



Cisco ASA 5500 Series Release Notes

Version 7.1(2)

March 2006, OL-10087-01

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Important Notes, page 3](#)
- [Caveats, Version 7.1\(2\), page 6](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation and Submitting a Service Request, page 9](#)

Introduction

The Cisco ASA 5500 series security appliance are purpose-built solutions that combine best-of-breed 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. This version introduces significant enhancements to major functional areas including: new Anti-X Services, VPN services, and management/monitoring.

Additionally, the adaptive security appliance software supports Adaptive Security Device Manager. 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 security



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

© 2006 Cisco Systems, Inc. All rights reserved.

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 2](#)

Memory Requirements

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

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/kobayashi/sw-center/>

You must upgrade from Version 7.0(x) or 7.1(1) to 7.1(2) because older versions of the ASA images do not recognize new ASDM images and new ASA images do not recognize old ASDM images. Similarly, if you downgrade to an earlier version of ASA software, you must also downgrade the ASDM image.

You can also use 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 7.0.(x) or 7.1(1) to 7.1(2), you must perform the following steps:

-
- Step 1** Load the new 7.1(2) image from the following website: <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>

- Step 2** Reload the device so that it uses the 7.1(2) image.
- Step 3** Load the new ASDM 5.1(2) image from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
-

To downgrade from Version 7.1(2) to an earlier version, you must perform the following steps:

- Step 1** Load the 7.0(x) or 7.1(1) image from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>
- Step 2** Reload the device so that it uses the earlier image.
- Step 3** Load the ASDM 5.0(x) or 5.1(1) image from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>.
-

Features

ASA Version 7.1(2) is a sustaining release that fixes product deficiencies. It includes no new features. For information about features new for ASA Release 7.1, see the *Cisco ASA 5500 Series Release Notes, Version 7.1(1)*.

Important Notes

This section lists important notes related to Version 7.1(2).

SSL VPN Licenses

Beginning with Version 7.1(1), SSL VPN (WebVPN) services require a license. These services are now licensed on a per-user session basis, with licensing levels at 10, 50, 100, 250, 500, 750, 1000, and 2500 user sessions. The complete SSL VPN feature functionality offered by the adaptive security appliance is included in this single SSL VPN license. No per-feature licenses are required. This SSL VPN license has a one-time fee and lasts for the lifetime of the adaptive security appliance. Upon installation of Version 7.1(1) or later, two simultaneous SSL VPN user sessions are included for evaluation.

ActiveX and WebVPN

Many ActiveX controls are custom and require special treatment by WebVPN. Please contact Cisco TAC if your application uses ActiveX controls and you have problems with its functionality over a WebVPN connection (CSCsb85180).

CIFS Files

If a remote user accesses CIFS files using Internet Explorer, the filename in the File Download window might not display some Japanese Shift_JIS characters correctly. However, the Open and Save functions do work properly. This issue does not occur with Netscape.

Failover and WebVPN and SVC Connections

To ensure that WebVPN and SVC connections reconnect quickly in the event of a failover, enable the adaptive security appliance to respond to incoming client TCP packets with the **service resetoutside** command from global configuration mode:

```
[no] service resetoutside
```

This command causes the adaptive security appliance that takes over the existing WebVPN and SVC connections to send TCP RST packets in response to incoming client TCP packets, causing client connections to reestablish quicker. If you do not enable the **service resetoutside** command, the security appliance drops TCP packets from failed-over connections and waits for each client to reestablish the TCP connection. This may take longer or result in the session being lost due to timeout.

The following example enables the security appliance to send TCP RST packets:

```
hostname(config)# service resetoutside
```

FIPS 140-2

The adaptive security appliances are on the FIPS 140-2 Pre-Validation List.

WebVPN ACLS and DNS Hostname

When a deny webtype URL ACL (DNS-based) is defined, but the DNS-based URL is not reachable, the browser displays a “DNS Error” popup. The ACL hit counter does not increment.

If an IP address rather than a DNS name defines a deny webtype URL, then the hit counter does record the traffic flow hitting the ACL, and the browser displays a “Connection Error.”

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 displays it on the client browser.

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

Mismatch PFS

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

Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The 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.

VPN Load Balancing Requirements

VPN load balancing for the adaptive security appliance requires an ASA 5520 or ASA 5540. It also requires a 3DES-AES encryption license.

User Upgrade Guide

For a list of deprecated features, and user upgrade information, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/migr_vpn/index.htm

Features not Supported in Version 7.1(2)

The following features are not supported in Version 7.1(2):

- PPPoE
- L2TP over IPSec
- PPTP

MIB Support

For information on MIB Support, go to:

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

Downgrading to a 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, Version 7.1(2)

The following sections describe open and resolved VPN caveats for version 7.1(2).

Open Caveats

The following sections describe the caveats that remain open for Version 7.1(2).

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 might 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>

Table 2 lists open caveats in Version 7.1(2).

Table 2 Open Caveats, Version 7.1(2)

ID Number	Caveat Title
CSCsd07703	Oracle Forms (Java) Applet not loading via WebVPN
CSCsd13921	IBM WebSphere Host On-Demand: Applet Throws ClassNotFoundException
CSCsd16222	ASA fails to allow TCP resets pass when IP SSM module is used inline
CSCsd21821	Traceback eip: sessmgrmain:_CheckSubRecConnectTime+23 after appl. act-key
CSCsd21887	WebVPN applies content transformation to URLs in e-mails when accessing OWA
CSCsd36030	In multiple policy maps, packets should match the first map, not the last
CSCsd36281	Traceback after administratively disconnecting a L2L tunnel with filters applied
CSCsd36359	Traceback eip: _vpnfo_fsm_get_ha_state+514 on FO UUT after 32 seconds
CSCsd36388	Traceback on sec FO eip:_dllobj_remove+12 rapidly establishing IPsec tunnel
CSCsd36400	Traceback: eip_shash_remove+158 on secondary (standby) after VPN system test
CSCsd40080	WebVPN: ASA reboots while downloading from CIFS Server
CSCsd41442	Checkheap asserts due to a free buffer validation failure
CSCsd45406	Traceback in "accept/http" while configuring object-group with ASDM
CSCsd45628	Traceback when entering http server enable command

Table 2 Open Caveats, Version 7.1(2) (continued)

ID Number	Caveat Title
CSCsd07703	Oracle Forms (Java) Applet not loading via WebVPN
CSCsd46111	Traceback when using show xlate via telnet over VPN tunnel
CSCsd46685	Traceback eip::_snp_sp_action_construct_ip_key+1013 after ipsec rule cfg
CSCsd46922	High CPU usage when configuring or compiling ACLs
CSCsd48311	WEBVPN: Session disconnects when Domino Web Access function is used
CSCsd52578	Traceback in thread: snp_timer_thread
CSCsd53321	Sysopt connection time wait causes SSH sessions to timeout prematurely
CSCsd56547	Traceback with no thread name after upgrading
CSCsd59064	ASA stops passing traffic after http server enable command
CSCsd60662	Traceback occurs in snp_timer_thread, but no ACL edits
CSCsd62529	WebVPN CIFS download: non-standard characters in filename do not render correctly
CSCsd62875	Traceback in tmatch compile thread
CSCsd64698	Memory leakage in IKE
CSCsd64912	URL-server: TCP connections fail when TCP stack users are exhausted
CSCsd64920	URL-server: URL lookup requests are not retried when using TCP
CSCsd65192	WebVPN: Debug webvpn svc will not show up in show debug command
CSCsd65209	URL-block block: HTTP response buffering feature does not work
CSCsd65215	Capture access-list shows only 1 hit count for outbound traffic

Resolved Caveats

Table 3 lists caveats resolved in Version 7.1(2).

Table 3 Resolved Caveats

ID Number	Caveat Title
CSCeh90617	Recompiling ACLs can cause packet drops on low-end platforms
CSCei43588	Traceback when trying to match a packet to acl with deny
CSCek21837	PDM with Command Authorization requires the write command for read-only
CSCek21846	SIP: xlate timeout not updated by expire value in register message
CSCek26572	TFTP fixup does not allow error message from client
CSCek27919	PIX reload with Thread Name: tcp_slow
CSCsc06239	French language VPN Client xauth prompt not translated into French
CSCsc12094	AAA fallback authentication does not work with reactivation-mode timed
CSCsc16041	Using clear local host command results in memory leak
CSCsc16507	Cannot remove url-server despite having removed url-block command
CSCsc33385	GTP - pdp context creation failed - GSN tunnel limit exceeded

Table 3 **Resolved Caveats (continued)**

ID Number	Caveat Title
CSCsc36332	Traceback: Thread Name:ci/console w/sh run all and priority class config
CSCsc44591	Traceback in Thread Name: ARP Thread in multicontext mode
CSCsc46976	SIP: traceback when failed to pre-allocate early rtp
CSCsc51939	Performance throughput problems when http inspect enabled
CSCsc64621	VPN syslog 402123 should include a meaningful error message
CSCsc73942	TCP RST is dropped when there is outstanding data that is not acked
CSCsc78010	Traceback in Thread Name: Checkheaps
CSCsc78900	Reload with Thread Name: Dispatch Unit at tcp_check_packet
CSCsc81565	Idle conn timeout reset when packet dropped by TCP normalizer
CSCsc81668	https://<ip>/config does not have the same privilege level as "write"
CSCsc86217	Voice proxy function does not preserve DSCP bits.
CSCsc90944	Malformed https proxy authentication page with linebreak
CSCsc91450	FTP control channel timing out although data channel is active.
CSCsc93061	Traceback after activation of vpn-filter
CSCsc94945	ASA generates incorrect startup-config errors
CSCsc97999	Syslog Message ID 313003 is used incorrectly
CSCsc98339	Standby unit may reload if active unit powered off
CSCsc99263	GTPv1: Subsequent Create Req to modify PDP context IEs are not processed
CSCsc99364	SSL Certs from Verisign managed PKI do not install
CSCsd00051	SNMP polling of ASA management interface stats may cause packet loss
CSCsd00175	ASA w/ IPS may drop FIN/ACK packets resulting in half open FTP sessions
CSCsd03391	TCP Intercept doesn't negate CPU impact when SYN flood from adjacent net
CSCsd04327	ASA all out of order packets are dropped when sending to ssm
CSCsd04700	Match port option for setting connection time-outs does not work
CSCsd07783	Transient NAT-T packets silently dropped if NAT-T is enabled
CSCsd08060	Memory corruption caused by vpn session db when events are out of sync
CSCsd11179	SNMP polling of resource MIBS may cause packet loss
CSCsd13334	ASA, memory leaking tunnel-group authorization-dn-attributes
CSCsd13636	ASA reload with Thread Name: dispatch unit
CSCsd15475	Secondary unit doesn't get full config file after SSH reload on Primary
CSCsd16751	GTP: wrong service-policy used when connection is re-used
CSCsd17718	IGMP forward interface command fails to sync to the standby unit
CSCsd17763	PIX should not respond to TCP segment w/ RST+ACK and bad ACK number
CSCsd17879	Deny rules in crypto acl blocks inbound tcp/udp after tunnel formed
CSCsd22910	Users with passwords longer than 11 characters can no longer authenticate
CSCsd25537	Failover unit traceback in Thread Name: fover_FSM_thread

Table 3 **Resolved Caveats (continued)**

ID Number	Caveat Title
CSCsd28581	Failover: Secondary traceback in Thread Name: IKE Daemon
CSCsd30879	Additional MS control for RDP/TS over WebVPN
CSCsd34070	H.245 inspect skipped if GK RCS and wrong H.225 callSignalAddress for GK
CSCsd38929	SSL Verisign imported certificate fails when establishing SSL session

Related Documentation

For additional information on the adaptive security appliance, see the following documentation found on Cisco.com:

- *Cisco ASA 5500 Hardware Installation Guide*
- *Cisco Adaptive Security Appliance Getting Started Guide*
- *Cisco ASDM Release Notes*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Release Notes for Cisco SSL VPN Client*
- *Cisco Secure Desktop Configuration Guide*
- *Release Notes for Cisco Secure Desktop*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

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.

©2006 Cisco Systems, Inc. All rights reserved.