



Text Part Number: 78-6804-02

Release Notes for the PIX Firewall Version 4.4(2)

October 1999

This document describes only the changes for the 4.4(2) version of the PIX Firewall software. For information on 4.4(1) features, installation notes, limitations and restrictions, usage notes, and caveats, refer to the version 4.4(1) release notes at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn44.htm

Contents

- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Related Documentation
- Cisco Connection Online
- Documentation CD-ROM

System Requirements

The information contained in these release notes applies to all PIX Firewall hardware models running software version 4.4 or later.

Version 4.4 requires at least 16 MB of RAM (optional memory upgrades are available) and at least 2 MB of Flash memory. You can verify both of these requirements with the **show version** command.

Version 4.4 supports one of the following interface combinations:

- One 4-port Ethernet card and one or two Ethernet or Token Ring cards, which can be intermixed such as a 4-port Ethernet card and two Token Ring cards
- Up to four single-port Ethernet or Token Ring cards, either separate or intermixed
- Two FDDI cards

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Note PIX Firewall Manager version 4.3(2)c and later works with version 4.4 but does not support the new features in version 4.4. You can view the PIX Firewall Manager version 4.3(2)c release notes online at the following site:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/pfm432c.htm

New and Changed Information

Version 4.4(2) contains bug fixes and minor enhancements to the PIX Firewall command set as described in the sections that follow.

New Commands

The **sysopt noproxyarp if_name** command disables sending ARP requests on an interface. This command was available in version 4.4(1), but was not documented.

Changed Commands

Table 1 lists command changes in version 4.4(2).

Command	Change
aaa	RADIUS authentication now permits three retries to let a user enter their login information correctly.
clock	Dates are now checked to see if they are correct for a leap year or a non-leap year. For example, February 29 is now accepted as correct in a leap year, but not in a year that is not a leap year.
filter activex	Checks are now made for “< OBJECT ID” instead of “< OBJECT” as one of the possible permutations of an ActiveX “<object>” HTML command in the data stream.
outbound	Up to 10,000 outbound command entries are now permitted in a configuration.
route	Up to 1,024 route command statements are now permitted in a configuration.
virtual http	The maximum length of a host name is now 127 characters.

Removed Components

No new components were removed in version 4.4(2).

Installation Notes

No new installation notes were added in version 4.4(2).

Limitations and Restrictions

No new limitations and restrictions were added in version 4.4(2).

Important Notes

The following usage notes apply to version 4.4(2):

alias Command

The translation of the inbound source address occurs before inbound filtering takes place, so a **conduit** command statement must refer to the DNAT IP address rather than the real foreign IP address.

For example, an **alias** command statement should appear in the configuration as follows:

```
alias (inside) 209.165.201.6 192.168.100.6 255.255.255.255
```

The correct **conduit** command statement for this command is as follows:

```
conduit permit tcp host global_ip_address eq smtp host 209.165.201.6
```

auth-prompt Command

The prompt string that you specify with the **auth-prompt accept** command appears twice when a user is authenticated. For example:

```
auth-prompt prompt Enter your user name and password:
auth-prompt accept Success!
```

When a user logs on, the following appears:

```
Enter your user name and password:
User Name: username
Password: *****
Success!
Success!
```

The repeating prompt text will be fixed in the next release.

Failover

The **failover timeout** command does not work in this release.

show conn Command

The **show conn protocol udp** command lists the DNS destination port as 1 instead of 53. For the UDP DNS service, the port field is overloaded with the ID of the request; the **show conn** command incorrectly returns the request ID instead of the port number.

Syslog

- Syslog message %PIX-2-106002 is incorrectly listed in the *System Log Messages for the PIX Firewall Version 4.4* guide as “TCP Connection denied by outbound list.” The actual text of the message as it appears in a syslog message is “6 Connection denied by outbound list” when the message refers to TCP and “17 Connection denied by outbound list” when the message refers to UDP. All other information in the guide for this syslog message is correct.
- Syslog message %PIX-5-304001 is incorrectly listed as %PIX-6-304001 in the *System Log Messages for the PIX Firewall Version 4.4* guide. The “-5-” in the message number indicates that the message is a level 5 notification message. The incorrect number “-6-” indicated that the message was a level 6 informational message.

For more information, refer to the **logging** command page in Chapter 5, “Command Reference,” in the *Configuration Guide for the PIX Firewall Version 4.4*.

TFTP

If you have an existing PIX Firewall configuration on a TFTP server and create a shorter configuration with the same filename to the TFTP server, some of the original configuration will remain after the first “:end” mark. This does not affect the PIX Firewall because the **configure net** command stops reading when it reaches the first “:end” mark. However, this may cause confusion when you view the configuration and see the extra text at the end of the configuration.

Caveats

This section lists resolved caveats.

Open Caveats

No new open caveats were introduced in version 4.4(2). All open caveats in version 4.4(1) still apply to version 4.4(2).

Resolved Caveats

Table 2 lists resolved DDTs bug reports. All resolved caveats in version 4.4(1) apply to version 4.4(2).

Table 2 **Resolved Caveats**

DDTS Number	Description
CSCdp09462	A zero length TCP option seldom causes PIX Firewall to crash. The previous workaround was to include the sysopt connection tcpmss 0 command statement in your configuration. This is no longer necessary.
CSCdp08368	Up to 10,000 outbound command entries are now permitted in a configuration.
CSCdp08239	Outbound pings are no longer blocked when the configuration contains an explicit permit using the except option in an outbound command statement list.
CSCdp07819	Users can now log into hotmail.com when WebSENSE filtering is enabled. The fix increased the size of the internal buffer that handles the HTTP GET requests when WebSENSE is enabled. Previously, after entering the username and password prompts, the message “document contains no data” would appear at the browser. In addition, this would work incorrectly with Netscape Navigator version 4.x and Internet Explorer version 4.x, but would work correctly with Netscape Navigator version 3.x.
CSCdp00072	The virtual http command now works correctly even if the host name is longer than 24 characters. Previously, after the user was authenticated, the browser was redirected to an incomplete URL. The maximum size of a host name is now 127 characters.
CSCdm94131	The %PIX-2-106001 syslog message now lists flag information. Previously, the message ended with “flags,” but no value followed it.
CSCdm86086	The filter activex command now checks for “< OBJECT ID” instead of “< OBJECT” as one of the possible permutations of an ActiveX “<object>” HTML command in the data stream. Previously, code text that contained a less than symbol and the word “object” in a variable name, was commented out.
CSCdm82481	Applications can now have multiple Sun RPC calls. Previously, only the first call was allowed. This fix enables multiple sessions per RPC service advertised by the RPC portmapper.
CSCdm71816	SNMP traps are now sent to all specified hosts. Previously, if more than two SNMP hosts (NMS) were specified, SNMP traps were only sent to the first and the second SNMP hosts listed in the output of the show snmp-server command. The rest of the SNMP hosts would not receive traps from the PIX Firewall. The second SNMP host occasionally received duplicate traps.

Table 2 Resolved Caveats (Continued)

DDTS Number	Description
CSCdm71086	<p>The PIX Firewall now checks the global address you specify in the static command statement to be sure it is not in use by another static command statement. Previously, you could enter command statements such as the following that incorrectly had the same global address mapped to two different hosts.</p> <pre>static (inside,outside) 209.165.201.2 192.168.1.2 static (inside,outside) 209.165.201.2 192.168.1.42</pre>
CSCdm70489	<p>Return ports on inbound TFTP are no longer denied by outbound command statement lists. Previously, if you allowed inbound TFTP, and if you had an outbound command statement that denied access to the high ports (1024-65535), the TFTP request failed unless the outbound lists were removed or an exception created to allow UDP high ports from the internal server to the external client.</p>
CSCdm69799	<p>The SNMP MIB-II ifEntry.ifAdminStatus object no longer returns only zero. In version 4.4(2), this object now only returns 1, which indicates that the interface is not shut down. In PIX Firewall version 5.1, the object will return 1 if the interface is accessible and 2 if the interface has been administratively shut down using the version 5.1 shutdown option to the interface command.</p>
CSCdm58225	<p>PIX Firewall no longer reboots when there are more than 256 route command statements in a configuration. The maximum is now 1024 command statements.</p>
CSCdm57189	<p>The clock command now checks that a date is correct for a leap year or for a year that is not a leap year.</p>
CSCdm54961	<p>In the show uauth command display, the IP address of a previously authenticated user is no longer replaced by the IP address of a newly authenticated user using the virtual telnet command.</p>
CSCdm53662	<p>The sysopt noproxyarp if_name command disables sending ARP requests on an interface.</p>
CSCdm49291	<p>PIX Firewall now checks the syntax of a static command statement. Also, “mask” cannot be used as a shortened form of “netmask.”</p>
CSCdm46934	<p>RADIUS authentication now permits three retries to let a user enter their login information correctly.</p>
CSCdm39607	<p>PIX Firewall now reports the correct number of outbound packets in the MIB-II ifOutUcastPkts object.</p>
CSCdm02779	<p>PIX Firewall no longer sends the message “Server: PIX Firewall HTTP version 1.1” when a Telnet connection is established. This message was removed to keep intruders from knowing what type of firewall is in use.</p>

Related Documentation

Use this document in conjunction with the version 4.4 PIX Firewall documentation set. You can view these documents at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/index.htm

Use also with the *Release Notes for the PIX Firewall Manager Version 4.3(2)c*, which applies to versions 4.3, 4.4, and 5.0. You can view this document at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/pfm432c.htm

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems’ primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco’s customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

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

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Service Node, VisionWay, VlanDirector, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9910R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.