Cisco ASA 5500 Series Release Notes Version 8.0(2)

January 2008

Contents

This document includes the following sections:

Introduction

This release supports the following products:

- Cisco ASA 5500 Series adaptive security appliance, Version 8.0(2)
- ASDM, Version 6.0(2)
- Cisco AnyConnect VPN Client, Version 2.0(1)
- Cisco Secure Desktop, Version 3.2
- Cisco Intrusion Prevention System, Version 6.0

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

Cisco ASA 5500 Series Adaptive Security Appliance

The Cisco ASA 5500 series adaptive security appliances are purpose-built solutions that combine the most effective security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture.

Designed as a key component of the Cisco Self-Defending Network, the adaptive security appliance provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network adaptive security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

For more information on all the new features, see New Features, page 7.

Additionally, the adaptive security appliance software supports Cisco Adaptive Security Device Manager (ASDM). ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use web-based management interface. Bundled with the adaptive security appliance, ASDM accelerates adaptive security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of the adaptive security appliance. Its secure, web-based design enables anytime, anywhere access to adaptive security appliances. For more information on ASDM, see the *Cisco ASDM Release Notes Version 6.0(2).*

Cisco AnyConnect VPN Client

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

Cisco Intrusion Prevention System

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

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

System Requirements

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

Memory Requirements

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

Table 1 DRAM Memory Requirements

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

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

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

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

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

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

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

For example:

```
hostname # dir
Directory of disk0:/

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

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

62881792 bytes total (3854336 bytes free)

hostname #
```

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

Note If you use two units with different flash memory sizes, make sure that the unit with the smaller flash memory has enough space for the software images and configuration files.

Operating System and Browser Requirements

For the latest OS and browser test results, see the *Cisco ASA 5500 Series VPN Compatibility Reference*.

Determining the Software Version

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

Upgrading to a New Software Version

ASA Version 8.0(2) delivers major enhancements to SSL VPN Remote Access services providing advanced capabilities that simplify the management and deployment of SSL VPNs while enhancing end-user services and ease-of-use. Highlights of Version 8.0(2) for Remote Access include:

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

- Microsoft Windows Vista (32- and 64-bit) and MacOS X support

SSL VPN customers are encouraged to upgrade to Version 8.0(2).

ASA Version 8.0(2) also provides new functionality for firewall customers, as listed below. However, given this release is primarily targeted towards our SSL VPN customers, customers who remain satisfied with the firewall feature content of the ASA Version 7.x series are encouraged to remain on 7.x until such time as they have a business requirement for Version 8.0(2). To support customers choosing to remain on 7.x versions, release updates across all 7.x have been made available.

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

http://www.cisco.com/kobayashi/sw-center/

You must upgrade or downgrade from Version 7.2.(x) to Version 8.0(2) and vice versa, because older versions of the ASA images do not recognize new ASDM images, and new ASA images do not recognize old ASDM images.

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

To upgrade from Version 7.2.(x) to Version 8.0(2), perform the following steps:

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

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

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

Step 3 Load the new Version 8.0(2) image from the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/asa

Step 4 Restart the device to load the Version 8.0(2) image.

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

http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

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

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

Upgrading to Version 8.0 for Portal Customization and URL Lists

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

Note Version 7.2 portal customizations and URL lists work only if clientless SSL VPN (WebVPN) configuration is enabled on the appropriate interface in the Version 7.2(x) configuration file *before* you upgrade to Version 8.0(2).

After you upgrade to Version 8.0(2), to make any changes to existing URL lists or customizations, you must use the new **export/import webvpn url-list** commands that replace the 7.2 **url-list** a commands in webvpn mode.

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

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

Downgrading to Version 7.2(x) Software

To downgrade from Version 8.0(2) to 7.2(x), perform the following steps:

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

http://www.cisco.com/cgi-bin/tablebuild.pl/asa

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

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

http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

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

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

Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2 requires ASA Version 8.0(2). You do not need to restart the adaptive security appliance after you install or upgrade Cisco Secure Desktop.

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

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

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

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

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

http://www.cisco.com/pcgi-bin/tablebuild.pl/securedesktop

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

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

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

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

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

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

New Features

This section lists the new features for Version 8.0(2). All new features are supported in ASDM Version 6.0.

ASA Feature Type	Feature	Description
General Features		
Routing	EIGRP routing	The adaptive security appliance supports EIGRP or EIGRP stub routing.

ASA Feature Type	Feature	Description
High Availability	Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This works for both Active/Standby and Active/Active failover.
	CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature in failover configurations.
	Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configuration in failover pairs.
	Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
	Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the adaptive security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs.
SSMs	Password reset	You can reset the password on the SSM hardware module.
VPN Features		
Authentication Enhancements	Combined certificate and username/password login	An administrator requires a username and password in addition to a certificate for login to SSL VPN connections.
	Internal domain username/password	Provides a password for access to internal resources for users who log in with credentials other than a domain username and password, for example, with a one-time password. This is a password in addition to the one a user enters when logging in.
	Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support available for authentication and authorization.
	Onscreen keyboard	The adaptive security appliance includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.
	SAML SSO verified with RSA Access Manager	The adaptive security appliance supports Security Assertion Markup Language (SAML) protocol for Single Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Identity Manager).
	NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-based clients.
Certificates	Local certificate authority	Provides a certificate authority on the adaptive security appliance for use with SSL VPN connections, both browser- and client-based.
	OCSP CRL	Provides OCSP revocation checking for SSL VPN.

ASA Feature Type	Feature	Description
Cisco Secure Desktop	Host Scan	As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the adaptive security appliance. The adaptive security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP). With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements. Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.
	Simplified prelogin assessment and periodic checks	Cisco Secure Desktop now simplifies the configuration of prelogin and periodic checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. You can configure the adaptive security appliance to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.
Access Policies	Dynamic access policies (DAP)	VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration. Dynamic Access Policies (DAP) on the adaptive security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the adaptive security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.
	Administrator differentiation	Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS service-type attribute.

ASA Feature Type	Feature	Description
Platform Enhancements	VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPsec and SSL tunnel-based connections.
	VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 adaptive security appliances that have a Security Plus license.
	Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPSec operations and reducing the amount of debug output, you can better troubleshoot the adaptive security appliance with a large number of tunnels.
Browser-based SSL VPN Features	Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly organized and visually appealing.
	Customization	Supports administrator-defined customization of all user-visible content.
	Support for FTP	You can provide file access via FTP in additional to CIFS (Windows-based).
	Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications without requiring a pre-installed client application. Java applets let users access these applications from the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, RDP, and VNC.
	Smart tunnels	A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with the adaptive security appliance as the pathway. Version 8.0(2) lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application and the SHA-1 hash of its checksum to check before granting it access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access. The remote host originating the smart tunnel connection must be running Microsoft Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.
	RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed information, which lets company news or other information display on a user screen.

ASA Feature Type	Feature	Description
Browser-based SSL VPN Features (continued)	Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a file server.
	Transformation enhancements	Adds support for several complex forms of web content over clientless connections, including Adobe flash and Java WebStart.
	IPv6	Allows access to IPv6 resources over a public IPv4 connection.
	Web folders	Lets browser-based SSL VPN users connecting from Windows operating systems browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.
	Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Microsoft Office applications available on the machine with the browser to view, change, and save documents shared on a server. Version 8.0(2) supports Windows Sharepoint Services 2.0 in Windows Server 2003.
HTTP Proxy	PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.
HTTPS Proxy	Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the adaptive security appliance can send to an external proxy server.
NAC	SSL VPN tunnel support	The adaptive security appliance provides NAC posture validation of endpoints that establish AnyConnect VPN client sessions.
	Support for audit services	You can configure the adaptive security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the adaptive security appliance for application to the traffic on the tunnel.

ASA Feature Type	Feature	Description
Firewall Features		
Application Inspection	Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.
	AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in WebVPN HTTP and HTTPS streams.
	TLS Proxy for SCCP and SIP	Enables inspection of encrypted traffic. Implementations include SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
	SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.
	Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.
Access Lists	Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.
	Ability to rename access list	Lets you rename an access list.
	Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.
Attack Prevention	Set connection limits for management traffic to the adaptive security appliance	For a Layer 3/4 management class map, you can specify the **set connection** command.
	Threat detection	You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.
NAT	Transparent firewall NAT support	You can configure NAT for a transparent firewall.
IPS	Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode adaptive security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.
Logging	Secure logging	You can enable secure connections to the syslog server using SSL or TLS with TCP, and encrypted system log message content. Not supported on the PIX series adaptive security appliance.
IPv6	IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields.

Important Notes

This section lists important notes related to Version 8.0(2).

Web Folders May Require a Microsoft Patch

Web folders do not work if both of the following are true:

- Microsoft Internet Explorer 7 is installed on Microsoft Windows XP or 2000.
- Microsoft Office is not installed.

In the initial 8.0(2) release, the adaptive security appliance software disables web folders in the portal when this occurs. In releases following 8.0(2), including maintenance releases, the software does not disable web folders. In that case, the user sees "My Computer" opened instead of the targeted web folder. Remote users can use web folders after installing a Microsoft patch from either of the following pages:

- http://support.microsoft.com/kb/892211/en-us
- http://support.microsoft.com/kb/907306/en-us

In some language versions of Windows, web folders also fail to open if web folder requests have non-ASCII characters. In this case, the requests of the corresponding locale fail to specify the encoding in use. Remote users can also avoid this issue by installing the patch from either of the pages above.

JInitiator and SSL Certificates

Oracle JInitiator is the licensed Oracle version of Sun JVM. Some forms-based applications require JInitiator to run. This requirement might apply to some applications running over clientless SSL VPN on the adaptive security appliances.

Complications occur in applying an SSL certificate to the JInitiator, a requirement for loading JInitiator onto the adaptive security appliance. The solution is to import the SSL certificate to the JInitiator keystore.

To import the SSL certificate to the JInitiator keystore, perform the following steps:

Step 1 Double-click the yellow lock in the status bar of Internet Explorer.

Step 2 Navigate to the Certification Path tab to see whether the self-signed certificate has a root certificate. If it does, select the root certificate and click the **View Certificate** button. If no root certificate exists, continue with the self-signed certificate.

Step 3 Click the **Details** tab and click **Copy to File**.

Step 4 Save the certificate as Base-64 encoded.

Step 5 Open the Base-64 encoded certificate in a text-editor. Copy the entire contents (including the BEGIN CERTIFICATE and END CERTIFICATE lines).

Step 6 Open the certdb.txt file in the lib/security directory of Oracle JInitiator (for example, C:\Program Files\Oracle\JInitiator 1.3.1.18\lib\security\certdb.txt). Add the copied certificate to this file and prepend it with comment lines (beginning with #) to explain what the certificate is.

Step 7 Close any open web browsers to close the associated JVMs and start the application again. The JInitiator application should work.

CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN client and Cisco Secure Desktop to interoperate with the adaptive security appliance.

To enable the AnyConnect VPN client and Cisco Secure Desktop, perform the following steps:

Step 1 Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:

- The CD that shipped with the adaptive security appliance.
- The software download page for the ASA 5500 Series adaptive security appliance at http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip

Step 2 Extract the .export files from the .zip package files.

Step 3 Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.

Step 4 Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

Step 5 Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations.*

Toggling the HTTP Server Off and On While Using ASDM

ASDM becomes nonfunctional if you toggle the HTTP server off and on. The work around is to reload the adaptive security appliance.

Using the Priority-Queue Configuration on ASA 5505

On ASA 5505 only, configuring priority-queue on one interface overwrites the same configuration on all other interfaces (that is, only the last applied configuration is present on all interfaces). In addition, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue-limits and the smallest of all tx-ring-limits on any one interface (CSCsi13132).

VLAN ID Range Support on ASA 5505

The range for VLAN IDs has been increased from 1-1001 to 1-4090.

Java Applet Plug-in Connected Status

Some open-source, Java applet plug-ins display a status of “connected” and “online” even if the session to the destination service is not set up. The applet displays the incorrect status information, not the adaptive security appliance.

Cache Cleaner Support

Cache Cleaner, available as part of Cisco Secure Desktop, supports clientless (browser-based) SSL VPN connections over Macintosh; Linux; and Windows 98, ME, 2000, XP, and Vista. Cache Cleaner also supports Weblaunch of Cisco AnyConnect on a PC running Windows 2000 or XP. Cache Cleaner does not support the standalone startup of AnyConnect client from any computer.

Sharepoint Restrictions

When you access Microsoft Word from Sharepoint in a clientless SSL VPN session, do not use the "Save As" option to save a file with its existing filename. Use the "Save" option to overwrite the existing file, and the "Save As" option to save the file with a new filename (CSCsi21048).

ASA Version 8.0(2) clientless SSL VPN software does not support Explorer View in Sharepoint 2.0.

Insertion or Removal of Flash Memory Card

If you use the Linux OS, when you insert or remove an external flash memory card, a system log message is not recorded (CSCsg64799).

AnyConnect Client Sessions

A reestablished AnyConnect client session fails to displace an AnyConnect client session that is terminated abnormally (CSCsi40917).

High Availability Active/Standby Configuration

When the adaptive security appliance is operating in a high-availability active/standby configuration and a failover occurs, causing the standby adaptive security appliance to resume current connections, the MacOS X AnyConnect connections might disconnect. If the MacOS X AnyConnect connection disconnects after a failover, you must reconnect (CSCsi44920).

IPv6

IPv6 SSL VPN failover (as well as IPv6 failover in general) is not supported in ASA Version 8.0(2).

MAPI

Version 8.0(2) does not support MAPI proxy either via Port Forwarding or Smart Tunnels. The work around is to use AnyConnect for Microsoft Exchange.

Open Source Software Usage

For a list of the open source software used in ASA Version 8.0(2), see the *Open Source Software Licenses for ASA and PIX Security Appliances* document on Cisco.com.

Certificates

- Symptom: SSL connections from browsers and AnyConnect fail if the certificate being used contains the following enhanced key usage “IP security IKE intermediate (1.3.6.1.5.5.8.2.2)”. This is the default way of issuing certificates via SCEP enrollment to a Microsoft 2003 Enterprise CA with the newer certificate templates.

  Workaround:

  - Use terminal enrollment instead of SCEP to get an ASA certificate.
  - Changing the SCEP policy module on the 2003 CA may alleviate this issue.
- Symptom: If the validity date for a a certificate is issued beyond the year 2099, it will fail to authenticate and an error will be generated when attempting to authenticate it.

  Workaround:

  - Limit the validity period of the certificate to less than the recommended end date of 03:14:08 UTC, January 19, 2038
- Symptom: User prompted for credentials when permstore and auto-signon are both enabled.

  Conditions:

  Both auto-signon and permanent-storage are enabled for the server requiring authentication.

  Workaround:

  - Disable auto-signon for this server. Enable auto-signon only for servers having the same login credentials as WebVPN.

Note Because credentials used by auto-signon take precedence over permanent-storage of user credentials, do not enable auto signon for servers that do not require authentication or that use credentials different from the adaptive security appliance. When auto signon is enabled, the adaptive security appliance passes on the login credentials that the user entered to log into the adaptive security appliance regardless of what credentials are in user storage.

DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs

The adaptive security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Prelogin Assessment and Host Scan modules of Cisco Secure Desktop return information to the adaptive security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes.

Most, but not all, anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is memory-resident as follows:

- If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program.
- If the installed program does support active scan, and active scan is enabled for the program, Host Scan reports the presence of the software. Again the adaptive security appliance selects DAP records that specify the program.
- If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The adaptive security appliance does not select DAP records that specify the program. Further, the output of the **debug trace** command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

This behavior provides improved security from 8.0 Beta releases, which counted as matches users who had anti-virus, anti-spyware, and personal firewall programs installed but not running.

DAP Examples

Online help for Dynamic Access Policies mentions but does not include examples. The examples are in the ASDM Configuration Guide, available on cisco.com.

Backing Up Configuration Files

Configuration files in Version 8.0(2) include the following:

- Startup and running configuration files.
- Files you import using the **import webvpn** command. Currently these files include customizations, URL lists, web contents, plug-ins, and language translations.
- DAP policies (dap.xml).
- CSD configurations (data.xml).
- Digital keys and certificates (we do not recommend automatic backups for security reasons).
- Local CA user database and certificate status files (we do not recommend automatic backups of the CA key for security reasons).

The CLI lets you back up and restore individual elements of your configuration using the **copy, save, export** and **import** commands.

We now also provide a sample script that lets you automate these backups. That is, you can use a script to back up and restore multiple files, rather than executing a series of CLI commands.

For more information and step-by-step instructions for using CLI commands and/or a script to back up and restore your configuration files, see the "Backing Up Configuration Files" in the *Cisco Security Appliance Command Line Interface Configuration Guide.OL-14932-01*

Cache Filesystem

The default size of the cache filesystem (20 Mb) is not enough to support all four versions of the AnyConnect packages (Windows, Linux, Mac OS X arch386, Mac OS X ppc) and CSD. If you want to install all five client packages on the adaptive security appliance, you should first increase the maximum size of cache filesystem entering the **(config-webvpn)# cache-fs limit** command The recommended size of cache filesystem is 22 Mb.

Caveats

The following sections describe the caveats for Version 8.0(2).

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

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

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats - Version 8.0(2)

Table 2 Open Caveats

DDTS Number	Software Version 8.0(2)	
	Corrected	Caveat
CSCsj15448	No	Group-policy names with embedded space(s) are not usable
CSCsj08209	No	In some instances 'clear ospf process causes traceback
CSCsj22800	No	clearing shuns during an attack causes traceback
CSCsj20475	No	WebVPN: Group-URL fails without a /
CSCsi09586	No	Conflict between aaa listener and http redirect commands
CSCej04099	No	static xlate breaks management-access inside
CSCsg47023	No	L2TP Connections with Certificates to ASA Fail to Connect

Table 2 Open Caveats (continued)

DDTS Number	Software Version 8.0(2)	
	Corrected	**Caveat**
CSCsg65434	No	Multiple ipsec peers: PIX/ASA stops processing the IPSEC peers list
CSCsh15861	No	VPN client fails to connect, external DHCP server
CSCsh28991	No	IKE sessions are getting stuck in AM_WAIT_DELETE state
CSCsh29836	No	Clientless WebVPN traffic not transmitted out separate L2L interface
CSCsh40829	No	LDAP: multiple Cisco-AV-Pair need to be enforced on vpn-session
CSCsh67528	No	L2TP/IPSec OSX client disconnection after 45 minutes when NAT-T in used
CSCsh68314	No	NAC-default-access list doesn't work as expected with l2tp/ipsec
CSCsi00074	No	Incorrect values returned by SSL VPN OIDs
CSCsi04673	No	FW may drop packets when VPN address pool overlaps with interface subnet
CSCsi08317	No	PIX using Authentication Proxy and Wildcard causes Certificates error
CSCsi12180	No	SSH connections may cause interface errors (no buffer and overruns)
CSCsi15611	No	Traceback may occur with debugs webvpn citrix 255
CSCsi32502	No	packet/byte counters are not populated for the session table of CRAS MIB
CSCsi43492	No	ASA 7.2 CIFS: incomplete upload a file with size of ~100M for Firefox 2
CSCsi51600	No	Misleading prompt with radius/sdi authentication on 7.2.2
CSCsi58109	No	ASA requests username/password until next available aaa server found
CSCsi75355	No	5505 WebVPN: hw accelerator errors with >1024 bit cert
CSCsi98464	No	ASA injects another 'BrowserProtocol' keyword in ICA file
CSCsi98616	No	After two consecutive failovers SVC connections won't replicate
CSCsi98617	No	VPNFO: Standby stale sessions not removed
CSCsj01643	No	IPSec VPN first auth fails when SDI SoftID is in Cleared PIN Mode
CSCsj03319	No	WebVPN: Infopath XML fails to open correctly
CSCsj03437	No	WebVPN: RDP Icon fails after a redirect action to a Citrix Presentation
CSCsj13797	No	SSH connection fails when first server in AAA group is unreachable
CSCsj14874	No	AAA Authentication against local database working inconsistently
CSCsj19829	No	WebVPN: http-proxy interferes with port-forward
CSCsj24914	No	vpn-simultaneous-logins does not work when configuring PKI and no-xauth
CSCeg00330	No	DHCPACK in reply to DHCPINFORM might get dropped
CSCsf07135	No	ASDM connection may cause packet loss
CSCsg61719	No	SNMP: Coldstart Trap is not sent
CSCsh78681	No	In use memory count displayed incorrectly
CSCsi46292	No	Coldstart trap isn't sent in failover settings
CSCsi65122	No	alias with overlapping static and NAT exemption xlate errors on standby
CSCsi68321	No	Pix DHCP relay stops passing traffic after a period of time

Table 2 Open Caveats (continued)

DDTS Number	Software Version 8.0(2)	
	Corrected	**Caveat**
CSCsj01620	No	Type 0 Client-ID for RA clients not supported by some DHCP servers
CSCsj10869	No	SNMP interface counters incorrect on PIX/ASA 7.2.2.22
CSCsg39338	No	to-the-box traffic from a higher metric route Int dropped for no route.
CSCsh48208	No	Directly connected network missing in route table
CSCsi41045	No	OSPF: default-info originate with route-map fails with next hop or source address
CSCsi53577	No	OSPF goes DOWN after reload of VPN Peer
CSCsj03706	No	activex or java filter suppresses the syslog message 304001
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCsi98786	No	Potential HW failure: Traceback in Thread Name: Dispatch Unit
CSCsj14865	No	SMTP fixup consistently drops '250 Ok' SMTP reply
CSCsh21462	No	esmtp ehlo masking drops packet instead of masking
CSCek21850	No	SIP: Standby PIX show the wrong value of xlate timeout for sip media.
CSCsd31162	No	PPPoE: debug ppp doesn't display any debug messages
CSCse96428	No	PIX/ASA drops packets with IP Option Router Alert set
CSCse99033	No	tracked route removed from Standby firewall after failover
CSCsh43799	No	SIP Invite does not go to connect state in SIP Trunk Scenario
CSCsh60480	No	Unable to disconnect a call immediately with ip-address-privacy cmd
CSCsh64554	No	TCP sessions to the box denied because TCP connection limit exceeded
CSCsh91283	No	ASA/PIX: SunRPC inspect dropping packets on 7.0.6
CSCsi00628	No	CPU utilization spike observed with ASDM connected
CSCsi27609	No	ASA may drop MESSAGE requests due to sip-invite timeout
CSCsj12938	No	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj18055	No	Traceroute fails through ASA if outside interface is pppoe and doing PAT
CSCsh55107	No	DHCP relay fails when static translation for all hosts configured
CSCsj09223	No	In some conditions Error initializing main application window
CSCsi05637	No	Can not connect to CSD 3.2 from the computer with pre-installed ActiveX for CSD 3.1
CSCsj03825	No	Secure Desktop Icons not shown in secure desktop
CSCsj00288	No	CSD - Keystroke Logger check fails when HP Quick Launch app is running

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, go to:

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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