



# Cisco ASA 5500 Series Release Notes Version 7.0(5)

---

April 2006

## Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Important Notes, page 4](#)
- [Caveats, page 6](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation and Submitting a Service Request, page 11](#)

## Introduction

The Cisco ASA 5500 series 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 significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high-availability services, and management/monitoring.

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



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

Additionally, the Cisco ASA 5500 series 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 security appliance, then used to configure, monitor, and manage the device.

## System Requirements

The sections that follow list the system requirements for operating a Cisco ASA 5500 series 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 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 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 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/public/sw-center/index.shtml>

## New Features

This section describes the new features in this release. This section includes the following topics:

### Command to Control DNS Guard

Version 7.0(5) introduces a new global configuration command, **dns guard** to control the DNS guard function. In releases prior to 7.0(5), the DNS guard functions are always enabled regardless of the configuration of DNS inspection:

- Stateful tracking of the DNS response with DNS request to match the ID
- Tearing down the DNS connection when all pending requests are responded

This command is effective only on interfaces with **inspect dns** disabled. When DNS inspection is enabled, the DNS guard function is always performed. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### Enhanced IPSEC Inspection

The ability to open specific pinholes for ESP flows based on existence of an IKE flow is provided by the enhanced IPsec inspect feature. This feature can be configured within the MPF infrastructure along with other inspects. The idle-timeout on the resulting ESP flows is statically set at 10 minutes. There is no maximum limit on number of ESP flows that can be allowed.

A new policy-map command **inspect ipsec-pass-thru** is added to enable this feature.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### Command to Disable RST for Denied TCP Packets

When a TCP packet is denied, the adaptive security appliance always sends a reset when the packet is going from a high security to a low security interface. The **service resetinbound** command is used to enable or disable sending resets when a TCP packet is denied when going from a low security to a high security interface. The **service resetinbound** command is introduced to control sending RESETs when a packet is denied when going from a high security to a low security interface. The existing **service resetinbound** command is enhanced to take an additional interface option.

```
[no] service resetoutbound [interface <ifc name>]
```

```
[no] service resetinbound [interface <ifc name>]
```

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### Increased Connections and VLANs

The maximum connections and VLANs is increased to the following numbers.

- ASA5510 base license conns 32000->50000 vlans 0->10
- ASA5510 plus license conns 64000->130000 vlans 10->25

- ASA5520 conns 130000->280000 vlans 25->100
- ASA5540 conns 280000->400000 vlans 100->200

## Password Increased in Local Database

Username and enable password length limits increased from 16 to 32 in the LOCAL database.

## Enhanced show interface and show traffic Commands

The traffic statistics displayed in both the **show interface** and **show traffic** commands now support 1 minute rate and 5 minute rate for input, output and drop. The rate is calculated as the delta between the last two sampling points. For a 1 minute rate and a 5 minute rate, a 1 minute timer and a 5 minute timer are run constantly for the rates respectively. An example of the new display follows:

```

1 minute input rate 128 pkts/sec, 15600 bytes/sec
1 minute output rate 118 pkts/sec, 13646 bytes/sec
1 minute drop rate 12 pkts/sec
5 minute input rate 112 pkts/sec, 13504 bytes/sec
5 minute output rate 101 pkts/sec, 12104 bytes/sec
5 minute drop rate 4 pkts/sec
    
```

## Important Notes

### Important Notes in Release 7.0

This section lists important notes related to release 7.0(5).

#### FIPS 140-2

The Cisco ASA 5500 series security appliance is on the FIPS 140-2 Pre-Validation List.

#### 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 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 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](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(5):

- 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 7.0(5) release.

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/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

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

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

## Open Caveats - Release 7.0(5)

**Table 2** Open Caveats

ID Number	Software Release 7.0(5)	
	Corrected	Caveat Title
CSCei47678	No	SNMP packet size standards in RFC3417 not fully supported.
CSCek21836	No	SIP: BYE embryonic connection timestamp not updated.
CSCsc36891	No	Higher CPU utilization for url filtering in recent releases.
CSCsc37965	No	IP-directed broadcasts no longer allowed through device.
CSCsc68575	No	CPU usage is higher for given traffic throughput in recent releases.
CSCsc97602	No	Traceback is sometimes observed in tmatch compile thread.
CSCsd00086	No	ASDM connection may cause packet loss
CSCsd08170	No	UDP 500 not removed from pat port pool when crypto map is applied
CSCsd59936	No	Registering to the RP for PIM fails if fragmented in more than 12 packs
CSCsd69625	No	EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth

**Table 2** Open Caveats (continued)

ID Number	Software Release 7.0(5)	
	Corrected	Caveat Title
CSCsd75865	No	VPN address pool overlap may cause packet drop.
CSCsd78428	No	Traceback may occur in Checkheaps on standby unit
CSCsd79596	No	H245 connection going idle although traffic on RTP stream and H225.
CSCsd82355	No	Malformed syslog packets may be generated.
CSCsd82714	No	RTSP fails with Windows media player
CSCsd84394	No	IPSec: Invalid block submitted to outbound packet processing
CSCsd85345	No	Traceback may occur in fover_parse on 7.0.4
CSCsd89503	No	Traceback during failover in routing module
CSCsd93207	No	Show failover indicates different uptimes on devices in failover pair
CSCsd93380	No	Packets for VPN-I2I peer get dropped instead of encrypted

## Resolved Caveats - Release 7.0(5)

**Table 3** Resolved Caveats

ID Number	Software Release 7.0(5)	
	Corrected	Caveat Title
CSCeh46345	Yes	Dynamic L2L could pass clear text traffic when tunnel terminates
CSCeh60845	Yes	Logginig queue incorrectly registers 8192 256-byte blocks
CSCeh70043	Yes	DOC: sh asp drop needs further clarification in doc
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCei43588	Yes	traceback when trying to match a packet to acl with deny
CSCek21835	Yes	Higher metric OSPF external route is selected
CSCek21837	Yes	PDM with Command Authorization requires the write command for Read-Only
CSCek21838	Yes	SIP: fail to open a conn for Record route in NOTIFY
CSCek21843	Yes	SIP: Not translate c= address if first m= has port 0 in SDP body.
CSCek21849	Yes	Backspace sent in cut-through proxy authentication
CSCek26572	Yes	tftp fixup does not allow error message from client
CSCsc02485	Yes	Session Cmd: sendind 036xr to exit session to ssm causes Traceback
CSCsc03061	Yes	CLI should generate Warning if kerberos-realm is not in all uppercase
CSCsc07614	Yes	Minimum unit poll time causes trouble for failover with 4GE card
CSCsc08188	Yes	5540 crash during 1000+ tunnel, multi-encapsulation system testing
CSCsc12094	Yes	AAA fallback authentication does not work with reactivation-mode timed
CSCsc15434	Yes	Assertion violation w/icmp traffic and icmp inspection
CSCsc16041	Yes	'clear local host' results in memory leak

Table 3 Resolved Caveats (continued)

Software Release 7.0(5)		
ID Number	Corrected	Caveat Title
CSCsc16507	Yes	url-server: cannot remove despite having removed url-block cmd
CSCsc18444	Yes	Tunnel-group for specific peer not created upgrading to 7.0 w/ certs
CSCsc18911	Yes	ASA does not remove OSPF route for global PAT entry after deleting
CSCsc20102	Yes	webfo: traceback during bulk sync in vpnfol_thread_sync
CSCsc26331	Yes	PKI: CR should not be used to terminate certificate console input
CSCsc27972	Yes	Traceback when changing crypto maps when Answer-Only in lower sequence
CSCsc31762	Yes	Fixup RTSP does not re-write the SET Parameter to the NATed IP address
CSCsc31788	Yes	Failover Primary access-list delete problem crashes secondary
CSCsc33385	Yes	GTP - pdp context creation failed - GSN tunnel limit exceeded
CSCsc34022	Yes	ASA requires improved failover testing method
CSCsc36332	Yes	Crash with show running-config all when priority class configured
CSCsc36898	Yes	FIPS: POST Bypass test failure
CSCsc37492	Yes	ASA: snmp-server host is not working in some circumstances
CSCsc39334	Yes	Crash due to check-retransmission from the tcp-map
CSCsc39559	Yes	APPFW:Obfuscated characters causing alert with firefox browser
CSCsc42204	Yes	Syslog ID 111005 no longer being logged when user exits config mode
CSCsc44566	Yes	Traceback in Dispatch Unit - pm_rcv_cb_ids
CSCsc44591	Yes	Traceback in ARP Thread - arp_sendbp in mulicontext mode
CSCsc46976	Yes	SIP: crash when failed to pre-allocate early rtp
CSCsc48330	Yes	OpenSSL Security Advisory: Potential SSL 2.0 Rollback
CSCsc48463	Yes	Traceback on ASA 5510 in Thread Name: vpnfo_thread_msg
CSCsc49830	Yes	IKE daemon crashes after upgrading
CSCsc49873	Yes	VPN-filter not applied without for remote VPN clients without xauth
CSCsc56552	Yes	Adding user context causes traceback on Standby unit
CSCsc57901	Yes	Memory leak when the standby unit fails to parse IKE messages
CSCsc57935	Yes	ASA FO should give warning when there is OS version difference
CSCsc58416	Yes	ASA crash in Dispatch Unit thread
CSCsc59298	Yes	VPN: IPsec errors are reported when trying to fragment compressed pkts
CSCsc60506	Yes	Large banner from RADIUS is causing traceback
CSCsc67347	Yes	VPN locks up under throughput stress
CSCsc73580	Yes	traceback in logger_save after clear config logging
CSCsc73942	Yes	TCP RST is dropped when there is outstanding data that is not acked
CSCsc77884	Yes	GTP: should check spare bits in header
CSCsc78817	Yes	ASA crashes in FWTask() during clear config all
CSCsc78900	Yes	Reload with Thread Name: Dispatch Unit at tcp_check_packet

**Table 3 Resolved Caveats (continued)**

ID Number	Software Release 7.0(5)	
	Corrected	Caveat Title
CSCsc81668	Yes	https://<ip>/config does not have the same privilege level as 'write'
CSCsc83854	Yes	ASA endlessly sends Radius Access-Requests when requesting a BIG dACL
CSCsc84291	Yes	When using SSL the warning message is not returned back
CSCsc86217	Yes	Voice Proxy Function does not preserve DSCP bits.
CSCsc90944	Yes	ASA sends malformed https proxy authentication page.
CSCsc92575	Yes	Upgrade Activation Key reduces permitted interfaces
CSCsc97846	Yes	CPU utilization increase when adding more logging hosts.
CSCsc97905	Yes	traceback when running codenomicon snmp suite. eip 0x00ebf294
CSCsc98336	Yes	Large group-policy names cause crash if used with IPsec
CSCsc99263	Yes	GTPv1: Subsequent Create Req to modify PDP context IEs are not processed
CSCsc99339	Yes	traceback when running ospf codenomicon suite.eip 0x00ef5f7c
CSCsc99364	Yes	SSL Certs from Verisign Managed PKI do not install
CSCsd00051	Yes	SNMP polling may cause packet loss
CSCsd00175	Yes	ASA5510 drops FIN/ACK packets resulting in half open FTP sessions
CSCsd01096	Yes	Primary active crash and both primary and secondary are non-active
CSCsd01722	Yes	ASA 7.0 logging message 419001 always sent in message lists
CSCsd02938	Yes	ASA doesn't reconnect if websense server goes down
CSCsd03391	Yes	TCP Intercept doesn't negate CPU impact when SYN flood from adjacent net
CSCsd04700	Yes	match port option for setting connection time-outs does not work
CSCsd08060	Yes	Memory corruption caused by session DB when events are out of sync..
CSCsd10138	Yes	Crash in Checkheaps thread when enabling LAN2LAN vpn
CSCsd11179	Yes	SNMP polling of resource MIBS may cause packet loss
CSCsd11511	Yes	Crash due to memory corruption in sanity check of the Checkheaps thread
CSCsd11908	Yes	Traceback in logger_save thread
CSCsd13334	Yes	ASA, Memory Leaking tunnel-group authorization-dn-attributes
CSCsd13938	Yes	Traceback and Assertion in "fover_dev.c", line 513
CSCsd16751	Yes	GTP: wrong service-policy used when connection is re-used
CSCsd22910	Yes	users with passwords longer than 11 chars can no longer authenticate
CSCsd25553	Yes	ASA crashes when VPN client tries to make connection to inside interface
CSCsd28581	Yes	ASA failover : Secondary crashes with Thread Name: IKE Daemon
CSCsd31068	Yes	platform image read as ascii if uploaded by asdm to flash:
CSCsd34070	Yes	H.245 inspection skipped when malformed GKRCs packet
CSCsd36030	Yes	in multiple policy-maps, packets should match the first map,not the last
CSCsd37075	Yes	DSH API should check for 0 handle
CSCsd38929	Yes	SSL Verisign imported certificate fails when establishing SSL session

Table 3 Resolved Caveats (continued)

Software Release 7.0(5)		
ID Number	Corrected	Caveat Title
CSCsd39029	Yes	Traceback with Thread Name: Dispatch Unit
CSCsd44349	Yes	PIM codenomicon suite crashes box - eip 0x010811f3
CSCsd45099	Yes	logging debug-trace should not prevent debugs from printing to console
CSCsd46111	Yes	Traceback when using sh xlate via telnet over VPN tunnel
CSCsd46922	Yes	High CPU usage when configuring/compiling ACL's
CSCsd48512	Yes	Duplicate ASP crypto table entry causes firewall to not encrypt traffic
CSCsd51884	Yes	Restore debug icmp trace functionality - showing nat translation
CSCsd58620	Yes	H.323: Memory Leak Under Load
CSCsd58848	Yes	Memory allocated for connections not freed
CSCsd63673	Yes	ASA with dhcprelay doesnt reply with unicast DHCP offer
CSCsd64394	Yes	Deny syslog not generated for denied URLs trafic
CSCsd64912	Yes	url-server: tcp connections fail when tcp stack users are exhausted
CSCsd64920	Yes	url-server: url lookup requests are not retried when using tcp
CSCsd65209	Yes	url-block block: http response buffering feature does not work
CSCsd65215	Yes	Capture access-list shows only 1 hit count for outbound traffic
CSCsd67647	Yes	Traceback in obj-f1/tcp:_q_copydata+26 on copying image to ftp server
CSCsd70242	Yes	Some syslogs are incorrectly logged to an event list, when not specified
CSCsd70812	Yes	HA: Traffic Stall after config syncing running Act/Act fover
CSCsd72617	Yes	Dispatch Unit Crash when HTTP inspect enabled...ASA 7.1.2, 7.0.4-11
CSCsd72951	Yes	Traceback: Thread Name: IKE Daemon (Old pc 0x00507433 ebp 0x03bdc498)
CSCsd74964	Yes	SNP Inspect Http drops messages other than GET
CSCsd75794	Yes	MFWR:R applfw crash on codenomicon http suite, test 39614 or 39615
CSCsd76384	Yes	dhcpc fails when management-access is configured
CSCsd77018	Yes	Traceback in obj-f1/snp_fp_main:_snp_fp_fragment+260
CSCsd77155	Yes	All out of order packets dropped by tcp normalizer
CSCsd78595	Yes	Global buffer drop output under show service-policy
CSCsd79775	Yes	ASA VPN: all packets for a l2l peer get dropped instead of encrypted
CSCsd81496	Yes	crash when websense service is restarted while requests are pending
CSCsd82114	Yes	Change of log options on the ACE doesn't take immediate effect
CSCsd83007	Yes	Need ability to disable dns guard in 7.0
CSCsd83863	Yes	Reload with Thread Name: Dispatch Unit
CSCsd85007	Yes	Dispatch unit crash at snp_fp_fragment with SSM card enabled
CSCsd85451	Yes	SAs not created when crypto map group and isakmp policy group are differ
CSCsd86841	Yes	F1 crash immediately after sending ping traffic thru GTP tunnel
CSCsd87779	Yes	fips self test power on never completes

## Related Documentation

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

[http://www.cisco.com/en/US/products/ps6120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html)

## Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CDC account you can visit the following websites for assistance:

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

<http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/>

## 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 “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc.  
All rights reserved.