PIX Device Manager

Terms you'll need to understand:

- ✓ PDM
- ✓ Unsupported commands
- ✓ Access Rules tab
- ✓ Translation Rules tab
- ✓ VPN tab
- ✓ Host/Network tab
- ✓ System Properties tab
- ✓ Monitoring tab

Techniques you'll need to master:

- ✓ Knowing which operating systems are supported
- ✓ Locating mroute
- ✓ Locating VPN settings
- ✓ Using the Startup Wizard
- ✓ Locating Java and ActiveX filters

Up to this point, you have been using the command-line interface to make changes and view information about the PIX firewall. The PIX Device Manager (PDM) is Cisco's Web-based interface, and it enables a graphical user interface (GUI) to configure the PIX via HTTPS. The interface enables you to view, configure, and monitor PIX functions and settings. This chapter covers system requirements and installation and an overview of the PDM interface.

PIX PDM Requirements

The PDM is just one of several GUI interface tools used to configure and monitor the PIX firewall. PDM is a Java Web-based interface that enables configuration of your firewall via a secure HTTPS connection. The tool is designed for a single firewall system. However, Cisco does have another GUI interface tool called the Cisco Secure Policy Manager (CSPM) that supports centralized management of several security systems simultaneously—PIX is one such security system.

PIX Device Requirements, Client Needs, and Limitations

The PIX PDM version 2.1 supports all models—501, 506/506E, 515/515E, 520, 525, and 535 models that run the PIX firewall software 6.2 or higher. The following is a list of all the requirements for these models:

- PIX software 6.2 or higher
- Minimum of 8MB of flash memory
- DES or 3DES activation keys

The encryption of DES or 3DES is required because of the HTTPS, Secure Socket Layer (SSL) connection needed to use the PDM interface. This SSL connection allows secure traffic to pass between the interface and Web browsers and typically used port 443.

The PDM software also supports the Cisco Firewall Service Module (FWSM) version 1.1 that can be installed in a Catalyst 6500 series switch.

Clients Using the PDM

The Java-based interface doesn't require a client installation; only an HTTPS connection to the firewall, which will download and execute the Java applets required to run the interface, is needed. Table 13.1 lists the client platforms that can run the interface.

Table 13.1 Supported Clients

Client	Description
Solaris	Version 2.6 or higher with a windows manager
Linux	Red Hat 7.0 or higher with KDE or GNOME as an X Window System manager
Windows	Windows 98, NT 4.0, 2000, XP, or Me

To execute the PDM Java, the Web browser must support JavaScript and the Java Development Kit (JDK) version 1.1.4 or higher.

The PDM is supported on Windows, Linux, and Sun Solaris operating systems.

PDM Limitations

The PDM can configure almost all commands necessary to make the PIX firewall work. However, several commands and features are not supported; the PDM might, in fact, prevent you from setting up certain configurations on the firewall with the GUI. When this happens, the only option you can use is the Monitoring tab, which we will look at later. Following is a list of commands not supported on the PDM:

- The `alias` command
- The `aaa` command with the `match` option when other commands use the `include` and `exclude` options
- The `same access-lists and outbound` command linked to more than one interface
- The `established` command

See Cisco's Web site for other unsupported commands. Figure 13.1 displays the error message displayed when an unsupported command, such as the `alias` command, is found.

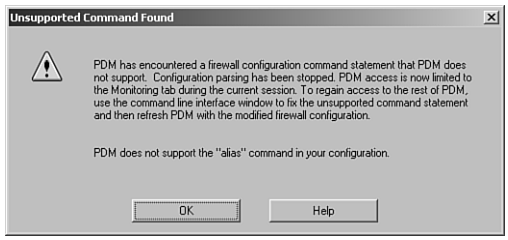

Figure 13.1 The unsupported commands alert box.

Unsupported commands on the PDM disable all configuration functionality on the interface. If unsupported commands are detected, the PDM locks out access to all tabs except the Monitoring tab.

Installing the PDM

The PDM is actually software stored on the PIX firewall itself and downloaded to create the GUI after an HTTPS connection is made by a client. In addition, the PDM image can be acquired from Cisco. Before installing the PDM software, be sure the firewall meets the minimum requirements listed previously. The following are the basic steps needed to configure a new PIX firewall that has no current PDM or configuration:

1. Activate DES or 3DES.
2. Configure a basic IP address on the PIX.
3. Place the PDM software (image) on a TFTP server.
4. Upload the PDM image.

Activating DES or 3DES

Encryption licensing can be obtained from Cisco. The DES activation key is free, whereas the 3DES key comes at a small cost. The `show version` command can display your current activation keys.

Configuring a Basic IP Address

To upload the PDM image, a basic IP address needs to be set on an interface. The command shown here demonstrates this:

```
pixfirewall(config)# ip address inside 192.168.1.1 255.255.255.255
```

PDM Software on a TFTP Server

After the PDM image/software is obtained from Cisco, save it on a basic TFTP server. A free TFTP server can be obtained from Cisco and be easily installed. After it's installed, make sure your TFTP server and the firewall can connect to each other.

Uploading the PDM Image

By now, everything should be ready to upload the image. The example shown here states that the TFTP server address is 192.168.1.2 and the image name is `pdm-211.bin`:

```
pixfirewall(config)# copy tftp flash:pdm
Address or name of remote host [127.0.0.1]? 192.168.1.2
Source file name [cdisk]? pdm-211.bin
copying tftp://192.168.1.2/pdm-211.bin to flash:pdm
[yes¦no¦again]? yes
Erasing current PDM file
Writing new PDM file
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
PDM file installed.
```

The **copy tftp flash:pdm** command needs to have the **pdm** option; otherwise, you can overwrite the PIX operating system.

Configuring an HTTP Server

Now that the PDM is installed, let's see it in action. The PIX first must have the `http server enable` command set. This command enables the PIX to be a Web server and host PDM Web pages. The next step is to define which managed clients will be allowed HTTPS access to the PIX. This is very similar to the command for enabling Telnet users' access. The following commands

are necessary to enable the Web server function and allow a single host access:

```
pixfirewall(config)# http server enable
pixfirewall(config)# http 192.168.1.2 255.255.255.255 inside
pixfirewall(config)# show http
http server enabled
192.168.1.2 255.255.255.255 inside
```

You can also allow an entire subnet access by using the following commands:

```
pixfirewall(config)# http 192.168.1.0 255.255.255.0 inside
pixfirewall(config)# show http
http server enabled
192.168.1.0 255.255.255.0 inside
192.168.1.2 255.255.255.255 inside
```

Connecting to the PDM

After the HTTP server functionality and managed clients have been configured, HTTPS clients can connect. To do so, open a Web browser on a supported operating system and browser, such as Microsoft Internet Explorer, and enter the PIX IP address on the HTTP server-enabled interface. Follow these steps to establish your first connection to the PDM:

1. Enter the PIX IP address in a Web browser.
2. Accept the certificate security alert.
3. Enter the password.
4. Accept the security warning.
5. Enter the PDM interface.

The following is the syntax for your 192.168.1.1 PIX inside interface:

```
https://192.168.1.1
```

When the browser connects to the PIX, HTTPS provides an SSL connection between the client and the PIX. The certificate dialog box is then displayed, warning you that this is an untrusted certificate. Figure 13.2 displays the first dialog box you will see.

Click Yes to proceed. Next, you are presented with the authentication dialog box. If you have configured AAA services, a username is required; otherwise, leave the Username field blank and enter the current enable password. Figure 13.3 shows the login dialog box.

Figure 13.2 The security alert box.

Figure 13.3 The Login dialog box.

After the authentication succeeds, a security warning dialog box might be displayed requesting consent to install a publisher's certificate. Click Yes. Figure 13.4 shows this dialog box.

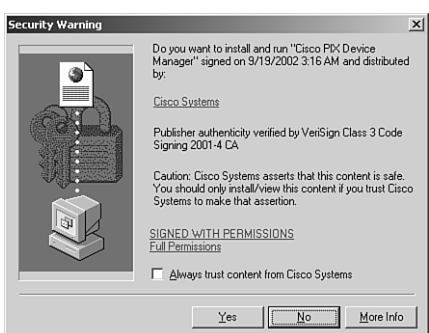

Figure 13.4 The security warning dialog box.

After it's installed, the PDM interface takes a few seconds to load. Figure 13.5 displays the window that appears during the loading stage.

Figure 13.5 Loading the PDM.

After the PDM has loaded, you will see one of three possible screens.

The Startup Wizard is displayed if you don't have a configuration. The Startup Wizard automatically launches and walks you through several easy steps to configure the basic PIX system. Figure 13.6 displays this screen.

Figure 13.6 The Startup Wizard.

The Access Rules tab is displayed if you already have a configuration and all the commands in the configuration are supported. Figure 13.7 displays this screen.

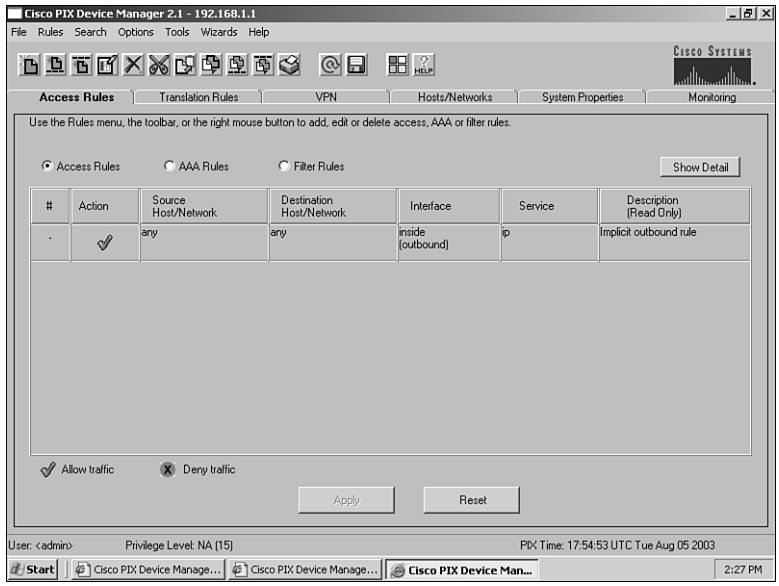

Figure 13.7 The Access Rules tab.

The Unsupported Commands dialog box is displayed if any unsupported commands are configured on the firewall. Figure 13.1, shown earlier in this chapter, displays this warning. After you click Yes, you are only able to monitor items on the firewall in the Monitoring tab. Figure 13.8 displays the only tab you will be able to access.

When your PIX has not been configured, the PDM Startup Wizard automatically is displayed.

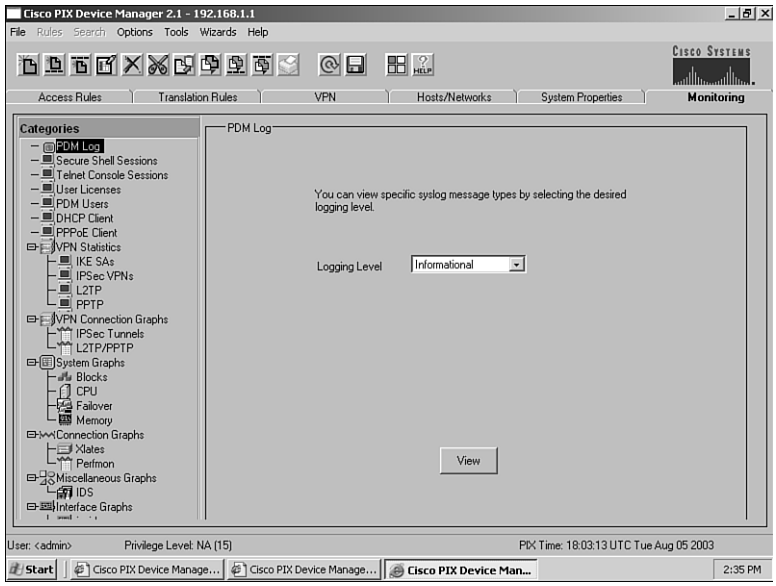

Figure 13.8 The Monitoring tab.

Using the PDM to Configure the PIX Firewall

The PDM can be used to edit almost all the commands supported on the PIX firewall. Most of the PDM functionality is broken up into six main tabs and wizards. This section provides an overview of the following wizards and main tabs:

- Access Rules
- Transition Rules
- VPN
- Host/Networks
- System Properties
- Monitoring

Make sure you know that the five main configuration areas are Access Rules, Translation Rules, VPN, Host/Networks, and System Properties.

The Access Rules Tab

The Access Rules tab enables configuration of which traffic is permitted or denied access through the firewall. Access lists, AAA rules, and URL filter rules can be configured on this tab (refer to Figure 13.7).

The Translation Rules Tab

The Translation Rules tab enables you to configure NAT pools and PAT configuration. On this screen you can manage pools of addresses by clicking the Manage Pools button. Figure 13.9 displays this screen.

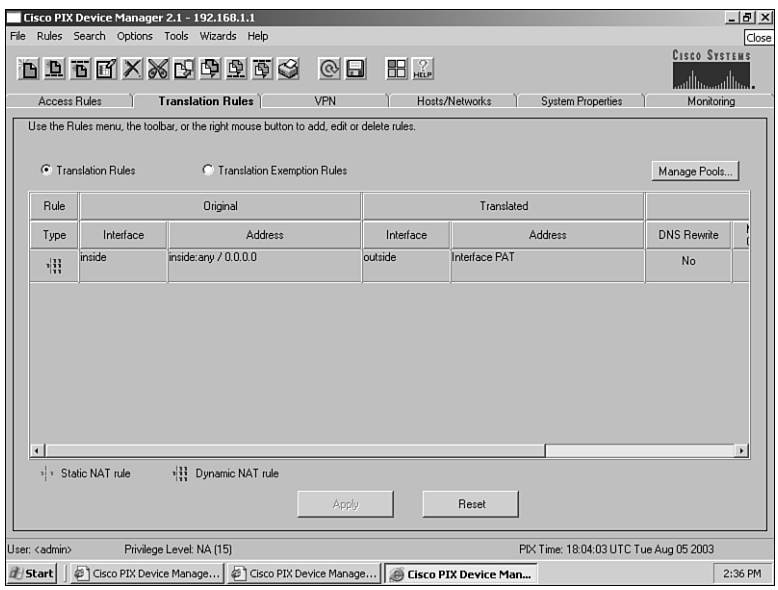

Figure 13.9 The Translation Rules tab.

The VPN Tab

The VPN tab is a very powerful screen that enables you to create VPN connections. This screen enables you to set the transform sets, IKE parameters, site-to-site settings, and even remote-access VPN settings, to name a few. Figure 13.10 displays this screen.

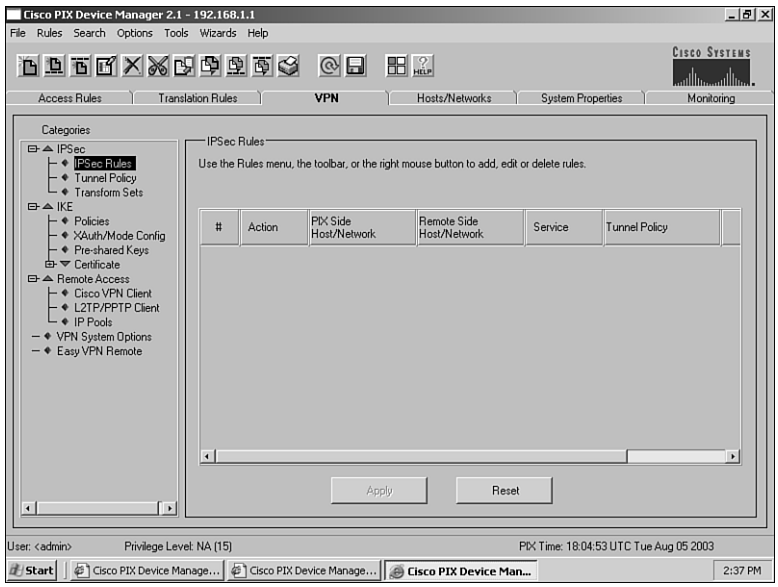

Figure 13.10 The VPN tab.

The Host/Network Tab

The Host/Network tab enables you to configure access list object groups for networks and hosts. The Host/Network section of the screen creates hosts and networks that can be used on the groups' commands on the right side of the screen. For example, you can create WWW, mail, and FTP server entries and then group them together in an object group using the Host and Network group section of the screen. Figure 13.11 displays this screen.

The System Properties Tab

The System Properties tab enables you to configure just about everything else, including interfaces, failover, routing, DHCP servers, logging, AAA services, intrusion detection, and multicast (see Figure 13.12).

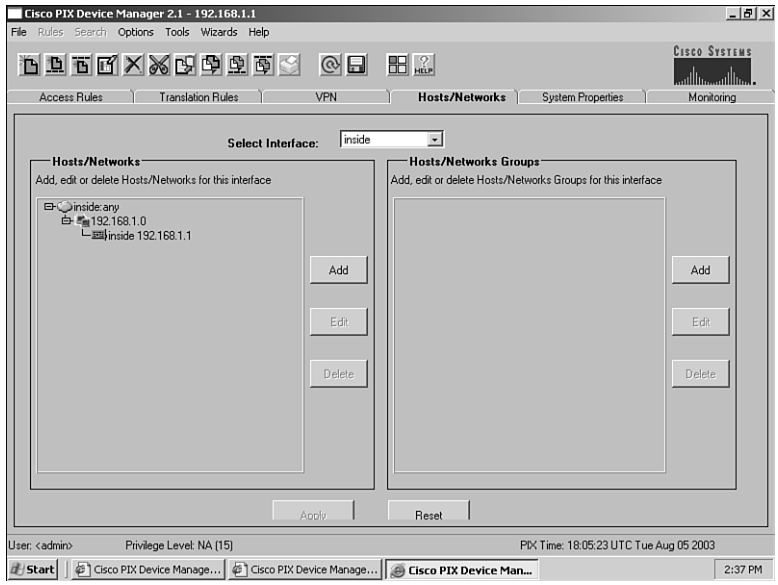

Figure 13.11 The Host/Network tab.

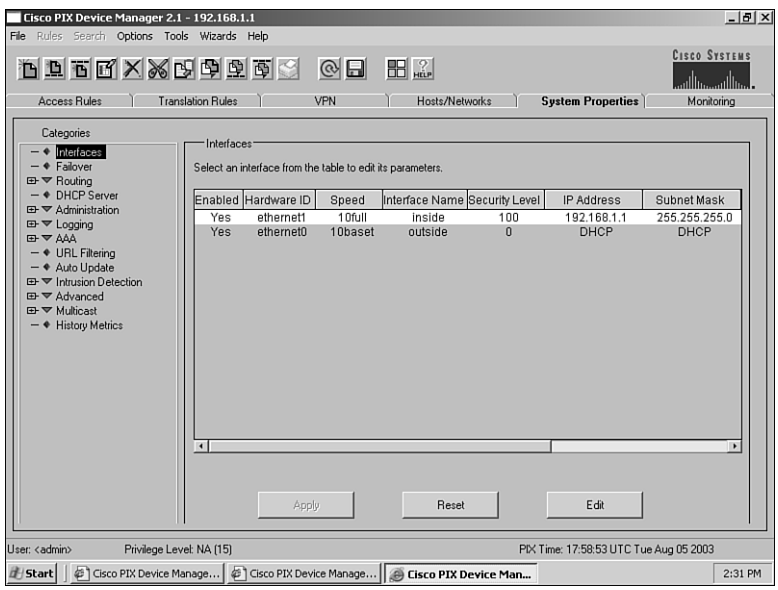

Figure 13.12 The System Properties tab.

The Monitoring Tab

The Monitoring tab, as its name suggests, is used to provide several monitoring features of the PIX firewall. The PIX provides a wealth of information that can be monitored via this screen, shown in Figure 13.13.

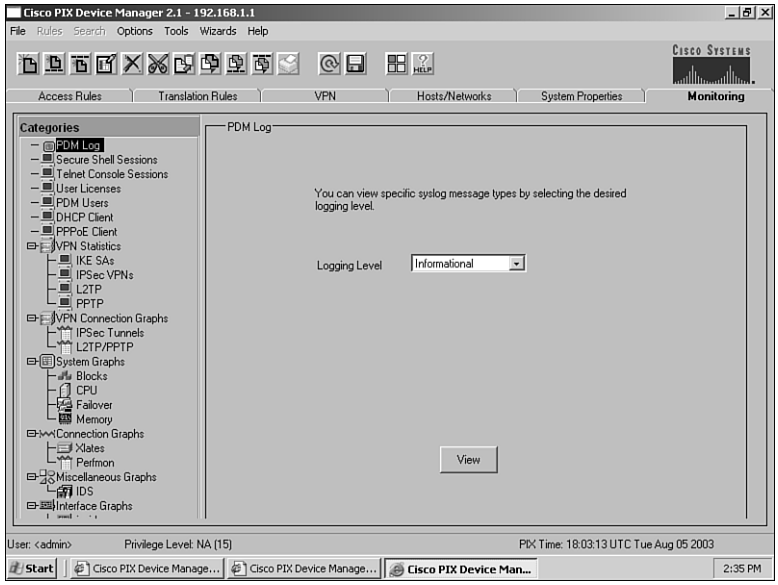

Figure 13.13 The Monitoring tab.

PDM Pull-down Menus

The pull-down menus also provide several configuration features and options. Figure 13.14 displays a snapshot of the PDM pull-down menu options.

The File Pull-down Menu

The File pull-down menu enables you to reset the firewall to the factory defaults, save the running configuration to flash or a TFTP server, or simply refresh the PDM interface. Figure 13.15 displays the options in the File menu.

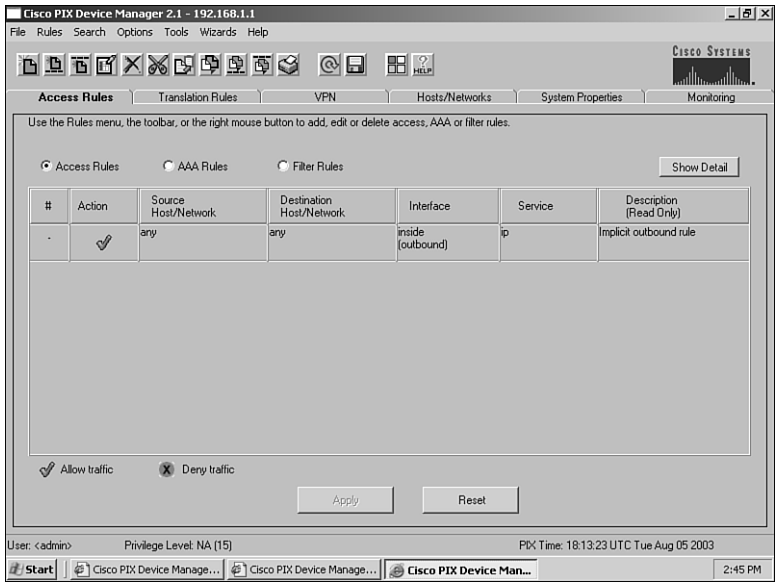

Figure 13.14 Pull-down menus.

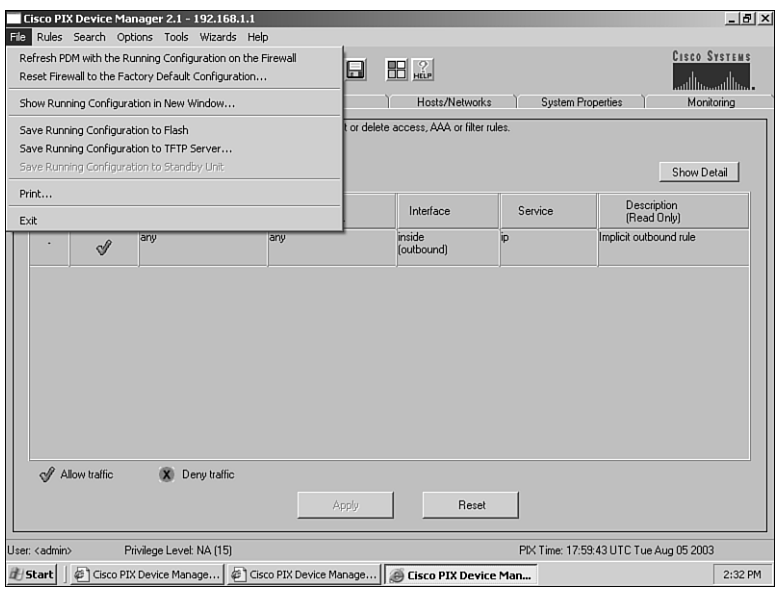

Figure 13.15 File pull-down options.

The Options Pull-down Menu

The Options pull-down menu enables you to select preferences and define three main settings: namely, preview commands, confirm before exiting, and display dialog about VPN wizards. The preview command preference is handy when you want to learn which commands the PDM is actually sending down to the firewall via the CLI. Figure 13.16 displays the preferences dialog box.

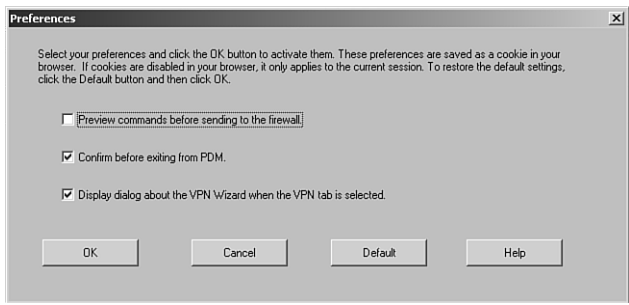

Figure 13.16 Preference options.

The Wizards Pull-down Menu

The Wizards pull-down menu contains two wizards that help you configure the PIX firewall (see Figure 13.17). The Setup Wizard enables you to configure a basic firewall by answering simple questions, whereas the VPN Wizard enables you to configure a VPN configuration for either site-to-site or remote access. Figure 13.18 displays the first screen of the VPN Wizard.

The PDM interface enables you to configure the PIX firewall using a Web-based interface. The PDM can be installed on almost all the PIX firewall products, and it provides several interface screens for PIX configuration. If commands are found that are not supported by the PDM, the interface warns you about them and sometimes even locks you out of all the configuration screens, thus limiting your monitoring ability. Lastly, the PDM contains two wizards that assist in the initial setup of the firewall's standard and VPN configurations.

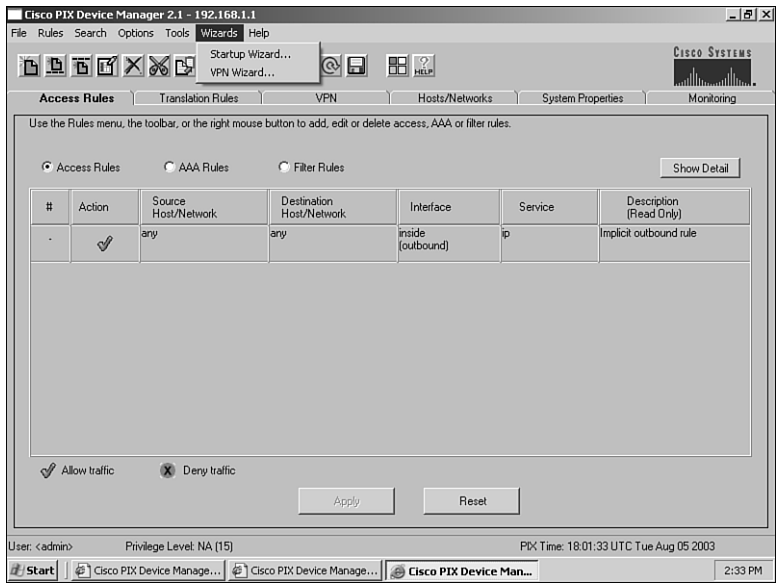

Figure 13.17 The available wizards.

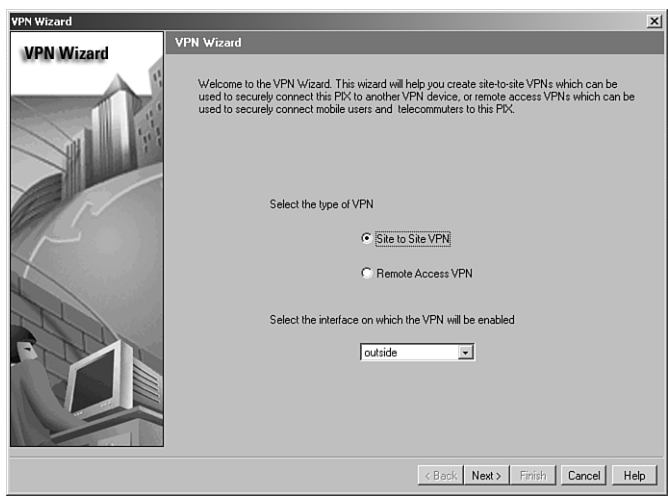

Figure 13.18 The VPN Wizard's first screen.