



Text Part Number: 78-6423-01

Release Notes for the PIX Firewall Manager Version 4.3(2)b

June 1999

This document describes how to install and configure the Cisco's PIX Firewall Manager for use with software versions 4.3 and 4.4.

Contents

- Introduction
- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Related Documentation
- Cisco Connection Online
- Documentation CD-ROM

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Introduction

The PIX Firewall Manager (PFM) lets you administer one or more PIX Firewall units, view syslog messages, and define customized alarms for each type of syslog message. You can use the PIX Firewall Manager to view, add, and modify the configuration of each PIX Firewall unit.

This version of PIX Firewall Manager does not support use of the new version 4.4 features, but will work with features that are common to both versions. PIX Firewall Manager version 4.3(2)b does not support the following version 4.4(1) features:

- 1 AAA—show RADIUS server, show TACACS+ server, show AAA authentication, show AAA authorization, and show AAA accounting
- 2 FDDI network interface cards
- 3 ActiveX blocking
- 4 The **timeout** command's new **half-closed** option

If you are using version 4.4(1), features not supported by PIX Firewall Manager version 4.3(2)b can be set from the PIX Firewall command line interface.

Note If you have a problem with PFM, save the pfm.log file immediately after the problem occurs so you can give it to Cisco's Technical Assistance Center (TAC).

Components

PIX Firewall Manager software includes these components:

- Management Server—a Windows NT service that runs in the background and receives requests from the Management Client, sends them to the specified PIX Firewall unit, and then passes the PIX Firewall's responses back to the Management Client. The Management Server starts automatically when the installation completes. An icon for the server does not display in the task bar.
- Management Client—a Java applet that you access from the network browser. The Management Client network browser must be Java 1.02 compliant. Refer to "Management Client Requirements" for more information.

PIX Firewall Manager provides two access levels: user-level with read-only (non-modifying) access and administrator-level with read and write access.

Diskettes for installing PIX Firewall Manager are provided in the PIX Firewall accessory kit.

If you are upgrading from a previous version of PIX Firewall Manager software, refer to the *Configuration Guide for the PIX Firewall Version 4.3*, which is included with your PIX Firewall accessory kit. This document has instructions for downloading the latest software. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for these instructions.

PIX Firewall Manager can be installed and uninstalled on Workstation and Server versions of Windows NT 4.0.

System Requirements

The following sections describe system requirements.

Windows NT Requirements

The Windows NT system on which you install the Management Server requires the following:

- Windows NT Workstation or Windows NT Server version 4.0 or later with Service Pack 3.
- The Windows NT system must contain a Pentium processor and at least 32 MB RAM.
- TCP/IP must be enabled and the system's IP address must not be dynamically allocated, such as with DHCP.
- The Windows NT system must be on the PIX Firewall's inside network.
- Users must be part of the PIX Admins or PIX Users groups on the Windows NT system. These two user groups and two temporary user accounts are created by the PIX Firewall Manager installation program. Refer to "Limiting Access to the Management Client" for more information on how to add users to these groups.

PIX Firewall Requirements

Note Each PIX Firewall you manage must have been configured with the PIX Firewall **telnet** command or PIX Firewall Setup Wizard to permit the Management Server to access the PIX Firewall. The PIX Firewall Setup Wizard is not available in version 4.4.

All PIX Firewall units managed by PIX Firewall Manager version 4.3(2)b must be running PIX Firewall software version 4.3(2), version 4.4(1) or later. To check the version of the PIX Firewall software, go to the PIX Firewall console and enter the **show version** command.

If you intend to manage PIX Firewall units on the outside network, each foreign unit must run Private Link and at least one firewall on the local network must also run Private Link. The local PIX Firewall must be configured to communicate with the foreign Private Link firewalls.

You must have console access to each local and foreign PIX Firewall you manage in order to perform the configuration required to run the PIX Firewall Manager. If you are managing remote firewalls, work with the site administrator to get the PIX Firewall to communicate with PIX Firewall Manager.

To configure each PIX Firewall unit from the Setup Wizard, follow the instructions in the *Quick Installation Guide for the PIX Firewall Version 4.3*. The PIX Firewall Setup Wizard is not available in version 4.4.

To configure each PIX Firewall unit from the command line, enter these commands at the PIX Firewall console:

- Step 1 enable**—to enter privileged mode. When prompted, enter the privileged mode password. The default is no password and you can press the **Enter** key at the prompt.
- Step 2 configure terminal**—to enter configuration mode.
- Step 3 nameif**—to specify the name or security level of the outside or optional third interface on the PIX Firewall. The inside interface cannot be renamed or given a different security level. Each security level must be a unique number between 0 and 99.
- Step 4 interface**—to set options for the Ethernet or Token Ring network interfaces.
- Step 5 ip address**—to assign IP addresses and network masks to each interface.

Step 6 telnet—to let the PIX Firewall communicate with the PIX Firewall Manager:

```
: Telnet for PIX Firewall Manager  
telnet Windows_NT_IP_Address 255.255.255.255
```

Replace *Windows_NT_IP_Address* with the IP address of the Windows NT system.

Add the comment before the **telnet** statement to ensure that the next person configuring the firewall knows the purpose of this **telnet** statement.

Step 7 link and linkpath—if you are managing remote PIX Firewall units, configure each for Private Link access. Refer to Chapter 2, “Configuring the PIX Firewall,” in the *Configuration Guide for the PIX Firewall Version 4.3* for information on configuring Private Link, and Chapter 5, “Command Reference,” to view the **link** command page for more information. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

Step 8 write memory—save the configuration in Flash memory.

All commands are described in the *Configuration Guide for the PIX Firewall Version 4.3* supplied in your PIX Firewall accessory kit. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

Management Server Requirements

The Management Server has the following requirements:

- Windows NT Workstation or Windows NT Server version 4.0.
- PIX Firewall Manager comes with a sound file, T1.AU, for the syslog audio alarm. All sound files must be in .AU format as follows:
 - mu-low: 8 bit
 - Sample Rate: 8000 Hz
 - Channel: mono

To use another .AU format sound file:

- Step 1** Place the sound file on the Windows NT system running the Management Server in the JClient\Netscape subdirectory of the Management Server's target directory.
- Step 2** Click the Management Client's **Setting** tab to modify the audio filename.
- All machines running the Management Server must be on the PIX Firewall's inside network.

Management Client Requirements

The Management Client has the following requirements:

- All machines running the Management Client must be on the PIX Firewall's inside network.
- The Management Client network browser must be Java 1.02 or 1.1 compliant.
- The following browsers are supported:
 - Netscape Navigator version 3.0 or 3.01.
 - Netscape Navigator Gold version 3.0 or 3.01.
 - Netscape Communicator version 4.0, 4.01, 4.02, 4.04, 4.05.
 - Netscape Navigator (standalone) version 4.0, 4.01, 4.02, 4.04, 4.05.

Note Using Netscape Navigator and Communicator version 4.04 or 4.05 with the JDK 1.1 Patch are not compatible with the Management Client. Additionally, Netscape Navigator and Communicator version 4.06 or later is not compatible with the Management Client. Earlier versions of Netscape browsers are available for download at the following URL:
[ftp://archive:oldies@archive.netscape.com/archive/index.html](ftp://archive.oldies@archive.netscape.com/archive/index.html)

— Microsoft Internet Explorer 4.0 version 4.72.3110.8; updated version: SP1.

The system running the browser must use Windows 95, Windows NT 4.0 Workstation, Windows NT 4.0 Server, or Solaris. On Windows 95 or Windows NT 4.0, 32 MB RAM is highly recommended.

New and Changed Information

Features

The PIX Firewall Manager provides the following features:

- Manage up to 10 PIX Firewall units from the PIX Firewall Manager.
- Configure most PIX Firewall features from the **Administrator** tab in the Management Client.
- Create common configurations for multiple PIX Firewall units from the **Common Configuration** tab in the Management Client.
- Encrypt all communications between the PIX Firewall and the PIX Firewall Manager.
- Generate reports using the report wizard from the **Alarm and Report** tab by clicking a PIX Firewall folder and then clicking the **Report** button.
- Generate a three-dimensional bar chart report showing network traffic through the PIX Firewall. Information on up to 50 hosts can be reported. Reports can be viewed but not printed from PIX Firewall Manager. You can use the extended reporting capability with Microsoft Excel 97 to print and export report information. The PIX Firewall Manager Excel database supports up to 64,000 entries.
- Generate reports of FTP and HTTP file transfer activity by host, including source IP address and filename. These reports are not available using Microsoft Excel 97.
- Generate the initial inbound and outbound connection statements in the PIX Firewall configuration using the **Tasks** button in the Management Client to access a series of dialog boxes.

Note The Tasks button generates statements in the PIX Firewall configuration that allow connections to or from hosts on internal (protected) networks. If you have additional configuration requirements, such as access control for outbound connections and user authentication or authorization, other configuration commands apply. Refer to the *Configuration Guide for the PIX Firewall Version 4.3* for detailed configuration information. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

- Avoid conflicts between Open Systems Solutions Private I and PIX Firewall Manager installed on the same system using the **SYSLOG Redirection** button on the **SYSLOG Notification Settings** tab. The **SYSLOG Redirection** button copies syslog event information received from port 514 to port 515.

- Set the time interval for updating syslog message files using an option in the **SYSLOG Notification Settings** tab.
- Capture quickly scrolling messages in the SYSLOG Message Window using the **Message Snapshot** button. The snapshot displays up to 200 lines of messages in a separate window. To display the SYSLOG Message Window, select the **SYSLOG Notification Settings** tab and change the Immediate SYSLOG Message setting to ON.

Refer to the *Configuration Guide for the PIX Firewall Version 4.3* for detailed information about PIX Firewall system features. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

Installation Notes

- 1 Each PIX Firewall you wish to manage must be running PIX Firewall version 4.3(2), 4.4(1), or later.
- 2 Each PIX Firewall you manage must have previously been configured with the PIX Firewall **telnet** command or PIX Firewall Setup Wizard to permit access to the PIX Firewall from the PIX Firewall Manager's Management Server. PIX Firewall Setup Wizard is not available in version 4.4.
- 3 A PIX Firewall Syslog Server (PFSS) is available for logging PIX Firewall event information on a Windows NT system. PFSS provides logging features not available with the PIX Firewall Manager (PFM), such as using TCP for highly reliable message delivery and control. PFM has features not available with PFSS, such as generating reports from syslog information.

The PIX Firewall does not support running both the PFM and PFSS applications at the same time. You must use either PFM or PFSS, but not both. For more information on installing and running PFSS, refer to the *Quick Installation Guide for the PIX Firewall Version 4.3*. If you are using PIX Firewall version 4.4(1), refer to the *Installation Guide for the PIX Firewall* for this information.

- 4 The Windows NT computer running the PIX Firewall Manager Management Client (graphical user interface) must have a network browser that is Java 1.02 compliant. Refer to "Management Client Requirements" for more information.
- 5 Selecting a menu item (or screen) is indicated by the following convention:
Select **screen1>screen2>screen3**.
- 6 The initial PIX Firewall Manager password is set to expire after 42 days. Refer to "Changing Passwords" for more information.
- 7 PIX Firewall Manager Version 4.3(2)b encrypts all communication with the PIX Firewall software version 4.3(2) or 4.4(1). Managing PIX Firewall units running earlier software versions is not supported.

- 8 After installation and setup, if you change the IP address of the Windows NT system, you need to update the FIREWALL.HTML file installed on the system. The file is in the JClient\Netscape subdirectory on the Management Server's target directory. In the FIREWALL.HTML file, swap the old IP address with the current IP address, which is only visible from the inside network.

Interface entries can be specified as either IP addresses or domain names; however, you must remember to log on to the management server using the exact entry listed in the FIREWALL.HTML file or an IP address security violation error message can appear. This message indicates the Management Server could not locate the interface specified in the FIREWALL.HTML file, having tried the possible interfaces on the Windows NT computer running the Management Server.

The sections that follow describe other installation topics.

Before Installing

Before installing PIX Firewall Manager, you need to know the following:

- Passwords
 - PIX Firewall privileged mode password. This is set by the **enable password** command at the PIX Firewall console. Once set, the password cannot be viewed and must be obtained from its creator.
 - PIX Firewall Telnet password. The default value is **cisco**, but if this is changed with the PIX Firewall's **passwd** console command, you must get the password from the PIX Firewall's system administrator because you cannot display this value at the PIX Firewall console.
 - Password for a user with Windows NT Administrator privileges.
- Configuration—for each PIX Firewall you manage, you need to configure it as explained in “PIX Firewall Requirements.” After configuring the PIX Firewall, determine its inside IP address with the **show ip address** console command.
- Port number—during installation, you are asked to supply a port number for the PIX Firewall Manager's built-in web server. The default port for this server is 8080. It is very unlikely, but possible, that this port could be in use by another server. If that is the case, pick another port for the web server. To pick a port, view the IANA web site to determine which port is appropriate.
<ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers>
- IP address—you need the IP address of the Windows NT system running PIX Firewall Manager. If the computer has more than one network interface and you do not know which one connects to the same network as the PIX Firewall, contact your network administrator.

To view the IP address:

- Step 1** Select **Start>Settings>Control Panel**.
- Step 2** Double-click the **Network** icon.
- Step 3** Click the **Protocols** tab and select **TCP/IP Protocols>Properties**.
- Step 4** When the Microsoft TCP/IP Properties dialog box opens, click the **IP Address** tab. The IP address appears on the lower part of this tab.
- Step 5** If the **Obtain an IP address from a DHCP server** item is checked, click it to disable it. Then click **Specify an IP address** and enter an IP address, subnet mask, and default gateway IP address for this system.

Installing PIX Firewall Manager

Note Only users with Windows NT Administrator privileges can run the installer or uninstaller program.

During installation, if a previous version of the PIX Firewall Manager is found, the installation program replaces the old version with the new. To install PIX Firewall Manager:

- Step 1** If you used the PIX Firewall Setup Wizard to configure the PIX Firewall with the IP address and network mask of the Windows NT computer running the PIX Firewall Manager, skip to Step 2. If you have not set up the IP address for the Windows NT computer, verify network connectivity before starting by following these steps:
- (a) From each PIX Firewall you intend to manage, ping the Windows NT system. Use the PIX Firewall **ping inside** command. The ping is successful if the “response received” message appears. If the ping is unsuccessful, verify the IP address of the Windows NT system and check the network cabling. For example, if the Windows NT system has an IP address of 192.168.42.42, you would use the following commands from the PIX Firewall to enter privilege mode and run the **ping** command:

```
enable
Password: (press Enter)
ping inside 192.168.42.42
```
 - (b) From the Windows NT system, ping the inside interface of each PIX Firewall. To ping from Windows NT, click the **Start** menu. Then choose the **Run...** item and enter the **ping** command, or select the **Programs>Command Prompt** and enter the command there. The ping is successful if the “Reply from” message appears. If the ping is unsuccessful, verify the IP address of the inside interface of the PIX Firewall and check the network cabling. For example, if a PIX Firewall has an inside IP address of 192.168.42.54, you would enter this command:

```
ping 192.168.42.54
```
 - (c) From the Windows NT system, establish a Telnet session with each target PIX Firewall. The Telnet is successful if the “PIX password” prompt appears. The default password is **cisco**. Enter the password to receive access to the PIX Firewall command prompt. If the Telnet is unsuccessful, go to the PIX Firewall console and use the **show telnet** command to ensure that the configuration has a **telnet** command entry for the IP address of the Windows NT system. Refer to “PIX Firewall Requirements” for information on how to enter the PIX Firewall console commands to get to configuration mode, give Telnet access, and store the configuration in Flash memory. For example, if a PIX Firewall has an IP address of 192.168.42.54, enter these commands to access configuration mode, let administrators start Telnet sessions with the PIX Firewall console, and store the configuration in Flash memory:

```
enable
Password: (press Enter)
configure terminal
: Created for PIX Firewall Manager
telnet 192.168.42.54
write memory
```

- Step 2** Exit all Windows programs.
- Step 3** Log in to the Windows NT system as **Administrator** or as any user who is a member of the **Administrator** group or who has Windows NT Administrator privileges.
- Step 4** From the Windows NT system, insert the first PIX Firewall Manager diskette in the diskette drive. You can install the software:
- From the Add/Remove Programs icon in the Control Panel, accessed by choosing the Settings item from the **Start** menu.
 - From My Computer by double-clicking the diskette icon and then double-clicking the miniature computer Setup icon.
 - By choosing the Run item from the **Start** menu and entering the starting filename as **a:\setup.exe**. (If the diskette is in another drive, use that drive letter instead.)
- Step 5** Once the installation program starts, you are prompted with a series of dialog boxes. You can simply click **Next** and the installation will proceed without interruption. Alternately, you can designate an installation directory other than the default.
- Step 6** During the installation you are prompted for a port number for the PIX Firewall Manager's built-in web server; use the default, 8080, unless that port is in use already. Any port between 1025 and 64000 can be entered as an alternative. To pick another port, view <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers> to find the ports in use. The installation program then copies its files and prompts you to insert the second diskette. Insert the diskette and the remaining files are copied.
- Step 7** At the last dialog box, click **Finish**. The Management Server starts automatically.
- Step 8** To check whether the Management Server is running, select **Start>Settings>Control Panel** and double-click the **Services** icon. Look for the "PIX Firewall Management Server" service name. A server is running if its status appears as Started. If the status field is blank, you may run the server by selecting its name and then clicking **Start**. If you need to stop the Management Server, refer to the instructions for doing so in "Management Client Requirements."
- Step 9** After the software setup completes, change the default passwords of the **pixadmin** and **pixuser** users with the Windows NT User Manager program described in the following section, "Changing Passwords."

Changing Passwords

To change passwords for the **pixadmin** and **pixuser** default usernames:

- Step 1** Select **Start>Programs>Administrative Tools (Common)>User Manager**. If your Windows NT system is a domain controller, select **User Manager for Domains**.
- Step 2** When the User Manager starts, locate the two users, **pixadmin** and **pixuser** in the Username section of the screen.
- Step 3** Select the **pixadmin** username and select **User>Properties**.
- Step 4** In the User Properties dialog box, enter the new password in the Password and Confirm Password fields.

- Step 5** In the User Properties dialog box, check **Password Never Expires** to prevent the password from expiring. If the box is not checked, the password expires after the number of days set in the Account Policy Maximum Password Age configured in the Windows NT system. The default value set during Windows NT system installation is 42 days. Click **OK** to exit.
- Step 6** Select the **pixuser** username and select **User>Properties**. Enter the new password in the Password and Confirm Password fields.
- Step 7** In the User Properties dialog box, check **Password Never Expires** to prevent the password from expiring.
- Step 8** Click **OK** to exit and select **User>Exit** to leave the User Manager.

Limiting Access to the Management Client

You can specify which users can access the Management Client by creating user accounts on the Windows NT system on which PIX Firewall Manager is installed and giving the user either PIX Firewall Manager administrative or read-only access privileges. When the Management Client starts, users enter their login ID and password and, if accepted, they can then run PIX Firewall Manager.

Note Before limiting access to the Management Client, change the default password to a new value as described in the preceding section, “Changing Passwords.”

To limit access to the Management Client:

- Step 1** Start the User Manager as described in Step 1 in the preceding section, “Changing Passwords.” The User Manager dialog box appears. If you want to authorize access for users who already have accounts on the Windows NT system, proceed to Step 2. To add new users to the Windows NT system, select **User>New User**. Specify the information for the user including the user’s login name, full name, and password.
- Step 2** To give a user access to the Management Client, locate the Groups area at the bottom of the User Manager dialog box.
- Step 3** From the Groups area, if you want users to be able to change PIX Firewall settings, double-click **PIX Admins**. If you want users only to have read access and no change privileges, double-click **PIX Users**. The Local Group Properties dialog box then appears.
- Step 4** Click **Add** to add an existing user to the selected group. The Add Users and Groups dialog box appears.
- Step 5** From the Names field, select the name of the user you wish to add, click **Add**, and then click **OK** to complete adding this user. Control returns to the Local Group Properties dialog box where you can continue adding users. To exit back to the User Manager dialog box, click **OK**. Then exit User Manager by clicking **OK**.

Note Do not assign a user to both the **PIX Admins** and **PIX Users** groups.

Starting the Management Client

To start the Management Client, restart the network browser, disable proxies, and then access the Management Client:

Windows 95, Windows NT, Solaris Netscape Navigator Version 3.x

- Step 1** Choose the **Network Preferences** option from the **Options** menu.
- Step 2** Click the **Proxies** tab, check the **No Proxies** option, and click **OK**.
- Step 3** Choose the **Open Location** option from the **File** menu, enter ^L, or click **Open**, and enter the following:

```
http://IP_address:port
```

where *IP_address* is the system running PIX Firewall Manager Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

Windows 95, Windows NT, Solaris Netscape Communicator 4.0, 4.01, 4.02, 4.04, 4.05, Netscape Navigator 4.0, 4.01, 4.02, 4.04, 4.05

- Step 1** Choose the **Preferences...** item from the **Edit** menu. A dialog box appears.
- Step 2** In the hierarchy display at the left, double-click the **Advanced** item. (In Solaris, click the arrow beside **Advanced**.) The hierarchy expands to display additional choices.
- Step 3** Click the **Proxies** item from the expanded hierarchy list.
- Step 4** Check the **Direct connection to the Internet** option, and click **OK**.
- Step 5** Choose the **Open Location** option from the **File** menu, enter ^L, or click **Open**, and enter the following:

```
http://IP_address:port
```

where *IP_address* is the system running PIX Firewall Manager Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

Windows 95 or Windows NT Microsoft Internet Explorer 4.0 Version 4.72.3110.8; Updated Version: SP1

- Step 1** Choose the **Internet Options...** item from the **View** menu.
- Step 2** Click the **Connections** tab.
- Step 3** In the **Proxies Server** group box, disable the **Access the Internet using a proxy server** option.
- Step 4** Return to the main menu and enter the following:

```
http://IP_address:port
```

where *IP_address* is the system running PIX Firewall Manager Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

Using the Management Client

You can view the Management Client applet with any network browser described in “Management Client Requirements.”

- Step 1** After you have disabled browser proxies as described in “Starting the Management Client” and started the Management Client, the home page appears.
- Step 2** You can generate reports using Microsoft Excel 97 by following the instructions on the home page.
- Step 3** Select Run Management Client.
- Step 4** After the Management Client is loaded, you are then prompted for a username and password. For the username, enter **pixadmin** for read-write access, or **pixuser** for read-only access. Enter either the default password, **cisco**, or the new password entered in “Installation Notes.”

You can also use any username that is in either the **PIX Admins** or **PIX Users** group. When you complete entering a username and password, click **OK**. The Management Client then opens after it loads into memory.

Note When the program is loading, do not minimize the web browser.

- Step 5** If you need to restart the applet, you can click the browser's **Reload** button.

Navigating the Management Client

After you enter your login credentials, the Management Client window appears.

- Step 1** To view or modify the PIX Firewall configuration, go to the Main Tree window on the left side of the Management Client window and double-click a PIX Firewall folder. If the Main Tree window is empty, click **Add A PIX Firewall** in the Contents window to add PIX Firewall units to the Main Tree. Click the **Reload Configuration** button in the Contents window to get the most current configuration.

Note Any change to the configuration of a PIX Firewall made in the Management Client is sent immediately to the firewall and automatically saved in the firewall's RAM.

Note If you have made changes to the configuration as described in the *Configuration Guide for the PIX Firewall Version 4.3*, click the **Reload Configuration** button following the upgrade to get the current configuration information. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

The areas of the Management Client window are as follows:

- The tabs:
 - **Administrator** tab lets you view and change information for a firewall unit.
 - **Alarm and Report** tab lets you receive notification when errors occur and display system usage reports.
 - **Common Configuration** tab lets you configure specific authentication and administration information for multiple PIX Firewall units at the same time.
 - **SYSLOG Notification Settings** tab lets you set information used by the **Alarm and Report** tab.
- The **Tasks** button provides a wizard-like function that allows you to generate inbound and outbound connection statements in the PIX Firewall configuration from a series of dialog boxes.
- The **Save to Flash Mem of PIX** button saves all configuration changes to Flash memory in the PIX Firewall. Flash memory retains configuration information when the system power is lost for any reason.
- The Main Tree lists the PIX Firewall folders. The PIX Firewall Manager assigns a folder icon to each PIX Firewall unit available on the network. When you double-click the top-level firewall icon, it displays the possible task areas for which you can view or change information. By double-clicking each subsequent folder, you work down to the individual task options.
- The PIX Firewall IP Addresses area keeps interface information visible at all times while configuring the PIX Firewall unit. Use the scroll bar to view all interfaces.
- The Contents area displays task information based on the PIX Firewall folder selection from the Main Tree. This area has several functions:
 - Displays help information on PIX Firewall folders and on other task selections.
 - Displays the configuration for the current task.
 - Provides button selections for viewing and changing configuration settings. Button selection varies based on the task selection. Buttons include Add, Delete, Help, Refresh, Edit, and Cancel. Use the **Save to Flash Mem of PIX** button to save all changes made in this area.

Step 2 Double-click the configuration option you want from the folder in the Main Tree. The folder then opens into a series of subfolders or files for each configuration feature. The Contents area displays information about each configuration feature. Use the button selections to get help information, view current configuration information, or change configuration settings.

Step 3 To ensure that the firewall can reload the new configuration after reboot, save the configuration in the firewall's Flash memory by clicking the **Save to Flash Mem of PIX** button. To back up the configuration to a diskette, follow these steps:

- (a) Place an IBM-formatted diskette in the PIX Firewall's drive.
- (b) In the PIX Firewall Manager's Main Tree window, click the PIX Firewall folder's **Administration** folder.
- (c) Select **Save/Erase Config**, and click **to Floppy**.

Stopping the Management Client

To stop the Management Client, stop the network browser on which it runs.

Stopping the Management Server

If you need to stop the Management Server:

- Step 1** Select **Start>Settings>Control Panel>Services**.
- Step 2** When the Services dialog box opens, select the PIX Firewall Management Server item from the Service list. You can stop this service by clicking the **Stop** button.

Generating and Printing Syslog Reports

The PIX Firewall generates syslog messages for system events, such as security alerts and resource depletion. Syslog messages are stored in log files and can be used to create alerts and reports.

The PIX Firewall Manager provides two ways to view syslog connection information: using the PIX Firewall Management Client graphical user interface, or using a Microsoft Excel macro and data files provided for Microsoft Excel 97. Options for printing reports are available only using Microsoft Excel 97. This section includes the following topics:

- Configuration Requirements
- Viewing Reports
- Troubleshooting Syslog Reporting Problems

Configuration Requirements

Prior to using the Alarm and Report features, you must configure each PIX Firewall to generate syslog messages and send them to a syslog server host, one of which can be the host running the PIX Firewall Manager. The syslog server in the PIX Firewall Manager listens for messages from the PIX Firewall on UDP port 514. Messages are stored in daily log files on the Windows NT computer running the PIX Firewall Manager. The PFM uses the information in the daily log files to generate reports. To configure each PIX Firewall unit from the Management Client, select **Administrator>SYSLOG** to view options for configuring syslog host and message information.

Viewing Reports

To view syslog reports from the PIX Firewall Management Client, follow the instructions for “Navigating the Management Client.” From the Management Client, click the **Alarm and Report** tab to view options for generating reports.

- To view and print syslog reports from the macro, follow the instructions for “Starting the Management Client” to display the PIX Firewall Manager home page. From the home page, follow the instructions on how to log in and generate reports. The procedure for generating and printing syslog reports uses the Microsoft Excel macro REPORT.XLS. To use this file, start the Microsoft Excel application and open the file from within the application. If you try to open the file directly by double-clicking it, the following error message appears:

Cannot open the corresponding DBF file

Note When downloading the files from the web browser, be sure to save all files (report.xls, dns.dbf, monday.dbf, sunday.dbf, and so on) to the same directory on the local drive. After all the files are in the same directory, use Microsoft Excel 97 to open the report.xls file.

Note The macro does not support viewing or printing detailed reports of FTP and HTTP file transfers as provided in reports generated by the PIX Firewall Management Client.

The PIX Firewall Manager saves syslog information in daily log files. For example, PIX Firewall connection information for Monday is saved in the *monday.log* file. The log files are located in *\PIX Firewall Manager\protect\<weekday>.log* on the Windows NT computer.

Log files are retained for one week, allowing a separate log file for each day of the week. After one week, daily log files are overwritten, starting with the daily file that was created first. For example, if log files were first started on Monday, the Monday log file will be overwritten in seven days. This also means that you can access a six-day archive of log information for a given day.

Note For reporting purposes, hosts on a perimeter network are considered “outside.” When setting up syslog reports from the PIX Firewall Management Client, you must specify “outside” to include the hosts on the perimeter network in the report.

Troubleshooting Syslog Reporting Problems

Problems generating syslog reports can mean that one or both of the configuration settings for the syslog host or Message type is not correct, or that data is not reaching the syslog host. If you have problems displaying syslog report information, or you receive a “Database Empty” error message, check the following items:

- Review the section “Generating and Printing Syslog Reports” for configuration requirements. Configure the SYSLOG Host and Message Types settings.
- Verify that messages are occurring at the PIX Firewall. From the Management Client, click the **Alarm and Report** tab. Under the heading, **Immediate SYSLOG Message**, click **ON** to display a syslog message window that reports messages as they are received at the syslog host. If no messages appear in the SYSLOG Message Window, it might indicate that no syslog messages are being generated by the PIX Firewall. This can be normal if no activity is occurring at the PIX Firewall. To generate a syslog message, use Telnet to log in to a PIX Firewall that has been configured with the IP address of the syslog host running this PIX Firewall Manager. If configured properly, a message should appear in the SYSLOG Message Window indicating that the connection was permitted.

Note Close the SYSLOG Message Window after you have verified that information is being received at the syslog host. These messages can fill up system memory on the host, slowing performance.

- Verify that the Message Type is set to capture level 7 messages. The PIX Firewall Manager requires you set the Message Type to level 7 before generating reports. From the Management Client, click the **Administration** tab and select **Administration>SYSLOG** from the Main Tree. Click **Edit** to display the Edit SYSLOG Output dialog box, and change the Message Types level if necessary.

Note The Facility setting in the Edit SYSLOG Output dialog box is not used by the PIX Firewall Manager Management Client for generating reports. The report wizard provided with the Management Client references hosts by IP address.

If syslog reports display both host names and IP addresses, verify that the Windows NT system running the Management Server is able to resolve host names. The PIX Firewall Manager attempts to resolve IP addresses with host names when the Management Server receives syslog messages. If it finds a host name for an IP address, the address and host name pair is stored in a database on the Management Server. This database is used to create SYSLOG reports. If the Management Server is unable to resolve the IP address with a host name within 15 seconds, only the IP address is logged in the database. As a result, SYSLOG reports might include both host names and IP addresses.

Limitations and Restrictions

- 1 PIX Firewall Manager cannot be installed or uninstalled under Windows NT domain administration logins. If you attempt to install PIX Firewall Manager on this type of login, the following message appears:

```
You are not authorized to run this installer.  
Terminating...
```

- 2 When installing the PIX Firewall Manager on a backup domain controller, be sure that the backup domain controller has connectivity with the primary domain controller. If connectivity is lost between the backup domain controller and the primary domain controller, the following message appears:

```
Could not find the domain controller for the domain.
```

In this case, the installation procedure cannot add the PIX Firewall Manager users and groups to the Windows NT Security Account Manager database, and attempts to use the PIX Firewall Manager will fail.

- 3 PIX Firewall Manager does not support the following PIX Firewall commands. To view, add, or change these configuration features, use the PIX Firewall's console port or start a Telnet session to access the PIX Firewall.
 - **aaa authentication enableserialtelnet console tacacs+radius** —**aaa authentication enable console** requires authentication to access the PIX Firewall console and lets you log changes made to the PIX Firewall configuration from a serial console session.
 - **clear logging disabled**—lets you enable all previously disabled system messages.
 - **clock set** —lets you set the clock in the PIX Firewall that is used in conjunction with adding a timestamp to syslog messages that will be received by the syslog server.
 - **config net**—read the configuration from the TFTP server.
 - **hostname**—change the PIX Firewall host name.
 - **name** or **names**—permit users to map hostnames to IP addresses, thus allowing users to specify host names in the places where IP addresses are permitted.
 - **ping**—determine if other IP addresses are visible from the PIX Firewall.
 - **sysopt**—tune advanced PIX Firewall TCP cut through proxy features and enable or disable the PIX Firewall IP Frag Guard feature.

Note The **established** command in the command line interface is same as the multimedia feature in the Management Client. To use this feature, select **Administrator>Administration>Multimedia**.

- 4 The following configuration features can be viewed on the Management Client but must be added or changed at the PIX Firewall's console port or Telnet session:
 - MTU size. You only need to change this if you have a Token-Ring interface. Use the **mtu** command.
 - Interface configuration. Use the **interface**, **nameif**, and **ip address** commands to change the values if needed.
 - Failover. Use the **failover** command if needed.
 - Private Link. Use the **link** and **linkpath** commands.
- 5 ICMP protocol services, such as ping, are initially blocked in both directions by the PIX Firewall and require a **conduit** configuration. To configure a **conduit**, select **Inbound>Static>Conduit**.

If a help topic is not available, information on the topic can be found in the *Configuration Guide for the PIX Firewall Version 4.3*. Also view the *Release Notes for the PIX Firewall Version 4.3*. If you are using PIX Firewall version 4.4(1), refer to the *Configuration Guide for the PIX Firewall Version 4.4* for this information.

Important Notes

- 1 When a Management Client is running, only the following configuration changes to the PIX Firewall units made through the console or Telnet sessions are reflected in the client applet: **conduit**, **static**, **global**, **nat**, **outbound**, **apply**, and **alias**. To view the updated configuration for any other PIX commands modified via the console or Telnet sessions, click a PIX Firewall folder, then click the **Reload Configuration** button.
- 2 If a client is already connected to a Management Server and a second client on the same machine tries to connect to the same Management Server, then the first client will be disconnected and the second client will be connected.
- 3 All members in the PIX Admins group have read and write access, and all members in the PIX Users group have only read access; do not change the PIX Firewall configurations. Usernames that do not belong to one of these two groups cannot use the Management Client applet.
- 4 When accessing the Management Server from the Management Client, do not use the loopback address (127.0.0.1) in the URL. Using the loopback address causes an "I/O Exception" error on all online help and description pages. Refer to "Starting the Management Client" for more information on using the Management Client.
- 5 If you change the PIX Firewall enable password in **Administrator>Administration>Password**, wait for confirmation of password change prior to entering additional commands. If you enter an invalid password, confirmation of the change can take several minutes while the server tries to validate the entry. In the case of an invalid password, additional commands can appear to hang until the server returns confirmation that the change was unsuccessful.
- 6 Initially, no syslog setting information displays in the **Administration>SYSLOG** panel. Press the Refresh button to display the current information. Syslog information in the daily syslog file is now saved every 10 minutes by default. You can change the time interval for saving syslog information by setting the value in the **SYSLOG Notification Settings** tab.
- 7 You can specify that syslog messages be marked with the current time. To configure each PIX Firewall unit with the timestamp option, select **Administrator>SYSLOG**, set the logging type to **Timestamp** and set the status to **Enable**.

Note You must set the date and time from the PIX Firewall command line interface using the **clock set** command before timestamp information will appear in syslog messages. You cannot set the date and time from the PFM Management Client.

If you have problems installing or using the PIX Firewall Manager, check the following items:

- Installing the PIX Firewall Manager generates the following error message:

```
A version of the PIX Firewall SYSLOG SERVER is detected on this machine. You must
uninstall PIX Firewall SYSLOG SERVER before installing the PIX Firewall Manager.
```

If the PIX Firewall Manager installation detects the presence of the PIX Firewall Syslog Server application on the same system, it displays a message warning you that both applications exist. The PIX Firewall does not support running both the PFM and PFSS applications at the same time. You must use either PFM or PFSS, but not both.

- The PIX Firewall Manager reports that it cannot connect with the PIX Firewall unit.

Verify that the PIX Firewall has been configured for Telnet access from the Windows NT computer where the PIX Firewall Manager Server is installed.

- The PIX Firewall Manager denies user login access.

Verify that the user is a member of the PIX Admins or PIX Users groups on the Windows NT computer. If the user is not a member of a group, add the user.

- The PIX Firewall Manager installs but does not run.

This can indicate that the client portion of the application is not communicating with the server portion. To determine where errors might be occurring, use the following procedure to launch the PIX Firewall Manager to the desktop:

Step 1 Select **Start>Settings>Control Panel>Services** on the Windows NT computer.

Step 2 Scroll through the services to locate the PIX Firewall Manager Server.

Step 3 Double-click **PIX Firewall Manager Server**, which displays the Service dialog box.

Step 4 In the Service dialog box, check **Allow Service to Interact with Desktop** and click **OK**.

Step 5 In the Services dialog box, click **Stop** to halt the PIX Firewall Manager Server; then click **Start** to restart the service.

Step 6 Start the PIX Firewall Manager. Errors generated by the application appear in the PIX Management dialog box.

Copy the errors messages in the dialog boxes and use Cisco Connection Online (CCO) for additional support.

- The Management Client stops running and reports Java applet errors in the status bar.

If the Management Client appears to stop working and reports Java applet errors, use the following procedure to launch the Java console from the web browser.

— From Netscape Navigator, select **Communicator>Java Console** from the browser menu.

— From Internet Explorer, select **View>Internet Options>Advanced** and select **Java Console** from the menu options.

The error messages appear in the Java console panel. If the error messages report security violations, it can mean that the Management Client is having trouble communicating with the Management Server.

In such cases, try the following:

- Close the Management Client and enter the client location in the browser again using the HTTP protocol as shown here:

```
http://192.168.0.4:8080
```

Do not use **File>Open** from the browser menu to access the Management Client.

- Verify that you have not changed the IP address of the Windows NT workstation running the Management Client. Changing this address can generate security violation messages. If you change the IP address of the Windows NT workstation, you must edit the IP address of the Management Client in the following file on your local disk:

```
\Program Files\Cisco\PIX Firewall\jclient\netscape\firewall
```

If the problems persist, use Cisco Connection Online (CCO) for additional support.

Related Documentation

Use this document in conjunction with the following PIX Firewall documents.

Version 4.3

- *Configuration Guide for the PIX Firewall Version 4.3*
- *Release Notes for the PIX Firewall Version 4.3*
- *Quick Installation Guide for the PIX Firewall Version 4.3*
- *System Log Message for the PIX Firewall Version 4.3*
- *Regulatory Compliance and Safety Information for the PIX Firewall Version 4.3*

You can view these documents online at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v43/index.htm

Version 4.4

- *Configuration Guide for the PIX Firewall Version 4.4*
- *Release Notes for the PIX Firewall Version 4.4(1)*
- *Installation Guide for the PIX Firewall*
- *System Log Messages for the PIX Firewall Version 4.4*
- *Regulatory Compliance and Safety Information for the PIX Firewall Version 4.4*

You can view these documents online at:

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

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

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

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9905R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.