



On completion of this chapter, you will be able to perform the following tasks:

- Describe the PIX Device Manager (PDM) and its capabilities.
- Describe PDM's browser and PIX Firewall requirements.
- Install PDM and prepare the PIX Firewall to use PDM.
- Navigate the PDM configuration windows.
- Perform basic configuration of the PIX Firewall using PDM.
- Test and verify PDM functionality.

Cisco PIX Device Manager

The Cisco PIX Device Manager, or PDM, is a browser-based configuration and monitoring tool that allows you to easily configure and manage a single PIX Firewall without extensive knowledge of the command-line interface (CLI). The first version of PDM, introduced with PIX Firewall Version 6.0, had limited capabilities and was suitable for basic configurations.

With each new release of the software, however, Cisco has improved and expanded the capabilities of PDM. The latest release, Version 3.0, is the most capable version of the PDM to date and adds support for many of the new features introduced in PIX Firewall Version 6.3. This chapter provides an overview of PDM, system requirements, and configuration guidelines.

PDM Overview

PDM provides a graphical console for monitoring and configuring a single PIX Firewall. The PDM software image must be installed and executed on each individual PIX Firewall that you intend to configure and monitor using PDM. However, after the software is properly installed, you can point your browser to more than one PIX Firewall and administer several PIX Firewalls from a single workstation.

NOTE

If you are interested in a GUI-based management console to manage a large number of Cisco PIX Firewalls, you should consider the Cisco Management Center for Firewalls (Firewall MC), which is covered in Chapter 19, “PIX Firewall Management in Enterprise Networks.”

PDM is secure, versatile, and easy to use. It works with PIX Firewall 500 series models and runs on a variety of platforms.

NOTE You can also use PDM to configure and monitor the Firewall Services Module (FWSM) on a Cisco Catalyst 6500 switch. This use of PDM is discussed later in Chapter 21, “Firewall Services Module.”

PDM enables you to securely configure and monitor your PIX Firewall remotely. Its ability to work with the Secure Socket Layer (SSL) protocol ensures that communication with the PIX Firewall is secure, and because it is implemented in Java, it offers robust, real-time monitoring.

PDM works with PIX Firewall Software Versions 6.0 and higher and comes preloaded into Flash memory on new PIX Firewalls running Software Versions 6.0 and higher. If you are upgrading from a previous version of the PIX Firewall, you can download PDM from Cisco and then copy it to the PIX Firewall via Trivial File Transfer Protocol (TFTP).

NOTE The specific version of the PDM that you use depends on the version of PIX Firewall you are running. PIX Firewall Versions 6.0 and 6.1 work with PDM Versions 1.0 or 1.1. If you are running PIX Firewall Version 6.2, you should use PDM 2.0 or 2.1. PDM Version 3.0 is specifically designed for use with PIX Firewall Version 6.3.

PDM runs on Windows, Sun Solaris, and Linux platforms and requires no plug-ins or complex software installations. The PDM applet uploads to your workstation when you access the PIX Firewall from your browser.

Using the PIX Firewall CLI, Firewall MC, or even legacy Cisco Secure Policy Manager (CSPM) systems, you can use PDM to create a new configuration or view, alter, and maintain configurations you previously created.

In its current release (Version 3.0), PDM is a robust, capable, and powerful management and monitoring tool that deserves consideration as the primary management tool for your PIX Firewall. Whether you choose to use PDM or other tools such as the CLI or Firewall MC depends largely on your preference. However, you might want to avoid using the PDM if

- You are managing a large number of PIX Firewalls. Firewall MC and even CLI are better suited for managing large numbers of PIX Firewalls.
- You have a large number of access; authentication, authorization, and accounting (AAA); filter; or translation rules, which are typically created more efficiently using CLI.
- You are using commands that are not yet supported in PDM such as the **alias** command.
- You are creating a configuration file that is significantly larger than 100 KB.

NOTE

Always check Cisco.com for the latest version of the PIX Firewall image, PDM image, and documentation to determine which commands are supported. The list of commands supported by the PDM has increased significantly since the first release, and support for additional commands in future versions of PDM is expected.

If your project does not involve any of the items in the preceding list and you prefer a GUI-based management console to a CLI-based one, PDM is for you, and it can serve as your primary management and monitoring tool for PIX Firewall implementations.

You can also use the PDM as a learning tool by viewing the CLI commands that it generates when you configure various components of the PIX Firewall. For example, virtual private network (VPN) commands tend to be somewhat cryptic, and PDM greatly simplifies the process of creating VPN configurations. (VPN topics are discussed in detail in Chapters 15, 16, and 17.) You can then view the generated CLI commands to better understand VPN configurations and proper CLI techniques for configuring site-to-site and remote access VPN connections.

PDM Operational Requirements

New PIX Firewalls that contain Version 6.0 also have a pre-installed Data Encryption Standard (DES) activation key. If you are using a new PIX Firewall with PIX Firewall Version 6.0 or higher pre-installed, you have all the requirements discussed in this section and you can continue to the next section, “Preparing for PDM.”

A PIX Firewall must meet the following requirements to run PDM:

- You must have an activation key that enables DES or the more secure Triple DES (3DES) and Advanced Encryption Standard (AES), which PDM requires for support of the SSL protocol. If your PIX Firewall is not enabled for DES or 3DES/AES encryption, you can receive a new activation key by completing the appropriate form available on Cisco.com.

NOTE

You can request a free DES or 3DES/AES encryption license using the Customer Registration site at Cisco.com. You might need a Cisco Connection Online (CCO) account to access and complete the online request form for a new license and activation key.

- Verify that the PIX Firewall meets all requirements listed in the release notes for the PIX Firewall software version in use.

- Verify that your PIX Firewall hardware model, PIX Firewall software version, and PDM version are compatible. Refer to the Table 6-1 to ensure compatibility. If you need to update the software on the PIX Firewall, download PIX Firewall and PDM software from the following URL on Cisco.com: <http://www.cisco.com/cgi-bin/tablebuild.pl/pix>.

NOTE

You might need a CCO account to access and download PIX Firewall and PDM software from Cisco.com.

- You must have at least 8 MB of Flash memory on the PIX Firewall.
- Ensure that your configuration is less than 100 KB (approximately 1500 lines). Configurations over 100 KB cause PDM performance degradation.

NOTE

You can determine the size of your configuration by using the **show flashfs** command at the PIX Firewall CLI console. When you issue this command, the PIX Firewall displays several lines of output. The configuration file size is specified as “file 1” within the output of the **show flashfs** command.

Table 6-1 Valid PIX Firewall and PDM Version Combinations

PDM Version	Supported PIX Firewall Version	Supported PIX Firewall Model
1.0	6.0 or 6.1	506, 515, 520, 525, 535
1.1	6.0 or 6.1	506, 515, 520, 525, 535
2.0	6.2	501, 506/506E, 515/515E, 520, 525, 535
2.1	6.2	501, 506/506E, 515/515E, 520, 525, 535
2.1	FWSM 1.1	FWSM
3.0	6.3	501, 506/506E, 515/515E, 520, 525, 535

To access PDM from a browser, the system must meet the following requirements:

- JavaScript and Java must be enabled. If you are using Microsoft Internet Explorer, the native Java Virtual Machine (JVM) is supported. You can also use Java Runtime Environment (JRE) Version 1.3.1, 1.4.0, or 1.4.1. These requirements are for PDM Version 3.0. Earlier versions of the PDM also work with the latest versions of the

Microsoft JVM or Sun Microsystems JRE. If you have an older version of these environments, you can download the latest version of the JVM for Internet Explorer and the latest version of the JRE from the Microsoft and Sun Microsystems websites, respectively.

- Browser support for SSL must be enabled. The supported versions of Internet Explorer and Netscape Navigator support SSL without requiring additional configuration.

PDM can operate in browsers running on Windows, Sun Solaris, or Linux operating systems. The requirements for running PDM 3.0 on each operating system appear in the following subsections.

Windows Requirements

PDM 3.0 is supported on Windows 98, ME, NT 4.0 (Service Pack 4 [SP4] or higher), Windows 2000 (SP3), and Windows XP. Windows 3.1 and Windows 95 are not supported. Windows XP and Windows 2000 with SP3 are the preferred and recommended Windows platforms for PDM 3.0. Specific browser and Java requirements for PDM 3.0 appear in Table 6-2.

NOTE

Hardware and software requirements listed in this chapter refer to Version 3.0 of the PDM. Check Cisco.com for specific requirements for running earlier or later versions of PDM.

Table 6-2 *Browser and Java Requirements for Windows Platforms Using PDM 3.0*

Operating System	Browser	JAVA Environment
Windows 98 Windows ME Windows NT 4.0 (SP4 or higher) Windows 2000 (SP3) Windows XP	Internet Explorer 5.5 or 6.0 (6.0 recommended)	Built-in JVM (VM 3167 or higher, VM 3809 recommended)
	Internet Explorer 5.5 or 6.0 (6.0 recommended)	JRE plug-in 1.3.1, 1.4.0, or 1.4.1 (1.4.1_02 recommended)
	Netscape 4.7x	Built-in JVM 1.1.5
	Netscape 7.0x (recommended)	JRE plug-in 1.4.0 or 1.4.1 (1.4.1_02 recommended)

In addition to the software requirements in Table 6-2, the following hardware requirements apply for Windows systems using PDM 3.0:

- Pentium III or compatible processor running at 450 MHz or higher
- 256 MB of RAM
- 1024-by-768 pixel display with at least 256 colors (16-bit color is recommended)

Sun Solaris Requirements

PDM 3.0 is supported on Sun Solaris 2.8 or 2.9 running CDE window manager. The following requirements apply to the use of PDM 3.0 on Solaris-based systems:

- Sun Solaris 2.8 or 2.9 running CDE window manager. Sun Solaris 2.8 is recommended.
- Netscape 4.78 with built-in JVM.

NOTE Netscape Communicator 4.79 is not supported with PDM 3.0.

- Sparc microprocessor.
- At least 128 MB of RAM.
- A 1024-by-768 pixel display with at least 256 colors.

Linux Requirements

You can also use PDM 3.0 on Linux systems. Table 6-3 lists the operating system and browser requirements for Linux systems using PDM 3.0.

Table 6-3 *Browser and Java Requirements for Linux Platforms Using PDM 3.0*

Operating System	Browser	Java Environment
Red Hat Linux 7.0, 7.1, 7.2, 7.3, or 8.0 running GNOME or KDE (Red Hat Linux 8.0 is recommended)	Netscape 4.7x on Red Hat Version 7.x	Built-in JVM
	Mozilla 1.0.1 on Red Hat Linux 8.0 (recommended)	JRE plug-in 1.4.1 (1.4.1_02 recommended)

In addition to the software requirements listed in Table 6-3, the following hardware requirements apply for Linux systems using PDM 3.0:

- Pentium III or compatible processor running at 450 MHz or higher
- At least 128 MB of RAM
- 1024-by-768 pixel display with at least 256 colors (16-bit color is recommended)

General Guidelines

The following are a few general guidelines for workstations running PDM:

- You can run several PDM sessions on a single workstation. The maximum number of PDM sessions depends on workstation's resources, such as memory, CPU speed, and browser type.
- The time required to download the PDM applet can be greatly affected by the speed of the link between the workstation and the PIX Firewall. A minimum of 56 Kbps link speed is required; however, 1.5 Mbps or higher is recommended. After you load the PDM applet on the workstation, the link speed impact on PDM operation is negligible.
- The use of virus-checking software might dramatically increase the time required to start PDM, especially for Netscape Communicator on any Windows platform or Windows 2000 and Windows XP running any type of browser.
- Accessing the PDM using fully qualified domain names (FQDNs) is recommended. This process does require appropriate Domain Name System (DNS) entries or the use of a hosts file on the workstation. With some JVMs, you can experience degraded performance when using the IP address of the PIX to access PDM.

If a workstation's resources are running low, close and re-open the browser before launching PDM.

Preparing for PDM

As mentioned earlier, new PIX Firewalls with PIX Firewall Version 6.0 or higher are preloaded with PDM. If your PIX Firewall has PDM 2.0 or higher, you can use PDM's Startup Wizard for the initial configuration. Simply connect the PC to the inside interface (Ethernet 1) of the PIX Firewall and use Dynamic Host Configuration Protocol (DHCP) or specify an address in the range 192.168.1.2 to 192.168.1.254. Then, access the PIX Firewall through PDM using the URL <https://192.168.1.1/startup.html>. PIX Firewalls with default factory settings have an IP address of 192.168.1.1 for their inside interfaces.

You must configure the PIX Firewall with the following information before you can install or use PDM. You can either preconfigure a new PIX Firewall through the interactive

prompts, which appear after the PIX Firewall boots, or you can enter the commands shown here for each information item:

- **Enable password**—Enter an alphanumeric password to protect the PIX Firewall privileged mode. The alphanumeric password can be up to 16 characters in length. You must use this password to log in to PDM. The command syntax for enabling a password is as follows:
`enable password password [encrypted]`
- **Time**—Set the PIX Firewall clock to Universal Coordinated Time (UTC, also known as Greenwich Mean Time, or GMT). For example, if you are in the Pacific Daylight Savings time zone, set the clock 7 hours ahead of your local time to set the clock to UTC. Enter the year, month, day, and time. Enter the UTC time in 24-hour time as hour:minutes:seconds. The command syntax for setting the clock is as follows:
`clock set hh:mm:ss {day month | month day} year`
- **Inside IP address**—Specify the IP address of the PIX Firewall’s inside interface. Ensure that this IP address is unique on the network and not used by any other computer or network device, such as a router. The command syntax for setting an inside IP address is as follows:
`ip address if_name ip_address [netmask]`
- **Inside network mask**—Use the **ip address** command to specify the network mask for the inside interface. An example is 255.255.255.0. You can also specify a subnetted mask (for example, 255.255.255.224). Do not use all 255s, such as 255.255.255.255; this prevents traffic from passing on the interface. If a network mask is not specified, the default major network mask is applied (255.0.0.0 for Class A addresses, 255.255.0.0 for Class B addresses, and 255.255.255.0 for Class C addresses).
- **Host name**—Specify up to 16 characters as a name for the PIX Firewall. The command syntax for setting a host name is as follows:
`hostname newname`
- **Domain name**—Specify the domain name for the PIX Firewall. The command syntax for enabling the domain name is as follows:
`domain-name name`
- **IP address of the host running PDM**—Specify the IP address of the workstation that accesses PDM from its browser. The command syntax for granting permission for a host to connect to the PIX Firewall with SSL is as follows:
`http ip_address [netmask] [if_name]`
- **HTTP Server**—Enable the HTTP server on the PIX Firewall with the **http server enable** command.

If you are installing PDM on a PIX Firewall with an existing configuration, you might need to restructure your configuration from the PIX Firewall CLI before installing PDM to obtain full PDM capability. There are certain commands that PDM does not support in a configuration. If these commands are present in your configuration, you have access to only the Monitoring tab. PDM handles each PIX Firewall command in one of the following ways:

- Parse and allow changes (supported commands)
- Parse and only permit access to the Monitoring tab (unsupported commands)
- Parse without allowing changes (partially supported commands that PDM handles transparently without preventing further configuration)
- Only display in the unparseable command list (partially supported commands that PDM handles transparently without preventing future configuration)

NOTE

The different modes with which PDM handles each command and the list of commands in each mode are explained in detail in the document “PDM Support for PIX Firewall CLI Commands,” available on Cisco.com.

An unconfigured PIX Firewall starts in an interactive setup dialog to enable you to perform the initial configuration required to use PDM. You can also access the setup dialog by entering **setup** at the configuration mode prompt.

NOTE

You can also use PDM’s Startup Wizard for the initial configuration of a new PIX Firewall with PDM 2.0 or higher. Simply connect the PC to the inside interface (Ethernet 1) of the PIX Firewall and use DHCP or specify an address in the range 192.168.1.2 to 192.168.1.254. You can then access the PIX Firewall through PDM using the URL <https://192.168.1.1/startup.html>.

The dialog asks for several responses, including the inside IP address, network mask, host name, domain name, and PDM host. The host name and domain name are used to generate the default certificate for the SSL connection.

Pressing the **Enter** key instead of entering a value at the prompt causes the default value within the brackets to be accepted. You must fill in any fields that show no default values and change default values as necessary. After the configuration is written to Flash memory, the PIX Firewall is ready to start PDM.

CAUTION You must set the clock for PDM to generate a valid certification. Set the PIX Firewall clock to UTC (also known as GMT).

Table 6-4 lists the prompts in the setup dialog.

Table 6-4 *PIX Firewall Interactive Setup Dialog*

Prompt	Definition	Sample Value
Enable password	Enable password for this PIX Firewall, up to 16 characters.	cisco123
Clock (UTC)	Enables you to set the PIX Firewall clock to UTC (also known as GMT).	N/A
Year [system year]	Enables you to specify the current year or return to the default year stored in the host computer.	2003
Month [system month]	Enables you to specify the current month or return to the default month stored in the host computer.	June
Day [system day]	Enables you to specify the current day or return to the default day stored in the host computer.	4
Time [system time]	Enables you to specify the current time in hh:mm:ss format or return to the default time stored in the host computer.	20:30:00
Inside IP address	The network interface IP address of the PIX Firewall.	10.0.0.1
Inside network mask	A network mask that applies to the inside IP address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.	255.255.255.0
Host name	The host name you want to display in the PIX Firewall command-line prompt.	pixfirewall
Domain name	The DNS domain name of the network on which the PIX Firewall runs.	Cisco.com
IP address of host running PIX Device Manager	IP address on which PDM connects to the PIX Firewall.	10.0.0.11
Use this configuration and write to flash?	Enables you to store the new configuration to Flash memory. It is the same as the write memory command. If the answer is yes, the inside interface is enabled and the requested configuration is written to Flash memory. If the user answers anything else, the setup dialog repeats, using the values already entered as the defaults for the questions.	Yes or No

Using PDM to Configure the PIX Firewall

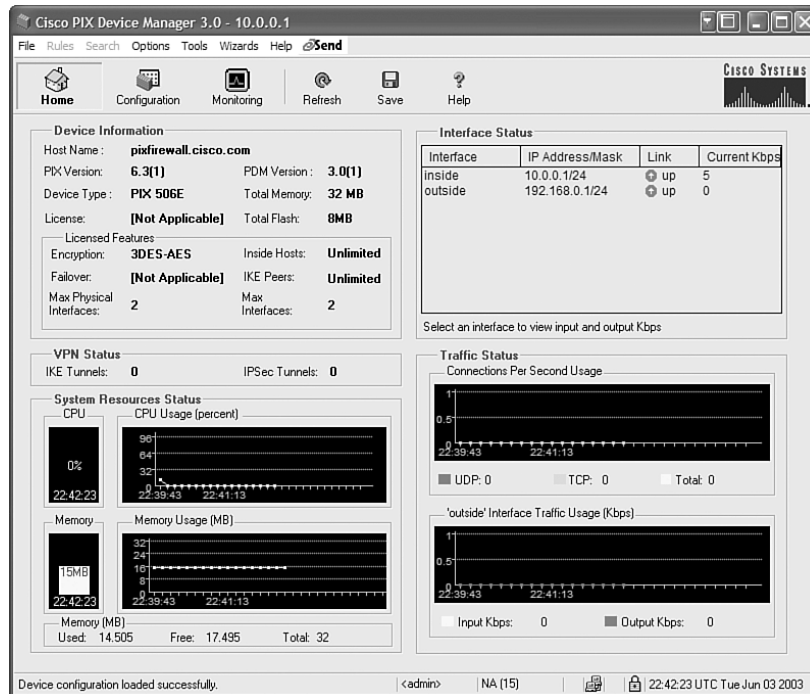
You access the PDM using an SSL-encrypted connection (HTTPS) to the PIX Firewall. For example, to access the PDM on a PIX Firewall with an IP address of 10.0.0.1, you use the URL `https://10.0.0.1`.

The PDM Startup Wizard (available with PDM 2.0 and higher) is an easy way to begin the process of configuring your PIX Firewall. The wizard steps you through such tasks as

- Enabling the PIX Firewall interfaces
- Assigning IP addresses to the interfaces
- Configuring a host name and password
- Configuring Point-to-Point Protocol over Ethernet (PPPoE)
- Configuring Easy VPN Remote
- Configuring Auto Update
- Configuring network address translation (NAT) and port address translation (PAT)
- Configuring the DHCP server

You can run the Startup Wizard at any time by choosing **Tools > Startup Wizard**, and it automatically starts if you are accessing a PIX Firewall with PDM 2.0 or higher for the initial configuration.

Figure 6-1 PDM 3.0 Home Screen

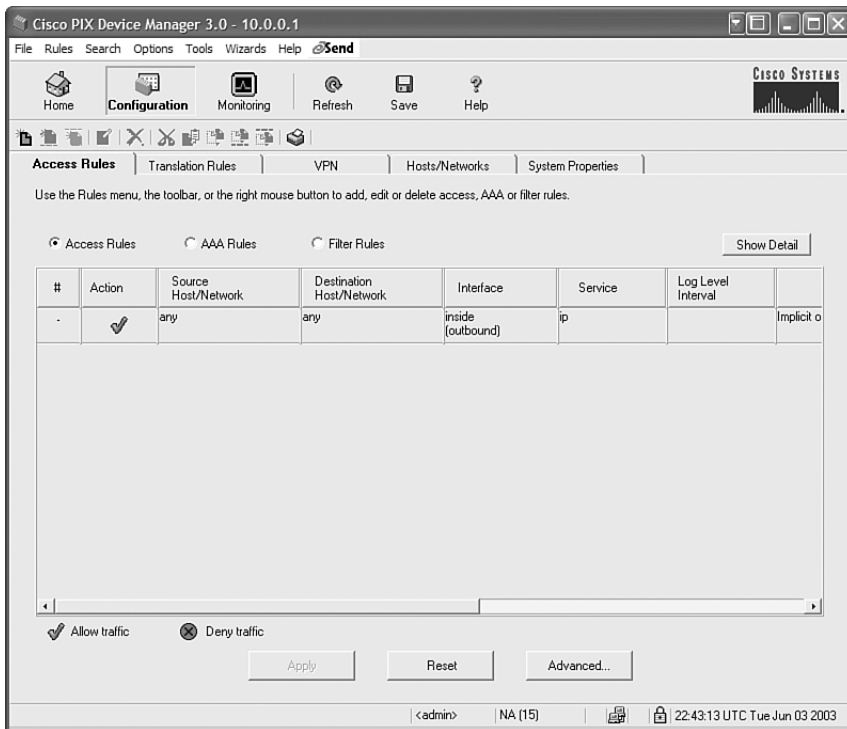


When you first start PDM, you see the home screen shown in Figure 6-1. This screen provides a quick snapshot of the firewall's status and includes five specific areas:

- **Device Information**—Information about the PIX Firewall model, PIX version, PDM version, memory, and available licenses
- **Interface Status**—Information on interfaces, IP address, link status, and throughput
- **VPN Status**—Number of active Internet Key Exchange (IKE) and IP Security (IPSec) tunnels
- **System Resources Status**—Information on CPU and memory usage
- **Traffic Status**—Information on traffic throughput and TCP and User Datagram Protocol (UDP) connections per second

You can access other functions of the PDM from the initial screen. You access configuration and monitoring screens by clicking the **Configuration** or **Monitoring** buttons at the top of the page, as shown in Figure 6-1. Clicking the **Configuration** button brings up the configuration page of the PDM, shown in Figure 6-2.

Figure 6-2 PDM 3.0 Configuration Screen



The configuration page consists of the PDM toolbar and five tabs, which enable you to configure various aspects of the product:

- **Access Rules**—Shows configured access rules for your network
- **Translation Rules**—Enables you to view all the address translation rules applied to your network
- **VPN**—Enables you to create VPNs using IPsec
- **Hosts/Networks**—Enables you to view, edit, add to, or delete from the list of hosts and networks defined for the selected interface
- **System Properties**—Enables you to configure many other aspects of the PIX Firewall, such as management protocols, logging, intrusion detection, AAA, and routing settings

You access various monitoring features of the PIX Firewall by clicking the **Monitoring** button. Figure 6-3 shows the main monitoring screen on PDM 3.0. Monitoring capabilities of the PDM are discussed later in this chapter.

Figure 6-3 PDM 3.0 Monitoring Screen



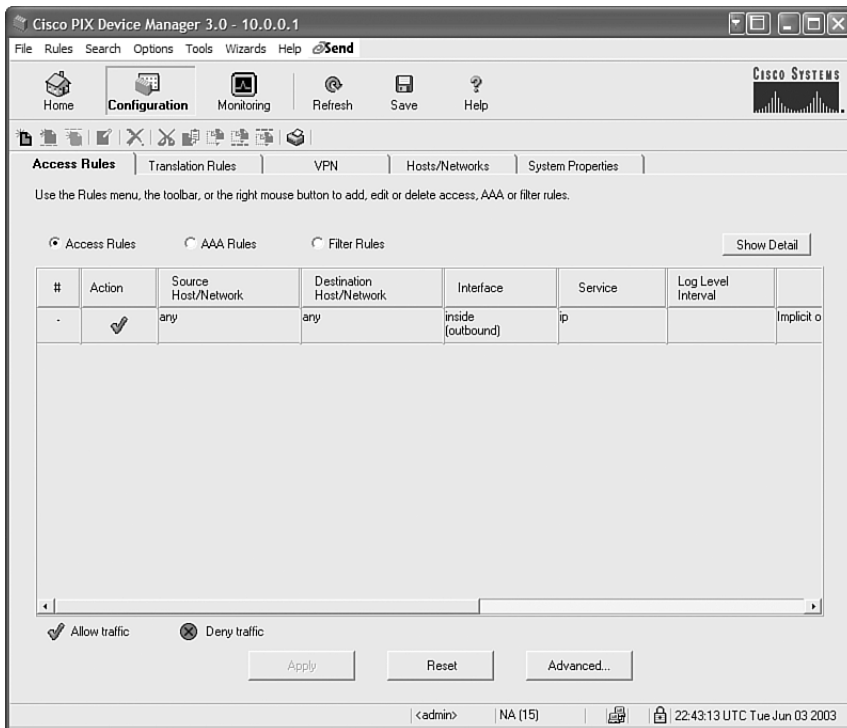
Configuration

Configuration screens and associated procedures are covered in detail in the following subsections. PDM provides excellent context-based online help, which you can utilize.

Access Rules Tab

Figure 6-4 shows the Access Rules screen (tab). It combines the concepts of access control lists (ACLs), outbound lists, and conduits to describe how an entire subnet or specific network host interacts with another to permit or deny a specific service, protocol, or both. The implicit outbound rule and any other access rules configured on the PIX Firewall appear on this screen. ACLs are covered in detail in Chapter 8, “Access Control Lists and Content Filtering.”

Figure 6-4 *Access Rules Configuration Screen*



PDM does not support the use of ACLs, conduits, and outbounds together. You can use only one of the three at one time, ACLs being the preferred choice. PDM continues to use the choice you make. If you attempt to use more than one of these choices in your configuration, you will be able to only perform monitoring tasks.

NOTE

PIX Firewall Software Version 6.3 will be the last release to support the **conduit** and **outbound** commands. You should use ACLs for all new configurations and consider converting existing conduit-based configurations to ACLs.

When you work in either the Access Rules or the Translation Rules tab, you can access the task menus for creating or modifying rules in one of four ways:

- Using the PDM toolbar (the row of icons immediately above the tabs)
- Using the Rules menu
- Right-clicking anywhere in the rules table
- Double-clicking an existing rule (for inspection or modification)

Figure 6-5 shows the Add Rule screen, which enables you to perform a number of tasks:

- Define source and destination hosts and networks using the IP address and mask, previously defined names, or groups.
- Specify protocol and services that are affected by the rule.
- Use predefined service groups to simplify the access rules.
- Define new service groups by clicking **Manage Service Groups**.

Figure 6-5 Add Rule Screen

This tab also enables you to define AAA rules and filter rules for ActiveX and Java. The configuration edits you perform on the Access Rules tab are captured by PDM but are not sent to the PIX Firewall until you click **Apply**. This applies to all configurations performed with PDM, including those performed in the Translation Rules tab, the Hosts/Networks tab, and the System Properties tab. Always click **Apply** to send your configuration edits to the PIX Firewall. Also remember, it is important to save your configuration to Flash memory by choosing **File > Save Running Configuration to Flash** from the main menu or clicking the **Save** icon in the toolbar.

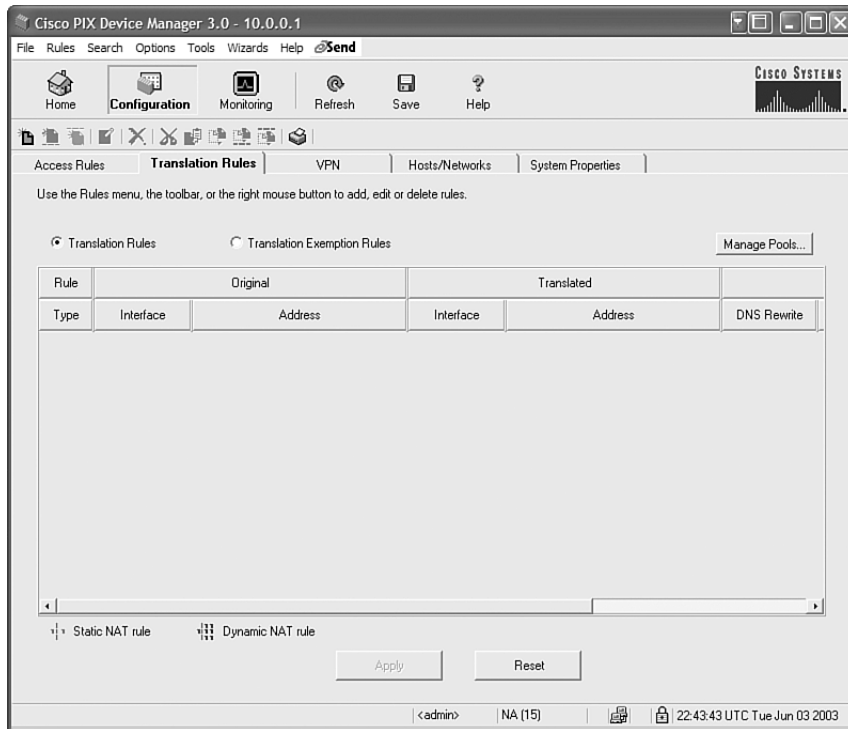
NOTE

You can also use the Access Rules tab to create object groups and apply them to access lists.

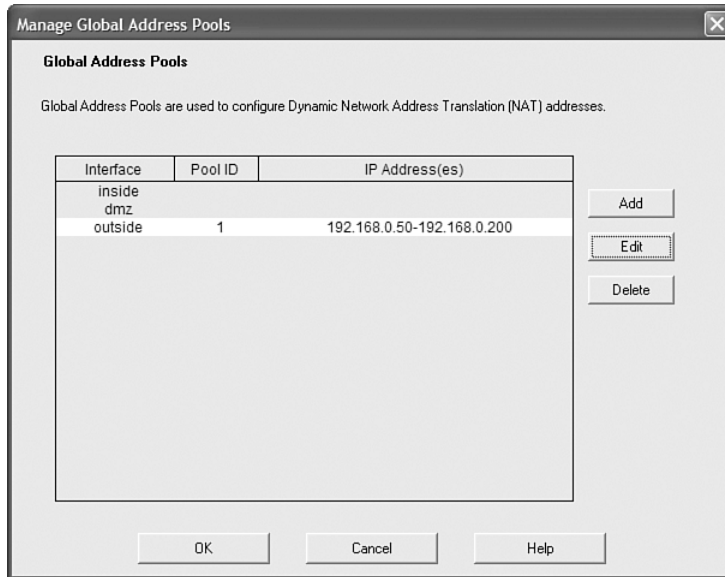
Translations Rules Tab

Figure 6-6 shows the Translations Rules screen. The Translations Rules tab enables you to create and view static and dynamic address translation rules for the network. Before you can designate access and translation rules for your network, you must first define each host or server for which a rule will apply. To do so, select the **Hosts/Networks** tab to define hosts and networks. Address translation concepts are presented in detail in Chapter 7, “Translation and Connections.”

Figure 6-6 *Translations Rules Configuration Screen*



The Manage Global Address Pools window shown in Figure 6-7 enables you to configure global address pools to be used by NAT. From this window, you can edit or delete existing global pools or add new pools. You can access the Manage Global Address Pools window from the Manage Pools button on the Translation Rules tab.

Figure 6-7 *Manage Global Address Pools Window*

Remember that it is necessary to configure translation rules even if you have routable IP addresses on your secure networks. This is a unique feature of the PIX Firewall. You can use a routable address by translating the IP address to itself on the outside.

To add a new translation rule, you must use the Add Address Translation Rule screen shown in Figure 6-8. You access this screen within the Translation Rules tab by selecting **Rules > Add**, by clicking the **Add New Rule** button on the toolbar, or by right-clicking within the rules list window and selecting **Add** from the popup menu. As shown in Figure 6-8, you specify the original interface, original host, and network using the IP address and mask, translation interface, and the translated address (static or dynamic).

NOTE

The order in which you apply translation rules can affect the way the rules operate. PDM lists the static translations first and then the dynamic translations. When processing NAT, the PIX Firewall first translates the static translations in the order they are configured. You can use the **Insert Before** or **Insert After** commands from the Rules menu to determine the order in which static translations are processed. Because dynamically translated rules are processed on a best-match basis, the option to insert a rule before or after a dynamic translation is disabled.

Figure 6-8 *Add Translations Rules Screen*

If you want to exclude a specific host or network from NAT, you can select the **Translation Exemption Rules** option on the Translation Rules tab. You use the Add Address Exemption Rule screen shown in Figure 6-9 to configure exemption rules. After activating the Translation Exemption Rules option, you can access the Add Address Exemption Rule screen by selecting **Rules > Add**, by clicking the **Add New Rule** button on the toolbar, or by right-clicking within the rules list window and selecting **Add** from the popup menu.

VPN Tab

Figure 6-10 shows the VPN configuration screen of the PDM. From the VPN tab, you can create site-to-site or remote access VPNs. You can also configure the PIX Firewall to act as an Easy VPN Remote device using the configuration options on this screen.

Figure 6-9 Add Address Exemption Rules Screen

Add Address Exemption Rule

Action
Select an action:

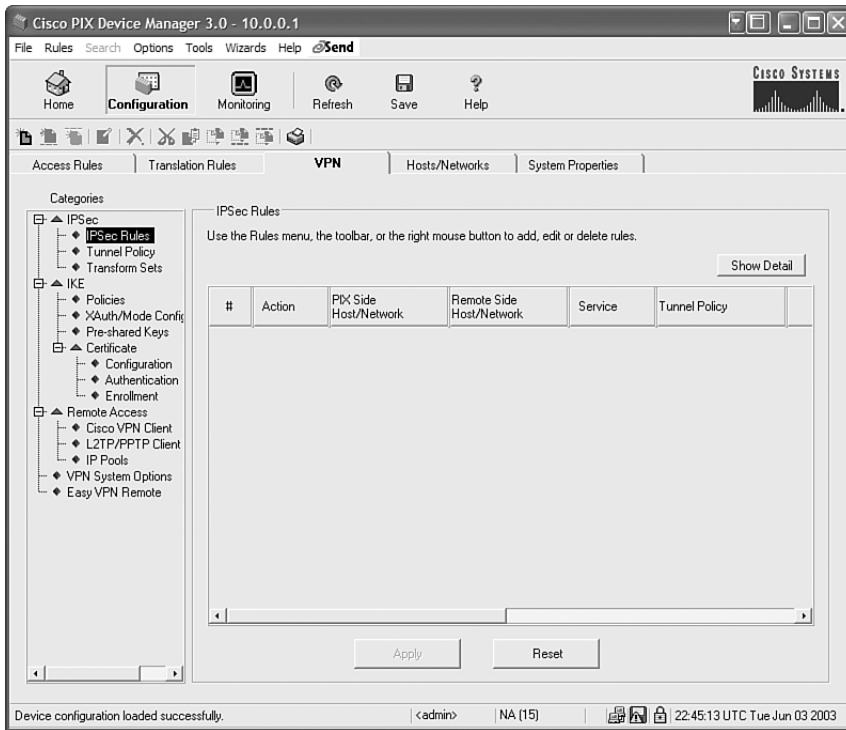
Host/Network Exempted From NAT
 IP Address Name Group
Interface:
IP address:
Mask:

When Connecting To
 IP Address Name Group
Interface:
IP address:
Mask:

Please enter the description below (optional):

VPN topics and configuration procedures are covered in detail in Chapter 15, “Virtual Private Networks,” Chapter 16, “Site-to-Site VPNs,” and Chapter 17, “Client Remote Access VPNs,” and are not presented here. CLI commands for configuring VPN settings tend to be somewhat complicated. PDM does an excellent job of simplifying VPN configuration tasks on the PIX Firewall and should be given strong consideration as the primary tool for VPN configurations. You are less likely to commit errors in configuration using the PDM. After you create your VPN configuration with PDM, you can view the running configuration on your PIX Firewall to see the specific CLI commands generated by the PDM.

Figure 6-10 VPN Configuration Screen



Hosts/Networks Tab

The PDM requires that you define any host or network that you intend to use in ACLs and translation rules. These hosts or networks are organized below the interface from which they are reachable. When defining either type of rule, you can reference a host or network by clicking the **Browse** button in the appropriate add or edit rule window. Additionally, you can reference the host or network by name if a name is defined for that host or network. It is recommended that you name all hosts and networks.

Figure 6-11 shows the Hosts/Networks configuration screen of the PDM. In addition to defining the basic information for these hosts or networks, you can define route settings and translation rules (NAT) for any host or network. You can also configure route settings in the Static Route panel on the System Properties tab and translation rules on the Translation Rules tab. These different configuration options accomplish the same results. The Hosts/Networks tab provides another view to modify these settings on a per-host and per-network basis. You can also define groups and add hosts and networks to a specific group. Figure 6-12 shows the Add Host/Network Group screen used to define groups and group members.

Figure 6-11 *Hosts/Networks Configuration Screen*

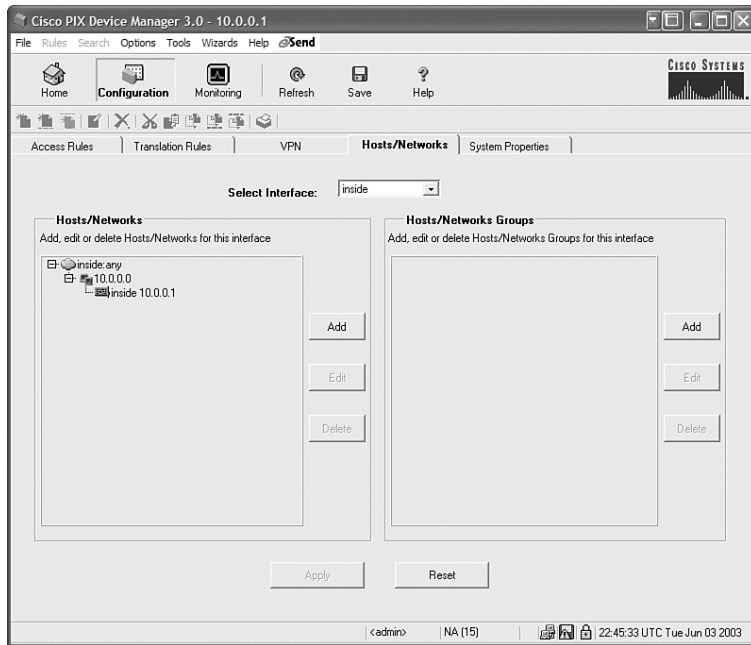
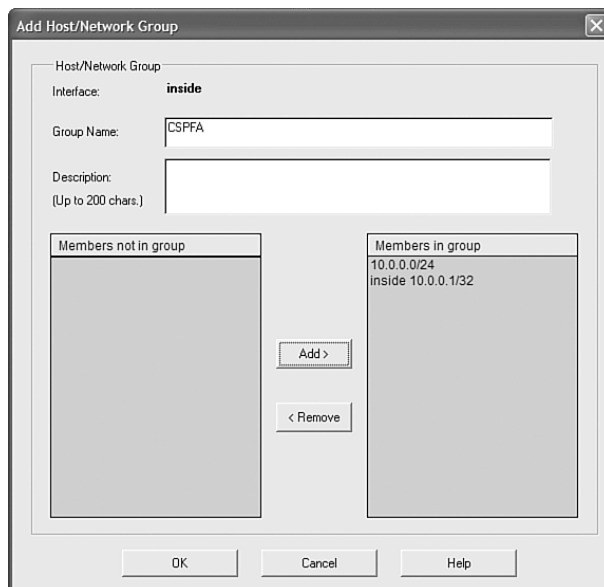


Figure 6-12 *Add Host/Network Group Screen*

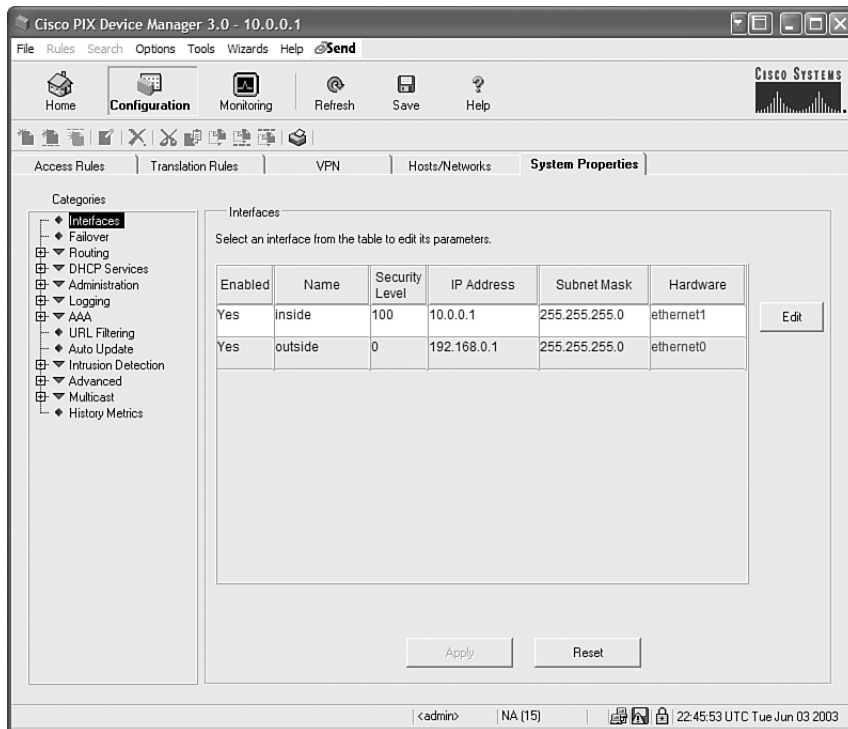


The information provided in this window enables the basic identification information for that host or network. It includes values for the IP address, netmask, interface, and name of the host or network. PDM uses the name and IP address and netmask pair to resolve references to this host or network in the source and destination conditions of access rules and in translation rules. PDM uses the interface value to apply access and translation rules that reference this host or network to the correct interface. The interface delivers network packets to the host or network; therefore, it enforces the rules that reference that host or network.

System Properties Tab

Figure 6-13 shows the System Properties configuration screen.

Figure 6-13 *System Properties Configuration Screen*



The System Properties tab enables you to configure many aspects of the PIX Firewall, including the following:

- **Interfaces**—In addition to their names, the Interfaces panel displays and enables you to edit additional configuration information required for each interface. You can configure a PIX Firewall interface with a static IP address or you can configure it to use DHCP or PPPoE.

NOTE

Your configuration edits are captured by PDM but not sent to the PIX Firewall until you click **Apply**.

- **Failover**—Enables you to enable, disable, and configure serial and LAN-based failover and stateful failover.
- **Routing**—The routing panel is divided into the following four sections dealing with different routing configurations:
 - Routing Information Protocol (RIP)
 - Static Routes
 - Proxy Address Resolution Protocols (ARPs)
 - Open Shortest Path First (OSPF)

NOTE

The categories listed are based on PDM 3.0. Earlier versions of PDM are similar, but they might not include all of the items listed or display them in the same order shown here.

- **DHCP Services**—Enables you to configure DHCP Server and Relay settings.
- **PIX Administration**—This panel contains the following sections:
 - Device
 - Password
 - Authentication/Authorization
 - User Accounts
 - Banner
 - Console
 - PDM/HTTPS
 - Telnet

- Secure Shell
- Management Access
- Simple Network Management Protocol (SNMP)
- Internet Control Message Protocol (ICMP)
- TFTP Server
- Clock
- Network Time Protocol (NTP)
- **Logging**—This panel is divided into the following sections:
 - Logging Setup
 - PDM Logging
 - Syslog
 - Others
- **AAA**—This panel contains the following sections:
 - AAA Server Groups
 - AAA Servers
 - Auth. Prompt
- **URL Filtering**—This panel enables you prevent users from accessing external WWW URLs that you designate using a WebSense or N2H2 URL filtering server.
- **Auto Update**—This panel enables you to specify the Auto Update server and polling parameters for image and configuration updates.
- **Intrusion Detection**—This panel is divided into the following two sections:
 - IDS Policy
 - IDS Signatures
- **Advanced**—This panel consists of the six panels listed here, with the Fixup panel having further selections nested beneath it:
 - Fixup
 - Computer Telephony Interface Quick Buffer Encoding (CTIQBE)
 - Encapsulating Security Payload (ESP)-IKE
 - FTP
 - H.323 H225
 - H.323 Registration, Admission, and Status (RAS)
 - HTTP
 - ICMP Error

- Internet Locator Service (ILS)
- Media Gateway Control Protocol (MGCP)
- Point-to-Point Tunneling Protocol (PPTP)
- Remote shell (RSH)
- Real-Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP) over TCP
- SIP over UDP
- Skinny
- Simple Mail Transfer Protocol (SMTP)
- SQL*Net
- Anti-Spoofing
- Fragment
- TCP Options
- Timeout
- Turbo Access Rules
- **Multicast**—This panel consists of the three panels in the list that follows, with the Internet Group Management Protocol (IGMP) panel having further selections nested beneath it:
 - Stub Multicast Routing
 - IGMP
 - Protocol
 - Access Group
 - Join Group
 - MRoute
- **History Metrics**—This panel enables the PIX Firewall to keep a history of many statistics, which you can display with PDM through the Monitoring tab.

NOTE

If PDM History Metrics is not enabled, the only view available in the Monitoring tab is the “real-time” view. PDM History Metrics is enabled by default.

Tools and Options

You can use CLI commands and change some of the settings on the PDM using the Tools and Options menus.

Choosing **Options > Preferences > Preview Commands Before Sending** to PIX enables you to preview commands generated by any panel before they are sent to the PIX Firewall. This choice is useful when you use PDM as a learning tool or if you simply want to verify settings before they are applied to the firewall.

Select **Tools > Command Line Interface** to enter CLI commands to be sent to the PIX Firewall. This option allows you to use the CLI commands without the need for a separate Telnet session. If you need to send a quick CLI command, using this tool is a time-saver. You can also access the ping tool from the tools menu by selecting **Tool > Ping**.

Monitoring

You access the monitoring screen in Figure 6-14 by clicking the **Monitoring** button above the toolbar.

Figure 6-14 *Monitoring Screen*

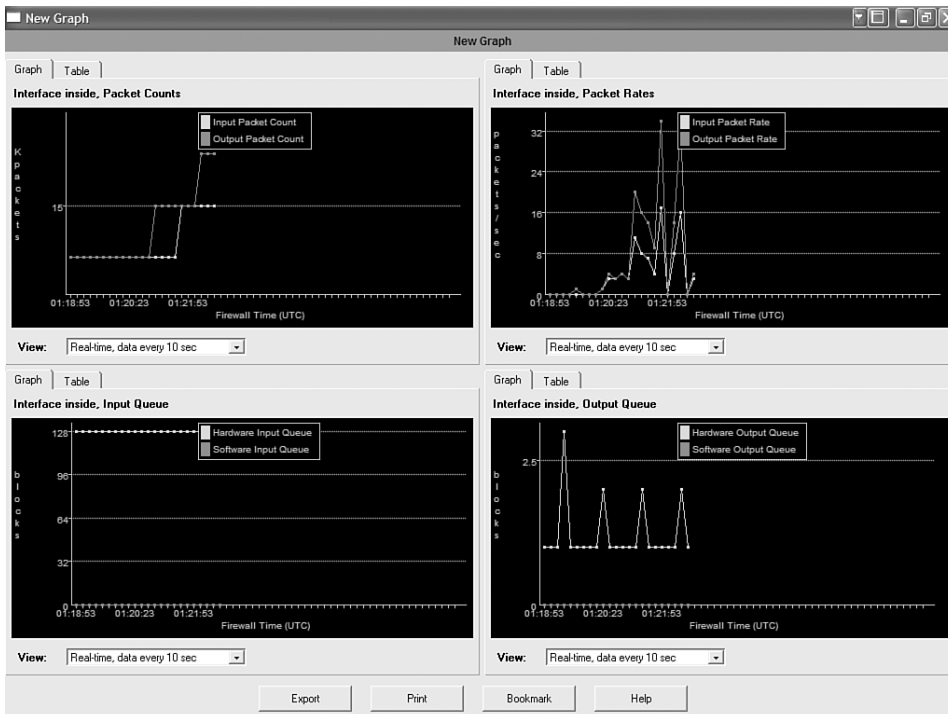


You can monitor many different items using PDM, including but not limited to the following:

- PDM Log
- PDM/HTTPS Sessions
- Secure Shell Sessions
- Telnet Console Settings
- PDM Users
- Number of Licenses in Use
- VPN Status, Statistics, and Connection Graphs
- System Performance Graphs
- Connection statistics
- Interface Graphs

The Interface Graphs panel enables you to monitor per-interface statistics, such as packet counts and bit rates, for each enabled interface on the PIX Firewall. You can select the interface and up to four variables for each graph. Figure 6-15 shows a graph for the inside interface displaying Packet Count, Packet Rate, Input Queue, and Output Queue.

Figure 6-15 *Interface Graph*



The list of graphs available is the same for every interface. You can view each graph as a line graph and in table form. You can also display each graph with different time horizons.

Summary

This section summarizes the information you learned in this chapter:

- PDM is a browser-based tool used to configure your PIX Firewall.
- To date, PDM 3.0 is the version of the tool with the greatest functionality and is suitable as the primary management and monitoring tool for many implementations.
- Minimal setup on the PIX Firewall is required to run PDM.
- PDM contains several tools in addition to the GUI to help configure your PIX Firewall.
- You can use PDM to create site-to-site and remote access VPNs.
- PDM is an excellent learning tool.

Chapter Review Questions

To test what you have learned in this chapter, answer the following questions and then refer to Appendix A, “Answers to Chapter Review Questions,” for the answers:

- 1 What version of the PDM is supported on PIX Firewall Version 6.3?
- 2 Can you use conduits and ACLs concurrently with PDM?
- 3 Which version of the PDM is supported on the FWSM?
- 4 What is the minimum recommended amount of RAM for a Windows client running PDM 3.0?
- 5 True or False: Configuration changes made by PDM are automatically saved to the PIX Firewall.

Lab Exercise—Configure the PIX Firewall with PDM

Complete the following lab exercises to practice the PDM concepts and configuration techniques you learned in this chapter. An initial configuration is not provided for this lab because you perform an initial configuration of the PIX Firewall using the PDM.

Objectives

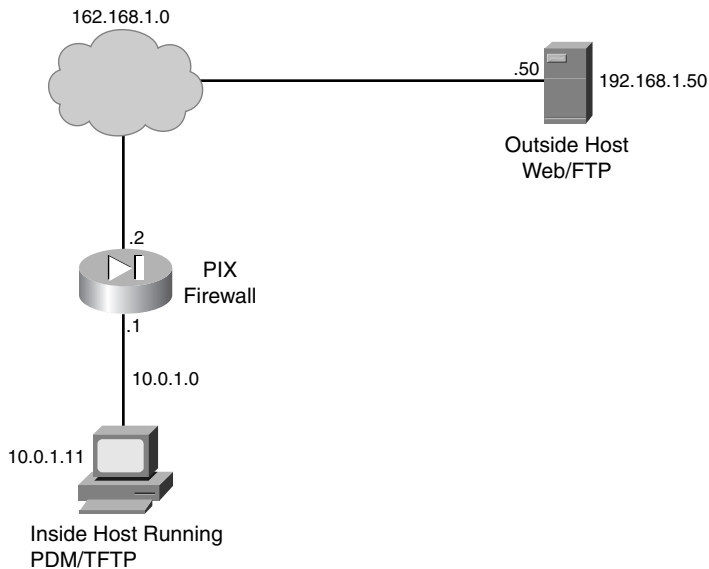
In this lab, you perform the following tasks:

- Clear the PIX Firewall's configuration and access the PDM Startup Wizard.
- Use the PDM Startup Wizard to configure a privileged mode password.
- Configure outbound access with NAT.
- Test connectivity through the PIX Firewall.
- Configure and test inbound access.
- Configure and test logging to a syslog server.
- Configure intrusion detection.
- Configure the PIX Firewall to monitor intrusion. Intrusion detection concepts are covered in detail in Chapter 12, "Attack Guards, Intrusion Detection, and Shunning."

Lab Topology

Figure 6-16 displays the topology for the lab exercises in this chapter.

Figure 6-16 *Topology for PDM Lab Exercises*



Equipment required to perform the lab includes the following:

- A PIX Firewall with two interfaces and PDM
- Category 5 patch cables

- PC host for outside subnet with web server and FTP server
- PC host for the inside subnet running TFTP and PDM

NOTE

In the following lab exercise, you bypass the initial security alert regarding the site security certificate. However, remember that when you remotely configure the PIX Firewall with PDM, you can use the security certificate for secure encrypted communication between PDM and the PIX Firewall. To do so, install the certificate by clicking **View Certificate** in the initial Security Alert window and following the prompts. Because the certificate is assigned to the PIX Firewall by name rather than by IP address, you should establish the connection with the PIX Firewall by entering its FQDN, rather than the IP address, in the browser. Using the name rather than an IP address requires that name resolution be enabled through DNS or a hosts file.

Task 1—Use the PDM Startup Wizard

The PIX Firewall used for these lab exercises should be loaded with PDM. If your PIX Firewall does not have PDM loaded on it, download the appropriate PDM image and install it on your firewall using the **copy tftp flash** command. For example, if you want to install an image file named `pdm-301.bin` located on a TFTP server at `10.0.1.11`, issue the following command:

```
copy tftp://10.0.1.11/pdm-301.bin flash:pdm
```

If the PIX Firewall you are using has been previously configured, complete the following steps to erase the current PIX Firewall configuration and access the PDM wizard:

Step 1 In the console window, erase the current PIX Firewall configuration. When prompted to confirm, press **Enter**:

```
pixfirewall(config)# write erase
Erase PIX configuration in flash memory? [confirm] <Enter>
```

Step 2 In the console window, reload the PIX Firewall. When prompted to confirm, press **Enter**.

```
pixfirewall(config)# reload
Proceed with reload? [confirm] <Enter>
```

Step 3 When prompted to preconfigure the PIX Firewall through interactive prompts, press **Enter**.

Step 4 Agree to use the current password by pressing **Enter**:

```
Enable password [<use current password>]: <Enter>
```

Step 5 Accept the default year by pressing **Enter**:

```
Clock (UTC):
Year [2003]: <Enter>
```


Step 6 Accept the default month by pressing **Enter**:

Month [Nov]: **<Enter>**

Step 7 Accept the default day by pressing **Enter**:

Day [14]: **<Enter>**

Step 8 Accept the default time stored in the host computer by pressing **Enter**:

Time [11:21:25]: **<Enter>**

Step 9 Enter the IP address of the PIX Firewall's inside interface:

Inside IP address: **10.0.1.1**

Step 10 Enter the network mask that applies to the inside IP address:

Inside network mask: **255.255.255.0**

Step 11 Enter the host name you want to display in the PIX Firewall command-line prompt:

Host name: **pixfirewall**

Step 12 Enter the DNS domain name of the network on which the PIX Firewall runs:

Domain name: **cisco.com**

Step 13 Enter the IP address of the host running PDM:

IP address of host running PIX Device Manager: **10.0.1.11**

Step 14 Enter **y** at the prompt to save the information to the PIX Firewall's Flash memory.

Step 15 Access the PDM console by completing the following substeps:

1. In the browser, enter **https://10.0.1.1**
2. In the Security Alert window, click **Yes**.
3. When prompted for the username and password, do not enter a username or password. Click **OK** to continue. The Security Warning window opens.
4. Click **Yes**. The Update Config window opens.
5. Click **Proceed**. If the Preview CLI Commands window opens, click **Send**. The PIX Device Manager main window opens.

Task 2—Use the PDM Startup Wizard to Configure a Privileged Mode Password

Complete the following steps to configure a privileged mode password:

- Step 1** In the PIX Device Manager Startup Wizard window, click **Next**. The Startup Wizard's Basic Configuration group box appears.
- Step 2** Verify that `pixfirewall` appears in the PIX Host Name field.
- Step 3** Verify that `cisco.com` appears in the Domain Name field.
- Step 4** Select **Change Enable Password** within the Enable Password group box.
- Step 5** Enter `cisco` in the New Enable Password text box.
- Step 6** Enter `cisco` in the Confirm New Enable Password text box.
- Step 7** Click **Finish**. The Enter Network Password window opens.
- Step 8** Leave the Username field blank, enter `cisco` in the password field, and click **OK**. The main Cisco PIX Device Manager window opens.

Task 3—Configure Outbound Access with NAT

Complete the following steps to configure the PIX Firewall inside and outside interfaces, establish a default route, enable NAT for the internal network, and create a global pool of addresses for address translation:

- Step 1** Select the **System Properties** tab.
- Step 2** Configure the inside interface by completing the following substeps:
 1. Select **ethernet1** in the Interfaces table and click the **Edit** button. The Edit Interface window opens.
 2. Verify that the Enable Interface check box is selected.
 3. Verify that `inside` appears in the Interface Name field.
 4. Verify that `10.0.1.1` appears in the IP Address field.
 5. Verify that `255.255.255.0` appears in the Subnet Mask drop-down menu.
 6. Choose **100full** from the Speed drop-down menu.
 7. Verify that `100` appears in the Security Level field.
 8. Click **OK**. You return to the Cisco PIX Device Manager main window.

Step 3 Configure the outside interface by completing the following substeps:

1. Select **ethernet0** in the Interfaces table, and then click the **Edit** button. The Edit Interface window opens.
2. Select the **Enable Interface** check box.
3. Verify that outside appears in the Interface Name field.
4. Verify that the Static IP Address radio button is selected within the IP Address group box.
5. Enter **192.168.1.2** in the IP Address field.
6. Choose **255.255.255.0** from the Subnet Mask drop-down menu.
7. Choose **100full** (10baset if using a PIX Firewall 501) from the Speed drop-down menu.
8. Verify that 0 appears in the Security Level field.
9. Click **OK**. You return to the Cisco PIX Device Manager main window.
10. Click **Apply**.

Step 4 Configure a global pool of addresses to be used for address translation by completing the following substeps:

1. Select the **Translation Rules** tab.
2. Click the **Manage Pools** button. The Manage Global Address Pools window opens.
3. Click **Add**. The Add Global Pool Item window opens.
4. Choose outside from the Interface drop-down menu.
5. Enter **1** in the Pool ID field.
6. Verify that the Range radio button is selected.
7. Enter **192.168.1.20** in the first IP address field.
8. Enter **192.168.1.40** in the second IP address field.
9. Enter **255.255.255.0** in the Network Mask field.
10. Click **OK**. You return to the Manage Global Address Pools window.
11. Click **OK**. You return to the Cisco PIX Device Manager main window.
12. Click **Apply**.

Step 5 Configure NAT by completing the following substeps:

1. Verify that the Translation Rules tab is still active.
2. Verify that the Translation Rules radio button is selected.
3. Choose **Rules > Add** from the main menu. The Add Address Translation Rule window opens.
4. Verify that the inside interface is chosen in the Interface drop-down menu.
5. Click **Browse**. The Select host/network window opens.
6. Verify that the inside interface is chosen in the drop-down menu.
7. Select the inside network by clicking **10.0.1.0**.
8. Click **OK**. You return to the Add Address Translation Rule window.
9. Verify that outside is chosen in the Translate Address on Interface drop-down menu.
10. Verify that Dynamic is selected in the Translate Address to group box.
11. Choose **1** from the Address Pool drop-down menu.
12. Verify that the global pool you configured earlier (192.168.1.20–192.168.1.40) appears under Address.
13. Click **OK** in the Add Address Translation Rule window. The new rule appears on the Translation Rules tab.
14. Click **Apply**.

Task 4—Test Connectivity Through the PIX Firewall

Complete the following steps to test interface connectivity and NAT:

Step 1 Test interface connectivity by completing the following substeps:

1. Choose **Tools > Ping**.
2. In the IP Address field, enter **10.0.1.1**.
Click **Ping**.

3. Observe the output in the Ping Output window. The output should appear similar to the following:

```
10.0.1.1 response received -- 0ms
10.0.1.1 response received -- 0ms
10.0.1.1 response received -- 0ms
```

4. Click **Clear Screen**.

Step 2 Repeat Step 1 for the following IP addresses. You should receive responses for all pings:

- The inside host: 10.0.1.11
- The outside interface: 192.168.1.2

Step 3 Exit the Ping window by clicking **Close**.

Test the operation of the global and NAT you configured by originating connections through the PIX Firewall. To do so, open a web browser on the inside host and access the outside host at IP address 192.168.1.50 by entering **http://192.168.1.50**.

Step 4 Observe the translation table by completing the following substeps:

1. Choose **Tools > Command Line Interface**. The Command Line Interface window opens.
2. In the Command field, enter **show xlate**.
3. Click **Send**.
4. Observe the output in the Response field. It should appear similar to the following:

```
Result of the PIX command: "show xlate"
1 in use, 1 most used
Global 192.168.1.20 Local 10.0.1.11
```

NOTE

Note that a global address chosen from the low end of the global range has been mapped to the inside host.

Step 5 Exit the Command Line Interface window by clicking **Close**.

Task 5—Configure and Test Inbound Access

Complete the following steps to configure the PIX Firewall to permit inbound access to hosts on the inside interface:

Step 1 Enable command preview by completing the following substeps:

1. Choose **Options > Preferences** from the main menu. The Preferences window opens.
2. Select **Preview Commands Before Sending to Firewall**.
3. Click **OK**.

Step 2 Create a static translation for the inside host by completing the following substeps:

1. Select the **Translation Rules** tab.
2. Select the **Add New Rule** icon in the toolbar. The Add Address Translation Rule window opens.
3. Verify that the inside interface is chosen in the Interface drop-down menu.
4. Click **Browse**. The Select Host/Network window opens.
5. Verify that the inside interface is chosen in the drop-down menu.
6. Select the inside host: Click **10.0.1.11**.
7. Click **OK**. You are returned to the Add Address Translation Rule window.
8. Verify that outside is chosen in the Translate Address on Interface drop-down menu.
9. Select **Static** in the Translate Address to group box.
10. Enter **192.168.1.10** in the IP Address field.
11. Click **OK**. The new rule appears on the Translation Rules tab.
12. Click **Apply**. The Preview CLI Commands window opens.
13. Click **Send**.

Step 3 Ping the inside host from the outside host. The ping should fail because the policy presently prevents pinging:

```
C:\> ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Step 4 Configure an ACL to allow ping through the PIX Firewall by completing the following substeps:

1. Select the **Access Rules** tab.
2. Choose **Rules** from the main menu.
3. Click **Add**. The Add Rule window opens.
4. Verify that **permit** is chosen in the Select an action drop-down menu.
5. Choose **outside** from the Interface drop-down menu in the Source Host/Network group box.
6. Choose **inside** from the Interface drop-down menu in the Destination Host/Network group box.
7. Select **ICMP** in the Protocol or Service group box.
8. Verify that **any** is selected in the ICMP type group box.
9. Click **OK**. The new rule appears on the Access Rules tab.
10. Click **Apply**. The Preview CLI Commands window opens.
11. Observe the ACLs to be sent to the PIX Firewall.
12. Click **Send**.

Step 5 Ping the inside host again from the outside host:

```
C:\> ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.1.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.1.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.1.10: bytes=32 time<10ms TTL=125>
```

Step 6 Configure an ACL to allow Web access to the inside host from the outside by completing the following substeps:

1. Select the **Access Rules** tab.
2. Choose **Rules > Add**. The Add Rule window opens.

3. Verify that permit is chosen in the Select an Action drop-down menu.
4. Choose outside from the Interface drop-down menu within the Source Host/Network group box.
5. Choose inside from the Interface drop-down menu within the Destination Host/Network group box.
6. Click **Browse** in the Destination Host/Network group box. The Select Host/Network window opens.
7. Verify that inside is chosen in the Interface drop-down menu.
8. Select the IP address of the inside host: **10.0.1.11**.
9. Click **OK**. The Add Rule window becomes active.
10. Select **TCP** in the Protocol and Service group box.
11. Verify that = is chosen in the Service drop-down menu within the Source Port group box.
12. Verify that **any** appears in the Service field within the Source Port group box.
13. Verify that = is chosen in the Service drop-down menu within the Destination Port group box.
14. Click the **Ellipsis** button within the Destination Port group box. The Service window opens.
15. Choose **http** from the Service list.
16. Click **OK**. You return to the Add Rule window.
17. Click **OK**.
18. Click **Apply**. The Preview CLI Commands window opens.
19. Observe the ACLs to be sent to the PIX Firewall.
20. Click **Send**.

Step 7 Clear current translations by completing the following substeps:

1. Choose **Tools > Command Line Interface**. The Command Line Interface window opens.
2. Enter **clear xlate** in the Command field.
3. Click **Send**.

4. Verify that the output in the Response field is similar to the following:

```
Result of firewall command: "clear xlate"  
The command has been sent to the firewall.
```

Step 8 View current translations by completing the following substeps:

1. Click **Clear Response** in the Command Line Interface window.
2. Enter **show xlate** in the Command field.
3. Click **Send**.
4. Verify that the output in the Response field is similar to the following:

```
Result of firewall command: "show xlate"  
0 in use, 3 most used
```

5. Click **Close** in the Command Line Interface window.
6. Test web access to the inside host by opening a web browser on the outside host and entering **http://192.168.1.10**. You should be able to establish a web connection to the inside host if the ACL has been correctly configured.

Test FTP access to the inside host from the outside host by choosing **Start > Run > ftp 192.168.1.10**. You should be unable to access FTP.

Step 9 Observe the transactions by completing the following substeps:

1. Choose **Tools > Command Line Interface**. The Command Line Interface window opens.
2. Enter **show arp** in the Command field.
3. Click **Send**.
4. Verify that the output in the Response box is similar to the following:

```
result of firewall command: "show arp"  
outside 192.168.1.50 0003.6ba4.ca60  
inside 10.0.1.11 0050.da31.6130
```

5. Click **Clear Response**.
6. Enter **show conn** in the Command field.
7. Click **Send**.

8. Verify that the output in the Response field is similar to the following:

```
result of firewall command: "show conn"  
0 in use, 6 most used  
TCP out 192.168.1.10:80 in 10.0.1.11: 3893 idle 0:00:07 Bytes  
463 flags UIO  
TCP out 192.168.1.10:80 in 10.0.1.11: 3893 idle 0:00:07 Bytes  
463 flags UIO
```

9. Click **Clear Response**.
10. Enter **show xlate** in the Command field.
11. Click **Send**.
12. Verify that the output in the Response field is similar to the following:

```
result of firewall command: "show xlate"  
2 in use, 3 most used  
Global 192.168.1.10 Local 10.0.1.11
```

13. Click **Close**.

Task 6—Configure Intrusion Detection

Chapter 12 covers the intrusion detection features of the PIX Firewall in greater detail. It also includes CLI-based lab exercises for configuring and monitoring intrusion detection, which you can compare and contrast to this PDM-based exercise. Complete the following steps to configure the PIX Firewall to detect ICMP packet attacks, drop the packets, and send an alarm to a syslog server:

- Step 1** Verify that the System Properties tab is still active.
- Step 2** Expand Intrusion Detection from the Categories tree on the left of the panel. IDS Policy appears under Intrusion Detection.
- Step 3** Select **IDS Policy**. The IDS Policy group box opens on the right.
- Step 4** Click **Add**. The Add IDS Policy window opens.
- Step 5** Enter **ATTACKPOLICY** in the Policy Name field.
- Step 6** Verify that **Attack** is selected in the Policy Type group box.
- Step 7** Select **Drop and Alarm** in the Action group box.
- Step 8** Click **OK**. You return to the System Properties tab.
- Step 9** Choose **ATTACKPOLICY** from the drop-down menu for the inside interface under Attack Policy.

Step 10 Click **Apply**. The Preview CLI Commands window opens.

Step 11 Click **Send**.

Task 7—Configure PDM to Monitor Intrusion Detection

Complete the following steps to configure monitoring of intrusion detection:

Step 1 Select the **Monitoring** tab.

Step 2 Expand Miscellaneous Graphs from the Categories tree on the left of the panel. IDS appears under Miscellaneous Graphs.

Step 3 Select **IDS**.

Step 4 Choose **ICMP Attacks** from the Available Graphs for: list.

Step 5 Click **Add**.

Step 6 Click **Graph It**. The New Graph window opens.

Step 7 Verify that Real-time, data every 10 sec is chosen in the View drop-down menu.

Step 8 From the Windows command line, ping the PIX Firewall's inside interface with an ICMP packet size of 10,000:

```
C:\> ping -l 10000 10.0.1.1
Pinging 10.0.1.1 with 10000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Step 9 From the Windows command line, ping the PIX Firewall's inside interface with an increased ICMP packet size:

```
C:\> ping -l 65000 10.0.1.1
Pinging 10.0.1.1 with 65000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Step 10 Observe the graph in the Graph tab.

- Step 11** Select the **Table** tab and observe the statistics in the table view.
- Step 12** Save the PIX Firewall configuration to Flash memory by clicking the **Save Running Configuration to Flash** icon in the PDM toolbar. The Save Running Configuration to Flash window opens.
- Step 13** Click **Apply**. The Preview CLI Commands window opens.
- Step 14** Click **Send**. The Save Successful window opens.
- Step 15** Click **OK**.