



Release Notes for the Cisco PIX Firewall Version 6.0(1)

August 2001

Contents

This document includes the following sections:

- [Introduction](#)
- [System Requirements](#)
- [New and Changed Information](#)
- [Command Reference](#)
- [Debug Commands](#)
- [Important Notes](#)
- [Caveats](#)
- [Related Documentation](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)
- [Obtaining Additional Publications and Information](#)

Introduction

The Cisco Secure PIX Firewall provides secure networking and NAT (Network Address Translation). Version 6.0(1) adds support for Cisco PIX Device Manager (PDM), L2TP, the Cisco VPN Client version 3.0, and other feature enhancements.



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

Copyright © 2001 Cisco Systems, Inc. All rights reserved.

System Requirements

The sections that follow list the system requirements for operating a Cisco Secure PIX Firewall with version 6.0(1) software.

Memory Requirements



Note

All PIX Firewall units *must* have at least 32 MB of RAM memory or the PIX Firewall will not boot. In addition, all units except the PIX 506 must have 16 MB of Flash memory to boot. The PIX 506 has 8 MB of memory, which works correctly with version 6.0(1).

The following table lists Flash memory requirements for this release:

PIX Firewall Model	Flash Memory Required in 6.0(1)	Flash Memory Sold with Unit
PIX 506	8 MB	8 MB (not upgradeable)
PIX 515	16 MB	16 MB
PIX 520	16 MB	Older units have 2 MB, new units have 16 MB
PIX 525	16 MB	16 MB
PIX 535	16 MB	16 MB

Software Requirements

The following is required for version 6.0(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 from Cisco.com 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://tools.cisco.com/RPF/register/register.do>. 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://tools.cisco.com/RPF/register/register.do>. 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), we recommend 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 “[Upgrading to a New Software Release](#)” for new installation requirements.

Cisco IOS Software Interoperability

Cisco VPN Series	Interoperability
Cisco IOS Routers	If using IKE mode configuration on the PIX Firewall, the router must be running Cisco IOS Release 12.0(6)T or later.
Cisco VPN 3000 Concentrators	PIX Firewall version 6.0(1) requires Cisco VPN 3000 Concentrator version 2.5.2 or later for correct VPN interoperability.

Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco Secure VPN Client v1.x	PIX Firewall version 6.0(1) requires Cisco Secure VPN Client version 1.1. Cisco Secure VPN Client version 1.0 and 1.0a are no longer supported.
Cisco VPN 3000 Client v2.5	PIX Firewall version 6.0(1) requires Cisco VPN 3000 Client version 2.5 or later. This VPN client can be used with Windows 95, Windows 98, and Windows NT version 4.0. It is not supported on Windows 2000.
Cisco VPN Client v3.0 (Unified VPN Client Framework)	PIX Firewall version 6.0(1) supports the Cisco VPN Client version 3.0. The Cisco VPN Client runs on all current Microsoft Windows platforms. At this time, the Cisco VPN Client is not supported on UNIX, Linux, or Mac platforms.

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.com user name and password, you can obtain software from the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>

New and Changed Information

New Hardware Features in Release 6.0(1)

PIX 535 Interfaces

The PIX 535 now supports up to ten interfaces. A maximum of eight interfaces are available with a restricted license, and ten interfaces are available with an unrestricted license.

These practices must be followed to achieve the best possible system performance on the PIX 535:

- PIX-1GE-66 interface cards should be installed first in the 64-bit/66 MHz buses before they are installed in the 32-bit/33 MHz bus. If more than four PIX-1GE-66 cards are needed, they may be installed in the 32-bit/33 MHz bus but with limited potential throughput.
- PIX-1GE and PIX-1FE cards should be installed first in the 32-bit/33 MHz bus before they are installed in the 64-bit/66 MHz buses. If more than five PIX-1GE and/or PIX-1FE cards are needed, they may be installed in a 64-bit/66 MHz bus but doing so will lower that bus speed and limit the potential throughput of any PIX-1GE-66 card installed in that bus.

The PIX-1GE Gigabit Ethernet adaptor is supported in the PIX 535; however, its use is strongly discouraged because maximum system performance with the PIX-1GE card is much lower than that with the PIX-1GE-66 card. The software displays a warning at boot time if a PIX-1GE is detected.

The following table summarizes the performance considerations of the different interface card combinations.

Figure 1 Gigabit Ethernet Interface Card Combinations

Interface Card Combination	Installed In Interface Slot Numbers	Potential Throughput
Two to four PIX-1GE-66	0 through 3	Best
PIX-1GE-66 combined with PIX-1GE or just PIX-1GE cards	0 through 3	Degraded
Any PIX-1GE-66 or PIX-1GE	4 through 8	Severely degraded



Caution

The PIX-4FE and PIX-VPN-ACCEL cards can only be installed in the 32-bit/33 MHz bus and must never be installed in a 64-bit/66 MHz bus. Installation of these cards in a 64-bit/66 MHz bus may cause the system to hang at boot time.



Caution

If Stateful Failover is enabled, the interface card and bus used for the Stateful Failover LAN port must be equal to or faster than the fastest card used for the network interface ports. For example, if your inside and outside interfaces are PIX-1GE-66 cards installed in bus 0, then your Stateful Failover interface must be a PIX-1GE-66 card installed in bus 1. A PIX-1GE or PIX-1FE card cannot be used in this case, nor can a PIX-1GE-66 card installed in bus 2 or sharing bus 1 with a slower card.

Changed Hardware Features in Release 6.0(1)



Note

The PIX Firewall Classic, PIX10000, and PIX 510 platforms are not supported on version 6.0(1).

New Software Features in Release 6.0(1)

AAA—Authentication, Authorization, and Accounting

The **aaa authentication** command has been modified to support HTTP authentication. The PIX Firewall allows authentication verification of the HTTP server through the **aaa authentication http console** command before PDM can access the PIX Firewall. More information about this command is available in the “[Command Reference](#)” section.

Cisco VPN Client Version 3.0

PIX Firewall version 6.0(1) supports the Cisco VPN Client version 3.0. The Cisco VPN Client is a cross-platform Virtual Private Network (VPN) client.

CiscoView Support

The existing MIB II support on PIX Firewall version 6.0(1) has been enhanced to provide PIX Firewall platform-specific Object ID in the **SNMP mib-2.system.sysObjectID** variable.

The **SNMP mib-2.system.sysObjectID** variable now provides one of the following PIX Firewall platform-specific Object IDs:

```
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa 11506 (same
as .1.3.6.1.4.1.9.1.389)
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa 11515 (same
as .1.3.6.1.4.1.9.1.390)
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa 11520 (same
as .1.3.6.1.4.1.9.1.391)
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa 11525 (same
as .1.3.6.1.4.1.9.1.392)
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa 11535 (same
as .1.3.6.1.4.1.9.1.393)
```

For other PIX Firewall platforms not mentioned in the preceding text:

```
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.ciscoPIXFirewa
11 (same as .1.3.6.1.4.1.9.1.227)
```

clear logging Command

The **clear logging** command now works in privileged mode. More information about this command is available in the “[Command Reference](#)” section.

CPU Utilization Monitoring

The **show cpu usage** command has been added to the PIX Firewall for CPU Utilization monitoring support. More information about this command is available in the “[Command Reference](#)” section.

DHCP Support

The PIX Firewall Dynamic Host Configuration Protocol (DHCP) client/server support has been extended to allow the user to automatically leverage the DNS, WINS, and domain name values obtained by the PIX Firewall DHCP client for use by the hosts served by the DHCP server.

The following commands have been modified or added to the PIX Firewall to provide DHCP client/server support:

- **ip address**
- **dhcpcd**

The **ip address** command has been enhanced to allow you to enter the number of times the PIX Firewall will poll for DHCP information. Refer to the “[Command Reference](#)” section for more information.

Failover Support for HTTP

For PIX Firewall version 6.0(1), the following commands have been modified or added to the PIX Firewall allow the stateful replication of HTTP sessions in a Stateful Failover environment:

- **failover replicate http**
- **show failover**

When HTTP replication is enabled, the **show failover** command displays the **failover replicate http** command.

Refer to the “[Command Reference](#)” section for more information.

fragment Command

The **fragment** command provides additional management of packet fragmentation and improves compatibility with NFS. Refer to the “[Command Reference](#)” section for more information.

L2TP—Layer 2 Tunnel Protocol

Layer 2 Tunneling Protocol (L2TP) is a Virtual Private Network (VPN) tunneling protocol that allows remote clients to use public networks to communicate securely with servers at private corporate networks.

PIX Firewall version 6.0(1) supports terminating the Microsoft Windows 2000 OS L2TP/IPSec client. This feature does not work with L2TP/IPSec clients from other vendors. L2TP traffic must be protected by the IPSec traffic, or the PIX Firewall will discard unsecured L2TP traffic.

The following commands have been modified or added to the PIX Firewall to provide L2TP support:

- **debug ppp**
- **show vpdn**
- **sysopt connection permit**
- **vpdn group**

- [crypto ipsec transform-set](#)

Refer to the “[Command Reference](#)” section for more information.

PDM—Cisco PIX Device Manager

The Cisco PIX Device Manager (PDM) is a browser-based configuration tool designed to help you set up, configure, and monitor your PIX Firewall graphically, without requiring an extensive knowledge of the PIX Firewall command line interface (CLI). PDM ships with every PIX Firewall running software version 6.0(1) and above.

The following commands have been modified or added to the PIX Firewall to provide this PDM support:

- [aaa authentication](#)
- [clear logging](#)
- [copy tftp flash](#)
- [http](#)
- [pdm](#)
- [Syntax Descriptionsetup](#)

Refer to the “[Command Reference](#)” section for more information.

Port Redirection

The PIX Firewall now provides static Port Address Translation (PAT) capability. This capability can be used to send multiple inbound TCP or UDP services to different internal hosts through a single global address. The global address can be a unique address, a shared outbound PAT, or shared with the external interface.

The [static](#) command has been modified to accommodate this feature. Refer to the “[Command Reference](#)” section for more information.

RADIUS Support

Two new [aaa-server](#) command options now support selection of RADIUS accounting and authentication ports. More information about this command is available in the “[Command Reference](#)” section.



Note

The *Release Notes for the Cisco Secure PIX Firewall Version 5.3.1* contained an error which included two [sysopt](#) command options, [sysopt radius acct-port](#) and [sysopt radius auth-port](#), as performing this function. Those commands were not implemented and do not exist in version 5.3.1 or any other release.

show interface Command

The [show interface](#) command has been modified to display buffer counters. Refer to the “[Command Reference](#)” section for more information.

shun Command

The **shun** command, when issued from an appropriately configured Cisco Secure IDS unit (PIX Firewall shunning is supported in Cisco Secure IDS 3.0), provides dynamic packet filtering in response to a Cisco Secure IDS signature by preventing new connections from an attacking host and disallowing packets from the attacking host on any existing connection(s). When possible, the connection that caused the event is terminated. More information about this command is available in the “[Command Reference](#)” section.

SNMP Enhancements

Support for the PIX Firewall platform-specific object IDs has been added to the **SNMP mib-2.system.sysObjectID** variable. This enhancement is necessary for [CiscoView Support](#) of the PIX Firewall.

PIX Firewall Version 6.0(1) supports up to 32 SNMP management stations.

Two new options have been added to the **snmp-server host** command to support specific configuration of trap and poll activities. Refer to the “[Command Reference](#)” section for more information.

SSL debug Support

Support for the Secure Socket Layer (SSL) protocol has been added to the **debug** command. SSL is a protocol for authenticated and encrypted communications between client and servers such as the PIX Device Manager and the PIX Firewall. Refer to the “[Debug Commands](#)” section for more information.

Voice Over IP Skinny Protocol Support

The **fixup protocol** command has been enhanced to support the Skinny Client Control Protocol (SCCP), used for IP telephony.

Refer to the “[Command Reference](#)” section for more information.

Command Reference

This section documents new or modified commands in version 6.0(1). All other commands used with this version are documented in the [Cisco PIX Firewall Configuration Guide, Version 6.0](#).

- [aaa authentication](#)
- [aaa-server](#)
- [clear logging](#)
- [copy tftp flash](#)
- [crypto ipsec transform-set](#)
- [dhcpcd](#)
- [failover replicate http](#)
- [fixup protocol](#)
- [fragment](#)
- [http](#)

- **ip address**
- **isakmp policy**
- **pdm**
- **reload**
- **service**
- **setup**
- **show cpu usage**
- **show interface**
- **show vpdn**
- **shun**
- **snmp-server host**
- **static**
- **sysopt connection permit**
- **vpdn group**

aaa authentication

The **aaa authentication** command has been modified to support PDM authentication. The PIX Firewall allows authentication verification of the HTTP server through the **aaa authentication http console** command before PDM can access the PIX Firewall.

[no] aaa authentication [serial | enable | telnet | ssh | http] console *group_tag*

Syntax Description

authentication	Enable or disable user authentication, prompt user for username and password, and verify information with the authentication server.
serial	Access verification for the PIX Firewall unit's serial console.
enable	Access verification for the PIX Firewall unit's privilege mode.
telnet	Access verification for the Telnet access to the PIX Firewall console.
ssh	Access verification for the SSH access to the PIX Firewall console.
http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM).
console	Specifies that access to the PIX Firewall console requires authentication.
<i>group_tag</i>	The AAA server group tag defined by the aaa-server command.

Defaults

If an **aaa authentication http console *group_tag*** command statement is not defined, you can gain access to the PIX Firewall (via PDM) with no username and the PIX Firewall enable password (set with the **password** command). If the **aaa** command is defined but the HTTP authentication requests a time out, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using the username **pix** and the enable password (set with the **enable password** command).

Use of the **aaa authentication** command requires that you previously used the **aaa-server** command to designate an authentication server.

The web browser prompts for the username and password with a pop-up window.

Examples

```
router(config) aaa authentication telnet console radius
```

Related Commands

- [aaa-server](#)
- [http](#) Syntax Description
- [setup](#)

aaa-server

Two new **aaa-server** commands, **aaa-server radius-authport** and **aaa-server radius-acctport**, have been added to support selection of the RADIUS server ports, which will be used for authentication and accounting.

aaa-server radius-authport *port*

aaa-server radius-acctport *port*



Note

sysopt radius acct-port and **sysopt radius auth-port**, documented in *Release Notes for the Cisco Secure PIX Firewall Version 5.3.1* were in error. Those commands do not exist.

Syntax Description

radius-authport	Sets the port number of the RADIUS server which the PIX Firewall will use for authentication functions. The default port number used for RADIUS authentication is 1645 .
radius-acctport	Sets the port number of the RADIUS server which the PIX Firewall unit will use for accounting functions. The default port number used for RADIUS accounting is 1646 .
<i>port</i>	Specifies the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions for the PIX Firewall. These port pairs are listed as assigned to authentication and accounting services on RADIUS servers: <ul style="list-style-type: none"> • 1645 (authentication), 1646 (accounting) - default for PIX Firewall • 1812 (authentication), 1813 (accounting) - alternate You can view these and other commonly used port number assignments online at the following website: http://www.isi.edu/in-notes/iana/assignments/port-numbers

Defaults

By default, the PIX Firewall listens for RADIUS on ports **1645** for authentication and **1646** for accounting.

Usage Guidelines

If your RADIUS server uses ports 1812 for authentication and 1813 for accounting, you are required to reconfigure the PIX Firewall to use ports 1812 and 1813.



Note

This is a global setting that takes effect when RADIUS service 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.

Examples

```
aaa-server radius-authport 1812
aaa-server radius-acctport 1813
```

clear logging

The **clear logging** command clears the syslog message queue accumulated by the **logging buffered** command. New to version 6.0(1), the **clear logging** command is now permitted in privileged mode.

clear logging

copy tftp flash

This command has been enhanced to allow you to copy a PDM image to Flash memory using TFTP.

copy tftp:[[*//location*] [*/pathname*]] **flash**:[**image** | **pdm**]

Syntax Description

copy tftp flash	Download Flash memory software images via TFTP without using monitor mode.
<i>location</i>	Either an IP address or a name that resolves to an IP address via the PIX Firewall naming resolution mechanism.
<i>pathname</i>	PIX Firewall must know how to reach this location via its routing table information. This information is determined by the ip address command, the route command, or also RIP, depending upon your configuration. The pathname can include any directory names in addition to the actual last component of the path to the file on the server.
image	Download the selected PIX Firewall image to Flash memory. An image you download is made available to the PIX Firewall on the next reload (reboot).
pdm	Download the selected PDM image files to Flash memory. These files are available to the PIX Firewall immediately, without a reboot.

Defaults

If the **pdm image** type is not specified, the default copies the PIX Firewall **image**.

Examples

```
copying tftp://171.69.38.195/cdisk to flash
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 2156544 bytes.
Erasing current image.
Writing 2060344 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed.
```

Related Commands

- [setup](#)

crypto ipsec transform-set

For PIX Firewall version 6.0(1), L2TP is the only protocol that can use the IPsec transport mode. PIX Firewall discards all other types of packets using IPsec transport mode.

crypto ipsec transform-set *trans-name* **mode transport**

Syntax Description

crypto ipsec transform-set	A transform set specifies one or two IPsec security protocols (either Encapsulating Security Payload (ESP) or Authentication Header (AH) or both) and specifies which algorithms to use with the selected security protocol. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.
<i>trans-name</i>	IPsec transform set name.
mode	Specify IPsec transport mode for a transform set.
transport	Windows 2000 L2TP/IPsec client uses IPsec transport mode, so you need to select transport mode on the transform set.

Usage Guidelines

A transport-mode **transform** can only be used on a **dynamic** crypto map and causes the PIX Firewall to fail if you attempt to tie a transport-mode transform to a **static** crypto map.

Examples

```
crypto ipsec transform-set myset mode transport
```

dhcpd

Dynamic Host Configuration Protocol (DHCP) client/server support has been extended to allow the user to automatically leverage the DNS, WINS and domain name values obtained by the PIX Firewall DHCP client for use by the hosts served by the DHCP server.

dhcpd auto_config [*client_ifx_name*]

Syntax Description	auto_config	Enable PIX Firewall to automatically configure DNS, WINS and domain name values from the DHCP client to the DHCP server.
	<i>client_ifx_name</i>	This optional argument supports only the outside interface at this time. When more interfaces are supported, this argument will specify which interface supports the DHCP auto_config feature.

Usage Guidelines DHCP must be enabled to use this command. Use the **dhcpd enable** command to turn on DHCP. The DHCP address pool is increased to 256 for all the PIX Firewall version 6.0(1) supported platforms. PIX 506 remains at 32.

Related Commands

- [ip address](#)

failover replicate http

The **failover replicate http** command allows the stateful replication of HTTP sessions in a Stateful Failover environment. The **no** form of this command disables HTTP replication in a Stateful Failover configuration. When HTTP replication is enabled, the **show failover** command displays the **failover replicate http** command.

[no] failover replicate http
show failover

Usage Guidelines

Enabling Stateful Failover of HTTP sessions has a significant impact on PIX Firewall system resources due to the large number of short-lived HTTP sessions. This command should be used with caution.

Examples

```
router (config)# show failover
Failover On
Cable status:Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
failover replication http
  This host:Secondary - Standby
    Active time:0 (sec)
    Interface FailLink (172.16.31.2):Normal
    Interface 4th (172.16.16.1):Normal
    Interface int5 (192.168.168.1):Normal
    Interface intf2 (192.168.1.1):Normal
    Interface outside (209.165.200.225):Normal
    Interface inside (10.1.1.4):Normal
  Other host:Primary - Active
    Active time:242145 (sec)
    Interface FailLink (172.16.31.1):Normal
    Interface 4th (172.16.16.2):Normal
    Interface int5 (192.168.168.2):Normal
    Interface intf2 (192.168.1.2):Normal
    Interface outside (209.165.200.226):Normal
    Interface inside (10.1.1.5):Normal

Stateful Failover Logical Update Statistics
Link :FailLink
Stateful Obj   xmit      xerr      rcv       rerr
General        10389     0          10392     0
sys cmd        10389     0          10388     0
up time        0         0          2         0
xlate          0         0          2         0
tcp conn       0         0          0         0
udp conn       0         0          0         0
ARP tbl        0         0          0         0
RIP Tbl        0         0          0         0

Logical Update Queue Information
          Cur      Max      Total
Recv Q:   0        1      10392
Xmit Q:   0        1      10389
```

fixup protocol

The **fixup protocol** command now supports the Skinny Client Control Protocol (SCCP), and support for the Session Initiation Protocol (SIP) has been enhanced.

fixup protocol [**protocol** **skinny** [**port**[-**port**]]

no fixup protocol [**protocol**] [**port**]

show fixup [**protocol** *protocol*]

show timeout sip

Syntax Description

fixup protocol	Performs enabling, disabling, viewing, or changing the configuration of a service or protocol through the PIX Firewall.
no	Disables the fixup of a protocol by removing all fixups of the protocol from the configuration using the no fixup command. After removing all fixups for a protocol, the no fixup form of the command or the default port is stored in the configuration.
<i>port</i>	The port over which the designated protocol travels.
protocol	Specifies the protocol to fix up.
sip	Enables SIP.
show conn state	Displays the connection state of the designated protocol.
show fixup	The show fixup command lists all values or the show fixup protocol protocol command lists an individual protocol.
show timeout	Displays the timeout value of the designated protocol.
skinny	Enables SCCP. SCCP protocol supports IP telephony and can coexist in an H.323 environment. An application layer ensures that all SCCP signaling and media packets can traverse the PIX Firewall and interoperate with H.323 terminals.

Defaults

The default for **fixup protocol sip** is 5060.

The default for **fixup protocol skinny** is 2000.

Usage Guidelines

SCCP (skinny) protocol supports IP telephony and can coexist in an H.323 environment. An application layer ensures that all SCCP signaling and media packets can traverse the PIX Firewall and interoperate with H.323 terminals.

To support SIP calls through the PIX Firewall, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Therefore, SIP is a text-based protocol and contains the IP addresses throughout the text. The packets are inspected and NAT is provided for the IP addresses.



Note

If Call Manager (CM) is configured for NAT and outside phones register to it via TFTP, the connection will fail because PIX Firewall currently does not NAT the configuration file transferred via TFTP.

For additional information about the SIP protocol see RFC 2543. For additional information about the Session Description Protocol (SDP) see RFC 2327.

fragment

The **fragment** command provides additional management of packet fragmentation and improves compatibility with NFS.

fragment size *database-limit* [*interface*]

fragment chain *chain-limit* [*interface*]

fragment timeout *seconds* [*interface*]

clear fragment

show fragment [*interface*]

Syntax Description

size	Sets the maximum number of packets in the fragment database.
chain	Specifies the maximum number of packets into which a full IP packet can be fragmented.
timeout	Specifies the maximum number of seconds that a packet fragment will wait to be reassembled after the first fragment is received before being discarded.
clear	Resets the fragment databases and defaults. All fragments currently waiting for reassembly are discarded and the size , chain , and timeout options are reset to their default values.
show	Displays the state of the fragment database: <ul style="list-style-type: none"> • Size - Maximum packets set by the size option. • Chain - Maximum fragments for a single packet set by the chain option. • Timeout - Maximum seconds set by the timeout option. • Queue - Number of packets currently awaiting reassembly. • Assemble - Number of packets successfully reassembled. • Fail - Number of packets which failed to be reassembled. • Overflow - Number of packets which overflowed the fragment database.
<i>database-limit</i>	The default is 200. The maximum is 1,000,000 or the total number of blocks.
<i>chain-limit</i>	The default is 24. The maximum is 8,200.
<i>seconds</i>	The default is 5 seconds. The maximum is 30 seconds.
<i>interface</i>	The PIX Firewall interface. If not specified, the command will apply to all interfaces.

Usage Guidelines

In general, the default values should be used. However, if a large percentage of the network traffic through the PIX Firewall is NFS, additional tuning may be necessary to avoid database overflow. See system log message 209003 for additional information.

In an environment where the MTU between the NFS server and client is small, such as a WAN interface, the **chain** option may require additional tuning. In this case, NFS over TCP is highly recommended to improve efficiency.

Setting the *database-limit* of the **size** option to a large value can make the PIX Firewall more vulnerable to a DoS attack by fragment flooding. Do not set the *database-limit* equal to or greater than the total number of blocks. The default values will limit DoS due to fragment flooding to that interface only.

http

New **http** commands allow you to enable the PIX Firewall HTTP server and specify the clients that are allowed to access it.

http *ip_address* [*netmask*] [*if_name*]

no http *ip_address netmask if_name*

[no] http server enable

clear http

show http



Note

The HTTP server must be enabled to configure and monitor the PIX Firewall through PDM.

Syntax Description

http	Relating to the Hypertext Transfer Protocol.
<i>ip_address</i>	Specifies the host or network authorized to initiate an HTTP connection to the PIX Firewall.
<i>netmask</i>	Specifies the network mask for the http <i>ip_address</i> .
<i>if_name</i>	PIX Firewall interface name on which the host or network initiating the HTTP connection resides.
http server enable	Enables the HTTP server required to run PDM.
clear http	Removes all HTTP hosts and disables the server.
show http	Lists the allowed hosts and the enable state of the HTTP server.

Defaults

If you do not specify a netmask, the default is **255.255.255.255** regardless of the class of IP address. The default *if_name* is **inside**.

Usage Guidelines

Access from any host will be allowed if **0.0.0.0 0.0.0.0** (or **0 0**) is specified for *ip_address* and *netmask*.

Examples

The following **http** command example is used for one host:

```
http 16.152.1.11 255.255.255.255 outside
```

The following **http** command example is used for any host:

```
http 0.0.0.0 0.0.0.0 inside
```

ip address

The **ip address** command has been enhanced to allow you to enter the number of times the PIX Firewall will poll for DHCP information.

ip address outside dhcp [setroute] [retry *retry_cnt*]

Syntax Description

dhcp	Specifies PIX Firewall will use DHCP to poll for information.
outside	Interface from which the PIX Firewall will poll for information.
setroute	Tells the PIX Firewall to set the default route using the default gateway parameter the DHCP server returns.
retry	Enables PIX Firewall to retry a poll for DHCP information.
<i>retry_cnt</i>	Specifies the number of times PIX Firewall will poll for DHCP information. The values available are 4 to 16. If no value is specified, the default is 4.

By default the PIX Firewall will not retry to poll for DHCP information. The default value for *retry_cnt* is 4.

Examples

```
ip address outside dhcp retry 10
```

Related Commands

- [dhcpcd](#)

isakmp policy

The **isakmp policy** command allows you to negotiate IPSec security associations and enable IPSec secure communications.

isakmp policy [*priority*] group 2

Syntax Description

<i>priority</i>	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.

Usage Guidelines

Cisco VPN Client version 3.0 uses Diffie-Hellman group 2 and VPN Client version 2.5 uses Diffie-Hellman group 1. If you are using Cisco VPN Client version 3.0, configure Diffie-Hellman group 2 by using the **isakmp policy** command.

To configure Diffie-Hellman group identifier two, use the **isakmp** command as noted in the “[Command Reference](#)” section of the *Cisco PIX Firewall IPSec User Guide, Version 6.0*.

**Note**

The Cisco VPN Client version 3.0 does not require the **crypto map *map-name* client configuration address initiate | respond** command.

Examples

```
isakmp policy 93 group 2 n
```

pdm

A new family of commands support PDM communication with a PIX Firewall over an HTTP server. The **pdm disconnect** command allows you to disconnect a specific PDM session using a *session_id* obtained with the **show pdm sessions** command. The **show pdm sessions** command lists all the open PDM sessions going to a PIX Firewall.

**Note**

The **pdm disconnect** command, and the **show pdm sessions** command are accessible through the command line. The **clear pdm**, **pdm history commands**, **pdm location**, and **pdm logging** commands may appear in your configuration and are available through the CLI, but they are designed to work as internal PDM-to-PIX Firewall commands accessible through PDM.

clear pdm

pdm disconnect *session_id*

show pdm sessions

[no] **pdm history enable**

show pdm history [view {all|12h|5d|60m|10m}][snapshot] [feature {all|blocks|cpul|failover|ids|interface *if_name*|memory|perfmon|xlates}][pdmclient]

pdm location *ip_address netmask if_name*

pdm logging [level [*messages*]]

no pdm logging

show pdm logging

Syntax Description

pdm	Pertaining to the Cisco PIX Device Manager.
clear pdm	Removes all locations, disables logging, and clears the PDM buffer. Internal PDM command.
pdm disconnect	Disconnects the specified PDM session from the PIX Firewall.
<i>session_id</i>	PDM session ID number available from the show pdm sessions command.
show pdm sessions	Displays a <i>session_id</i> for each active PDM session to the PIX Firewall, beginning with session number 0.
history enable	Internal PDM command. Take a data sample and store the sample data to the PDM history buffer. The no version of this command disables PDM data sampling.
show pdm history	Internal PDM command. Displays the contents of the PDM history buffer.
12h 5d 60m 10m all	Specifies the PDM history view to display: 12 hours (12h), 5 days (5d), 60 minutes (60m), 10 minutes (10m), or all history contents in the PDM history buffer.

snapshot	Displays only the last PDM history data point.
pdmclient	Displays the PDM history in PDM-display format.
location	Internal PDM command. Associates an interface with an IP address.
<i>ip_address</i>	Specifies the host or network.
<i>netmask</i>	Specifies the network mask for the pdm location <i>ip_address</i> .
<i>if_name</i>	Specifies the interface name for the pdm location <i>ip_address</i> .
logging	Internal PDM command. Specifies the type and number of syslog messages displayed through the PDM syslog option.
<i>level</i>	Specifies the priority level of syslog messages displayed in the PDM syslog option.
<i>messages</i>	Specifies the number of messages stored in the PDM buffer. Once the buffer is full, old messages will be discarded.
show pdm logging	Internal PDM command. Displays the contents of the PDM buffer within PDM.

Defaults

Default PDM syslog *level* is **0**. Default logging *messages* is **100** and the maximum is **512**.

Usage Guidelines

The **pdm location** command can only associate one interface to an *ip_address* *netmask* pair. Specifying an existing pair will replace the old definition. The PDM syslog messages are stored separately from the PIX Firewall syslog accessed through the **logging buffered** command.

Examples

This example shows how to report the last data point in PDM-display format:

```

pix(config)# show pdm history 10m snapshot pdmclient
INTERFACE|outside|up|IBC|0|OBC|1088|IPC|0|OPC|0|IBR|17|OBR|0|IPR|0|OPR|0|IERR|1|NB|0|RB|0|
RNT|0|GNT|0|CRC|0|FRM|0|OR|0|UR|0|OERR|0|COLL|0|LCOLL|0|RST|0|DEF|0|LCR|0:PIXoutsideINTERF
ACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|1952|METRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTORY
|SNAP|IPR|VIEW|10|17|METRIC_HISTORY|SNAP|OPR|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0|
METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:PIXinsideINTERFACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|0|M
ETRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTORY|SNAP|IPR|VIEW|10|0|METRIC_HISTORY|SNAP|OP
R|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0|METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:PIXSYS:
METRIC_HISTORY|SNAP|MEM|VIEW|10|52662272|METRIC_HISTORY|SNAP|BLK4|VIEW|10|1600|METRIC_HIST
ORY|SNAP|BLK80|VIEW|10|400|METRIC_HISTORY|SNAP|BLK256|VIEW|10|998|METRIC_HISTORY|SNAP|BLK1
550|VIEW|10|676|METRIC_HISTORY|SNAP|XLATES|VIEW|10|0|METRIC_HISTORY|SNAP|CONNS|VIEW|10|0|M
ETRIC_HISTORY|SNAP|TCPCONNS|VIEW|10|0|METRIC_HISTORY|SNAP|UDPCONNS|VIEW|10|0|METRIC_HISTOR
Y|SNAP|URLS|VIEW|10|0|METRIC_HISTORY|SNAP|WEBSNS|VIEW|10|0|METRIC_HISTORY|SNAP|TCPFIXUPS|V
IEW|10|0|METRIC_HISTORY|SNAP|TCPINTERCEPTS|VIEW|10|0|METRIC_HISTORY|SNAP|HTPPFIXUPS|VIEW|1
0|0|METRIC_HISTORY|SNAP|FTPPFIXUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAAUTHENUPS|VIEW|10|0|MET
RIC_HISTORY|SNAP|AAAAUTHORUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAACCOUNTS|VIEW|10|0|

```

This example shows how to report the last data point in non-PDM format:

```

pix(config)# show pdm history 10m snapshot
INTERFACE|outside|up|IBC|0|OBC|1344|IPC|0|OPC|0|IBR|21|OBR|0|IPR|0|OPR|0|IERR|1|NB|0|RB|0|
RNT|0|GNT|0|CRC|0|FRM|0|OR|0|UR|0|OERR|0|COLL|0|LCOLL|0|RST|0|DEF|0|LCR|0
:PIX outside INTERFACE:
Input Byte Count: [ 10s] : 1952
Output Byte Count: [ 10s] : 64
Input Packet Count: [ 10s] : 17
Output Packet Count: [ 10s] : 1
Input Error Packet Count: [ 10s] : 0

```

```

Output Error Packet Count: [ 10s] : 0
:PIX inside INTERFACE:
Input Byte Count: [ 10s] : 0
Output Byte Count: [ 10s] : 64
Input Packet Count: [ 10s] : 0
Output Packet Count: [ 10s] : 1
Input Error Packet Count: [ 10s] : 0
Output Error Packet Count: [ 10s] : 0
MEM|50479104
BLOCK|BLK4|1600|BLK80|0|BLK256|400|BLK1550|0|BLK1552|997|BLK2560|0|BLK4096|1188|BLK8192|0|
BLK16384|0|BLK65536|0
Available Memory: [ 10s] : 52662272
Available 4 bytes Blocks: [ 10s] : 1600
Available 80 bytes Blocks: [ 10s] : 400
Available 256 bytes Blocks: [ 10s] : 998
Available 1550 bytes Blocks: [ 10s] : 676
PERFMON|XLATES|0|CONNECTIONS|0|TCP CONNS|0|UDP CONNS|0|URLS|0|WEBSNS|0|TCP FIXUP|0|TCP
INTERCEPT|0|HTTP FIXUP|0|FTP FIXUP|0|AAA AUTHEN|0|AAA AUTHOR|0|AAA ACCOUNT|0
Xlate Count: [ 10s] : 0
Connection Count: [ 10s] : 0
TCP Connection Count: [ 10s] : 0
UDP Connection Count: [ 10s] : 0
URL Filtering Count: [ 10s] : 0
WEBSNSE Filtering Count: [ 10s] : 0
TCP Fixup Count: [ 10s] : 0
TCP Intercept Count: [ 10s] : 0
HTTP Fixup Count: [ 10s] : 0
FTP Fixup Count: [ 10s] : 0
AAA Authentication Count: [ 10s] : 0
AAA Authorzation Count: [ 10s] : 0
AAA Accounting Count: [ 10s] : 0

```

Related Commands

- [copy tftp flash](#)
- [http](#)
- [setup](#)

reload

The **reload** command has been enhanced with the new option **noconfirm**. It permits the PIX Firewall without user confirmation.

reload noconfirm

Syntax Description

reload	Reboot and reload configuration.
noconfirm	Permits the PIX Firewall to reload without user confirmation.

Usage Guidelines

The PIX Firewall does not accept abbreviations to the keyword **noconfirm**.

Command History

The **noconfirm** option was added to the **reload** command for PIX Firewall version 6.0(1).

Examples

```
reload noconfirm
```

service

This command has been enhanced with the **resetoutside** option. The **resetoutside** option allows the PIX Firewall to quickly terminate the identity request (IDENT) from an external SMTP or FTP server. Actively resetting these connections avoids the 32 second time-out delay. This option is recommended with dynamic or static interface PAT (available with 6.0(1)).

```
service {resetinbound | resetoutside}
```

setup

The **setup** command allows you to provide pre-configuration information to a new PIX Firewall, so you can then configure and monitor your PIX Firewall graphically using PDM.

setup

```
Pre-configure PIX Firewall now through interactive prompts [yes]?
Enable Password [<use current password>]:
Clock (UTC)
  Year [system year]:
  Month [system month]:
  Day [system day]:
  Time [system time]:
Inside IP address:
Inside network mask:
Host name:
Domain name:
IP address of host running PIX Device Manager:
```

Syntax Description

setup	Prompts for the basic operational information for the PIX Firewall if no configuration is found in the Flash memory.
Enable password:	Specify an enable password for this PIX Firewall unit.
Clock (UTC)	Set the PIX Firewall clock to Universal Coordinated Time (also known as Greenwich Mean Time).
Year [system year]:	Specify current year, or default to the year stored in the host computer.
Month [system month]:	Specify current month, or default to the month stored in the host computer.
Day [system day]:	Specify current day, or default to the day stored in the host computer.
Time [system time]	Specify current time in <i>hh:mm:ss</i> format, or default to the time stored in the host computer.
Inside IP address:	Network interface IP address of the PIX Firewall unit.
Inside network mask:	A network mask that applies to <i>inside</i> IP address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0 .
Host name:	The host name you want to display in the PIX Firewall command line prompt.
Domain name:	The DNS domain name of the network on which the PIX Firewall runs, for example <i>cisco.com</i> .

IP address of host running PIX Device Manager:	IP address on which PDM connects to the PIX Firewall.
Use this configuration and write to flash?	Store the new configuration to Flash memory. Same as the write memory command. If the answer is yes , the inside interface will be enabled and the requested configuration will be written to Flash memory. If the user answers anything else, the setup dialog repeats using the values already entered as the defaults for the questions.

Usage Guidelines

A PIX Firewall requires some initial configuration before PDM can connect to it. The setup dialog appears, via the console, at boot time if there is no configuration in the Flash memory. You can also access the **setup** command by typing **setup** from the Config mode.

The dialog asks for the inside IP address, network mask, host name, domain name and PDM host. The host and domain names are used to generate the default certificate for the SSL connection. The interface type is determined from the hardware.

Examples

The following example shows how to complete the **setup** command prompts.

```
router (config)# setup
Pre-configure PIX Firewall now through interactive prompts [yes]? y
Enable Password [<use current password>]: ciscopix
Clock (UTC)
  Year [2001]: 2001
  Month [Aug]: Sep
  Day [27]: 12
  Time [22:47:37]: <Enter>
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting_pix
Domain name: example.com
IP address of host running PIX Device Manager: 192.168.1.2
```

```
The following configuration will be used:
Enable Password: ciscopix
Clock (UTC): 22:47:37 Sep 12 2001
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting_pix
Domain name: example.com
IP address of host running PIX Device Manager: 192.168.1.2
```

```
Use this configuration and write to flash? y
```

Related Commands

- [aaa authentication](#)
- [copy tftp flash](#)
- [http](#)

show cpu usage

The **show cpu usage** command displays CPU utilization. This command is now permitted from privileged or configuration mode.

show cpu usage

Examples

The following example shows the new output:

```
CPU utilization for 5 seconds: p1%; 1 minute: p2%; 5 minutes: p3%
```

A more generic form of the output is:

```
CPU utilization for 5 seconds: p1%; 1 minute: p2%; 5 minutes: p3%
```

where:

- *p1* is the percentage utilization for 5 seconds.
- *p2* is the average percentage utilization for 1 minute.
- *p3* is the average percentage utilization for 5 minutes.

The percentage usage will be printed as NA (not available) if the usage is not available for any of the time intervals. This can happen if the user asks for CPU usage before the 5-second, 1-minute, or 5-minute time interval has elapsed.

show interface

The **show interface** command displays network interface information. The **show interface** command has been enhanced to include buffer counters. The buffer counters are only valid for Ethernet interfaces.

show interface

Usage Guidelines

Use the **show interface** command to view information about the interface. The **show interface** command displays the packet drop count of Unicast RPF for each interface. This value appears as the “unicast rpf drops” counter.

Examples

The following example shows the new output:

```
pix# 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 unicast rpf drops
    0 output errors, 28075 collisions, 0 interface resets
    0 babbles, 0 late collisions, 117573 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/1)
    output queue (curr/max blocks): hardware (0/2) software (0/1)
...

```

The counters in the last two lines are as follows:

- Input queue—the input (receive) hardware and software queue.
 - Hardware—(current and maximum blocks). The number of blocks currently present on the input hardware queue, and the maximum number of blocks previously present on that queue. In the example, there are currently 128 blocks on the input hardware queue, and the maximum number of blocks ever present on this queue was 128.
 - Software—(current and maximum blocks). The number of blocks currently present on the input software queue, and the maximum number of blocks previously present on that queue. In the example, there are currently 0 blocks on the input software queue, and the maximum number of blocks ever present on this queue was 1.
- Output queue—the output (transmit) hardware and software queue.
 - Hardware—(current and maximum blocks). The number of blocks currently present on the output hardware queue, and the maximum number of blocks previously present on that queue. In the example, there are currently 0 blocks on the output hardware queue, and the maximum number of blocks ever present on this queue was 2.
 - Software—(current and maximum blocks). The number of blocks currently present on the output software queue, and the maximum number of blocks previously present on that queue. In the example, there are currently 0 blocks on the output software queue, and the maximum number of blocks ever present on this queue was 1.

For Fast Ethernet and Gigabit Ethernet interfaces, the current and maximum count for the number of blocks on the input (receive) queue will always be the same. Currently the count is 128 for Fast Ethernet and 63 for Gigabit Ethernet. The number of blocks on the receive queue is always fixed.

show vpdn

The **show vpdn** command has been enhanced to display L2TP tunnel and session information.

show vpdn tunnel [**l2tp** | **pptp**] [**id** *tunnel_id* | **packets** | **state** | **summary** | **transport**]

show vpdn session [**l2tp** | **pptp**] [**id** *session_id* | **packets** | **state** | **window**]

The **l2tp** and **pptp** command options display either the L2TP or PPTP tunnel information. The PIX Firewall shows both tunnel protocols if this option is not specified.

Syntax	Description
show vpdn tunnel	Display tunnel information.
show vpdn session	Display session information.
l2tp pptp	Select either l2tp or pptp to display that tunnel information. The PIX Firewall shows both tunnel protocols if this option is not specified.
id	Identify tunnel or session.
<i>tunnel_id</i>	Unique tunnel identifier.
<i>session_id</i>	Unique session identifier.
packets state summary transport	Display tunnel packets, state, summary, or transport information.
packets state window	Display session packets, state, or window information.

Examples

The following example shows a display for the **show vpdn tunnel l2tp** command:

```

pix# show vpdn tunnel l2tp

L2TP Tunnel Information (Total tunnels=1 sessions=1)

Tunnel id 1 is up, remote id is 7, 1 active sessions
Tunnel state is established, time since change 12 secs
Remote Internet Address 171.69.39.85, port 1701
Local Internet Address 172.23.58.48, port 1701
15 packets sent, 48 received, 377 bytes sent, 4368 received
Control Ns 3, Nr 4
Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 2
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
pix#

```

The following example lists the **show vpdn tunnel** command:

```

pix# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)

Tunnel id 1 is up, remote id is 7, 1 active sessions
Tunnel state is established, time since change 12 secs
Remote Internet Address 171.69.39.85, port 1701
Local Internet Address 172.23.58.48, port 1701
15 packets sent, 48 received, 377 bytes sent, 4368 received
Control Ns 3, Nr 4
Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 2
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
% No active PPTP tunnels
pix#

```

The following example lists the **show vpdn session** command:

```

pix# show vpdn session

L2TP Session Information (Total tunnels=1 sessions=1)

Call id 1 is up on tunnel id 1
Remote tunnel name is abc-win2ke2
Internet Address is 171.69.39.85
Session username is guest, state is established
Time since change 158 secs, interface outside
Remote call id is 1
PPP interface id is 1
15 packets sent, 83 received, 377 bytes sent, 8412 received
Sequencing is off

% No active PPTP tunnels

```

shun

The **shun** command allows a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. The **shun** command is intended for use primarily by a Cisco Secure IDS device.

```
[no] shun src_ip [dst_ip sport dport [protocol]]
clear shun [statistics]
show shun src_ip
```

Syntax Description

shun	Enable a blocking function (shun) based on <i>src_ip</i> .
no	Disable a shun based on <i>src_ip</i> , the actual address used by the PIX Firewall for shun lookups.
clear	Disable all shuns currently enabled and clears shun statistics. Specifying statistics only clears the counters for that interface.
show	Display all shuns currently enabled in the exact format specified.
<i>src_ip</i>	The address of the attacking host.
<i>dst_ip</i>	The address of the of the target host.
<i>sport</i>	The source port of the connection causing the shun.
<i>dport</i>	The destination port of the connection causing the shun.
<i>protocol</i>	The optional IP protocol, such as UDP or TCP.
<i>statistics</i>	Clear only interface counters.

Defaults

If the **shun** command is used only with the source IP address of the host, then the other defaults will be 0. No further traffic from the offending host will be allowed.

Usage Guidelines

The **shun** command applies a blocking function to the interface receiving the attack. Packets containing the IP source address of the attacking host will be dropped and logged until the blocking function is removed manually or by the Cisco Secure IDS master unit. No traffic from the IP source address will be allowed to traverse the PIX Firewall unit and any remaining connections will time out as part of the normal architecture. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

Examples

In the following example, the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the PIX Firewall connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

if the **shun** command is applied in the following way:

```
shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The preceding command would delete the connection from the PIX Firewall connection table, and it would also prevent packets from 10.1.1.27 from going through the PIX Firewall. The offending host can be inside or outside of the PIX Firewall.

snmp-server host

PIX Firewall version 6.0(1) supports up to 32 SNMP management stations. The **snmp-server host** command has been modified to facilitate finer granularity in configuring trap and poll activities. There are two enhanced **snmp-server host** command options.

```
snmp-server host [if_name] ip_addr [trap | poll]
```

Syntax Description

snmp-server host	Specify an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come. You can specify up to 32 SNMP management stations.
<i>if_name</i>	The interface name where the SNMP management station resides.
<i>ip_addr</i>	The IP address of a host to which SNMP traps should be sent and/or from which the SNMP requests come.
trap poll	Specify whether traps, polls, or both are acted upon. Use with these parameters: <ul style="list-style-type: none"> trap—Only traps will be sent. This host will not be allowed to poll. poll—Traps will not be sent. This host will be allowed to poll. The default allows both traps and polls to be acted upon.

Defaults

If you do not specify either option, the **snmp-server host** command behaves as in previous versions. The polling is permitted from all configured hosts on the affected interface. Traps are sent to all configured hosts on the affected interface.

Usage Guidelines

Use the **trap** and **poll** command options to configure hosts to participate only in specific SNMP activities. Poll responses and traps are sent only to the configured entities. Hosts configured with the **trap** command option will have traps sent to them, but will not be allowed to poll. Hosts configured with the **poll** command option will be allowed to poll, but will not have traps sent to them.

Accessibility to the PIX Firewall MIBs is based on configuration, MIB support, and authentication based on the community string. Unsuccessful polling attempts, except for failed community string authentication, are not logged or otherwise indicated. Community authentication failures result in a trap where applicable.

Examples

```
snmp-server host perimeter 10.1.2.42 trap poll
```

static

This command has been modified to allow TCP and UDP port redirection.

```
static [(internal_if_name, external_if_name)] {tcp | udp} {global_ip | interface} global_port local_ip
local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]
```

Syntax Description

<i>internal_if_name</i>	The internal network interface name. The higher security level interface you are accessing.
<i>external_if_name</i>	The external network interface name. The lower security level interface you are accessing.
tcp	Specifies TCP port redirection.
udp	Specifies UDP port redirection.
<i>global_ip</i>	The global IP address used for redirection.
interface	The outside interface address is taken to be the global address.
<i>global_port</i>	Global TCP or UDP port for port redirection.
<i>local_port</i>	Local TCP or UDP port for port redirection.
<i>global_ip</i>	A global IP address. The IP address on the lower security level interface you are accessing.
<i>local_ip</i>	The local IP address from the inside network. The IP address on the higher security level interface you are accessing.
netmask	Reserve word required before specifying the network mask.
<i>mask</i>	Mask pertains to both <i>global_ip</i> and <i>local_ip</i> . For host addresses, always use 255.255.255.255. For network addresses, use the appropriate class mask or subnet mask; for example, for Class A networks, use 255.0.0.0. An example subnet mask is 255.255.255.224.
<i>max_conns</i>	The maximum number of connections permitted through the static at the same time.
<i>em_limit</i>	The embryonic connection limit. An embryonic connection is one that has started but not yet completed. Set this limit to prevent attack by a flood of embryonic connections. The default is 0, which means unlimited connections.
norandomseq	Do not randomize the TCP/IP packet's sequence number. Only use this option if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Use of this option opens a security hole in the PIX Firewall.

Usage Guidelines

If the **tcp** or **udp** keyword is specified, a static UDP or TCP port redirection is configured. If the **interface** keyword is specified, the outside-interface address is taken to be the global IP address.



Note

A **conduit** or **access-list** command statement must be configured in addition to the **static** command to enable an inbound connection.

Examples

This example redirects Telnet traffic from the PIX Firewall unit's outside interface to inside host 10.1.1.15:

```
static (inside,outside) tcp interface telnet 10.1.1.15 telnet
```

This example redirects FTP traffic to the PIX Firewall outside interface to inside host 10.1.1.30:

```
static (inside,outside) tcp interface ftp 10.1.1.15 ftp
```

This example redirects DNS traffic to the PIX Firewall outside interface to inside host 10.1.1.30:

```
static (inside,outside) udp interface domain 10.1.1.30 domain
```

This example redirects all traffic to the PIX Firewall outside interface to inside host 10.1.1.15:

```
static (inside, outside) interface 10.1.1.15
```

sysopt connection permit

This **sysopt connection permit-12tp** command allows L2TP traffic to bypass conduit or **access-list** command statement checking. The **sysopt connection permit-ipsec** command implicitly permits all L2TP or IPSec traffic.

```
sysopt connection permit-12tp
sysopt connection permit-ipsec
```

Syntax Description

permit-12tp	Allows L2TP traffic to bypass conduit or access-list command statement checking.
permit-ipsec	Allows IPSec traffic to bypass conduit or access-list command statement checking.

Usage Guidelines

There is no need to enter the **sysopt connection permit-12tp** command if the **sysopt connection permit-ipsec** command is present.

Examples

```
sysopt connection permit-12tp
```

vpdn group

New functionality has been added to implement the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunnelling Protocol (L2TP) feature within virtual private dial-up network (VPDN) groups.

```
vpdn group group_name accept dialin [pptp | l2tp]
vpdn group group_name l2tp tunnel hello [hello_timeout]
vpdn group group_name client accounting [aaa_server_tag]
```

Syntax Description

vpdn group	Identify the virtual private dial-up network group.
<i>group_name</i>	An ASCII string identifying a VPDN group. Maximum <i>group_name</i> length is 128 bytes.
accept dialin	Accept PPTP or L2TP dial-in request.
pptp l2tp	Select PPTP or L2TP protocol.
l2tp tunnel hello	Specify the L2TP keep-alive hello timeout value. The default is 60 seconds if not specified. The minimum is 10 seconds and maximum is 300 seconds.
<i>hello_timeout</i>	Tunnel hello keep-alive message timeout period (in seconds).
client accounting	Generate AAA accounting start and stop record for the L2TP (and PPTP) session.
<i>aaa_server_tag</i>	The <i>aaa_server_tag</i> defined from the aaa-server command. The AAA server does not need to be the same server as the AAA authentication server.

Usage Guidelines

The accounting record consists of the following fields:

<i>user-name</i>	Login username.
<i>caller-id</i>	Client's IP address.
<i>acct-flag</i>	Start or stop.
<i>elapsed_time</i>	The duration of the session.
<i>bytes_in/bytes_out</i>	Input and output byte count.
<i>task_id</i>	A unique ID to identify a task.
<i>Nas-P-addr</i>	Address of PIX Firewall.

Examples

The following examples show different configurations of the **vpdn group** command.

```
vpdn group 1 accept dialin l2tp
vpdn group 1 l2tp tunnel hello 60
vpdn group 1 client accounting myaaa
```

Related Commands

- **aaa-server**

Debug Commands

This section documents new or modified **debug** commands in release 6.0(1). All other commands used with this release are documented in the *Cisco PIX Firewall IPSec User Guide, Version 6.0*.

- [service](#)
- [debug ppp](#)
- [debug sip](#)
- [debug ssl](#)

debug pdm history

The **debug pdm history** command turns on the PDM history metrics debugging information. The **no** version of this command disables PDM history metrics debugging.

[no] debug pdm history

debug ppp

There are three new **debug ppp** command options supporting Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) and Microsoft CHAP (MS-CHAP).

debug ppp io lerror | uauth | upap | chap | negotiation

Syntax Description	
upap	Turn on debug for PAP authentication.
chap	Turn on debug for CHAP/MS-CHAP authentication.
negotiation	Equivalent of the error , uauth , upap and chap debug command options.

debug sip

Allows users to enable debugging of the fixup SIP (Session Initiation Protocol) module.

[no] debug sip

Syntax Description	
debug sip	Debug packets or tracings through the PIX Firewall.

debug ssl

Debug information and error messages associated with the **ssl** command.

[no] **debug ssl** [**cypher** | **device**]

Syntax Description	debug	ssl	cypher	device
	Debug packets or tracings through the PIX Firewall.	Enable SSL packet debugging.	Display information about the cipher negotiation between the HTTP server and the client.	Display information about the SSL device including session initiation and ongoing status.

Defaults

If no parameters are specified, both **cypher** and **device** are enabled or disabled.

Related Commands

- [ca generate rsa key](#)

Important Notes

The following section describes important notes for the 6.0(1) release.

aaa authentication

Configure the access-list specified in Attribute 11 (specifies per-user access-list name) on the PIX Firewall. Otherwise, remove Attribute 11 from the aaa RADIUS server configuration if no access-list is intended for user authentication. If the access-list is not configured on the PIX Firewall when the user attempts to login, the login will fail.

Downloading PIX Firewall image

Fast Ethernet cards in 64-bit slots are not visible in monitor mode. This problem means that the TFTP server cannot reside on one of these interfaces. The user should use the **copy tftp flash** command to download the PIX Firewall image file via TFTP.

DHCP Server Functionality

The functionality of the DHCP server on the PIX Firewall has been changed to allow users to define a pool of up to 256 DHCP addresses on the PIX 515 and larger platforms. The PIX 506 remains at 32 addresses.

Restrictions

Version 6.0(1) does not support FDDI, PL2, or Token Ring interfaces.

Version 6.0.(1) and above no longer support PFM; PFM is replaced by the PIX Device Manager. However, the PFM thread is still on and is being used by CSPM to communicate with the PIX.

Caveats

The following sections describe the open caveats for the 6.0(1) release.



Note

Please use Bug Toolkit on Cisco.com to view additional caveat information. Bug Toolkit may be accessed at the following website:

http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml

Open Caveats

The caveats in [Table 1](#) are yet to be resolved in this release.

Table 1 *Open Caveats*

DDTS Number	Description
CSCds10112	The system reloads after experiencing continuous denied enroll attempts.
CSCds29190	The PIX Firewall fails over silently when generating an RSA key the size of 2048.
CSCds54310	The PIX crypto map can become corrupted when multiple show crypto commands are issued while the VPN client is running.
CSCds60366	The PIX Firewall reloads after being unable to establish a tunnel.
CSCds80108	Cisco Secure Intrusion Detection System (Cisco Secure IDS) signature number 1101 is not supported by PIX Firewall. When attempted to be accessed, PIX Firewall returns an incorrect error message: Invalid signature number.
CSCds83357	If the certificates and keys are changed, under some circumstances, the PIX Firewall reloads if it is then unable to establish a tunnel.
CSCds89340	If the user enables "debug skinny," the messages accumulate to a certain size and triggers the Watchdog Timeout. Workaround: Do not enable the "debug skinny".
CSCdt09454	The primary unit's large configuration did not synchronize to the secondary unit.
CSCdt21999	The graphing tables do not load in realtime with Internet Explorer and PDM history metrics disabled on the PIX Firewall. Workaround: Enable PDM history metrics on your PIX Firewall. This is the default setting.

Table 1 Open Caveats (continued)

DDTS Number	Description
CSCdt51419	The logging settings on the PIX Firewall are not shown in the configuration when it is configured for no logging on . The logging settings (such as logging monitor debug , etc.) are shown under show logging but not show configuration . When logging is on, then the logging settings show up.
CSCdt58542	Configure the access-list specified in Attribute 11 (specifies per-user access-list name) on the PIX Firewall. Otherwise, remove Attribute 11 from the AAA RADIUS server configuration if no access-list is intended for user authentication. If the access-list is not configured on the PIX Firewall when the user attempts to log in, the login will fail.
CSCdt63922	Fast Ethernet cards in 64-bit slots are not visible in monitor mode. This problem means that the TFTP server cannot reside on one of these interfaces. The user should use the copy tftp flash command to download the PIX Firewall image file via TFTP.
CSCdt73216	This problem is seen only when an outbound call is made and the outside phone places an inside phone on hold. The Re-INVITE was denied. Workaround: Configure a conduit to allow the Re-INVITE into the inside Gateway for port 5060.
CSCdt77025	Sporadically, under automated IPSec stress testing, the system indicates that an internal memory packet block has become corrupted.
CSCdt78562	When a refresh is requested, a message dialog is sent: "PDM is unable to get the current version information about your PIX. Your PIX may be unreachable for this moment." This can give the appearance that the PDM is hanging. The solution would be to open this window as a Frame and not as a dialog message. If this window is a Frame, it will be seen on the task bar and will be easier for the user to locate it. Workaround: The only way to get to the message is to use the alt-tab to the PDM window.
CSCdt79999	When initially bringing up a graph in Internet Explorer, it occasionally picks up one or two extra data points. The table is correct though.
CSCdt81787	Refresh time for PDM is 3 minutes with Sun Sparc Ultra-2/Solaris 2.8/296 MHz/512 MB/Netscape 4.76 and 10 seconds with Windows NT 4.0/500 MHz/128 MB/Internet Explorer 5.50 for 100 KB configuration.
CSCdt83330	The command buffer does not clear after discarding.
CSCdt83450	Many of the realtime graphs are showing the same information as in the 10m graph. They should show the information from the time they are opened.
CSCdt87109	The system slows down and the screen may not refresh properly. The Java console reports a ComFailException error as PDM loads (Low System Resources). This problem typically occurs with Internet Explorer on Windows ME 9. It may happen on other platforms as well and also in Netscape. If you run PDM and close the PDM window without closing the browser, and then launch PDM again, each time you do this, it consumes more resources, approximately 10% more each time. Eventually, you will run out of resources and the system starts behaving erratically.
CSCdt90421	Memory is not released after clearing all IPSec and ISA SAS connections.

Table 1 Open Caveats (continued)

DDTS Number	Description
CSCdt92714	In the Hosts/Networks tab on PDM, a network object is edited but no changes are applied. PDM always asks to apply the changes and it does not verify if there are changes or not.
CSCdt93673	Call forwarding from the SIP Proxy server does not work in a single or double PIX Firewall scenario when the call is forwarded to a SIP gateway.
CSCdt94747	Interoperability occurs when using the command fixup protocol H3231720 between a Skinny phone (on the outside) and a Gateway (with a POTs phone) on the inside of a network.
CSCdu00850	NICs (network interface cards) that use the 82542 controller chip are not recommended for installation in the PIX 525. It will result in degraded performance.
CSCdu01836	PIX Device Manager sessions are not released after closing all of the browsers.
CSCdu03550	At startup time, PDM seems frozen if you are using Solaris 2.8, CDE 1.4, Netscape 4.7x environments, but continues to load when you move the mouse.
CSCdu08222	PDM does not accept an 'any any' destination address when 'static' is not defined when adding a Rule.
CSCdu09113	In the multiple-line command window, it is not clear how to paste a CLI into this window. Right-clicking does not work. The only way to paste CLIs into the command window is to use Ctrl-v.
CSCdu10483	PIX Firewall version 6.0.1 does not delete the ISA SAS if the peer does not negotiate SA.
CSCdu10680	When you copy and paste multiple CLI commands in the CLI window, not all of the commands are configured on the PIX Firewall and there are no errors reported. This problem occurs when you configure the hostname or password in PDM using the CLI window in the multiple line command mode.
CSCdu10826	When configuring the TFTP server on the outside interface by using PDM, the configuration file name defaults to a TFTP directory name. We just need a file name not a directory/file name.
CSCdu12321	The PIX Firewall fails to perform the write memory command when a long command line precedes it.
CSCdu12552	On some Linux machines running only Netscape, when you select an item on the System Properties tab or the Monitoring tab, the entire PDM window shifts up a few pixels to the left and up. Eventually, the title bar of the PDM window may move out of view. On some window managers, you may have to right-click on the edge of the window to get a menu so that you can move the PDM window back into view. On other window managers, pressing the middle mouse button on the edge of the window and dragging it will move the window.
CSCdu12628	The user may have to wait without any hour-glass signal from the PDM after configuring the DHCP Client to run on the PIX Firewall outside interface through the PDM.
CSCdu12990	The graphs for the 2560 byte blocks for both "Blocks Used" and "Blocks Free" always show up as 0.
CSCdu13592	The history view time is incorrect if the connection is lost or the clock is changed.
CSCdu13760	Performance monitoring values increase when you use the show perfmon command.

Table 1 *Open Caveats (continued)*

DDTS Number	Description
CSCdu16015	Clicking the Help button a second time causes the help screen to stall.
CSCdu19903	The PDM graphs no longer plot new points when the connection from the PIX Firewall is lost. Workaround: Close the PDM window and restart.
CSCdu20593	When the Cisco Secure VPN Client version 1.1 is using the mode configuration address, on rekey, the user is prompted for the username and password. On entering the username and password, if you type the show uauth command on the PIX Firewall, one can see two entries for the same client with the same username, one with the mode configuration address and one with the internal address.
CSCdu22069	An xlate entry appears for an outside Proxy's IP address. The call from the inside SIP Phone to the outside SIP Phone through the OUT Proxy is successful but bytes or responses to bytes from the outside phone do not go through.
CSCdu22771	PIX Firewall is sending initial contact during rekeying from PIX Firewall to PIX Firewall. Initial contact should be sent only during the first isakmp negotiation.
CSCdu23013	After adding a policy, it is impossible to cancel or discard changes.
CSCdu23112	PIX Firewall sends invalid data to Entrust CA while getting root certificate.
CSCdu23894	First enrollment request to Baltimore CA fails.
CSCdu24080	System ID window does not support scroll bar.
CSCdu24181	If a packet used in setting up an L2TP tunnel arrives late, then the PIX Firewall may reload.
CSCdu25228	Modifying the interface after a change is made to the security level always brings up the security level dialog.
CSCdu25691	L2TP does not respond to a ping for packets larger than 1373 bytes.

Resolved Caveats

The caveat descriptions listed in this section are drawn directly from the DDTS caveat headlines. These caveat descriptions are not intended to be read as complete sentences because the headline field in DDTS is limited in length. In DDTS headlines, some truncation of wording or punctuation may be necessary to provide the most complete and concise caveat description. The only modifications made to these headlines are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

The caveats in the [Table 2](#) are resolved:

Table 2 *Resolved Caveats*

DDTS Number	Description
CSCdk56623	Static PAT
CSCdm19803	Enhancement:show xlate should numbers in use & most used of xlates
CSCdm65465	Error msg for exceeding limit for domain-name length needs fixing.
CSCdm88690	wr floppy with 500k config causes PIX to ARF
CSCdm91548	assertion !f->dirty failed:file flash.c, line 85
CSCdp33425	Software support for 535 motherboard and flash I/O
CSCdp58921	Support for Kodiak
CSCdp60588	Interface routing should be based on local foreign (dnat) address
CSCdp67764	Show traffic displays incorrect information
CSCdp73853	debug crypto ca messages
CSCdp90785	clear isa does not remove isa identity address
CSCdr04004	small arp timeouts cause short periods of packet loss
CSCdr34819	Clear conf all does not reset arp timeout to default values
CSCdr42214	vpdn command displayed in wrong order
CSCdr43633	URL size exceeds buffer size
CSCdr48266	PIX assertion STKINIT thread.c uauth1 traceback crash
CSCdr48472	conn needs to be deleted from clear ? command page
CSCdr62725	Determine the current CPU load
CSCdr63197	Kodiak card doesn't work on PIX515
CSCdr68251	Port nos not appearing in syslog when using acl
CSCdr68928	When the certificate request fails it still says pending
CSCdr70978	Help alignment problem in aaa when no access-list is defined
CSCdr76192	Persistent connection problem with PIX and websense opern server
CSCdr77168	Microsoft win2k l2tp/ipsec client support
CSCdr77921	Opening a web page with ms2000 mail results continous authentication
CSCdr78189	No syslog when ssh/telnet/pfm connection limit exceeds
CSCdr78505	PIX does not compute the RIP v2 updates for the default route
CSCdr80268	SNMP ifTable.ifEntry.ifDescr not updated after swapping ifc names
CSCdr84397	PIX does not reset sixth consecutive requested ssh/telnet/pfm sessions
CSCdr84484	Write net command causes 1550-byte block leak
CSCdr93435	PIX does not open 3rd party Media Channel correctly
CSCdr93478	PPTP tunnel hashtable insert failed
CSCdr98471	Support more than 256M RAM (PIX535)
CSCdr99484	Certificate transfer fails over unreliable link
CSCds02901	Syslog msgs print protocol number instead of string (i.e., udp)

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCds04902	PIX 535 4port ethernet card not recognized
CSCds07597	PIX does not poll the CRL during first attempt when CRL is expired
CSCds07842	Active PIX in FDDI failover goes to failed state on 525
CSCds07862	Failover Sync is faster in FDDI causing config to fail in pix525
CSCds07872	One unit in FDDI failover always shows waiting on PIX 525 and PIX 520
CSCds08768	PIX crashes when displaying sh ipsec sa and IKE rekeys
CSCds09730	ISAKMP does not work if same network exists on different interfaces
CSCds10112	Crash after twice enrolling and getting denied both times
CSCds11341	PIX525 with gigabit, prints console msgs, reboots with heavy load
CSCds11378	H323 call, Call hangs after 30-40 minutes
CSCds14735	Increase dhcp server address pool to 32 addresses
CSCds14773	Checksum error when alias command is activated
CSCds16915	Watchdog timeout when doing ping with debug packet on token-ring int
CSCds18774	PIX should not respond to its own ARP request
CSCds19078	PIX key cutter uses ports allowed verbiage
CSCds21095	PIX pptp stop accepting new connections after sometimes of operation
CSCds22194	Alias not working when DNS server address is included in alias addr
CSCds23698	PIX sends RSET in response to tcp connections with ECN bits set
CSCds24580	PIX needs configurable radius port number
CSCds25070	PIX crashing with stateful failover every two hours
CSCds26054	RSA key disappears on standby PIX after failover
CSCds26115	Negative value displayed when log queue set to a big number
CSCds26568	No help online for command logging standby
CSCds29226	SIP 6.0 features
CSCds29656	Need nat 0 0 0 along with nat 0 access-list for no nat tunnel
CSCds29676	Websense caching not working -sho url-cache stat displays wrong info
CSCds29676	Websense caching not working -sho url-cache stat displays wrong info
CSCds29684	PIX history metrics support
CSCds30449	VPDN/AAA command not returning an error when entered into config
CSCds30523	nat 0 access-list with deny permits instead of denying
CSCds30699	SMTP stop filtering if DATA command failed
CSCds31061	PIX can have 2 pairs of rsa keys at the same time
CSCds31605	Add HTTP server
CSCds31721	PIX RIP multicast support feature addition
CSCds31739	TCP performance slow for bulk transfer

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCds32842	Fixup h323 does not nat 3rd party local/global
CSCds34475	PIX should consume pre-allocate channel by direction
CSCds34622	AAA accounting causes panic
CSCds34721	Checkpoint FW1 interop:failure when CP initiates QM to PIX
CSCds34732	Some H245 packets not processed because of TPKT lookup in PIX
CSCds35219	AAA commands should be more clear
CSCds37098	isakmp_receiver crash during performance testing
CSCds37126	WDT when clearing high number of ipsec sas (around 7500).
CSCds37133	With Kodiak, 1550 blocks not returning when send traffic just > NDR
CSCds37459	no <rip rule> for a rip rule that doesnt exist gives misleading msg
CSCds38147	SIP Third Party IP not Natted
CSCds38456	PIX timeout function wakeup earlier than the specified timeout value
CSCds38708	Disallowed commands can piggyback through SMTP with the DATA command
CSCds39158	SIP fails when message has no checksum
CSCds39293	PIX creates a default route when RIPv2 packet with no mask is sent
CSCds39657	SIP:checksum error when using nat between Gateways
CSCds41311	SIP TCP NAT enhancement.
CSCds41480	PIX doesn't negotiate keepalive interval
CSCds41775	Hummingbird Exceed XDMCP (Xwindows) does not work with PIX 5.2.1
CSCds42036	Stateful Failover HTTP suport
CSCds42440	Crash in IPsec response handler while running pixIosIpsec* script
CSCds42628	RIPv2 config. on FDDI/TR doesnt work; configs RIPv1 instead
CSCds43973	Cannot telnet to PIX inside intf - 402106:Recd packet not IPSEC...
CSCds44064	kprint with AH with pep card
CSCds44305	After reboot, PIX goes to monitor mode
CSCds44839	nameif does not err when trying to configure Eth6 or 7 on PIX 525R
CSCds45347	PIX crash if Ctrl-Y is pressed constantly
CSCds45357	Typo in error message, should be millisecond, not mille-second
CSCds45528	debug packet output always print tcp hlen field as 0
CSCds46335	PIX-535:DA28F320J5 4MB flash part device driver support
CSCds46349	211001:Memory allocation Error during H.323 stress testing
CSCds46439	Redistribut connected and static is not removed
CSCds47010	After ifx swap, changing dhcpd addr crashes PIX
CSCds48592	Cannot load new image from monitor mode using tftp
CSCds49141	H323:fixup is not translating static fixed network addr correctly

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCds49492	PIX Classic crash with copy tftp flash , reboots with monitor
CSCds49510	Cannot load image using monitor prompt
CSCds49584	H323:rtp media ports are not being opened using alias
CSCds50002	PPTP:win95 CHAP authentication loops forever when it should fail.
CSCds50982	PIX cannot retrieve CRL if first attempt failed because of CA server
CSCds51762	VPN IPsec with Kodiak card will have decapsulation failed
CSCds51955	tracert does not work with interface PAT
CSCds51957	ICMP id in show xlate not correct
CSCds51960	ping with ICMP identification of zero and PAT failed
CSCds52405	PIX-535 interface numbering is in wrong order in
CSCds53316	Unable to re-establish IPsec SA after default 24hr expiration
CSCds53633	No syslog(603104:PPTP Tunnel created) displayed until tunnel delete
CSCds54451	max-time out, is not timing out if we keep creating new IPSEC sas
CSCds54777	PPTP:Wrong EchoID and ResultCode transmitted in response to EchoRQ
CSCds54786	interface command does not recognise unit for hw_speed
CSCds54886	PIX crashed in AAA trying to parse the URL in an HTTP GET request
CSCds55694	Need show commands for H323
CSCds55734	negative byte count in show conn output
CSCds55750	PIX-535 Front Panel ACTIVE LED not work.
CSCds55770	boot message .Config Error -- The during bootup
CSCds56384	ingsum error, boothelper does not come up, PIX reboots
CSCds56721	H323:WDT if debug ras asn/event on
CSCds56725	Pix crashes in Crypto CA thread when getting a large CRL
CSCds57285	No error when timeout due to net down, only partial conf is ported
CSCds57737	PIX 525 Production version will hang after installed 4port FastEther
CSCds58313	PIX crash when no memory & using Cisco Gatekeepers
CSCds58358	Sysopt connection enforcesubnet not deprecated correctly.
CSCds58542	PIX-535 crashes with more than 4 Gigabit-ethernet cards installed
CSCds58667	PIX-535 show version displays 1022 MB RAM instead 1024 MB.
CSCds60165	PIX NFS mount / sunrpc does not work without opening ports gt 1024
CSCds60270	Pix unable to establish tunnel with peer if peer changes keys or id
CSCds61151	H323:Debug messages during call setup
CSCds61417	route is not stored in config if DHCP client is configured
CSCds62051	Clear config secondary does not clear ca related config
CSCds62734	improper casting shortens SA lifetimes

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCds63404	Pix crash pressing Ctrl-R and then holding any key
CSCds63477	add capability to autoconfigure dhcp server dns, wins.. parameters
CSCds63501	LU updates for UDP conn are not properly propagated to standby unit
CSCds63569	max sockets/tcp_channels need to set according to max channels
CSCds63626	ip verify fails if ip spoofed packets destined to PIX outside ifx
CSCds63626	ip verify fails if ip spoofed packets destined to PIX outside ifx
CSCds63735	Skinny Support
CSCds64958	Strict FTP does not work in active mode with verbose FTP server
CSCds65704	AAA acl not working after adding IPsec config
CSCds65716	aaa-server radius-acctport displayed in config even for default
CSCds66052	H323:PIX crash trying to decode non-Cisco nonStandard msg
CSCds66550	out of channels error causes watchdog timeout in logger
CSCds67745	H323:Bad source IP on ACF RAS message using Static Network with NAT
CSCds67865	PIX520 (secondary) crash
CSCds68537	Local & foreign IPs not saved in the PIX config for aaa acctg exclud
CSCds68660	PIX allows inside ifx to have same addr as DHCP addr pool
CSCds69038	Message 402103 misprints protocol field
CSCds69039	PIX reject ICMP errors as not matching IPsec identity
CSCds70898	fixup ftp strict does not work some ProFTPD setup
CSCds71849	dbgtrace_is_debug_trace_on() function need to be optimized
CSCds72499	PIX crashes when it receives faulty DHCPDISCOVER packet
CSCds72713	H323 debugs on console
CSCds72776	H323:H225 packets w/ invalid protocol discriminator not rejected
CSCds73666	copyright notice obscures config problems
CSCds73769	CA:detach the ca save all cmd from the write mem cmd
CSCds73818	Fixup H323 does not check signalling state
CSCds73884	Force PIX535 CPU speed to 1000Mhz
CSCds73999	config failed diagnostic prints only first word
CSCds74142	H323 RAS msg ACF should be rejected if didnt recv ARQ
CSCds74244	PIX crash if standby and active unit perform wr mem at the same time
CSCds74352	ip verify does not work if connection is established
CSCds74609	Retransmit causes connection to exit embryonic too early
CSCds74710	When hostname is changed don't delete the old keys but give a warning
CSCds74883	Clear config primary leads to a crash in ci/console thread
CSCds75822	H323:After a call is on hold, H245 msgs not NATd

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCds76248	PIX 525 hangs with two 4-port Fastethernet cards
CSCds76768	PIX 525 onboard ethernet card getting errors when connected to swite
CSCds77340	PIX crashes when trying to decrypt 1518-byte packets
CSCds77371	Static ARP is not static
CSCds79949	CRL Distrubution point should be resolved using a DNS Resolver
CSCds80132	PIX535:Interface numbering of a 4 port card is wrong in monitor mode
CSCds80481	show version shows wrong MAC addresses in FDDI failover PIXes
CSCds81003	Wrong err msg when enter invalid interface for ip audit interface
CSCds81948	CA:crash after trying to enroll w/Balt and after type some cmds
CSCds82096	B flag set for both inbound and outbound connection
CSCds82103	can not manually release or renew dhcp address
CSCds82116	Enhancement:CLI for IDS counters
CSCds82362	add hardware platform name to a MIB var for CiscoView support
CSCds82362	add hardware platform name to a MIB var for CiscoView support
CSCds82454	no rip ifx default version 2 will un-config RIPv2 passive on ifx
CSCds82455	VPN:last QM packet not retransmitted - causes invalid spi errors
CSCds82521	PIX should unconfigure MCAST addr. from ifx when RIPv1 is configured
CSCds84487	dhcp server need to guard against malformed dhcp pkt
CSCds84837	add support for Unity client
CSCds85080	IKE Main mode proposal flooding reboots PIX
CSCds86173	extern inlines break GDB compiles
CSCds86963	Bogus name-server saved in config
CSCds87365	H323:PIX does not inspect Progress message
CSCds87968	WDT in HTTP server for command requiring user input
CSCds87968	WDT in HTTP server for command requiring user input
CSCds88063	PIX dhcp client w/ failover lic fails to get addr auto. after reboot
CSCds88093	TCP write should allow unlimited buffer size
CSCds88097	Cannot connect to pdm_handler if history is disabled & using IE
CSCds88107	Default HTTP configuration is incorrect
CSCds88117	Remove certain fover history metrics
CSCds89077	PIX does not open 3rd party H245 connection
CSCds89302	Clear needed for domain-lookup and name-server commands
CSCds89953	HTTP authentication compromised when same IP address
CSCds90077	Pix crashed when trying to change the transform set.
CSCds90283	Show PDM Version as part of sh tech

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCds90474	Assertion error when tcp log server is configured.
CSCds90641	PIX alias does not work with PAT
CSCds90792	fixup smtp blocks emails when . and <CR><LF>are not in the same pack
CSCds90802	PIX - NFS-disallow packets of more than 12 fragments
CSCds90932	Blocks info need to be dynamic
CSCds91331	add shun support
CSCds92693	sh loc and/or sh conn during GC could cause list corruption
CSCds92738	standby PIX print confusing inconsistent xlate.. debug msg.
CSCdt00162	service resetinbound does not work with interface PAT
CSCdt00199	Ability needed to reload without user input
CSCdt00272	add support for 32 snmp servers
CSCdt00305	customer wants clear log in enable mode
CSCdt00345	add ftp port ids signatures
CSCdt00459	Debug message for PKI content which sent and recv from PIX
CSCdt00845	name command should accept . as a valid character
CSCdt01283	Need to remove IDS sig 8000
CSCdt01604	snmp needs trap and poll granularity
CSCdt01808	ARP does not proxy-arp for arp alias entry
CSCdt01825	PIX should proxy-arp for alias address
CSCdt02063	H245:should create new TPKT & discard original if TPKT recvd only
CSCdt02132	should check host list on 1st SYN for telnet, ssh, pfm & http
CSCdt02132	should check host list on 1st SYN for telnet, ssh, pfm & http
CSCdt02132	should check host list on 1st SYN for telnet, ssh, pfm & http
CSCdt02883	Cert. enrollment request is lost if CA is not available at that time
CSCdt04092	Allow libssl to build with parallel make
CSCdt04241	Remove debugging kprint statement from stateful failover
CSCdt04772	Make fragment database limits configurable
CSCdt04910	Utility:Eliminator Disk to test throughput in new platforms
CSCdt05005	name-server command causes crash
CSCdt05025	LU look NAT failed -> NAT is disabled
CSCdt05896	reduce stateful failover connection update traffic
CSCdt06176	H323:No audio/video with NetMeeting
CSCdt06447	PIX going out of memory block in stateful failover
CSCdt06571	ip thread priority should be high and not critical
CSCdt06571	ip thread priority should be high and not critical

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt06576	low block states hard to diagnose without driver queue counts
CSCdt07239	No IDS/Interface stats even though connected to pdm_Handler
CSCdt07329	Unity:PIX should sent Unity vendor id
CSCdt07338	shun output needs modification to facilitate csids parsing
CSCdt07720	Requirement to add address respond for unity interop be removed
CSCdt07794	Can not select private key - msg prints on standby during the Sync
CSCdt07896	Disconnect from Unity does not restore IP address to local pool
CSCdt07934	PIX disconnects unity client after 5 mins even with continuous ping
CSCdt08611	Termination of existing SSH connection by tcp flooding to port 22
CSCdt09791	dhcp client config lost if the cmd failed
CSCdt10417	Pix should support one time xauth with Unity client
CSCdt10520	Pix prints messages in a loop on hitting cancel on unity xauth dialo
CSCdt10759	Pix does not clear ipsec sas on clearing isa sas with unity
CSCdt11544	Http connections are replicated on the standby even it is turned off
CSCdt11561	PAT:IP addr. representation is backwards
CSCdt11716	clear xlate prints 305007 syslog message on standby unit
CSCdt12049	SIP call does not thru
CSCdt12051	SIP - open a 30 minute hole
CSCdt12570	Get rid of help ? message when user answers NO for pre-config
CSCdt12715	HTTP Server not compatible with Netscape 4.5
CSCdt12968	Replication of rsa needs to be removed from failover usage
CSCdt13307	Assert with regular PAT
CSCdt13324	Output of UDP connection should be similar to TCP connection
CSCdt13647	Missing syslogs for PDM sessions
CSCdt15819	Fail to dump UDP connection after DNS reply is seen
CSCdt16201	Skinny Support
CSCdt16476	Skinny DNAT
CSCdt16634	alias is not working with static in regression test
CSCdt16666	PIX on reboot wont get addr via dhcp if conn. thru switch to svr
CSCdt17425	Unity:PIX needs to extract OU field from certs and use that vpngroup
CSCdt17646	rip cmd should parse all input
CSCdt17923	CPU usage greater than 100%
CSCdt17979	SIP - termination error on UDP with Proxy
CSCdt18207	Syntax for static command in help incorrect
CSCdt18433	H225:syslog 405104 for signalling protocol is wrong

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt18451	Clear config all does not clear icmp command.
CSCdt19062	if peer supports DPD, PIX should not send old version of keepalives
CSCdt20223	PDM sessions cannot be started up from some machines.
CSCdt20719	All transform sets are deleted from the config if downgrade from 6.0
CSCdt20936	Add Input Queues & Output Queues to interface graph
CSCdt20960	Watchdog timeout in http1 thread on Active unit while using PDM
CSCdt21344	http server enable CLI :ambiguous error message
CSCdt21498	if DPD is enabled, PIX should not allow dangling SAs
CSCdt21999	Graphing tables not loaded realtime w/ IE & PDM history disabled
CSCdt22085	PIX:with names, host route changes to default route on reload
CSCdt23749	PIX should send invalid spi notify if peer is out of sync
CSCdt23844	Pix crash when trying to connect from browser
CSCdt24354	Pix crashed at radius_rcvauth while SoftID authentication.
CSCdt24676	Add setting clock and enable password to Setup command
CSCdt25063	Failover replication does not give usage error for invalid commands
CSCdt25088	Unity:max-timeout not working between PIX and unity client
CSCdt25128	Connections on standby are not getting deleted after closing them
CSCdt25132	Unity:PIX does not terminate the tunnel after idle-timeout
CSCdt25195	DPD to Unity client not used unless isa keepalive is configured
CSCdt25206	Must use address initiate to work correctly with VPN 3000 client
CSCdt25271	Flags display in standby is different from Active.
CSCdt25271	Flags display in standby is different from Active.
CSCdt25302	No usage when invalid argument is given to show cpu
CSCdt25399	PIX cached Authentication doesnt work with UDP connections
CSCdt26387	PIX 535-R supports 8 interfaces, PIX 535-UR supports 10 interfaces
CSCdt26426	PIX accepts authentication command for http on non-std ports
CSCdt27187	Remove FDDI support for version 6.0
CSCdt27187	Remove FDDI support for version 6.0
CSCdt27453	isakmp password is displayed in plain text in the show tech output
CSCdt28073	PIX appending two bytes to RADIUS state attribute
CSCdt28219	Internal users cannot ping outside hosts with interface PAT
CSCdt29563	clear interface does not clear no buffer numbers
CSCdt29713	Error Msg - Image too small is confusing
CSCdt29741	PDM - need to send disco to PDM on command from PDM
CSCdt30598	sysopt conn permit-l2tp does not show in wr t but shows in sh sysopt

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt31217	DPD not needed while receiving IPSEC packets from peer
CSCdt31630	Block leaks in fragment database
CSCdt32830	RST always printed for syslog 106015 even if no RST in packet
CSCdt33178	autoconfig dns domain not reset after PIX dhcp client lease expires
CSCdt33450	cry ipsec trans mode tunnel not allowed but is in the ipsec help
CSCdt33465	Can enter more than 2 dns/wins for vpdn gp but PIX takes only 2
CSCdt33511	PIX doesnt error if incorrect commands are entered for l2tp vpdn gp
CSCdt33615	PIX cant discover pdm image when rebuilding the file system
CSCdt34127	DNS Resolver CLI should be disabled
CSCdt34375	SIP:Conduit permit needed if SIP Proxy on inside
CSCdt34923	Err message when deleting global pool
CSCdt35429	Naptha DoS tool vs. PIX ssh daemon causes high CPU load
CSCdt36326	Pix crashed in isakmp_receiver thread while running stress tests
CSCdt36491	debug icmp trace prints invalid type and code for fragmented packet
CSCdt36975	PIX CLI should not check for match between authen and author rules
CSCdt37028	err checking in c_passwd.c/showcfg() can cause crash in crashdump
CSCdt37354	PIX DHCP client tries total 5 times when retry cnt=4, but not default
CSCdt37361	PIX VPN IPsec tunnel mutiple interface termination is broken
CSCdt38205	stateful failover should not generate syslog when out of mem blk
CSCdt38404	Wrong character for Account rule in aaa accounting command
CSCdt38616	rip routes have a metric of one added.
CSCdt39002	write net:creates wrong path and fails to save file on tftp-server
CSCdt39174	vpdn group dns/wins command is not fully replaced by a new one
CSCdt39673	Extra vertical bars in vpdn help message
CSCdt39766	Erasedisk not support PIX-525 platforms
CSCdt39820	syslog for memory allocation error used inproperly in places
CSCdt39863	PIX crahed at Crypto_PKI_RCV while enrolling cert. request
CSCdt39869	Certificate requests to baltimore CA server are failing
CSCdt39871	logging priority consulted only after formatting overhead incurred
CSCdt40514	Setup program:when user hit <enter> for month, PIX prints error
CSCdt40579	without IPsec, host can telnet to PIX from least-secured interface
CSCdt40713	xlate error when portmap pool exhausted results in rogue conns
CSCdt40808	Crash in L2TP mgmt daemon thread while trying to negotiate a tunnel
CSCdt40824	L2TP tunnel is deleted soon after it is established with ah-md5-hmac
CSCdt40965	aaa-server (inside) (inside) host 3.3.3.3 timeout 5 not valid

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt41079	telnet, ssh & tftp-server always assume least-secured ifc at level 0
CSCdt41720	old keepalives should be disabled when running DPD
CSCdt41763	PIX:weird behavior when configuring static with names
CSCdt42223	clear logging at enable mode does not work
CSCdt42739	H323:PIX should open connections based on LogicalChannelNumber
CSCdt44399	Interface history metrics stats wrong when history enabled
CSCdt44501	Outbound/apply is not working in PIX 6.0
CSCdt44573	PIX crash doing AAA to outside AAA server through IPSec
CSCdt44701	DPD continues indefinitely even when no traffic, could be optimized
CSCdt44710	inactivity timeout expires prematurely while doing new pin mode
CSCdt45065	Small block pool causes traffic to hang with Livengood Gigabit Card
CSCdt45383	static NAT, option nailed lost after PIX reload
CSCdt45767	Redundant check for sp->econlimit in create_static()
CSCdt46647	UDP packet is invalid at destination when alias and NAT is set.
CSCdt47093	sending show hist through the CLI Window crashes PIX.
CSCdt47534	PIX uses IPSec lifetime configured on W2K client even if larger
CSCdt47534	PIX uses IPSec lifetime configured on W2K client even if larger
CSCdt47536	gdb toolchain disappearing from irp-view5
CSCdt48315	Only a few tx-set combinations successfully set up L2TP tunnel
CSCdt48570	Tunnel not established with Win2k client if its IKE lifetime is more
CSCdt49040	PIX does not allow packets with a UDP SRC (source) port of 0
CSCdt49606	vpngroup CLI accepts 2 args for attributes. Some use 1 only.
CSCdt49611	vpngroup idle-time and max-time accept out of range values
CSCdt49768	Crash in ci/console thread while running PIX IOS regression test
CSCdt49830	Current metrics should not be printed when printing history metrics
CSCdt49906	Virtual HTTP/Telnet doesnt work if intf 0 is not in lowest sec level
CSCdt50422	PIX should accept RADIUS cisco VSA in standard format
CSCdt50685	DPD:time stamps shouldnt be initialize upon ipsec tunnel establishm
CSCdt51029	PIX 535 crash while loading the 6.0(0.200) image
CSCdt51260	SIP - Third party embyonic connection does not work
CSCdt51419	PIX logging settings not shown on config when no logging on
CSCdt51883	Failover, Unity rekey may lead to 2 clients with same assigned IP
CSCdt52321	callerID not shown & Bytes in/out inconsistent in L2TP/PPTP aaa acct
CSCdt52331	PIX crashes in fixup_sip
CSCdt52428	Watchdog timeout in http2 thread

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt52454	Clear option not shown in vpdn help message
CSCdt52520	PIX crash when shutting down ifc, then turn back on
CSCdt53291	remove unsupported pal command
CSCdt53613	Need to remove checks for FDDI in CPU usage code as FDDI is not supp
CSCdt53742	Global/Nat does not work with VoIp Third Party address
CSCdt54465	PIX should accept RADIUS IETF Attribute 11 Filter-Id
CSCdt54951	standby unit incorrectly create udp conn and generate 210010 syslogs
CSCdt55485	SSL not sending certificate chain for Baltimore CA
CSCdt55597	Shun cmd doesnt delete conn if dnat is used
CSCdt56080	PIX crashes establishing a PPTP tunnel and Radius server unavailable
CSCdt56640	Skinny:Outside phone unable to set up TCP connection with inside CM
CSCdt57268	clear conf all does not clear fragment configuration
CSCdt57707	PDM fails to connect for the first time if no key present on PIX
CSCdt57945	PIX gets interface resets, hangs on More prompt, and affects PDM
CSCdt58717	Setup dialog runs after leaving enable mode if no saved config
CSCdt58791	PDM logging:syslog logging level overrides pdm logging level
CSCdt58805	PIX must not change isakmp lifetime in IKE initiators proposal
CSCdt58988	Feature to obtain stats using performance measuring counters
CSCdt59107	SIP:PIX crashes with static, OUT GW, Out Proxy and Inbound call
CSCdt59137	SIP:Denies on PIX but call goes thru fine with statics, out GW
CSCdt59154	monitoring:pkt rates/bit rates uses sh traffic instead of sh int.
CSCdt59162	need clear pdm location and show pdm location commands
CSCdt59255	Return if open() fails to open the channel in get_process_usage()
CSCdt60308	Certificate request fails if retried after cancelling.
CSCdt60487	PIX reboots dumping trace
CSCdt61216	Naptha (ESTABLISHED) Flooding causes PDM DoS
CSCdt61235	clear interface does not clear interface resets
CSCdt61428	Completed SSL Handshake flooding DoS against PDM
CSCdt61475	Remove Token ring Support for 6.0.x
CSCdt61478	Remove PL2 support in version 6.0.x
CSCdt61610	Remove 3com NIC support
CSCdt62053	ISAKMP dpd packets is not always sent at the expect interval
CSCdt62072	Overlapping PAT and static PAT failed
CSCdt62287	perfmon history metrics incorrect
CSCdt62902	Win2K client with SP1 cannot establish L2TP/IPSec tunnel with PIX

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt62968	Reboot with filter java and nat 0 access-list
CSCdt62994	Remove legacy platform support
CSCdt63037	VoIp:no voice between inside phones (static nat w/ no route)
CSCdt63953	Assertion violation in isakmp_time_keeper thread
CSCdt64177	PIX flooded with cgx_create_cc returned 0x102 messages
CSCdt64243	ike retransmit debug seen on console even with debug off
CSCdt64687	DHCP client does not interoperate with some relay agent or server
CSCdt64687	DHCP client does not interoperate with some relay agent or server
CSCdt65464	MIB-II object interfaces.ifSpeed not supporting GigE card
CSCdt65603	PIX IS GIVING WRONG PROMPT WHEN DOING XAUTH
CSCdt65673	remove the pfm command from PIX 6.0(1)
CSCdt66414	remove unused pal_check() function in lu_thread
CSCdt66614	SSH allowed after changing hname, dname when previous keypair exists
CSCdt66648	CA:Do no save .server key to the flash with ca save all command
CSCdt66732	Incompatible output on show xlate and show conn
CSCdt66744	Unity connection not closed when idle_time reached.
CSCdt67998	clear int on GE ports is not implemented
CSCdt68281	no historical data for AAA perfmon
CSCdt69147	AAA downloadable accesslist is not working after uauth is denied.
CSCdt69345	L2TP tunnel is deleted when IKE lifetime expires
CSCdt69519	ifc byte/packet counts for history metrics should be in kilo
CSCdt69545	Provide a way to clear logging on PDM
CSCdt69549	PDM cannot connect to PIX if PIX cpu utilization is 96%.
CSCdt69667	Encryption layer for tcp port 1467 uses up lots of memory
CSCdt69676	Enable UniRPF for-us traffic
CSCdt70750	sysopt conn tcpmss 0 behavior changed from 5.0 to 5.1
CSCdt71192	Statefull failover pix logs duplicate messages on syslog server
CSCdt71428	watchdog when clear isa sa with 2000 IKE tunnels
CSCdt72080	sh conn doesn't print udp dns flags properly
CSCdt72976	HTTP Server should support If-Modified-Since
CSCdt73011	setup command:Does not remember clock correctly
CSCdt73133	pdm_handler:Send back data for other views if applicable every 10s
CSCdt73168	Static command does not accept same l_port eve if l_ip is different
CSCdt73216	SIP:Re-Invite from OUT Ph when put on Hold gets denied
CSCdt73353	ssh - need to add CRC-32 compensation attack detection

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt73358	need unique tty # in ssh debug messages
CSCdt73865	H323 msg printed on console needs to be removed
CSCdt74158	flash down 5.x does not work, but flash down 4.x works
CSCdt74263	Do not allow more than one rsa key though with different attrs
CSCdt74520	PIX - uauth cache not working properly with browsers
CSCdt74595	Assertion violation in isakmp_receiver while clearing ipsec sas
CSCdt75054	Assertion in logger thread performing syslog thru IPSec tunnel.
CSCdt75093	PIX display nb_ipsec_sa* display useless message on the console.
CSCdt75715	fragment cmd handles input > max inconsistently
CSCdt75743	Hostname should not allow special characters
CSCdt75920	expand dhcp server features - feature request
CSCdt75960	ISA fragment method causes PIX to discard packet
CSCdt76696	IOS keepalives not occurring to IOS peers.
CSCdt77108	selectively allow unencrypted SSH sessions for debugging
CSCdt77818	Pix crashes at crypto CA if netscape CA server is misconfigured.
CSCdt79716	Turn PDM History Metrics on by default
CSCdt80572	ISA debug shows wrong IP for responding to peer config... message
CSCdt81292	Enhance show pdm history command to allow specifying metric
CSCdt82158	use sysObjectID to differentiate PIX hw platform for CiscoView
CSCdt82325	PIX in failover consumes all memory and then crashes
CSCdt82621	Skinny:Outside phone unable to setup TCP connections correctly
CSCdt83142	SIP:Call does not go thru with static network
CSCdt83901	user got aaa authned could not ping through firewall
CSCdt85788	Pix fails to get CRL with Verisign certificate.
CSCdt86132	709001:FO repliSorry :error message at boot up
CSCdt86568	PIX crash when url-server not available and URL-cache turns on
CSCdt87949	SIP:Inbound call from OUT POTS Ph to IN SIP Ph fails
CSCdt89747	Panic:kernel - ef_probe:unknown unable to reserve 1024 16384 byte
CSCdt90943	Remove NATINFO_T structure & use conn
CSCdt90953	fixup_skinny needs to be properly formatted
CSCdt91309	Interface PAT port detection with for-us traffic ineffective
CSCdt91313	ARG_USED is in wrong order
CSCdt92029	Xauth will not work with 3002 and crashes removing config w/o reboot
CSCdt92339	BUGTRAQ:PIX should limit number of uauth sessions per source IP
CSCdt92450	Multiple websns keepalive daemon starts

Table 2 Resolved Caveats (continued)

DDTS Number	Description
CSCdk56623	Static PAT
CSCdt93034	fixup_sip needs to be properly formatted
CSCdt93858	kprint message to console when failure to allocate block
CSCdt94165	Current metrics not sent when pdm history is disabled
CSCdt94616	Static PAT and DNS is not working.
CSCdt94747	Skinny:Interoperability fails with fixup H323
CSCdt94927	SIP:need debug & syslog
CSCdt94933	Skinny:need debug & syslogs
CSCdt95162	Interface static not saved correctly
CSCdt95770	clear config all does not remove pdm location commands
CSCdt96665	PIX accept same ip add to different int right after reload
CSCdt96972	One time xauth:Unity still prompted for xauth
CSCdu00856	Emit a warning if an 82542 *wiseman) in found in a PIX535
CSCdu00949	clear sysopt doesn't clear sysopt connection permit-l2tp command
CSCdu01056	PIX crash during backup
CSCdu02291	Failover timeout needs to be taken out from failover on line help
CSCdu02557	Xauth:With ACS+SecurID, wrong message for new pin mode
CSCdu02673	clear config should be a config mode command
CSCdu02674	Issues with the service command
CSCdu04084	PIX crashes when reading certificate from flash
CSCdu04466	Ftp data transfer not resumed after failover
CSCdu05028	PIX new dhcp server feature should have been 253 clients
CSCdu05694	Global:Invalid global command crashes pix
CSCdu05794	tepsic with random tcp options cause PIX to watchdog timeout
CSCdu05843	ip verify doesnt work w/ ipsec
CSCdu05903	SIP:Crash in PIX when outbound call made with Global/NAT
CSCdu06716	PIX show chunk only show ulimit chunk
CSCdu06725	PIX transmits two radius auth requests with same ID to Axent radius.
CSCdu06743	Auth fails with null password with ACS2.6 in between PIX and DSS
CSCdu07043	Transport mode trans-set can be configured for static crypto map
CSCdu07837	Xauth:with tacacs+ giving 2 syslog messages for xauth
CSCdu08103	Xauth:Does not work with Cryptocard ACS for Challenge response mode
CSCdu08574	Cert enroll request fails after deleting current CA and retrying
CSCdu09255	Can not delete interface static from the configuration
CSCdu10711	PIX crashed in isakmp_receiver thread while running ttcp tests
CSCdu10773	Xauth:challenge-response does not work with Tacacs+

Table 2 *Resolved Caveats (continued)*

DDTS Number	Description
CSCdk56623	Static PAT
CSCdu11109	Web browser connection corrupts CA cert
CSCdu11774	SIP:Call does not go thru with IN proxy (Regression)
CSCdu11781	PIX crash during DHCP req when PDM refreshes DHCP Client Info
CSCdu12909	SIP:Connections for Responses to INVITE not opened correctly
CSCdu13204	Xauth:Pix does not delete uauth entry with IRE internal address
CSCdu13395	Remove <nailed> parameter from static command online help.
CSCdu13533	Total SAs under sh isa sa shows incorrect number of SAs
CSCdu13547	L2TP:On W2K client L2TP tunnel details shows PIXs inside address
CSCdu15173	H323 RAS causes memory corruption & crash in malloc
CSCdu15271	Watchdog timeout failure in http1 thread
CSCdu16076	PIX slow when handling https connections with PDM
CSCdu16164	Assertion violation and pix crashed
CSCdu17372	PIX:Makefile.inc was accidentally changed
CSCdu18020	PIX to PIX or PIX to Unity connection fails using certificates
CSCdu18689	PDM history for failover not working
CSCdu19825	Memory leak through different panels on PDM, PIX

Related Documentation

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

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_technical_documentation.html

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_technical_documentation.html

http://www.cisco.com/en/US/products/sw/secursw/ps2276/prod_technical_documentation.html

Cisco provides PIX Firewall technical tips at the following website:

<http://www.cisco.com/en/US/support/index.html>

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a Cisco.com user name and password, you can visit the following websites for assistance:

TAC Customer top issues for PIX Firewall:

- <http://www.cisco.com/en/US/support/index.html>

TAC Sample Configs for PIX Firewall:

- http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX&s=Software_Configuration

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

- http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:PIX

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other 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. (0106R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

