Cisco ASA 5500 Series Release Notes Version 8.0(4)

March 26 2009

Contents

This document includes the following sections:

- Introduction, page 1
- Important Notes, page 2
- Limitations and Restrictions, page 2
- System Requirements, page 3
- New Features, page 5
- Caveats, page 13
- Related Documentation, page 30
- Obtaining Documentation and Submitting a Service Request, page 30

Introduction

This version supports the following products:

- Cisco ASA 5500 series adaptive security appliance, Version 8.0(4)
- ASDM, Version 6.1(3)

Cisco ASA 5500 Series Adaptive Security Appliance

The Cisco ASA 5500 series adaptive security appliances are purpose-built solutions that combine the most effective security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture.

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

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.

For more information on all of the new features, see New Features, page 5.

Additionally, the adaptive security appliance software supports Cisco Adaptive Security Device Manager (ASDM). 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 adaptive security 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. For more information on ASDM, see the *Cisco ASDM Release Notes Version 6.1(3).*

Important Notes

- ASA Compatible with EIGRP Version 3—EIGRP support was added in Version 8.0(2). However, due to a packet format change, Version 8.0(3) and later are not compatible with Version 8.0(2). Therefore, if you upgrade an adaptive security appliance to Version 8.0(3) or later, and it is peering with another adaptive security appliance running Version 8.0(2), then the peer must also be upgraded, or EIGRP will not operate correctly.
- Show Active Directory Groups—The DAP Usability feature, used to list active directory groups, is for ASDM only. The **show ad-groups** command is not intended for CLI use.
- IPSec VPN packets are dropped when compression is enabled—When you configure the **ip-comp enable** command under the group-policy, then large packets that are eligible for compression are silently dropped by the security appliance. VPN compression is only useful for very slow Internet connections, so we suggest that you disable compression (**ip-comp disable**). Alternatively, you can upgrade to interim build 8.0(4.16) or later. (CSCsu26649)

Limitations and Restrictions

Please note the following operational limitations.

- Stateful Failover with Phone Proxy—When using Stateful Failover with phone proxy, information is not passed to the standby unit; when the active unit goes down, the call fails, media stops flowing, and the call must be re-established.
- No .NET over Clientless sessions—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 up. 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.
- The adaptive security appliance does not support phone proxy and CIPC for remote access.

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 3
- Operating System and Browser Requirements, page 4
- Determining the Software Version, page 4
- Upgrading to a New Software Version, page 4

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 (MB)
5505	256
5510	256
5520	512
5540	1024
5550	4096

All adaptive security appliances require a minimum of 64 MB of internal CompactFlash, and they all ship with a minimum of 128 MB of internal CompactFlash.

If your adaptive security appliance has only 64 MB of internal CompactFlash, you should not store multiple system images, or multiple images of the new AnyConnect VPN client components, client/server plugins, or Cisco Secure Desktop.

We recommend that you purchase a 256 MB or 512 MB CompactFlash upgrade from Cisco, choosing from the following part numbers:

- ASA5500-CF-256 MB = ASA 5500 Series CompactFlash, 256 MB
- ASA5500-CF-512 MB = ASA 5500 Series CompactFlash, 512 MB

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—Click **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 on the bottom of the output.

For example:

```
hostname # dir
Directory of disk0:/

43       -rwx  14358528    08:46:02 Feb 19 2007   cdisk.bin
136      -rwx  12456368    10:25:08 Feb 20 2007   asdmfile
```

```
58      -rwx  6342320     08:44:54 Feb 19 2007  asdm-600110.bin
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
66      -rwx  425         11:45:52 Dec 05 2006  anyconnect
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.

Operating System and Browser Requirements

For the latest OS and browser test results, see the *Cisco ASA 5500 Series VPN Compatibility Reference*.

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.

Upgrading to a New Software Version

To upgrade from Version 7.2.(x) to Version 8.0(4), perform the following steps:

Step 1 Make a backup copy of your current configuration file.

Step 2 Load the new Version 8.0(4) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 3 Restart the device to load the Version 8.0(4) image.

Step 4 Load the new ASDM 6.1(3) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 5 Enter the following command to tell the adaptive security appliance where to find the ASDM image:

```
hostname(config)# asdm image disk0:/asdmfilename (no spaces after the / character, or
within the filename itself)
```

Downgrading to Version 7.2(x) Software

To downgrade from Version 8.0(4) to 7.2(x), perform the following steps:

Step 1 Load the 7.2(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 2 Restart the device to load the 7.2(x) image.

Step 3 Load the ASDM 5.2(x) image from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=268438162&i=rp

Step 4 Enter the following command to tell the adaptive security appliance where to find the ASDM image:

```
hostname(config)# asdm image disk0:/asdmfilename (no spaces after the / character, or
within the filename itself)
```

New Features

Released: August 11, 2008

Table 2 lists the new features forASA or PIX Version 8.0(4).

Table 2 New Features for ASA and PIX Version 8.0(4)

Feature	Description
Unified Communications Features[1]	
Phone Proxy	Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The ASA Phone Proxy has the following key features: • Secures remote IP phones by forcing the phones to encrypt signaling and media • Performs certificate-based authentication with remote IP phones • Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage servers • Terminates SRTP and initiates RTP/SRTP to the called party
Mobility Proxy	Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage clients and servers is supported. Cisco Unified Mobility Advantage solutions include the Cisco Unified Mobile Communicator, an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise. The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, the proprietary protocol between Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage. The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between the Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage.

Table 2 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Presence Federation Proxy	Secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can securely connect their Cisco Unified Presence clients back to their enterprise networks, or share Presence information between Presence servers in different enterprises. The ASA delivers functionality to enable Presence for Internet and intra-enterprise communications. An SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence Server. The ASA enables SSL connectivity between server to server communication including third-party Presence servers communicating with Cisco Unified Presence servers. Enterprises share Presence information, and can use IM applications. The ASA inspects SIP messages between the servers.
Remote Access Features	
Auto Sign-On with Smart Tunnels for IE[1]	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. 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. 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.
Entrust Certificate Provisioning[1]	ASDM includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.
Extended Time for User Reauthentication on IKE Rekey	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.
Persistent IPsec Tunneled Flows	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 **[no] sysopt connection preserve-vpn-flows** command. This option is disabled by default.

Table 2 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Show Active Directory Groups	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.
Smart Tunnel over Mac OS[1]	Smart tunnels now support Mac OS.
Local Address Pool Edit	Address pools can be edited without affecting the desired connection. If an address in use is not being eliminated from the pool, the connection is not affected. However, if the address in use is being eliminated from the pool, the connection is brought down. *Also available in Version 7.0(8) and 7.2(4).*
Firewall Features	
QoS Traffic Shaping	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. 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. *Also available in Version 7.2(4).*
TCP Normalization Enhancements	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. • 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) 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. The default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command). The following non-configurable actions have changed from drop to clear for these packet types: • Bad option length in TCP • TCP Window scale on non-SYN • Bad TCP window scale value • Bad TCP SACK ALLOW option *Also available in Version 7.2(4).*
TCP Intercept statistics	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.

Table 2 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Threat detection shun timeout	You can now configure the shun timeout for threat detection using the **threat-detection scanning-threat shun duration** command.
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command. *Also available in Version 7.2(4).*
clear conn Command	The **clear conn** command was added to remove connections. *Also available in Version 7.0(8) and 7.2(4).*
Fragment full reassembly	The **fragment** command was enhanced with the **reassembly full** keywords to enable full reassembly for fragments that are routed through the device. Fragments that terminate at the device are always fully reassembled. *Also available in Version 7.0(8) and 7.2(4).*
Ethertype ACL MAC Enhancement	EtherType ACLs have been enhanced to allow non-standard MACs. Existing default rules are retained, but no new ones need to be added. *Also available in Version 7.0(8) and 7.2(4).*
Troubleshooting and Monitoring Features	
capture command Enhancement	The **capture type asp-drop** *drop_code* command now accepts **all** as the *drop_code*, so you can now capture all packets that the adaptive security appliance drops, including those dropped due to security checks. *Also available in Version 7.0(8) and 7.2(4).*
show asp drop Command Enhancement	Output now includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command using the keyword. *Also available in Version 7.0(8) and 8.0(4).*
clear asp table Command	Added the **clear asp table** command to clear the hits output by the **show asp table** commands. *Also available in Version 7.0(8) and 7.2(4).*
show asp table classify hits Command Enhancement	The **hits** option was added to the **show asp table classify** command, showing the timestamp indicating the last time the asp table counters were cleared. It also shows rules with hits values not equal to zero. This permits users to quickly see what rules are being hit, especially since a simple configuration may end up with hundreds of entries in the **show asp table classify** command. *Also available in Version 7.0(8) and 8.0(4).*
MIB Enhancement	The CISCO-REMOTE-ACCESS-MONITOR-MIB is implemented more completely. *Also available in 8.0(4).*
show perfmon Command	Added the following rate outputs: TCP Intercept Connections Established, TCP Intercept Attempts, TCP Embryonic Connections Timeout, and Valid Connections Rate in TCP Intercept. *Also available in Version 7.0(8) and 7.2(4).*

Table 2 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
memory tracking Commands	The following new commands are introduced in this release: • **memory tracking enable**–This command enables the tracking of heap memory requests. • **no memory tracking enable**–This command disables tracking of heap memory requests, cleans up all currently gathered information, and returns all heap memory used by the tool itself to the system. • **clear memory tracking**–This command clears out all currently gathered information but continues to track further memory requests. • **show memory tracking**–This command shows currently allocated memory tracked by the tool, broken down by the topmost caller function address. • **show memory tracking address**–This command shows currently allocated memory broken down by each individual piece of memory. The output lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool. • **show memory tracking dump**–This command shows the size, location, partial callstack, and a memory dump of the given memory address. • **show memory tracking detail**–This command shows various internal details to be used in gaining insight into the internal behavior of the tool. *Also available in Version 7.0(8) and 7.2(4).*
Routing Features	
IPv6 Multicast Listener Discovery Protocol v2 Support	The adaptive security appliance now supports the Multicast Listener Discovery Protocol (MLD) Version 2, to discover the presence of multicast address listeners on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes. The adaptive security appliance becomes a multicast address listener, or a host, but not a a multicast router, and responds to Multicast Listener Queries and sends Multicast Listener Reports only. The following commands support this feature: • **clear ipv6 mld traffic** The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters. • **show ipv6 mld traffic** The **show ipv6 mld** command allows you to display all the Multicast Listener Discovery traffic counters. • **debug ipv6 mld** The enhancement to the **debug ipv6** command allows the user to display the debug messages for MLD, to see whether the MLD protocol activities are working properly. • **show debug ipv6 mld** The enhancement to the **show debug ipv6** command allows the user to display whether **debug ipv6 mld** is enabled or disabled. *Also available in Version 7.2(4).*
Platform Features	

Table 2 New Features for ASA and PIX Version 8.0(4) (continued)

Feature	Description
Native VLAN support for the ASA 5505	You can now include the native VLAN in an ASA 5505 trunk port using the **switchport trunk native vlan** command. *Also available in Version 7.2(4).*
SNMP support for unnamed interfaces	Previously, 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. Because the ASA 5505 has both unnamed switch ports and named VLAN interfaces, 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. These changes affect all models, and not just the ASA 5505.
Failover Features	
failover timeout Command	The **failover timeout** command no longer requires a failover license for use with the static nailed feature. *Also available in Version 7.0(8) and 7.2(4).*

1. This feature is not supported on the PIX security appliance.

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 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. Because the ASA 5505 has both unnamed switch ports and named VLAN interfaces, 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. These changes affect all models, and not just the ASA 5505.

This section includes the following topics:

- IF MIB Output Changes, page 10
- IP MIB Output Changes, page 12
- SNMP Link State Trap Changes, page 13

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.

For example, the ifPhysAddr output now includes the MAC addresses of switch ports on the ASA 5505; before, only named VLAN interfaces were shown with a MAC address of 0:0:0:0:0:0.

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 11
- Sample ifDescr Output, page 12

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 12.

```
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.

Caveats

The following sections describe the caveats for Version 8.0(4).

- Open Caveats - Version 8.0(4), page 13
- Resolved Caveats - Version 8.0(4), page 16

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. 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 - Version 8.0(4)

Table 3 Open Caveats - Version 8.0(4)

DDTS Number	Caveat
CSCsj08209	clear ospf process causes traceback
CSCsj28099	ASA can hang on certain tasks if disk is corrupt.
CSCsk89022	ASA traceback while removing dhcpd configuration.
CSCsl08271	Standby Unit show incorrect memory usage in Admin context
CSCsl94835	Dispatch Unit reload with hash_table_simple assert message
CSCsm20204	Extended ping command with no ip specified causes stuck thread
CSCsm21859	Privileged commands being shown in unprivileged mode
CSCsm24047	DNS query is sent out before cmd is completed when dns enabled

Table 3 Open Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsm36960	DAP: Error selecting any DAP records
CSCsm58230	Traceback in Thread Name: tmatch compile thread
CSCsm74180	MFM A/S Failover is not syncing after config from blank config
CSCsm77414	Traceback while applying a large regex config twice and then removing it
CSCsm90099	Perfmon interval 1 causes cpu-hog on pm_timer_thread
CSCsm99532	RTlog viewer is hanging when websense log messages are seen
CSCso64944	ASA memory leak due to IPSEC
CSCso65967	SIP inspection possible memory leak
CSCso69141	WebVPN: Password and internal password macro fails
CSCso71741	Traceback in IPsec message handler
CSCso84215	"High CPU by using ASDM with ""log asdm info"" configured"
CSCso92730	ASA might not respond properly to SNMP polls
CSCso95135	Zero-downtime upgrade from 7.2 not possible anymore after 8.0.3.10
CSCso98724	TCP flow count and TCP intercept values stuck once xlate is built
CSCsq10022	High CPU when large number of VPN clients with per-user ACLs disconnect
CSCsq20042	'vpnclient enable' breaks 'aaa mac-exempt match'
CSCsq31399	Traceback in Thread Name: vpnfol_thread_msg when doing write standby
CSCsq39905	Traceback in IPsec message handler
CSCsq43283	ASA traceback in thread webvpn_session_free
CSCsq45101	WebVPN - object mangling is not working for SAP Netweaver
CSCsq45843	WebVPN - Ironport interface fails through rewriter.
CSCsq55969	show parser dump all causes Traceback in ci/console
CSCsq56045	SSO with Radius challenge/response - OTP is reused for internal sites
CSCsq65437	ASA 8.0 does not correctly calculate TCP MSS for traffic to the box
CSCsq77355	IKE peer ID validation cert fails
CSCsq77997	SSL VPN: Rewriting errors when caching enabled
CSCsq78576	High CPU and memory results in %ASA-0-716507 message on cli
CSCsq84093	"PIX/ASA: Accounting packet shows ""unknown"" as username"
CSCsq89467	Plugins cause java.io.IOException when web ACL is applied
CSCsq90450	"on asdm can't use feature ""save running config to tftp server"" thru vpn"
CSCsq94560	Challenge response string gets cut off without resizing window
CSCsq94871	ASDM hangs at 77% loading bar
CSCsq94981	ASA 8.0(3) traceback in process Dispatch Unit
CSCsr02395	copying config via tftp breaks ipsec l2l tunnel
CSCsr09436	FTP buffer logging queue not cleared when logging is disabled
CSCsr11242	ASA 8.0 - Standby unit stuck in Sync Config state after write standby

Table 3 Open Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsr17063	Traceback in Thread Name Dispatch Unit
CSCsr18010	manual certificate enrollment request lost over ASA reload
CSCsr23628	"ASA ignores webtype ACLs with ""?"" char in URL"
CSCsr29027	Traceback in thread name Checkheaps related to WebVPN
CSCsr38644	"Service column in Top 10 Access Rules shows object-group, not service"
CSCsr39311	CM SIP Trunk call failures due to ASA closing connection by inspection
CSCsr39880	Insert and removal of compact flash may result in system hang
CSCsr40409	WebVPN: Group-URL feature fails when connection profile name has spaces
CSCsr41534	ASA may traceback with Thread Name: emweb/https
CSCsr52990	ASA5505 silently terminates AnyConnect client connection
CSCsr53737	AnyConnect sessions dropped when Failover occurs with HostScan
CSCsr56975	"Traceback while executing the ""ddns update hostname xxxx"" command"
CSCsr58601	SCCP does not handle new msg StartMediaTransmissionACK
CSCsr59417	Port Forwarding Fails Intermittently due to DNS
CSCsr60721	IKE FSM gets into state with multiple Ph1 SAs in MM_FREE - reload needed
CSCsr63375	Webvpn: citrix plug-in doesn't accept CTL keys
CSCsr64970	ASA big dap.xml file partially replicated in failover
CSCsr65102	ASA 8.0.3.12 Traceback in Thread: aaa
CSCsr66402	Tracebacks on standby unit (Thread Name: lu_rx)
CSCsr68384	assertion in ptr + size == block->memory + block->pos
CSCsr68915	ASA 8.0.3: Traceback during LDAP lookup
CSCsr71069	ASA - OSPF over IPSEC over PPPoe connection not working correctly
CSCsr74265	ASA crypto HW error when trying to fragment small IP packet
CSCsr75077	Certificate authentication produces cpu-hogs
CSCsr75910	Smart-tunnel (bookmark): the hyperion apps don't load correctly with IE
CSCsr81535	CUCM SDL Links go out of service under load when ASA is put inline
CSCsr81712	Memory leak with inspection IM enabled
CSCsr84465	"failover mode, using backup option on ASDM crashes secondary unit"
CSCsr85091	PIX/ASA may reload with traceback in CMGR Server Process
CSCsu26649	Large packets dropped with ip-comp enable configured

Resolved Caveats - Version 8.0(4)

Table 4 Resolved Caveats - Version 8.0(4)

DDTS Number	Caveat
CSCsg69408	Need warning when using time based ACLs with policy NAT/PAT
CSCsg75094	LDAP: ASA cannot authenticate to Active Directory using MD5
CSCsh56136	Failed or Cancelled Authens should drop user to Main File Access page.
CSCsh91747	SSL VPN stress cause SSL lib error. Function: DO_SSL3_WRITE
CSCsi06469	Inactivating then reactivating nat 0 multiple access-lists breaks nat 0
CSCsi41346	user session and idle timeout values not honored by cut-thru-pxy
CSCsi49983	Periodic HW crypto errors 402123 & 402125 see with L2TP/IPSEC
CSCsi60244	webvpn_session struct is not correctly validated in failover code
CSCsi79159	admin connections to PIX with crypto card via management-access fail
CSCsi84143	Mem del-free-poisoner fails to svc alloc requests from the poisoned pool
CSCsj12938	PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational
CSCsj25896	ASA may reload with traceback in Thread name: CTM Message Handler
CSCsj71788	Slow response when entering commands via Telnet
CSCsj91809	Clientless email proxy POP3S with Outlook 2007 not working
CSCsk00089	No snmp object for failover lan interface status .
CSCsk01987	ASA Crash file system node is getting deallocated .
CSCsk08454	ASA 8.0 fails to send TACACS request over L2L tunnel
CSCsk14532	ASA - FTP Type Mount remains inaccessible if FTP server goes offline .
CSCsk18083	nat exemption access-list not checked for protocol or port when applied
CSCsk18084	cikeTunnelTable MIB does not populate for some of the ISAKMP SA's. .
CSCsk19065	Excessive High CPU and packets drops when applying ACL to an interface .
CSCsk27107	ldap CRL retrieval fails - ldap-default not used
CSCsk36399	Traceback in PIX Garbage Collector (Old pc 0x008b619d ebp 0x0261ed60)
CSCsk42595	ASA:: 2 Factor Authentication with Password-Management Fails for SSL VPN
CSCsk43103	Traceback in Thread Name emweb/https
CSCsk47949	ASDM hangs at 47% if packet losses on the network
CSCsk48355	ISAKMP SA stuck in AM_WAIT_DELETE after ASA upgrade
CSCsk49506	Local-host for u-turn traffic on lowest sec level used for license limit
CSCsk50583	IPV6: Anyconnect does not work when using ipv6 with vlans.
CSCsk50879	L2TP with EAP authenticatio In use List count session leaking
CSCsk58346	Memory leak when adding/removing nameif
CSCsk59083	ASA 5505 failover: rebooted unit becomes active after reload
CSCsk59189	Top N data sent to ASDM is incorrect when ACE changes
CSCsk63633	WebVPN: ERROR: Invalid tunnel group name <certs> during replication

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsk64117	CPU Hog seen generating RSA keys during SSH session establishment
CSCsk64428	High CPU when polling VPN MIBs via SNMP
CSCsk65211	ASA5505 inside interface w/23bit or smaller subnet mask becomes unstable
CSCsk65788	FO: Webvpn customization import not replicated to Standby device
CSCsk65863	traceback in ppp_timer_thread
CSCsk65940	"crashinfo file corrupted, extra text appended to bottom"
CSCsk66924	ASDM: Monitoring Used memory records different stats history
CSCsk68895	Traceback in thread name Dispatch Unit with IDS packet recv
CSCsk69537	Traceback in Dispatch Unit during ASDM access
CSCsk69878	ASA running 8.0.2 rejects DHCP leases less than 32 seconds
CSCsk70941	Traceback in Thread Dispatch Unit: snp_tcp_timeout_cb
CSCsk71006	ipv6 acl don't have acl options when using MPF .
CSCsk71135	ASA 7.2.3 - Traceback in Unicorn Proxy Thread
CSCsk76770	vpn-filter may prevent renegotiation of the tunnel
CSCsk77197	RDP and citrix plugins fail with java error when ACL applied in DAP
CSCsk77613	webvpn: 3 MB/day mem leak with 76288 byte frag on lightly used device
CSCsk79728	ASA5550 7.2.3 traceback with Dispatch Unit
CSCsk80789	RTSP inspection changes Media Player version to 0.0.0.0
CSCsk81765	ASA webvpn APCF command is not in config: re-occurence of CSCsk60110
CSCsk82261	ASA 8.0.2: threat-detection command does not work with names
CSCsk84801	WCCP GRE packets decapsulated when passing through pix
CSCsk85428	Traceback in scheduler
CSCsk85441	Traceback in thread https_proxy
CSCsk86073	debug webvpn javascript trace user not seen in show debug
CSCsk87951	Group URL not working as expected with AnyConnect
CSCsk88517	Accessing webvpn URL via WEBVPN portal with same-security restarts ASA
CSCsk88562	CSC-SSM: 1550-byte block depletion
CSCsk89452	Remote-access users are mapped to RADIUS Service-Type 1 Login
CSCsk89639	Traceback with Thread Name: Checkheaps
CSCsk90689	telnet to the box and vpn tunnels fail due to 0-byte block depletion
CSCsk91498	CIFS: access denied w/special character in password - anonymous login
CSCsk93067	no management-access Inside still allows telnet over IPSec tunnel
CSCsk93628	Packet dropped when mss-exceed is configured to allow
CSCsk95133	Traceback in Thread Unicorn Proxy related to WebVPN page rewrite
CSCsk96050	traceback may occur when enabling and disabling EIGRP
CSCsk96804	Traceback in Thread Name: Dispatch Unit with inspect h323

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsk97406	AnyConnect standalone with CSD pre-login failure takes 4 min
CSCsk97671	VPN client with NULL Encryption L2TP-IPSec behind NAT drops on 71st sec
CSCsk97830	Traceback in thread name Dispatch Unit .
CSCsl01053	ASA doesn't handle the multiple CPS entries in the Issuing CA cert .
CSCsl03839	WebVPN does not modify URLs in Sharepoint .iqy files .
CSCsl03985	ASA DHCP client unable to renew the IP address if DHCP ACK is lost
CSCsl04218	vpn-filter for ios ezvpn w/secondary ip address broken in 8.0
CSCsl04900	SIP invite fixup'd with name rather than IP address
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
CSCsl11139	ASA context listed as Unknown in 'show event alert' output .
CSCsl11321	ASA doesn't send coldStart trap when speed/duplex is fixed as 100/full
CSCsl11678	"Error: Failed to register 750 blocks for inspection,..."
CSCsl12010	flash memory corruption issues
CSCsl12239	WebVPN: OWA 2K -> shortcuts pane does not load
CSCsl12449	DHCP Client - remove minimum lease time restriction .
CSCsl12472	Traceback in emweb/https observed on ASA
CSCsl14914	webvpn rewriter causing webpage to fail .
CSCsl15013	DHCPrelay broken with 2 DHCPrelay servers when second one out of service
CSCsl17136	H323: Video breaks. Problem in locating UUIE in SETUP message.
CSCsl18404	WebVPN: OWA -> text undefined being appended to HTML message body .
CSCsl19419	enabling acl-netmask-convert wildcard does not accept acl with host .
CSCsl21500	Traceback with 'no capture <name>' for ISAKMP type capture .
CSCsl21953	Failover configured w/ Redundant I/F is unstable after conf-replication
CSCsl23542	"User Certificate mappings against the ""whole field"" failing"
CSCsl26135	Memory leak when FTP filter is enabled
CSCsl26200	ASA SSL VPN ACL bypass
CSCsl26957	SNMP Remote Access MIB crasSessionTable does not return data
CSCsl28306	PIX/ASA default route redistributed into EIGRP when explicitly disabled
CSCsl28971	ASA reloads in IPsec message handler thread
CSCsl29315	Syslog 713902 appears on standby unit when disconnecting VPN connection
CSCsl29851	ASA sends 0.0.0.0 as caller-id for command authorization
CSCsl30307	PIX/ASA fails to install cert with an empty subject/issuer alt name ext
CSCsl31908	ASA: SIP inspection drops SIP message 200 OK from 3rd party CosmoCall
CSCsl32225	Traceback in Thread Name: Checkheaps when Simultaneous login set to 1
CSCsl32785	Traceback in Thread Name: pix_flash_config_thread

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsl33600	Traceback when show service after removing global policy with police
CSCsl34791	WebVPN: Traceback in Thread Name: Dispatch Unit
CSCsl35591	Bulk skinny registration creates 2048 block leak .
CSCsl35603	Memory corruption with csc and nat testing .
CSCsl35949	ASA: Webvpn rewriter causing Javascript rewrite error
CSCsl37063	DTLS crash in TLS fragment handling
CSCsl37371	anyconnect (DTLS failover) - idle timeout not effective
CSCsl37767	Traceback when timeout with L2TP and delay-free-poisoner enabled .
CSCsl38314	HA: SNMP trap authentication replicated to standby improperly
CSCsl38482	Outlook web access 2007 premium issues with clientless webvpn
CSCsl40225	CPU usage eventually hits 90% and that causes call failures .
CSCsl40367	DDNS updates append duplicate domain name
CSCsl41666	Crypto debug command should not dump keys as part of the SA
CSCsl43246	L2TP with EAP authentication In use List count session slowly leaking
CSCsl44845	bad vPifNum errors on AAA accounting for a RA vpn session on boot
CSCsl45763	Syslog message during config-replication: invalid function
CSCsl46310	"ASA error: ""Unable to download NAT policy for ACE"" with nat 0 ACL"
CSCsl47479	ASA not checking certificate key usage for AnyConnect
CSCsl48060	show route <intf> <ip addr> : Could display wrong information
CSCsl49999	"! used in downloadable ACL yields ""error unable to apply access list"""
CSCsl51292	IPSEC VPN tunnel on 8.0.3 fails every couple days
CSCsl51797	ASA traceback in AAA thread
CSCsl52765	TD may put target of no-reply UDP sessions to shunned list
CSCsl52895	ASA 7.2.3 number of IPSec SA not replicated in failover unit
CSCsl53995	5510 interface can be set to1000Mbps with base license
CSCsl54352	8.0.3: snp_td_init_acl_hit_top_history not being freed when ACLs removed
CSCsl55623	SNMP link trap varbind list missing values
CSCsl56635	Input errors remains 0 even when CRC counts up
CSCsl57533	"setting privilege for capture does not affect ""no capture"""
CSCsl59108	Auto-signon servers not inherited from DfltGrpPolicy
CSCsl59247	Unable to request CRL for trustpoint with only ID certificate
CSCsl59266	PKI: export/import of pkcs12 containing only ID cert fails
CSCsl59572	ASA LDAP Mapping should not map 0 to values with no match
CSCsl63265	"Error message: ""Customization <> is in use, unable to remove."
CSCsl63901	some url links dont work with smarttunnel in Vista
CSCsl64946	5510 Ethernet interface fail speed auto negotiation when boot up.

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsl66538	"ASA ""hardware accelerator encountered an error (Invalid PKCS Type)"""
CSCsl66758	TCP intercept comes before ACL checks. All TCP ports appear open.
CSCsl67229	ASA: timeout sip_media is not working properly
CSCsl68785	Confusing Error message when Interfaces have overlapping networks
CSCsl70296	failover link is lost with redundant int and EIGRP after rebooting
CSCsl70685	Traceback in Thread Name: accept/http
CSCsl70934	ASA 5540 traceback due to DFS/CIFS issue
CSCsl71113	'Configure Memory' command with DDNS config causes traceback
CSCsl71223	Clearing webvpn channels may cause traceback in Unicorn Proxy Thread
CSCsl73850	Traceback occurs when SIP session is active and switchover occurs twice
CSCsl73906	Traceback on network command under rip config mode under load
CSCsl74327	Traceback in fover_parse when editing ACL config
CSCsl74552	Webvpn misinterpreting asp url's
CSCsl74889	ASA/PIX crashes ASA -IOS l2tp IPSEC
CSCsl75006	"Traceback on entering command ""vpnclient nem-st-autoconnect"""
CSCsl78110	Downloadable ACL does not get removed from memory in some scenarios
CSCsl78638	"stateful subinterface would not become Up, remains Failed"
CSCsl79211	Traceback: AAA task overflow when object-group acls and virtual telnet
CSCsl82188	AnyConnect fails to connect with /32 mask (255.255.255.255)
CSCsl82200	IPSec not encrypting after failover.
CSCsl82211	Nas-Port attribute different for authentication and accounting in sslvpn
CSCsl82984	HT: Traceback proxy_block_cpy+829 at inspect/tcp_proxy_utils.c:108
CSCsl83313	access-group sometimes take more than 10 min to execute
CSCsl83503	Threat detection - Scanning drops occur even with basic TD disabled
CSCsl84122	Xlate timers for RTP/RTCP in version 7.2 are always 30 seconds
CSCsl84179	Traceback at ssh thread when working with 'capture'
CSCsl84204	Xlate timers for RTP/RTCP on standby unit aren't synched with active
CSCsl85169	Inspect WAAS causing the memory leak
CSCsl87918	IPSec: RESPONDER-LIFETIME not properly created.
CSCsl88161	CSD not starting on Linux - webstart.xml parsing error (malformed)
CSCsl88730	"Crash at chunk_free, chunk absent with Skinny"
CSCsl89105	Traceback when enabling blocks queue history w/ hi load/low mem
CSCsl89162	"show cheakheaps displays negative number for ""total memory in use"""
CSCsl89537	SIP: Improperly adding some value in From-tag when sending BYE
CSCsl89602	ASA ignores direct WebVPN URLs (favicon.ico problem)
CSCsl89653	SIP connection entry not be cleared after sip_disconnect timeout

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsl91005	Traceback in Thread Name: CP Processing under TCP/UDP load
CSCsl91061	Traceback while adding regex with Synsend and Udpsend SIP traffic load
CSCsl93003	"TACACS+ allow enable command but output has ""Command authorization fail"""
CSCsl93495	SIP: ASA shows 4xx response message as 500 on debug sip
CSCsl94183	ASA- Clientless webvpn 'error contacting host' accessing CIFS shares
CSCsl95043	"PIX/ASA: L2TP/IPsec needs both ""ipsec"" and ""l2tp-ipsec"" in group-policy"
CSCsl95244	Traceback in Dispatch Unit caused by rapid connection successions
CSCsl95286	Control-plane feature not working for https traffic to-the-box
CSCsl95856	DHCP learned default route not in route table if other DHCP interfaces
CSCsl95928	High CPU utilization due to OSPF
CSCsl96219	SIP: Failure to associate re-invites to the original SIP session
CSCsl96502	SIP: sess is not kept around for ACK in response to non2xx final RESP
CSCsl97339	WebVPN: A page is not properly displayed if accessed by Webvpn
CSCsl98404	CIFS: access denied with percentage symbol in password.
CSCsl99322	Traceback at ids_put in Thread Name: Dispatch Unit
CSCsm00894	LDAP map fails for IETF-Radius-Framed-IP-Address
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
CSCsm03104	"ASA, write standby copies a no crypto isakmp nat-traversal"
CSCsm03751	SNMP Coldstart Trap is Only Sent to the Last Configured NMS
CSCsm05055	Traceback seen when 'established udp 0 0' command is enabled
CSCsm05181	traceback in Thread: vpnfol_thread_msg
CSCsm07888	Authenticator value on retransmitted RADIUS request pkt changed
CSCsm09584	EAP l2tp authentication fails if mschapv2 is configured on the same TG
CSCsm10187	Both Pri/Sec don't send coldstart trap when both units are available
CSCsm10353	AnyConnect password that contains brackets <> will fail authentication
CSCsm11925	"ASA WebVPN generates bad Citrix ticket causing ""SSL Error 35"" on client"
CSCsm12064	ASA 8.0.3.2 traceback in Dispatch Unit Old pc 0x0816a874 ebp 0xc791e828
CSCsm13195	Clientless SSL VPN needs to reset session clock during FTP transfers
CSCsm13717	SNMP Remote Access MIB crasSessionTable returns incorrect data
CSCsm14283	"ICMP (type 3, code 4) packet not returned from PPPoE interface"
CSCsm17247	H323/NAT-Setup msg with SupportedFeatures extensions malformed after NAT
CSCsm18372	show input hardware queue max counters incorrect
CSCsm18437	clear interface doesn't clear max queue counter
CSCsm21493	SSLVPN : 'vlan' restriction in a group-policy propagated to all policies

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsm21708	DAP: Tunnel Group returns Null after new pin mode challenge
CSCsm21719	threat-detection not releasing cached memory after being disabled
CSCsm22002	Traceback in qos/qos_rate_limiter while processing pakt with TCP flow
CSCsm22241	PIX/ASA vlan mapping fails when username is less than 4 characters
CSCsm22781	PIX/ASA: RPF(reverse path forwarding)chk fails when PMTUD packet is sent
CSCsm23464	CTM HW memory debug feature
CSCsm23689	SSL session cache size is too large for some platforms
CSCsm24814	CSD: HostScan does not work on Linux using JRE 1.5 and higher
CSCsm25189	Inconsistent behavior for different kind of SIP packets
CSCsm26011	Traceback on Active occurs when replicating large # of WebVPN sessions
CSCsm26841	Watchdog failure: TLS fragmented client hello message.allocb+185
CSCsm28529	page fault in fover_parse - eip og_rem_objgrp with DFP
CSCsm29337	Dest unicast address to multicast address NAT not working in 7.x
CSCsm30926	ASA: Traceback with high voice traffic and voice inspection
CSCsm31973	cefcMIBEnableStatusNotification value is always false in single mode.
CSCsm32507	External group policy authentication failure with password-management
CSCsm32828	Traceback when clear config all with logging commands.
CSCsm32904	Login fails when CRL not cached
CSCsm32972	SNMP Counters Get Stuck on Repeated Polls
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
CSCsm39684	Boston AT: IPSEC rekey does not occur
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
CSCsm44660	5505 in EzVPN mode cannot establish a VPN tunnel to the head end
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
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

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsm48412	SSL rec paramater list continues to grow without boundaries.
CSCsm49741	Clientless SSl 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
CSCsm54473	FO:standby box is unable to sync config and reloads with acl config
CSCsm55261	Cannot establish WebVPN session to ASA-5510 - memory allocation error
CSCsm55447	ASA/WebVPN Citrix sessions randomly dropped
CSCsm55520	ASA Traceback in Thread Name: vpnfol_thread_msg when using citrix-plugin
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
CSCsm67466	"Apply Control-plane ACL fail, need clear/apply it again to work properly"
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	" assertion ""cli_cfg_rwlock[vcid].rwlock.cnt == -1"" failed: file ""cfglck."

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsm73654	Syslog 111111 appears when both active/standby units reload at once
CSCsm75212	Traceback in Thread Name: IKE Daemon (Old pc 0x0050a493 ebp 0x0346e)
CSCsm76163	BetaBox: Phase 2 rekeys are failing after a failover.
CSCsm77958	"Traceback in ""IP Thread"" when clientless webvpn started."
CSCsm80984	show version: command displays incorrect value for total RAM
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 crash 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.
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:Fails to update to-tag when recevied no-2xx response
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 recevied
CSCso03722	L2TP/IPSec session increases MIB active user statistics

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCso05327	Cert from 3k imported into ASA causes Hardware error on use
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

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCso40520	re-INVITE is dropped when it's exceeded 119ch after establishing 400ch
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
CSCso50996	ASA dropping the packet instead of encrypting it.
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 ...
CSCso65634	ASA image not recognizing disk1 after reload
CSCso65837	write mem from HTTPS adds no monitor-interface CLIs to startup config
CSCso66807	Sometimes Group field is missing in UI when connecting using AnyConnect
CSCso68547	PIX/ASA HTTP inspection: Multiple content-length headers issue
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 (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCso79906	TCP reset sent for AnyConnect session
CSCso81153	Traceback in dispatch unit with MGCP inspection
CSCso82264	ASA: icmp inspection may drop icmp error packets
CSCso83246	Traceback seen while connecting via asdm running on osx platform.
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	Crash 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 value is not preserved by sapi inspection
CSCso93088	Fragmented multicast traffic gets repeated and corrupted
CSCso94098	"SIP:""o=""address in SDP is not translated when ""c="" is in all media desc."
CSCso94668	2048 bytes block memory leak
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 crash
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
CSCsq09925	Assertion failure in thread name vpnfol_thread_msg and nested page fault
CSCsq11726	Traceback in PPP callback from AAA thread (UPAP/PAP)
CSCsq12934	"Auth proxy fails w/ ""too many pending auths"" in syslog"

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
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
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
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
CSCsq31279	New IPSec SA deleted after rcving P2 DEL for old SA from MS L2TP/IPSec
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 is broken in 8.0.4
CSCsq37050	PPPoE causing routing change on identity interface
CSCsq37647	Overrun/Underrun/NoBuffer cntrs are incremented when sip-invite timeout
CSCsq40755	CSD: WebVPN users get stuck in login loop when CSD enabled
CSCsq42302	With very small probability legitimate cmd is rejected by ASA
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)
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

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
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 crashes on compac flash insert
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
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
CSCsq73588	"ASA - CIFS ""Error contacting host"""
CSCsq75341	Traceback in Thread Name: Unicorn Proxy Thread
CSCsq77055	Hidden shares keep prompting for authentication and changes file type
CSCsq78418	WebVPN portal susceptible to Cross Site Scripting (XSS) attacks
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
CSCsq81621	WebVPN: Smart Tunnels on MAC fails using process / application
CSCsq85924	Interface name is missing in syslog 411001 and 411002
CSCsq86976	ASA 5550 running 8.0.3(12) is crashing Thread Name: Unicorn Proxy
CSCsq89358	SSL VPN: Rewriting of META HTTP-EQUIV='Refresh' with an empty URL
CSCsq94183	"ASA - WebFolder ""Documents in this folder are not available"""
CSCsq94478	Memory leak in crypto_pki_compare_DN
CSCsr01991	VPN load-balancing fails crypto negotiation
CSCsr02605	ASA crashes if session logout is done using asdm
CSCsr02624	Smart tunneled bookmarks fail in Internet Explorer with Proxy
CSCsr06900	watchdog failure in sqlnet inspection engine
CSCsr07177	Traceback on adding acl element to acl associated with nat
CSCsr11626	skinny inspection breaks sccp calls through the firewall
CSCsr20582	CSD: app error when launching (non-default webvpn port)
CSCsr27940	sqlnet inspection should not handle multiple TNS frames in one packet

Table 4 Resolved Caveats (continued)- Version 8.0(4)

DDTS Number	Caveat
CSCsr28008	PAT src port allocation policy negates effect of host port alloc. policy
CSCsr32030	ASA 5510 not able to upgrade to Security Plus License from Base License
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
CSCsr41612	Traceback in IP Address Assign
CSCsr45985	ASA 8.x WEBVPN: Web-Type ACL Filter incorrectly denies traffic
CSCsr46571	Additional WebVPN licenses are being used during every auth challenge
CSCsr65901	ASA crashes under heavy SIP traffic
CSCsr66684	TD Shun doesn't work if except list is specified
CSCsr66685	ASA crashes on the text message test
CSCsr68315	second close to netfs thread causing traceback
CSCsr71463	ASDM not receiving historical data from platform thru asdm_handler

Related Documentation

For additional information on the adaptive security appliance, go to:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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.