/asa/compatibility/vpn-platforms-82.html">http://www.cisco.com/en/US/docs/security/asa/compatibility/vpn-platforms-82.html</a>                                                                                             |
| SSM and SSC applications | For information about SSM and SSC application requirements, see <i>Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility</i> :<br><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>                                                             |

## New Features


**Note**

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

Table 3 lists the new features for Version 8.2(1).

**Table 3**      **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> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPD/Telnet/SSH.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Customizing Secure Desktop                        | <p>You can use ASDM to customize the Secure Desktop windows displayed to remote users, including the Secure Desktop background (the lock icon) and its text color, and the dialog banners for the Desktop, Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows.</p> <p>In ASDM, see Configuration &gt; CSD Manager &gt; Secure Desktop Manager.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 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> <p>In ASDM, see In ASDM, see Configuration&gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect or Clientless SSL VPN Connection Profiles &gt; Advanced. Settings are in Authentication, Secondary Authentication, and Authorization panels.</p> |

**Table 3**      ***New Features for ASA Version 8.2(1) (continued)***

| Feature               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access or Clientless SSL VPN &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Advanced &gt; Secondary Authentication.</p> |

**Table 3**      **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> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; AnyConnect Essentials License. The AnyConnect Essentials license must be installed for ASDM to show this pane.</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> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Connection Profiles &gt; Add or Edit &gt; Advanced, Clientless SSL VPN Configuration.</p> <p>or</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add or Edit &gt; Advanced &gt; SSL VPN.</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> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Basic.</p> <p>or</p> <p>Configuraiton &gt; Remote Access VPN &gt; Clientless SSL VPN &gt; Connection Profiles &gt; Add/Edit&gt;Basic.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 3 New Features for ASA Version 8.2(1) (continued)

| Feature                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> <p>In ASDM, use the IPsec Certificate to Connection Maps &gt; Rules pane, or Certificate to SSL VPN Connections Profile Maps pane.</p>                    |
| SSL VPN SharePoint Support for Win 2007 Server                                        | Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 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> <p>In ASDM, see Configuration &gt; Device Management &gt; Licensing &gt; Shared SSL VPN Licenses. Also see, Monitoring &gt; VPN &gt; Clientless SSL VPN &gt; Shared Licenses.</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> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Rule Actions &gt; Connection Settings.</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> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; Media Termination Address.</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>                                                                                                                                                                                                                                                                                                                                                                         |

**Table 3**      **New Features for ASA Version 8.2(1) (continued)**

| Feature                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225. Click <b>Configure</b> and then choose the H.323 Inspect Map.</p> |
| Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck | <p>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).</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225.</p>                                                                                                                                                                                                                                                                                                                                                                                             |
| IPv6 in transparent firewall mode                                | <p>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.</p> <p>All IPv6 functionality is supported unless specifically noted.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; Management IP Address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 3 New Features for ASA Version 8.2(1) (continued)

| Feature                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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><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> <p>In ASDM, see Configuration &gt; Firewall &gt; Botnet Traffic Filter.</p> |
| AIP SSC card for the ASA 5505 | <p>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>.</p> <p>In ASDM, see Configuration &gt; Device Setup &gt; SSC Setup and Configuration &gt; IPS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IPv6 support for IPS          | <p>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.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <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> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; SNMP.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Routing Features</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Multicast NAT                 | The adaptive security appliance now offers Multicast NAT support for group addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 3** *New Features for ASA Version 8.2(1) (continued)*

| Feature                         | Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Troubleshooting Features</b> |                                                                                                                                                                                                                                                                                                                                                                                                               |
| 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.<br><br>To enable coredump, see the <b>coredump enable</b> command. |

## Open Caveats in Software Version 8.2

The caveats listed in [Table 4](#) are open in software Version 8.2. 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 4** *Open Caveats in Version 8.2*

| Caveat ID  | Description                                                              |
|------------|--------------------------------------------------------------------------|
| CSCsw51570 | VPNFO: assertion "(ret_code == VPNFOL_SUCCESS)" failed: file "vpnfol_upd |
| CSCsw70465 | HT VPN F/O assertion ha_error == HA_EOK vpf_message_peer.c", line 411    |
| CSCsx29692 | "show parser dump exec" command causes traceback                         |
| CSCsy57838 | 5505 HWclient/LB - auth fail results in never ending connection attmpt   |
| CSCsz24748 | Assert violation in TCP channel during tcp_open_connect                  |
| CSCsz33877 | traceback in schedctl_start - clientless/FO/LOCAL aaa                    |
| CSCsz37492 | traceback eip 0x09307337 <mem_get_owner+55 at slib/malloc.c:5785>        |
| CSCsz40667 | Traceback in fiber_scheduler following stress test                       |

The caveats listed in [Table 5](#) are recently-found caveats that were fixed in interim builds for previous versions; however, they are still open in Version 8.2 (they will be addressed in future releases).

**Table 5** *Open Caveats from Previous Releases*

| Caveat ID  | Description                                                            |
|------------|------------------------------------------------------------------------|
| CSCsi27903 | L2TP & NAC; Default NAC policy prevents data from passing              |
| CSCsl04124 | SIP does not support "early RTCP"                                      |
| CSCsm39914 | match resp body length for http class-map doesnt take correct value    |
| CSCso80611 | context using SSM app in promiscuous mode shows incorrect memory usage |
| CSCsq34317 | dynamic acls downloaded as part of authorization are not being deleted |
| CSCsq34317 | dynamic acls downloaded as part of authorization are not being deleted |
| CSCsq34336 | ASA: rate-limiting for encrypted s2s traffic not consistently hand     |
| CSCsu27257 | how asp table classify doesn't show WCCP domain                        |

**Table 5**      **Open Caveats from Previous Releases (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| CSCsu56483       | Extend show ak47 to display per pool and per block information           |
| CSCsu56483       | Extend show ak47 to display per pool and per block information           |
| CSCsv36948       | ASA NTLM authentication with Windows 2008 server                         |
| CSCsv37979       | Changing interface IP Address does not clear existing connections        |
| CSCsv40504       | Telnet connection permitted to lowest security level interface           |
| CSCsv89645       | ASA 8.04 - certificate chain not being sent when configured w/ IPS       |
| CSCsv91391       | L2TP with EAP auth stuck [%ASA-4-403102 - authentication pending]        |
| CSCsv91564       | Multiple certificates are installed to one trustpoint when importing.    |
| CSCsw19588       | Standby console freezes if user logs in prior to detecting mate          |
| CSCsw25253       | ssl vpn related memory corruption causes traceback                       |
| CSCsw41161       | PMTUD - ICMP type 3 code 4 generated for GRE flow is dropped 313005      |
| CSCsw47441       | Java Applet Signing Error..plugins still use old expired certifica       |
| 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                            |
| 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                       |
| CSCsx22842       | PPPoE re-negotiation does not start after short disconnect               |
| CSCsx23611       | VPN: TCP traffic allowed on any port with management-access enable       |
| CSCsx25628       | %PIX ASA-3-713128 should be logged as a lower level message              |
| CSCsx27609       | 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                                 |
| CSCsx50318       | OCSP revocation stops working after some time on Cisco ASA               |
| CSCsx52598       | No focus on "More information required" radius challenge/response page   |
| CSCsx54449       | ASA may processe LDAP password policy with no password-management        |
| CSCsx54893       | dlambert TEA 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        |
| CSCsx59746       | Tacacs Command Accounting does not send packet for nat-control           |
| CSCsx65702       | ASA crash upon failover with interface monitor enabled                   |

**Table 5** *Open Caveats from Previous Releases (continued)*

| <b>Caveat ID</b> | <b>Description</b>                                                      |
|------------------|-------------------------------------------------------------------------|
| 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                   |
| 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 Assesment matches wrong DAP Policy      |
| CSCsx94849       | Failover pair both become active after failover w/shortest timeout      |
| 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       | Traceback in Session Manager with Page Fault                            |
| 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 certifica      |
| CSCsy21727       | Failover pair is not able to sync config and stuck in Sync Config state |
| CSCsy23275       | Smart Tunnels and POST parameters should be interoperable               |
| 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       |
| 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                    |
| CSCsy48250       | clear crypto ipsec sa entry command doesnt work                         |
| CSCsy48626       | Traceback due to illegal address access in Thread Name:DATAPATH-0-466   |

**Table 5**      **Open Caveats from Previous Releases (continued)**

| <b>Caveat ID</b> | <b>Description</b>                                                       |
|------------------|--------------------------------------------------------------------------|
| 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               |
| 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 r       |
| 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 authenticati       |
| 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 connection to dynamic webpage pulling from webvpn cache hangs     |
| CSCsy74773       | page fault in fover _parse on a/s stress with 240 vlan on 2 red if       |
| CSCsy75345       | subintefaces on 4ge-ssm ports fail with mac-address auto and failo       |
| CSCsy75684       | Traceback from thread DATAPATH-0-483 on failover                         |
| CSCsy75800       | Shared int Mac add auto reload primary there will be some packet         |
| 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                          |
| 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            |
| 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       |
| 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   |

**Table 5**      **Open Caveats from Previous Releases (continued)**

| Caveat ID  | Description                                                             |
|------------|-------------------------------------------------------------------------|
| 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 0xa      |
| 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                   |
| CSCsz02807 | Logging standby can create logging loop with syslogs 418001 and 10      |
| CSCsz02849 | Long delay before standby becomes active if unit holdtime misconfi      |
| CSCsz06329 | Unexpect Syslog: No SPI to identify Phase 2 SA                          |
| CSCsz10339 | console hangs for extended period of time when config-url is appli      |
| CSCsz10924 | Management port in promiscuous mode processes packets not destined      |
| CSCsz17027 | L2TP: DACL w/ Wildcard Mask not applied to L2TP over IPsec Clients      |
| CSCsz24401 | Stuck EIGRP ASP entry prevents neighbor from coming up                  |
| CSCsz34300 | acl-netmask-convert auto-detect cannot convert wildcard mask of 0.0.0.0 |
| CSCsz34811 | snmpwalk for crasSVCNumSessions gives incorrect output                  |
| CSCsz35484 | Failover pair with CSC-SSM: High CPU usage by SSM Accounting Thread     |

## 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](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](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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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

©2009 Cisco Systems, Inc. All rights reserved.