



# Cisco PIX Firewall Release Notes Version 6.2(3)

---

July 2003

## Contents

This document includes the following sections:

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

## 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)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

PIX Firewall software Version 6.2(3) provides the secure networking features included in previous releases and adds support for the following features:

- [Incomplete Crypto Map Enhancements](#)

PIX Firewall software Version 6.2(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 Filtering 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 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:

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(3)

#### Incomplete Crypto Map Enhancements

Every static crypto map must define an access list and an IPsec peer. If either is missing, the crypto map is considered incomplete and a warning message is printed. Traffic that has not been matched to an complete crypto map is skipped, and the next entry is tried. Failover hello packets are now exempt from the incomplete crypto map check; previously they were dropped. Use the **show conf** command to ensure that every crypto map is complete.

For more information on this feature, refer to “[Crypto Maps](#)” in the *Cisco PIX Firewall and VPN Configuration Guide*. For a complete description of the command syntax for this new command, refer to the *Cisco PIX Firewall Command Reference*.

## New Software Features in Release 6.2(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 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](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](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](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

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:  
[http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)

To become a registered cisco.com user, go to the following website:  
<http://tools.cisco.com/RPF/register/register.do>

## Open Caveats - Release 6.2(3)

The caveats in [Table 3](#) are yet to be resolved in this release.

**Table 3** *Open Caveats*

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCdv04354	No	PIX needs to better handle incomplete authentications.
CSCea43211	No	Potential failure of TCP connection recovery scenario through PIX

## Resolved Caveats - Release 6.2(3)

The caveats in [Table 4](#) are resolved in this release.

**Table 4** *Resolved Caveats*

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCdv33495	Yes	static PAT and fixup ftp breaks ACTIVE ftp
CSCdw00291	Yes	402103 message for ICMP, although the identities
CSCdw25718	Yes	uauth_thread uap->proxy 0 scrolling on console &
CSCdw34273	Yes	Watchdog with overlapping static and dynamic PAT address
CSCdw37960	Yes	VSA in accounting records not defined correctly
CSCdw77148	Yes	cfwConnectionStatValue snmpget is incorrect

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCdw82839	Yes	H323:wrong TCP length in proxy ACK with TCP options
CSCdx81167	Yes	FTP long banner problem when using PIX AAA - v6.2.1
CSCdx84107	Yes	SIP:2nd 200 OK from Cancel on same interface dropped
CSCdx85024	Yes	H323: Error decoding tunneled H245 message
CSCdx86769	Yes	SIP PAT: should add port to Via if it is not present
CSCdx87332	Yes	Traceback: While testing SIP PAT
CSCdx87758	Yes	PIX should send source IP of the traffic being
CSCdx89579	Yes	PIX 525 Crashes intermittently
CSCdx90840	Yes	Failure Detected - No Block Memory (size 272) in failover
CSCdx95442	Yes	FTP does not honor norandomseq with PAT
CSCdx95494	Yes	PIX w/ Websense: Out of order (non-sequential TCP packet)
CSCdy01111	Yes	Cant TFTP across the VPN between router and PIX (w/VPN accl
CSCdy02422	Yes	PIX sending cookies in wrong order in initial contact
CSCdy09114	Yes	WinCE and Pocket PC2002 clients cannot get IP address from
CSCdy13293	Yes	PIX H225 fixup protocol breaks zero byte TCP keepalives
CSCdy14129	Yes	WDT possibility in fixup_h245
CSCdy16100	Yes	Block 256 running LOW with syslog severity level =
CSCdy16100	Yes	Block 256 running LOW with syslog severity level = information
CSCdy17145	Yes	SIP: Wrong PAT port added to Contact:field
CSCdy17426	Yes	PIX501:vpn tunnel LED is on even without any vpn tunnel
CSCdy19067	Yes	SIP: does not open conn based on Route info for responses
CSCdy23522	Yes	PIX 525 crashing in fixup xdmcp
CSCdy23887	Yes	Secondary PIX in a stateful failover keeps rebooting
CSCdy27157	Yes	Telnet to PIX does not prompt for username or password
CSCdy27158	Yes	PIX gig interface does not support non-auto negotiation
CSCdy27185	Yes	H323:new TTL from registration is not updated
CSCdy28750	Yes	SIP: Call forwarding with Pingtel phones do not work
CSCdy29514	Yes	TCP window size > 64k breaks NT drive maps through PIX
CSCdy30094	Yes	H323:PIX should not drop packets when TTL in RCF > TTL in
CSCdy30421	Yes	PIX: Unnecessary failover happens when issuing write
CSCdy31615	Yes	ability to disable SIP UDP fixup
CSCdy34949	Yes	Command aaa authentication include exclude ip rejected on
CSCdy39216	Yes	Easy VPN Client should have the option to send DPD when
CSCdy40004	Yes	PIX may reload at rn_match with high number of routes
CSCdy41134	Yes	SIP: Route addr not NATd if using PAT

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCdy43488	Yes	Standby PIX misrepresenting the status of an interface/s
CSCdy44911	Yes	SIP: Session not found when port added to To and/or From
CSCdy47457	Yes	standby cfg replicate fails after removing and connecting
CSCdy49165	Yes	PIX - snmpwalk from net connected to pix via vpn causes
CSCdy51806	Yes	SIP:Registered xlates for 6th+ endpoint using PAT times
CSCdy51810	Yes	PIX outside subnet IP is vulnerable to TCP/22 attacks
CSCdy53135	Yes	FTP port command can cause the PIX to stop responding
CSCdy54211	Yes	URL filtering in 6.2.1 is causing incomplete %PIX-5-304001
CSCdy56000	Yes	SIP: Fails to find session when Call-ID differs in # of LWS
CSCdy58717	Yes	xlate table does not timeout entries.Need clear xlate to
CSCdy64251	Yes	Enable authentication does not prompt for TAC+ username
CSCdy65109	Yes	first HTTP GET after uauth lacks CR in the end of request
CSCdy68931	Yes	Call transfer/no answer fails. Pix doesn't send back 200-OK
CSCdy72759	Yes	IKE rekey problem between 501 vpnclient and VPN 3000
CSCdy72967	Yes	PIX truncates syslogmesg on 255 bytes boundary
CSCdy74157	Yes	PIX - WDT traceback in ci/console when removing
CSCdy78026	Yes	Inbound TCP connection denied (2nd SYN having same dest
CSCdy78256	Yes	PIX should send gratuitous ARP if new Primary inserted in
CSCdy85743	Yes	inbound AAA authentication on pix breaks for DNS requests
CSCdz00255	Yes	Traceback in isakmp_receiver thread
CSCdz01677	Yes	vpngroup passwd for (default) grp overwrites lan-lan
CSCdz06901	Yes	Sip fails with Error-no matching session found for
CSCdz07228	Yes	VoIP embryonic conn lookup should match on exact match
CSCdz07525	Yes	npdisk does not remove LOCAL authorization config lines
CSCdz07673	Yes	PIX - SSH via CW2000 will crash PIX during Inventory Update
CSCdz08403	Yes	VoIP: Some embryonic TCP conns not marked as Embryonic
CSCdz09957	Yes	PIX - DHCP Client - remove minimum lease time restriction
CSCdz14833	Yes	SIP: No matching session found when lws after; before tag
CSCdz16846	Yes	PIX IPSec SA remaining lifetime differs significantly on
CSCdz17578	Yes	PIX - traceback in tcp_slow from AAA issue
CSCdz17893	Yes	Active MAC of Giga Ethernet remains on Standby after
CSCdz18345	Yes	100,000+ ACL causes crash during turboacl compilation
CSCdz22128	Yes	H245:data structures deleted early & causes out of state,
CSCdz23236	Yes	PIX crashes with 557poll old pc 0x800aa33f when MSExchange
CSCdz29265	Yes	SIP: error in sip_skip_lws()

Table 4 Resolved Caveats (continued)

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCdz31844	Yes	PIX does not pass SIP 200 OK messages
CSCdz32478	Yes	H.323:one-way audio for scenario with POTS and Skinny
CSCdz35775	Yes	Static w/ dns option taking precedence over nat 0
CSCdz37904	Yes	tftp accepts ack from a different host
CSCdz45121	Yes	DNS doctoring is not being performed with the outside
CSCdz49886	Yes	H323:RTCP conns sometimes not marked with H flag
CSCdz51937	Yes	big number of statics impacts the performance
CSCdz54598	Yes	SIP: content length wrong if URI contains l:
CSCdz57754	Yes	uauth:absolute timeout gets reset upon the tacacs authorization
CSCdz58273	Yes	PIX crashes while running out of memory when building new
CSCdz58644	Yes	SIP:UDP conns not opened from 100 Trying response
CSCdz60418	Yes	PIX reload due to stack overflow of the uauthN thread
CSCdz62308	Yes	PIX - filtering with N2H2 generates 304004 syslog messages
CSCdz64205	Yes	Authentication Fails with PIX Sending Incorrect Radius
CSCdz74497	Yes	Unable to pass traffic after dhcp renew
CSCdz82967	Yes	SIP: Drop 200 OK due to w/ or w/o display-name of From
CSCea08170	Yes	corrupted lu update msg crash standby pix
CSCea15381	Yes	PPPoE and EZVPN mem leak with pix622124diag.bin
CSCea18759	Yes	Netmeeting: whiteboard and other T.120 features not
CSCea20540	Yes	CHUNKPARTIAL attempted..error received when ftping TACL to
CSCea39838	Yes	PIX uauth becomes unresponsive after auth in progress
CSCea50882	Yes	PIX allocates more uauth_net objects than necessary.
CSCea61756	Yes	PIX: Tracebacks in lu_rx thread when peer is running diff
CSCea70416	Yes	after burst traffic, PIX need to be rebooted
CSCea70434	Yes	Inside to outside DNS server queries translated by
CSCea76209	Yes	SIP: Calls fail if it is not completed after 30 seconds
CSCea79747	Yes	SIP: content-length not modified if body is not SDP & is
CSCea82252	Yes	SIP: PIX does not open the sip_media conn via 180/183
CSCea83595	Yes	SIP:PIX does not update xlate timer when receiving
CSCea84806	Yes	PIX arp for deleted static after clear xlate
CSCea86451	Yes	SIP: sip_sessions should be deleted based on Expires:value
CSCea89724	Yes	Investigate sending a warning msg to CLI before making
CSCea89765	Yes	Keepalive/heartbeat do not pass thru PIX, due to
CSCea90382	Yes	SIP:PIX doesn't open dynamic sip_media if call comes from outside
CSCeb01565	Yes	PIX crash upon receipt of malformed IPSec/ESP packet -

**Table 4** Resolved Caveats (continued)

ID Number	Software Release 6.2(3)	
	Corrected	Caveat Title
CSCeb05297	Yes	PIX might reboot with many tunnels after issuing show vpdn
CSCeb06362	Yes	SIP: transient connections not timing out after 1 minute
CSCeb11246	Yes	SIP:PIX does not open media when receiving Ack w/ SDP
CSCeb11274	Yes	SIP:PIX drop 200 OK from Transfer Target during Call
CSCeb13380	Yes	max uauth queue len too short, users sporadically unable
CSCeb13449	Yes	SIP:PIX drop 202 response of REFER method during Call
CSCeb16907	Yes	SIP:PIX keep unnecessary xlate after SIP calls are
CSCeb23737	Yes	tcp intercept delay when embryonic threshold at max
CSCeb28943	Yes	PIX fails to delete SA when receiving invalid-spi notify
CSCeb33762	Yes	Segmented SMTP traffic not passed thru fixup

## 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](http://www.cisco.com/warp/public/110/top_issues/pix/pix_index.shtml)

TAC Sample Configs for PIX Firewall:

[http://www.cisco.com/cgi-bin/Support/PSP/psp\\_view.pl?p=Hardware:PIX&s=Software\\_Configuration](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](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](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](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](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](mailto: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](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](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 the documents listed in "[Related Documentation](#)" section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0304R)

Copyright © 2003 Cisco Systems, Inc.  
All rights reserved.