



Cisco ASA 5500 Series Release Notes Version 7.0(8)

June 2008

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Important Notes, page 5](#)
- [Caveats, page 7](#)
- [Related Documentation, page 12](#)
- [Obtaining Documentation and Submitting a Service Request, page 12](#)

Introduction

The Cisco ASA 5500 series adaptive security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability. This release introduces enhancements to the following areas: firewall services, and management/monitoring.

For more information on all the new features, see [New Features, page 3](#).

Additionally, the Cisco ASA 5500 series adaptive security appliance software supports Adaptive Security Device Manager. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the adaptive security appliance, then used to configure, monitor, and manage the device.



Americas Headquarters:

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

© 2008 Cisco Systems, Inc. All rights reserved.

System Requirements

The sections that follow list the system requirements for operating a Cisco ASA 5500 series adaptive security appliance. This section includes the following topics:

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

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the Cisco ASA 5500 series adaptive security appliance.

Table 1 *DRAM Memory Requirements*

ASA Model	DRAM Memory
ASA 5510	256 MB
ASA 5520	512 MB
ASA 5540	1 GB

All Cisco ASA 5500 series adaptive security appliances require a minimum of 64 MB of internal CompactFlash.

Determining the Software Version

Use the **show version** command to verify the software version of your Cisco ASA 5500 series adaptive security appliance.

Upgrading to a New Software Release

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

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

New Features

Released: June 2, 2008

Table 2 lists the new features for ASA and PIX Version 7.0(8).

Table 2 **New Features for ASA and PIX Version 7.0(8)**

Feature	Description
Firewall Features	
EtherType ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Remote Access Features	
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Connection Features	
clear conn Command	The clear conn command was added to remove connections. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Fragment full reassembly	The fragment command was enhanced with the reassemble full keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Troubleshooting and Monitoring Features	
capture command Enhancement	The capture type asp-drop drop_code command now accepts all as the <i>drop_code</i> , so you can now capture all packets that the adaptive security appliance drops, including those dropped due to security checks. <i>Also available in Version 7.2(4) and 8.0(4).</i>
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the clear asp drop command). It also displays the drop reason keywords next to the description, so you can easily use the capture asp-drop command using the keyword. <i>Also available in Version 7.2(4) and 8.0(4).</i>
clear asp table Command	Added the clear asp table command to clear the hits output by the show asp table commands. <i>Also available in Version 7.2(4) and 8.0(4).</i>
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. <i>Also available in Version 7.2(4) and 8.0(4).</i>

Table 2 New Features for ASA and PIX Version 7.0(8) (continued)

Feature	Description
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept. <i>Also available in Version 7.2(4) and 8.0(4).</i>
memory tracking Commands	The following new commands are introduced in this release: • memory tracking enable—This command enables the tracking of heap memory requests. • no memory tracking enable—This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system. • clear memory tracking—This command clears out all currently gathered information but continues to track further memory requests. • show memory tracking—This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address. • show memory tracking address—This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool. • show memory tracking dump—This command shows the size, location, partial callstack, and a memory dump of the given memory address. • show memory tracking detail—This command shows various internal details to be used in gaining insight into the internal behavior of the tool. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Failover Features	
failover timeout Command	The failover timeout command no longer requires a failover license for use with the static nailed feature. <i>Also available in Version 7.2(4) and 8.0(4).</i>
Usability Features	
show access-list Output	Expanded access list output is indented to make it easier to read. <i>Also available in Version 7.2(4) and 8.0(4).</i>
show arp Output	In transparent firewall mode, you might need to know whether an ARP entry is statically configured or dynamically learned. ARP inspection drops ARP replies from a legitimate host if a dynamic ARP entry has already been learned. ARP inspection only works with static ARP entries. The show arp command now shows each entry with its age if it is dynamic, or no age if it is static. <i>Also available in Version 7.2(4) and 8.0(4).</i>
show conn Command	The syntax was simplified to use source and destination concepts instead of “local” and “foreign.” In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like foreign and port to determine the destination address and port.

Important Notes

This section lists important notes related to Version 7.0(8).

Common Criteria EAL4+

For information on common criteria EAL4+, see the *Installation and Configuration for Common Criteria EAL4 Evaluated Cisco Adaptive Security Appliance, Version 7.0(6)* document.

FIPS 140-2

Cisco ASA 5510, 5520, and 5540 adaptive security appliances are FIPS 140-2, Level 2 validated. You can view the official certificate (#655) via the following URL:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt655.pdf>

See the *FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5500 Series Security Appliance* at the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa70/hw/fips_asa.html

Hostname and Domain Name Limitation

When using ASDM, the hostname and domain names combined should not be more than 63 characters long. If the hostname and domain names combined is more than 63 characters, you will get an error message.

WebVPN ACLS and DNS Hostname

When a deny webtype URL ACL (DNS-based) is defined, but the DNS-based URL is not reachable, a “DNS Error” popup is displayed on the browser. The ACL hitcounter is also not incremented.

If the URL ACL is defined by an IP instead of DNS name, then the traffic flow hitting the ACL will be recorded in the hitcounter and a “Connection Error” is displayed on the browser.

Proxy Server and ASA

If WebVPN is configured to use an HTTP(S)-proxy server to service all requests for browsing HTTP and/or HTTPS sites, the client/browser may expect the following behavior:

1. If the ASA cannot communicate with the HTTPS or HTTPS proxy server, a “connection error” is displayed on the client browser.
2. If the HTTP(S) proxy cannot resolve or reach the requested URL, it should send an appropriate error to the ASA, which in turn will display it to the client browser.

Only when the HTTP(S) proxy server notifies the ASA of the inaccessible URL, can the ASA notify the error to the client browser.

Mismatch PFS

The PFS setting on the VPN client and the adaptive security appliance must match.

ACS Radius Authorization Server

When certificate authentication is used in conjunction with Radius authorization, the ACS server sends a bogus Group=CISCOACS:0003b9c6/5a940131/username and is displayed in the vpn-session database.

Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The Cisco ASA 5500 series adaptive security appliance Outbound/Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefit:

- ACE Insertion capability - System configuration and management is greatly simplified by the ACE insertion capability that allows users to add, delete or modify individual ACEs.

User Upgrade Guide

- For a list of deprecated features, and user upgrade information, go to the following URL:
http://www.cisco.com/en/US/docs/security/asa/asa70/vpn3000_upgrade/upgrade/guide/migr_vpn.html

Features not Supported in Version 7.0

The following features are not supported in Version 7.0(8):

- PPPoE
- L2TP over IPSec
- PPTP

MIB Supported

For information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode. For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

Caveats

The following sections describe the caveats for the Version 7.0(8).

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

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

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

Open Caveats

Table 3 lists the open caveats for Version 7.0(8).

Table 3 **Open Caveats**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCso76065	No	Traceback when viewing access-list that is simultaneously deleted
CSCsq06129	No	PIX/ASA: Standby unit may reboot without recording a crash file
CSCsj32989	No	ASA traceback when running 100 user Avalanche webvpn goodput test
CSCso98107	No	HTTPS url stuck after large config deployment from CSM
CSCsl55476	No	HT transparent: Secondary gig3/0 port goes orange for sometime after FO
CSCsq43878	No	multi mode A/A failover write standby will see crypto CLI error in stby
CSCsj61214	No	Lower cpu-hog syslog 711002 from Level 7 to Level 4
CSCsm05455	No	Xlate timers for RTP/RTCP in version 7.0 are always 30 seconds
CSCsm20204	No	Extended ping command with no ip specified causes stuck thread
CSCso65837	No	"write mem" from HTTPS adds no monitor-interface CLIs to startup config
CSCeh98117	No	Tunnel-group/ldap-login passwords in cleartext when viewed with more
CSCsd22469	No	DHCP relay and DHCP proxy conflict when both enabled
CSCsq46179	No	Longer timer needed for eToken credential entry

Resolved Caveats

Table 4 lists the resolved caveats for Version 7.0(8).

Table 4 *Resolved Caveats*

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCeg00330	Yes	DHCP relay: ACK in reply to INFORM may be dropped
CSCsc98412	Yes	Pix console accounting doesn't appear in ACS Logged-In User report
CSCsd65922	Yes	webvpn acs should allow wildcard * hostnames
CSCsg61719	Yes	SNMP: Coldstart Trap is not sent
CSCsg96247	Yes	ASA traceback - RSA keypair generation SSH function calls
CSCsh55107	Yes	DHCP relay fails when static translation for all hosts configured
CSCsh74009	Yes	Show/Clear uauth command will not work for username with spaces
CSCsh91283	Yes	Inspect SunRPC drops segmented packets
CSCsi08317	Yes	PIX using Authentication Proxy and Wildcard causes Certificates error
CSCsi46292	Yes	SNMP coldstart trap not sent in failover scenario
CSCsi49983	Yes	Periodic HW crypto errors 402123 & 402125 see with L2TP/IPSEC
CSCsi53577	Yes	OSPF goes DOWN after reload of VPN Peer
CSCsi65122	Yes	Overlapping static with NAT exemption causes xlate errors on standby
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
CSCsj03278	Yes	Traceback in Dispatch Unit thread (page fault)
CSCsj03706	Yes	activex or java filter suppresses the syslog message 304001
CSCsj05830	Yes	Syslog 405001 reports incorrect IP when arp collision detected
CSCsj12938	Yes	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj13797	Yes	SSH connection fails when first server in AAA group is unreachable
CSCsj20942	Yes	ASA stops accepting IP from DHCP when DHCP Scope option is configured
CSCsj31537	Yes	Interface keyword in ACL not permitting traffic
CSCsj33267	Yes	traceback in SSH/console with show runn access-list <webtype-CL-name>
CSCsj37564	Yes	Traceback in Thread Name: IP Thread
CSCsj37760	Yes	h323 inspection does not open RTP pinholes in certain scenarios
CSCsj40295	Yes	Policy NAT not functioning properly after boot
CSCsj43076	Yes	Logging into standby ASA via SSH fails.
CSCsj44098	Yes	traceback caused by gtp inspect handling bad packets
CSCsj46062	Yes	Inconsistent state of failover pair may exist during config sync
CSCsj46729	Yes	ASA: Active and Standby unit have the same MAC address after failover
CSCsj56378	Yes	Traceback in Thread Name: Crypto CA with LDAP CRL query
CSCsj72903	Yes	Additional sanitization needed for syslog message %ASA-5-111008

Table 4 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsj77560	Yes	Traceback in Thread Name: IKE Daemon with CRL checking
CSCsj78675	Yes	HTTP host header not included in PKI requests with terminal enrollment
CSCsj80563	Yes	ASA dynamic VPN match address disconnects some peers as duplicate proxy
CSCsj82105	Yes	ASA vulnerable to HTTP Splitting
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
CSCsj90479	Yes	IPS and fragments cause Traceback in Thread Name: Dispatch Unit
CSCsj91809	Yes	Clientless email proxy POP3S with Outlook 2007 not working
CSCsj96831	Yes	half-closed tcp connection behaves as an absolute timer on ASA
CSCsj99660	Yes	ASA CONSOLE TIMEOUT does not timeout
CSCsk00547	Yes	Traceback in ci/console when modifying cmap inspection_default
CSCsk00589	Yes	Traceback in Thread Name: Dispatch Unit
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
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
CSCsk18083	Yes	nat exemption access-list not checked for protocol or port when applied
CSCsk19065	Yes	Excessive High CPU and packets drops when applying ACL to an interface
CSCsk28972	Yes	Traceback:Thread Name: IKE Daemon when connecting w/ certain certificate
CSCsk39154	Yes	PIX/ASA dynamic l2l vpn does not work in 8.0.2.16
CSCsk41454	Yes	Traceback in thread name: ssh
CSCsk43103	Yes	Traceback in Thread Name emweb/https
CSCsk44832	Yes	Primary does not become active when pri & sec are booted together
CSCsk45943	Yes	PIX: proxy-arps on all interfaces for the vpn-pool
CSCsk59083	Yes	ASA 5505 failover: rebooted unit becomes active after reload
CSCsk59816	Yes	Traceback in the process Crypto CA when retrieving the CRL
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
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

Table 4 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsk71006	Yes	ipv6 acl don't have acl options when using MPF
CSCsk76770	Yes	vpn-filter may prevent renegotiation of the tunnel
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'
CSCsk85428	Yes	Traceback in scheduler
CSCsk86002	Yes	Memory accounting for aaa chunks is incorrect
CSCsk89639	Yes	Traceback with Thread Name: Checkheaps
CSCsk90689	Yes	telnet to the box and vpn tunnels fail due to 0-byte block depletion
CSCsk96804	Yes	Traceback in Thread Name: Dispatch Unit with inspect h323
CSCsk97671	Yes	VPN client with NULL Encryption L2TP-IPSec behind NAT drops on 71st sec
CSCsl01053	Yes	ASA doesn't handle the multiple CPS entries in the Issuing CA cert
CSCsl12010	Yes	flash memory corruption issues
CSCsl12449	Yes	DHCP Client - remove minimum lease time restriction
CSCsl17136	Yes	H323: Video breaks with inspection enabled
CSCsl19419	Yes	enabling acl-netmask-convert wildcard does not accept acl with host
CSCsl23542	Yes	User Certificate mappings against the "whole field" failing
CSCsl26604	Yes	Traceback in Dispatch Unit with VPN (not ported to 7.2)
CSCsl28306	Yes	PIX/ASA default route redistributed into EIGRP when explicitly disabled
CSCsl29315	Yes	Syslog 713902 appears on standby unit when disconnecting VPN connection
CSCsl30307	Yes	PIX/ASA fails to install cert with an empty subject/issuer alt name ext
CSCsl33600	Yes	Traceback when show service after removing global policy with police
CSCsl37767	Yes	Traceback when timeout with L2TP and delay-free-poisoner enabled
CSCsl38314	Yes	HA: SNMP trap authentication replicated to standby improperly
CSCsl55623	Yes	SNMP link trap varbind list missing values
CSCsl56635	Yes	Input errors remains 0 even when CRC counts up
CSCsl57533	Yes	setting privilege for capture does not affect "no capture"
CSCsl59247	Yes	Unable to request CRL for trustpoint with only ID certificate
CSCsl59266	Yes	PKI: export/import of pkcs12 containing only ID cert fails
CSCsl66758	Yes	TCP intercept comes before ACL checks. All TCP ports appear open
CSCsl68785	Yes	Confusing Error message when Interfaces have overlapping networks
CSCsl70685	Yes	Traceback in Thread Name: accept/http
CSCsl73850	Yes	Traceback occurs when SIP session is active and switchover occurs twice
CSCsl74327	Yes	Traceback in fover_parse when editing ACL config
CSCsl75006	Yes	Traceback on entering command "vpnclient nem-st-autoconnect"

Table 4 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCsl78638	Yes	stateful subinterface would not become Up, remains Failed
CSCsl79211	Yes	Traceback: AAA task overflow when object-group acls and virtual telnet
CSCsl82200	Yes	IPSec not encrypting after failover
CSCsl84179	Yes	Traceback at ssh thread when working with 'capture'
CSCsl87918	Yes	IPSec: RESPONDER-LIFETIME not properly created
CSCsl93003	Yes	TACACS+ allow enable command but output has "Command authorization fail"
CSCsl95244	Yes	Traceback in Dispatch Unit caused by rapid connection successions
CSCsl95856	Yes	DHCP learned default route not in route table if other DHCP interfaces
CSCsl97161	Yes	RTSP connections failing when RTSP inspection enabled
CSCsl99322	Yes	Traceback at ids_put in Thread Name: Dispatch Unit
CSCsm00894	Yes	LDAP map fails for IETF-Radius-Framed-IP-Address
CSCsm05055	Yes	PIX traceback occurs when 'established udp 0 0' is enabled
CSCsm07888	Yes	Authenticator value on retransmitted RADIUS request pkt changed
CSCsm17247	Yes	H323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT
CSCsm18437	Yes	clear interface doesn't clear max queue counter
CSCsm22002	Yes	Traceback in qos/qos_rate_limiter while processing pakt with TCP flow
CSCsm28529	Yes	page fault in fover_parse - eip og_rem_objgrp with DFP
CSCsm29337	Yes	Dest unicast address to multicast address NAT not working in 7.x
CSCsm30926	Yes	ASA: Traceback with high voice traffic and voice inspection
CSCsm31973	Yes	SNMP walk on cefcMIBEnableStatusNotification : value returned : 2
CSCsm32972	Yes	SNMP Counters Get Stuck on Repeated Polls
CSCsm36660	Yes	DHCP Server: Must send DHCP decline if DHCP proposes in-use address
CSCsm41986	Yes	Need to handle fragmented IP packets with 8-byte first frag
CSCsm50135	Yes	Memory leakage caused by catcher_recv_packet_have_sa
CSCsm50494	Yes	Device is not able to process CRL with extension CRL number > 65535
CSCsm51093	Yes	Cannot establish WebVPN session to ASA-5550 - memory allocation error
CSCsm56957	Yes	Traceback occurs in Dispatch Unit with QoS
CSCsm57920	Yes	H323: inspection on video call may cause traceback within 5 min
CSCsm68097	Yes	SSH resource exhausted preventing further sessions
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
CSCsm77958	Yes	Traceback in "IP Thread" when clientless webvpn started
CSCsm91261	Yes	Traceback in 'ssh' thread
CSCsm92266	Yes	Traceback may occur when AAA command authorization is enabled
CSCsm93083	Yes	Syslog 713254 does not get generated for 7.0 and 7.1

Table 4 **Resolved Caveats (continued)**

DDTS Number	Software Version 7.0(8)	
	Corrected	Caveat
CSCso08335	Yes	ISAKMP: Add syslog when Aggressive mode aborted when Spoof Protection
CSCso15583	Yes	Traceback when many remote peers try to establish ipsec L2L tunnels
CSCso17900	Yes	DFP may not background free due to memory calculation
CSCso24494	Yes	PIX/ASA: DHCP server fails to respond to Vista DHCPINFORM request
CSCso35351	Yes	Firewall may crash in thread vpnfol_thread_msg while viewing config
CSCso36070	Yes	Value returned by sysServices MIB is incorrect
CSCso40008	Yes	PIX is sending DN during rekey instead of FQDN
CSCso50996	Yes	ASA dropping the packet instead of encrypting it.
CSCso64731	Yes	security-association lifetime cannot be removed with no crypto map ...
CSCso81153	Yes	Traceback in dispatch unit with MGCP inspection
CSCso82264	Yes	ASA: icmp inspection may drop icmp error packets
CSCso84996	Yes	ASA truncates CN field at 11 characters if CN contains '@' (W2K CA)
CSCso85452	Yes	h323 messages on console; performance degrade
CSCso87435	Yes	NAT-T not working when client source port not 4500 with ACL match

Related Documentation

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

© 2008 Cisco Systems, Inc.

All rights reserved.