Cisco PIX Firewall Release Notes Version 6.2(2)

September 2002

Contents

This document includes the following sections:

Introduction

The PIX Firewall delivers unprecedented levels of security, performance, and reliability, including robust, enterprise-class security services such as the following:

- Stateful inspection security, based on state-of-the-art Adaptive Security Algorithm (ASA)
- Over 85 predefined applications, services, and protocols for flexible access control
- Virtual Private Networking (VPN) for secure remote network access using IKE/IPSec standards
- Intrusion protection from over 55 different network-based attacks
- URL filtering of outbound web traffic through third-party server support
- Network and Port Address Translation Support (NAT and PAT)

CISCO SYSTEMS

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

PIX Firewall software Version 6.2 provides the secure networking features included in previous releases and adds support for the following features:

- Auto Update Support
- Bi-Directional Network Address Translation (NAT)
- Command-Level Authorization
- Command-Line Interface (CLI) Activation Key Management
- Configurable RAS Fixup
- CPU Utilization Monitoring Through SNMP
- DHCP Option 66 and 150 Support
- Downloadable Access Control Lists (ACLs)
- Easy VPN Remote Support
- Factory Default Configurations for the PIX 501 and PIX 506/506E
- Failover Enhancements
- ILS Fixup
- LAN-Based Failover
- Multicast Support (IGMP v2 and Stub Multicast Routing)
- Network Time Protocol (NTP) Support
- Object Grouping
- Packet Capture
- PIX 501 User Licensing and VPN Support Enhancements
- PIX Firewall Image Flash Compression
- PPPoE Support
- Software Performance Enhancements
- TurboACL
- URL Fltering Enhancements

Additionally, PIX Firewall software Version 6.2 supports Cisco PIX Device Manager (PDM) Version 2.0 and adds enhancements to features introduced in earlier releases.

System Requirements

The sections that follow list the system requirements for operating a PIX Firewall with Version 6.2(2) software.

Memory Requirements

The PIX 501 has 16 MB of RAM and will operate correctly with Version 6.2, while all other PIX Firewall platforms continue to require at least 32 MB of RAM (and therefore are also compatible with Version 6.2 and higher).

In addition, all units except the PIX 501 and PIX 506/506E require 16 MB of Flash memory to boot. (The PIX 501 and PIX 506/506E have 8 MB of Flash memory, which works correctly with Version 6.2.)

Table 1 lists Flash memory requirements for this release.

Table 1 Flash Memory Requirements

PIX Firewall Model	Flash Memory Required in 6.2
PIX 501	8 MB
PIX 506/506E	8 MB
PIX 515/515E	16 MB
PIX 520	16 MB (Some PIX 520 units may need a memory upgrade because older units had 2 MB, though newer units have 16 MB.)
PIX 525	16 MB
PIX 535	16 MB

Use the PIX-1GE-66 card in systems with a 64-bit/66 MHz PCI bus; for example, in a PIX 535. (If you use the PIX-1GE-66 cards in a PIX Firewall, the system RAM should be at least 128 MB.) For a PIX Firewall with only a 32-bit/33 MHz bus, such as the PIX 520 and PIX 525, use the PIX-1GE card.

Software Requirements

The following is required for Version 6.2(2):

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 Connection Online (CCO) to let you download the PIX Firewall image with TFTP.
2. If you are upgrading from Version 4 or earlier and want to use the Auto Update, IPSec, SSH, PDM, or VPN features or commands, you must have a new 56-bit DES activation key. Before getting a new activation key, write down your old key in case you want to retrograde to Version 4. You can have a new 56-bit DES activation key sent to you by completing the form at the following website:

   http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324
3. If you are using PIX Firewall Syslog Server (PFSS), 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.

Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum configuration file size limit is increased to 2 MB for PIX Firewall software Versions 5.3(2) and higher. For other PIX Firewall platforms and earlier software versions, the maximum configuration file size limit remains the same. (In these cases, the maximum configuration size is most likely 1 MB.)

While configuration files up to 2 MB are now supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as **write term** and **show conf**
- Failover (the configuration synchronization time)
- During a system reload

Cisco Secure Policy Manager (Cisco Secure PM) may also experience limitations if a PIX Firewall configuration file near 2 MB is used, and the optimal configuration file size for use with Cisco PIX Device Manager is less than 100 KB (which is approximately 1500 lines). Please take these considerations into account when planning and implementing your configuration.

Cisco VPN Software Interoperability

Cisco VPN Series	Interoperability Comments
Cisco IOS Routers	PIX Firewall Version 6.2 requires Cisco IOS Release 12.0(6)T or higher running on the router when using IKE Mode Configuration on the PIX Firewall.
Cisco VPN 3000 Concentrators	PIX Firewall Version 6.2 requires Cisco VPN 3000 Concentrator Version 2.5.2 or higher for correct VPN interoperability.

Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco Secure VPN Client v1.x	PIX Firewall Version 6.2 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 6.2 requires Cisco VPN 3000 Client Version 2.5 or higher. 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.x (Unified VPN Client Framework)	PIX Firewall Version 6.2 supports the Cisco VPN Client Version 3.x that runs on all Microsoft Windows platforms. It also supports the Cisco VPN Client Version 3.5 or higher that runs on Linux, Solaris, and Macintosh platforms.

Cisco Easy VPN Remote Interoperability

Cisco Easy VPN Remote	Interoperability Comments
PIX Easy VPN Remote v6.2	PIX Firewall software Version 6.2 Cisco Easy VPN Server requires PIX Firewall software Version 6.2 Easy VPN Remote.
VPN 3000 Easy VPN Remote v3.0+	PIX Firewall software Version 6.2 Cisco Easy VPN Server requires the VPN 3000 Version 3.0+ Easy VPN Remote that runs on the VPN 3002 platform.
IOS Easy VPN Remote v12.2(8)YJ	PIX Firewall software Version 6.2 Cisco Easy VPN Server interoperates with IOS 806 Easy VPN Remote Version 12.2(8)YJ.

Cisco Easy VPN Server Interoperability

Cisco Easy VPN Server	Interoperability Comments
PIX Easy VPN Server v6.0+	PIX Firewall software Version 6.2 Cisco Easy VPN Remote requires a PIX Firewall Version 6.0 or higher Easy VPN Server. PFS and split-dns do not work with PIX Easy VPN server Version 6.0 and 6.1, but do work with Version 6.2.
VPN 3000 Easy VPN Server v3.1+	PIX Firewall software Version 6.2 Cisco Easy VPN Remote requires VPN 3000 Version 3.1 or higher Easy VPN Server. VPN 3000 Easy VPN Server v3.5 does not support split-dns.
IOS Easy VPN Server v12.2(8)T	PIX Firewall software Version 6.2 Cisco Easy VPN Remote requires IOS Version 12.2(8)T Easy VPN Server. This version of IOS Easy VPN Server does not support split-dns.

Determining the Software Version

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

Upgrading to a New Software Release

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

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

New and Changed Information

New Features in Release 6.2(2)

This release resolves a number of caveats. The PIX-4FE-66 card is also supported, except for PIX Classic, 10000 and 510 platforms.

New Software Features in Release 6.2

Auto Update Support

PIX Firewall software Version 6.2 supports Auto Update, a next-generation feature set for Cisco and third-party applications, that provides secure remote network management.

Bi-Directional Network Address Translation (NAT)

PIX Firewall software Version 6.2 allows Network Address Translation (NAT) of external source IP addresses for packets traveling from the outside interface to an the inside interface. All functionality available with traditional NAT such as fixups, Stateful Failover, dynamic NAT, static NAT, and PAT are available bidirectionally in this release.

Command-Level Authorization

PIX Firewall software Version 6.2 supports Command-Level authorization, which is user-defined command privilege levels (from 0 to 15) for all PIX Firewall CLI commands, and Local User Database authorization. With Local User Database authorization, you can create user accounts tied to these privilege levels. Additionally, command set functionality is available through an access control server (ACS), which allows definition of authorized CLI command sets on a per-user basis without the dependency of defining command sets across all users.

Privilege-level command tracing is provided through the PIX Firewall syslog, and privilege configuration updates are displayed in the **show version** command output. User authentication may occur either locally or through a TACACS+ server.

When a PIX Firewall sends a command authorization request to a CiscoSecure ACS for Windows Version 3.0.1, it is possible that the CSTACACS service may crash. (See CSCdw78255.) To rectify this, use the **CSCdw78255.zip** patch, which contains an updated **CSTacacs.exe** to use with CiscoSecure ACS for Windows 3.0.1 (build 40) instead of the existing CSTacacs.exe.

Command-level authorization sets work correctly with Cisco Secure ACS for Windows Version 3.0.2 or higher, and command-level authorization of users and groups works correctly with Version 3.0.1 and previous versions of CiscoSecure ACS for Windows.

Command-Line Interface (CLI) Activation Key Management

PIX Firewall software Version 6.2 lets you enter a new activation key through the PIX Firewall command-line interface (CLI), without using the system monitor mode and having to TFTP a new image. Additionally, the PIX Firewall CLI displays the currently running activation key when you enter the **show version** command.

Configurable RAS Fixup

PIX Firewall software Version 6.2 includes an option to turn off the H.323 RAS (Registration, Admission, and Status) fixup and displays this option, when set, in the configuration. This enables customers to turn off the RAS fixup if they do not have any RAS traffic, they do not want their RAS messages to be inspected, or if they have other applications that utilize the UDP ports 1718 and 1719.

CPU Utilization Monitoring Through SNMP

PIX Firewall software Version 6.2 supports monitoring of the PIX Firewall CPU usage through SNMP. CPU usage information is still available directly on the PIX Firewall through the **show cpu usage** command, but SNMP provides integration with other network management software. Specifically, this release supports the **cpmCPUTotalTable** of the Cisco Process MIB (**CISCO-PROCESS-MIB.my**).

DHCP Option 66 and 150 Support

PIX Firewall software Version 6.2 enhances the DHCP Server on the inside interface of the PIX Firewall to provide TFTP address information to the served DHCP clients. The implementation responds with one TFTP server for DHCP option 66 requests and with, at most, two servers for DHCP option 150 requests.

DHCP options 66 and 150 simplify remote deployments of Cisco IP Phones and Cisco SoftPhone by providing the Cisco CallManager contact information needed to download the rest of the IP phone configuration.

Downloadable Access Control Lists (ACLs)

PIX Firewall software Version 6.2 supports the download of access control lists (ACLs) to the PIX Firewall from an access control server (ACS). This enables the configuration of per-user access lists on an AAA server, to provide per-user access list authorization, that are then downloadable through the ACS to the PIX Firewall.

This feature is supported for RADIUS servers only and is not supported for TACACS+ servers.

Easy VPN Remote Support

PIX Firewall software Version 6.2 supports Cisco Easy VPN Remote. (Cisco Easy VPN Server has been supported starting with PIX Firewall software Version 6.0.) Cisco Easy VPN Remote is designed to function seamlessly with existing VPN headends configured to support Unity Clients and to minimize the administrative overhead for the client by centralizing VPN configuration at the Cisco Easy VPN Server. For example, as Easy VPN Remote products, the PIX 501 and PIX 506/506E can accept dynamic push policy from an Easy VPN Server. Other examples of Cisco Easy VPN Remote products include the Cisco VPN Client v3.x and the Cisco VPN 3002 Hardware Client.

Note The PIX Firewall already acts as a central site VPN device and supports the termination of remote access VPN clients.

Factory Default Configurations for the PIX 501 and PIX 506/506E

The PIX 501 (since its introduction) and the PIX 506/506E ship with factory-default configurations as of PIX Firewall software Version 6.2. (The PIX 501 and PIX 506/506E can be reset to their factory default configuration with the **configure factory-default** command.) For more information on the PIX 501 and PIX 506/506E default configurations, please refer to the *Cisco PIX 501 Firewall Quick Start Guide* and the *Cisco PIX 506/506E Firewall Quick Start Guide.*

Failover Enhancements

PIX Firewall software Version 6.2 enhances failover functionality so that the standby unit in a PIX Firewall failover pair can be configured to use a virtual MAC address. This eliminates potential "stale" ARP entry issues for devices connected to the PIX Firewall failover pair, in the unlikely event that both PIX Firewalls in a failover pair fail at the same time and only the standby unit remains operational.

In addition, the performance of Stateful Failover has been enhanced.

ILS Fixup

PIX Firewall software Version 6.2 provides an Internet Locator Service (ILS) fixup to support NAT for ILS and Lightweight Directory Access Protocol (LDAP). Also, with the addition of this fixup, the PIX Firewall supports H.323 session establishment by Microsoft NetMeeting. Microsoft NetMeeting, SiteServer, and Active Directory products leverage ILS, which is a directory service, to provide registration and location of endpoints. ILS supports the LDAP protocol and is LDAPv2 compliant.

LAN-Based Failover

LAN-based Failover extends PIX Firewall failover functionality to operate through a dedicated LAN interface, without the serial failover cable. This overcomes the distance limitation of the current serial cable. Failover configuration synchronization can now occur through the serial cable or a LAN interface. However, the PIX Firewall failover pair must be on the same subnet, and the PIX Failover model remains a hot-standby model, with one unit active and the other standby.

For LAN-based Failover, use a dedicated switch or hub (or VLAN) to connect the PIX Firewall failover pair so that the secondary unit can detect the failure of the dedicated LAN failover interface of the primary unit and become active. Crossover Ethernet cables cannot be used to connect the LAN-based Failover interface. Additionally, we recommend that you dedicate a LAN interface for LAN-based Failover, but the interface can be shared with Stateful Failover under lightly loaded configurations.

Multicast Support (IGMP v2 and Stub Multicast Routing)

PIX Firewall software Version 6.2 enables you to statically configure multicast routes or use an IGMP helper address for forwarding IGMP reports and leave announcements.

The following summarizes multicast support in this release:

- Access-list filters can be applied to multicast traffic to permit or deny specific protocols and ports.
- NAT and PAT can be performed on the multicast packet source addresses only.
- Multicast data packets with destination addresses in the 224.0.0.0/24 address range are not forwarded. However, everything else in the 224.0.0.0/8 address range is forwarded.

- IGMP packets for address groups within the 224.0.0.0-224.0.0.255 range are not forwarded because these addresses are reserved for protocol use.
- NAT is not performed on IGMP packets. When IGMP forwarding is configured, the PIX Firewall forwards the IGMP packets (report and leave) with the IP address of the helper interface as the source IP address.

Network Time Protocol (NTP) Support

The Network Time Protocol (NTP) synchronizes the times of devices operating over an IP data network.

PIX Firewall software Version 6.2 supports NTP, enabling the PIX Firewall to act as an NTP client and synchronize its time to a network time server. This enables the PIX Firewall to maintain precise network time for logging and certificate revocation list (CRL) validation. NTP server mode is not supported because the firewall would have to allow incoming requests to open ports, which is a security risk.

PIX Firewall software Version 6.2 supports Version 3 of NTP as this is currently the most common version in use and is the highest version supported by Cisco IOS software. The NTP authentication mechanism uses MD5 and is compatible with Cisco IOS software.

Object Grouping

To simplify your configuration, object grouping is supported in PIX Firewall software Version 6.2. object grouping enables you to define groups of objects such as hosts, IP addresses, or network services. You can use these groups, for example, when you create and apply access rules. When you include a PIX Firewall object group in a PIX Firewall command, it is the equivalent of applying every element of the object group to the PIX Firewall command.

Packet Capture

PIX Firewall software Version 6.2 supports packet capture. The PIX Firewall packet capture provides the ability to sniff or “see” any traffic accepted or blocked by the PIX Firewall. Once the packet information is captured, you have the option of viewing it on the console, transferring it to a file over the network using a TFTP server, or accessing it through a web browser using Secure HTTP. However, the PIX Firewall does not capture traffic unrelated to itself on the same network segment, and this packet capture feature does not include file system, DNS name resolution, or promiscuous mode support.

PIX 501 User Licensing and VPN Support Enhancements

The PIX 501 can act as a VPN headend, supporting up to five remote VPN users. These remote VPN users count against the total number of VPN peers supported by the PIX 501, which is five.

The PIX 501 supports up to 10 active users on the inside network (an optional 50-user license is also available). A user is considered active when any one or more of the following is true:

- The user has passed traffic through the PIX in the last xlate timeout seconds.
- The user has an established NAT or PAT translation through the PIX Firewall.
- The user has an established TCP connection or UDP session through the PIX Firewall.
- The user has an established user authentication through the PIX Firewall.

PIX Firewall Image Flash Compression

By default, PIX Firewall software Version 6.2 compresses the PIX Firewall image stored in Flash memory to optimize memory usage.

Port Address Translation (PAT) for H.323 and SIP fixups

PIX Firewall software Version 6.2 enhances support for the existing H.323 and SIP fixups by adding support for Port Address Translation (PAT). Adding support for PAT with H.323 and SIP enables our customers to expand their network address space using a single global address.

PPPoE Support

PIX Firewall software Version 6.2 supports Point-to-Point Protocol over Ethernet (PPPoE). (PPPoE provides a standard method for using PPP authentication over an Ethernet network and is used by many Internet service providers (ISPs) to grant client machine access to their networks, commonly through DSL.) PPPoE is only supported on the outside interfaces of the PIX 501 and PIX 506/506E.

Software Performance Enhancements

PIX Firewall software Version 6.2 has a number of internal software performance enhancements.

TurboACL

PIX Firewall software Version 6.2 supports TurboACL. TurboACL enhances the performance of PIX Firewall access list processing by providing an access list match in a deterministic amount of time for small and large access control lists (ACLs). (TurboACL compiles ACLs into a set of lookup tables, while maintaining first-match requirements. Packet headers enable you to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries.)

URL FIltering Enhancements

PIX Firewall software Version 6.2 supports N2H2 URL filtering services for URLs up to 1159 bytes.

For Websense, long URL filtering is supported for URLs up to 4096 bytes in length.

Additionally, this release provides a configuration option to buffer the response from a web server if its response is faster than the response from either an N2H2 or Websense filtering service server. This prevents the web server's response from being loaded twice.

For technical documentation on new features in previous PIX Firewall software versions, refer to the following website:

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

Important Notes

This section describes important notes for the 6.2(2) release.

Denying ICMP Traffic to the Outside Interface

By default the PIX Firewall denies all inbound traffic through the outside interface. Based on your network security policy, you should consider configuring the PIX Firewall to deny all ICMP traffic to the outside interface, or any other interface you deem necessary, by entering the **icmp** command. The **icmp** command controls ICMP traffic that terminates on the PIX Firewall. If no ICMP control list is configured, then the PIX Firewall accepts all ICMP traffic that terminates at any interface (including the outside interface).

For example, to deny all ICMP traffic, including ping requests, to the outside interface enter:

```
icmp deny any outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

For more information about the **icmp** command, refer to the *Cisco PIX Firewall Command Reference* at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/gl.htm#xtocid5

Preventing Fragmented Packets

By default the PIX Firewall accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the PIX Firewall to prevent fragmented packets from traversing the firewall by entering the **fragment chain 1** *interface* command on each interface. Setting the limit to 1 means that all packets must be whole; that is, unfragmented.

For example, to prevent fragmented packets on the outside and inside interfaces enter:

```
fragment chain 1 outside
fragment chain 1 inside
```

Continue entering the **fragment chain 1** *interface* command for each additional interface on which you want to prevent fragmented packets.

For more information about the **fragment** command, refer to the *Cisco PIX Firewall Command Reference* at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/df.htm#xtocid15

The PIX Firewall also includes FragGuard for additional IP fragmentation protection. For more information, refer to the *Cisco PIX Firewall and VPN Configuration Guide* at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/overvw.htm#1046527

Downloading PIX Firewall Image

Only Fast Ethernet cards can be used in monitor mode; Gigabit Ethernet cards cannot be used in monitor mode. Additionally, Fast Ethernet cards in 64-bit slots on the PIX 535 are not visible in monitor mode. This 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.

PIX 535 Interfaces

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.

Table 2 summarizes the performance considerations of the different interface card combinations.

Table 2 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 share bus 1 with a slower card.

Restrictions

Starting with PIX Firewall software Version 6.0(1), FDDI, PL2, and Token Ring interfaces are not supported.

Starting with PIX Firewall software Version 6.0(1), PFM is no longer supported; PFM has been replaced by the Cisco PIX Device Manager (PDM).

Starting with PIX Firewall software Version 6.0(1), and in all subsequent higher versions, the PIX Firewall Classic, PIX10000, and PIX 510 platforms are not supported.

Caveats

The following sections describe the caveats for the 6.2(2) release.

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

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

Open Caveats - Release 6.2(2)

The caveats in Table 3 are yet to be resolved in this release.

Table 3 Open Caveats

ID Number	Software Release 6.2(2)	
	Corrected	**Caveat Title**
CSCds54310	No	Traceback (ci/console) doing sh map, IPSec tunnel exists.
CSCds80108	No	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.
CSCdv91040	No	Slow response to write mem command when heavy traffic load.
CSCdw00291	No	402103 message for ICMP, although the identities in the message is ok.
CSCdw04354	No	PIX authentication is vulnerable to incomplete authentications.
CSCdw25718	No	uauth_thread uap->proxy 0 scrolling on console & perf.degraded.
CSCdw29206	No	Reboot with traceback while running ipsec stress on PIX-501.
CSCdw34273	No	Watchdog with overlapping static and dynamic PAT address.
CSCdw37960	No	VSA in accounting records not defined correctly.
CSCdw81126	No	PIX sourced UDP traffic to non-existing ip may use many blocks.
CSCdx09368	No	traceback upgrading to 6.2 with failover.
CSCdx10962	No	VPNC/RMS: IKE fails after RMS is triggered (bad config).
CSCdx17123	No	Traceback in isakmp receiver while testing xauth aaa rollover, ire.

Table 3 Open Caveats (continued)

ID Number	Software Release 6.2(2)	
	Corrected	Caveat Title
CSCdx26515	No	DHCPD: PIX fails to renew lease with a Cisco 7935 Conference Phone.
CSCdx48302	No	PIX 501 console unable to view debug crypto commands.
CSCdx54753	No	out of mem, telnet shutdown with PIX-501 and 1000 igmp join groups.
CSCdx60802	No	CPU Utilization 80-85% when PIX flooded with SIP Invite Messages.
CSCdx67314	No	Traceback on reloading IRE2141 with 0KB and no thread name.
CSCdx72090	No	Traceback in ci/console after upgrade to 6.2.
CSCdx78331	No	PIX crash,Thread Name: pix/intf0 (Old pc 0x800b1480 ebp 0x811d195c).
CSCdx78907	No	traceback on no thread name when upgrade to 6.2.2 from 6.1.4
CSCdx79285	No	IKE nego failed with Invalid SPI notification between 501 & 520.
CSCdx80701	No	H323: H225 channel denied though ACF seen by PIX.
CSCdx81167	No	FTP long banner problem when using PIX AAA - v6.2.1.
CSCdx81284	No	PKI: PIX cannot poll CRL after reboot.
CSCdx81692	No	Write Net sources from wrong interface.
CSCdx84022	No	performance degradation with tcp intercept; block depletion.
CSCdx84107	No	SIP: 2nd 200 OK from Cancel on same interface dropped.
CSCdx84647	No	PIX rekeys QM continuously w/ kilobytes lifetime set to certain value.
CSCdx85168	No	When you type show ssh session in your browser you fail to get debug.
CSCdx85433	No	PPPoE:Store-local username/password lost from flash if changed.
CSCdx86769	No	SIP PAT: should add port to Via if it is not present.
CSCdx87332	No	Traceback: While testing SIP PAT.
CSCdx87400	No	SIPPAT: Outbd Call from Px to Px fails with Static PAT (same addr).
CSCdx88350	No	Traceback no thread name when upgraded from 6.0.4 to 6.2.2.
CSCdx89025	No	PKI: memory leak when requesting and denying certificate requests.
CSCdx89336	No	Temporary 1550 byte block exhaustion with udp traffic.
CSCdx89579	No	PIX 525 Crashes intermittently.
CSCdx90840	No	Failure Detected - No Block Memory (size 272) in failover.
CSCdx91760	No	Reload hangs PIX515: This is after upgrading new bupgdisk.

Resolved Caveats - Release 6.2(2)

The caveats in Table 4 are resolved in this release.

Table 4 Resolved Caveats

ID Number	Software Release 6.2(2)	
	Corrected	**Caveat Title**
CSCds12981	Yes	Ssh client disconnected on typing any letter while debug packet on it.
CSCds54310	Yes	Traceback (ci/console) doing sh map, IPSec tunnel exists.
CSCdw94583	Yes	PIX should use the same radius request ID for the same request.
CSCdx35035	Yes	url-block feature not working for N2H2(PAT/NAT) and Websense (PAT).
CSCdx35823	Yes	Unexpected reaction to TACACS+authenticated HTTP packet.
CSCdx39570	Yes	long switchover time when running lan-based fover.
CSCdx41456	Yes	rip version 1 default sent out with broadcast ip, but multicast mac.
CSCdx42706	Yes	Clear uauth for selected user clears all user authentications.
CSCdx45064	Yes	SIP:PIX does not correctly parse <> in the To:and From:
CSCdx45069	Yes	stateful failover broken with dynamic nat.
CSCdx45370	Yes	PIX - Removing Outside NAT command requires ordered arguements.
CSCdx47789	Yes	PIX Reboots when receiving fragmented SIP INVITE messages.
CSCdx47975	Yes	Downloadable ACLs do not work for VPN users (Xauth).
CSCdx48296	Yes	SIP:Registered dynamic PAT xlates time out early.
CSCdx48817	Yes	PIX not correctly opening a conduit for SIP RTP.
CSCdx48930	Yes	Traceback in handling ICMP error from echo-reply over PAT.
CSCdx49424	Yes	traceback:lan_fover_thread. clear config all right after reload.
CSCdx52407	Yes	Static route getting overwritten by RIP learnt route.
CSCdx53187	Yes	PIX as EZVPN client using NEM does not properly establish IPSec SAs.
CSCdx54495	Yes	SIP:new content length is incorrect if > 255.
CSCdx57852	Yes	ISAKMP Failure with seconds/kilobytes lifetime set to certain values.
CSCdx58065	Yes	SIP:named static ip address causes crash or call failure.
CSCdx60754	Yes	DHCPC:Address becomes 127.0.0.1 if configure dhcp to static to PPPoE.
CSCdx60807	Yes	PPP:padded frame length not adjusted. causes tcp seq num error.
CSCdx61012	Yes	SIP:200 OK for the BYE not passing thru PIX.
CSCdx62838	Yes	PPPoE:Code field being tested as type short S/B char.
CSCdx64091	Yes	Cannot connect to HTTP server,SSL:crypto_pki_get_certificates failed.
CSCdx65119	Yes	PIX waiting for enable password restarts when closing.

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.2(2)	
	Corrected	Caveat Title
CSCdx68948	Yes	402103:Identity doesn't match negotiated identity (ip).
CSCdx69408	Yes	dhcp client failed to get addr from QWEST VDSL router.
CSCdx70054	Yes	SIP:Compact form of Content-Length not parsed.
CSCdx71320	Yes	replication does not start by power OFF/ON the Standby.
CSCdx72488	Yes	config different icmp types in access-list not accepted.
CSCdx72571	Yes	active-x filtering is not done when there are no quotes.
CSCdx76813	Yes	assertion applying a command during config replication.
CSCdx77189	Yes	Generating RSA key on active causes stand-by PIX to crash.

Open Caveats - Release 6.2

The caveats in Table 5 are yet to be resolved in this release.

Table 5 Open Caveats

ID Number	Software Release 6.2(1)	
	Corrected	Caveat Title
CSCds54310	No	Traceback (ci/console) doing sh map, IPSec tunnel exists.
CSCdx09368	No	traceback upgrading to 6.2 with failover
CSCds10112	No	Traceback (Crypto PKI RECV) after twice enrolling and getting denied
CSCdv21580	No	Cert enrollments fails with 2048bits sp keys with serial/ip options
CSCdv91040	No	Slow response to **write mem** command when heavy traffic load.
CSCdw29206	No	Reboot with traceback while running ipsec stress on PIX-501
CSCdw81126	No	PIX sourced UDP traffic to non-existing ip may use many blocks
CSCdw94583	No	PIX should use the same radius request ID for the same request
CSCdx10962	No	VPNC/RMS: IKE fails after RMS is triggered (bad config)
CSCdx17123	No	Traceback in isakmp receiver while testing xauth aaa rollover, ire
CSCdx26515	No	PIX fails to renew lease with a Cisco 7935 Conference Phone
CSCdx27406	No	Watchdog timeout for user with >190 dACL and debug radius on.
CSCdx27920	No	Traceback when PPPoE configured and AUS triggered with bad config.
CSCdw34273	No	Watchdog with overlapping static and dynamic PAT address

Resolved Caveats - Release 6.2

The caveats in Table 6 are resolved in this release.

Table 6 Resolved Caveats

ID Number	Software Release 6.2(1)	
	Corrected	**Caveat Title**
CSCdj76633	Yes	Outside Source NAT
CSCdm39125	Yes	ILS (internet locator service) fails when using NAT
CSCdm44118	Yes	feature key should not require installing new image
CSCdm47044	Yes	PIX enable authentication only requires login password
CSCdm74651	Yes	PIX: Provide CPU utilization info over SNMP
CSCdr48204	Yes	PIX Need Network Time Protocol Support - NTP
CSCdr61507	Yes	Duration and Byte Count added to SYSLOG message
CSCdr84768	Yes	PIX Enh. Command to clear conduit or access-list hit count
CSCds16799	Yes	Websense creates multiple http gets without passing data
CSCds35349	Yes	PIX needs tcpdump/snoop like packet debugging
CSCdt11135	Yes	DNS UDP lookups through PIX dont show fport correctly
CSCdt17577	Yes	PIX can’t send filter URLs to WebSense longer than 1159
CSCdt27445	Yes	telnet to PIX & login Welcome message prevents prosecution
CSCdt42853	Yes	H225: should create new TPKT & discard original if TPKT recvd only
CSCdt47829	Yes	PIX won’t learn MAC addresses in range 0008.xxxx.xxxx
CSCdt53815	Yes	Fixup RAS drops SNMP packets
CSCdu14966	Yes	Nat 0 is not working properly for IPSec
CSCdu27669	Yes	Virtual MAC support to allow sec. PIX to boot by
CSCdu59514	Yes	PIX syslogs sent with standby rather than active IP
CSCdu78272	Yes	SIP debugs does not show correct message ID
CSCdu85817	Yes	hostobjdb being corrupted.
CSCdv24986	Yes	Assertion if conf net and command **write mem** in config file.
CSCdv26953	Yes	Skinny: Need to update to Version 3.1 code
CSCdv32237	Yes	Active-X filter does not work correctly
CSCdv39306	Yes	PIX loses ARP entry for HSRP address
CSCdv40404	Yes	IKE mode config bug - causes PIX crash with dump
CSCdv53837	Yes	after 1st IPSEC peer down, 60 second delay before switch
CSCdv55044	Yes	ESP packets routed basing on encapsulated destination address
CSCdv56552	Yes	Session counts are inconsistent UDP vs. TCP
CSCdv57122	Yes	AAA proxy limit exceeded and out of Tcb_user errors
CSCdv57570	Yes	PIX crashes when vpn client 3.1 connects

Table 6 Resolved Caveats (continued)

ID Number	Software Release 6.2(1)	
	Corrected	**Caveat Title**
CSCdv60361	Yes	H.225: Call fails when newly encoded message is smaller
CSCdv63087	Yes	ENH: need debugs for hardware accelerator (VAC)
CSCdv64039	Yes	TCP connection to PIX from token ring client hangs
CSCdv65961	Yes	1550 byte blocks go to zero, PIX stops passing traffic
CSCdv72013	Yes	H323: Inbound call w/ indirect voice due to early removal of data
CSCdv74412	Yes	pptp - non-zero reserved field in header
CSCdv75812	Yes	VoIP fixups drop 1-byte TCP keep-alive
CSCdv83025	Yes	DNS Flakiness. Some outbound UDP DNS replies being denied by PIX
CSCdv86755	Yes	icmp type is not correctly interpreted with aaa authentication
CSCdw00328	Yes	wrap into debug/rate limit invalid hdr.len in isakmp check
CSCdw00398	Yes	Alias with overlapping networks broken
CSCdw00450	Yes	should not accept broadcast/subnet addresses for interfaces
CSCdw01653	Yes	PIX stops prompting for Authentication - out of tcb objects
CSCdw04410	Yes	no failing over should be possible while replicating the config
CSCdw05284	Yes	PIX Accounting records need to use unique NAS-Port value per session
CSCdw10863	Yes	High DNS query-rate (more than 4000/second) causes memory exhaustion
CSCdw10880	Yes	PIX snmp response on failover status incorrect after PIX failover
CSCdw11539	Yes	PIX dhcp client need to get new addr if current lease expired
CSCdw15057	Yes	Large DNS query message stops old connection removal
CSCdw17097	Yes	PIX - DHCP client does not accept dhcp offer with broadcast bit set
CSCdw17161	Yes	With AAA, incorrect syslog when telnet fails and no log when succ.
CSCdw17490	Yes	ENH - PIX needs a **show run** and **show start** command
CSCdw18939	Yes	executing config floppy, no errors report and config is not restored
CSCdw24283	Yes	Traceback after entering **show xlate local** command.
CSCdw25718	Yes	uauth_thread uap-
CSCdw27548	Yes	PIX is sending wrong authentication type with RIP v2
CSCdw36415	Yes	PIX traceback in ci/console after assertion in limit.c.
CSCdw38189	Yes	memory leak with ipsec/certificates + packet loss + delay + bad cert
CSCdw39040	Yes	PIX denies its own ICMP unreachable with PPTP
CSCdw42039	Yes	H323: Should not drop RAS packets if
CSCdw44380	Yes	PIX crash in fover_rep when strange auth-prompt configured
CSCdw45045	Yes	SIP: PIX does not NAT some Via fields
CSCdw45615	Yes	standby PIX does not return correct MIB-II ipAddrTable

Table 6 Resolved Caveats (continued)

ID Number	Software Release 6.2(1)	
	Corrected	**Caveat Title**
CSCdw46749	Yes	Incorrect processing of ICMP error with nat 0 0 0
CSCdw49277	Yes	RIP2 updates case PIX interface loss of communication and failover
CSCdw52033	Yes	PIX - need syslog when Embryonic limit is exceeded
CSCdw53729	Yes	need to warn user if pri connector plug into PIX with fover only lic
CSCdw54290	Yes	PIX - uptime in show ver of Standby PIX wraps at 49 days
CSCdw55700	Yes	H323: TCP connections incorrectly marked with Fin flag
CSCdw56153	Yes	IKE memory leak w/ PFS enabled crypto map
CSCdw57969	Yes	static arp entries replying for the arp requests
CSCdw60558	Yes	PIX ignores subnet mask when natting using the **global** command
CSCdw62717	Yes	VPN 3.x Client to PIX - DPD not working correctly
CSCdw63021	Yes	PIX crashes upon receiving malformed SNMP packet
CSCdw64258	Yes	PIX crash with traceback triggered by uauth
CSCdw65148	Yes	SIP: Should support Notify with Subscribe
CSCdw67516	Yes	Two PIX535s configured in failover mode keep rebooting
CSCdw71916	Yes	name with hyphen cause dhcpd cmd parsing to fail
CSCdw72647	Yes	PIX-2-108002 should not emit non-printable chars w/o encoding
CSCdw74095	Yes	PKI: certificate with serial number 0 gets lost upon reload
CSCdw78269	Yes	Authentication stops through PIX, must reboot or clear tcp stats
CSCdw87877	Yes	Workaround for checkpoint limitation ftp authentication
CSCdw94427	Yes	sqlnet fixup creates incorrect embryonic for redirect
CSCdx06775	Yes	allow ssh clients with unsupported features enabled to ssh to PIX
CSCdx06796	Yes	Traceback in Crypto PKI RECV thread
CSCdx10247	Yes	Skinny: Need debug when rejecting msg because of invalid msg ID
CSCdx11660	Yes	NIC media and driver type field intermingling
CSCdx25089	Yes	PIX intercept bad IPSec packet causing Watchdog timeout failure

Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN Client Version 3.x documentation at the following websites:

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

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

Cisco provides PIX Firewall technical tips at the following website:

http://www.cisco.com/warp/public/707/index.shtml#pix

Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CCO account you can visit the following websites for assistance:

TAC Customer top issues for PIX Firewall:

http://www.cisco.com/warp/public/110/top_issues/pix/pix_index.shtml

TAC Sample Configurations 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

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following 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 is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

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

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the "Leave Feedback" at the bottom of the Cisco Documentation home page.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

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