



# Cisco PIX Security Appliance Release Notes Version 7.2(2)

---

November 2006

## Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 5](#)
- [Important Notes, page 6](#)
- [Caveats, page 7](#)
- [Related Documentation, page 22](#)
- [Obtaining Documentation and Submitting a Service Request, page 22](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# Introduction


**Note**

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.2(2).

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 [New Features, page 5](#).

Additionally, the 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 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 7.2(2).

## Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you need to upgrade your memory before performing an upgrade to PIX Version 7.0. PIX Version 7.0 requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses. The following security appliance platforms require at least 64 MB of RAM. [Table 1](#) lists Flash memory requirements for Version 7.2(2).

**Table 1** *Flash Memory Requirements*

Security Appliance Model	Flash Memory Required in Version 7.2(2)
PIX 515/515E	16 MB
PIX 525	16 MB
PIX 535	16 MB

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

## Software Requirements

Version 7.2(2) requires the following:

1. The minimum software version required before performing an upgrade to PIX Version 7.2(2) is PIX Version 7.0. If you are running a PIX version prior to PIX Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can begin the upgrade to PIX Version 7.0.

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

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

2. 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/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)
3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. See <http://www.cisco.com/public/sw-center/index.shtml> for new installation requirements.

## Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 7.2(2). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.2(2). 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 7.2(2) 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 7.2(2) requires Cisco VPN 3000 concentrator Version 3.6 or higher for correct VPN interoperability.

## Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco VPN client v3.x/4x (Unified VPN client framework)	Version 7.2(2) supports the Cisco VPN client Version 3.6 or higher that runs on all Microsoft Windows platforms. It also supports the Cisco VPN client Version 3.6 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 7.2(2) 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 7.2(2) 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 7.2(2) 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 see the software version, on the Cisco ASDM home page.

## Upgrading to a New Software Version

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

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

If you want to upgrade or downgrade from Version 7.1.(x) to 7.2(x) and vice versa You must follow the steps below because older versions of the security appliance images does not recognize new ASDM images, new security appliance images does not recognize old ASDM images.

You can also use command-line interface to download the image, see the “Downloading Software or Configuration Files to Flash Memory” section in the *Cisco Security Appliance Command Line Configuration Guide*.

To upgrade from Version 7.1.(x) to 7.2(x), you must perform the following steps:

- 
- Step 1** Load the new Version 7.2(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 2** Reload the device so that it will start using the Version 7.2(x) image.

**Step 3** Copy new 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, this will tell the security appliance where to find the ASDM image:

```
hostname(config)# asdm image flash:/ asdm file
```

---

To downgrade from Version 7.2(x) to 7.1.(x), you must perform the following steps:

---

**Step 1** Load the earlier Version 7.1(x) image from the following website:

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

**Step 2** Reload the device so that it will be use the Version 7.1(x) image.

**Step 3** Copy the ASDM Version 5.1(x) image from the following website:

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

**Step 4** Enter the following command, this will tell the security appliance where to find the ASDM image:

```
hostname(config)# asdm image flash:/ asdm file
```

---

## New Features

This section lists the new feature for Version 7.2(2). All new features are supported in ASDM 5.2(2).

### HTTP(S) Authentication Challenge Flexible Configuration

In Version 7.2(2), the security appliance authenticates HTTP network connections using basic HTTP authentication and authenticates HTTPS connections by generating similar custom login windows. This is the same exact behavior that was present in Version 7.1 and prior. You can use basic HTTP authentication if:

- You do not want the security appliance to open listening ports
- You use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance
- Basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

The new **aaa authentication listener** command enables the security appliance to authenticate web pages and select the form based redirection approach that is currently used in Version 7.2(1). In the absence of this new command, Version 7.1 authentication method is used.



#### Note

By default the the **aaa authentication listener** command is not present in the configuration, making Version 7.1 **aaa** behavior the default for 7.2(2). However, when a Version 7.2(1) configuration is upgraded to Version 7.2(2), the appropriate **aaa authentication listener** commands are added to the configuration so that the **aaa** behavior will not be changed by the upgrade.

---

In Versions 7.1 and prior, the security appliance authenticated HTTP and HTTPS network connections by interacting with the client in a transparent manner, by using basic authentication for HTTP connections and by generating similar custom login windows for HTTPS connections. After successfully authenticating the client, the security appliance would connect through to the intended server. This approach did not require listening ports to be opened on the security appliance interfaces.

In Version 7.2(1), this functionality was replaced by a form based authentication approach where HTTP and HTTPS connections are redirected to authentication pages that are served from the security appliance. After successful authentication, the browser is again redirected to the originally-intended URL. This was done to provide:

- More graceful support authentication challenge processing
- An identical authentication experience for http and https users
- A persistent logon/logoff URL for network users This approach does require listening ports to be opened on the security appliance on each interface on which **aaa authentication** was enabled.

## Important Notes

This section lists important notes related to Version 7.2(2).

### virtual http Command

The **virtual http** command has been restored. This is needed with basic authentication when you have cascading authentication requests.

### FIPS 140-2

Version 7.2(2) has been submitted for FIPS 140-2 Level 2 validation.

## User Upgrade Guide

Before upgrading to Version 7.2(2), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*. This guide includes information about deprecated features and other changes in the Cisco PIX software Version 7.0. For a list of deprecated features and user upgrade information, go to the following URL:

[http://www.cisco.com/en/US/docs/security/asa/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)



#### Caution

If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Do not upgrade until you have corrected your configuration, as this is not a supported configuration and Version 7.2(2) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.2(2) with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.

## Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The security appliance Outbound and Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and optimize the ACL feature set. ACL-based configurations provide the following benefits:

- ACE insertion capability— Provides simplified system configuration and management, which allows you to add, delete or modify individual ACEs.
- Outbound ACLs and time-based ACLs— Provides administrators with improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling and Disabling of ACL entries — Provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs without the need to remove and replace ACL entries.

### Features not Supported in Version 7.2(2)

The PPTP feature is not supported in Version 7.2(2).

### Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode. Use the **downgrade** command only if you want to downgrade to a version other than 7.x.

For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.



#### Caution

---

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. If you load a software image from monitor mode onto a PIX security appliance that has a PIX Version 7.0 file system, unpredictable behavior may occur and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

---

## Caveats

The following sections describe the caveats for the Version 7.2(2).

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation 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://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 7.2(2)

**Table 2** Open Caveats

DDTS Number	Software Version 7.2(2)	
	Corrected	Caveat
CSCsd50888	No	L2TP: connections fail intermittently -> error 678: There was no answer
CSCse88291	No	ASA crashes with WEBVPN user login when memory is running low.
CSCse92565	No	Traceback in Thread Name: tmatch compile thread after clear config all
CSCsf04123	No	Packet drops through VPN due to No route to VPN_peer_ip_address
CSCsf05298	No	Citrix not supported with CSC module
CSCsf13404	No	PIX cosmetic high memory use in context show memory
CSCsf25418	No	Traceback in Thread Name: tmatch compile after assert
CSCsf27202	No	AAA Radius NAS-Port-Type not sent in authentication request
CSCsg03102	No	Minor correction to vpn-addr-assign command reference documentation
CSCsg20953	No	WebVPN sessions created in the Secure Desktop don't expire
CSCsg26668	No	Undefined CSCO functions in JavaScript-generated HTML
CSCsg34853	No	Traceback with Thread Name: Dispatch Unit
CSCsg38186	No	Traceback in Thread Name: Dispatch Unit
CSCsg43591	No	SCP connection to PIX fails
CSCsg46962	No	WebVPN some functions do not work in javascript
CSCsg47023	No	L2TP Connections with Certificates to ASA Fail to Connect
CSCsg47241	No	Traceback when parsing LDAP config
CSCsg48442	No	Ping through ASA fails when using interface PAT on PPPoE interface
CSCsg53120	No	ASA WebVPN Time-out on Database Requests
CSCsg56876	No	ASA may crash after applying http or IM deep inspection
CSCsg60095	No	VPN traffic permitted by vpn-filter is denied
CSCsg61719	No	SNMP: Coldstart Trap is not sent
CSCsg62488	No	Traceback in Thread Name: Unicorn Proxy Thread
CSCsg62878	No	ocsp signer crl checking with crl none is not falling back to none

**Table 2**      **Open Caveats**

DDTS Number	Software Version 7.2(2)	
CSCsg63145	No	Traceback with Thread Name: PIX Garbage Collector
CSCsg64427	No	Compression: Can't turn off http-comp
CSCsg64450	No	FO: http auth message should be suppressed on standby console
CSCsg64948	No	1550 blocks exhausted during radius authentication stress test
CSCsg65434	No	Multiple ipsec peers : PIX/ASA stops processing the IPSEC peers list
CSCsg66126	No	Large H.323 Registrations Fail through PIX
CSCsg67443	No	ASA Fails Recursive Route Lookup
CSCsg67961	No	L2TP: IKE rekeying prior to IPsec rekey terminates MAC L2TP
CSCsg68141	No	Show run router causes traceback in thread name: ci/console
CSCsg69275	No	1017-88 byte blocks leaked: _tmatch_summary_func+2877 after vpn sys test
CSCsg69281	No	3000 - 576 byte blocks leaked: _kernel_delete_sa+39 after vpn sys stress
CSCsg69408	No	Need warning when using time based ACLs with policy NAT/PAT
CSCsg69448	No	Need to update 7.x conf guides, time based ACLs not supported w/nat-pat
CSCsg69469	No	Incorrect user privileges when logging in with ASDM 5.2.1.54
CSCsg69998	No	tcp intercept not working when the inside host is running windows OS.
CSCsg70012	No	no sysopt noproxyarp c1in failed to remove noproxyarp for interface c1in
CSCsg70698	No	Session timer is not reset during WebVPN ActiveX and Java tunneling
CSCsg71369	No	P1 SA stuck in AM_FREE on secondary for ipsec sessions using net ext mod
CSCsg71416	No	encrypt rules added in wrong order - NEM misconfig causes data issues
CSCsg71534	No	40 P1 sa's got stuck in MM_Wait_Delete on secondary w/vpn system test
CSCsg71579	No	Programming assertion malloc.c:3822 on secondary after failover from pri
CSCsg73076	No	L2TP/IPSEC to ASA with certificates fails over low speed ISDN
CSCsg73376	No	Traceback in Thread Name: ci/console with large config tftp download
CSCsg75094	No	LDAP: ASA cannot authenticate to Active Directory using MD5
CSCsg75996	No	Radius authentication with downloadable acls causes crash
CSCsg76777	No	7.2 transparent / change of behavior : ASA does not retain the src mac
CSCsg77097	No	WebVPN OWA 2003 email.cisco.com inbox fails to load intermittent
CSCsg77099	No	WebVPN Java archives with uncompressed entries fail through rewriter
CSCsg77390	No	AAA: port-to-port static for port 80 and aaa http listener on same ifc
CSCsg77841	No	Cfg Guide: remove flash size match from failover hw criteria
CSCsg78524	No	With WebVPN login we type it once incorrectly and the ASA tries 3 times
CSCsd50888	No	L2TP: connections fail intermittently -> error 678: There was no answer
CSCse88291	No	ASA crashes with WEBVPN user login when memory is running low.
CSCse92565	No	Traceback in Thread Name: tmatch compile thread after clear config all

## Resolved Caveats - Version 7.2(2)

**Table 3**      *Resolved Caveats*

DDTS Number	Software Version 7.2(2)	
	Corrected	Caveat
CSCei33965	Yes	MPC embryonic timeout value overwrite global conn timeout
CSCek62768	Yes	crash in Unicorn Proxy Thread with large WebVPN session count in build30
CSCsb54431	Yes	clear in unprivileged mode should be removed if not applicable.
CSCsb63230	Yes	Need a command to perform SSM password recovery from the ASA CLI
CSCsc01694	Yes	CRC errors on SSM-4GE Electrical ports on initial bringup
CSCsc37965	Yes	IP-directed broadcasts no longer allowed through device.
CSCsc89262	Yes	Syslog 722007 (WEBVPN_SVC_MSG_EMERG) severity needs to be changed
CSCsd13314	Yes	'show service policy flow' command shows incorrect flow match
CSCsd40989	Yes	L2TP: Populate client type/version within session database
CSCsd45605	Yes	2 routes to same n/w w same metric different ifx should not be allowed
CSCsd52578	Yes	Traceback in thread: snp_timer_thread
CSCsd54495	Yes	Traceback eip_strdup(0xebacac)+0x78 with large customer configuration
CSCsd57264	Yes	MPF: type syntax in help policy-map is missing a ]
CSCsd58688	Yes	SVC connections are not exempt from aaa authentication rules like IPsec
CSCsd59295	Yes	WCCP static bypass not working with vlan interfaces
CSCsd59936	Yes	Registering to the RP for PIM fails if fragmented in more than 12 packs
CSCsd60448	Yes	Proxy-bypass with automatic choice of target server
CSCsd64749	Yes	Failover: automatic removal of SSL trustpoint not replicated to stdby
CSCsd67093	Yes	PPPoE:Vpdn group for PPPoE shouldn't be configurable in Transparent mode
CSCsd67160	Yes	PPPoE:ip address pppoe cmd shouldn't be configurable in multi mode
CSCsd70581	Yes	Crash output to console has incomplete configuration
CSCsd71387	Yes	EzVPN: Tback IKE Daemon (Old pc 0x00507425 ebp 0x0333c6d8)
CSCsd74328	Yes	Traceback when changing sec level on an ifc and failover cfg with NAT
CSCsd74551	Yes	Add NP drop reason documentation for WCCP drops
CSCsd81262	Yes	CA cert with spaces could fail to install
CSCsd81294	Yes	'crypto ca import' of SSL cert may traceback in Thread Name: accept/http
CSCsd82307	Yes	FO: CLI position can get out of sync causing cmd replication failures
CSCsd82575	Yes	unexpected IGMP joins sent when configuring multicast routing
CSCsd84011	Yes	REGEX: ^ (match from beginning of text) does not work in some cases
CSCsd88471	Yes	VPNLB SVC uses virtual cluster certificate after redirecting to a master
CSCsd91587	Yes	functioning email proxy session generates syslog message error
CSCsd93380	Yes	Packets for VPN-12l peer get dropped instead of encrypted

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(2)	
CSCsd94372	Yes	dhcp proxy: no RELEASE sent after failover and disconnect of vpn client
CSCse00996	Yes	tcp normalizer drop to-the-box traffic not conforming to RFC793 (MSS)
CSCse01293	Yes	Traceback in Thread Name: arp_forward_thread
CSCse02354	Yes	Traceback in Thread Name: Dispatch Unit
CSCse03176	Yes	Problem of group-name used in 'sas1-mechanism kerberos group-name'
CSCse05819	Yes	PIX: 33MHz GIG cards show speed/duplex unknown if nonegotiate configured
CSCse07242	Yes	Traceback in pix_flash_config_thread
CSCse08726	Yes	LDAP group-based policy Enforcement shouldn't require Cisco schema
CSCse08746	Yes	ASA send Radius attribute 31 source IP address as 0.0.0.0
CSCse09458	Yes	RadiusSDI feature of VPN Client fails with blank XAUTH text
CSCse09503	Yes	Syslog 304001 not generated when strict-http action allow log configured
CSCse10096	Yes	i2c_write_byte_w_suspend() error after rebooting ASA5505
CSCse10714	Yes	Shun behavior change in 7.x
CSCse12021	Yes	Error msg change when attempt auth-srvr-group None in ipsec tunn-grp
CSCse13544	Yes	Increase in memory usage after enabling-disabling webvpn
CSCse14296	Yes	Trustpoint not found if ASA not enrolled with the trustpoint
CSCse15854	Yes	clear config webvpn only partially clean-up proxy-bypass...
CSCse15977	Yes	Traceback when two admin sessions are working on the same capture
CSCse17176	Yes	SUA policy is unspecified -WEB login requires user to authenticate twice
CSCse17638	Yes	IM: Misc CLI issues
CSCse17660	Yes	Incorrect LDAP debug error when incorrect RDN configured
CSCse18005	Yes	PIX/ASA originate-only VPN fails to create dynamic ACL
CSCse19020	Yes	PPTP Pass-through not working due to inspection
CSCse20501	Yes	Passive FTP to Multinet server fails
CSCse20538	Yes	IKE Syslogs 713041 713042 should specify interface name
CSCse21451	Yes	Memory leak in VPN fover module during failover config syncing
CSCse22330	Yes	Traceback in Thread Name: Dispatch Unit
CSCse22332	Yes	Failed to deploy config when first line in config contain ! character
CSCse22659	Yes	CIFS server names limited to 15 characters
CSCse22668	Yes	CIFS should use DNS lookups for long server names
CSCse23164	Yes	traceback in thread Name: qos_metric_daemon
CSCse23165	Yes	Message sent to client when aaa authorization fails has changed
CSCse23554	Yes	Memory leak within event_smtpmgr:es_SmtpSndMSG function
CSCse23751	Yes	Nested tracebacks may not stop without manual device reload
CSCse24432	Yes	DHCPRelay: Some clients may not get NACKs

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(2)	
	Yes	
CSCse24537	Yes	RIP: [no] access-list defined in distribute-list should display err msg
CSCse24921	Yes	debug icmp does not show request packet being sent
CSCse25515	Yes	FO: dhcpd warnings seen on standby during replication of config
CSCse26317	Yes	inspect radius-acct: show user with IP causing err msg w/ multiple pmaps
CSCse26469	Yes	Cannot store more than one vpdn username/password pairs locally
CSCse27184	Yes	basic attribute is not checked in all mode config attributes, may reload
CSCse27249	Yes	FO: interface monitoring not working on most recent created interface
CSCse27787	Yes	AIC SIP: SIP messages might fail state-check knob when record-route on
CSCse28430	Yes	MS AD-LDAP: set default RDN-Naming Attribute to be sAMAccountName
CSCse28540	Yes	LDAP admin bind: support secure SASL-MD5 and SASL-Kerberos methods
CSCse29700	Yes	WebVPN and SVC Sessions being disconnected due to Idle Timeouts 40+Days.
CSCse29840	Yes	AdmissionConfirm received without an AdmissionRequest, ACF dropped
CSCse30049	Yes	SSH conns to the box not removed after a Failover
CSCse30061	Yes	VPN decompress error when decrypting packet with IP compression
CSCse30102	Yes	VPN dynamic ACL can be deleted from the CLI
CSCse30616	Yes	ASA VPN load balancing cannot ping cluster ip address
CSCse32309	Yes	Timeout of secondary flow causes traceback in Thread Name: Checkheaps
CSCse33143	Yes	Dynamic ACL created under with command access-list <name> d ...
CSCse33211	Yes	aaa http authentication doesnt work when interface IP is named
CSCse33736	Yes	DoD Certs:Subject Alternative Name support for VPN Author for IPSec RA
CSCse33851	Yes	H.225 releasecomplete message was dropped by the firewall
CSCse33986	Yes	Small memory leak when tunnel denied due to unavailable Integrity Server
CSCse34179	Yes	MFW-R: traceback in 'clear cfg all' during a performance test.
CSCse34477	Yes	ESMTP: mail-relay param w/o any action accepted, junk chars in sho run
CSCse34508	Yes	ESMTP: help mail-relay display needs changes
CSCse34540	Yes	telnet and http(asdm) conns are not removed after failover
CSCse35370	Yes	AIC SIP: should not allow overwrite inspect sip <pmap> @ default class
CSCse35566	Yes	Traceback with 'Thread Name: Dispatch Unit' on clear xlate
CSCse35610	Yes	traceback in ci/console after editing group-p CLI sitting at more prompt
CSCse35636	Yes	RTP Conformance print SSRC re-initializing message for bad SSRC Packet
CSCse36112	Yes	PIX/ASA never processes huge access-list if it runs short of memory
CSCse36519	Yes	IM: MSN code improvement to reduce the risk of false positives
CSCse36691	Yes	Traceback on 'cl conf all' with delay-free-poisoner enabled
CSCse37315	Yes	AIC DNS - Traceback after removing certain MPF actions with DNS traffic
CSCse37733	Yes	ASA Crash with nat ID as 0

**Table 3**      **Resolved Caveats (continued)**

DTS Number	Software Version 7.2(2)	
CSCse37787	Yes	Traceback after becoming Active with VPN connections
CSCse38062	Yes	ICA Client users cannot connect to Citrix through WebVPN
CSCse38087	Yes	Kerberos authentication fails after during stress test in multiple-mode
CSCse38659	Yes	unexpected IGMP rejoins when joins previously cfg'd and mcast re-enabled
CSCse39344	Yes	AD UserAccountControl attrib not enforced if using LDAP Authorization
CSCse40332	Yes	ASA multiple mode rollback of config failed for admin and other VC
CSCse40671	Yes	RTSP w/PAT, PIX set client_ports to NULL
CSCse40704	Yes	Lock IMB boot code
CSCse41071	Yes	ldap-login-password not hidden in config
CSCse41663	Yes	WebVPN using SDI Auth - New PIN mode does not work - IPSec OK
CSCse42014	Yes	Java applets archive mangling fails when the codebase is a full url
CSCse42332	Yes	ASA5505: PORT up/down stat is not reflected in show stat + more
CSCse42413	Yes	Traceback after WebVPN authentication with FreeRadius
CSCse43078	Yes	WebVPN: links at <a href="http://www.microsoft.com">www.microsoft.com</a> <outbind://111/www.microsoft.com> fail to work
CSCse43152	Yes	WebVPN/SVC Radius Passwd-Mngt fails when using domain\username format
CSCse43611	Yes	Flash: Wr mem running-config to flash has some issues
CSCse43807	Yes	webvpn url entry with embedded user:Passwd fails with URI is invalid
CSCse44138	Yes	WebVPN Citrix ICA connection losing connectivity due to client_tx_q_full
CSCse44258	Yes	Modifying vpn-filter acl blocks normal traffic from inside to outside
CSCse45308	Yes	Static nailed rule does not match conn destined for that address
CSCse45327	Yes	VPN stateful failover gets out of sync
CSCse45694	Yes	Standby: Traceback in Thread Name: IKE Daemon with dACL
CSCse45948	Yes	write memory all did not report failure for failing to save config
CSCse45971	Yes	Calling-Station-ID passed to radius as 0.0.0.0 for webvpn with pw mgmt
CSCse46220	Yes	ASA: Poor Performance and Out-of-Order packets with SSM module enabled
CSCse46292	Yes	Traceback in Thread Name: snmp
CSCse46874	Yes	Enhancement: per-interface authorization for IPSec connections
CSCse47150	Yes	Traceback in Thread Name: Dispatch Unit with ESMTP Inspect enabled
CSCse47328	Yes	Fix RM flow drop reason #defines
CSCse47400	Yes	WebVPN: Unable to Authenticate using DoD Certificate
CSCse48146	Yes	AIC SIP: fails to match request method <unknown> in inspect SIP pmap
CSCse48193	Yes	ASA vulnerable to cross-site scripting when using WebVPN
CSCse49450	Yes	AAA - dACL and Cisco-AV-Pair ACLs are only applied to the 1st SVC user
CSCse49851	Yes	7.2 5510 security plus license should support only 2 contexts by default
CSCse50716	Yes	URL Filtering: Traceback with Thread Name: Dispatch Unit

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(2)	
	Yes	
CSCse50772	Yes	L2TP/IPSec: MS-Clients unable to connect when ASA is behind a NAT device
CSCse50782	Yes	DNS-based LDAP Authentication/Authorization fails
CSCse50804	Yes	OSPF stuck in EXCHANGE in certain assymmetric routing scenarios
CSCse52050	Yes	Very large ACL applied to NAT or Crypto may traceback in Checkheaps
CSCse53294	Yes	Configuration begin syslog 111007 shows wrong local ip address with ssh
CSCse53987	Yes	'vPif_getVpif: bad vPifNum' errors with cut-through proxy enabled
CSCse54543	Yes	ASA cosmetic high memory use in context show memory
CSCse54582	Yes	AAA: Traceback in Thread Name: Dispatch Unit with Radius auth
CSCse54749	Yes	210007 LU allocate xlate failed syslog generated by overlapping nat cfg
CSCse55066	Yes	VPN: originate-only VPN fails after failover
CSCse55931	Yes	1550 byte block depletion prohibits websense communication
CSCse57386	Yes	5505: EZVPN Remote: DPD timeout is 5 minutes,should be 90 sec
CSCse57889	Yes	Execute certain fover cmds trigger interface testing
CSCse58602	Yes	SVC fails to establish if Cisco-AV-Pair contain both ip and webvpn ACEs
CSCse59113	Yes	5510 base license should not limit 4ge card
CSCse59498	Yes	WebVPN: Citrix traffic may cause Traceback in Thread Name: Dispatch Unit
CSCse59955	Yes	Rommon in ASA5505 main card would reset ASA-SSC-10 card.
CSCse61225	Yes	Support daylight savings changes in Energy Policy Act of 2005
CSCse61315	Yes	SSMIO-4GE SFP interfaces G1/1 - G1/3 don't operate
CSCse61696	Yes	HTTP server enable doesn't take Port number change in Multiple-router mo
CSCse62603	Yes	alias command does not work
CSCse62914	Yes	Standby device Traceback in Thread Name: tcp_thread
CSCse63079	Yes	cpu hog in ssh_init process when connecting via SSH
CSCse63596	Yes	inspect RSH fails when 1st segment contains more than just port
CSCse65000	Yes	WebVPN: Cisco Call Manager is failing thru rewriter
CSCse66007	Yes	AAA commands not working for serial console in multi context mode
CSCse66133	Yes	Traceback in Thread Name: ssh when ACLs are displayed in SSH or ASDM
CSCse66235	Yes	Memory exhausts with logging flash-bufferwrap and high syslog level
CSCse66442	Yes	cut-thru proxy: 'Authentication not required' returned on browse to pix
CSCse66490	Yes	Traceback with 'Thread Name: accept/http' after editing time-based ACLs
CSCse67584	Yes	ldap attr map CLI renders console/session unusable in multi mode
CSCse67916	Yes	Potential memory leakages in webvpn_ica_socks.c with ASA internal errors
CSCse68781	Yes	Traceback in Thread Name: emweb/https when starting to load WebVPN
CSCse70163	Yes	5505/SSC I2C lock up in Rommon.
CSCse70181	Yes	WebVPN: Traceback when using 'debug webvpn citrix 10'

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(2)	
CSCse70993	Yes	Traceback when applying large ACL to NAT or Crypto Map
CSCse71146	Yes	IPSec RA clients with large dACL may cause Traceback in Thread Name:aaa
CSCse73812	Yes	Traceback in Thread Name: Dispatch Unit when L2L VPN Initiator
CSCse74097	Yes	Mac-exempt: mac spoofing does not generate the expected syslog
CSCse74391	Yes	WebVPN not using custom text color for some dialogs
CSCse74778	Yes	Traceback in Thread Name: IP Thread with PPPoE enabled
CSCse74838	Yes	WebVPN: DSF Referral messages missing on distributed Servers over WebVPN
CSCse75485	Yes	Traceback in Thread Name: fover_parse during config sync
CSCse75523	Yes	Received ARP request collision when issuing write standby
CSCse76085	Yes	WebVPN: OWA: file download with size>100KB stops
CSCse76095	Yes	Traceback in Thread Name: Checkheaps when starting WebVPN
CSCse76115	Yes	Cascade delimiter not inserted with correct priority for dynamic crypto.
CSCse76150	Yes	No TACACS+ authorization request sent for show run command
CSCse76171	Yes	ASA reverse bytes order of DHCP scope when using SVC
CSCse76480	Yes	4 byte block allocation lacks the padding
CSCse77122	Yes	FTP-data connection not replicated back to primary after failover
CSCse77261	Yes	Traceback in Thread Name: MFIB with pim mcast routing
CSCse77680	Yes	P2 in progress test broken - could cause unexpected rekey.
CSCse77855	Yes	buffer leak upon IPSEC spoofing.
CSCse77943	Yes	Failover: Primary takes over as Active after reload
CSCse78065	Yes	# sign in config not replicated to Standby unit
CSCse78228	Yes	7.2.1 Crash in snp_tcp_ha_flow_belongs_to_active_context
CSCse78299	Yes	Primary/Secondary units become Active state when failover link failed
CSCse78755	Yes	Traceback in Thread Name: Dispatch Unit when starting DPD timer for SVC
CSCse78779	Yes	Standby become active after fo link failed with fover hold time > 15 sec
CSCse79422	Yes	RA VPN Phase 2 fails when local pool with classless mask is used
CSCse80001	Yes	Traceback in IKE daemon while trying to post event (syslog)
CSCse80897	Yes	AAA: User-Password and EAP-Proxy should not be in same RADIUS request
CSCse81073	Yes	WebVPN: Traceback with Thread Name: emweb/https
CSCse81232	Yes	Failover pair loses failover state configuration after upgrade to 7.2.1
CSCse81273	Yes	Traceback 'Thread Name: Dispatch Unit with PPPOE and SSM-CSC
CSCse81330	Yes	Strict HTTP inspection ignores '304 Not Modified' -syslog message 415014
CSCse81633	Yes	ASA 4GE-SSM Gig ports silently drop IGMP joins
CSCse81656	Yes	LDAP CLI is not displaying quotes when parameters contain spaces
CSCse82262	Yes	No specific error message while uploading a file via HTTPS

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(2)	
CSCse82743	Yes	Java applet fails to load through WebVPN
CSCse83515	Yes	ASA-5550 reports incorrect amount of RAM in show version output
CSCse83905	Yes	dhcprelay stops working if FW interface ip address is modified
CSCse85490	Yes	SSC Rommon resets 5505 switch ports.
CSCse86877	Yes	WebVPN: DNS resolving Port Forwarding hostname entries when it shouldn't
CSCse86968	Yes	Standby unit sends accounting records for replicated DACL commands
CSCse88572	Yes	SIP: Does not parse the compact form of Call-ID
CSCse88632	Yes	WebVPN: Kronos Applet doesn't launch
CSCse88873	Yes	IPV6: TCP SYN-ACK with layer 2 padding dropped
CSCse89013	Yes	debug radius decode does not show all attributes in Radius requests
CSCse89471	Yes	WebVPN: RDP client VBScript function not recognized correctly
CSCse90732	Yes	copy command prevents copying old asdm to tftp
CSCse90796	Yes	ASA with PPPOE crashes in IP Thread
CSCse90864	Yes	3DES license is not accepted in 7.2
CSCse90886	Yes	MacOS VPN Client does not pass traffic with client-update feature on Asa
CSCse91039	Yes	WebVPN: SSL Cert Request from ASA should include all trusted issuer DN's
CSCse91930	Yes	Traceback when using packet tracer with multiple ACL rules
CSCse92016	Yes	WebVPN: Refresh URL in http header not mangled - port CSCse00556 to asa
CSCse94012	Yes	VPN: wrong event generated when concurrent IKE negotiation max exceeded
CSCse94158	Yes	FIPS: Add CRNG callback for new RNGs added since 7.0.4
CSCse94162	Yes	FIPS: Porting damage in content-mangling code
CSCse94241	Yes	Traceback: Thread Name:vpnlb_thread when taking over as failover active
CSCse95357	Yes	WebVPN: reply/forward action of OWA2000 does not attach message
CSCse95408	Yes	Go button shows in pages opened from homepage with url entry disabled
CSCse95437	Yes	Capture: Circular buffer stops capture when buffer full
CSCse96289	Yes	VPN: Traceback with Thread Name: Dispatch Unit
CSCse96559	Yes	vpn-filter does not work when used with IOS ESVPN client
CSCse98397	Yes	EAP state engine triggers retransmission and corrupts EAP session
CSCse98516	Yes	Webvpn: special character '?' cannot be configure in url-list
CSCse98719	Yes	Connection fails with the CA cert of 4096 bits fails with Error #72eh
CSCse98959	Yes	Static Analysis: Add options to make sa for changelist
CSCse99033	Yes	tracked route removed from Standby firewall after failover
CSCse99107	Yes	webvpn/ssl - flow control issues transferring large OWA attachments
CSCse99257	Yes	WebVPN: ActiveX port-forwarder problem
CSCse99783	Yes	DHCP Relay fails when static specified

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(2)	
CSCsf00368	Yes	Crashinfo file may incorrectly show 0% free memory
CSCsf01451	Yes	Inspect IM breaks websense
CSCsf02102	Yes	SIP, show conn after phone registration has wrong information displayed
CSCsf02349	Yes	Traceback in ThreadName: ci/console when add certificate in wrong format
CSCsf04271	Yes	WebVPN connections fail after reload with self signed certs
CSCsf05931	Yes	AAA: group-lock does not handle tunnel-group names with spaces
CSCsf07036	Yes	ASA hangs during initialization after 4GE card is shutdown
CSCsf08950	Yes	AAA: Memory leak with ACL in cut-through-proxy
CSCsf09795	Yes	Using SecureID to auth users may cause high CPU
CSCsf10185	Yes	ASA should allow 255.255.255.255 mask on PPPoE interface
CSCsf10248	Yes	Unable to pass traffic from one context to other through shared int
CSCsf10663	Yes	High CPU / System locks up when adding a network object entry
CSCsf10973	Yes	SSM-4GE I/O card hangs after backplane GPIO power off
CSCsf11095	Yes	show conn display problems for secondary conns with static network
CSCsf11672	Yes	SMTP Inspection with multiple line response fails
CSCsf12352	Yes	Remove unwanted console messages related 4GE SSM
CSCsf12436	Yes	show version on 5505 display cpu as Pentium
CSCsf13906	Yes	ASA may hang during boot
CSCsf14075	Yes	WebVPN: OWA 2007 does not send response/forward
CSCsf14370	Yes	cut-through authentication redirects port, causing connectivity issues
CSCsf15361	Yes	L2TP: disconnects thru PAT/ DSL topology
CSCsf15525	Yes	L2TP: Failure to connect within 120 seconds of initial disconnect
CSCsf16622	Yes	Firewall should log syslog when IGMP report denied by IGMP ACL
CSCsf16633	Yes	ASA - OSPF over VPN tunnel not working correctly
CSCsf17256	Yes	ASA 7.2.1 crash with thread emweb/cifs from snp_tcp_intercept_cb()
CSCsf18590	Yes	show failover not show stateful vlan link failed in link failed scenario
CSCsf18739	Yes	OWA2003 gives an &nbsp; error when used with Webvpn
CSCsf19244	Yes	Traceback in Thread Name: pix_flash_config_thread with vpdn config
CSCsf20095	Yes	ASA5505: Potential issue - GE controller may get stuck at transmit
CSCsf20856	Yes	ASA should return FQDN on HTTP authentication (Socks)
CSCsf21159	Yes	CRL checking fails when using Entrust CA on ASA
CSCsf21253	Yes	Linux VPN Client does not pass traffic when client-update is enabled
CSCsf21488	Yes	vpnfo client timeout causes standby to reload due to failover reset
CSCsf21675	Yes	Change the password reset command string for CSC SSM
CSCsf21882	Yes	Traceback in Thread: Dispatch Unit with QOS police configuration

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(2)	
	Yes	
CSCsf21932	Yes	packet-tracer does not show access-list and object-group information
CSCsf22694	Yes	ESMTP connection not terminated with malformed mail from address
CSCsf23145	Yes	Unable to complete large uploads through VPN if packet loss occurs
CSCsf23672	Yes	Traceback in garbage collector with SIP inspection configured
CSCsf24173	Yes	IPv6: Fixup FTP is not working with IPv6
CSCsf24272	Yes	IPv6: ACL corruption with service object-group
CSCsf24409	Yes	User lockout functionality for telnet to box not working in multimode
CSCsf24901	Yes	WebVPN returns a blank page with error HTTP/1.1 302 Moved Temporarily
CSCsf25601	Yes	OWA2003 SP2 with hotfix Support Required
CSCsf25691	Yes	Authentication not happening with Openldap server
CSCsf25963	Yes	WebVPN OWA 2003 404 error while inbox is loading Premium Client
CSCsf28690	Yes	L2TP/IPsec ASA rejects clients certificate
CSCsf29064	Yes	Management SSH Connections denied - waiting on AAA srv reply
CSCsf29437	Yes	Output for show failover state command needs improvement
CSCsf30454	Yes	Crash in fover_parse due to SNMP during failover replication
CSCsf31731	Yes	First IPv6 connection to the box fails, subsequent connections pass
CSCsf31767	Yes	comma cannot be used in Subject DN in certificate parameters of ASA
CSCsf32319	Yes	Unable to pass traffic between contexts using unique MACs
CSCsf96488	Yes	Need stack trace capability to identify the session disconnection flow
CSCsf97902	Yes	HTTP Inspect regex match of Request header will not match Header-Type
CSCsf98271	Yes	traceback in dns_cache_timer or dns_process using clientless browsing
CSCsf98572	Yes	Webvpn prompt for SecureID pin shows in clear text
CSCsf98804	Yes	Wrong TCP sequence numbers in ICMP Unreachable when sent through ASA
CSCsf99289	Yes	Traceback in Thread Name: aaa
CSCsf99335	Yes	Traceback in Thread Name: IKE Daemon and Checkheaps memory corruption
CSCsf99833	Yes	Traceback in fover_FSM_thread w/deb fover switch and stateful link down
CSCsf99945	Yes	Remove FWSM specific 'show pc ....' cli
CSCsg00066	Yes	Traceback in accept/http with ASDM 'clear configure crypto dynamic-map'
CSCsg00748	Yes	Clear window-scale sack option in non-syn packets instead of dropping it
CSCsg00914	Yes	OSPF neighbors don't form due to corrupted arp entry
CSCsg01099	Yes	ASA: Files on flash show incorrect date when looked using a Windows PC
CSCsg03411	Yes	WebVPN CIFS file delete when client try to rename
CSCsg04083	Yes	TG cookie is not properly set before redirection to CSD installation
CSCsg04324	Yes	VPN: high cpu usage with DHCP assigned IP addresses
CSCsg05160	Yes	name command doesn't accept 128.0.0.0 and 192.0.0.0 as a network

**Table 3**      **Resolved Caveats (continued)**

DTS Number	Software Version 7.2(2)	
CSCsg05422	Yes	WebVPN OWA2003:page not displayed properly when the address book is used
CSCsg05519	Yes	Port 443 is not available for IPSEC over TCP
CSCsg05587	Yes	access-lists not downloaded from aaa server in some cases
CSCsg07077	Yes	server-side DPD never sent out - connection dropped
CSCsg07425	Yes	Need to update OpenSSL to 0.9.7k
CSCsg07720	Yes	VPN Session DB: Potential stale point access in SESS_ACTIVE_REC
CSCsg08629	Yes	webvpn customization title..help for style and text reversed
CSCsg08725	Yes	Traceback: Thread Name: Dispatch Unit when timeout TCP keepalive message
CSCsg08799	Yes	Traceback in Dispatch Unit and assertion flow->vpn_handle == NULL
CSCsg08833	Yes	CSC may failover with syslog 323006 when 'dir disk1:/' executed
CSCsg09045	Yes	URL redirect not working
CSCsg10386	Yes	Webvpn not using custom text color for conection error dialog
CSCsg10605	Yes	ASA: TCP normalizer spoofs an ACK with all zeroes src MAC address
CSCsg10950	Yes	SIP registration using Camelot fails with inspect enabled
CSCsg11701	Yes	WebVPN: Java Security exception: SHA1 digest error-> Java applet
CSCsg11706	Yes	Unable to reconnect ssl/vpn when DPD keepalive expires
CSCsg11817	Yes	Disable Back button in denied access page
CSCsg11957	Yes	CSC cutting link speed by 60%, and download speeds are very slow.
CSCsg13717	Yes	snmpwalk on CISCO-IPSEC-FLOW-MONITOR-MIB returns OIDs out of order
CSCsg14238	Yes	Remove invalid commands from 5505 interface configuration
CSCsg14743	Yes	TCP connections through L2TP/IPSEC not routable with route...tunneled
CSCsg15224	Yes	WebVPN: Java applet fails to load
CSCsg16888	Yes	VPNLB: HTTP to HTTPS redirect does not work after re-enabling
CSCsg17150	Yes	Traceback in Thread Name: Dispatch Unit with Large Multicast Packets
CSCsg17709	Yes	Inspect information not displayed in packet-tracer output
CSCsg17712	Yes	AAA: Auth-Proxy session expired when using multiple connections
CSCsg18637	Yes	Unable to telnet to more than one IPv6 addr on interface
CSCsg20027	Yes	LDAP msRadiusFramedIPAddress doesn't assign IP in 7.2.x, OK in 7.1.x
CSCsg20301	Yes	Originate-Only/Answer-Only data being dropped
CSCsg20773	Yes	FIPS self test failure on new image upgrade
CSCsg21230	Yes	EASTERN is hardcoded as SMTP date timezone
CSCsg21242	Yes	ASA: Outbound ESP blocked by VPN-Filter when using Originate-Only
CSCsg21515	Yes	Traceback in Thread Name: Dispatch Unit when enabling Webvpn
CSCsg21527	Yes	FOVER: Traceback in Thread Name: fover_FSM_thread when booting up
CSCsg23113	Yes	WebVPN: java.lang.ClassFormatError: Truncated class file

Table 3 Resolved Caveats (continued)

DDTS Number	Software Version 7.2(2)	
	Yes	
CSCsg23233	Yes	VPN: 'show isa sa' may cause traceback in Thread Name: telnet/ci
CSCsg23270	Yes	Traceback in Thread Name: telnet/ci with 'show local   grep 1.1.1.1'
CSCsg23473	Yes	ASA 7.0 ssh process vulnerable to CRC32 compensation DOS attack
CSCsg24602	Yes	Malformed LDAP AD debug message
CSCsg25616	Yes	ASA put PATed src port in ICMP (type3, code4)
CSCsg27124	Yes	PIX 7.x does not allow RST pkt to pass from srv to client after failover
CSCsg27173	Yes	WebVPN: Linux/Mac Location Criteria fails when Home Page is Configured
CSCsg27896	Yes	SDI Cross-Realm authentication does not work
CSCsg29839	Yes	Reply/Forward does not work with Domino Web Access and WEBVPN
CSCsg29988	Yes	WebVPN: Java - java.lang.ClassNotFoundException: vminitializer.VMinitial
CSCsg30214	Yes	ISAKMP threshold value in primary and secondary not the same
CSCsg30885	Yes	Traceback: Thread Name: emweb/https and assert count <= payload failed
CSCsg31458	Yes	PKI: cannot enter url with more than one '?'
CSCsg31633	Yes	no ipsec-udp-port gives error type return through HTTPS
CSCsg31948	Yes	Trace back in Thread Name: snmp (Old pc 0x009fa5a0 ebp 0x0202cfcc)
CSCsg31956	Yes	VPN: Traceback in Thread Name: IKE Daemon
CSCsg32519	Yes	Traceback in Thread Name: RIP Router
CSCsg34819	Yes	Traceback in ssh thread after ssh timeout expires
CSCsg35215	Yes	Syslog server down causes ICMP flood if ICMP is denied at interface
CSCsg35721	Yes	Traceback in Thread Name: netfs_thread_init when auth with Kerberos
CSCsg35747	Yes	ERROR: Failed to find ldap context after clear config all entered
CSCsg39502	Yes	ASA 7.0.6 Traceback in tmatch compile
CSCsg39762	Yes	5510 show ver misleadingly indicates backplane FE as Not license
CSCsg40572	Yes	Traceback in Thread Name: IKE Daemon
CSCsg40894	Yes	ASA s/w crash due to memory mem_get_owner
CSCsg41593	Yes	If 2 DHCP servers for VPN clients, failover for DHCP not successful
CSCsg43075	Yes	VPN external group-policy timeout can cause various issues
CSCsg43077	Yes	L2TP_IPSEC - VPN filters in group-policy matches udp 1701 l2tp traffic
CSCsg43384	Yes	L2TP/IPSec - User filters configured using vpn-filter attr not applied
CSCsg43844	Yes	In failover pair standby ASA used memory is higher than in active
CSCsg44868	Yes	Same user in ACS and LOCAL database of aaa authorization causes error
CSCsg44875	Yes	TACACS+ accounting records do not include port number
CSCsg46536	Yes	alSslStatsActiveSessions from ALTIGA-SSL-STATS-MIB returns bad values
CSCsg48691	Yes	WebVPN: Java applets failing thru the rewriter
CSCsg48881	Yes	MCAST: improve direct connect multicast performance

**Table 3**      **Resolved Caveats (continued)**

DDTS Number	Software Version 7.2(2)	
CSCsg48997	Yes	RST-ACK sent by service resetoutbound uses wrong sequence number
CSCsg49205	Yes	Re-writing of SIP on-hold invite fails without a translation for 0.0.0.0
CSCsg49473	Yes	The url-server stats contain counter discrepancies
CSCsg49497	Yes	Do not trust Content-Type when forcing no-cache
CSCsg49825	Yes	Traceback at snp_fp_frag_v4 (Old pc 0x00218bc7 ebp 0x01853738)
CSCsg50453	Yes	LDAP Authent setup crashing ASA ldap_client:ldap_client_scope_get+177
CSCsg50757	Yes	Memory corruption of dispatch_ctxt_t in checkheaps
CSCsg51932	Yes	ISAKMP Phase 2 failure when NAT with NAT-T
CSCsg52108	Yes	The uauth timeout is not enforced via TACACS+
CSCsg52277	Yes	Certain SMTP messages cannot be sent through ASA with 'inspect esmtp' on
CSCsg52606	Yes	RSA signature forgery vulnerability in SSL code
CSCsg52749	Yes	AAA:realm string has a unique session-id suffixed to it
CSCsg53569	Yes	PIX-ASA: state-checking not compliant to H225 standards
CSCsg58837	Yes	ASA crash in Dispatch Unit during configuration replication
CSCsg60257	Yes	SIP inspect leading to unexpected Deny with no connection impacting BHCC
CSCsg62775	Yes	RAS seeing incorrect H.323 state transition RCF-> GRQ
CSCsg63037	Yes	Command rejected for single digit vlan number
CSCsg63297	Yes	CPU hog when update large object group in policy nat
CSCsg64280	Yes	FO: crypto ca cert map not replicated until after trustpoint match cmd
CSCsg64743	Yes	VPN: Ambiguity with isakmp keepalive command
CSCsg65794	Yes	WebVPN OWA 2003 Cannot save large files to disk with Save Target as...
CSCsg67322	Yes	WebVPN: DFS Failure to open folders on a W2K server
CSCsg68430	Yes	The clear arp <int> option is missing from 7.2 docs and help
CSCsg69270	Yes	717 - 72 byte blocks of mem leaked: _ber_memalloc_x+66 after vpn sys tst
CSCsg70099	Yes	FIPS: PRNG not used for async/no_pend rand requests
CSCsg76664	Yes	System out-of-block with 2700 active WebVPN sessions
CSCsg77799	Yes	ASA not forwarding multicast traffic with bidirectional RP

## Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN client Version 3.x 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.

---

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

© 2006 Cisco Systems, Inc.

All rights reserved.