



Cisco ASA 5580 Series Release Notes Version 8.1(2)

April 6, 2009

These release notes describe the features and caveats for Cisco ASA 5580 software Version 8.1(2). This document includes the following sections:

- [System Requirements, page 1](#)
- [New Features, page 5](#)
- [Important Notes, page 10](#)
- [Caveats, page 11](#)
- [End-User License Agreement, page 24](#)
- [Related Documentation, page 24](#)
- [Obtaining Documentation and Submitting a Service Request, page 24](#)

System Requirements

This section lists the system requirements for operating an adaptive security appliance, and includes the following topics:

- [Supported Models, page 2](#)
- [Management Support, page 2](#)
- [Memory Requirements, page 2](#)
- [Determining the Software Version, page 3](#)
- [Downloading the Software, page 3](#)
- [Installing or Upgrading Cisco Secure Desktop, page 4](#)



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

© 2009 Cisco Systems, Inc. All rights reserved.

Supported Models

Software Version 8.1(2) supports the following platform models:

- ASA 5580-20
- ASA 5580-40

Management Support

Software Version 8.1(2) is supported by ASDM Version 6.1(5).

Memory Requirements

[Table 1](#) lists the DRAM memory requirements for the adaptive security appliance. The memory listed in this table is the default value that ships with each adaptive security appliance.

Table 1 DRAM Memory Requirements

ASA Model	Default DRAM Memory
5580-20	8 GB
5580-40	12 GB



Note

On both the ASA 5580-20 and the ASA 5580-40 adaptive security appliances only 4 GB of memory is available for features. The rest are reserved or used by the OS. The **show memory** command will only display values relative to 4GB.

You can check the size of internal flash and the amount of free flash memory on the adaptive security appliance by doing the following:

- ASDM—Choose **Tools > File Management**. The amounts of total and available flash memory appear on the bottom left in the pane.
- CLI—In privileged EXEC mode, enter the **dir** command. The amounts of total and available flash memory appear at the bottom of the output.

For example:

```
hostname # dir
Directory of disk0:/

 2      drwx  4096      11:22:00 Dec 01 2006  cisco_config
 43     -rwx 14358528   08:46:02 Feb 19 2007  cdisk.bin
 44     -rwx  4634     14:32:48 Sep 17 2004  first-backup
 45     -rwx  4096     09:55:02 Sep 21 2004  fsck-2451
 46     -rwx  4096     09:55:02 Sep 21 2004  fsck-2505
 47     -rwx   774     10:48:04 Nov 21 2006  profile.tpl
 48     -rwx 406963    12:45:34 Feb 06 2007  svc
 3      drwx  8192     03:35:24 Feb 02 2007  log
 49     drwx  4096     07:10:54 Aug 09 2006  1
 50     -rwx 21601     14:20:40 Dec 17 2004  tftp
 51     -rwx 17489     06:36:40 Dec 06 2006  custom.xml
 136    -rwx 12456368  10:25:08 Feb 20 2007  asdmfile
```

```

53  -rwx 20498      13:04:54 Feb 12 2007  tomm_english
54  drwx 4096      14:18:56 Jan 14 2007  sdesktop
56  -rwx 14358528  08:32:30 Feb 19 2007  asa800-215-k8.bin
57  -rwx 10971     09:38:54 Apr 20 2006  cli.lua
58  -rwx 6342320  08:44:54 Feb 19 2007  asdm-600110.bin
59  -rwx 0         04:38:52 Feb 12 2007  LOCAL-CA-SERVER.udb
60  -rwx 322      15:47:42 Nov 29 2006  tmpAsdmCustomization1848612400
8   -rwx 65111     10:27:48 Feb 20 2007  tomm_backup.cfg
61  -rwx 416354    11:50:58 Feb 07 2007  sslclient-win-1.1.3.173.pkg
62  -rwx 23689    08:48:04 Jan 30 2007  asa1_backup.cfg
63  -rwx 45106    07:19:18 Feb 12 2007  securedesktop_asa_3_2_0_54.pkg
64  -rwx 224      01:22:44 Oct 02 2006  LOCAL-CA-SERVER.crl
65  drwx 4096     12:37:24 Feb 20 2007  LOCAL-CA-SERVER
66  -rwx 425      11:45:52 Dec 05 2006  anyconnect
67  -rwx 1555     10:18:04 Sep 29 2006  LOCAL-CA-SERVER_00001.p12
68  -rwx 0        12:33:54 Oct 01 2006  LOCAL-CA-SERVER.cdb
69  -rwx 3384309  07:21:46 Feb 12 2007  securedesktop_asa_3_2_0_57.pkg
70  -rwx 774      05:57:48 Nov 22 2006  cvcprofile.xml
71  -rwx 338      15:48:40 Nov 29 2006  tmpAsdmCustomization430406526
72  -rwx 32       09:35:40 Dec 08 2006  LOCAL-CA-SERVER.ser
73  -rwx 2205678  07:19:22 Jan 05 2007  vpn-win32-Release-2.0.0156-k9.pkg
74  -rwx 3380111  11:39:36 Feb 12 2007  securedesktop_asa_3_2_0_56.pkg

```

62881792 bytes total (3854336 bytes free)

hostname #

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



Note

If you use two units with different flash memory sizes, make sure that the unit with the smaller flash memory has enough space for the software images and configuration files.

Determining the Software Version

Use the **show version** command to verify the software version of your adaptive security appliance. Alternatively, the software version appears on the Cisco ASDM home page.

Downloading the Software

You can download the software from the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

To download the software to flash memory, choose one of the following commands for the appropriate download server type:

- To copy from a TFTP server, enter the following command:

```
hostname# copy tftp://server[/path]/filename {flash:/ | disk0:/ |
disk1:/} [path/] filename
```

You can enter **flash:/** or **disk0:/** for the internal flash memory on the adaptive security appliance. The **disk1:/** keyword represents the external flash memory on the adaptive security appliance.

- To copy from an FTP server, enter the following command:

```
hostname# copy ftp://[user[:password]@]server[/path]/filename {flash:/ | disk0:/ |
disk1:/}[path/]filename
```

- To copy from an HTTP or HTTPS server, enter the following command:

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename {flash:/ |
disk0:/ | disk1:/}[path/]filename
```

- To use secure copy, first enable SSH, then enter the following command:

```
hostname# ssh scopy enable
```

Then from a Linux client, enter the following command:

```
scp -v -pw password filename username@asa_address
```

The **-v** specifies verbose. If **-pw** is not specified, you are prompted for a password.

Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2 requires ASA Version 8.1. You do not need to restart the adaptive security appliance after you install or upgrade Cisco Secure Desktop.



Note Archive and delete the Secure Desktop desktop/data.xml configuration file before upgrading to Cisco Secure Desktop 3.2. To create a clean configuration file, uninstall Cisco Secure Desktop before reinstalling it.

The expanded flexibility provided by a prelogin assessment sequence editor, and replacement of the Cisco Secure Desktop feature policies with a dynamic access policy (DAP) configured on the adaptive security appliance, are incompatible with Cisco Secure Desktop 3.1.1 configurations. Cisco Secure Desktop automatically inserts a new, default configuration file when it detects that one is not present.

For consistency with the previous release notes, these instructions provide the CLI commands needed to install Secure Desktop. You may, however, prefer to use ASDM. To do so, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup** and click **Help**.

To install or upgrade the Cisco Secure Desktop software, perform the following steps:

- Step 1** Download the latest Cisco Secure Desktop package file from the following website and install it on the flash memory card of the adaptive security appliance:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

- Step 2** Enter the following commands to access webvpn configuration mode:

```
hostname# config terminal
hostname(config)# webvpn
hostname(config-webvpn)#
```

- Step 3** To validate the Cisco Secure Desktop distribution package and add it to the running configuration, enter the following command in webvpn configuration mode:

```
hostname(config-webvpn)# csd image disk0:/securedesktop_asa_3_2_0_build.pkg
hostname(config-webvpn)#
```

- Step 4** To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in webvpn configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.

```
hostname(config-webvpn) # csd enable
hostname(config-webvpn) #
```

New Features

Table 2 lists the new features for Version 8.1(2).



Note

Version 8.1(x) is only supported on the Cisco ASA 5580 adaptive security appliance.

Table 2 ***New Features for ASA Version 8.1(2)***

Feature	Description
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE	<p>This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature.</p> <p>Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host.</p> <p>To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy.</p> <p>In ASDM, see Configuration > Firewall > Advanced > ACL Manager.</p>
Entrust Certificate Provisioning	<p>ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x) includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.</p> <p>In ASDM, see Configuration > Remote Access VPN > Certificate Management > Identity Certificates > Enroll ASA SSL VPN head-end with Entrust.</p>
Extended Time for User Reauthentication on IKE Rekey	<p>You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.</p> <p>In ASDM, see Configuration > Device Management > Certificate Management > Identity Certificates.</p>

Table 2 New Features for ASA Version 8.1(2) (continued)

Feature	Description
Persistent IPsec Tunneled Flows	<p>With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a hardware client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the sysopt connection preserve-vpn-flows command. This option is disabled by default.</p> <p>In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options. Check the Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM) checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command show ad-groups was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy.</p> <p>In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit DAP > Add/Edit AAA Attribute.</p>
Smart Tunnel over Mac OS	<p>Smart tunnels now support Mac OS.</p> <p>In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels.</p>
Firewall Features	
NetFlow Filtering	<p>You can filter NetFlow events based on traffic and event-type, and then send records to different collectors. For example, you can log all flow-create events to one collector, but log flow-denied events to a different collector. See the flow-export event-type command.</p> <p>In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > NetFlow.</p>
NetFlow Delay Flow Creation Event	<p>For short-lived flows, NetFlow collecting devices benefit from processing a single event as opposed to seeing two events: flow creation and teardown. You can now configure a delay before sending the flow creation event. If the flow is torn down before the timer expires, only the flow teardown event will be sent. See the flow-export delay flow-create command.</p> <p>Note The teardown event includes all information regarding the flow; there is no loss of information.</p> <p>In ASDM, see Configuration > Device Management > Logging > NetFlow.</p>
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the adaptive security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the shape command.</p> <p>See also the crypto ipsec security-association replay command, which lets you configure the IPsec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPsec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms.</p> <p>In ASDM, see Configuration > Firewall > Security Policy > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p>

Table 2 **New Features for ASA Version 8.1(2) (continued)**

Feature	Description
TCP Normalization Enhancements	<p>You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.</p> <ul style="list-style-type: none"> • TCP invalid ACK check (the invalid-ack command) • TCP packet sequence past window check (the seq-past-window command) • TCP SYN-ACK with data check (the synack-data command) <p>You can also set the TCP out-of-order packet buffer timeout (the queue command timeout keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.</p> <p>The default action for packets that exceed MSS has changed from drop to allow (the exceed-mss command).</p> <p>The following non-configurable actions have changed from drop to clear for these packet types:</p> <ul style="list-style-type: none"> • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option <p>In ASDM, see Configuration > Firewall > Objects > TCP Maps.</p>
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the threat-detection statistics tcp-intercept command, and view them using the show threat-detection statistics command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Threat detection shun timeout	<p>You can now configure the shun timeout for threat detection using the threat-detection scanning-threat shun duration command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Threat detection host statistics fine tuning	<p>You can now reduce the amount of host statistics collected, thus reducing the system impact of this feature, by using the threat-detection statistics host number-of-rate command.</p> <p>In ASDM, see Configuration > Firewall > Threat Detection.</p>
Platform Features	
Increased VLANs	<p>The number of VLANs supported on the ASA 5580 are increased from 100 to 250.</p>
SNMP support for unnamed interfaces	<p>Formerly, SNMP only provided information about interfaces that were configured using the nameif command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. SNMP was enhanced to show information about all physical interfaces and logical interfaces; a nameif command is no longer required to display the interfaces using SNMP.</p>

SNMP Changes

This section describes the updated approach used by SNMP to display adaptive security appliance interfaces, and the additional link state traps that are sent for interfaces.

Before Version 7.2(5)/8.0(4)/8.1(2), SNMP only provided information about interfaces that were configured using the **nameif** command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. SNMP was enhanced to show information about all physical interfaces and logical interfaces; a **nameif** command is no longer required to display the interfaces using SNMP.

This section includes the following topics:

- [IF MIB Output Changes, page 8](#)
- [IP MIB Output Changes, page 10](#)
- [SNMP Link State Trap Changes, page 10](#)

IF MIB Output Changes

SNMP was enhanced to show information about all physical interfaces and logical interfaces, including internal interfaces; a **nameif** command is no longer required to display the interfaces using SNMP.

You might see information about the following internal interfaces:

- Null0—Not currently in use.
- Internal-Data or Internal-Control—Internal interfaces for communicating with SSMs or SSCs.
- `_internal_loopback`—The loopback interface.
- Virtual—Used for phone proxy media termination functions.

The following topics show a sample interface configuration on the ASA 5505, and sample ifDescr output:

- [Sample Interface Configuration, page 8](#)
- [Sample ifDescr Output, page 9](#)



Note

Although these examples show the ASA 5505, Version 8.1 only supports the ASA 5580. The SNMP changes apply to all supported platforms.

Sample Interface Configuration

The following example shows the interface configuration for an ASA 5505; refer to this example when looking at the ipDescr sample output in the [“Sample ifDescr Output” section on page 9](#).

```
interface Vlan1
 nameif user
 security-level 40
 ip address 192.168.4.1 255.255.255.0

interface Vlan40
 no nameif
 security-level 0
 no ip address

interface Vlan41
 no nameif
 security-level 100
 no ip address

interface Vlan46
 no nameif
 security-level 0
```

```

no ip address

interface Vlan47
  no nameif
  security-level 100
  no ip address

interface Vlan100
  nameif inside
  security-level 100
  ip address 10.7.1.80 255.255.255.0

interface Vlan112
  no nameif
  security-level 10
  no ip address

interface Vlan114
  nameif mgmt
  security-level 10
  ip address 10.8.1.80 255.255.255.0

interface Vlan200
  nameif outside
  security-level 0
  ip address 10.9.1.80 255.255.255.0

interface Ethernet0/0
  switchport trunk allowed vlan 100
  switchport mode trunk

interface Ethernet0/1
  switchport trunk allowed vlan 1,200
  switchport mode trunk

interface Ethernet0/2
  switchport access vlan 114

interface Ethernet0/3

interface Ethernet0/4

interface Ethernet0/5

interface Ethernet0/6

interface Ethernet0/7

```

Sample ifDescr Output

The following ifDescr output shows the difference before and after the SNMP changes (changes are shown in bold):

Before:

```

IF-MIB::ifDescr.1 = Adaptive Security Appliance 'user' interface
IF-MIB::ifDescr.2 = Adaptive Security Appliance 'inside' interface
IF-MIB::ifDescr.3 = Adaptive Security Appliance 'mgmt' interface
IF-MIB::ifDescr.4 = Adaptive Security Appliance 'outside' interface

```

After:

```

IF-MIB::ifDescr.1 = Adaptive Security Appliance 'Null0' interface
IF-MIB::ifDescr.2 = Adaptive Security Appliance 'Internal-Data0/0' interface
IF-MIB::ifDescr.3 = Adaptive Security Appliance 'Ethernet0/0' interface
IF-MIB::ifDescr.4 = Adaptive Security Appliance 'Ethernet0/1' interface
IF-MIB::ifDescr.5 = Adaptive Security Appliance 'Ethernet0/2' interface
IF-MIB::ifDescr.6 = Adaptive Security Appliance 'Ethernet0/3' interface
IF-MIB::ifDescr.7 = Adaptive Security Appliance 'Ethernet0/4' interface
IF-MIB::ifDescr.8 = Adaptive Security Appliance 'Ethernet0/5' interface
IF-MIB::ifDescr.9 = Adaptive Security Appliance 'Ethernet0/6' interface
IF-MIB::ifDescr.10 = Adaptive Security Appliance 'Ethernet0/7' interface
IF-MIB::ifDescr.11 = Adaptive Security Appliance 'Internal-Data0/1' interface
IF-MIB::ifDescr.12 = Adaptive Security Appliance '_internal_loopback' interface
IF-MIB::ifDescr.13 = Adaptive Security Appliance 'Virtual254' interface
IF-MIB::ifDescr.14 = Adaptive Security Appliance 'user' interface
IF-MIB::ifDescr.15 = Adaptive Security Appliance 'Vlan40' interface
IF-MIB::ifDescr.16 = Adaptive Security Appliance 'Vlan41' interface
IF-MIB::ifDescr.17 = Adaptive Security Appliance 'Vlan46' interface
IF-MIB::ifDescr.18 = Adaptive Security Appliance 'Vlan47' interface
IF-MIB::ifDescr.19 = Adaptive Security Appliance 'inside' interface
IF-MIB::ifDescr.20 = Adaptive Security Appliance 'Vlan112' interface
IF-MIB::ifDescr.21 = Adaptive Security Appliance 'mgmt' interface
IF-MIB::ifDescr.22 = Adaptive Security Appliance 'outside' interface

```

IP MIB Output Changes

Walking the IP MIB now shows IP addresses assigned to all interfaces, not just those configured using the **nameif** command.

SNMP Link State Trap Changes

SNMP now sends traps at bootup, when an interface is shut down, or when an interface is brought up for all physical interfaces and logical interfaces; a **nameif** command is no longer required to send traps about interfaces. Before this enhancement, traps were sent only for interfaces that had a name configured.

Important Notes

Please note the following upgrade and operational considerations:

- **flow-export enable** Command Conversion—If you are upgrading from Version 8.1(1) to 8.1(2), and you configured the **flow-export enable** command, then it is converted to the Modular Policy Framework **flow-export event-type all destination** command. It is added to the class-default class map in the global service policy. If a global service policy does not exist, one is created. For example, the **flow-export enable** command is converted to the following:

```

hostname(config-pmap)# policy-map global_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# flow-export event-type all destination flow_export_host1
flow_export_host2
hostname(config-pmap-c)# service-policy global_policy global

```

The *flow_export_host1* and *flow_export_host1* arguments are populated by the **flow-export destination** commands.

- No .NET over Clientless—Clientless sessions do not support .NET framework applications (CSCsv29942).
- When using Clientless SSL VPN Post-SSO parameters for the Citrix Web interface bookmark, Single-Signon (SSO) works, but the Citrix portal is missing the Reconnect and Disconnect buttons. Only the Log Off button shows. When not using SSO over Clientless, all three buttons show up correctly.

Workaround: Use the Cisco HTTP-POST plugin to provide single signon and correct Citrix portal behavior.

Caveats

The following sections describe the caveats for Version 8.1(2):

- [Open Caveats - Version 8.1\(2\), page 11](#)
- [Resolved Caveats - Version 8.1\(2\), page 12](#)

For your convenience in locating caveats in the Cisco 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.



Note

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://www.cisco.com/support/bugtools>

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

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

Open Caveats - Version 8.1(2)

Table 3 Open Caveats in Version 8.1(2)

Caveat ID	Description
CSCsm12724	Traceback while enrolling multiple users with local CA
CSCsm69576	"FT: ""failover active"" with 5000 IPsec RAS tunnels causes FO instability"
CSCsm77414	Traceback while applying a large regex config twice and then removing it
CSCsr78362	ASA 8.1.1 : ACL corruption with DNS traffic
CSCsu05551	brief outage re-establishing failover link/state in active/active mode
CSCsu11412	Watchdog traceback in CTM under high data load/small packets
CSCsu77465	connection is not locked when releasing a child connection on standby
CSCsu92454	Standby 5580 Traceback in Thread Name: DATAPATH-7-563

Resolved Caveats - Version 8.1(2)

Table 4 Resolved Caveats in Version 8.1(2)

Caveat ID	Description
CSCsg69408	Need warning when using time based ACLs with policy NAT/PAT
CSCsg75094	LDAP: ASA cannot authenticate to Active Directory using MD5
CSCsh91747	SSL VPN stress cause SSL lib error. Function: DO_SSL3_WRITE
CSCsi06469	Inactivating then reactivating nat 0 multiple access-lists breaks nat 0
CSCsi79159	admin connections to PIX with crypto card via management-access fail
CSCsj05862	Traceback in Thread Name: radius_snd
CSCsj25896	Crypto Accelerator Memory Leak
CSCsk08454	ASA 8.0 fails to send TACACS request over L2L tunnel
CSCsk27107	ldap CRL retrieval fails - ldap-default not used
CSCsk42595	ASA:: 2 Factor Authentication with Password-Management Fails for SSL VPN
CSCsk47949	ASDM hangs at 47% if packet losses on the network
CSCsk48355	ISAKMP SA stuck in AM_WAIT_DELETE after ASA upgrade
CSCsk50583	IPV6: Anyconnect does not work when using ipv6 with vlans.
CSCsk59189	Top N data sent to ASDM is incorrect when ACE changes
CSCsk63633	WebVPN: ERROR: Invalid tunnel group name <certs> during replication
CSCsk87951	Group URL not working as expected with AnyConnect
CSCsk89022	ASA traceback while removing dhcpd configuration.
CSCsk96804	Traceback in Thread Name: Dispatch Unit with inspect h323
CSCsk97830	Traceback in thread name Dispatch Unit .
CSCsl02630	WebVPN: Traceback in Thread Name: emweb/https
CSCsl10052	new L2TP sessions are denied after %ASA-4-403103 is seen in the logs
CSCsl10066	ASDM states ASDM is temporarily unable to contact the firewall
CSCsl32785	Traceback in Thread Name: pix_flash_config_thread
CSCsl34791	WebVPN: Traceback in Thread Name: Dispatch Unit
CSCsl43246	L2TP with EAP authentication In use List count session slowly leaking
CSCsl51292	IPSEC VPN tunnel on 8.0.3 fails every couple days
CSCsl51797	ASA traceback in AAA thread
CSCsl52895	ASA 7.2.3 number of IPsec SA not replicated in failover unit
CSCsl57533	"setting privilege for capture does not affect ""no capture"""
CSCsl59247	Unable to request CRL for trustpoint with only ID certificate
CSCsl66538	"ASA ""hardware accelerator encountered an error (Invalid PKCS Type)"""
CSCsl79211	Traceback: AAA task overflow when object-group acls and virtual telnet
CSCsl82200	IPSec not encrypting after failover.
CSCsl84204	Xlate timers for RTP/RTCP on standby unit aren't synched with active

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsI94183	ASA- Clientless webvpn 'error contacting host' accessing CIFS shares
CSCsI95244	Traceback in Dispatch Unit caused by rapid connection successions
CSCsI95286	Control-plane feature not working for https traffic to-the-box
CSCsI95856	DHCP learned default route not in route table if other DHCP interfaces
CSCsI96219	SIP: Failure to associate re-invites to the original SIP session
CSCsI96502	SIP: sess is not kept around for ACK in response to non2xx final RESP
CSCsI99322	Traceback at ids_put in Thread Name: Dispatch Unit
CSCsm01524	"Outlook, Outlook express email proxy functionality broken in 8.0.2"
CSCsm02280	Status says registering but device does not send Register packets
CSCsm02939	Memory leak while processing SSL transactions
CSCsm05055	Traceback seen when 'established udp 0 0' command is enabled
CSCsm09584	EAP I2tp authentication fails if mschapv2 is configured on the same TG
CSCsm10353	AnyConnect password that contains brackets <> will fail authentication
CSCsm14283	"ICMP (type 3, code 4) packet not returned from PPPoE interface"
CSCsm20204	Extended ping command with no ip specified causes stuck thread
CSCsm21493	SSLVPN : 'vlan' restriction in a group-policy propagated to all policies
CSCsm22002	Traceback in qos/qos_rate_limiter while processing pakt with TCP flow
CSCsm22781	PIX/ASA: RPF(reverse path forwarding)chk fails when PMTUD packet is sent
CSCsm25189	Inconsistent behavior for different kind of SIP packets
CSCsm26841	Watchdog failure: TLS fragmented client hello message.allocb+185
CSCsm30926	ASA: Traceback with high voice traffic and voice inspection
CSCsm32507	External group policy authentication failure with password-management
CSCsm32904	Login fails when CRL not cached
CSCsm36660	DHCP Server: Must send DHCP decline if DHCP proposes in-use address
CSCsm36857	External group-policy via Radius can cause duplicate IP assignment
CSCsm37151	skinny inspection blocking pinhole w/ high skinny load on rsvp agent
CSCsm39241	PIX/ASA: Traceback in Thread Name: netfs_thread_init
CSCsm39781	ASA High CPU under certain configuration conditions
CSCsm39805	Unable to configure http access in order to manage ASDM
CSCsm40251	ASDM falsely shows interface status as down/down
CSCsm41986	Need to handle fragmented IP packets with 8-byte first frag
CSCsm44988	ASA does not send authentication request to http-form aaa-server
CSCsm45722	SIP:Caller's RTP/RTCP timeout should set to sip_invite
CSCsm46182	DHCP Client: Device's DHCP client does not renew when lease expires
CSCsm46248	ASA traceback in netfs thread unit
CSCsm46880	Aware HTTP Server: memory leak

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsm47185	traceback when an interface configured for IPV6 changes to link up state
CSCsm48386	ASA with local command authorization not able to download conf from AUS
CSCsm49741	Clientless SSI VPN: Max session timeout popup not displayed
CSCsm50135	Memory leakage caused by catcher_recv_packet_have_sa
CSCsm50494	Device is not able to process CRL with extension CRL number > 65535
CSCsm50856	L2L: Phase 2 SA fails when both sides try to initiate at the same time.
CSCsm51093	Cannot establish WebVPN session to ASA-5550 - memory allocation error
CSCsm51459	GTP: IMSI prefixing doesn't work with 2 digit MNC
CSCsm55261	Cannot establish WebVPN session to ASA-5510 - memory allocation error
CSCsm55447	ASA/WebVPN Citrix sessions randomly dropped
CSCsm55947	"Failover interface is not listed in ""ifTable"" MIB"
CSCsm56957	Traceback occurs in Dispatch Unit with QoS
CSCsm57803	DAP: network filter is deleted for all clients upon disconnect of user
CSCsm57920	H323: inspection on video call may cause traceback within 5 min
CSCsm59304	SIP: INVITE not passing after failover
CSCsm60846	DAP: Tunnel Group attribute is not populated with Cert Authentication
CSCsm61494	"SIP: Inspection may open unknown port ""50195"""
CSCsm61775	SIP: Unnecessary xlate created after a voice device hands over
CSCsm62080	ASA 8.0 webvpn corrupts radius request when using domain
CSCsm62831	SIP: Unneeded half-open xlate entry is generated
CSCsm63108	2048 blocks depleted with swebsense url-filtering enabled
CSCsm64838	Traceback occurs in Dispatch Unit with 7.2.3.15 and L2TP/PPP
CSCsm65019	Websense encryption is not supported error on ASA
CSCsm66887	Nas-Port attribute differs for authentication/accounting for l2tp/ipsec
CSCsm66982	PIX/ASA: L2TP session should not establish when authorization fails
CSCsm68097	SSH resource exhausted preventing further sessions
CSCsm69116	L-L tunnels still failing upon IP addr change on peer.
CSCsm70077	SIP:Local/Local connection entry is created
CSCsm70101	Unable to apply priority command in policy map while configuring QOS-ASA
CSCsm70246	"SIP: Duplicate ""mi"" connections when receiving REINVITE"
CSCsm71691	Plug-in client fails when the Citrix farm is set with heightened encrypt
CSCsm71772	Memory leak in 141824 size block when using cut-through authentication
CSCsm73565	Traceback in Thread Name Dispatch Unit during network scan
CSCsm73574	ASA 5505 asserts when configuration is cleared
CSCsm73654	Syslog 111111 appears when both active/standby units reload at once
CSCsm75212	Traceback in Thread Name: IKE Daemon (Old pc 0x0050a493 ebp 0x0346e)

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsm77958	ASA may crash while processing PPPoE and SSL VPN transactions
CSCsm80984	show version: command displays incorrect value for total RAM
CSCsm81609	ASDM: users go to portal page instead of SVC starting automatically
CSCsm82753	Phase 2 fails if PFS is required. - ASA -IOS l2tp IPSEC
CSCsm82803	webvpn load balancing presents wrong certificate after reboot
CSCsm82887	FO: IPsec RA session not replicated if addr pool defined in group policy
CSCsm82893	Existing Local CA Users are deleted when modifying User Database
CSCsm83007	WebVPN: Message body is blank when sent w/ Firefox via Lotus iNotes Web
CSCsm83098	SIP:Fails to create m connection when ACK to 407 is lost
CSCsm83636	CPU hog during config sync
CSCsm84110	ASA may traceback with malformed TCP packets
CSCsm85736	shutdown interface e0/6 triggers interface e0/0 shutdown on ASA5505
CSCsm85872	snmp trap for PHYSICAL interface is not sent when a port goes down.
CSCsm86188	ASA 5580: Management interface causes packet loss in transparent mode
CSCsm86644	sunrpc tcp inspect fragment reassembly fails in certain cases.
CSCsm87035	DHCP Relay: offer msg is not egressing to ASA interface going to another
CSCsm87351	simultaneous accounting - the request are not forwarded to FAILED serve
CSCsm87892	ASA 5505 Interface Hangs
CSCsm88116	SIP:Failure to update to-tag when no-2xx response is received
CSCsm90239	ASA traceback in Unicorn Admin Handler Thread
CSCsm90267	SIP: media pinholes not opened when callers SDP is sent in ACK
CSCsm91261	Traceback seen in 'ssh' thread
CSCsm92266	Traceback may occur when AAA command authorization is enabled
CSCsm92275	SQL inspection rewrites IP addresses embeded in SQL data
CSCsm92423	Memory leak found in DTLS
CSCsm92613	ASP drop capture missing type for vpn-handle-error
CSCsm93071	5505: 'no buffer' and 'input error' not correct on InternalData0/0
CSCsm93115	Memory leak in DMA free crypto memory 8.0.3.6
CSCsm95566	EIGRP: Does not send ALL redistributed static routes to peer devices
CSCsm95593	Accounting-start sent before access-request for L2TP VPN
CSCso00670	Move ssl debug commands from menu to real CLI
CSCso01090	ASA5505:copy config from disk0:/ to running-config makes int e0/0 down
CSCso03100	SSL cache entries timing out prematurely
CSCso03582	Overrun counter increments when REINVITE is received
CSCso03722	L2TP/IPsec session increases MIB active user statistics
CSCso05327	Cert from 3k imported into ASA causes Hardware error on use

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCso05797	ASA stops accepting L2TP/IPSec connections with rsa-sig
CSCso06690	ASA 8.0.3.2 memory leak in 0x089a27a5 <cifs_browse_server_sync+1349>
CSCso07025	Memory is leaked whenever directory is opened.
CSCso08335	ISAKMP: Add syslog when Aggressive mode aborted when Spoof Protection
CSCso08954	Traceback in Unicorn Proxy Thread (Old pc 0x08acb2dc <fiber_yield+92>)
CSCso10078	Traceback occurs when wr mem command is entered
CSCso10129	PIX puts user in unusable prompt when webvpn attributes command is used
CSCso10876	ASA Completes SSL Handshake With Non-Authorized HTTPS Clients
CSCso15583	Traceback when many remote peers try to establish ipsec L2L tunnels
CSCso17518	Traceback with 200+ ldap group memberships and radius accounting
CSCso17578	VPNLB: WebVPN client cannot connect to VPN load-balancing cluster
CSCso17900	DFP may not background free due to memory calculation
CSCso17920	SIP media connection cannot be created more than 13 when PBX is used
CSCso18045	PKI: session opening checks client-types instead of id-usage setting
CSCso18239	Certificate authentication failing because of the certificate size
CSCso18757	SNMP crasSessionTable Remote Access MIB returns some incorrect entries
CSCso20009	ASA DHCP proxy not working for L2TP connections
CSCso21019	SNMP crasSessionTable Remote Access MIB incorrect EncryptionAlgo
CSCso21063	l2tp/ipsec client on IOS - tunnel does not go up when behind nat
CSCso22981	Traceback in Thread Dispatch unit related to IM inspection
CSCso24103	Delivering shape average command through https failed
CSCso24494	PIX/ASA: DHCP server fails to respond to Vista DHCPINFORM request
CSCso26240	Not able to configure redundant subinterfaces in multicontext
CSCso31622	"WebACLs ""log disable"" changes ACE to ""log informational internal 300"""
CSCso33343	5505: CPU usage averages 60+% on idle device
CSCso33791	VPNC: Erroneous Tunnel Rejected Syslog when connecting
CSCso33873	L2TP/IPsec connection cannot pass data
CSCso35351	Traceback in Thread Name: vpnfol_thread_msg with show run
CSCso35664	http server leaks AWARE contexts
CSCso36070	Value returned by sysServices MIB is incorrect
CSCso37056	Memory leak when generating Diffie-Hellman keys.
CSCso38699	CPU Hog when replicating config to standby unit
CSCso38702	IPSec Pass-through breaks after enabling RA VPN on ASA
CSCso40008	PIX is sending DN during rekey instead of FQDN
CSCso40159	Ports used by static PAT configurations are not removed from PAT pool
CSCso40520	re-INVITE is dropped when it's exceeded 119ch after establishing 400ch

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCso41122	WebVPN Citrix connection should disable idle timeout and Nagle
CSCso42643	WebFO: WebVPN sessions not replicated until after FO forced
CSCso42664	"cifs://Macro#1:Password_Macro#2@server url, Macro#2 not substituted"
CSCso43026	Traceback in Thread Name: Dispatch Unit (Old pc 0x00223a67 ebp 0x018b
CSCso43383	SIP:media xlate idle timer is not refreshed when receiving 200ok
CSCso43850	enhance redun ifc as failover ifc to handle comm failure after reload
CSCso46028	ASA 8.0 CLI : Unable to edit http-form server
CSCso48906	DAP User Message not displayed for DfltAccessPolicy
CSCso50226	PIX/ASA does not send invalid SPI notification for non-existent IPSEC sa
CSCso50272	PIX/ASA:'vpn-simultaneous-logins 1' prev session disc reason not correct
CSCso51034	Disconnect redundant interface active member cable stops traffic
CSCso51223	Traceback in Thread Name: logger_save
CSCso51544	ASA overwirtes default config when rate-interval is set to 600
CSCso52787	AAA: Radius accounting for mail-proxy SMTPS POP3S fails
CSCso53162	Traceback in DTLS with TLS fragment handling
CSCso55494	Traceback in PPP callback from AAA thread
CSCso58409	'vpn-sessiondb logoff all' does not logoff embryonic sessions
CSCso58622	"IPv6: IP services are reachable from the ""far side of the box"""
CSCso60533	Non-existing hosts counted towards the license on ASA 5505
CSCso60605	ISAKMP : ASA installs permit rule with the interface network mask
CSCso61549	Performance Monitor doesn't show all ASAs in the Load Balancing Cluster
CSCso62906	ASA traceback when running show pim tunnel <interface> command
CSCso62916	allocate interface command fails to execute intermittantly.
CSCso63159	Traceback in fover_thread while testing licensing regression scripts
CSCso63371	Panic: Dispatch Unit - Fmsg_free() - non null next on MMP traffic
CSCso64731	security-association lifetime cannot be removed with no crypto map ...
CSCso65837	write mem from HTTPS adds no monitor-interface CLIs to startup config
CSCso66472	Crypto memory leak causing Clientless SSL VPNs to hang
CSCso66807	Sometimes Group field is missing in UI when connecting using AnyConnect
CSCso68547	PIX/ASA HTTP inspection: Multiple content-length headers issue
CSCso69942	Traceback in Remote Access Authentication Code
CSCso73918	WebVPN: Standby Traceback in Thread Name: vpnfol_thread_sync
CSCso76162	Traceback in Dispatch Unit possibly with tcp proxy
CSCso76164	Traceback in Dispatch Unit with SSLVPN connection
CSCso79412	traceback in dispatch thread/occam during CUMA testing
CSCso79675	After CSD Host scan AAA doesn't execute on ASA 8.0.3.11 with group-url

Table 4 *Resolved Caveats in Version 8.1(2) (continued)*

Caveat ID	Description
CSCso79906	TCP reset sent for AnyConnect session
CSCso81153	Traceback in dispatch unit with MGCP inspection
CSCso82264	ICMP inspection may drop ICMP error packets
CSCso83246	Traceback seen while connecting via asdm running on osx platform.
CSCso84215	"High CPU by using ASDM with ""log asdm info"" configured"
CSCso84996	ASA truncates CN field at 11 characters if CN contains '@' (W2K CA)
CSCso85005	WebVPN: No disconnection due to idle timeout when using OWA with IE6
CSCso85369	CSD: DfltCustomization loaded if pre-login check enabled
CSCso85433	VPNLB: does't work when using non-default webvpn port 8.0
CSCso85452	h323 messages on console; performance degrade
CSCso85492	http redirect doesn't redirect to configured webvpn port if not 443
CSCso85547	ipAdEntIFIndex MIB value not sent at failover interface
CSCso87435	NAT-T not working when client source port not 4500 with ACL match
CSCso88533	Traceback attempting federation from LCS to CUP
CSCso89246	PP: media termination ifc doesnt come up on 5505 with base license
CSCso90892	RDP client with MAC OS using Firefox and safari fails to open
CSCso91010	ASA doesn't send RootCA cert in chain
CSCso91051	WebVPN: Broken logic with Passcode caption in the portal
CSCso91190	Traceback while deleting static NAT configuration
CSCso91658	IP tos byte for skinny/ sip packet is lost if inspection is configured
CSCso93088	Fragmented multicast traffic gets repeated and corrupted
CSCso93969	ASA mangling errors with certain webpages
CSCso94098	"SIP: ""o=""address in SDP is not translated when ""c="" is in all media desc."
CSCso94668	2048 bytes block memory leak
CSCso95135	Zero-downtime upgrade from 7.2 not possible anymore after 8.0.3.10
CSCso97405	ASA should allow configurable MSS or use from MTU for to-the-box traffic
CSCsq00551	" CSD: It will show ""please wait..."" instead of providing the logon page"
CSCsq01754	SYSOPT CONNECTION RECLASSIFY-VPN command doesn't work
CSCsq02543	Inspect waas under several applied policy causing memory leak
CSCsq03137	Traceback at thread emweb/https
CSCsq03893	Segmented HTTP GET request are not parsed by Filtering and HTTP inspect
CSCsq04082	LDAP AAA server with null hostname causes traceback
CSCsq06129	PIX/ASA: Standby unit may reboot without recording a crash file
CSCsq07395	Adding shaping service-policy fails if policy-map has been edited
CSCsq08550	Traffic shaping with priority queueing causes traffic failure on ASA
CSCsq08990	PIX/ASA certificate authorization fails if UPN is not last attr in SAN

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsq09925	Assertion failure in thread name vpnfol_thread_msg and nested page fault
CSCsq10581	ASA5580 traceback when using ASDM
CSCsq11691	Traceback occurs in Dispatch Unit with 7.2.3.19 and L2TP/PPP
CSCsq11726	Traceback in PPP callback from AAA thread (UPAP/PAP)
CSCsq12934	"Auth proxy fails w/ ""too many pending auths"" in syslog"
CSCsq13321	Standby Failover unit traceback in Thread Name: vpnfol_thread_msg
CSCsq14358	ASA: traceback in Thread Name: netfs_thread_init
CSCsq17879	Memory leaks while parsing subject alternate name (SAN) from a cert
CSCsq18133	Standalone AnyConnect prompts for user/pass instead of user cert
CSCsq19369	URI Processing Error in Clientless SSL VPN connections
CSCsq20042	'vpnclient enable' breaks 'aaa mac-exempt match'
CSCsq22716	Threat Detection - incorrectly classifying drops as scanning threat
CSCsq24213	ASA HEAP memory leak in ldap_client_root_dse_get
CSCsq24468	PIX/ASA ipsec start/stop trap is sent by standby unit
CSCsq24915	ASA traceback in thread name netfs_thread_init
CSCsq27110	Remove asdm location and group commands from startup config
CSCsq27132	Top 10 Access Rules show multiple lines for same ACL
CSCsq27193	ASA HEAP memory leak in webvpn_ParseURL
CSCsq29263	Case Sensitivity of Issuer check for certificates on ASA
CSCsq30162	TCP proxy needs global timeout for reassembled packets
CSCsq31279	New IPsec SA deleted after rcving P2 DEL for old SA from MS L2TP/IPsec
CSCsq31399	Traceback in Thread Name: vpnfol_thread_msg when doing write standby
CSCsq33551	SIP/ACK session remains if ASA receives ACK as the 1st packet
CSCsq34316	idle ssl vpn conns do not timeout
CSCsq35987	"ASA 7.2/8.0: ""dhcpd auto_config"" breaks L2TP split-tunneling on Win XP"
CSCsq36847	WebVPN: HTML editor shows a blank page
CSCsq37050	PPPoE causing routing change on identity interface
CSCsq37647	Overrun/Underrun/NoBuffer cnts are incremented when sip-invite timeout
CSCsq39905	Traceback in IPsec message handler
CSCsq40755	CSD: WebVPN users get stuck in login loop when CSD enabled
CSCsq40777	ASA traceback when AIP module is reloaded
CSCsq42302	With very small probability legitimate cmd is rejected by ASA
CSCsq43878	multi mode A/A failover write standby will see crypto CLI error in stby
CSCsq44735	"ASA: redudant failover interface is failed, but ping works"
CSCsq44802	ASA EzVPN server preserves static RRI routes when interface is shut down
CSCsq44918	Traceback in vpnfol_thread_timer (Address not mapped)

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsq45636	Potential Information Disclosure in Clientless SSL VPNs
CSCsq46071	ASA 8.0: Should escape special characters in WebVPN Macro substitution
CSCsq46120	Traceback in PPP AAA callback routines when DFP is enabled
CSCsq46179	Longer timer needed for eToken credential entry.
CSCsq46425	Traceback in Dispatch Unit (Page Fault)
CSCsq47894	POP3s email proxy stuck with zero window to POP3 server during mail read
CSCsq50310	Management intf forward BPDU to the layer 2 FW
CSCsq50448	Traceback in Thread Name: netfs_thread_init
CSCsq50471	Traceback in Thread Name: Unicorn Proxy Thread
CSCsq50494	PIX/ASA: NAT-T Keepalive should not generate UDP request discarded msg
CSCsq51210	TCP/TLS segments from CUP dropped
CSCsq53954	RRI route not removed if more specific dynamic route for same net exists
CSCsq54870	WebVPN: ASA reloads when accessing CIFS share
CSCsq55969	show parser dump all causes Traceback in ci/console
CSCsq57163	SNMP ifSpeed incorrect for internal/data interfaces
CSCsq57465	Snmpwalk returns 0 counters for inside & outside interface
CSCsq58887	WebVPN: Smart Tunnels on Mac is failing to load page
CSCsq59163	WebVPN: CIFS Browse Networks icon not removed when browsing is disabled
CSCsq59967	SSL VPN: incorrect handling of cookie expiration date
CSCsq60414	ASA fails to update mac address table after failover
CSCsq60646	SSL VPN: Incorrect handling of HTTP in META HTTP-EQUIV
CSCsq61406	ASA 8.0.3 traceback on compac flash insert
CSCsq62883	SSL VPN: POST plugin does not work with Macro Substitutions
CSCsq63824	"ASA5580 assert failure on ""punt_elem == flow->punt_q_head"""
CSCsq65437	ASA 8.0 does not correctly calculate TCP MSS for traffic to the box
CSCsq65580	set nat-t-disable does not override crypto isakmp nat-traversal
CSCsq65899	"Change syslog ""ASA-0-716507: Fiber scheduler has reached unreachable..."""
CSCsq66348	Unable to SSH into Standby Firewall
CSCsq66561	Static arp entry for active or standby ips causes failover instability
CSCsq66899	Firewall replies with no data when optional firewall is configured
CSCsq67685	ASA 8.0.3(14) - GRE connections are not replicated to the standby unit
CSCsq68451	ASA5580 reloads during connection stress test
CSCsq68617	ASA5540 - High CPU during vpn auth if the AAA server is down
CSCsq70797	Unable to reserve port for static PAT
CSCsq71768	WebVPN shows 0.0.0.0 caller-ID in ACS Tacacs+ passed authentications
CSCsq71794	High cpu when redundant routes from multiple OSPF peers are processed

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsq73010	ASA 7.2.3.19 traceback in Thread Name: IKE Receiver
CSCsq73588	"ASA - CIFS ""Error contacting host"""
CSCsq74923	ASA - no support for auto update when used with webvpn on same int.
CSCsq75341	Traceback in Thread Name: Unicorn Proxy Thread
CSCsq77055	Hidden shares keep prompting for authentication and changes file type
CSCsq77160	telnet connection to management interface fails in routed mode
CSCsq78418	WebVPN portal susceptible to Cross Site Scripting (XSS) attacks
CSCsq78598	ASA5580 monitored interfaces bounce between Normal/Testing mode
CSCsq78902	Interim code 8.0(3)15 doesn't allow LDAP password change through WebVPN
CSCsq79382	ASA 8.0.3.12 aaa authentication listener with redirect will block conns
CSCsq80095	PIX/ASA: Console gets frozen if user logs in during failover replication
CSCsq81621	WebVPN: Smart Tunnels on MAC fails using process / application
CSCsq85304	Traceback with Thread 0 in thread group
CSCsq85924	Interface name is missing in syslog 411001 and 411002
CSCsq86976	Traceback in Thread Name: Unicorn Proxy
CSCsq89358	SSL VPN: Rewriting of META HTTP-EQUIV='Refresh' with an empty URL
CSCsq89467	Plugins cause java.io.IOException when web ACL is applied
CSCsq90760	Traceback in ci/console
CSCsq94183	"ASA - WebFolder ""Documents in this folder are not available"""
CSCsq94478	Memory leak in PKI name processing
CSCsq95023	Traceback when NULL parent conn has group lock points to another conn
CSCsq99869	Traceback on active ASA and switch to standby
CSCsr01745	"WebVPN: smart-tunnel bootup errors, config line disappears from config"
CSCsr01991	VPN load-balancing fails crypto negotiation
CSCsr02605	Logging out L2TP over IPsec sessions via ASDM can cause assert
CSCsr02624	Smart tunneled bookmarks fail in Internet Explorer with Proxy
CSCsr04639	traceback after SSH connection close from ASA5550
CSCsr05453	ASA/PIX:CPU spike may be noticed when removing objects from object-group
CSCsr06900	watchdog failure in sqlnet inspection engine
CSCsr07177	Traceback on adding acl element to acl associated with nat
CSCsr09163	webvpn - +webvpn+/index.html http response splitting problem
CSCsr11242	ASA 8.0 - Standby unit stuck in Sync Config state after write standby
CSCsr11626	skinny inspection breaks sccp calls through the firewall
CSCsr12367	WebVPN: http-form CLI commands broken
CSCsr17905	Slow memory leak due to crypto key generation
CSCsr20582	CSD: app error when launching (non-default webvpn port)

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsr23204	ARP collision detected: Primary MAC used by both active and standby
CSCsr23628	"ASA ignores webtype ACLs with "?" char in URL"
CSCsr25122	Page fault in IP thread under high traffic load
CSCsr25353	Scanning threat-detection reports incorrect victim subnets
CSCsr27940	sqlnet inspection should not handle multiple TNS frames in one packet
CSCsr28008	PAT src port allocation policy negates effect of host port alloc. policy
CSCsr29027	Traceback in thread name Checkheaps related to WebVPN
CSCsr32030	ASA 5510 not able to upgrade to Security Plus License from Base License
CSCsr32208	Active firewall fails to replicate any ICMP connections to standby
CSCsr39457	Skinny callgens fail to register due to small messages
CSCsr40360	iPhone 2.0 SW requires that ASA/PIX 7.x+ address mask is 255.255.255.255
CSCsr41534	ASA may traceback with Thread Name: emweb/https
CSCsr41612	Traceback in IP Address Assign
CSCsr41868	Cisco ASA w/ VPN- Array index out of bounds Software Failure
CSCsr45985	ASA 8.x WEBVPN: Web-Type ACL Filter incorrectly denies traffic
CSCsr46157	Traceback when 'no nameif' executed under an interface
CSCsr46385	ASA needs to support host ACE Entries for Multicast RP mapping
CSCsr46571	Additional WebVPN licenses are being used during every auth challenge
CSCsr47319	vpn-sessiondb data counters for webvpn sessions incorrect
CSCsr47881	Out of 80 byte blocks leads to Flow closed by inspection with TLS-Proxy
CSCsr50655	asa crash in dispatch unit
CSCsr57537	ASA Impossible to send mail with OWA when using CSC and WebVPN
CSCsr59417	Port Forwarding Fails Intermittently due to DNS
CSCsr60908	WebVPN CIFS failing with STATUS_NO_LOGON_SERVERS
CSCsr62405	reload occurs when url-server is unavailable and using udp transport
CSCsr63074	DPD not sent when peer is dead & tunnel not idle on s2s with 7.2.4
CSCsr63082	SSL VPN: link adds two extra slashes cifs:// to \\server\share/filename
CSCsr64970	ASA big dap.xml file partially replicated in failover
CSCsr65235	Samba authentication failure - CIFS implementation is case insensitive
CSCsr65574	Memory leak in AAA [eap proxy]
CSCsr65901	ASA reloads under heavy SIP traffic
CSCsr66684	TD Shun doesn't work if except list is specified
CSCsr66685	ASA re-loads on the text message test
CSCsr67861	"WebVPN: Can not open custom profile "webfo" (a nil value)"
CSCsr68315	second close to netfs thread causing traceback
CSCsr68455	CPU spike when deleting IKE SA with VPN-Filters

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsr69563	Traceback if policies are modified while traffic is being processed
CSCsr71069	ASA - OSPF over IPSEC over PPPoe connection not working correctly
CSCsr73107	Pix traceback fover_parse page fault in route processing
CSCsr74439	PIX/ASA: Certain malformed NAT-T packets may cause IKE process to hang
CSCsr75077	Fallback case fails when OCSP revocation check configured
CSCsr75653	'set connection decrement-ttl' does not work
CSCsr81712	Memory leak with inspection IM enabled
CSCsr84998	SSL VPN: CSD tokens not cleaned up correctly
CSCsr91721	FOVER: Error trying to delete acl when used as a network-acl in DAP
CSCsr94152	ASA 5580 traceback due to vpn encryption
CSCsr98211	Smart tunnel connections remain active indefinitely after user's session
CSCsu00776	ASA 5580 traceback due to vpn encryption
CSCsu01332	PIX 6.x to 7.x upgrade removes nonegotiate from interface
CSCsu02317	ASA strips domain in RADIUS accounting packet
CSCsu02718	snmp get-next-request incorrect value IP-MIB::ipAdEntAddr from standby
CSCsu04547	Radius Challenge Message include <tag> make anyconnect fail
CSCsu06543	Proxy auth when in RSA Next-Token-Mode fails 50% of the redirection
CSCsu08061	ASA:RRI:Routes incorrectly deleted when split-tunneling enabled
CSCsu11361	Phone quickly re-registering with new IP requires additional license
CSCsu12382	"Some TLS packets may cause incorrect DMA mappings, leading to traceback"
CSCsu21846	smart tunnel fail behind proxy server
CSCsu23121	"Cannot access CIFS shares based on ""name"" commands"
CSCsu26649	Large packets dropped with ip-comp enable configured
CSCsu29376	ASA 5580-20 traceback occurs when running multicast.
CSCsu37362	http inspection shouldn't reset for protocol-violation if not configured
CSCsu38292	interface Virtual254 appears in show interface output
CSCsu38385	Debug wevpn javascript trace user not disabled by undebug all
CSCsu40015	management-only cmd not synced. when m0/0 configured for failover
CSCsu41224	Crash in Thread Name: CMGR Server Process
CSCsu43121	Traceback: Long IKE attributes can cause buffer overrun
CSCsu46588	Heuristic based scanners report smart tunnel as malware
CSCsu50074	Traceback in Thread Name: IPsec message handler
CSCsu52268	SSH won't work to interface with ip address assigned via DHCP
CSCsu55368	Traceback caused by assert in snp_loopback_ifc.c
CSCsu55642	redundant interface switchover in transparent mode not stable
CSCsu63272	"reload after issuing show crypto ipsec sa, related to anti-replay"

Table 4 **Resolved Caveats in Version 8.1(2) (continued)**

Caveat ID	Description
CSCsu65383	QOS: L2L Police will not pass traffic
CSCsu66300	WebVPN CIFS bookmarks causes memory leak requiring a reboot
CSCsu80531	IPv6:Traceback after configuring ipv6 enforce-eui64

End-User License Agreement

For information on the end-user license agreement, go to:

https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

See *Navigating the Cisco ASA 5500 Series Documentation* at

<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html>.

Obtaining Documentation and Submitting a Service Request

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

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

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

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

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc.

All rights reserved.