Release Notes for Cisco ASA 5500 Version 7.2(5)

May 2010

This document includes the following sections:

- New Features, page 1
- System Requirements, page 1
- Open Caveats, page 9
- Resolved Caveats, page 9
- Related Documentation, page 10
- Obtaining Documentation and Submitting a Service Request, page 10

New Features

There are no new features in Version 7.2(5).

System Requirements

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

- Memory Information, page 2
- Determining the Software Version, page 3
- Upgrading to a New Software Version, page 4
- ASDM, SSM, and VPN Compatibility, page 5
- Supported Models and Feature Licenses, page 5

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

Memory Information

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 Memory, page 2
- Memory Upgrade Kits, page 2
- Viewing Flash Memory, page 3
- DRAM, Flash Memory, and Failover, page 3

Standard Memory

Table 1 lists the standard memory shipped with the adaptive security appliance if manufactured before February 2010 or after February 2010. See the "Memory Upgrade Kits" section on page 2 to order an upgrade kit.

Table 1 Standard Memory and Memory Requirements

ASA Model	Default Internal Flash Memory	Default DRAM Before Feb. 2010	Default DRAM After Feb. 2010
5505	128 MB	256 MB	512 MB
5510	256 MB	256 MB	1 GB
5520	256 MB	512 MB	2 GB
5540	256 MB	1 GB	2 GB
5550	512 MB	4 GB	4 GB

Note In the past, the adaptive security appliance might have shipped with 64 MB of internal CompactFlash.

Memory Upgrade Kits

Table 2 lists the DRAM upgrade kits.

Table 2 DRAM Upgrade Kits

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

Table 3 lists the CompactFlash upgrade kits.

Table 3 CompactFlash Upgrade Kits

Size	Part Number
256 MB	ASA5500-CF-256MB=
512 MB	ASA5500-CF-512MB=

Viewing Flash Memory

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

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

For example:

```
hostname# dir
Directory of disk0:/

43      -rwx  14358528    08:46:02 Feb 19 2007  cdisk.bin
136     -rwx  12456368    10:25:08 Feb 20 2007  asdmfile
58      -rwx  6342320     08:44:54 Feb 19 2007  asdm-600110.bin
61      -rwx  416354      11:50:58 Feb 07 2007  sslclient-win-1.1.3.173.pkg
62      -rwx  23689       08:48:04 Jan 30 2007  asa1_backup.cfg
66      -rwx  425         11:45:52 Dec 05 2006  anyconnect
70      -rwx  774         05:57:48 Nov 22 2006  cvcprofile.xml
71      -rwx  338         15:48:40 Nov 29 2006  tmpAsdmCustomization430406526
72      -rwx  32          09:35:40 Dec 08 2006  LOCAL-CA-SERVER.ser
73      -rwx  2205678     07:19:22 Jan 05 2007  vpn-win32-Release-2.0.0156-k9.pkg
74      -rwx  3380111     11:39:36 Feb 12 2007  securedesktop_asa_3_2_0_56.pkg

62881792 bytes total (3854336 bytes free)

hostname#
```

DRAM, Flash Memory, and Failover

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

Determining the Software Version

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

Upgrading to a New Software Version

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

http://www.cisco.com/cisco/software/navigator.html

Note ASA and ASDM images must be compatible, for example ASA Version 7.2(5) is compatible to ASDM Version 5.2(5). ASDM will not work with an incompatible ASA version. You will get an error message and ASDM will close.

You can also use the command-line interface to download the image, see the "Downloading Software or Configuration Files to Flash Memory" section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.1.(x) to 7.2(5), you must perform the following steps:

Step 1 Load the new image from the following website:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Reload the device so that it uses the new image.

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

http://www.cisco.com/cisco/software/navigator.html

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

```
hostname(config)# asdm image disk0:/ asdm file
```

To downgrade from Version 7.2(5) to 7.1.(x), you must perform the following steps:

Step 1 Load the 7.1(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Reload the device so that it uses the 7.1(x) image.

Step 3 Load the ASDM 5.1(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html

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

```
hostname(config)# asdm image disk0:/ asdm file
```

ASDM, SSM, and VPN Compatibility

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

Table 4 ASDM, SSM, and VPN Compatibility

Application	Description
ASDM	ASA 5500 Version 7.2 requires ASDM Version 5.2. For information about ASDM requirements for other releases, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html
VPN	For the latest OS and browser test results, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html
SSM applications	For information about SSM application requirements, see *Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility*: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Supported Models and Feature Licenses

This software version supports the following models; see the associated tables for the feature support for each model:

- ASA 5505, Table 5
- ASA 5510, Table 6
- ASA 5520, Table 7
- ASA 5540, Table 8
- ASA 5550, Table 9

Note The Cisco PIX security appliance is not supported on ASA 7.2(5).

Note Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

Table 5 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License			Security Plus		
Users, concurrent[1]	10	*Optional Licenses:*		10	*Optional Licenses:*	
		50	*Unlimited*		*50*	*Unlimited*

Table 5 ASA 5505 Adaptive Security Appliance License Features (continued)

ASA 5505	Base License		Security Plus	
Security Contexts	No support		No support	
VPN Sessions[2]	10 combined IPSec and WebVPN		25 combined IPSec and WebVPN	
Max. IPSec Sessions	10		25	
Max. WebVPN Sessions	2	*Optional License: 10*	2	*Optional License: 10*
VPN Load Balancing	No support		No support	
Failover	None		Active/Standby (no stateful failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns[3]	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*	Base (DES)	*Optional license: Strong (3DES/AES)*
Minimum RAM	256 MB		256 MB	

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit only when they communicate with the outside (Internet VLAN). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host command** to view the host limits.
2. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
3. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table 6 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License					Security Plus					
Users, concurrent	Unlimited					Unlimited					
Security Contexts	No support					2	*Optional Licenses:*				
							5				
VPN Sessions[1]	250 combined IPSec and WebVPN					250 combined IPSec and WebVPN					
Max. IPSec Sessions	250					250					
Max. WebVPN Sessions	2	*Optional Licenses:*				2	*Optional Licenses:*				
		10	*25*	*50*	*100*	250	*10*	*25*	*50*	*100*	250
VPN Load Balancing	No support					No support					
Failover	None					Active/Standby or Active/Active					
GTP/GPRS	No support					No support					
Max. VLANs	50					100					

Table 6 ASA 5510 Adaptive Security Appliance License Features (continued)

ASA 5510	Base License		Security Plus	
Concurrent Firewall Conns[2]	50 K		130 K	
Max. Physical Interfaces	Unlimited		Unlimited	
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*	Base (DES)	*Optional license: Strong (3DES/AES)*
Min. RAM	256 MB		256 MB	

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 7 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License						
Users, concurrent	Unlimited					Unlimited	
Security Contexts	2	*Optional Licenses:*					
		5	10	20			
VPN Sessions[1]	750 combined IPSec and WebVPN						
Max. IPSec Sessions	750						
Max. WebVPN Sessions	2	*Optional Licenses:*					
		10	*25*	*50*	*100*	250	*500*	*750*
VPN Load Balancing	Supported						
Failover	Active/Standby or Active/Active						
GTP/GPRS	None	*Optional license: Enabled*					
Max. VLANs	150						
Concurrent Firewall Conns[2]	280 K						
Max. Physical Interfaces	Unlimited						
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*					
Min. RAM	512 MB						

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 8 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License				
Users, concurrent	Unlimited				Unlimited
Security Contexts	2	Optional licenses:			
		5	*10*	*20*	*50*
VPN Sessions[1]	5000 combined IPSec and WebVPN				
Max. IPSec Sessions	5000				

Table 8 ASA 5540 Adaptive Security Appliance License Features (continued)

ASA 5540	Base License								
Max. WebVPN Sessions	2	*Optional Licenses:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
VPN Load Balancing	Supported								
Failover	Active/Standby or Active/Active								
GTP/GPRS	None	*Optional license: Enabled*							
Max. VLANs	200								
Concurrent Firewall Conns[2]	400 K								
Max. Physical Interfaces	Unlimited								
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*							
Min. RAM	1 GB								

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table 9 ASA 5550 Adaptive Security Appliance License Features

ASA 5550	Base License									
Users, concurrent	Unlimited									
Security Contexts	2	Optional licenses:								
		5	*10*	*20*	*50*					
VPN Sessions[1]	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	*Optional Licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	5000
VPN Load Balancing	Supported									
Failover	Active/Standby or Active/Active									
GTP/GPRS	None	*Optional license: Enabled*								
Max. VLANs	250									
Concurrent Firewall Conns[2]	650 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*								
Min. RAM	4 GB									

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the adaptive security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Open Caveats

Table 10 lists the open caveats for Version 7.2(5). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 10 Open Caveats in Version 7.2(5)

Caveat ID	Description
CSCsk45220	Regex used in CLI command filtering causes device reload
CSCsk48344	Inspect http is not matching server response fields
CSCsl04448	Cannot remove url-server despite having removed url-block cmd
CSCso28374	Monitoring graphs will not display historical values
CSCsv22198	Traceback when downgraded from 8.2.0.167 to 7.2.2
CSCsx64778	show memory in a context shows incorrect memory usage
CSCsy82284	IKE FSM stuck in MM_WAIT_DELETE because of QM stuck
CSCsy93944	Traceback on ACL modify: assertion "status" at "stride_terminal_node.c"
CSCsz59846	Capture: Backport CL58139 to Boston Branch
CSCte16295	system does not show correct uptime, but contexts do
CSCte61760	APCF not accepting http-scheme as condition
CSCte74580	Traceback in Thread Name: arp_timer
CSCtf23134	ASA 7.2.4 - multicontext - intermittent concurrent write failure
CSCtf23147	ASA/PIX may generate an ACK packet using TTL received by sender
CSCtf28466	ASA Fails to assign available addresses from local pool
CSCtf95080	ASA: Traceback in Thread Name Dispatch Unit
CSCtg05446	Traceback in Thread Name: Dispatch Unit
CSCtg48603	ASA traceback in Thread Name: Dispatch Unit

Resolved Caveats

Table 11 lists the resolved caveats for Version 7.2(5). If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 11 Resolved Caveats in Version 7.2(5)

Caveat ID	Description
CSCsm81114	traceback with session-timeout %n with radius115 suite
CSCsv52239	ASA may traceback with certain HTTP packets
CSCsx23387	Recoverable crash condition within aware http server
CSCta38452	ICMP unreachable dropped with unique Nat configuration

Table 11 Resolved Caveats in Version 7.2(5) (continued)

Caveat ID	Description
CSCtb20340	Removed ACL permits inbound packets
CSCtb38344	ASA tracebacks in Thread Name: vPif_stats_cleaner
CSCtc06171	L2TP/IPSec not being assigned to correct group-policy using Radius
CSCtc27448	ASA failovers when Management interface resets
CSCtc77567	MU portmap suite causes ASA to tracekback with call credentials null
CSCte23816	Telnet NOOP command sent to ASA cause next character to be dropped

Related Documentation

For additional information on the Cisco ASA 5500 series adaptive security appliances, see the following URL on Cisco.com:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation and Submitting a Service Request

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

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

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

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