



# Cisco PIX Security Appliance Release Notes Version 8.0(4)

---

August 2008

## Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 5](#)
- [Caveats, page 6](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation and Submitting a Service Request, page 16](#)

## Introduction



### Note

---

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 8.0(4).

---

The Cisco PIX 500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability.

For more information on all the new features, see the [“New Features” section on page 5](#).



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

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 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 security appliance. Its secure, web-based design enables anytime, anywhere access to security appliances.

## System Requirements

The sections that follow list the system requirements for operating a security appliance.



### Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 8.0(4).

## Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you must increase your memory before upgrading to PIX Version 8.0(4). This version requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses. [Table 1](#) lists the default value for the memory that ships with each security appliance and flash memory requirements for Version 8.0(4).

**Table 1** Default Memory Shipped and Flash Memory Requirements

| PIX Security Appliance Model | Default Memory (MB) | Flash Memory Required (MB) |
|------------------------------|---------------------|----------------------------|
| 515/515E                     | 64                  | 16                         |
| 525                          | 128                 |                            |
| 535                          | 512                 |                            |

For more information about minimum memory requirements, see the “Minimum Memory Requirements” section in the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*.

## Software Requirements

Version 8.0(4) requires the following:

- The minimum software version required before upgrading to PIX Version 8.0(4) is PIX Version 7.2. If you are running a PIX version earlier than Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can upgrade to PIX Version 7.2.

To upgrade your PIX software image, go to the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

- For information on specific licenses supported on each model of the security appliance, go to the following website: <http://www.cisco.com/en/US/docs/security/asa/asa80/license/license80.html>

If you are upgrading from a previous PIX version, save your configuration and record your activation key and serial number. For new installation requirements, go to the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>

## Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 8.0(4). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 8.0(4). If you are using ASDM, we recommend no more than a 500 KB configuration file, because larger configuration files can interfere with the performance of ASDM on your workstation.

While configuration files up to 2 MB are supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as the **write terminal** and **show running-config** commands
- Failover (the configuration synchronization time)
- During a system reload

## Cisco VPN Software Interoperability

| Cisco VPN Series             | Interoperability Comments   |
|------------------------------|---|
| Cisco IOS routers            | Version 8.0(4) requires Cisco IOS Release 12.3(T)T or higher running on the router when using IKE Mode Configuration on the security appliance. |
| Cisco VPN 3000 concentrators | Version 8.0(4) requires Cisco VPN 3000 concentrator Version 4.1 or higher for correct VPN interoperability.                                     |

## Cisco VPN Client Interoperability

| Cisco VPN Client   | Interoperability Comments  |
|--|--|
| Cisco VPN client v3.x/4x<br>(Unified VPN client framework) | Version 8.0(4) supports the Cisco VPN client Version 5.x or higher that runs on all Microsoft Windows platforms. This version also supports the Cisco VPN client Version 5.x or higher that runs on Linux, Solaris, and Macintosh platforms. |

## Cisco Easy VPN Remote Interoperability

| Cisco Easy VPN Remote                             | Interoperability Comments  |
|---|--|
| Cisco PIX security appliance Easy VPN remote V6.3 | Version 8.0(4) Cisco Easy VPN server requires the Cisco PIX security appliance Version 6.3 Easy VPN remote that runs on the PIX 501 and PIX 506 platforms. |
| VPN 3000 Easy VPN remote V3.x/4x                  | Version 8.0(4) Cisco Easy VPN server requires the Version 3.6 or higher of the Easy VPN remote that runs on the VPN 3002 platform.                         |
| Cisco IOS Easy VPN remote Release 12.2(16.4)T     | Version 8.0(4) Cisco Easy VPN server interoperates with Cisco IOS 806 Easy VPN remote Release (16.4)T.   |

## Determining the Software Version

Use the **show version** command to verify the software version installed on your security appliance. Alternatively, you can view the software version on the Cisco ASDM home page.

## Upgrading or Downgrading Software

If you have a Cisco.com login, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

If you want to upgrade from Version 7.2.(x) to Version 8.0(4) or downgrade from Version 8.0(4) to Version 7.2.(x), you must follow the subsequent procedure, because older versions of the security appliance images do not recognize new ASDM images, and new security appliance images do not work with old ASDM images.

You can also use the CLI to download the image. For more information, see the “Downloading Software or Configuration Files to Flash Memory” section in the *Cisco Security Appliance Command Line Configuration Guide*.

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

- 
- Step 1** Load the new Version 8.0(4) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
  - Step 2** Reload the device to upgrade to the Version 8.0(4) image.
  - Step 3** Copy the new ASDM Version 6.0 image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
  - Step 4** Enter the following command to tell the security appliance where to find the ASDM image:  
hostname(config)# **asdm image flash:/asdmfile**
-

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

- 
- Step 1** Load the earlier Version 7.2(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 2** Reload the device to downgrade to the Version 7.2(x) image.
- Step 3** Copy the earlier ASDM Version 5.2(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 4** Enter the following command to tell the security appliance where to find the ASDM image:  
 hostname(config)# **asdm image flash:/asdmfile**
- 

## New Features

Table 2 lists the new features for Version 8.0(4).



**Note** Unified Communication features are only supported by the Cisco ASA 5500 series adaptive security appliance.

---

**Table 2** *New Features for PIX Version 8.0(4)*

| Feature  | Description  |
|--|--|
| <b>Remote Access Features</b>                        |  |
| 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.  |

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

| Feature                           | Description   |
|-----------------------------------|---|
| Show Active Directory Groups      | The CLI command <b>show ad-groups</b> was added to list the active directory groups. This feature is useful for the configuration of DAP, which requires the administrator to know the names of the groups on a Microsoft LDAP Active Directory.  |
| <b>Firewall Features</b>          |   |
| QoS Traffic Shaping               | If you have a device that transmits packets at a high speed, such as a 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 <b>shape</b> command. See also the <b>crypto ipsec security-association replay</b> 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.   |
| 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"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> 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 <b>exceed-mss</b> 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"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> |
| TCP Intercept statistics          | You can enable collection for TCP Intercept statistics using the <b>threat-detection statistics tcp-intercept</b> command, and view them using the <b>show threat-detection statistics</b> command.   |
| Threat detection shun timeout     | You can now configure the shun timeout for threat detection using the <b>threat-detection scanning-threat shun duration</b> command.  |
| Timeout for SIP Provisional Media | You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.   |

## Caveats

This section lists the open and resolved caveats for Version 8.0(4).

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description.

**Note**

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

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

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

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

## Open Caveats - Version 8.0(4)

**Table 3**      *Open Caveats*

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsj08209  | No                      | clear ospf process causes traceback                                      |
| CSCsm20204  | No                      | Extended ping command with no ip specified causes stuck thread           |
| CSCsm21859  | No                      | Privileged commands being shown in unprivileged mode                     |
| CSCsm24047  | No                      | DNS query is sent out before cmd is completed when dns enabled           |
| CSCsm74180  | No                      | MFEM A/S Failover is not syncing after config from blank config          |
| CSCsm99532  | No                      | RTlog viewer is hanging when websense log messages are seen              |
| CSCso64944  | No                      | ASA memory leak due to IPSEC   |
| CSCso65967  | No                      | SIP inspection possible memory leak                                      |
| CSCso95135  | No                      | Zero-downtime upgrade from 7.2 not possible anymore after 8.0.3.10       |
| CSCso98724  | No                      | TCP flow count and TCP intercept values stuck once xlate is built        |
| CSCsq31399  | No                      | Traceback in Thread Name: vpnfol_thread_msg when doing write standby     |
| CSCsq65437  | No                      | ASA 8.0 does not correctly calculate TCP MSS for traffic to the box      |
| CSCsq77355  | No                      | IKE peer ID validation cert fails  |
| CSCsq78576  | No                      | High CPU and memory results in %ASA-0-716507 message on cli              |
| CSCsq84093  | No                      | PIX/ASA: Accounting packet shows "unknown" as username                   |
| CSCsr09436  | No                      | FTP buffer logging queue not cleared when logging is disabled            |
| CSCsr17063  | No                      | Traceback in Thread Name Dispatch Unit                                   |
| CSCsr23628  | No                      | ASA ignores webtype ACLs with "?" char in URL                            |
| CSCsr38644  | No                      | Service column in Top 10 Access Rules shows object-group, not service    |
| CSCsr56975  | No                      | Traceback while executing the "ddns update hostname xxxx" command        |
| CSCsr60721  | No                      | IKE FSM gets into state with multiple Ph1 SAs in MM_FREE - reload needed |

**Table 3** Open Caveats (continued)

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsr66402  | No                      | Tracebacks on standby unit (Thread Name: lu_rx)                      |
| CSCsr68384  | No                      | assertion in ptr + size == block->memory + block->pos                |
| CSCsr68915  | No                      | ASA 8.0.3: Traceback during LDAP lookup                              |
| CSCsr74265  | No                      | ASA crypto HW error when trying to fragment small IP packet          |
| CSCsr85091  | No                      | PIX/ASA may reload with traceback in CMGR Server Process             |
| CSCsr89122  | No                      | Inactive keyword on ACL should not be allowed on NAT ACL at all.     |
| CSCsr96463  | No                      | ASA denial of service on dhcp server                                 |
| CSCsr96775  | No                      | ASA source MAC address to request DHCP - dont work properly QIP srvr |
| CSCsu02718  | No                      | snmp-get-next incorrect value IP-MIB::ipAdEntAddr from standby       |

## Resolved Caveats - Version 8.0(4)

**Table 4** Resolved Caveats

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsg69408  | Yes                     | Need warning when using time based ACLs with policy NAT/PAT              |
| CSCsh91747  | Yes                     | SSL VPN stress cause SSL lib error. Function: DO_SSL3_WRITE              |
| CSCsi06469  | Yes                     | Inactivating then reactivating nat 0 multiple access-lists breaks nat 0  |
| CSCsi41346  | Yes                     | user session and idle timeout values not honored by cut-thru-pxy         |
| CSCsi79159  | Yes                     | admin connections to PIX with crypto card via management-access fail     |
| CSCsi84143  | Yes                     | Mem del-free-poisoner fails to svc alloc requests from the poisoned pool |
| CSCsj12938  | Yes                     | PIX/ASA - show ip audit count - signatures 6050 - 6053 are Informational |
| CSCsj25896  | Yes                     | ASA may reload with traceback in Thread name: CTM Message Handler        |
| CSCsj71788  | Yes                     | Slow response when entering commands via Telnet                          |
| CSCsk18083  | Yes                     | nat exemption access-list not checked for protocol or port when applied  |
| CSCsk19065  | Yes                     | Excessive High CPU and packets drops when applying ACL to an interface . |
| CSCsk43103  | Yes                     | Traceback in Thread Name emweb/https                                     |
| CSCsk47949  | Yes                     | ASDM hangs at 47% if packet losses on the network                        |
| CSCsk49506  | Yes                     | Local-host for u-turn traffic on lowest sec level used for license limit |
| CSCsk50879  | Yes                     | L2TP with EAP authentication In use List count session leaking           |
| CSCsk58346  | Yes                     | Memory leak when adding/removing nameif                                  |
| CSCsk59083  | Yes                     | ASA 5505 failover: rebooted unit becomes active after reload             |

**Table 4**      **Resolved Caveats (continued)**

| DDTS Number | Software Version 8.0(4) |   |
|-------------|-------------------------|---|
|             | Corrected               | Caveat  |
| CSCsk59189  | Yes                     | Top N data sent to ASDM is incorrect when ACE changes                   |
| CSCsk65863  | Yes                     | traceback in ppp_timer_thread   |
| CSCsk69878  | Yes                     | ASA running 8.0.2 rejects DHCP leases less than 32 seconds              |
| CSCsk70941  | Yes                     | Traceback in Thread Dispatch Unit: snp_tcp_timeout_cb                   |
| CSCsk76770  | Yes                     | vpn-filter may prevent renegotiation of the tunnel                      |
| CSCsk80789  | Yes                     | RTSP inspection changes Media Player version to 0.0.0.0                 |
| CSCsk82261  | Yes                     | ASA 8.0.2: threat-detection command does not work with names            |
| CSCsk85428  | Yes                     | Traceback in scheduler  |
| CSCsk85441  | Yes                     | Traceback in thread https_proxy   |
| CSCsk89452  | Yes                     | Remote-access users are mapped to RADIUS Service-Type 1 Login           |
| CSCsk89639  | Yes                     | Traceback with Thread Name: Checkheaps                                  |
| CSCsk96804  | Yes                     | Traceback in Thread Name: Dispatch Unit with inspect h323               |
| CSCsl04218  | Yes                     | vpn-filter for ios ezvpn w/secondary ip address broken in 8.0           |
| CSCsl04900  | Yes                     | SIP invite fixup'd with name rather than IP address                     |
| CSCsl10052  | Yes                     | new L2TP sessions are denied after %ASA-4-403103 is seen in the logs    |
| CSCsl11139  | Yes                     | ASA context listed as "Unknown" in 'show event alert' output .          |
| CSCsl11321  | Yes                     | ASA doesn't send coldStart trap when speed/duplex is fixed as 100/full  |
| CSCsl12449  | Yes                     | DHCP Client - remove minimum lease time restriction .                   |
| CSCsl15013  | Yes                     | DHCP relay broken with 2 DHCP relay servers when 2nd one out of service |
| CSCsl21500  | Yes                     | Traceback with 'no capture <name>' for ISAKMP type capture .            |
| CSCsl26135  | Yes                     | Memory leak when FTP filter is enabled                                  |
| CSCsl26200  | Yes                     | ASA SSL VPN ACL bypass  |
| CSCsl26957  | Yes                     | SNMP Remote Access MIB crasSessionTable does not return data            |
| CSCsl28306  | Yes                     | PIX/ASA default route redistributed into EIGRP when explicitly disabled |
| CSCsl29315  | Yes                     | Syslog 713902 appears on standby unit when disconnecting VPN connection |
| CSCsl30307  | Yes                     | PIX/ASA fails to install cert with an empty subject/issuer alt name ext |
| CSCsl31908  | Yes                     | ASA: SIP inspection drops SIP message 200 OK from 3rd party CosmoCall   |
| CSCsl32225  | Yes                     | Traceback in Thread Name: Checkheaps when Simultaneous login set to 1   |
| CSCsl32785  | Yes                     | Traceback in Thread Name: pix_flash_config_thread                       |
| CSCsl33600  | Yes                     | Traceback when show service after removing global policy with police    |
| CSCsl34337  | Yes                     | CSD:DAP_ERROR: Unable to load Host Scan data, error = 3 .               |
| CSCsl35591  | Yes                     | Bulk skinny registration creates 2048 block leak .                      |
| CSCsl35603  | Yes                     | Memory corruption with csc and nat testing .                            |
| CSCsl37767  | Yes                     | Traceback when timeout with L2TP and delay-free-poisoner enabled .      |

Table 4 Resolved Caveats (continued)

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCs138314  | Yes                     | HA: SNMP trap authentication replicated to standby improperly            |
| CSCs141666  | Yes                     | Crypto debug command should not dump keys as part of the SA              |
| CSCs143246  | Yes                     | L2TP with EAP authentication In use List count session slowly leaking    |
| CSCs144845  | Yes                     | bad vPifNum errors on AAA accounting for a RA vpn session on boot        |
| CSCs146310  | Yes                     | ASA error: "Unable to download NAT policy for ACE" with nat 0 ACL        |
| CSCs148060  | Yes                     | show route <intf> <ip addr> : Could display wrong information            |
| CSCs149999  | Yes                     | ! used in downloadable ACL yields "error unable to apply access list"    |
| CSCs151797  | Yes                     | ASA traceback in AAA thread  |
| CSCs152765  | Yes                     | TD may put target of no-reply UDP sessions to shunned list               |
| CSCs152895  | Yes                     | ASA 7.2.3 number of IPSec SA not replicated in failover unit             |
| CSCs154352  | Yes                     | 8.0.3: snp_td_init_acl_hit_top_history not being freed when ACLs removed |
| CSCs155623  | Yes                     | SNMP link trap varbind list missing values                               |
| CSCs157533  | Yes                     | setting privilege for capture does not affect "no capture"               |
| CSCs166538  | Yes                     | ASA "hardware accelerator encountered an error (Invalid PKCS Type)"      |
| CSCs166758  | Yes                     | TCP intercept comes before ACL checks. All TCP ports appear open.        |
| CSCs168785  | Yes                     | Confusing Error message when Interfaces have overlapping networks        |
| CSCs170296  | Yes                     | failover link is lost with redundant int and EIGRP after rebooting       |
| CSCs170685  | Yes                     | Traceback in Thread Name: accept/http                                    |
| CSCs171113  | Yes                     | 'Configure Memory' command with DDNS config causes traceback             |
| CSCs178110  | Yes                     | Downloadable ACL does not get removed from memory in some scenarios      |
| CSCs179211  | Yes                     | Traceback: AAA task overflow when object-group acls and virtual telnet   |
| CSCs182200  | Yes                     | IPSec not encrypting after failover.                                     |
| CSCs183503  | Yes                     | Threat detection - Scanning drops occur even with basic TD disabled      |
| CSCs184179  | Yes                     | Traceback at ssh thread when working with 'capture'                      |
| CSCs187918  | Yes                     | IPSec: RESPONDER-LIFETIME not properly created.                          |
| CSCs188161  | Yes                     | CSD not starting on Linux - webstart.xml parsing error (malformed)       |
| CSCs188730  | Yes                     | Crash at chunk_free, chunk absent with Skinny                            |
| CSCs189105  | Yes                     | Traceback when enabling blocks queue history w/ hi load/low mem          |
| CSCs189162  | Yes                     | show cheakheaps displays negative number for "total memory in use"       |
| CSCs189537  | Yes                     | SIP: Improperly adding some value in From-tag when sending BYE           |
| CSCs189653  | Yes                     | SIP connection entry not be cleared after sip_disconnect timeout         |
| CSCs191005  | Yes                     | Traceback in Thread Name: CP Processing under TCP/UDP load               |
| CSCs191061  | Yes                     | Traceback while adding regex with Sys send and Udp send SIP traffic load |
| CSCs193495  | Yes                     | SIP: ASA shows 4xx response message as 500 on debug sip                  |

**Table 4**      **Resolved Caveats (continued)**

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCs195043  | Yes                     | PIX/ASA: L2TP/IPsec needs both "ipsec" and "l2tp-ipsec" in group-policy  |
| CSCs195856  | Yes                     | DHCP learned default route not in route table if other DHCP interfaces   |
| CSCs196219  | Yes                     | SIP: Failure to associate re-invites to the original SIP session         |
| CSCs196502  | Yes                     | SIP: sess is not kept around for ACK in response to non2xx final RESP    |
| CSCsm02280  | Yes                     | Status says registering but device does not send Register packets        |
| CSCsm03104  | Yes                     | ASA, write standby copies a no crypto isakmp nat-traversal               |
| CSCsm03751  | Yes                     | SNMP Coldstart Trap is Only Sent to the Last Configured NMS              |
| CSCsm05055  | Yes                     | Traceback seen when 'established udp 0 0' command is enabled             |
| CSCsm05181  | Yes                     | traceback in Thread: vpnfol_thread_msg                                   |
| CSCsm07888  | Yes                     | Authenticator value on retransmitted RADIUS request pkt changed          |
| CSCsm09584  | Yes                     | EAP l2tp authentication fails if mschapv2 is configured on the same TG   |
| CSCsm11925  | Yes                     | ASA WebVPN generates bad Citrix ticket causing "SSL Error 35" on client  |
| CSCsm13717  | Yes                     | SNMP Remote Access MIB crasSessionTable returns incorrect data           |
| CSCsm18372  | Yes                     | show input hardware queue max counters incorrect                         |
| CSCsm18437  | Yes                     | clear interface doesn't clear max queue counter                          |
| CSCsm21708  | Yes                     | DAP: Tunnel Group returns Null after new pin mode challenge              |
| CSCsm21719  | Yes                     | threat-detection not releasing cached memory after being disabled        |
| CSCsm22241  | Yes                     | PIX/ASA vlan mapping fails when username is less than 4 characters       |
| CSCsm22781  | Yes                     | PIX/ASA: RPF(reverse path forwarding)chk fails when PMTUD packet is sent |
| CSCsm23689  | Yes                     | SSL session cache size is too large for some platforms                   |
| CSCsm25189  | Yes                     | Inconsistent behavior for different kind of SIP packets                  |
| CSCsm26841  | Yes                     | Watchdog failure: TLS fragmented client hello message.allocb+185         |
| CSCsm29337  | Yes                     | Dest unicast address to multicast address NAT not working in 7.x         |
| CSCsm30926  | Yes                     | ASA: Traceback with high voice traffic and voice inspection              |
| CSCsm32972  | Yes                     | SNMP Counters Get Stuck on Repeated Polls                                |
| CSCsm36660  | Yes                     | DHCP Server: Must send DHCP decline if DHCP proposes in-use address      |
| CSCsm36857  | Yes                     | External group-policy via Radius can cause duplicate IP assignment       |
| CSCsm39684  | Yes                     | L2TP over IPsec rekeys are not reflected in statistics                   |
| CSCsm39781  | Yes                     | ASA High CPU under certain configuration conditions                      |
| CSCsm41986  | Yes                     | Need to handle fragmented IP packets with 8-byte first frag              |
| CSCsm45722  | Yes                     | SIP:Caller's RTP/RTCP timeout should set to sip_invite                   |
| CSCsm46182  | Yes                     | DHCP Client: Device's DHCP client does not renew when lease expires      |
| CSCsm46880  | Yes                     | Aware HTTP Server: memory leak   |
| CSCsm47185  | Yes                     | traceback when an interface configured for IPV6 changes to link up state |

Table 4 Resolved Caveats (continued)

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsm48386  | Yes                     | ASA with local command authorization not able to download conf from AUS  |
| CSCsm48412  | Yes                     | SSL rec paramater list continues to grow without boundaries.             |
| CSCsm50135  | Yes                     | Memory leakage caused by catcher_recv_packet_have_sa                     |
| CSCsm51459  | Yes                     | GTP: IMSI prefixing doesn't work with 2 digit MNC                        |
| CSCsm54473  | Yes                     | FO:standby box is unable to sync config and reloads with acl config      |
| CSCsm59304  | Yes                     | SIP: INVITE not passing after failover                                   |
| CSCsm61494  | Yes                     | SIP: Inspection may open unknown port "50195"                            |
| CSCsm61775  | Yes                     | SIP: Unnecessary xlate created after a voice device hands over           |
| CSCsm62831  | Yes                     | SIP: Unneeded half-open xlate entry is generated                         |
| CSCsm64838  | Yes                     | Traceback occurs in Dispatch Unit with 7.2.3.15 and L2TP/PPP             |
| CSCsm66887  | Yes                     | Nas-Port attribute differs for authentication/accounting for l2tp/ipsec  |
| CSCsm66982  | Yes                     | PIX/ASA: L2TP session should not establish when authorization fails      |
| CSCsm67466  | Yes                     | Apply Control-plane ACL fail, need clear/apply it again to work properly |
| CSCsm69116  | Yes                     | L-L tunnels still failing upon IP addr change on peer.                   |
| CSCsm70077  | Yes                     | SIP:Local/Local connection entry is created                              |
| CSCsm70246  | Yes                     | SIP: Duplicate "mi" connections when receiving REINVITE                  |
| CSCsm71772  | Yes                     | Memory leak in 141824 size block when using cut-through authentication   |
| CSCsm73565  | Yes                     | Traceback in Thread Name Dispatch Unit during network scan               |
| CSCsm73654  | Yes                     | Syslog 111111 appears when both active/standby units reload at once      |
| CSCsm75212  | Yes                     | Traceback in Thread Name: IKE Daemon (Old pc 0x0050a493 ebp 0x0346e)     |
| CSCsm82753  | Yes                     | Phase 2 fails if PFS is required. - ASA -IOS l2tp IPSEC                  |
| CSCsm83098  | Yes                     | SIP:Fails to create m connection when ACK to 407 is lost                 |
| CSCsm83636  | Yes                     | CPU hog during config sync   |
| CSCsm84110  | Yes                     | ASA may traceback with malformed TCP packets                             |
| CSCsm85736  | Yes                     | shutdown interface e0/6 triggers interface e0/0 shutdown on ASA5505      |
| CSCsm85872  | Yes                     | snmp trap for PHYSICAL interface is not sent when a port goes down.      |
| CSCsm86644  | Yes                     | sunrpc tcp inspect fragment reassembly fails in certain cases.           |
| CSCsm87351  | Yes                     | simultaneous accounting - the request are not forwarded to FAILED serve  |
| CSCsm88116  | Yes                     | SIP:Failure to update to-tag when no-2xx response is received            |
| CSCsm90239  | Yes                     | ASA traceback in Unicorn Admin Handler Thread                            |
| CSCsm90267  | Yes                     | SIP: media pinholes not opened when callers SDP is sent in ACK           |
| CSCsm91261  | Yes                     | Traceback seen in 'ssh' thread   |
| CSCsm92266  | Yes                     | Traceback may occur when AAA command authorization is enabled            |
| CSCsm92275  | Yes                     | SQL inspection rewrites IP addresses embeded in SQL data                 |

**Table 4**      **Resolved Caveats (continued)**

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsm92613  | Yes                     | ASP drop capture missing type for vpn-handle-error                       |
| CSCsm95566  | Yes                     | EIGRP: Does not send ALL redistributed static routes to peer devices     |
| CSCso00670  | Yes                     | Move ssl debug commands from menu to real CLI                            |
| CSCso03100  | Yes                     | SSL cache entries timing out prematurely                                 |
| CSCso03582  | Yes                     | Overrun counter increments when REINVITE is received                     |
| CSCso05797  | Yes                     | ASA stops accepting L2TP/IPSec connections with rsa-sig                  |
| CSCso07025  | Yes                     | Memory is leaked whenever directory is opened.                           |
| CSCso08335  | Yes                     | ISAKMP: Add syslog when Aggressive mode aborted when Spoof Protection    |
| CSCso10876  | Yes                     | ASA Completes SSL Handshake With Non-Authorized HTTPS Clients            |
| CSCso17920  | Yes                     | SIP media connection cannot be created more than 13 when PBX is used     |
| CSCso18045  | Yes                     | PKI: session opening checks client-types instead of id-usage setting     |
| CSCso18757  | Yes                     | SNMP crasSessionTable Remote Access MIB returns some incorrect entries   |
| CSCso20009  | Yes                     | ASA DHCP proxy not working for L2TP connections                          |
| CSCso21019  | Yes                     | SNMP crasSessionTable Remote Access MIB incorrect EncryptionAlgo         |
| CSCso21063  | Yes                     | l2tp/ipsec client on IOS - tunnel does not go up when behind nat         |
| CSCso22981  | Yes                     | Traceback in Thread Dispatch unit related to IM inspection               |
| CSCso24103  | Yes                     | Delivering shape average command through https failed                    |
| CSCso24494  | Yes                     | PIX/ASA: DHCP server fails to respond to Vista DHCPINFORM request        |
| CSCso35351  | Yes                     | Traceback in Thread Name: vpnfol_thread_msg with show run                |
| CSCso37056  | Yes                     | Memory leak when generating Diffie-Hellman keys.                         |
| CSCso38699  | Yes                     | CPU Hog when replicating config to standby unit                          |
| CSCso38702  | Yes                     | IPSec Pass-through breaks after enabling RA VPN on ASA                   |
| CSCso40008  | Yes                     | PIX is sending DN during rekey instead of FQDN                           |
| CSCso40159  | Yes                     | Ports used by static PAT configurations are not removed from PAT pool    |
| CSCso40520  | Yes                     | re-INVITE is dropped when it's exceeded 119ch after establishing 400ch   |
| CSCso43383  | Yes                     | SIP:media xlate idle timer is not refreshed when receiving 200ok         |
| CSCso43850  | Yes                     | enhance redun ifc as failover ifc to handle comm failure after reload    |
| CSCso46028  | Yes                     | ASA 8.0 CLI : Unable to edit http-form server                            |
| CSCso50226  | Yes                     | PIX/ASA does not send invalid SPI notification for non-existent IPSEC sa |
| CSCso50272  | Yes                     | PIX/ASA:'vpn-simultaneous-logins 1' prev session disc reason not correct |
| CSCso51544  | Yes                     | ASA overwrites default config when rate-interval is set to 600           |
| CSCso55494  | Yes                     | Traceback in PPP callback from AAA thread                                |
| CSCso58622  | Yes                     | IPv6: IP services are reachable from the "far side of the box"           |
| CSCso60605  | Yes                     | ISAKMP : ASA installs permit rule with the interface network mask        |

Table 4 Resolved Caveats (continued)

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCso62906  | Yes                     | ASA traceback when running show pim tunnel <interface> command           |
| CSCso62916  | Yes                     | allocate interface command fails to execute intermittently.              |
| CSCso63159  | Yes                     | Traceback in fover_thread while testing licensing regression scripts     |
| CSCso63371  | Yes                     | Panic: Dispatch Unit - Fmsg_free() - non null next on MMP traffic        |
| CSCso64731  | Yes                     | security-association lifetime cannot be removed with no crypto map ...   |
| CSCso68547  | Yes                     | PIX/ASA HTTP inspection: Multiple content-length headers issue           |
| CSCso79412  | Yes                     | traceback in dispatch thread/occam during CUMA testing                   |
| CSCso81153  | Yes                     | Traceback in dispatch unit with MGCP inspection                          |
| CSCso82264  | Yes                     | ICMP inspection may drop ICMP error packets                              |
| CSCso84996  | Yes                     | ASA truncates CN field at 11 characters if CN contains '@' (W2K CA)      |
| CSCso85369  | Yes                     | CSD: DfltCustomization loaded if pre-login check enabled                 |
| CSCso85452  | Yes                     | h323 messages on console; performance degrade                            |
| CSCso85547  | Yes                     | ipAdEntIFIndex MIB value not sent at failover interface                  |
| CSCso87435  | Yes                     | NAT-T not working when client source port not 4500 with ACL match        |
| CSCso91010  | Yes                     | ASA doesn't send RootCA cert in chain                                    |
| CSCso91190  | Yes                     | Traceback while deleting static NAT configuration                        |
| CSCso91658  | Yes                     | IP tos byte for skinny/ sip packet is lost if inspection is configured   |
| CSCso94098  | Yes                     | SIP:"o="address in SDP is not translated when "c=" is in all media desc. |
| CSCso97405  | Yes                     | ASA should allow configurable MSS or use from MTU for to-the-box traffic |
| CSCsq03893  | Yes                     | Segmented HTTP GET request are not parsed by Filtering and HTTP inspect  |
| CSCsq04082  | Yes                     | LDAP AAA server with null hostname causes traceback                      |
| CSCsq06129  | Yes                     | PIX/ASA: Standby unit may reboot without recording a crash file          |
| CSCsq07395  | Yes                     | Adding shaping service-policy fails if policy-map has been edited        |
| CSCsq08550  | Yes                     | Traffic shaping with priority queueing causes traffic failure on ASA     |
| CSCsq08990  | Yes                     | PIX/ASA certificate authorization fails if UPN is not last attr in SAN   |
| CSCsq11726  | Yes                     | Traceback in PPP callback from AAA thread (UPAP/PAP)                     |
| CSCsq12934  | Yes                     | Auth proxy fails w/ "too many pending auths" in syslog                   |
| CSCsq13321  | Yes                     | Standby Failover unit traceback in Thread Name: vpnfol_thread_msg        |
| CSCsq22716  | Yes                     | Threat Detection - incorrectly classifying drops as scanning threat      |
| CSCsq24213  | Yes                     | ASA HEAP memory leak in ldap_client_root_dse_get                         |
| CSCsq33551  | Yes                     | SIP/ACK session remains if ASA receives ACK as the 1st packet            |
| CSCsq37647  | Yes                     | Overrun/Underrun/NoBuffer cnts are incremented when sip-invite timeout   |
| CSCsq44735  | Yes                     | ASA: redudant failover interface is failed, but ping works               |
| CSCsq44802  | Yes                     | ASA EzVPN server preserves static RRI routes when interface is shut down |

**Table 4**      **Resolved Caveats (continued)**

| DDTS Number | Software Version 8.0(4) |  |
|-------------|-------------------------|--|
|             | Corrected               | Caveat   |
| CSCsq44918  | Yes                     | Traceback in vpnfol_thread_timer (Address not mapped)                    |
| CSCsq46179  | Yes                     | Longer timer needed for eToken credential entry.                         |
| CSCsq46425  | Yes                     | Traceback in Dispatch Unit (Page Fault)                                  |
| CSCsq50494  | Yes                     | PIX/ASA: NAT-T Keepalive should not generate UDP request discarded msg   |
| CSCsq53954  | Yes                     | RRI route not removed if more specific dynamic route for same net exists |
| CSCsq60414  | Yes                     | ASA fails to update mac address table after failover                     |
| CSCsq66348  | Yes                     | Unable to SSH into Standby Firewall                                      |
| CSCsq66561  | Yes                     | Static arp entry for active or standby ips causes failover instability   |
| CSCsq66899  | Yes                     | Firewall replies with no data when optional firewall is configured       |
| CSCsq79382  | Yes                     | ASA 8.0.3.12 aaa authentication listener with redirect will block conns  |
| CSCsq85924  | Yes                     | Interface name is missing in syslog 411001 and 411002                    |
| CSCsr07177  | Yes                     | Traceback on adding acl element to acl associated with nat               |
| CSCsr11626  | Yes                     | skinny inspection breaks sccp calls through the firewall                 |
| CSCsr28008  | Yes                     | PAT src port allocation policy negates effect of host port alloc. policy |
| CSCsr39457  | Yes                     | Skinny callgens fail to register due to small messages                   |
| CSCsr40360  | Yes                     | iPhone 2.0 SW requires that ASA/PIX 7.x+ address mask is 255.255.255.255 |
| CSCsr66684  | Yes                     | TD Shun doesn't work if except list is specified                         |
| CSCsr66685  | Yes                     | ASA re-loads on the text message test                                    |
| CSCsr71463  | Yes                     | ASDM not receiving historical data from platform thru asdm_handler       |

## Related Documentation

Use this document in conjunction with the PIX firewall documentation at the following websites:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/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.

---

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.