



Release Notes for the PIX Firewall Version 4.4(5)

June 2000

Contents

This document includes the following sections:

- Contents
- Introduction
- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

Introduction

This document describes only the changes for version 4.4(5) 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
- Version 4.4(4): http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pixrn444.htm



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 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

Memory Requirements

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.

Maximum Configuration Size

The maximum configuration size is 350 KB for all Flash memory sizes.

PIX Firewall Manager Interoperability

You can use PIX Firewall version 4.4(5) with the PIX Firewall Manager version 4.3(2)e. Refer to the *Release Notes for the PIX Firewall Manager Version 4.3(2)e* for more information. You can view this document online at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v44/pfm432e.htm

The PIX Firewall Manager (PFM) lets you manage PIX Firewall units; however, it does not let you configure any PIX Firewall features added after version 4.3(2).

The “Frequently Asked Questions” section in the PFM release notes provides useful troubleshooting information.

Cisco Security Policy Manager Interoperability

Cisco Security Policy Manager (CSPM), version 2.1, provides policy-based management support for PIX Firewall units running version 4.2(*n*), 4.4(*n*), and 5.1(*n*) software images.

Refer to the documentation set for CSPM at the following site:

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

New and Changed Information

Version 4.4(5) contains bug fixes and command changes described in the following sections.

fixup protocol ftp Command Option

The new **fixup protocol ftp strict** command option was added. The command syntax is as follows:

```
fixup protocol ftp [strict] [port]
```

The **strict** option indicates that this command prevents web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The **strict** option only lets an FTP server generate the 227 command and only lets an FTP client generate the PORT command. The 227 and PORT commands are checked to ensure they do not appear in an error string. In addition, the FTP port can now only be in the range of 1 to 1024.

The *port* parameter lets you specify the port at which the PIX Firewall listens for FTP traffic. Typically, this value is 21. [CSCdp86352]

ip verify reverse-path Command

The new **ip verify reverse-path** command implements unicast RPF IP spoofing protection. (Configuration mode.) [CSCdp70632] The command syntax is as follows:

```
ip verify reverse-path interface int_name
```

```
no ip verify reverse-path interface int_name
```

```
show ip verify [reverse-path [interface int_name]]
```

```
clear ip verify [reverse-path [interface int_name]]
```

Syntax Description

int_name Name of an interface you want to protect from a DoS attack.

Usage Guidelines

The **ip verify reverse-path** command lets you specify which interfaces to protect from an IP spoofing attack using network ingress and egress filtering, which is described in RFC 2267. This command is disabled by default and provides unicast RPF (Reverse Path Forwarding) functionality for the PIX Firewall. The **show ip verify** command lists the **ip verify** commands in the configuration. The **clear ip verify** command removes **ip verify** commands from the configuration. Unicast RPF is a unidirectional input function that screens inbound packets arriving on an interface. Outbound packets are not screened.

Due to the danger of IP spoofing in the IP protocol, measures need to be taken to reduce this risk when possible. Unicast RPF (Reverse Path Forwarding), or reverse route lookups, prevents such manipulation under certain circumstances.

The **ip verify reverse-path** command provides both ingress and egress filtering. Ingress filtering checks inbound packets for IP source address integrity, and is limited to addresses for networks in the enforcing entity's local routing table. If the incoming packet does not have a source address represented by a route, then it is impossible to know whether the packet has arrived on the best possible path back to its origin. This is often the case when routing entities cannot maintain routes for every network.

Egress filtering verifies that packets destined for hosts outside the managed domain have IP source addresses verifiable by routes in the enforcing entity's local routing table. If an exiting packet does not arrive on the best return path back to the originator, then the packet is dropped and the activity is logged. Egress filtering prevents internal users from launching attacks using IP source addresses outside of the local domain because most attacks use IP spoofing to hide the identity of the attacking host. Egress filtering makes the task of tracing the origin of an attack much easier. When employed, egress filtering enforces what IP source addresses are obtained from a valid pool of network addresses. Addresses are kept local to the enforcing entity and are therefore easily traceable.

Unicast RPF is implemented as follows:

- ICMP packets have no session so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.



Note

Before using this command, add static **route** command statements for every network that can be accessed on the interfaces you wish to protect. Only enable this command if routing is fully specified. Otherwise, PIX Firewall will stop traffic on the interface you specify if routing is not in place.

Use the **show interface** command to view the number dropped packets, which appears in the “unicast rpf drops” counter.

Examples

The following example protects traffic between the inside and outside interfaces and provides **route** command statements for two networks 10.1.2.0 and 10.1.3.0 that connect to the inside interface via a hub:

```
ip address inside 10.1.1.1 255.255.255.0
route inside 10.1.2.0 255.255.255.0 10.1.1.1 1
route inside 10.1.3.0 255.255.255.0 10.1.1.1 1
ip verify reverse-path interface outside
ip verify reverse-path interface inside
```

The **ip verify reverse-path interface outside** command statement protects the outside interface from network ingress attacks from the Internet, whereas the **ip verify reverse-path interface inside** command statement protects the inside interface from network egress attacks from users on the internal network.

Installation Notes

No new installation notes were added in version 4.4(5).

Limitations and Restrictions

No new limitations and restrictions were added in version 4.4(5).

Important Notes

This section lists all important notes that apply to this version.

FTP Change

PIX Firewall now restricts FTP commands so that only FTP servers can submit a 227 reply and only FTP clients can submit a PORT command. Furthermore, the only PORT command permitted can only be one port number lower than the FTP control channel. This change removes the wildcard port for connection created from the PORT command. PIX Firewall now also enforces that the first SYN packet from the dynamic back channel must be from the expected side. [CSCdp86352]

Inconsistent Syslog Message

Syslog message PIX-6-302002 listed the wrong number of bytes transferred during the last TCP connection. If a client tried to connect to an FTP server outside the PIX Firewall unit and FTP was not active, the server occasionally sent an RST (reset). The reset ended the connection, which created incorrect TCP header lengths. If the TCP header length was larger than the packet length, the result produced a negative number of bytes transferred that syslog displayed as an extremely large number.

Error checking has been updated to prevent the inconsistent syslog message and syslog message PIX-5-500003 was added to indicate when a bad TCP header length occurs. [CSCdp74486]

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

The sections that follow list open and resolved caveats in this release.

Open Caveats

The following open caveats were reported in version 4.4:

- 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

The following caveats were fixed in version 4.4(5):

- CSCdp95629
A failover Standby unit no longer sends Websense requests to the Websense server.
- CSCdp93492
The TACACS+ per-user idle and absolute timeouts now work correctly.
- CSCdp88122
PIX Firewall no longer fails when detecting a bad SQL*Net packet.
- CSCdp86352
If the new **fixup protocol ftp strict** command is entered, PIX Firewall now prevents FTP clients from initiating FTP server commands. Refer to “fixup protocol ftp Command Option” for more information.
- CSCdp85781
A command line error appears if you enter the **aaa** command with abbreviated matching letters of **aaa-server** command statements. For example, using the letter “t” when there is more than one server that starts with the letter “t.” The server name must be defined enough to differentiate between names.
- CSCdp75120
Syslog has been updated to correct the missing message PIX-6-302002.
- CSCdp74486
If a bad TCP header length was detected, syslog message PIX-6-302002 reported an incorrect number of bytes transferred. The PIX-5-500003 syslog message has been added to indicate when a bad TCP header length occurs.
- CSCdp70632 and CSCdp50953
Address spoofing is no longer possible using perimeter interface address ranges when the new **ip verify reverse-path** command is used. Refer to “ip verify reverse-path Command” for more information.
- CSCdp64244
Logging now occurs for a URL when performing JAVA filtering.
- CSCdp49663
When retransmitting an access request that has timed out, use the previously generated authenticator. Creating a new authenticator may cause the access reply to be ignored.
- CSCdp41051
The **terminal no monitor** command now works correctly.
- CSCdm94131
TCP flags are now printed for all SYS_DENY_TCP_OUT syslog messages.

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

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.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 is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value 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, Are You Ready, 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, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, 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 Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, 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 other company. (0005R)

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