



Cisco PIX Security Appliance Release Notes Version 7.0(6)

August 2006

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 4](#)
- [Caveats, page 6](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)

Introduction



Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.0.

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. This release introduces significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high-availability services, and management/monitoring.

For more information on all the new features, see [New Features, page 4](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

Additionally, the security appliance software supports ASDM. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

System Requirements

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



Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.0.

Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you need to upgrade the system 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 7.0.

Table 1 Flash Memory Requirements

Security Appliance Model	Flash Memory Required in Version 7.0
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 7.0(6) requires the following:

1. The minimum software version required before performing an upgrade to PIX Version 7.0 is PIX Version 6.2. If you are running a PIX release 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

3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. See the “[Upgrading to a New Software Release](#)” 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 7.0(6). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.0(6). 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 7.0(6) 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 7.0(6) 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 7.0(6) 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 7.0(6) 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.

Cisco Easy VPN Remote	Interoperability Comments
VPN 3000 Easy VPN remote v3.x/4x	Version 7.0(6) 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 7.0(6) 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.

Upgrading to a New Software Release

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

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

New Features

Version 7.0(6) includes several caveat resolutions

Important Notes

Important Notes in Release 7.0

This section lists important notes related to Version 7.0(6).

Common Criteria EAL4+

For information about common criteria EAL4+, see the *Installation and Configuration for Common Criteria EAL4 Evaluated Cisco Adaptive Security Appliance, Version 7.0(6)* document.

Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in release Version 7.0(6) for the PIX 535 are 50 tiers. The maximum number of VLANs supported are 150. For more information on the feature support for each platform license, see the “Platform Feature Licenses” section in the *Cisco Security Appliance Command Line Configuration Guide*.

IKE Delete-with-Reason

IKE system log messages for Delete-with-Reason do not contain the reason text unless the clients support this feature. Currently the VPN 3002 Version 4.7 and PIX 501 Version 6.3(4) hardware clients do not support this feature.

**Note**

The PIX 501 security appliance is not supported in software Version 7.0.

User Upgrade Guide

Before upgrading to Version 7.0(6), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*. This guide also 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

**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 7.0(6) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.0(6) 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/Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and leverage the powerful ACL feature set. ACL based configurations provide the following benefits:

- ACE insertion capability - System configuration and management is greatly simplified by the ACE insertion capability that allows users to add, delete or modify individual ACEs.
- Outbound ACLs and Time-based ACLs - Gives administrators improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling/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 7.0

The following features are not supported in Version 7.0(6) release:

- PPPoE
- L2TP over IPSec
- PPTP

MIB Supported

For information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.

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



Caution

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. Loading a software image from monitor mode, on a PIX security appliance that has a PIX Version 7.0 file system, results in unpredictable behavior 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 Version 7.0(6).

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

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

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

Open Caveats - Release 7.0(6)

Table 2 Open Caveats

ID Number	Software Release 7.0(6)	
	Corrected	Caveat Title
CSCeh98117	No	Tunnel-group passwords in cleartext when viewed with more
CSCsc36891	No	Higher CPU utilization for url filtering in recent releases.
CSCsc98412	No	PIX console accounting doesn't appear in ACS Logged-In User report
CSCsd69625	No	EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth
CSCsd99279	No	IKE: interop with Macintosh vpn client problem with transparent tunnel
CSCse06951	No	SNMP process stops working on PIX when the utilization is high
CSCse40999	No	SSH conns limited to 4 instead of 5
CSCse48144	No	cut-through proxy authentication misbehavior
CSCse67035	No	VPN filter deny outbound traffic if return is not permitted.
CSCse73922	No	Cmds executed in SSH / Telnet sessions continue after session disconnects
CSCse74721	No	complete IPSEC SA deleted upon receiving delete for old SPIs
CSCse86968	No	Standby unit sends accounting records for replicated DACL commands
CSCse88062	No	Standby pix crashes following replication
CSCse98719	No	Connection fails with the CA cert of 4096 bits fails with Error #72eh
CSCsf05931	No	AAA: group-lock does not handle tunnel-group names with spaces
CSCsf06947	No	Large FTP transfer over L2L tunnel between PIX and Netscreen breaking

Resolved Caveats - Release 7.0(6)

Table 3 Resolved Caveats

ID Number	Software Release 7.0(6)	
	Corrected	Caveat Title
CSCee00612	Yes	F1 floods network if Syslog is not available
CSCei47678	Yes	SNMP packet size standards in RFC3417 not fully supported.
CSCek40279	Yes	Increase in CPU utilization when OSPF is enabled
CSCsd03664	Yes	Reload w/ Thread Name:Session Manager w/ high volume of L2L VPN traffic
CSCsd47976	Yes	Traceback on nameif command on unused intf with 8000 static commands
CSCsd59936	Yes	Registering to the RP for PIM fails if fragmented in more then 12 packs
CSCsd82355	Yes	Malformed syslog packets may be generated.
CSCsd85345	Yes	Traceback may occur in fover_parse on 7.0.4
CSCsd89983	Yes	Access-list entered at line 1 is ineffective until access-group is rede
CSCsd90505	Yes	Traceback with assertion in file "vf_api.c", line 264

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(6)	
	Corrected	Caveat Title
CSCsd92296	Yes	DHCP relay failed after failover
CSCsd93207	Yes	Show failover indicates different uptimes on devices in failover pair
CSCsd93380	Yes	Packets for VPN-12l peer get dropped instead of encrypted
CSCsd94835	Yes	Proxy may queue too many packets when url filtering client is down
CSCsd94875	Yes	Traceback in VPN/IPSec CLI code when clear crypto ipsec sa counter
CSCsd95170	Yes	PIX 7.0(4)10: reporting incorrect context CPU usage
CSCsd97077	Yes	ASA/PIX - crash from SiVus SIP tester inside to outside w/ inspect/fixup
CSCsd97134	Yes	PIX/ASA ignores OSPF DBDs during adjacency building
CSCsd98071	Yes	conns fail after two successful authentications to virtual telnet IP
CSCsd98435	Yes	DHCPD pool does not allow to set ip add on interface once it is removed
CSCsd99200	Yes	Traceback in 7.1.2 caused by strict http inspection
CSCsd99709	Yes	PIX gets high CPU when type q to interrupt output of show conf
CSCse00173	Yes	PIX 515 fails to synch via serial based failover with VPN config
CSCse00303	Yes	Traceback during active/active config replication with 4 syslog servers
CSCse00756	Yes	URL filtering using Websense locks up downloads.
CSCse00996	Yes	TCP normalizer drop to-the-box traffic not conforming to RFC793 (MSS)
CSCse01293	Yes	Traceback in the arp_forward_thread
CSCse02354	Yes	PIX crash by dispatch unit
CSCse02703	Yes	Passwords in startup config may be changed without user intervention
CSCse02722	Yes	SSL Handshake failure with self signed cert
CSCse03299	Yes	VPN clients behind same PAT device using IPSEC/TCP & NAT-T fails IKE neg
CSCse04610	Yes	EzVPN: assert Thread Name: IKE Daemon (Old pc 0x00501f6d ebp 0x03401418)
CSCse06536	Yes	ASA 7.1: ASR not forwarding fragmented IP packets between contexts
CSCse07242	Yes	Crash in pix_flash_config_thread
CSCse08300	Yes	Show block shows in use and current values greater than max
CSCse08731	Yes	FIPS reload on failed ACL Checksum after clear config all
CSCse09591	Yes	ASA5540 crashes in IPsec message handler
CSCse10714	Yes	Shun behavior change in 7.x
CSCse11010	Yes	VPN:tback IKE Daemon (Old pc 0x001a9ee5 ebp 0x023d8dd8) 515 w/VAC +
CSCse11384	Yes	ASA crash in dhcp_daemon
CSCse14214	Yes	Malformed ICMPv6 NA packet causes PIX to crash and reload
CSCse14296	Yes	Trustpoint not found if ASA not enrolled with the trustpoint
CSCse14402	Yes	EzVPN:5505 Phase 2 SAs fail to establish causing tunnel to drop
CSCse15977	Yes	ASA/PIX reboot if 2 admin sessions are working on the same capture
CSCse19020	Yes	PPTP Pass-through not working due to inspection

Table 3 Resolved Caveats (continued)

ID Number	Software Release 7.0(6)	
	Corrected	Caveat Title
CSCse20501	Yes	Passive FTP to Multinet server fails
CSCse22150	Yes	Traceback during config synch and console at More
CSCse22853	Yes	Active unit crash in accept/http when disabling DHCP relay
CSCse23164	Yes	PIX crash
CSCse23554	Yes	Memory leak within event_smtpmgr:es_SmtpSndMSG function
CSCse23751	Yes	Nested crash dump doesn't stop
CSCse27184	Yes	basic attribute is not checked in all mode config attributes...
CSCse29840	Yes	AdmissionConfirm received without an AdmissionRequest, ACF dropped
CSCse30049	Yes	SSH conns to the box not removed after a Failover
CSCse30061	Yes	PIX/ASA VPN decompress error when decrypting packet with IP compression
CSCse32309	Yes	PIX/ASA: Timeout of secondary flow causes crash in thread Checkheaps
CSCse33143	Yes	Dynamic ACL created under with command access-list <name> d
CSCse34179	Yes	MFWR: traceback in 'clear cfg all' during a performance test.
CSCse35566	Yes	ASA 7.0.5 Traceback in Dispatch unit on clear xlate
CSCse37787	Yes	ASA: Standby crashed after becoming Active with VPN connections
CSCse38039	Yes	ASA drops small ICMP length packets with IPsec/UDP
CSCse40332	Yes	ASA multiple mode rollback of config failed for admin and other VC
CSCse40583	Yes	PIX 7 should not reply to the IP network address
CSCse40671	Yes	RTSP w/PAT, PIX set client_ports to NULL
CSCse45308	Yes	Static nailed rule does not match conn destined for that address
CSCse45450	Yes	PIX/ASA Crash in aaa thread
CSCse45694	Yes	Standby: Traceback in Thread Name: IKE Daemon with dACL
CSCse46292	Yes	Traceback in obj-f1/bld_pkt:_AddOctetString+17 in snmp thread
CSCse48193	Yes	ASA vulnerable to cross-site scripting when using WebVPN
CSCse50716	Yes	PIX 7.0.5.1 URL Filtering Traceback Thread Name: Dispatch Unit
CSCse50804	Yes	OSPF stuck in EXCHANGE in certain asymmetric routing scenarios
CSCse53294	Yes	ASA Crash- when an SSH connection is made and "conf t" is issued
CSCse53344	Yes	IKE: vpn-tunnel-protocol attribute is not checked if the value is 0
CSCse54749	Yes	210007 LU allocate xlate failed syslog generated by overlapping nat cfg
CSCse58985	Yes	sh uauth shows 32 in-progress and prevents SSH to ASA using LOCAL db
CSCse61315	Yes	SSMIO-4GE SFP interfaces G1/1 - G1/3 don't operate
CSCse62914	Yes	Standby device Traceback in Thread Name: tcp_thread
CSCse66235	Yes	Memory exhausts with logging flash-bufferwrap and high syslog level
CSCse70993	Yes	Traceback observed in Thread Name: ci/console
CSCse75523	Yes	Received ARP request collision when issuing write standby

Table 3 Resolved Caveats (continued)

Software Release 7.0(6)		
ID Number	Corrected	Caveat Title
CSCse76115	Yes	Cascade delimiter not inserted with correct priority for dynamic crypto.
CSCse77122	Yes	FTP-data connection not replicated back to primary after failover
CSCse77680	Yes	P2 in progress test broken - could cause unexpected rekey.
CSCse77855	Yes	buffer leak upon IPSEC spoofing.
CSCse78065	Yes	# sign in config not replicated to Standby unit
CSCse78299	Yes	Primary/Secondary units become Active state when failover link failed
CSCse80001	Yes	Traceback in IKE daemon while trying to post event (syslog)
CSCse81384	Yes	traffic delay when dynamic arp entry times out
CSCse81633	Yes	ASA 4GE-SSM Gig ports silently drop IGMP joins
CSCse83905	Yes	dhcprelay stops working if FW interface ip address is modified
CSCse88873	Yes	IPV6: TCP SYN-ACK with layer 2 padding dropped
CSCse94241	Yes	Reload with Thread Name:vpn1b_thread when taking over as failover active
CSCse96289	Yes	Traceback with Thread Name: Dispatch Unit
CSCsf00368	Yes	Crashinfo file may incorrectly show 0% free memory

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/ps2308/tsd_products_support_series_home.html

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CDC account you can visit the following websites for assistance:

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

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

Obtaining Documentation and Submitting a Service Request

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

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

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


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

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)

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.

© 2006 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.