



Text Part Number: 78-6804-03

Release Notes for the PIX Firewall Version 4.4(3)

January 2000

This document describes only the changes for version 4.4(3) of the PIX Firewall software.

For information on version 4.4(1) and version 4.4(2) features, installation notes, limitations and restrictions, usage notes, and caveats, refer to the version 4.4(1) and version 4.4(2) release notes at the following sites:

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

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn442.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. Use the **show version** command to verify how much Flash and RAM memory is in your PIX Firewall.

Corporate Headquarters

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

Copyright © 2000
Cisco Systems, Inc.
All rights reserved.

The maximum configuration size is 350 KB.

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

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_v44/pfm432c.htm

Cisco Security Manager Interoperability

Cisco Security Manager (CSM), version 1.1, provides policy-based management support for PIX Firewall units running version 4.2(4), 4.2(5), 4.4(1), 4.4(2), and 4.4(3) software images. Because the command set for version 4.4(3) differs from versions 4.4(2) or 4.4(1) in CSM, you must select version **4.4.3** in the Version box within the General panel for all selected PIX Firewall units.

Refer to Appendix A, “Using Unsupported PIX Firewall Commands,” in the *Cisco Security Manager Tutorial* for information about the PIX Firewall commands the CSM supports. You can view the CCO version of the *Cisco Security Manager Tutorial* at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/ismg/security/tutorial/index.htm>

New and Changed Information

Version 4.4(3) contains bug fixes and enhancements to the PIX Firewall command set as described in the sections that follow. No new commands were added or existing commands removed.

New Feature

The 16 MB Flash memory card is now supported; however, the maximum configuration size remains 350 KB.

Changed Commands

The following commands were changed in version 4.4(3):

- no failover Command
- show interface Command

no failover Command

When a failover cable connects two PIX Firewall units, the **no failover** command now disables failover until you enter the **failover** command to explicitly enable failover. Previously, when the failover cable connected two PIX Firewall units and you entered the **no failover** command, failover would automatically re-enable after 15 seconds.

If you reboot the PIX Firewall without entering the **write memory** command and the failover cable is connected, failover mode automatically enables.

show interface Command

The **show interface** command has been enhanced to include eight new status counters. The new counters are only valid for either 10 Mbps or 100 Mbps Ethernet interfaces. The following example shows the new output:

```
show interface
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 00aa.0000.003b
  IP address 209.165.201.7, subnet mask 255.255.255.224
  MTU 1500 bytes, BW 100000 Kbit half duplex
    1184342 packets input, 1222298001 bytes, 0 no buffer
    Received 26 broadcasts, 27 runts, 0 giants
    4 input errors, 0 CRC, 4 frame, 0 overrun, 0 ignored, 0 abort
    1310091 packets output, 547097270 bytes, 0 underruns
    0 output errors, 28075 collisions, 0 interface resets
    0 babbles, 0 late collisions, 117573 deferred
    0 lost carrier, 0 no carrier
```

The counters in the last three lines are as follows:

- output errors—(maximum collisions). The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
- collisions—(single and multiple collisions). The number of messages retransmitted due to an Ethernet collision. This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
- interface resets—the number of times an interface has been reset. If an interface is unable to transmit for three seconds, PIX Firewall resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
- babbles—unused. (“babble” means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
- late collisions—the number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait.

If you get a late collision, a device is jumping in and trying to send on the Ethernet while the PIX Firewall is partly finished sending the packet. The PIX Firewall does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks or Ethernet networks running beyond the specification.

- deferred—the number of frames deferred before transmission because of activity on the link.
- lost carrier—the number of times the carrier signal was lost during transmission.
- no carrier—unused.

Installation Notes

No new installation notes were added in version 4.4(3).

Limitations and Restrictions

No new limitations and restrictions were added in version 4.4(3).

Important Notes

The following usage notes apply to version 4.4(3):

- `aaa-server` Command timeout Option
- AAA Timeout Message for RADIUS and TACACS+
- DNS Root Name Server Access
- SNMP Enhancements

aaa-server Command timeout Option

The `aaa-server` command page in Chapter 5, “Command Reference” in the *Configuration Guide for the PIX Firewall Version 4.4* incorrectly lists the `timeout` option to the `aaa-server` command as an idle timer. This option is actually a retransmit timer that lets you specify the interval in seconds that the PIX Firewall attempts to retransmit data before accessing the next specified AAA server. PIX Firewall attempts four times to retransmit the data before accessing the next server.

For example, if the timeout value is 10 seconds, PIX Firewall initially retransmits for 10 seconds. If no acknowledgment is received, PIX Firewall tries three more 10-second intervals before selecting the next AAA server.

AAA Timeout Message for RADIUS and TACACS+

The PIX Firewall now displays the same timeout message for both RADIUS and TACACS+. The message “aaa server host machine not responding” displays when either of the following occurs:

- The AAA server system is down.
- The AAA server system is up, but the service is not running.

Previously, TACACS+ differentiated between these two states and provided two different timeout messages, while RADIUS did not differentiate between the two states and provided one timeout message.

DNS Root Name Server Access

A DNS server on a higher level security interface needing to get updates from a root name server on the outside interface cannot use PAT (Port Address Translation). Instead, a `static` command statement must be added to map the DNS server to a global address on the outside interface.

For example, PAT is enabled with these commands:

```
nat (inside) 1 192.168.1.0 255.255.255.0
global (inside) 1 209.165.202.128 netmask 255.255.255.224
```

However, a DNS server on the inside at IP address 192.168.1.5 cannot correctly reach the root name server on the outside at IP address 209.165.202.130.

To ensure that the inside DNS server can access the root name server, insert the following **static** command statement:

```
static (inside,outside) 209.165.202.129 192.168.1.5
```

The global address 209.165.202.129 provides a translated address for the inside server at IP address 192.168.1.5.

SNMP Enhancements

The following SNMP MIB-II objects now work correctly:

- ifInOctets—now correctly returns the total number of octets received on an interface.
- ifOutUcastPkts—now correctly returns the outbound packet count.

Syslog Messages

The *System Log Messages Guide for the PIX Firewall Version 4.4* has been upgraded to correct inaccuracies and to improve its usefulness. This guide is available online at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pix44em/index.htm

Caveats

This section lists open and resolved caveats.

Open Caveats

No new open caveats were introduced in version 4.4(3). All open caveats in version 4.4(1) and version 4.4(2) still apply to version 4.4(3).

Resolved Caveats

Table 1 lists caveats resolved by the PIX Firewall Engineering team in version 4.4(3). All resolved caveats in version 4.4(1) and version 4.4(2) apply to version 4.4(3).

Table 1 Resolved Caveats

| DDTS Number | Description |
|-------------|--|
| CSCdp32325 | During heavy traffic, the outside Ethernet interface no longer intermittently stops transmitting traffic. If an interface is unable to transmit for three seconds, PIX Firewall resets the interface to restart transmission. During the reset, the connection state is maintained. This problem only affects the PIX 515. |
| CSCdp54807 | The SNMP MIB-II “ifInOctets” object now works correctly. See “SNMP Enhancements” for more information. |
| CSCdp51282 | PIX Firewall now correctly displays the prompt you set with the auth-prompt accept command when a user authenticates using RADIUS. |
| CSCdp48907 | PIX Firewall no longer crashes under heavy UDP traffic. |
| CSCdp44875 | PIX Firewall no longer has unrecoverable crashes following a software downgrade. Previously, this problem occurred if you used the clear flashfs command, rebooted, and let the PIX Firewall restart without first loading a new image. |

Related Documentation

Table 1 **Resolved Caveats (Continued)**

| DDTS Number | Description |
|---------------------------|--|
| CSCdp37598 | PIX Firewall no longer crashes sporadically when using failover. |
| CSCdp33513 | AAA authentication over Telnet to an IBM AS400 UNIX server no longer fails. |
| CSCdp28499, CSCdp27950 | Up to 256 link command statements are now permitted in a configuration, which now conforms to the maximum specified in the configuration guide. Previously, only 64 link statements were permitted. |
| CSCdp20998 | Version 4.4(3) supports 16 MB Flash memory; however, the maximum configuration size remains 350 KB. |
| CSCdp19390 | When a failover cable connects two PIX Firewall units, the no failover command now disables failover until you explicitly enable failover with the failover command. See “no failover Command” for more information. |
| CSCdp18467 | The usage note within the version 4.4(2) release notes regarding the auth-prompt command is no longer valid. The prompt string you specify with the auth-prompt accept command no longer displays twice when a user is authenticated. |
| CSCdp17093 | An intermittent communications failure on a URL server no longer causes the PIX Firewall to enter and exit allow mode (configured with the filter url command). The PIX Firewall now sends status messages to the URL server every 5 seconds. If the PIX Firewall does not receive a reply after three tries, the URL server is marked as down and the next specified URL server becomes active. If no URL servers are available, and the PIX Firewall is configured for allow mode, the PIX Firewall enters allow mode. |
| CSCdp09563 | The show interface command has been enhanced to include eight new status counters. The new counters are only valid for Ethernet interfaces. See “show interface Command” for more information. |
| CSCdp06708 | The PIX Firewall no longer crashes when 80-block memory runs out. Previously, the message “duart_write(), no memory for <i>n</i> bytes” would display when the problem occurred. The crash was most prevalent on systems with failover enabled because failover status communications depended on 80-block memory. This dependency has been removed with the fix. In addition, the PIX Firewall would drop Telnet sessions to the PIX Firewall console because they also depended on 80-block memory. |
| CSCdm94076 | During heavy traffic, the outside Ethernet interface no longer intermittently stops transmitting traffic. See the listing for CSCdp32325 for more information. |
| CSCdm39607 | The SNMP “ifOutUcastPkts” object now correctly returns the outbound packet count. |
| CSCdm22985 | The use of the virtual http command with Microsoft Internet Explorer versions 4.0 and 5.0, no longer displays a blank page after the PIX Firewall authenticates a user. Previously the user needed to click Reload to view the browser page. |
| CSCdk91396 | See “AAA Timeout Message for RADIUS and TACACS+” for information about the timeout message for both RADIUS and TACACS+. |

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_v44/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, Browse with Me, CCDA, CCDE, CDDP, 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, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, WaRP, Wavelength Router, Wavelength Router Protocol, 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. (9912R)

Copyright © 2000, Cisco Systems, Inc.
All rights reserved.