



Cisco ASA 5500 Series Release Notes Version 7.2(4)

April 2008

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Supported Platforms and Feature Licenses, page 4](#)
- [New Features, page 7](#)
- [Important Notes, page 10](#)
- [Caveats, page 10](#)
- [Related Documentation, page 21](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 21](#)

Introduction

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 of the new features, see [New Features, page 7](#).



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

© 2007 Cisco Systems, Inc. All rights reserved.

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.

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 2](#)
- [Determining the Software Version, page 2](#)
- [Upgrading to a New Software Version, page 3](#)

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the adaptive security appliance.

Table 1 DRAM Memory Requirements

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

All adaptive security appliances require a minimum of 64 MB of internal CompactFlash.

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



Note

If using 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 (CDC) login, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

**Note**

ASA and ASDM images must be compatible, for example ASA Version 7.2(4) is compatible to ASDM Version 5.2(4). ASDM will not work with an incompatible platform 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(4), you must perform the following steps:

-
- Step 1** Load the new 7.2(4) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
 - Step 2** Reload the device so that it uses the 7.2(4) image.
 - Step 3** Load the new ASDM 5.2.(x) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
 - 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(4) 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/public/sw-center/index.shtml>
 - 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/public/sw-center/index.shtml>
 - 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
```

Supported Platforms and Feature Licenses

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

- ASA 5505, [Table 2](#)
- ASA 5510, [Table 3](#)
- ASA 5520, [Table 4](#)
- ASA 5540, [Table 5](#)
- ASA 5550, [Table 6](#)



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 2 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Users, concurrent ¹	10	<i>Optional Licenses:</i> 50 Unlimited	10	<i>Optional Licenses:</i> 50 Unlimited
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	<i>Optional License: 10</i>	2	<i>Optional License: 10</i>
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)	<i>Optional license:</i> <i>Strong (3DES/AES)</i>	Base (DES)	<i>Optional license:</i> <i>Strong (3DES/AES)</i>
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 3 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License					Security Plus						
Users, concurrent	Unlimited					Unlimited						
Security Contexts	No support					2	<i>Optional Licenses:</i>					
							5					
VPN Sessions ¹	250 combined IPSec and WebVPN					250 combined IPSec and WebVPN						
Max. IPSec Sessions	250					250						
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>				2	<i>Optional Licenses:</i>					
		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						
Concurrent Firewall Conns ²	50 K					130 K						
Max. Physical Interfaces	Unlimited					Unlimited						
Encryption	Base (DES)		<i>Optional license: Strong (3DES/AES)</i>			Base (DES)		<i>Optional license: Strong (3DES/AES)</i>				
Min. RAM	256 MB					256 MB						

- 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.
- 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 4 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License								
Users, concurrent	Unlimited							Unlimited	
Security Contexts	2	<i>Optional Licenses:</i>							
		5	10	20					
VPN Sessions ¹	750 combined IPSec and WebVPN								
Max. IPSec Sessions	750								
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>							
		10	25	50	100	250	500	750	
VPN Load Balancing	Supported								
Failover	Active/Standby or Active/Active								
GTP/GPRS	None		<i>Optional license: Enabled</i>						
Max. VLANs	150								
Concurrent Firewall Conns ²	280 K								
Max. Physical Interfaces	Unlimited								

Table 4 ASA 5520 Adaptive Security Appliance License Features (continued)

ASA 5520	Base License	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
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 5 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									
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	<i>Optional license: Enabled</i>								
Max. VLANs	200									
Concurrent Firewall Conns ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>								
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 6 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

Table 6 ASA 5550 Adaptive Security Appliance License Features (continued)

ASA 5550	Base License	
VPN Load Balancing	Supported	
Failover	Active/Standby or Active/Active	
GTP/GPRS	None	<i>Optional license: Enabled</i>
Max. VLANs	250	
Concurrent Firewall Conns ²	650 K	
Max. Physical Interfaces	Unlimited	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
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.

New Features

This section lists the new features for Version 7.2(4). For new feature support in ASDM 5.2(4), please refer to the Cisco ASDM Release Notes Version 5.2(4).

Application Profile Customization Framework

You can now use an Application Profile Customization Framework (APCF) script to modify the HTTP version in the HTTP header for clientless SSL VPN sessions. You might need to do so to view websites that work only if HTTP/1.1 is disabled in the browser, an impractical task to perform manually in large installations with multiple clients.

An APCF is an XML-based rule set for Clientless SSL VPN. It lets the security appliance handle non-standard applications and web resources so they display correctly over a Clientless SSL VPN connection. You can store APCF profiles on the security appliance flash memory, or on an HTTP, HTTPS, or TFTP server. Use either ASDM or the **apcf** command in webvpn mode to identify and locate an APCF profile that you want to load on the security appliance.



Note

We recommend that you configure an APCF profile only with the assistance of Cisco personnel.

capture command Enhancement

The **capture asp type asp-drop all** command captures all packets that the adaptive security appliance drops, including those dropped due to security checks.

clear conn Command

The **clear conn** command was added to remove connections.

IPv6 Multicast Listener Discovery Protocol v2 Support

The ASA adaptive security appliance now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. ASA becomes a multicast address listener, or a host, but not a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only.

The following commands support this feature:

- [show ipv6 mld Command](#)
- [debug ipv6 Command Enhancement](#)
- [show debug ipv6 mld Command Enhancement](#)

clear ipv6 mld traffic Command

The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters. the syntax is as follows:

```
clear ipv6 mld traffic
```

show ipv6 mld Command

The **show ipv6 mld** command allows you to display all the Multicast Listener Discovery traffic counters. the syntax is as follows:

```
show ipv6 mld traffic
```

debug ipv6 Command Enhancement

The enhancement to the **debug ipv6** command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly. This enhancement adds the **mld** option.

```
debug ipv6 {icmp | interface | mld | nd | packet | routing}
```

show debug ipv6 mld Command Enhancement

The enhancement to the **show debug ipv6** command allows the user to display whether **debug ipv6 mld** is enabled or disabled.

```
show debug ipv6 mld
```

MIB Enhancement

The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely.

Native VLAN Support on ASA 5505 Trunk Ports

You can now allow native VLANs on a trunk port (see the **switchport trunk native vlan** command).

QoS Traffic Shaping

If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the **shape** command. See also the **crypto ipsec security-association replay** command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms.

show asp drop Command Enhancement

The **show asp drop** command now displays the **capture asp-drop type** keywords. This enhancement displays the particular capture type as part of the output of the **show asp drop** command.

A timestamp was also added indicating when the last time the asp drop counters were cleared.

show asp table classify hits Command Enhancement

The **hits** option was added to the **show asp table classify** command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the **show asp table classify** command.

TCP Normalization Enhancements

You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.

- TCP invalid ACK check (the **invalid-ack** command)
- TCP packet sequence past window check (the **seq-past-window** command)
- TCP SYN-ACK with data check (the **synack-data** command)

You can also set the TCP out-of-order packet buffer timeout (the **queue** command **timeout** keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.

The default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command).

The following non-configurable actions have changed from drop to clear for these packet types:

- Bad option length in TCP
- TCP Window scale on non-SYN
- Bad TCP window scale value
- Bad TCP SACK ALLOW option

TCP Urgent Flag Syslog

When the TCP urgent flag of a TCP packet is cleared and debugging is enabled, a syslog is generated: ASA-7-419003.

Timeout for SIP Provisional Media

You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command.

Important Notes

This section lists important notes.

Caveats

The following sections describe the caveats for the Version 7.2(4).

For your convenience in locating caveats in Cisco's 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 7.2(4)

Table 7 lists open caveats for Version 7.2(4).

Table 7 **Open Caveats**

DDTS Number	Software Version 7.2(4)	
	Corrected	Caveat
CSCsg44891	No	Traceback in tmatch compile thread
CSCsg71579	No	Programming assertion malloc.c:3822 on secondary after failover from pri
CSCsg99492	No	SASL GSSAPI-Kerberos authentication not happening with Sunone Server
CSCsh91747	No	SSL VPN stress cause SSL lib error. Function: DO_SSL3_WRITE
CSCsk19485	No	syslog TCP_CONN_END shows Reset-O for ASA generated TCP RST
CSCsk30698	No	PIX/ASA may stop generating syslogs all together
CSCsk45220	No	Regex used in CLI command filtering causes device reload
CSCsk48344	No	Inspect http is not matching server response fields
CSCsk89474	No	URL filtering not performed for u-turn vpn traffic
CSCsk95246	No	no router rip, followed by router rip & network cause vPifnum & tracebac
CSCsk96804	No	Traceback in Thread Name: Dispatch Unit with inspect h323
CSCsl04448	No	Cannot remove url-server despite having removed url-block cmd in 7.2.3
CSCsl10052	No	new L2TP sessions are denied after %ASA-4-403103 is seen in the logs
CSCsl18071	No	Windows Media Player can not play media file with/without L-2-L Ipsec
CSCsl22480	No	CIFS share not working for Clientless SSL VPN
CSCsl41515	No	ASA traceback in Dispatch Unit (Old pc 0x00223a67 ebp 0x018b12f8)
CSCsl52895	No	ASA 7.2.3 number of IPsec SA not replicated in failover unit
CSCsl82200	No	IPsec not encrypting after failover
CSCsl90215	No	Traceback may occur when access-list changes pushed from SolSoft
CSCsl95928	No	High CPU utilization due to OSPF
CSCsm16160	No	Traceback may occur in pix_flash_config_thread w/ dynamic DNS cfg'ed
CSCsm55447	No	ASA/WebVPN Citrix sessions randomly dropped
CSCsm55491	No	ASA Disconnects voice call when # key is entered
CSCsm55947	No	Failover interface missing from ifTable
CSCsm57291	No	ASA/PIX traceback due to memory corruption during IPsec SA deletion
CSCsm57303	No	Communication failure between ASA and AIP-SSM
CSCsm65019	No	Websense encryption is not supported error on ASA
CSCsm68957	No	SIP inspection not fixing-up addr in Refer-To replaces section
CSCsm69219	No	GTP: Drop GTP message creating PDP context when no filter
CSCsm69271	No	GTP: Drop GTP message based on message ID when permitted
CSCsm73923	No	SIP:session timeout when forwarding a call is improperly set
CSCsm77854	No	%ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error
CSCsm79787	No	drop for inspect skinny is not counted in show service-policy
CSCsm85872	No	snmp trap for PHYSICAL interface is not sent when a port goes down

Table 7 Open Caveats (continued)

DDTS Number	Software Version 7.2(4)	
CSCsm87233	No	Traffic flow stops on a wireless hand-off or a reconnect
CSCsm87892	No	ASA 5505 Interface Hangs
CSCsm92275	No	SQL inspection rewrites IP addresses embeded in SQL data
CSCsm92613	No	ASP drop capture missing type for vpn-handle-error
CSCso01003	No	Crypto accelerator errors seen in syslog
CSCso01629	No	RTSP inspection doesn't drop non-RTSP traffic with TCP/554
CSCso01702	No	SIP: RTP/RTCP pinholes are allocated unexpectedly between same interface
CSCso03582	No	Overrun counter increments when REINVITE is received
CSCso38699	No	CPU Hog when replicating config to standby unit
CSCso39525	No	failed to open ASA webvpn homepage
CSCso43026	No	Traceback in Thread Name: Dispatch Unit (Old pc 0x00223a67 ebp 0x018b)
CSCso43383	No	SIP:media xlate idle timer is not refreshed when receiving 200ok
CSCso45557	No	Traceback in tmatch compile thread (user assertion)

Resolved Caveats - Version 7.2(4)

Table 8 lists resolved caveats for Version 7.2(4).

Table 8 Resolved Caveats

DDTS Number	Software Version 7.2(4)	
	Corrected	Caveat
CSCsc98412	Yes	Pix console accounting doesn't appear in ACS Logged-In User report
CSCsd65922	Yes	webvpn acls should allow wildcard * hostnames
CSCsg48442	Yes	Ping through ASA fails when using interface PAT on PPPoE interface
CSCsh55107	Yes	DHCP relay fails when static translation for all hosts configured
CSCsh91283	Yes	Inspect SunRPC drops segmented packets
CSCsi14147	Yes	SSH conn drops while writing a file to ASA5505 file system
CSCsi35603	Yes	L2TP/IPSec sessions hanging when authenticating with EAP
CSCsi41346	Yes	user session and idle timeout values not honored by cut-thru-pxy
CSCsi49983	Yes	Periodic HW crypto errors 402123 & 402125 see with L2TP/IPSEC
CSCsi53577	Yes	OSPF goes DOWN after reload of VPN Peer
CSCsi55386	Yes	PKI: oosp malformed request error - OpenCA/OCSPD responder
CSCsi60244	Yes	webvpn_session struct is not correctly validated in failover code
CSCsi65122	Yes	Overlapping static with NAT exemption causes xlate errors on standby

Table 8 **Resolved Caveats (continued)**

DTS Number	Software Version 7.2(4)	
CSCsi68911	Yes	ASA may traceback when pushing rules from SolSoft - corrupted conn_set_t
CSCsi84143	Yes	Mem del-free-poisoner fails to svc alloc requests from the poisoned pool
CSCsi94163	Yes	PPPOE connection does not renegotiate immediatly after short disconnect
CSCsi98616	Yes	The TCP connections in SVC won't survive after consecutive failovers
CSCsj01643	Yes	IPSec VPN first auth fails when SDI SoftID is in Cleared PIN Mode
CSCsj12938	Yes	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj40648	Yes	Traceback in Thread Name: emweb/https
CSCsj41977	Yes	cert handling inconsistent between physical and LB interfaces
CSCsj43076	Yes	Logging into standby ASA via SSH fails
CSCsj49481	Yes	WebVPN: HTTPS Page not rendered correctly while HTTP works fine
CSCsj51849	Yes	cpu-hog observed in process nic status poll thread
CSCsj62231	Yes	traceback pix_flash_config_thread while booting with a 4K key ID cert
CSCsj66185	Yes	ASA: Switching primary and secondary unit can cause duplicate MAC
CSCsj66667	Yes	group-url hostname should not be case-sensitive
CSCsj78675	Yes	HTTP host header not included in PKI requests with terminal enrollment
CSCsj80196	Yes	Clientless WebVPN traffic not sent when matching crypto dynamic map ACL
CSCsj80563	Yes	ASA dynamic VPN match address disconnects some peers as duplicate proxy
CSCsj82105	Yes	ASA vulnerable to HTTP Splitting
CSCsj82370	Yes	WebVPN: OWA left pane unresponsive when trying to access the folders
CSCsj82413	Yes	QoS: class-map : match tunnel-group <grp-name> errors on reboot
CSCsj83531	Yes	Dynamic VPN phase 2 neg with ID_IPV4_ADDR_RANGE accepted as 0.0.0.0/0
CSCsj84405	Yes	Poison route causes default route in ASP routing table to be deleted
CSCsj86636	Yes	Frames offset and toolbar missing in mangled site
CSCsj90274	Yes	Citrix sessions randomly disconnect
CSCsj90479	Yes	IPS and fragments cause Traceback in Thread Name: Dispatch Unit
CSCsj91809	Yes	Clientless email proxy POP3S with Outlook 2007 not working
CSCsj92194	Yes	Implicit ACL 'Deny IP Any Any' Ignored on EasyVPN Client
CSCsj96831	Yes	half-closed tcp connection behaves as an absolute timer on ASA
CSCsj97241	Yes	80 byte block depletion with stateful failover enabled
CSCsj98458	Yes	LDAP CRL checking failure for Cert Chain
CSCsj98622	Yes	SIP: Not translate c= address if first m= has port 0 in SDP body
CSCsj99242	Yes	Assert: Traceback in Thread Name: Dispatch Unit
CSCsj99660	Yes	ASA CONSOLE TIMEOUT does not timeout
CSCsk00089	Yes	ASA 7.2 : Firewall-MIB : no snmp object for failover lan int status
CSCsk00547	Yes	Traceback in ci/console when modifying cmap inspection_default

Table 8 *Resolved Caveats (continued)*

DDTS Number	Software Version 7.2(4)	
CSCsk01426	Yes	URL filtering broken if multiple inspection enabled on same traffic
CSCsk03550	Yes	ASA: Route injected through RRI disappear after failover
CSCsk05432	Yes	PKI: Default attribute for an LDAP CRL query should include a binary CRL
CSCsk06989	Yes	WebVPN: Traceback in Unicorn while rewriting Java applets
CSCsk06996	Yes	Leak in vpnfol_fragdb:vpnfol_fragdb_rebuild on standby
CSCsk10156	Yes	VPN traffic with static PAT to outside ip address denied by outside ACL
CSCsk12859	Yes	ASA 8.0.2 Traceback under heavy loads of traffic
CSCsk13421	Yes	Firewall may traceback while capturing WebVPN Data
CSCsk18083	Yes	nat exemption access-list not checked for protocol or port when applied
CSCsk18084	Yes	cikeTunnelTable does not populate for some of the ISAKMP SA's
CSCsk19065	Yes	Excessive High CPU and packets drops when applying ACL to an interface
CSCsk19882	Yes	Memory leak in ASA due to WEBVPN compression
CSCsk25164	Yes	IPSec VPN Client Update not working for mac-> headend issue
CSCsk26830	Yes	Certificate authorization broken when using all DN fields as username
CSCsk27085	Yes	ASA 5505 switch stops forwarding arp packets to ASA
CSCsk28847	Yes	ASA only sends six (6) Radius IETF class 25 attributes for accounting
CSCsk28972	Yes	Traceback:Thread Name: IKE Daemon when connecting w/ certain certificate
CSCsk31007	Yes	IP: traceback in Thread Name: Dispatch Unit
CSCsk31129	Yes	SIP inspection breaks SIP authentication
CSCsk33925	Yes	WebVPN: Regression with OWA as a result of CSCsj82370
CSCsk36399	Yes	Traceback in PIX Garbage Collector (Old pc 0x008b619d ebp 0x0261ed60)
CSCsk37130	Yes	Clear button goes away too much from Login button
CSCsk38962	Yes	memory leak in webvpn failover
CSCsk39154	Yes	PIX/ASA dynamic l2l vpn does not work in 8.0.2.16
CSCsk39286	Yes	ASA5505:Setting Duplex causes a 5 or 6 second outage on the interface
CSCsk41454	Yes	Traceback in thread name: ssh
CSCsk43103	Yes	Traceback in Thread Name emweb/https
CSCsk43232	Yes	traceback with http traffic when url filtering and http inspect enabled
CSCsk44832	Yes	Primary does not become active when pri & sec are booted together
CSCsk45117	Yes	Traceback in webvpn_url_mangle.c
CSCsk45867	Yes	clear conf sec causes trace back on EIGRP thread
CSCsk45943	Yes	PIX: proxy-arps on all interfaces for the vpn-pool
CSCsk47949	Yes	ASDM hangs at 47% if packet losses on the network
CSCsk48199	Yes	Traceback in thread: Dispatch Unit (Old pc 0x0021eae7 ebp 0x01887690)
CSCsk48629	Yes	Traceback in Unicorn Proxy Thread (Old pc 0x00c82197 ebp 0x1782f93c)

Table 8 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(4)	
	Yes	
CSCsk49149	Yes	mem leak with inspect esmtp
CSCsk49506	Yes	Local-host for u-turn traffic on lowest sec level used for license limit
CSCsk50378	Yes	SSH to device produces traceback
CSCsk50879	Yes	L2TP with EAP authenticatio In use List count session leaking
CSCsk53985	Yes	locked up at Error reading tftp unspecified error
CSCsk54686	Yes	HT: WCCP with bypass configured at CE causes traceback
CSCsk55097	Yes	WebVPN: OWA new contact functionality not working
CSCsk58034	Yes	L2L tunnels come down sometimes in failover setup after failover
CSCsk58346	Yes	Memory leak when adding/removing nameif (sp_actions)
CSCsk59083	Yes	ASA 5505 failover: rebooted unit becomes active after reload
CSCsk59816	Yes	Traceback in the process Crypto CA when retrieving the CRL
CSCsk62411	Yes	Traceback with memory tracking enabled
CSCsk63982	Yes	ASA with EzVPN client does not send DHCP renew packets, tunnel flaps
CSCsk64117	Yes	CPU Hog seen generating RSA keys during SSH session establishment
CSCsk64428	Yes	High CPU when polling VPN MIBs via SNMP
CSCsk65211	Yes	ASA5505 inside interface w/23bit or smaller subnet mask becomes unstable
CSCsk65425	Yes	failing to verify OCSP for RemoteAccess VPN - EJBCA CA infrastructure
CSCsk65863	Yes	traceback in ppp_timer_thread
CSCsk65940	Yes	crashinfo file corrupted, extra text appended to bottom
CSCsk66924	Yes	ASDM: Monitoring Used memory records different stats history
CSCsk67715	Yes	During Ipsec negotiation, peer ip address is seen reversed in the debugs
CSCsk68658	Yes	ICMP (type 3 code 4) messages generated against ESP flow dropped by ASA
CSCsk68895	Yes	Traceback in thread name Dispatch Unit with IDS packet recv
CSCsk69878	Yes	ASA running 8.0.2 rejects DHCP leases less than 32 seconds
CSCsk70101	Yes	Adding/Removing subinterface causes memory leak
CSCsk70941	Yes	Traceback in Thread Dispatch Unit: snp_tcp_timeout_cb
CSCsk71006	Yes	ipv6 acl don't have acl options when using MPF
CSCsk71135	Yes	ASA 7.2.3 - Traceback in Unicorn Proxy Thread
CSCsk73724	Yes	ASA 5505 default route via dhcp setroute goes away after link flap
CSCsk76401	Yes	set connection decrement-ttl does not work for traceroute
CSCsk76770	Yes	vpn-filter may prevent renegotiation of the tunnel
CSCsk79263	Yes	On link flap, DHCP REQUEST sent only once
CSCsk79728	Yes	ASA5550 7.2.3 traceback with Dispatch Unit
CSCsk80789	Yes	RTSP inspection changes Media Player version to 0.0.0.0
CSCsk81616	Yes	PIX/ASA Traceback in 'dhcp_daemon'

Table 8 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(4)	
CSCsk83113	Yes	emweb memory accounting is incorrect
CSCsk83425	Yes	OSPF with Message digest fails, no adjacencies, shows allocation error
CSCsk84801	Yes	WCCP GRE packets decapsulated when passing through pix
CSCsk84808	Yes	Unable to remove WebVPN capture CLI, ERROR:Unable to get real-time
CSCsk85428	Yes	Traceback in scheduler
CSCsk85441	Yes	Traceback in thread https_proxy
CSCsk86002	Yes	Memory accounting for aaa chunks is incorrect
CSCsk87093	Yes	L2TP /EAP-TLS sessions disconnect with 734 error the first time
CSCsk88562	Yes	CSC-SSM: 1550-byte block depletion
CSCsk89639	Yes	Traceback with Thread Name: Checkheaps
CSCsk90689	Yes	telnet to the box and vpn tunnels fail due to 0-byte block depletion
CSCsk93067	Yes	no management-access Inside still allows telnet over IPsec tunnel
CSCsk95133	Yes	Traceback in Thread Unicorn Proxy related to WebVPN page rewrite
CSCsk97671	Yes	VPN client with NULL Encryption L2TP-IPsec behind NAT drops on 71st sec
CSCsk97830	Yes	Traceback in thread name Dispatch Unit
CSCs101053	Yes	ASA doesn't handle the multiple CPS entries in the Issuing CA cert
CSCs103985	Yes	ASA DHCP client unable to renew the IP address if DHCP ACK is lost
CSCs111321	Yes	ASA doesn't send coldStart trap when speed/duplex is fixed as 100/full
CSCs112010	Yes	flash memory corruption issues
CSCs112239	Yes	WebVPN: OWA 2K -> shortcuts pane does not load
CSCs112449	Yes	DHCP Client - remove minimum lease time restriction
CSCs112472	Yes	Traceback in emweb/https observed on ASA
CSCs115013	Yes	DHCPrelay broken with 2 DHCPrelay servers when second one out of service
CSCs117136	Yes	H323: Video breaks with inspection enabled
CSCs119419	Yes	enabling acl-netmask-convert wildcard does not accept acl with host
CSCs121500	Yes	Traceback with 'no capture <name>' for ISAKMP type capture
CSCs123542	Yes	User Certificate mappings against the whole field failing
CSCs126135	Yes	Memory leak when FTP filter is enabled
CSCs126200	Yes	ASA SSL VPN ACL bypass
CSCs126604	Yes	Traceback in Dispatch Unit with VPN (not ported to 7.2)
CSCs128306	Yes	PIX/ASA default route redistributed into EIGRP when explicitly disabled
CSCs129315	Yes	ASA-3-713902 appears on standby unit when disconnecting VPN connection
CSCs129851	Yes	ASA sends 0.0.0.0 as caller-id for command authorization
CSCs130307	Yes	PIX/ASA fails to install cert with an empty subject/issuer alt name ext
CSCs131908	Yes	ASA: SIP inspection drops SIP message 200 OK from 3rd party CosmoCall

Table 8 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(4)	
CSCs132225	Yes	Traceback in Thread Name: Checkheaps when Simultaneous login set to 1
CSCs132785	Yes	Traceback in Thread Name: pix_flash_config_thread
CSCs133600	Yes	Traceback when show service after removing global policy with police
CSCs133833	Yes	ASA shouldn't install default route learned from PPPoE into running-conf
CSCs134791	Yes	WebVPN: Traceback in Thread Name: Dispatch Unit
CSCs135591	Yes	Bulk skinny registration creates 2048 block leak
CSCs135603	Yes	Memory corruption with csc and nat testing
CSCs137767	Yes	Traceback when timeout with L2TP and delay-free-poisoner enabled
CSCs138314	Yes	HA: SNMP trap authentication replicated to standby improperly
CSCs140225	Yes	CPU usage eventually hits 90% and that causes call failures
CSCs140367	Yes	DDNS updates append duplicate domain name
CSCs141666	Yes	Crypto debug command should not dump keys as part of the SA
CSCs143246	Yes	L2TP with EAP authentication In use List count session slowly leaking
CSCs145763	Yes	Syslog message during config-replication: invalid function
CSCs149999	Yes	! used in downloadable ACL yields error unable to apply access list
CSCs151292	Yes	IPSEC VPN tunnel on ASA 8.0.3 fails every couple days
CSCs151797	Yes	ASA traceback in AAA thread
CSCs153995	Yes	5510 interface can be set to 1000Mbps with base license
CSCs155623	Yes	SNMP link trap varbind list missing values
CSCs156635	Yes	Input errors remains 0 even when CRC counts up
CSCs157533	Yes	setting privilege for capture does not affect "no capture"
CSCs159108	Yes	Auto-signon servers not inherited from DfltGrpPolicy
CSCs159247	Yes	Unable to request CRL for trustpoint with only ID certificate
CSCs159266	Yes	PKI: export/import of pkcs12 containing only ID cert fails
CSCs163265	Yes	Error message: Customization <> is in use, unable to remove
CSCs164946	Yes	5510 Ethernet interface fail speed auto negotiation when boot up
CSCs166538	Yes	ASA "hardware accelerator encountered an error (Invalid PKCS Type)"
CSCs166758	Yes	TCP intercept comes before ACL checks. All TCP ports appear open
CSCs167229	Yes	ASA: timeout sip_media is not working properly
CSCs168785	Yes	Confusing Error message when Interfaces have overlapping networks
CSCs168914	Yes	traceback when upgrading license
CSCs170685	Yes	Traceback in Thread Name: accept/http
CSCs171113	Yes	DDNS: conf mem w/ DDNS config causes traceback
CSCs173850	Yes	Traceback occurs when SIP session is active and switchover occurs twice
CSCs173906	Yes	Traceback on network command under rip config mode under load

Table 8 *Resolved Caveats (continued)*

DDTS Number	Software Version 7.2(4)	
	Yes	
CSCs174327	Yes	Traceback in fover_parse when editing ACL config
CSCs174571	Yes	l2tp over ipsec accounting and 4-113019 do not reports Rx / Tx bytes
CSCs175006	Yes	Traceback on entering command vpnclient nem-st-autoconnect
CSCs178110	Yes	Downloadable ACL does not get removed from memory in some scenarios
CSCs178638	Yes	stateful subinterface would not become Up, remains Failed
CSCs179211	Yes	Traceback: AAA task overflow when object-group acls and virtual telnet
CSCs182984	Yes	HT: Traceback proxy_block_cpy+829 at inspect/tcp_proxy_utils.c:108
CSCs183313	Yes	access-group sometimes take more than 10 min to execute
CSCs184122	Yes	Xlate timers for RTP/RTCP on ASA are always 30 seconds
CSCs184179	Yes	Traceback at ssh thread when working with 'capture'
CSCs184204	Yes	Xlate timers for RTP/RTCP on standby ASA aren't synchronized with active
CSCs185169	Yes	Inspect WAAS causing the memory leak
CSCs187918	Yes	IPSec: RESPONDER-LIFETIME not properly created
CSCs189105	Yes	Traceback when enabling blocks queue history w/ high load/low memory
CSCs189162	Yes	show cheakheaps displays negative number for total memory in use
CSCs189537	Yes	SIP: ASA improperly adds some value in From-tag when sending BYE
CSCs189653	Yes	SIP connection entry not be cleared after sip_disconnect timeout
CSCs191005	Yes	Traceback in Thread Name: CP Processing under TCP/UDP load
CSCs191061	Yes	Traceback while adding regex with Sysrend and Udpnd SIP traffic load
CSCs193003	Yes	TACACS+ allow enable command but ASA output Command authorization fail
CSCs193495	Yes	SIP: ASA shows 4xx response message as 500 on debug sip
CSCs195043	Yes	PIX/ASA: L2TP/IPsec needs both ipsec and l2tp-ipsec in group-policy
CSCs195244	Yes	Traceback in Dispatch Unit caused by rapid connection successions
CSCs195856	Yes	DHCP learned default route not in route table if other DHCP interfaces
CSCs196219	Yes	SIP:ASA fails to associate re-invites to the original SIP session
CSCs196502	Yes	SIP: sess is not kept around for ACK in response to non2xx final RESP
CSCs197161	Yes	RTSP connections failing when RTSP inspection enabled
CSCs199322	Yes	Traceback at ids_put in Thread Name: Dispatch Unit
CSCsm00894	Yes	ASA LDAP MAP fails on IETF-Radius-Framed-IP-Address
CSCsm02280	Yes	ASA keeps registering but does not send Register packets
CSCsm02939	Yes	Memory leak while processing SSL transactions
CSCsm03751	Yes	SNMP Coldstart Trap is Only Sent to the Last Configured NMS
CSCsm05055	Yes	PIX traceback occurs when 'established udp 0 0' is enabled
CSCsm05181	Yes	traceback in Thread: vpnfol_thread_msg
CSCsm07888	Yes	Authenticator value on retransmitted RADIUS request pkt changed

Table 8 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(4)	
CSCsm09584	Yes	EAP l2tp authentication fails if mschapv2 is configured on the same TG
CSCsm10187	Yes	Both Pri/Sec ASA don't send coldstart trap when both units are available
CSCsm14283	Yes	ICMP (type 3, code 4) packet not returned from PPPoE interface
CSCsm17247	Yes	H323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT
CSCsm18372	Yes	show input hardware queue max counters incorrect
CSCsm18437	Yes	clear interface doesn't clear max queue counter
CSCsm22002	Yes	Traceback in qos/qos_rate_limiter while processing pakt with TCP flow
CSCsm22781	Yes	PIX/ASA: RPF(reverse path forwarding)chk fails when PMTUD packet is sent
CSCsm23689	Yes	SSL session cache size is too large for some platforms
CSCsm25189	Yes	ASA demonstrates inconsistent behavior for different kind of SIP packets
CSCsm26011	Yes	Active ASA traceback occurs when replicating large number of WebVPN sessions
CSCsm28270	Yes	ASA5550 only: all interfaces fail to pass data with 7.2.3.16-17-18
CSCsi62588	Yes	Dest unicast address to multicast address NAT not working in 7.x
CSCsm31973	Yes	ASA snmpwalk on cefcMIBEnableStatusNotification : value returned : 2
CSCsm32507	Yes	External group policy authentication failure with password-management
CSCsm32972	Yes	SNMP Counters Get Stuck on Repeated Polls
CSCsm36660	Yes	DHCP Server: ASA must send dhcp decline if dhcp proposes in-use address
CSCsm37151	Yes	skinny inspection blocking pinhole w/ high skinny load on rsvp agent
CSCsm39684	Yes	Boston AT: IPSEC rekey does not occur
CSCsm39781	Yes	ASA High CPU under certain configuration conditions
CSCsm40251	Yes	ASDM falsely shows interface status as down/down
CSCsm41986	Yes	Need to handle fragmented IP packets with 8-byte first frag
CSCsm44660	Yes	5505 in EzVPN mode cannot establish a VPN tunnel to the head end ASA
CSCsm45722	Yes	SIP:Caller's RTP/RTCP timeout should set to sip_invite
CSCsm46182	Yes	DHCP Client: ASA as dhcp client does not renew when lease expires
CSCsm47185	Yes	Traceback when an interface configured for IPV6 changes to link up state
CSCsm48386	Yes	ASA with local command authorization not able to download conf from AUS
CSCsm48412	Yes	SSL rec paramater list continues to grow without boundaries
CSCsm50494	Yes	ASA is not able to process CRL with extension CRL number > 65535
CSCsm51093	Yes	Cannot establish WebVPN session to ASA-5550 - memory allocation error
CSCsm51459	Yes	GTP: IMSI prefixing doesn't work with 2 digit MNC
CSCsm56957	Yes	Traceback occurs in Dispatch Unit with 8.0.3
CSCsm59304	Yes	SIP: INVITE not passing after failover
CSCsm61494	Yes	ASA may open unknown port "50195"
CSCsm61775	Yes	ASA creates unnecessary xlate after a voice device hands over

Table 8 *Resolved Caveats (continued)*

DDTS Number	Software Version 7.2(4)	
CSCsm62831	Yes	SIP:Half-open xlate entry is generated by ASAs
CSCsm63108	Yes	Block 2048 depleted with url-filtering enabled ASA Websense
CSCsm64838	Yes	Traceback occurs in Dispatch Unit with 7.2.3.15 and L2TP/PPP
CSCsm66982	Yes	PIX/ASA: L2TP session should not establish when authorization fails
CSCsm68097	Yes	ASA 8.0.x - SSH resource exhausted preventing further sessions
CSCsm70077	Yes	SIP:Local/Local connection entry is created
CSCsm70101	Yes	Unable to apply priority command in policy map while configuring QOS-ASA
CSCsm70246	Yes	SIP:ASA duplicates "mi" connection when receiving REINVITE
CSCsm70860	Yes	Difference of total vpn session via OID SNMP and vpn-sessiondb summary
CSCsm73565	Yes	Traceback in Thread Name Dispatch Unit during network scan
CSCsm73654	Yes	%ASA-1-111111 appears when both active/standby units reload at once
CSCsm75212	Yes	ASA Traceback Thread Name: IKE Daemon (Old pc 0x0050a493 ebp 0x0346e)
CSCsm77958	Yes	Traceback in "IP Thread" when clientless webvpn is started
CSCsm82753	Yes	Phase 2 fails if PFS is required. - ASA -IOS l2tp IPSEC
CSCsm82887	Yes	FO: IPsec RA session not replicated if addr pool defined in group policy
CSCsm83098	Yes	SIP:Fails to create m connection when ACK to 407 is lost
CSCsm83636	Yes	CPU hog during config sync
CSCsm85736	Yes	shutdown interface e0/6 triggers interface e0/0 shutdown on ASA5505
CSCsm88116	Yes	SIP:Fails to update to-tag when received no-2xx response
CSCsm91261	Yes	Traceback in 'ssh' thread aossipov
CSCsm92266	Yes	Traceback may occur when AAA command authorization is enabled
CSCsm93071	Yes	5505: 'no buffer' and 'input error' not correct on InternalData0/0
CSCsm93115	Yes	Memory leak in DMA free crypto memory 8.0.3.6
CSCso00670	Yes	Move ssl debug commands from menu to real CLI
CSCso01090	Yes	ASA5505:copy config from disk0:/ to running-config makes int e0/0 down
CSCso03100	Yes	SSL cache entries timing out prematurely
CSCso05327	Yes	Cert from 3k imported into ASA causes Hardware error on use
CSCso10078	Yes	Traceback occurs when wr mem command is entered
CSCso15583	Yes	Traceback when many remote peers try to establish ipsec L2L tunnels
CSCso17578	Yes	VPNLB: WebVPN client cannot connect to VPN load-balancing cluster
CSCso17920	Yes	SIP media connection cannot be created more than 13 when PBX is used
CSCso20009	Yes	ASA DHCP proxy not working for L2TP connections
CSCso24103	Yes	Delivering shape average command through https failed
CSCso33873	Yes	L2TP/IPsec connection cannot pass data
CSCso40520	Yes	re-INVITE is dropped when it's exceeded 119ch after establishing 400ch

Table 8 **Resolved Caveats (continued)**

Software Version 7.2(4)		
DDTS Number		
CSCso41232	Yes	traceback while executing 'show skinny'
CSCso42643	Yes	WebFO: WebVPN sessions not replicated until after FO forced

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 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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0903R)

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.

©2008 Cisco Systems, Inc. All rights reserved.

