

Cisco PIX Firewall (Version 4.3)

The information contained in this product bulletin applies to all Cisco PIX™ Firewall hardware models running software version 4.3 or later. Version 4.3 requires at least 16 MB (an optional 128 MB upgrade is available). Version 4.3 supports up to four Ethernet interfaces. Three Token Ring interfaces have been tested with the PIX Firewall.

Version 4.3.1 has also received TTAP certification, making the Cisco PIX Firewall the first and only firewall solution certified to be in full compliance with the Common Criteria and the US Government Protection Profile, established and maintained by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).

This Product Bulletin contains the following information:

New and Changed Information

TTAP Certification for Cisco PIX Firewall version 4.3.1

New Features

PIX Firewall TCP Syslog Server

Real-Time Clock

Telnet Console Access from All Internal Interfaces

Enable AAA Authentication Console

AAA Port Range Specification

Disabling and Re-Enabling of Syslog Messages

PIX Firewall SNMP Object ID

User-Based Timeout

Virtual Telnet Logout

Links to Other Documents

New and Changed Information

TTAP Certification for Cisco PIX Firewall version 4.3.1

Cisco Systems is pleased to announce the Common Criteria certification of the PIX 520 Firewall. The Common Criteria is an international standard, recognized in the United Kingdom, Canada, Germany, France, Netherlands and the United States that details functional and assurance requirements to test the IT security of a product or system. The PIX Firewall is the first and only firewall to be tested and certified against a Common Criteria based Protection Profile created by the National Institute of Standards and Technology and the National Security Agency.

The Cisco PIX Firewall, v.4.3.1, is the only firewall in the world to be certified of being compliant with the U.S. Government Protection Profile.

Details on Cisco's web site about TTAP certification of the PIX Firewall can be found at:

<http://www.cisco.com/warp/customer/779/gov/federal/TTAP/>

Additional information can be found on NSA's Common Criteria web site at:

http://www.radium.ncsc.mil/tpep/epl/cc_st.html

New Features

PIX Firewall Syslog Server

The PIX Firewall Syslog Server (PFSS) runs on a Windows NT system and receives syslog messages from up to 10 PIX Firewalls.

Note: The Windows NT filesystem where you install PFSS must be an NTFS partition and not FAT.

Note: When you install PFSS on the Windows NT system, write down the values you supply for the disk empty timer and the disk full timer. Once PFSS is installed, the only way you can view this information again is by examining the Windows NT Registry with the regedit command and searching for disk_empty_watch. Also, if you need to view the information in the Registry, do not change it in the Registry. The information can only be changed from the Start>Settings>Control Panel>Services setting. You can view the other parameter values in the pfss.log file that accompanies the daily log files.

Note 1: PFSS and the PIX Firewall Manager cannot be used together even if installed on separate Windows NT systems.

Note 2: If the Windows NT system on which PFSS is installed reaches the percentage of disk full value you set when installing PFSS, the Windows NT system causes the PIX Firewall to stop all of its connections until the log files are removed from the system.

Refer to the logging command page in the Configuration Guide for the PIX Firewall Version 4.3, Chapter 5, "Command Reference" for additional important information about configuring the PIX Firewall for use with PFSS. This page is located at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43cfg/pix43cmd.htm#xtocid2172525

Installation and configuration instructions for the PFSS on the Windows NT system are described in the Quick Installation Guide for the PIX Firewall Version 4.3, located at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43qig.htm

Real-Time Clock

The clock set command allows you to set the PIX Firewall's internal clock. The internal clock is used to time stamp syslog messages. You can use the show clock command to display the current time. *Note:* The clock set command only works until December 31, 2097.


Telnet Console Access from All Internal Interfaces

You can now access the PIX Firewall console via Telnet from all internal interfaces.

Enable AAA Authentication Console

You can now set the enable option on the aaa authentication console command. This command requires that access to the PIX Firewall console be authenticated from a TACACS+ or RADIUS server. After authentication is successful, all changes to the configuration from the serial console are logged to the syslog servers at syslog level 5. Changes made from Telnet console sessions are not logged.

If the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the PIX username and the enable password.



AAA Port Range Specification

You can now set port ranges for the TCP and UDP protocols with the aaa authorization command.

Disabling and Re-Enabling of Syslog Messages

You can now disable specific syslog messages with the no logging message syslog_id command, and re-enable specific syslog messages with the logging message syslog_id command. You can display all disabled messages with the show logging disabled command, and re-enable all disabled messages with the clear logging disabled command.

PIX Firewall SNMP Object ID

An SNMP object ID (OID) for PIX Firewall now displays in SNMP event traps sent from the PIX Firewall. OID 1.3.6.1.4.1.9.1.227 was assigned as the PIX Firewall system object ID.

User-Based Timeout

You can use the show uauth command to display CiscoSecure version 2.1 or later idletime and timeout values that provide user-based, rather than global, authentication timeouts.

The Cisco Secure user-based timer durations override the duration set with the timeout uauth command.

Virtual Telnet Logout

The virtual telnet command lets you log in to the virtual authentication server on first access and log out on second access to the specified IP address.

New Commands

clock set – allows you to set the PIX Firewall's internal clock. The current time is used for time stamped syslog messages, which you can set with the logging timestamp command.

show clock – displays the current time.

Links to Other Documents

Release Notes for the PIX Firewall Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pixrn43.htm

Release Notes for the PIX Firewall Manager Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pfmrn432.htm

Configuration Guide for the PIX Firewall Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43cfg/index.htm

Quick Installation Guide for the PIX Firewall Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pix43qig.htm

System Log Messages for the PIX Firewall Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/syslog/index.htm

Regulatory Compliance and Safety Information for the PIX Firewall Version 4.3

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/pixrcs43.htm

**Corporate Headquarters**

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

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France

<http://www-europe.cisco.com>

Tel: 33 1 69 18 61 00

Fax: 33 1 69 28 83 26

Americas**Headquarters**

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

<http://www.cisco.com>

Tel: 408 526-7660

Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan

<http://www.cisco.com>

Tel: 81 3 5219 6250

Fax: 81 3 5219 6001

**Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the
Cisco Connection Online Web site at <http://www.cisco.com/offices>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 1999 Cisco Systems, Inc. All rights reserved. Printed in the USA. PIX is a trademark; Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9904 R)