



Cisco PIX Security Appliance Release Notes Version 7.1(2)

March 2006

Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 5](#)
- [Caveats, page 7](#)
- [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 7.1.

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

Copyright © 2005 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 7.1.

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 7.1.

Table 1 Flash Memory Requirements

Security Appliance Model	Flash Memory Required in Version 7.1
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 7.1(2) requires the following:

1. The minimum software version required before performing an upgrade to PIX Version 7.1 is PIX Version 7.0. 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/go/license/index.html>

3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. For new installation requirements, see 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 7.1(2). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.1(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 7.1(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 7.1(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 7.1(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 7.1(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.

Cisco Easy VPN Remote	Interoperability Comments
VPN 3000 Easy VPN remote v3.x/4x	Version 7.1(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 7.1(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.

Upgrading to a New Software Release

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

If you want to upgrade or downgrade from Version 7.0.(x) to 7.1(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.

To upgrade from Version 7.0.(x) to 7.1(x), you must perform the following steps:

-
- Step 1** Load the new 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 start using the Version 7.1(x) image.
 - Step 3** Copy new ASDM Version 5.1(x) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
-

To downgrade from Version 7.1(x) to 7.0.(x), you must perform the following steps:

-
- Step 1** Load the earlier Version 7.0(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 7.0(x) image.
 - Step 3** Copy the ASDM Version 5.0(x) image from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
-

New Features

Version 7.1(2) includes several caveat resolutions.

Important Notes

Important Notes in Release 7.1

This section lists important notes related to Version 7.1(2).

Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in release 7.1(2) 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 syslogs 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 7.1.

User Upgrade Guide

Before upgrading to Version 7.1(2), 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 7.1(2) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.1(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/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 7.1

The following features are not supported in Version 7.1(2) 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 the 7.1(2) release.

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 7.1(2)

Table 2 Open Caveats

ID Number	Software Release 7.1(2)	
	Corrected	Caveat Title
CSCsc15434	No	Assertion violation w/icmp traffic and icmp inspection
CSCsd21821	No	traceback eip:sessmgrmain:_CheckSubRecConnectTime+23 after appl. act-key
CSCsd36030	No	in multiple policy-maps, packets should match the first map,not the last
CSCsd36281	No	traceback after administratively discon L2L Tun. w/ filters applied
CSCsd36359	No	Tback eip: _vpnfo_fsm_get_ha_state+514 on FO UUT after 32 sec
CSCsd36388	No	T-back on sec FO eip:_dllobj_remove+12 rapidly establishing ipsec tun
CSCsd36400	No	T-back: eip _shash_remove+158 on secondary (standby) after vpn sys test
CSCsd41442	No	Checkheap asserts due to a free buffer validation failure
CSCsd45406	No	Traceback in 'accept/http' while configuring object-group with ASDM
CSCsd46111	No	Traceback when using sh xlate via telnet over VPN tunnel
CSCsd46685	No	Traceback eip::_snp_sp_action_construct_ip_key+1013 after ipsec rule cfg
CSCsd46922	No	High CPU usage when configuring/compiling ACL's
CSCsd52578	No	Traceback in thread: snp_timer_thread
CSCsd53321	No	sysopt connection timewait causes SSH sessions to timeout prematurely
CSCsd56547	No	Traceback with No thread name after upgrading

Table 2 Open Caveats (continued)

Software Release 7.1(2)		
ID Number	Corrected	Caveat Title
CSCsd60662	No	Traceback occurs in snp_timer_thread, but no ACL edits
CSCsd62875	No	Traceback in tmatch compile thread
CSCsd64698	No	memory leakage in IKE
CSCsd64912	No	url-server: tcp connections fail when tcp stack users are exhausted
CSCsd64920	No	url-server: url lookup requests are not retried when using tcp
CSCsd65209	No	url-block block: http response buffering feature does not work
CSCsd65215	No	Capture access-list shows only 1 hit count for outbound traffic

Resolved Caveats - Release 7.1(2)

Table 3 Resolved Caveats

Software Release 7.1(2)		
ID Number	Corrected	Caveat Title
CSCsd22910	Yes	users with passwords longer than 11 chars can no longer authenticate
CSCek27919	Yes	PIX reload with Thread Name: tcp_slow
CSCsc12094	Yes	AAA fallback authentication does not work with reactivation-mode timed
CSCsc90944	Yes	Malformed https proxy authentication page w/ linebreak
CSCsc51939	Yes	Performance throughput problems when http inspect enabled
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCsc44591	Yes	Traceback in Thread Name: ARP Thread in multicontext mode
CSCsd03391	Yes	TCP Intercept doesn't negate CPU impact when SYN flood from adjacent net
CSCsc91450	Yes	FTP control channel timing out although data channel is active.
CSCsc16507	Yes	Cannot remove url-server despite having removed url-block cmd
CSCsc33385	Yes	GTP - pdp context creation failed - GSN tunnel limit exceeded
CSCei43588	Yes	traceback when trying to match a packet to acl with deny
CSCsc97999	Yes	Syslog Message ID 313003 is used incorrectly
CSCsd16751	Yes	GTP: wrong service-policy used when connection is re-used
CSCsc73942	Yes	TCP RST is dropped when there is outstanding data that is not acked
CSCsd04700	Yes	match port option for setting connection time-outs does not work
CSCek26572	Yes	tftp fixup does not allow error message from client
CSCsc99263	Yes	GTPv1: Subsequent Create Req to modify PDP context IEs are not processed
CSCsd25537	Yes	Failover unit traceback in Thread Name: fover_FSM_thread
CSCsd28581	Yes	Failover: Secondary traceback in Thread Name: IKE Daemon
CSCek21837	Yes	PDM with Command Authorization requires the write command for Read-Only

Table 3 *Resolved Caveats (continued)*

ID Number	Software Release 7.1(2)	
	Corrected	Caveat Title
CSCsc81668	Yes	/config"https://<ip>/config does not have the same privilege level as 'write'
CSCsd15475	Yes	Secondary unit doesn't get full config file after SSH reload on Primary
CSCsd11179	Yes	SNMP polling of resource MIBS may cause packet loss
CSCsd17718	Yes	IGMP forward interface command fails to sync to the standby unit
CSCsc16041	Yes	'clear local host' results in memory leak
CSCsc64621	Yes	VPN syslog 402123 should include a meaningful error message
CSCsc36332	Yes	Traceback: Thread Name:ci/console w/sh run all and priority class config
CSCsc99364	Yes	SSL Certs from Verisign Managed PKI do not install
CSCsd17763	Yes	PIX should not respond to TCP segment w/ RST+ACK and bad ACK number
CSCsc81565	Yes	Idle conn timeout reset when packet dropped by TCP normalizer
CSCsc78900	Yes	Reload with Thread Name: Dispatch Unit at tcp_check_packet
CSCsc98339	Yes	Standby unit may reload if active unit powered off
CSCsc86217	Yes	Voice Proxy Function does not preserve DSCP bits.
CSCek21846	Yes	SIP: xlate timeout not updated by Expire value in Register message
CSCsc46976	Yes	SIP: traceback when failed to pre-allocate early rtp
CSCsd34070	Yes	H.245 inspect skipped if GK RCS and wrong H.225 callSignalAddress for GK
CSCsc78010	Yes	Traceback in Thread Name: Checkheaps
CSCsd07783	Yes	Transient NAT-T packets silently dropped if NAT-T is enabled
CSCsd08060	Yes	Memory corruption caused by vpn session DB when events are out of sync
CSCsd17879	Yes	Deny rules in crypto acl blocks inbound tcp/udp after tunnel formed
CSCsc06239	Yes	French language VPN client xauth prompt not translated into French
CSCsd13334	Yes	Memory Leaking tunnel-group authorization-dn-attributes
CSCsc93061	Yes	Traceback after activation of vpn-filter

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/partner/products/sw/secursw/ps2120/tsd_products_support_series_home.html
- http://www.cisco.com/en/US/partner/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/partner/support/support/tsd_most_requested_tools.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 “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

© 2006 Cisco Systems, Inc.
All rights reserved.