Cisco ASA 5500 Series Release Notes Version 7.0(4)

October 2005

Contents

This document includes the following sections:

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

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

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/cisco/software/navigator.html

New Features

Released: October 15, 2005

Table 2 lists the new features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4).

Table 2 New Features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4)

Feature	Description
Platform Features	
Support for the 4GE SSM	The 4GE Security Services Module (SSM) is an optional I/O card for the adaptive security appliance. The 4GE SSM expands the total number of ports available on the security appliance, providing four additional ports with Ethernet (RJ-45) or SFP (fiber optic) connections.
VPN Features	
WebVPN Capture Feature	The WebVPN capture feature lets you log information about websites that do not display properly over a WebVPN connection. You can enable the WebVPN capture feature with the **capture** command, but note that it has an adverse affect on the performance of the security appliance. So, be sure to disable this feature after you have captured the information that you need for troubleshooting.
Auto Update Over a VPN Tunnel	With this release, the **auto-update server** command has a new **source** *interface* argument that lets you specify an interface, such as a VPN tunnel used for management access and specified by the **management-access** command: **auto-update server** *url* [**source** *interface*] [*verify-certificate*]
HTTP proxy applet	The HTTP proxy is an Internet Proxy, that supports both HTTP and HTTPS connections. The HTTP proxy code modifies the browser proxy configuration dynamically to redirect all browser HTTP/S requests to the new proxy configuration. This allows the Java Applet to take over as the proxy for the browser. HTTP Proxy can be used in conjunction with the Port Forwarding (Application Access) feature or by itself. **Note** The HTTP proxy feature only works when using Internet Explorer. On some of the older computers, running Windows XP, the RunOnce Reg-Key is not available, causing the Port Forwarding HTTP-Proxy feature to fail when attempting to modify Proxy settings on Internet Explorer. You can mannually change the registry. Complete the following steps to change the registry manually: **a.** Click **Start | Run**. **b.** Type **regedit** in the open text box, and click **OK**. **c.** Open this folder: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ **d.** Right click inside the CurrentVersion and select **New | Key**. **e.** Name the new key **RunOnce**. **f.** Click **OK**. To configure file access and file browsing, MAPI Proxy, HTTP Proxy, and URL entry over WebVPN for this user or group policy, use the **functions** command in WebVPN mode.

Table 2 New Features for ASA and PIX Version 7.0(4)/ASDM Version 5.0(4) (continued)

Feature	Description
IPSec VPN: Add support for cascading ACLs	Cascading ACLs involves the insertion of deny ACEs to bypass evaluation against an ACL and resume evaluation against a subsequent ACL in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security. The sequence number assigned to the crypto ACL determines its position in the evaluation sequence within the crypto map set.
Troubleshooting and Monitoring Features	
Crashinfo Enhancement	Output from the **crashinfo** command might contain sensitive information that is inppropriate for viewing by all users connected to the security appliance. The new **crashinfo console disable** command lets you suppress the output from displaying on the console.
Rate limiting of Syslog messages	The logging rate limit enables you to limit the rate at which system log messages are generated. You can limit the number of system messages that are generated during a specified time interval. You can limit the message generation rate for all messages, a single message ID, a range of message IDs, or all messages with a particular severity level. To limit the rate at which system log messages are generated, use the **logging rate-limit** command.
Firewall Features	
Connection timeout using Modular Policy Framework	The new **set connection timeout** command lets you configure the timeout period, after which an idle TCP connection is disconnected.
Downloadable ACL Enhancements	A new feature has been added to ensure that downloadable ACL requests sent to a RADIUS server come from a valid source through the Message-Authenticator attribute. Upon receipt of a RADIUS authentication request that has a username attribute containing the name of a downloadable ACL, Cisco Secure ACS authenticates the request by checking the Message-Authenticator attribute. The presence of the Message-Authenticator attribute prevents malicious use of a downloadable ACL name to gain unauthorized network access. The Message-Authenticator attribute and its use are defined in RFC 2869, RADIUS Extensions, available at http://www.ietf.org.
Converting Wildcards to Network Mask in Downloadable ACL	Some Cisco products, such as the VPN 3000 concentrator and Cisco IOS routers, require you to configure dowloadable ACLs with wildcards instead of network masks. The Cisco ASA 5500 adaptive security appliance, on the other hand, requires you to configure downloadable ACLs with network masks. This new feature allows the security appliance to convert a wildcard to a netmask internally. Translation of wildcard netmask expressions means that downloadable ACLs written for Cisco VPN 3000 series concentrators can be used by the security appliance without altering the configuration of the downloadable ACLs on the RADIUS server. You can configure ACL netmask conversion on a per-server basis, using the **acl-netmask-convert** command, available in the AAA-server configuration mode.
Application Inspection Features	
Support GTP Load Balancing Across GSNs	If the security appliance performs GTP inspection, by default the security appliance drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS. You can enable support for GSN pooling by using the **permit response** command. This command configures the security appliance to allow responses from any of a designated set of GSNs, regardless of the GSN to which a GTP request was sent.

Important Notes

Important Notes in Release 7.0

This section lists important notes related to release 7.0(4).

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(4)* document.

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 conjuction 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

Features not Supported in Version 7.0

The following features are not supported in Version 7.0(4):

- 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(4) 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://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 - Release 7.0(4)

Table 3 Open Caveats

	Software Release 7.0(4)	
ID Number	Corrected	Caveat Title
CSCeg57001	No	Packet does not come to inspect after no inspect and inspect
CSCeh15557	No	Assertion in tmatch_compile_proc, all memory is not freed.
CSCeh18115	No	Authentication not triggered sometimes when URL filtering enabled.
CSCeh32087	No	PIM sends Register with untranslated IP when NAT pool exhausted.
CSCeh43554	No	Device may reload if showing and removing config at the same time
CSCeh46345	No	Dynamic L2L could pass clear text traffic when tunnel terminates
CSCeh51949	No	Can no longer connect to ASA via WebVPN or ASDM->exhausted 8K blocks
CSCeh60845	No	Logginig queue incorrectly registers 8192 256-byte blocks
CSCeh84006	No	Wrong http version number should not be allowed
CSCeh90617	No	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh93834	No	RSA SecurID replica list is lost after reboot
CSCei02273	No	1st log message is not sent by mail in transparent firewall
CSCei43588	No	traceback when trying to match a packet to acl with deny
CSCej04099	No	static xlate breaks management-access inside
CSCsb28708	No	Console traceback using show route command
CSCsb40188	No	SCEP fails if RA cert has 4096 bit key
CSCsb41742	No	P2P/IM/tunneling traffic is only dropped if strict-http action is drop
CSCsb51038	No	Traceback: _snp_sp_create_flow+1937 with outbound ACL and Policy Statics
CSCsb80170	No	Address-pools needed in group-policy - missing functionality from VPN3K
CSCsb81593	No	removing sunrpc-server cli doesnt stop sunrpc traffic from getting thru
CSCsb90046	No	GTP context creation might fail w/ Tunnel Limit xxx exceeded error
CSCsb99385	No	strict-http: with a space before http ver should generate a tcp reset
CSCsc00176	No	clear xlate take 4.5+ mins to clear 60K PAT xlat
CSCsc01017	No	ASA to VPN3K L2L fails rekey w/ main mode, 3des, sha, rsa, pfs-2, dh-2
CSCsc02485	No	Session Cmd: sendind \036x\r to exit session to ssm causes Traceback
CSCsc07421	No	Traceback in Dispatch Unit - decoding h323 ras message
CSCsc07614	No	Minimum unit poll time causes trouble for failover with 4GE card
CSCsc10617	No	GTP: memory leakage after <clear config all> at gtp_init
CSCsc11724	No	Logging: Wrong behaivor if syslog is sent to a nonfunctioning tcp server
CSCsc12094	No	AAA fallback authentication does not work with reactivation-mode timed
CSCsc14591	No	xlate and xlate perfmon print graph are all zeros
CSCsc15434	No	Assertion violation w/icmp traffic and icmp inspection
CSCsc16041	No	'clear local host' results in memory leak

Table 3 Open Caveats (continued)

	Software Release 7.0(4)	
ID Number	**Corrected**	**Caveat Title**
CSCsc16503	No	Transparent firewall ASR UDP out traffic got errors and inbound failed
CSCsc16607	No	fixup pptp fails with static pat server configuration
CSCsc17051	No	VPNFO: VPN Failover fails to parse P2 SA when IPCOMP is used
CSCsc17409	No	dhcprelay: ASA blocks RELEASE packets
CSCsc17428	No	Tracebacks with ci/console with 'clear config all'
CSCsc18444	No	Tunnel-group for specific peer not created upgrading to 7.0 w/ certs
CSCsc18911	No	ASA does not remove OSPF route for global PAT entry after deleting

Resolved Caveats - Release 7.0(4)

Table 4 Resolved Caveats

	Software Release 7.0(4)	
ID Number	**Corrected**	**Caveat Title**
CSCeg67989	Yes	WebVPN: Logo file is not working correctly
CSCeh81062	Yes	wrong ip addr on outgoing packets when PAT and static port are used
CSCeh90309	Yes	Checkheaps process crashes while dumping corrupted memory blocks
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCeh97228	Yes	cTCP: cTCP connection are dropped sporadically when connected F1 Bet
CSCei00497	Yes	PIX/ASA 7.0 doesnt encrypt packets if next hop is PIX interface.
CSCei20466	Yes	Increase in CPU utilization when OSPF is enabled
CSCei20682	Yes	FWSM uptime stops at 49 days 17 hours
CSCei23290	Yes	DHCP Relay fails when static specified
CSCei24062	Yes	Some hosts in the network connects to inside intf cannot be reached
CSCei33166	Yes	Crash while pinging through a L2L tunnel w/ 10,000 byte pings
CSCei33782	Yes	Simultaneous TFTP connections are not closed properly
CSCei38012	Yes	DHCP Server should check for correct network upon REQUEST for rebind
CSCei38640	Yes	AAA: radius /w expiry does not work when using funk radius server
CSCei38644	Yes	VPN3000 does not properly handle State Attribute
CSCei38647	Yes	IKE SA stuck in MM_DONE state
CSCei38651	Yes	NT auth for VPN clients do not work with domainuser or user@domain
CSCei38657	Yes	P1 rekey may fail when P1/P2 rekeying and retransmit required
CSCei38667	Yes	Can’t differentiate between root CA certs that have been re-keyed
CSCei38669	Yes	IPSec rekey causes tunnel to drop
CSCei41326	Yes	AAA: fallback to LOCAL authentication does not work for SSH

Table 4 Resolved Caveats (continued)

	Software Release 7.0(4)	
ID Number	**Corrected**	**Caveat Title**
CSCei43065	Yes	Traceback - 0x004a21b0 ojb-f1/c_crypto_map:_crypto_map_remove_np+80
CSCei43133	Yes	traceback eip 0x006026a4 obj-f1/snp_ha_db in ci/console af cleconfal
CSCei44143	Yes	Crash in malloc.c if removing ACE from ACL
CSCei50190	Yes	ASA not accepting 2 ISAKMP policies with different AES types
CSCei50691	Yes	traceback with ASR enabled for session with 2ndary conn in TFW mode
CSCei51783	Yes	Group enumeration possible on Benetton platform
CSCei51867	Yes	Usability - crypto config should be grouped together in CLI output
CSCei52413	Yes	ASA fails to import cert if CA issuer has 4096 bits cert
CSCei52906	Yes	Routes assoc. w/ net ext tunnels fail to get removed after tun drop
CSCei54438	Yes	Inspects that use TCP proxy must enable dual TCP normalizer mode
CSCei56278	Yes	All access-lists removed when removing one
CSCei57279	Yes	Cascading ACL: Deny rules not working after tunnel established
CSCei62347	Yes	acl interval default value not show when inactive parameter used
CSCei64608	Yes	GTP: box reloads when Create Response has 3rd party GSN addr
CSCei67952	Yes	GTP: PDP Context expires even when data is present in the tunnel
CSCei68679	Yes	Traceback on telnet TACACS+ authentication through the firewall.
CSCei68679	Yes	Traceback on telnet TACACS+ authentication through the firewall.
CSCei70172	Yes	TCP dynamic proxy doesnt fast retransmit lost packet
CSCei70785	Yes	TCP proxy must send data from retransmit queue when ACK is received
CSCei71868	Yes	Deny message for inbound traffic with no access-list changed
CSCei75013	Yes	confg doesnt get copied to admin ctx when changing mode SRM->MRM
CSCei78667	Yes	URL filtering: misc issues related to request exhaustion and cleanup
CSCei81803	Yes	Assert in validate_chunk() during startup
CSCei83304	Yes	clear conf sec doesnt clear igmp and ospf param in ifx submode
CSCei84925	Yes	traceback obj-f1/snp_tfw:_snpi_tfw_update_l2_entry+75 af apply conf
CSCei87390	Yes	Removing failover group causes traceback with 4GE installed
CSCei87785	Yes	MGCP: Call cannot be placed with IP phone using BTS CA & version 1.0
CSCei92828	Yes	Authentication failing for virtual telnet/http in transperent mode
CSCei93112	Yes	Existing connections not replicated to standby after failover
CSCei93790	Yes	Clear configure all in single transparent mode causes traceback
CSCej08898	Yes	tcpintercept caused trcback.embconn=0,maxconn!=0,eip:0x00c32dbc
CSCej12123	Yes	OSPF external routes preferred over internal with multiple processes
CSCej24446	Yes	error in processing IKE
CSCsb32565	Yes	Device reboots unexpectedly with traceback
CSCsb36441	Yes	Traceback eip _snp_fp_inspect_ip_options with IP Frag and 10 KB ping

Table 4 Resolved Caveats (continued)

	Software Release 7.0(4)	
ID Number	**Corrected**	**Caveat Title**
CSCsb37531	Yes	Traceback after failover if TCP Intercept is triggered.
CSCsb45373	Yes	Traceback tcp_slow after vpn system test script strtd snd cfg setupUUT
CSCsb45584	Yes	Traceback eip _snp_ids_cleanup_cb with ips promiscuous and 100 byte ping
CSCsb46603	Yes	GTP: Responses that reject Create Requests are dropped
CSCsb46862	Yes	Assertion in ctm_sw_rng_x931.c:update_key
CSCsb47027	Yes	ASA crashed eip 0x00b8773c (image 7.0.2.1)
CSCsb47825	Yes	F1 fails to establish TCP remote access sessions with 3002 HW client
CSCsb49125	Yes	F1 crashes at <show debug> command
CSCsb49744	Yes	WebVPN: New crash behavior w buffer capture
CSCsb50946	Yes	High cpu due to shun command
CSCsb52950	Yes	With banner exec command and # as delimiter replication not correct
CSCsb53407	Yes	MFIB: tracebacks when bouncing multicast-routing
CSCsb54403	Yes	mcast: asa crashes after inside router pings 226.1.1.1
CSCsb54545	Yes	Traceback eip _keyword_option_flex_action with show ip local pool
CSCsb55282	Yes	sh inventory does not show 4GE module
CSCsb55550	Yes	traceback in pki_ctm:_pki_ctm_verify_signature+164 - 8192 bit certs conn
CSCsb56247	Yes	traceback in crypto_pki:_crypto_pki_poll_crl+52 - with crl opt PKI
CSCsb56367	Yes	webvpn: assertion in thread emweb/https when max webvpn sessions reached
CSCsb58364	Yes	VPNFO: tunnels get dropped when fover occurs
CSCsb58364	Yes	VPNFO: tunnels get dropped when fover occurs
CSCsb60861	Yes	WebVPN session attempt with proto=webvpn off, causes emweb crash
CSCsb61027	Yes	mcast: secondary crashes shortly after sync'd with primary
CSCsb61544	Yes	WebVPN: Traceback within obj-f1/http_ewa:_ewaNetHTTPSend+162
CSCsb61644	Yes	ASA crashes when acessing ASDM over IPSec/TCP-10000 tunnel
CSCsb61832	Yes	HTTP-Proxy functionality (Port Forwarding) not working on Windows ME
CSCsb62617	Yes	VPN: assertion 0 failed: file malloc.c, line 4570 RA dial/hang test
CSCsb62908	Yes	Closing the Port Forwarding Applet removes existing Proxy configuration
CSCsb63920	Yes	CLI: no ssl trust-point cmmd causes traceback, ssl_chain:_ssl_trustpoint
CSCsb64159	Yes	VPNLB: need ability to assign a trustpoint to the vcpip address
CSCsb64985	Yes	4ge module interface stops passing traffic after using QoS and L2L tunn
CSCsb67119	Yes	Inspect ESMTP incorrectly rewrites smtp reply containing 220 in text
CSCsb67166	Yes	Time based ACLs not working properly if object groups are used
CSCsb70268	Yes	'hw-module module 1 reload reloads 4GE module
CSCsb71198	Yes	incorrectly formatted DL ACL causes traceback in IKE daemon
CSCsb72604	Yes	crash in snmp thread after nmap UDP scan of port 161

Table 4 Resolved Caveats (continued)

	Software Release 7.0(4)	
ID Number	**Corrected**	**Caveat Title**
CSCsb72665	Yes	IX 7 may drop valid TCP segments that carry data in final segment
CSCsb72803	Yes	rash triggered when system is out of memory
CSCsb74050	Yes	F1 crashed when sweep-ping (G-PDU) thru GTP tunnel v0
CSCsb74836	Yes	MFW-R: ASA crash on SSM reboot from IDM
CSCsb75857	Yes	F1 hit memory corrution crash @ clear conf gtp then clear conf all
CSCsb76268	Yes	Immediately after upgrade to 7.0(1) - interfaces stuck in waitingstate
CSCsb77332	Yes	traceback in fover_parse on standby unit if config contains webtype acl
CSCsb77397	Yes	Traceback: eip 0x00c3426c strcpy:_strcpy+12, using deb menu ike commands
CSCsb78230	Yes	hw-module module 1 shut and reset do not bring up the 4ge module
CSCsb79742	Yes	incorrectly formatted downloadable acl causes traceback in emweb/https
CSCsb80196	Yes	DHCP ID String is limited to 50 characters, should be 128
CSCsb81575	Yes	key gen causes an assert if ASA has DES only license
CSCsb82663	Yes	Out of order TCP packets degrade HTTP inspection performance
CSCsb83962	Yes	F1 OSPF regression scripts hang with removal of router config
CSCsb85767	Yes	URL Filtering with long URLs could cause memory corruption
CSCsb85780	Yes	Malformed HTTP GET request causes URL filtering module to cause a crash.
CSCsb88557	Yes	Traceback at snap:_snap_mini_dump+26 with acl Logging: thread-arp_timer
CSCsb89147	Yes	certificate-to-username mapping broken for some DN attributes
CSCsb91835	Yes	ASA reload in smtp/esmtp inspection {insp_process_smtp_data}
CSCsb91837	Yes	vpn-filter incorrectly blocking traffic with echo, echo-response keyword
CSCsb93659	Yes	Local IP doesn't get translated with NAT Exemption
CSCsb94651	Yes	Overlapping static statements should be allowed
CSCsb94689	Yes	4GE card firmware accessing incorrect PHY address
CSCsb95027	Yes	Stadby Betabox rebooted while upgrading to 7.0.3.19
CSCsb95259	Yes	No hits shown on access-list associated to a group-policy vpn-filter
CSCsb97680	Yes	traceback in radpact:_RADPBldHWClientReauth+260 during 3002 New Pin Mode
CSCsb99192	Yes	Show access-list | inc xxx causes traffic through device to be delayed
CSCsb99360	Yes	Logging queue 0 is wrongly shown as being unlimited queue
CSCsc00709	Yes	ASA enable authentication issue
CSCsc02230	Yes	nat entry with outside keyword : ERROR: unable to download policy
CSCsc02485	Yes	Session Cmd: sendind 036xr to exit session to ssm causes Traceback
CSCsc02574	Yes	pki: ID cert signature validation failure allows successful connection
CSCsc06282	Yes	fover: ip local pool fails to replicate after issuing from grp submode
CSCsc06477	Yes	unable to manage running config with err msg: configuration in progress
CSCsc06702	Yes	VPN: Interface counters are incorrectly incremented on decrypted packets

Table 4 Resolved Caveats (continued)

ID Number	Software Release 7.0(4)	
	Corrected	Caveat Title
CSCsc08843	Yes	DHCP-Relay drops packets when source address is non-zero
CSCsc09527	Yes	VPNFO: cannot establish a vpn tunnel "session limit reached" sa cnt -1
CSCsc09932	Yes	Assertion in file "vf_api.c", line 264, traceback in strdup:_int3+4
CSCsc14837	Yes	ARP fails on the 4GE interfaces in routed firewall mode

Related Documentation

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

- *Cisco ASA 5500 Hardware Installation Guide*
- *Cisco ASA 5500 Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*

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.