



Doc. No. 78-4692-06

PIX Firewall Manager Version 4.1(7) Release Notes

October 1998

This document describes how to install and configure Cisco's PIX Firewall Manager.

The following topics are covered in these release notes:

- Important Notes on page 1
- Introduction on page 2
- PIX Firewall Manager Installation on page 7
- Starting the Management Client on page 13
- Using the Management Client on page 14
- Troubleshooting the PIX Firewall Manager on page 17
- Cisco Connection Online on page 18
- CD-ROM Documentation on page 19

Important Notes

- 1 Each PIX Firewall you wish to manage must be running PIX Firewall version 4.1(7) 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. Refer to "PIX Firewall Requirements" for other requirements.
- 3 The Windows NT Workstation or Server on which you install PIX Firewall Manager must be running version 4.0 or later. Refer to "Management Server Requirements" for other requirements.
- 4 The computer running the PIX Firewall Manager Management Client (graphical user interface) must have a network browser that is Java 1.02 or 1.1 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.

Corporate Headquarters

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

Copyright © 1998
Cisco Systems, Inc.
All rights reserved.

- 7 The PIX Firewall Manager (PFM) is not compatible with Cisco Resource Manager (CRM) because CRM and PFM both use the SYSLOG UDP port. Do not run both applications on the same system.

Introduction

Cisco's PIX Firewall Manager lets you administer one or more PIX Firewall units, view SYSLOG messages, define customized alarms for each type of SYSLOG message, and view reports. You can use the PIX Firewall Manager to view, add, and modify the configuration of each PIX Firewall unit.

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 Firewalls' responses back to the Management Client. The Management Server also includes a built-in SYSLOG server. The Management Server starts automatically when the installation completes or when a user logs in. 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 or 1.1 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 document *Installing PIX Firewall and PIX10000*, which is included with your PIX Firewall accessory kit. This document has instructions for downloading software from Cisco Systems, Inc.

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

Features

The following features are included in PIX Firewall software version 4.1(7):

- The **Authentication>Authentication** and the **Authentication>Authorization** screens allow configuration on any PIX Firewall interface.
- The **Inbound>Static>Conduit** screen includes **permit** or **deny** configuration options.

Note In PIX Firewall software version 4.1(7), ICMP protocol services, such as ping, are no longer automatically handled by the PIX Firewall and require a conduit configuration. Refer to the *PIX Firewall Series Version 4.1(7) Release Notes* for more information.

- The **Authentication>Virtual Servers** screen includes configurations for both the Virtual HTTP Server and Virtual Telnet Server. The Virtual HTTP Server prevents user credentials (username and password) from being exposed on outside networks. The **virtual http** command works with the **aaa** command to authenticate the user, separate the AAA server information from the web client's URL request, and direct the web client to the web server.

The Virtual Telnet Server provides a way to pre-authenticate users who require connections through the PIX Firewall using services or protocols that do not support authentication.

- The **Information>Private Link** screen displays information for any PIX Firewall interface.
- Manage up to 10 PIX Firewall units from the PIX Firewall Manager.
- The **Reload Configuration** button on the Administrator main window now retrieves the most current PIX Firewall configuration.
- Reports are generated by the report wizard from the **Alarm and Report** tab by clicking a PIX Firewall folder and clicking the **Report** button.
- The report wizard generates a three-dimensional bar chart report on PIX Firewall network traffic data. Information on up to 50 hosts is now 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.
- The report wizard reports FTP and HTTP file transfer activity by host, including source IP address and filename. These reports are not available using Microsoft Excel 97.
- If you have both Open Systems Solutions Private I and PIX Firewall Manager installed on the same system, you can enable the Redirect SYSLOG Messages option on the **Setting** tab to avoid conflicts between these products. Enabling Redirect SYSLOG messages copies SYSLOG event information received from port 514 to port 515.
- The **Information>Xlate** screen now supports host names. Both connection slot and translation slot information are available on this screen.
- The ARP table updates each time you choose the ARP table entry from the Main Tree.
- The **Setting** tab provides an option for setting the time interval for updating SYSLOG message files.

Usage Notes

- PIX Firewall Manager Version 4.1(7) encrypts all communication with the PIX Firewall software version 4.1(7). Managing PIX Firewall units running earlier software versions is not supported.
- 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...
```

- 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.

- 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.
 - **tftp-server**—specify a TFTP server for reading or saving the configuration.

- **config net**—read the configuration from the TFTP server.
- **write net**—save the configuration to the TFTP server.
- **hostname**—change the PIX Firewall host name. You can view the host name with the Failover item in the Information folder on the **Administrator** tab.
- **name** or **names**—permits users to map host names to IP addresses, thus allowing users to specify host names in the places where IP addresses are permitted.
- 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.
- If a help topic is not available, information on the topic can be found in the *PIX Firewall Series Configuration Guide*. Also view the *PIX Firewall Series Version 4.1(7) Release Notes*.
- 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**, **mailhost**, **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.
- 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.
- Do not run the PIX Firewall Manager and the Cisco Resource Manager on the same Windows NT computer because both try to listen at UDP port 514 for incoming SYSLOG messages. If both are run on the same computer, the PIX Firewall Manager cannot receive SYSLOG messages from the PIX Firewall.
- If Private I is not running on the same Windows NT system where PIX Firewall Manager was installed, but Redirect SYSLOG Messages is set to **Enable**, and at least one PIX Firewall is configured to send SYSLOG messages to this system, then the CPU usage of the Windows NT system can jump significantly and the system can become unresponsive. You must set the Redirect Syslog Messages option to **Disable** if Private I is not running on that system.

To check or modify the Redirect SYSLOG Messages option on the PFM client, select the **Setting** tab. The option is displayed in the bottom half of the page.
- 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, replace the old IP address with the current IP address, which is only visible from the inside network.
- 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.

- All members in the PIX Admins group have read and write access, and all members in the PIX Users group can only read, but not change the PIX Firewall configurations. User names that do not belong to one of these two groups cannot use the Management Client applet.
- PIX Firewall Manager does not initially send the SMTP HELO command on email notifications, as per RFC 821, for PIX Firewall SYSLOG events. This affects mail servers that expect HELO packets. If you set up the PIX Firewall Manager to use email notifications for SYSLOG events, specify a UNIX mail server.

Bug Fixes

The following PIX Firewall Manager bugs have been fixed. Bug fixes for version 4.1.4, 4.1.5, and 4.1(6) are included for reference.

Bug Number	Description of Fix	Fixed in Release
CSCdk39378	A vulnerability in the PIX Firewall Manager HTTP server allowed any attacker who could connect to the server to retrieve any file known in advance to exist on the Windows NT host. In almost all cases, this meant that the host was vulnerable to attack by any user inside the PIX Firewall, but not by users outside the PIX Firewall. This has been fixed.	4.1(7)
CSCdk34305	The Management Client no longer receives an error message when the Management Client attempts to download a configuration which has a large number of entries for a single command, and the time it takes for the Management Server to receive these entries from the PIX exceeds one minute.	4.1(7)
CSCdk23576	The Management Client no longer receives an error message when downloading a large configuration.	4.1(7)
CSCdk23534	If the Windows NT service called "Server" was not running on the Windows NT computer where the PIX Firewall Manager was being installed, the installer would erroneously report the following error and the installation was terminated: <code>You are not authorized to run this installer.</code>	4.1(7)
CSCdk22492	The PIX Firewall Manager now prompts users for the PIX Firewall enable password instead of the Telnet password when adding a firewall to the list of PIX Firewalls managed by the PIX Firewall Manager. As always, only the members of the Windows NT user group "PIX Admins" are permitted to add a PIX Firewall to the list of configuration entries.	4.1(7)
CSCdk22399	PIX Firewall Manager did not initially send HELO on email notifications as per RFC 821. This affected email applications that expected HELO packets.	4.1(7)
CSCdk20416, CSCdk29990	In the SYSLOG Notification Settings tab, the PIX Firewall Manager now saves the Redirect SYSLOG Messages setting after the PIX Firewall Management Server is restarted or the Windows NT computer is rebooted.	4.1(7)
CSCdk11430	The PIX Firewall Manager software is fixed to stop occurrences of the following error message: <code>Start Service FAILED! during install of PFM.</code>	4.1(7)
CSCdk06804	The PIX Firewall Manager SYSLOG message process (syslogd) could hang after logging 200 messages.	4.1(7)

Bug Number	Description of Fix	Fixed in Release
CSCdk06121	The PIX Firewall Manager software is fixed to display more than 200 lines when configured for Immediate SYSLOG in the Alarm and Report tab.	4.1(7)
CSCdk03171	The PIX Firewall Manager installer for 4.1.5 did not properly handle the installation and deinstallation on international versions of Windows NT that did not have a group named "Administrators." On installation, users that did not have administrative rights were allowed to run the installer. On deinstallation, the user would get the error message "You are not authorized to run this installer."	4.1(6)
CSCdk02501	The PFM server no longer generates a Dr. Watson error at reboot.	4.1(6)
CSCdj86302	Special characters, such as "#," in the PIX Firewall configuration file no longer cause the PIX Firewall Manager to stop downloading the configuration file.	4.1.5
CSCdj79959	The PIX Firewall Manager properly removes all previous versions of PIX Firewall server files during installation, eliminating messages that the files are in use.	4.1.5
CSCdj79957	The PIX Firewall Manager now properly installs on a Windows NT Server designated as a backup domain controller.	4.1.5
CSCdj76724	The PIX Firewall Manager now automatically deletes conduit entries when deleting static or mailhost entries. There is a one-to-many correspondence between a static entry and a conduit. Deleting a static without removing the associated conduits makes some entries in the conduit table invalid. The mailhost entry is a static setting.	4.1.5
CSCdj76715	The PIX Firewall Manager Management Client now displays the conduit entry for the mailhost. A mailhost entry in the PIX Firewall automatically generates a conduit entry for port 25 (mail server port). This conduit entry was not showing up in the PIX Firewall Manager Management Client (GUI display).	4.1.5
CSCdj76711	The PIX Firewall Manager checks static address entries for valid global address entries. The PIX Firewall disallows a static entry where the global IP address is a host address and the local IP address is a network address, or vice versa.	4.1.5
CSCdj76708	Configuration download from the PIX Firewall to the PIX Firewall Manager now uses caching to improve performance.	4.1.5
CSCdj76705	The PIX Firewall Manager periodically checks and updates DNS entries, maintaining host name information for use with the report building feature.	4.1.5
CSCdj76702	The Setting tab in the PIX Firewall Manager Management Client includes an option for setting the time interval for updating SYSLOG message files.	4.1.5
CSCdj46774	The Management Client now shows host names and service names on the Information>Xlate screen.	4.1.4
CSCdj46771	The Management Client now lists the connection slots in a separate table from translation slots on the Information>Xlate screen.	4.1.4
CSCdj46768	The Reload Configuration button was added to the Contents window to let you view the most current configuration for a PIX Firewall.	4.1.4
CSCdj46759	PIX Firewall Manager now works with Netscape Navigator version 4.0.	4.1.4

Bug Number	Description of Fix	Fixed in Release
CSCdj46758	The Management Client now shows well-known ports as names on the Information>Xlate screen.	4.1.4
CSCdj46748	PIX Firewall Manager now clears buffers correctly after an error is processed.	4.1.4
CSCdj36126	A check was added so that authentication cannot be added unless an authentication server was previously identified.	4.1.4
CSCdj36120	PIX Firewall Manager now deletes corresponding conduits when a static is deleted.	4.1.4
CSCdj32083	The PIX Firewall Manager now detects when IP addresses are entered incorrectly.	4.1.4
CSCdj31847	PIX Firewall Manager provides new information on the Information>System screen.	4.1.4
CSCdj31844	The Management Client now works correctly when the Management Server goes offline.	4.1.4
CSCdj31807	The PIX Firewall Manager Excel reporting macro, report.xls, no longer displays an error message when started.	4.1.4
CSCdj2395	Global and Outbound list IDs can now only be entered as positive numbers.	4.1.4
CSCdj12370	A button problem on the Routing>RIP screen was fixed.	4.1.4

PIX Firewall Manager Installation

The sections that follow describe how to install PIX Firewall Manager.

The following topics are described in this section:

- Information Requirements
- Software Requirements
- Installing PIX Firewall Manager
- Changing Passwords
- Limiting Access to the Management Client

Information Requirements

Before installing PIX Firewall Manager, you need the following:

- Passwords—you need these 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. You need this password to add a firewall to the list of firewalls managed by the PIX Firewall Manager.
 - 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.
- 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.
- 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 <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers> to find the ports in use.

Software Requirements

The following sections list software requirements for using PIX Firewall Manager.

PIX Firewall Requirements

Note Each PIX Firewall you manage must have been configured with the PIX Firewall **telnet** command to permit the Management Server to access the PIX Firewall.

All PIX Firewall units managed by PIX Firewall Manager version 4.1(7) must be running PIX Firewall version 4.1(7) or later. To check the version of the PIX Firewall software, go to the PIX 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 PIX Firewall you manage. 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, 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 *PIX Firewall Series Configuration Guide* for information on configuring Private Link, and Chapter 3, “Command Reference,” to view the **link** command page for more information.

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

All commands are described in the *PIX Firewall Series Configuration Guide* supplied in your PIX Firewall accessory kit.

Windows NT System 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. The system running Windows NT must contain a Pentium processor and have 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. Refer to “Limiting Access to the Management Client” for more information on how to add users to these groups.

Management Server Requirements

The Management Server has the following requirements:

- All machines running the Management Server must be on the PIX Firewall’s “inside” (most secure) network.
- PIX Firewall Manager comes with a sound file, T1.AU, for the SYSLOG audio alarm. All sound files must be in .AU format. 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.

Management Client 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 Communicator version 4.04 or 4.05 with the JDK 1.1 Patch is not compatible with the Management Client.

- 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.

Installing PIX Firewall Manager

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

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 Verify network connectivity before starting. This consists of successfully performing the following:

- (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 and after messages appear, you then 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 to 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 3.5-inch diskette is in another drive, use that drive’s 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 Server 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 user names:

- 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, 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 to only 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, start 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`

IP_address is the system running PIX Firewall Manager Server. *port* is the Management Server's web server port that you defined in Step 6 of "Installing PIX Firewall Manager."

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

IP_address is the system running PIX Firewall Manager Server. *port* is the Management Server's web server port that you defined in Step 6 of "Installing PIX Firewall Manager."

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
```

IP_address is the system running PIX Firewall Manager Server. *port* is the Management Server's web server port that you defined in Step 6 of "Installing PIX Firewall Manager."

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 in the Information section, or start the Management Client at the bottom of the page depending on the type of browser you are using.

Step 3 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 Step 9 in "Installing PIX Firewall Manager."

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 4 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. A dialog box appears prompting you to enter the IP address of the PIX Firewall and the privileged mode (enable) password for that firewall.

To get the most current configuration for a firewall, select a PIX Firewall from the Main Tree and click **Reload 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 upgraded PIX Firewall software as described in *Installing PIX Firewall and PIX10000*, click the **Reload Configuration** button following the upgrade to get the current configuration 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.
 - **Setting** tab lets you set information used by the **Alarm and Report** tab.
- 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 that have the file icon.
- 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 SYSLOG features, you must configure the PIX Firewall to generate messages and to send them to a host location. To configure each PIX Firewall unit, follow the instructions for “Navigating the Management Client.” From the Management Client, select **Administration>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.

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 consider “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 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.

Troubleshooting the PIX Firewall Manager

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

- 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 verify 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.

- 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 and verify the problem.

- 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.

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.html`

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

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](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.

CD-ROM Documentation

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 *PIX Firewall Series Configuration Guide* publication.

AccessPath, Any to Any, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratum, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn and Empowering the Internet Generation are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe 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. (9808R)

PIX Firewall Manager Version 4.1(7) Release Notes

Copyright © 1998, Cisco Systems, Inc.
All rights reserved. Printed in USA.