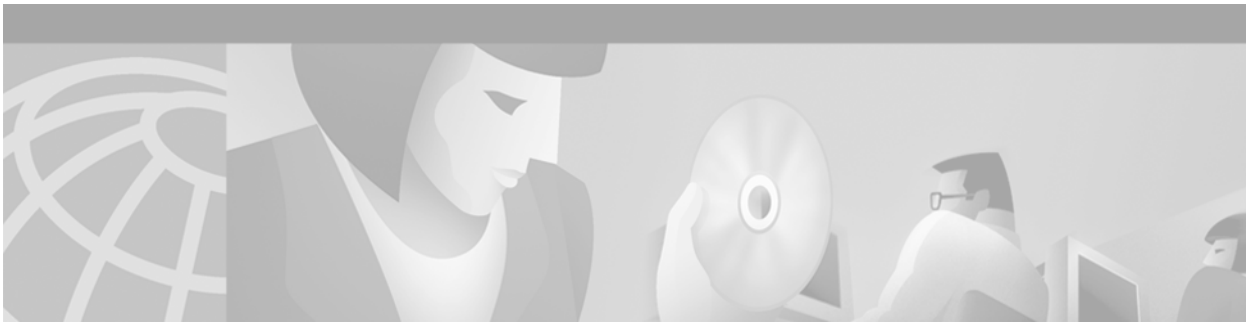

Release Notes for the Cisco Secure PIX Firewall Version 5.3(1)

December 2000

Contents

This document includes the following sections:

- Introduction
- System Requirements
- New and Changed Information
- Command Changes
- Syslog Messages
- Documentation Changes
- Important Notes
- Caveats
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

Introduction

This release note describes the new features, restrictions, and caveats for the Cisco Secure PIX Firewall 5.3(1) release.

CISCO SYSTEMS

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

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

78-11202-03

System Requirements

The following sections describe the system requirements for operating a Cisco Secure PIX Firewall unit with version 5.3(1) software.

Memory Requirements

Note All PIX Firewall units *must* have at least 32 MB of RAM memory or the PIX Firewall unit will not boot. In addition, all units except the PIX 506 must have at least 16 MB of Flash memory to boot. The PIX 506 has 8 MB of Flash memory, which works correctly with version 5.2 and higher.

The following table lists Flash memory requirements for this release:

PIX Firewall Model	Flash Memory Required in 5.2	Flash Memory Sold with Unit
PIX 506	8 MB	8 MB (not upgradeable)
PIX 510 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX 515, PIX 525, PIX 535	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 10000 (discontinued)	16 MB	2 MB (must be upgraded to 16 MB)
PIX Firewall Classic (discontinued)	16 MB	512 KB or 2 MB (must be upgraded to 16 MB)

Software Requirements

The following is required for version 5.3(1):

1. The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, you need to download the Boothelper file, bh531.bin, from Cisco Connection Online (CCO) to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from version 4 or earlier and want to use the IPSec or VPN features or commands, you must have an activation (license) key that enables Data Encryption Standard (DES) or the more secure 3DES.

   To obtain a DES (56-bit) license key for the PIX Firewall, use the IPSec 56-bit Customer Registration form. Accessing this form requires prior registration on Cisco.com at http://www.cisco.com/register. However, access to this form does not require a purchase or service contract. You can register as a guest and then proceed to fill out the form. The form is available at the following website:

   http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324

   You must purchase a 3DES (168-bit) license key, or have a service contract, to obtain a 3DES license key. If you have already purchased a 3DES upgrade, and you have your Cisco PIX Firewall 3DES upgrade document with the entitlement number printed on it, you can register your license

key for use on your PIX Firewall with the License Registration form. Accessing this form also requires prior registration on Cisco.com at http://www.cisco.com/register. The License Registration form is available at the following website:

http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=301

You must also purchase or have a service contract to download PIX Firewall software.

3. If you are using PFSS (PIX Firewall Syslog Server), Cisco recommends you install Windows NT Service Pack 6 to fix year 2000 conflicts in Windows NT.
4. If you are upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* for new installation requirements.

Cisco IOS Software Interoperability

If you use IKE Mode Config with the PIX Firewall, any routers on the IPSec connection must run Cisco IOS Release 12.0(6)T or later.

Cisco Secure Policy Manager Interoperability

Cisco Secure Policy Manager (Cisco Secure PM), version 2.1, provides policy-based management support for PIX Firewall units running version 4.2, 4.4, and 5.1 software images. Cisco Secure PM version 2.2 supports PIX Firewall version 5.2 and higher.

Refer to the documentation set for Cisco Secure PM at the following site:

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

Cisco Secure VPN Client Interoperability

PIX Firewall version 5.2 and higher requires Cisco Secure VPN Client version 1.1. The Cisco Secure VPN Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco Secure VPN Client is not supported for use with Windows 2000.

Cisco VPN 3000 Concentrator and Client Interoperability

PIX Firewall version 5.2 and higher requires Cisco VPN 3000 Client version 2.5 or later and Cisco VPN 3000 Concentrator version 2.5.2 or later. The Cisco VPN 3000 Client can be used with Windows 95, Windows 98, and Windows NT version 4.0. The Cisco VPN 3000 Client is not supported for use with Windows 2000.

PIX Firewall Manager Interoperability

You can use PIX Firewall version 5.2 and higher with the PIX Firewall Manager version 4.3(2)g. Refer to the *Release Notes for the PIX Firewall Manager Version 4.3(2)g* for more information. You can view this document online at the following site:

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

Determining the Software Version

Use the **show version** command to verify the software version of your PIX Firewall unit.

Upgrading to a New Software Release

If you have a Cisco Connection Online (CCO) login, you can obtain software from the following site:

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

New and Changed Information

The following describes the new software and hardware information in this 5.3(1) release.

New Hardware Features in Release 5.3(1)

The sections describe the new hardware features in the 5.3(1) release.

VPN Accelerator

The VPN Accelerator (PIX-VPN-ACCEL) is a new encryption accelerator board. For more information on the VPN Accelerator, refer to the *Installation Guide for the Cisco Secure PIX Firewall Version 5.3*. Observe the following before installing the VPN Accelerator:

- Do not use a Private Link board and a VPN Accelerator in the same PIX Firewall chassis. If your PIX Firewall has a Private Link board installed, you should remove the Private Link board before installing the VPN Accelerator.
- The VPN Accelerator uses a PCI interface and therefore can only be installed in PIX Firewall platforms with PCI slots.
- Before downgrading from version 5.3(1) to an earlier version, remove the VPN accelerator board from your PIX Firewall unit. The PIX 535 cannot be downgraded to earlier versions.

PIX 535

The new PIX 535 model has the fastest performance and highest capacity of any of the PIX Firewall series. Observe the following before installing the PIX 535:

- PIX 535 only supports PIX Firewall software version 5.3 or later. Installing a version earlier than 5.3 using the **copy tftp flash** command causes a condition in which the PIX 535 fails repeatedly. Should this occur, when the PIX 535 unit restarts, press the Escape key on your console workstation to access Monitor mode and load version 5.3 or later before proceeding with the startup.
- A PIX 535 configured with only Gigabit interfaces will not be capable of upgrading an Activation key. Activation key upgrades require Monitor mode for all systems without floppy disk drives. Monitor mode does not support Gigabit interfaces. A Fast Ethernet interface must be installed to use Monitor mode.

  A PIX 535 with Gigabit Ethernet should be populated only with PIX-1GE66 Gigabit Ethernet adaptors. The PIX-1GE functions, but with significantly reduced throughput (about 50 percent). The software displays a warning if a PIX-1GE is detected.

  If a PIX 535 is ordered with Gigabit interfaces only, an additional Fast Ethernet interface is included with the unit so that the Activation key may be upgraded.

- For the PIX 535, the only supported Ethernet interface types are the i82558 or i82559. You can view the interface type in the second line of the **show interface** command output. The correct interface type displays as "Hardware is i82558 ethernet" or "Hardware is i82559 ethernet."

For more information on the PIX 535, refer to the *Installation Guide for the Cisco Secure PIX Firewall Version 5.3*.

The PIX 535 provides the following features:

Features	PIX 535—R	PIX 535—UR
Failover	No	Yes
RAM	512 MB	1 GB
Flash memory	16 MB	16 MB
Maximum interfaces	6	8
Supported Interfaces	Fast Ethernet, Gigabit Ethernet, and VPN Accelerator	
Power Supplies	Dual, redundant, hot-swappable AC power supplies	

New Software Features in Release 5.3(1)

The following features are new in version 5.3(1):

- **DHCP**—DHCP Server now supports 32 clients instead of 10 clients.
- **nat 0 access list**—There is no longer a restriction on having **nat 0 access-list** and **nat 0** (Identity NAT) configured at the same time. Both **nat 0** and **nat 0 access-list** may be configured concurrently.
- **RIP Version 2**—RIP Version 2 multicast is now supported on the PIX Firewall.

Refer to the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* for complete information about each software feature. IPSec features are described in the *IPSec User Guide for the Cisco Secure PIX Firewall Version 5.3*.

Command Changes

1. **sysopt connection enforcesubnet**—This command has been deleted from the Command Line Interface.
2. **show eeprom**—Displays the current PIX Firewall eeprom contents.

   eeprom update—Update the eeprom contents.
3. Global RADIUS port definition option:

   aaa-server radius-authport <authport>—Specifies RADIUS server authentication.

   aaa-server radius-acctport <acctport>—Specifies RADIUS server accounting.

Note This is a global setting that takes effect when RADIUS is started. The default ports are 1645 for authentication and 1646 for accounting as defined in RFC 2058. Newer RADIUS servers may use the port numbers 1812 and 1813 as defined in RFC 2138 and 2139. If your server uses ports other than 1645 and 1646, then you should define ports using the **aaa-server radius-authport** and**aaa-server radius-acctport** commands prior to starting the RADIUS service with the **aaa-server** command.

Syslog Messages

The following are new or changed syslog messages in PIX Firewall software version 5.3(1):

- %PIX-3-305008—Free unallocated global IP detected
- %PIX-2-211002—Failed to allocate channel

  This syslog message,%PIX-2-211002, is no longer used.
- The following message has been changed from:

  %PIX-2-106002:*protocol#* Connection denied by outbound list

  list_ID src *laddr*/l*port* dest *faddr*/*fport*

  Explanation This is a connection-related message. This message is logged if the specified connection fails because of an **outbound deny** command statement. The *protocol#* variable is 1 for ICMP, 6 for TCP, and 17 for UDP.

  To the following:

  %PIX-2-106002:*protocol* Connection denied by outbound list

  list_ID src *laddr* dest *faddr*

  Explanation This is a connection-related message. This message is logged if the specified connection fails because of an **outbound deny** command statement. The *protocol* variable can be ICMP, TCP, or UDP.
- The following message has been changed from:

  %PIX-3-106010:Deny inbound from outside:*IP_addr* to inside:*IP_addr chars*

  To the following:

  %PIX-3-106010:Deny inbound icmp src outside:*IP_addr* dst inside:*IP_addr* (type *dec*, code *dec*)
- The following message has been changed from:

  %PIX-3-305006:Invalid dst is network/broadcast IP, translation creation failed for *protocol* src *int_name:IP_addr* dst *int_name:IP_addr*.

  To the following:

  %PIX-3-305006:Regular translation creation failed for *protocol* src *int_name:IP_addr*/*port* dst *int_name:IP_addr*/*port*

All syslog messages are described in the *System Log Messages for the Cisco Secure PIX Firewall Version 5.3* document.

Documentation Changes

AAA

The **clear aaa** command is shown in the "Command Reference" chapter of the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* as:

clear aaa [**accounting include | exclude** *authen_service* **inbound | outbound |** *if_name group_tag*]

clear aaa [**authentication include | exclude** *authen_service* **inbound | outbound |** *if_name local_ip local_mask foreign_ip foreign_mask group_tag*]

The description of this command should be shown with a bracket before the **include** and after **exclude,** and before **inbound** and after **outbound**:

clear aaa [**accounting** [**include | exclude**] *authen_service* [**inbound | outbound**] *if_name group_tag*]

clear aaa [**authentication** [**include | exclude**] *authen_service* [**inbound | outbound**] *if_name local_ip local_mask foreign_ip foreign_mask group_tag*]

Configuring Failover

There is a change in the failover installation instructions in the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3*. In the printed document, this change is in the section, "Configuring Failover" in Chapter 3, "Advanced Conversations." This change may be viewed at this website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/advanced.htm#xtocid227608

- Previous text:

  Step 2 Ensure that all active network interfaces are connected between both units.

- New text:

  Step 2 Attach a network cable between the Primary and Secondary units for each network interface to which you have configured an IP address.

Important Notes

The following sections describe important notes for the 5.3(1) release.

16 MB Board

8 MB or more of Flash is required to install and run PIX software version 5.3(1). The purchase and installation of Flash upgrade PIX-FLASH-16MB= is required for PIX, PIX10000, PIX 510, or PIX 520 revisions A0 through C0 to install version 5.3(1). PIX 520 revisions may be identified by the Flash type as reported in a **show version** command request. 2 MB models contain the AT29C040A Flash OR ATMEL , and 16 MB models contain the i28F640J5 Flash.

AAA

The *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* incorrectly states that the maximum number of AAA servers is 14. This information appears as usage note 15 on the **aaa** command page and in the *group_tag* description for the **aaa-server** command page. Both these command pages appear in Chapter 5, "Command Reference." You can have up to 16 AAA servers per tag group, up to 14 AAA server tag groups, and a total of up to 224 AAA servers.

Access-list

The new **access-list** option changes the behavior of the **nat 0** command. (Without the **access-list** option, the command is backward compatible with previous versions.) The **nat 0** implemented the identity feature; this new version of the command disables NAT. Specifically, the new behavior disables proxy ARPing for the IP addresses in the **nat 0** command statement.

Cisco Secure Policy Manager

PIX Firewall version 5.1(2) and later, by default, generates the **isakmp identity hostname** command prior to any crypto configuration. Subsequently, when attempting to configure Cisco Secure VPN Client (version 2.1.2), an IPSec tunnel cannot be established because it defaults to an IP address as its default ID Type. This causes failure with the Cisco Secure Policy Manager version 2.1 when it tries to configure the PIX Firewall through an IPSec tunnel.

Cisco Secure VPN Client

When using the Cisco Secure VPN Client with SoftID, the single password challenge prompt only appears for 30 seconds. When two passwords are required, the prompt only appears for approximately 60 seconds. You must enter your password information promptly before the timeout expires. Refer to caveat CSCds59105 for more information.

DHCP

The following notes apply to DHCP:

- A new DHCP command, **dhcpd ping_timeout**, is introduced. This command allows setting a ping timeout value before assigning an IP to a DHCP client.

  DHCP daemon can be enabled on inside interface only. The DHCP Server on the PIX Firewall does not support clients that not directly connected to the **inside** interface.

  The maximum lease supported on PIX is 2147483647, not 0xFFFFFFFF (as in RFC 2131).

- PIX Firewall removes an IP address from the pool of available DHCP IP addresses if a host responds to a ping request that the PIX Firewall sends prior to issuing the IP address to the DHCP client. The address removed from the pool can only be made available again by rebooting the PIX Firewall, or by disabling and then reenabling the DHCP server command statements in the configuration. Refer to CSCds51664 in the Bug Navigator on CCO to view more information.

DNS

PIX Firewall drops DNS packets sent to UDP port 53 that have a packet size larger than 512 bytes.

Failover

Ensure that all PIX Firewall interfaces to which you assign an IP address are connected between the Primary unit and Secondary unit.

Gigabit Ethernet

If, after configuring a PIX Firewall unit for Gigabit Ethernet boards, you replace the boards with 10/100 Ethernet boards, the order of the boards in the configuration changes from what you originally configured. For example, if you configure ethernet0 for a Gigabit Ethernet board assigned to the inside interface and replace this board with a 10/100 Ethernet board, the board may no longer appear as ethernet0.

ISAKMP

- When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0):Unknown error in cert validation, 0” and packets are lost until the PIX Firewall receives the CRL. Refer to caveat CSCdr89880 for more information.
- Use the following information to configure the **isakmp keepalive** command:

  isakmp keepalive <seconds> [retry <seconds>]

  The keepalive interval can be between 10 and 3600 seconds. The retry interval can be between 2 and 10 seconds, with the default being 2 seconds. The retry interval is the interval between retries after a keepalive response has not been received. For more information on keepalive see the following Cisco IOS software documentation:

  http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpne_an.htm

  http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/dplip_in.htm

PIX 525

- PIX 525 in version 5.3(1) supports up to eight interfaces with an unrestricted license (UR). The restricted license (R)supports up to six interfaces. The **show version** command lists the maximum number of supported interfaces on the unit. If you add more interfaces than are supported, the additional interfaces are ignored. However, when you first start the PIX 525 unit, the startup messages display the number of installed interfaces followed by two error messages stating that interfaces are disabled. You can ignore these messages and use only the information in the **show version** command to verify the correct number of supported interfaces. Refer to CSCds44827 in the Bug Navigator on CCO to view more information.
- There are no hardware or software limitations regarding using more than 2 Gigabit interfaces in the PIX 525 as of the 5.2 version software release.

  There is a performance limitation because the PIX 525 uses a 32-bit PCI bus.

PPTP

If you configure PIX Firewall for 128-bit encryption and if a Windows 95 or Windows 98 client does not support 128-bit or greater encryption, the connection to the PIX Firewall is refused. When this occurs, the Windows client moves the dial-up connection menu down to the screen corner while the PPP negotiation is in progress. This gives the appearance that the connection is accepted when it is not. When the PPP negotiation completes, the tunnel terminates and PIX Firewall ends the connection. The Windows client eventually times out and disconnects.

RAS

H.323 RAS fixups cannot be disabled through the PIX Firewall when the PIX Firewall unit is between the H.323 Gateway and Gatekeeper. When the PIX Firewall is between the Gateway and Gatekeeper, whenever PIX Firewall detects RAS packets, it enables packet checking. Use the **debug h323 ras event** command to determine if RAS packets are passing through the PIX Firewall.

Sample output from the **debug h323 ras event** command appears as follows:

57:RAS::RRQ received from 10.130.4.250/51527 to 10.132.4.6/1719

58:RAS::RCF received from 10.132.4.6/1719 to 10.132.4.250/51527

The first line shows that a RAS registration request was received by the PIX Firewall. The next line shows that the request was confirmed.

If the PIX Firewall unit is not between the Gateway and Gatekeeper, you can enable RAS fixups with the **fixup protocol h323 1720** command. If the PIX Firewall unit is not between the Gateway and Gatekeeper, you can disable RAS fixups with the **no fixup protocol h323 1720** command.

However, if the PIX Firewall unit *is* between the Gateway and Gatekeeper, the **no fixup protocol h323 1720** command has no effect and RAS fixups continue automatically.

RIP Version 2

With version 5.3, when RIP version 2 is configured in passive mode, the PIX Firewall accepts RIP version 2 multicast updates with IP destination of 224.0.0.9. For RIP version 2 default mode, the PIX Firewall will transmit default route updates using an IP destination of 224.0.0.9. Configuring RIP version 2 registers the multicast address 224.0.0.9 on the respective interface in order to be able to accept multicast RIP version 2 updates.

Only Intel 10/100 and Gigabit interfaces support multicasting. FDDI and Token Ring will still operate in broadcast mode (IP destination 255.255.255.255 not 224.0.0.9).

When the RIP version 2 commands for an interface are removed, the multicast address is unregistered from the interface card.

RTSP

You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside and the server on the inside.

SMTP

As of version 5.1 and later, the **fixup protocol smtp** command changes the characters in the SMTP banner to asterisks except for the “2”, “0”, “0 ”characters. Carriage return (CR) and linefeed (LF) characters are ignored. In version 4.4, all characters in the SMTP banner are converted to asterisks. Refer to CSCds33156 in the Bug Navigator on CCO to view more information.

Token Authentication

For use with the **crypto map token authentication** command, token based authentication for the Cisco VPN 3000 Client connecting to a PIX Firewall has been tested and verified for the following token devices:

- Security Dynamics (SDI) SecurID/ACE Server with SDI RADIUS
  - Next Token mode
  - New Pin mode
- SDI with CiscoSecure ACS NT version
  - Next Token mode
  - New Pin mode
- SDI with CiscoSecure ACS UNIX version
  - Next Token mode
  - New Pin mode does not work

Token based authentication using the SDI RADIUS server has also been tested and verified with the Cisco Secure VPN Client version 1.1 including:

- Next Token mode
- New Pin mode

Caveats

The following sections describe the open and resolved caveats for the 5.3(1) release.

Note Please use Bug Navigator II on CCO to view additional caveat information. Bug Navigator II may be accessed at the following URL:

http://www.cisco.com/support/bugtools

Open Caveats - Release 5.3(1)

- CSCds80108

  Cisco Secure Intrusion Detection System (Cisco Secure IDS) signature number 1101 is not supported by PIX Firewall. When an unsupported signature number is entered, PIX Firewall returns an error message:

  pixfirewall(config)# **ip audit signature 1101 disable** usage:ip audit signature *number* disable
  Type help or '?' for a list of available commands.
  pixfirewall(config)#

- CSCds69891

  Before downgrading from version 5.3(1) to an earlier version, remove the VPN accelerator board from your PIX Firewall unit. The PIX 535 cannot be downgraded to earlier versions.

- CSCds67745

  If you configure a network static where the network static is the same as a third party netmask and address, then an outbound H.323 connection fails. The following example clarifies this problem:

  The interfaces in the example are as follows:

  - The outside interface IP address:10.1.1.6
  - The inside interface IP address:10.0.0.5
  - Embedded address on inside interface:10.0.0.7

  Example network static command statement:

  static (inside,outside) 10.1.1.0 10.0.0.0

  This command maps the inside host address of 10.0.0.5 to the outside global address of 10.1.1.5 and the inside host address 10.0.0.7 to the outside global address of 10.1.1.7.

  If the PIX Firewall encounters a packet from 10.1.1.5 to 10.0.0.5 with the embedded IP address of 10.1.1.7, the PIX Firewall unit will not be able to determine if the embedded IP address belongs to the inside or outside network.

- CSCds59105

  When using the Cisco Secure VPN Client with SoftID, the single password challenge prompt only appears for 30 seconds. When two passwords are required, the prompt only appears for approximately 60 seconds. You must enter your password information promptly before the timeout expires.

- CSCds51664

PIX Firewall removes an IP address from the pool of available DHCP IP addresses if a host responds to a ping request that the PIX Firewall sends prior to issuing the IP address to the DHCP client. The address removed from the pool can only be made available again by rebooting the PIX Firewall, or by disabling and then reenabling the DHCP server command statements in the configuration.

- CSCds44827

  PIX 525 in version 5.3(1) supports up to eight interfaces with an unrestricted license (UR). The restricted license (R)supports up to six interfaces. The **show version** command lists the maximum number of supported interfaces on the unit. If you add more interfaces than are supported, the additional interfaces are ignored. However, when you first start the PIX 525 unit, the startup messages display the number of installed interfaces followed by two error messages stating that interfaces are disabled. You can ignore these messages and use only the information in the **show version** command to verify the correct number of supported interfaces.

- CSCds33156

  As of version 5.1 and later, the **fixup protocol smtp** command changes the characters in the SMTP banner to asterisks except for the “2”, “0”, “0 ” characters. Carriage return (CR) and linefeed (LF) characters are ignored. In version 4.4, all characters in the SMTP banner are converted to asterisks.

- CSCdr89880

  When CRL checking is configured as mandatory, PIX Firewall takes about two minutes to poll the CRL from the VeriSign CA Server during ISAKMP negotiation. As a result, ISAKMP negotiation fails with the message “ISAKMP (0):Unknown error in cert validation, 0” and packets are lost until the PIX Firewall receives the CRL.

- CSCdr82395

  PIX Firewall by default generates the **isakmp identity hostname** command prior to any IPSec configuration. Subsequently, when attempting to configure the Cisco Secure VPN Client version 2.1.2, an IPSec tunnel cannot be established because the IPSec tunnel defaults to IP address as its default ISAKMP ID type. This also causes the Cisco Secure Policy Manager version 2.1 to fail when it tries to configure the PIX Firewall through an IPSec tunnel.

- CSCdr78383

  H.323 RAS fixups cannot be disabled through the PIX Firewall when the PIX Firewall unit is between the H.323 Gateway and Gatekeeper. When the PIX Firewall is between the Gateway and Gatekeeper, whenever PIX Firewall detects RAS packets, it enables packet checking. Use the **debug h323 ras event** command to determine if RAS packets are passing through the PIX Firewall.

- CSCds44827

  If two four-port Ethernet boards are inserted in a PIX 525 with an R license, which only supports 6 interfaces, the last two interfaces are ignored. The following messages appear at startup:

  - Ignoring NIC in PCI slot 3
  - Ignoring NIC in PCI slot 3

  These messages indicate that the PIX Firewall unit detected more interfaces than permitted by the license and ignored the extra two.

- CSCds11526

  The following information applies to use of the **crypto map token authentication** command. Token based authentication for the Cisco VPN 3000 Client connecting to a PIX Firewall has been tested and verified for the following:

  - Security Dynamics (SDI) SecurID and ACE Server with SDI RADIUS:

    Next Token mode

    New Pin mode
  - SDI with Cisco Secure ACS Windows NT version:

    Next Token mode

    New Pin mode
  - SDI with Cisco Secure ACS UNIX version:

    Next Token mode

    New Pin mode *does not* work

  Token based authentication using the SDI RADIUS server has also been tested and verified with the Cisco Secure VPN Client version 1.1 for Next Token mode and New Pin mode.

Resolved Caveats - Release 5.3(1)

CSCds66550, CSCds66052, CSCds62734, CSCds58313, CSCds56721, CSCds55734, CSCds55694, CSCds54886, CSCds53316, CSCds51955, CSCds50982, CSCds46349, CSCds38708, CSCds34732, CSCds34622, CSCds34475, CSCds32842, CSCds30699, CSCds29676, CSCds26054, CSCds25070, CSCds24580, CSCds23698, CSCds22194, CSCds21095, CSCds11378, CSCds09730, CSCdr93478, CSCdr93435, CSCdr84484, CSCdr77921, CSCdr48266, CSCdp67764

Note Please use Bug Navigator II on CCO to view additional information for the resolved caveats. Bug Navigator II may be accessed at the following URL:

http://www.cisco.com/support/bugtools

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN 3000 documentation at the following sites:

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

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm

Cisco provides PIX Firewall technical tips at the following site:

http://www.cisco.com/warp/public/110/index.shtml#pix

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- 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 and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered CCO users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

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 your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com 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.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, 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 Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, Cisco Powered Network logo, Cisco Systems Networking Academy, 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 Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0010R)

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