



Text Part Number: 78-6804-04

Release Notes for the PIX Firewall Version 4.4(4)

February 2000

This document describes only the changes for version 4.4(4) of the PIX Firewall software.

For information on previous version 4.4 features, installation notes, limitations and restrictions, usage notes, and caveats, refer to the release notes at these following sites:

- Version 4.4(1):
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn44.htm
- Version 4.4(2):
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn442.htm
- Version 4.4(3):
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn443.htm

Contents

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

Corporate Headquarters

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

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

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.

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(4) differs from previous 4.4 versions in CSM, you must select version **4.4.4** 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(4) only contains bug fixes, one new command, and improved syslog messages.

New Command

The **sysopt radius ignore-secret** command is new in this release. Some commonly used RADIUS servers, such as Livingston version 1.16, have a usage caveat where they do not include the key in the authenticator hash in the accounting acknowledgment response. This can cause the PIX Firewall to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to cause the PIX Firewall to ignore the key in the authenticator of accounting acknowledgments thus avoiding the retransmit problem. (The key described here is the key you set with the **aaa-server** command.)

New Syslog Message

Syslog message “%PIX-6-302010: *connections* in use, *connections* most used” is new in PIX Firewall version 4.4(4). This message indicates the number of connections currently in use and the maximum number of connections that have been used since the PIX Firewall was last rebooted. [CSCdp57181]

Changed Syslog Message

Syslog message “%PIX-6-304004: URL Server IP_addr request failed URL chars” is now only called at severity level 6 (informational). Previously, this message appeared at both severity level 6 and severity level 3 (error). [CSCdp57937]

Installation Notes

No new installation notes were added in version 4.4(4).

Limitations and Restrictions

No new limitations and restrictions were added in version 4.4(4).

Important Notes

The following sections list important notes introduced in version 4.4(4):

- DNS Root Name Server Access
- Failover
- static Command

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. [CSCdp48115]

Failover

The **failover timeout** command does not work in this release. [CSCdm64497]

static Command

Command statements for the **static** command cannot contain overlapping IP addresses. When IP addresses are overlapped, PIX Firewall experiences service denials without sending denial statements to syslog. [CSCdp22217] In this caveat report, an FTP session was attempted but was denied without a denial message sent to syslog.

For example, the following command statements do not work:

```
nat (inside) 0 10.0.0.0 255.0.0.0
static (inside,outside) 10.0.0.0 10.0.0.0 netmask 255.0.0.0
static (inside,perim1) 10.64.0.0 10.64.0.0 netmask 255.255.0.0
```

In this example, the **nat 0** command statement enables the identity feature so that any host on the 10.0.0.0 network can start connections to a lower security level interface. The first **static** command statement lets all hosts on the inside 10.0.0.0 network be visible on the outside network. The second **static** statement attempts to use a subset of the 10.0.0.0 address range on another interface. Because 10.64.0.0 is a part of the 10.0.0.0 range of addresses, the addresses overlap.

Caveats

This section lists open and resolved caveats.

Open Caveats

Table 1 lists open caveats introduced in version 4.4(4). All open caveats in version 4.4(1) through version 4.4(3) also apply to version 4.4(4).

Table 1 Open Caveats

DDTS Number	Description
CSCdp48115	A DNS server behind the PIX Firewall cannot use PAT; however, adding a static command statement can be used as a workaround.
CSCdp22217	Command statements for the static command cannot contain IP addresses that overlap between statements.
CSCdm64497	The failover timeout command does not work in this release.

Resolved Caveats

Table 2 lists caveats resolved by the PIX Firewall Engineering team in version 4.4(4). All resolved caveats in version 4.4(1) through version 4.4(3) also apply to version 4.4(4):

Table 2 Resolved Caveats

DDTS Number	Description
CSCdp59021	Two-interface PIX Firewall units no longer continuously reboot after upgrading to the current software version.

Table 2 Resolved Caveats (Continued)

DDTS Number	Description
CSCdp57937	Syslog message “%PIX-6-304004: URL Server <i>IP_addr</i> request failed URL <i>chars</i> ” is now only called at severity level 6 (informational). Previously, this message appeared at both severity level 6 and severity level 3 (error).
CSCdp57181	Previously, syslog message %PIX-6-302009 had two different messages. In version 4.4(4), %PIX-6-302009 now has the message, “Rebuilt TCP connection number for faddr <i>IP_addr/port</i> gaddr <i>IP_addr/port</i> laddr <i>IP_addr/port</i> ” and a new message, %PIX-6-302010, has the message, “ <i>connections</i> in use, <i>connections</i> most used.” See “New Syslog Message” for more information on %PIX-6-302010.
CSCdp51439	The ACT (active) light on the PIX 515 now turns off if the unit fails.
CSCdp49663	The PIX Firewall RADIUS code no longer creates a new authenticator during retransmission, causes md5 to fail, causes the reply to be ignored, or causes an authentication timeout.
CSCdp45595	AAA accounting no longer fails if the RADIUS server is not Livingston version 1.16.
CSCdp19793	A Token-Ring connected Route Switch Module (RSM) unit no longer loses connection with the PIX Firewall. The PIX Firewall now clears the first three RIF bits for any ARP reply to force all ARP replies from the PIX Firewall to not broadcast in case there is a RIF bit set.
CSCdm64126	Syslog message %PIX-5-304001 was incorrectly listed as severity level 6; it has been corrected to be severity level 5. You can view the version 4.4 syslog messages at the following site: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pix44em/index.htm

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, 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, 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, Stratum, 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.