



Set Up Your PIX Security Appliance

[Home](#) > [Work With My Security Devices](#) > [Cisco Security Appliances](#) > [Set Up Your PIX Security Appliance](#)

Service Requests

[Open a service request](#)

[Update a service request](#)

Step 2: Hardware Setup Procedure for the PIX Security Appliance

Step 1: [SMB Support Assistant Site Survey](#)

Step 2: Set Up Your PIX Security Appliance Hardware

[Introduction](#)

[Requirements](#)

[Install the PIX](#)

[Connect the Cables](#)

[Connect the Power](#)

[Next Step](#)

[Troubleshoot the Procedure](#)

[Related Information](#)

Step 3: [Prepare to Configure Your PIX Security Appliance](#)

Step 4: [Configure Your PIX Security Appliance with PIX Device Manager](#)

Step 5: [Set Up Internet Security on the PIX Security Appliance](#)

Download PDF



[Step 2: Hardware Setup Procedure for the PIX Security Appliance](#)



[Set Up Your PIX Security Appliance](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

Introduction

This document describes how to install your Cisco PIX 515E or 506E Security Appliance and connect the power supply module.

[Back to Top](#)

Requirements

To perform the steps described in this document, you need to have these items:

- PIX 515E or 506E device
- Two [straight-through Ethernet cables](#)
- External AC-to-DC power supply module (506E)
- AC power cord
- Rubber feet

[Back to Top](#)

Install the PIX

This section describes how to set up your PIX and connect the power.

Connect the Cables

Complete these steps to install your PIX:

1. Affix the rubber feet to the bottom of the PIX.
2. Place the PIX on a flat, stable surface. The PIX 506E is not rack mountable.

3. Connect one end of the Ethernet cable to the outside PIX Ethernet interface—Ethernet 0. Connect the other end of this Ethernet cable to a DSL modem, cable modem, or router.

For more information on cables, refer to [Cable Descriptions](#).

4. Connect one end of the other Ethernet cable to the inside PIX Ethernet interface—Ethernet 1. Connect the other end of this Ethernet cable to a switch or hub.

The Ethernet cables connect your PIX to the Internet and to your computer.

Connect the Power

Complete the steps in this section to connect the power to your PIX. Use this information in conjunction with the document that shipped with your unit.

1. The power cord for the PIX 506E has two parts. Connect the AC power cord to the power supply module. Then, connect the power supply module to the rear panel 8-pin connector of the PIX. On the 516E connect the power cord to the back of the PIX.
2. Connect the AC power cord to your AC power receptacle.
3. Press the toggle switch located directly above the power cord to the on position. This step is successful when the Power LED light on the back of the unit turns green.

[Back to Top](#)

Next Step

You have completed the installation process of the PIX Security Appliance.

Proceed to [Prepare to Configure Your PIX Security Appliance](#) to configure the PIX.

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter. If this information does not solve your problem, contact the [SMB Technical Assistance Center \(SMB TAC\)](#) for assistance.

Problem	Cause(s) and Suggested Solution(s)
The ACT LED is off.	If the LINK/ACT LED does not light up, you might have used the wrong type of cable. Ensure that you use a straight-through Ethernet cable. Refer to Cable Descriptions for more information.
The PIX unit shut down after being on a short time.	Check the fans. If the fans are not working, the PIX Security Appliance will overheat and shut itself down. Contact the SMB TAC for support. Ensure that the chassis intake and exhaust vents are clear.

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Cable Descriptions](#)
- [Prepare to Configure Your PIX Security Appliance](#)
- [Configure the PIX Security Appliance With PIX Device Manager](#)



Set Up Your PIX Security Appliance

Home > [Work With My Security Devices](#) > [Cisco Security Appliances](#) > Set Up Your PIX Security Appliance

Service Requests

[Open a service request](#)

[Update a service request](#)

Step 3: Prepare to Configure Your PIX Security Appliance

Step 1: [SMB Support Assistant Site Survey](#)

Step 2: [Set Up Your PIX Security Appliance Hardware](#)

Step 3: Prepare to Configure Your PIX Security Appliance

[Introduction](#)

[Requirements](#)

[Configure Your Ethernet Interface](#)

[Next Step](#)

[Related Information](#)

Step 4: [Configure Your PIX Security Appliance with PIX Device Manager](#)

Step 5: [Set Up Internet Security on the PIX Security Appliance](#)

Download PDF

[Step 3: Prepare to Configure Your PIX Security Appliance](#)

[Set Up Your PIX Security Appliance](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Introduction

This document explains how to prepare to configure your PIX Security Appliance with PIX Device Manager (PDM).

[Back to Top](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:
Email:

Requirements

To perform the steps described in this document, you need to have these items:

- A [console cable](#)
- A PIX that has been installed and powered on
- Completed worksheets as instructed in the [Site Survey](#):

- o Remote Networking Assignments worksheet
- o LAN Addressing Worksheet

[Back to Top](#)

Configure Your Ethernet Interface

Before you access PDM, follow these steps to configure the Ethernet interface on your PIX:

1. Consult your Remote Networking Assignments worksheet to locate the IP address you entered on line R12.
2. Create a HyperTerminal connection to your PIX. For more information, refer to [Create a HyperTerminal Connection](#).
3. Log in to the PIX. The default login is username **cisco**, password **cisco**.
4. Type **enable** and press **Enter** to use privileged mode.

```
pixfirewall> enable
Password:
pixfirewall#
```

5. Type **configure terminal** and press **Enter** to use configuration mode.

```
pixfirewall# configure terminal
Enter configuration commands, one per line.
pixfirewall(config)#
```

6. Type **show ip** and press **Enter** to determine the IP address of the PIX.

```
pixfirewall(config-if)# show ip
System IP Addresses:
    ip address outside 164.120.40.182 255.255.255.128
    ip address inside 192.168.1.1 255.255.255.0
Current IP Addresses:
    ip address outside 164.120.40.182 255.255.255.128
    ip address outside 164.120.40.182 255.255.255.128
```

7. Before you can change the IP address, you must remove the IP addresses for the DHCP pool. Type **no**

dhcp address 192.168.1.2-192.168.1.254 inside.

```
pixfirewall(config-if)# no dhcp address 192.168.1.2-192.168.1.254 inside
```

8. Type **ip address *ip address subnet mask* inside**. Use the IP address from the Remote Networking Assignments worksheet (field R12) and the subnet mask from the LAN Addressing Worksheet (field L2A). Press **Enter**.

```
pixfirewall(config-if)# ip address inside 192.168.10.1 255.255.255.0
```

9. Type **http *ip address subnet mask* inside** with the same IP address. Press **Enter**.

```
pixfirewall(config-if)# http 192.168.10.1 255.255.255.0 inside
```

10. Type **write memory** and press **Enter** to save the configuration.

```
pixfirewall(config-if)# write memory
```

11. Type **quit** and press **Enter** to exit configuration mode.

```
pixfirewall(config-if)# quit  
pixfirewall>
```

[Back to Top](#)

Next Step

Your PIX Security Appliance is now ready to run the PDM.

To configure your PIX with PDM, refer to [Configure the PIX Security Appliance With PIX Device Manager](#).

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Cable Descriptions](#)
- [Configure an IP Address on Your PC](#)
- [Create a HyperTerminal Connection](#)
- [Configure the PIX Security Appliance With PIX Device Manager](#)

© 1992-2005 Cisco Systems, Inc. All rights reserved. [Terms and Conditions](#), [Privacy Statement](#), [Cookie Policy](#) and [Trademarks](#) of Cisco Systems, Inc.



Set Up Your PIX Security Appliance

Home > Work With My Security Devices > Cisco Security Appliances > Set Up Your PIX Security Appliance

Step 4: Configure the PIX Security Appliance with PIX Device Manager

Step 1: [SMB Support Assistant Site Survey](#)

Step 2: [Set Up Your PIX Security Appliance Hardware](#)

Step 3: [Prepare to Configure Your PIX Security Appliance](#)

Step 4: Configure Your PIX Security Appliance with PIX Device Manager

[Introduction](#)

[Requirements](#)

[Connect to the PIX](#)

[Configure the PIX with the Startup Wizard](#)

[Basic Configuration](#)

[Outside Interface Configuration](#)

[Easy VPN Remote Configuration](#)

[Auto Update Configuration](#)

[Other Interfaces Configuration](#)

[NAT and PAT Configuration](#)

[DHCP Server Configuration](#)

[Create an Administrative Account](#)

[Next Step](#)

[Troubleshoot the Procedure](#)

[Related Information](#)

Step 5: [Set Up Internet Security on the PIX Security Appliance](#)

Introduction

This document describes how to use the Startup Wizard to configure the PIX Security Appliance.

[Back to Top](#)

Requirements

This section lists the items you need to use the PIX Device Manager (PDM) to access and configure your PIX:

Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Download PDF

- [Step 4: Configure the PIX Security Appliance with PIX Device Manager](#)
- [Set Up Your PIX Security Appliance](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

- Ensure that your PIX 506E/515E is connected properly to your PC. If you have not installed your PIX hardware, refer to [Hardware Setup Procedure for the PIX Security Appliance](#) for instructions.
- A [straight-through Ethernet cable](#).
- A Completed [Site Survey](#)
 - Completed Remote Networking Assignments worksheet
 - Completed Internet Worksheet
 - Completed Firewall Worksheet
 - Completed LAN Addressing Worksheet
- One of these web browsers:
 - Netscape version 7.1 or later
 - Internet Explorer version 5.5 or later
- Ensure that JavaScript and Java are enabled in your web browser and are the correct version. For more information on how to check this see [Enable Java and JavaScript on Your PC](#).

[Back to Top](#)

Connect to the PIX

The PIX 506E/515E contains the integrated utility PDM. PDM is a browser-based tool designed to help you set up, configure, and monitor the PIX Security Appliance. The PDM is preinstalled on the PIX 506E/515E.

Complete these steps to access the PIX with PDM:

1. If you have not already done so, use an Ethernet cable to connect your PC to the inside port (Ethernet 1) on the rear panel of the PIX Security Appliance.
2. Configure your computer to use DHCP (to receive an IP address automatically from the PIX firewall).
3. Check the ACT LED on the PIX front panel to verify that your PC has basic connectivity to the inside port—Ethernet 1. When connectivity occurs, the ACT LED on the front of the PIX lights up solid green.
4. Open a browser window and type **https:// <pix_interface_ip_address>** in your browser address field. This new IP address is found on line R12 of the Remote Networking Assignments worksheet.

Note: Ensure that you add the "s" to "https" or the web browser cannot connect. HTTPS (HTTP over SSL) provides a

secure connection between your browser and the PIX Security Appliance.

5. Leave both the user name and password boxes empty and press **Enter**.
6. Accept the security certificates.

To avoid the certificate from appearing in Windows Internet Explorer when the certificate dialog (titled "**Security Alert**") is shown, perform the following steps:

- a. Click **View Certificate**.
 - b. Click **Install Certificate**.
 - c. Click **next > next > Finish > Yes**.
 - d. Click **OK** in the certificate dialog box.
 - e. In the Security Alert dialog box, click **Yes**.
7. The next logon screen appears. No password has been set, click **OK** to continue.
 8. Answer **Always** to the Security Warning asking "Do you want to install and run `Cisco PIX Device Manager`" PDM starts after the certificates are accepted.

[Back to Top](#)

Configure the PIX with the Startup Wizard

The Startup Wizard starts immediately the first time you connect to the PDM. You can access the Startup Wizard at any time using the Wizards menu. The Wizard can be aborted at any time by clicking Cancel. This will preserve your original PIX settings. The Back button allows you to go back and change the information on previous screens before you click Finish. The following panels will take you step by step through the initial setup of the PIX firewall.

Basic Configuration

On the Basic Configuration panel, you configure the host name of your firewall and set the Enable Password, as well as a domain name for the firewall.

Follow these steps for the basic configuration panel:

1. Enter the Host Name from your Internet Worksheet line B63. The PIX Host Name can be up to 63 alphanumeric characters of mixed case.

Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard

Startup Wizard

Basic Configuration

Please specify the host name for the PIX. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to enter the device name given to you by your ISP as your firewall Host Name.

PIX Host Name:

Domain Name:

Enable Password

The Enable Password is used to administer the firewall by PDM or the Command Line Interface (CLI).

(Change Enable Password):

Old Enable Password:

New Enable Password:

Confirm New Enable Password:

< Back Next > Finish Cancel Help

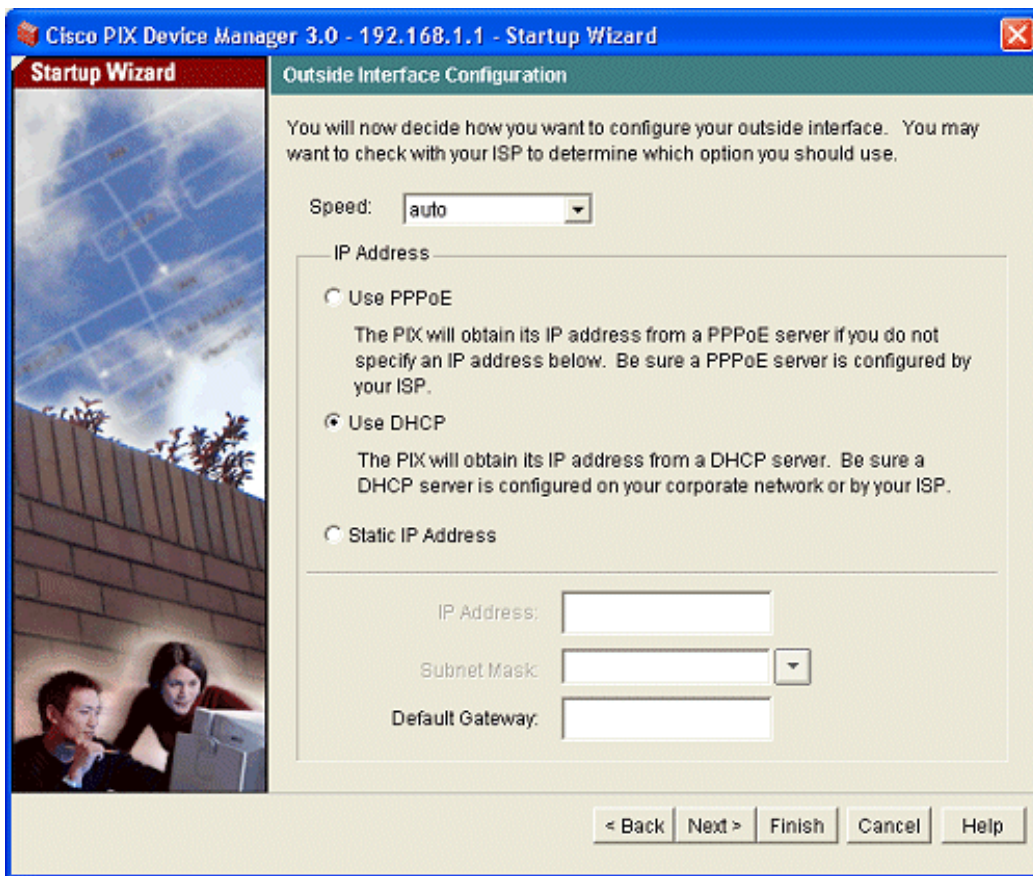
2. Enter the domain name the of the PIX Firewall found on line B48 of the Internet Worksheet. There is a 64 alphanumeric character limit on the domain name. No special characters or spaces may be used.
3. Check the box Change Enable Password.
4. Leave the Old Enable Password field blank. Enter the New Enable password. The password is case-sensitive and up to 16 alphanumeric characters. This password is found on line B12 of the Internet Worksheet.
5. Enter the password a second time in the Confirm New Enable Password box.
6. Click **Next**.

Outside Interface Configuration

On the Outside Interface Configuration panel you configure the outside interface IP address, subnet mask, and default gateway.

Follow these steps to configure the outside interface:

1. Speed—Leave the speed set to auto.

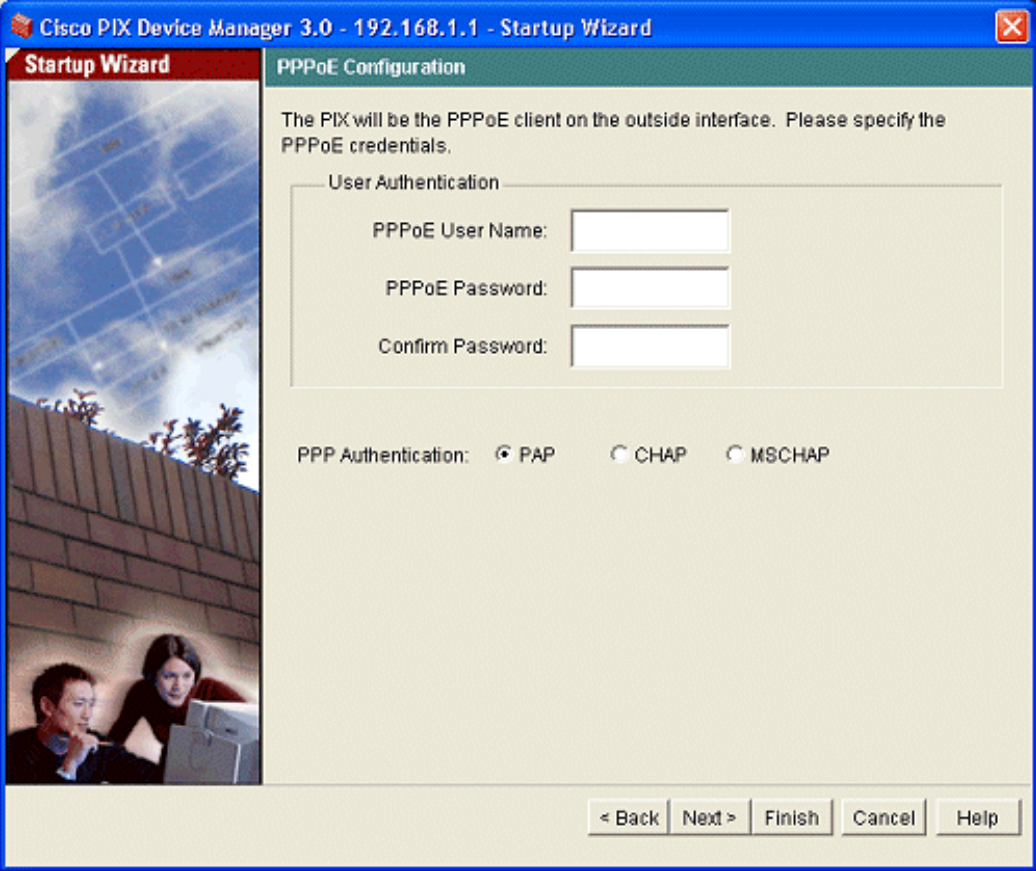


2. To configure the outside interface IP address consult lines B45 and B46 on the Internet Worksheet.

Use only one of the following procedures:

- If you selected DHCP on the Internet Worksheet:
 - Click **Use DHCP**.
 - Click **Next**.
- If you selected Static IP on the Internet Worksheet:
 - Click **Static IP Address**.
 - Enter the IP address from line B46.
 - Enter the subnet mask found on line B41.
 - Enter the gateway IP address found on line B47.
 - Click **Next**.

- If you selected Static PPP on the Internet Worksheet:
 - Click **Use PPPoE**. The PPPoE Configuration screen will appear:
 - Enter the User Name (Remote Host Name) from line B63 of the Internet worksheet.
 - Enter the PPPoE password (Shared Secret) from line B64 of the Internet worksheet.
 - Enter the password again in the Confirm password box.
 - Click the PPP authentication you chose from line B62 of the Internet Worksheet.
 - Click Next.



The screenshot shows the 'Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard' window. The title bar includes the Cisco logo and window controls. The main window is divided into two panes. The left pane, titled 'Startup Wizard', shows a background image of a network diagram and two people working at a computer. The right pane, titled 'PPPoE Configuration', contains the following text: 'The PIX will be the PPPoE client on the outside interface. Please specify the PPPoE credentials.' Below this is a 'User Authentication' section with three input fields: 'PPPoE User Name:', 'PPPoE Password:', and 'Confirm Password:'. At the bottom of the right pane, there is a 'PPP Authentication:' section with three radio buttons: 'PAP' (selected), 'CHAP', and 'MSCHAP'. At the very bottom of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Easy VPN Remote Configuration

On the Easy VPN Remote Configuration screen, follow these steps:

1. Ensure the box Enable Easy VPN Remote is **not** checked.

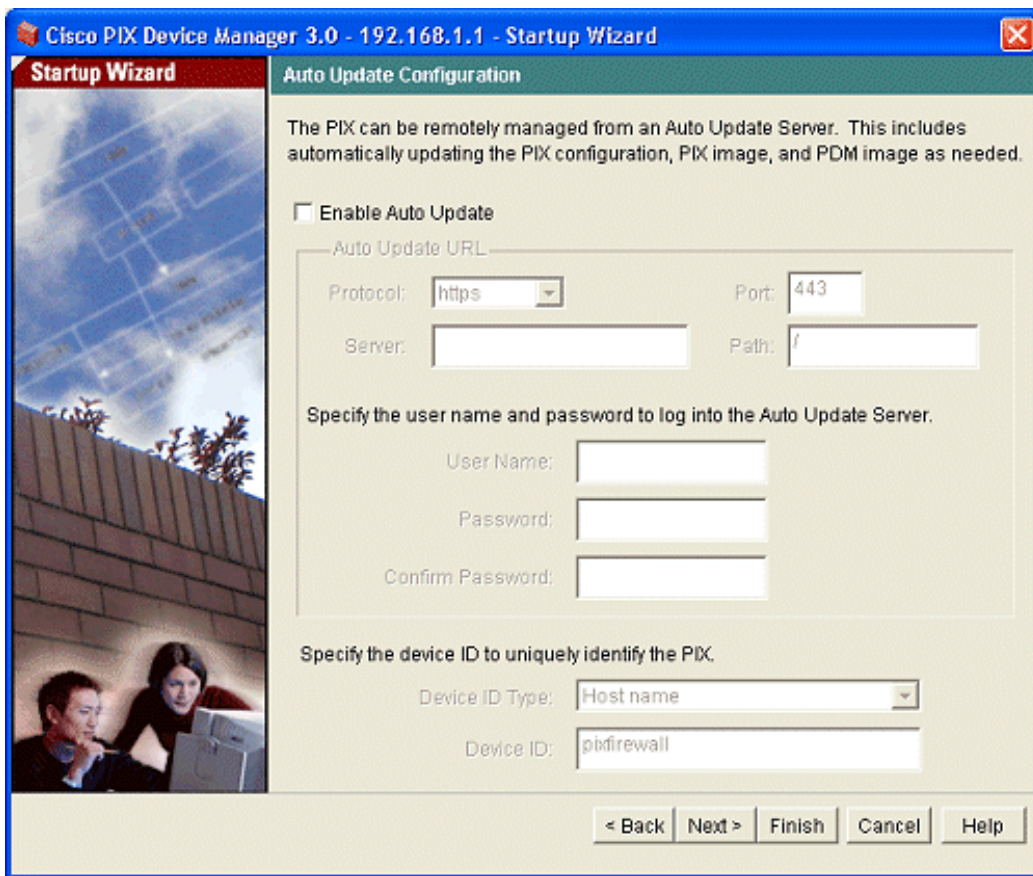
The screenshot shows the 'Easy VPN Remote Configuration' screen in the Cisco PIX Device Manager 3.0 Startup Wizard. The window title is 'Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard'. The left sidebar contains a 'Startup Wizard' tab and a background image of a network diagram. The main content area has a green header with the title 'Easy VPN Remote Configuration'. Below the header is a paragraph explaining that the PIX can act as an Easy VPN Remote device. A checkbox labeled 'Enable Easy VPN Remote' is present and is currently unchecked. Below this is a 'Mode' section with a text box explaining that 'Client Mode' should be selected for DHCP servers and 'Network Extension Mode' for static IP addresses. Two radio buttons are shown: 'Client Mode' (selected) and 'Network Extension Mode'. Below the mode section are two main options: 'Use Group Password' (unchecked) and 'Use X.509 Certificate' (checked). The 'Use Group Password' option includes fields for 'Group Name', 'Group Password', 'Confirm Password', 'Primary EasyVPN Server', 'Secondary EasyVPN Server', 'User Name', and 'User Password'. The 'Use X.509 Certificate' option includes a 'Confirm Password' field. At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

2. Click **Next**.

Auto Update Configuration

On the Auto Update Configuration screen, follow these steps:

1. Ensure the box Enable Auto Update is **not** checked.



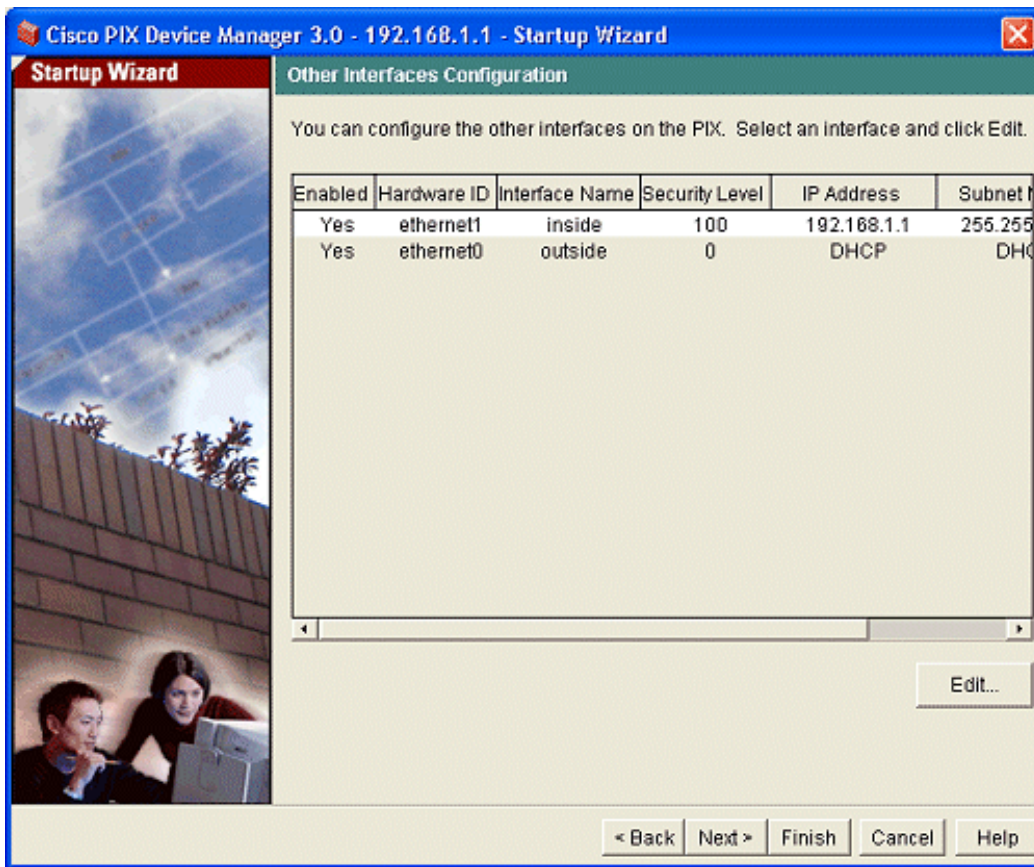
The screenshot shows the 'Auto Update Configuration' window in Cisco PIX Device Manager 3.0. The window title is 'Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard'. The left sidebar is labeled 'Startup Wizard' and features a background image of a network diagram and two people working at a computer. The main content area has a green header 'Auto Update Configuration' and a descriptive paragraph: 'The PIX can be remotely managed from an Auto Update Server. This includes automatically updating the PIX configuration, PIX image, and PDM image as needed.' Below this is a checkbox for 'Enable Auto Update' which is currently unchecked. Underneath is the 'Auto Update URL' section with fields for Protocol (set to 'https'), Port (set to '443'), Server, and Path (set to '/'). The next section is 'Specify the user name and password to log into the Auto Update Server.' with fields for User Name, Password, and Confirm Password. The final section is 'Specify the device ID to uniquely identify the PIX.' with a dropdown for Device ID Type (set to 'Host name') and a text field for Device ID (set to 'pixfirewall'). At the bottom are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

2. Click **Next**.

Other Interfaces Configuration

The Other Interfaces Configuration panel lets you configure the IP addresses of the inside interface on the firewall. PDM automatically lists the interfaces available for configuration, and in this panel you can set the IP address, speed, interface name, and security level to make each inside interface unique.

To configure the internal interfaces follow these steps:



1. Highlight the preferred inside interface and click **Edit**.

Another panel will appear with the highlighted information.

Edit Interface

Hardware ID: **ethernet1**

Enable Interface Speed: auto

Interface Name: inside Security Level: 100

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

OK Cancel Help

- a. Ensure that the Enable Interface box is checked.
- b. Ensure the speed is set to Auto.
- c. Set the Security Level to 100.
- d. Click **OK**.

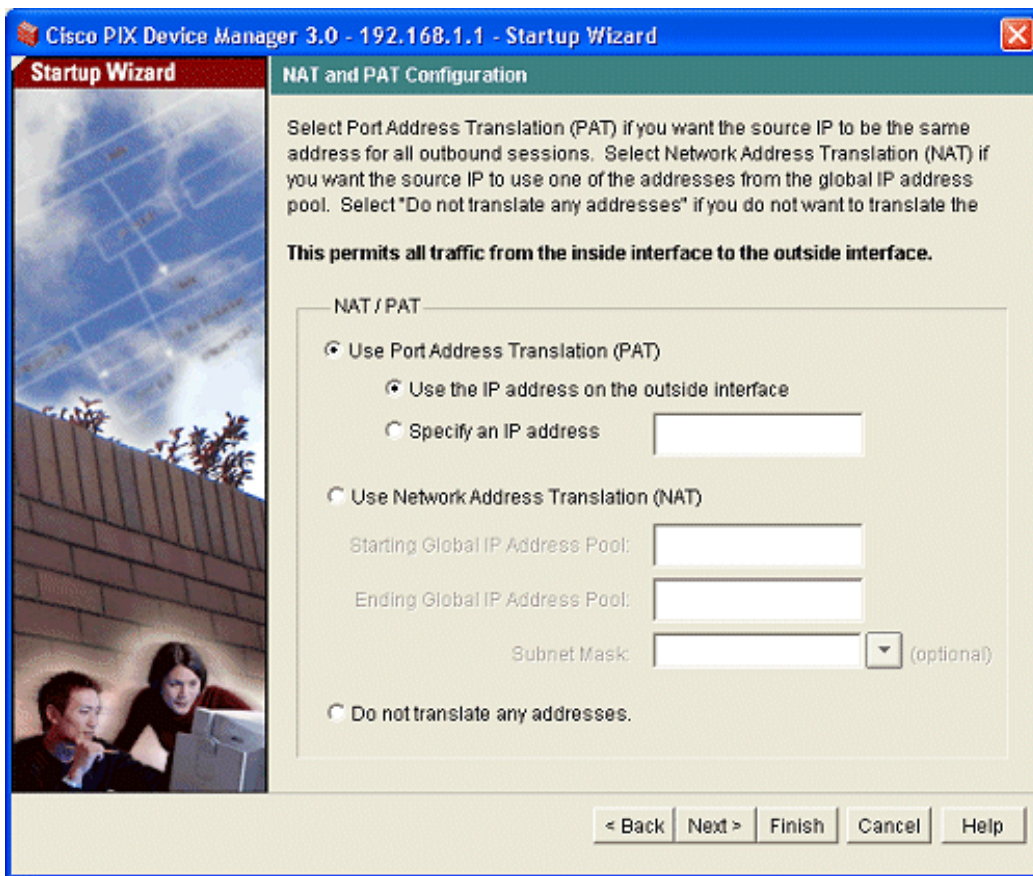
2. Click **Next**.

NAT and PAT Configuration

On the NAT and PAT Configuration panel you configure Port Address Translation (PAT) to protect your network.

Follow these steps to configure PAT Configuration:

1. Select **Use Port Address Translation**.



2. Click **Use the IP address on the outside interface.**
3. Click **Next.**

DHCP Server Configuration

The DHCP Server Configuration panel lets you configure the firewall as a DHCP server to clients on the inside interface. Here you can configure a range of IP addresses in the address pool to be assigned to those clients upon request.

If line L3 on the LAN Addressing Worksheet is your PIX firewall the DHCP server needs to be enabled. If not skip this step and click Next.

Follow these steps to configure the DHCP server:

1. Check **Enable DHCP on inside interface.**

Cisco PIX Device Manager 3.0 - 192.168.1.1 - Startup Wizard

Startup Wizard

DHCP Server Configuration

The PIX can be a DHCP server and provide IP addresses to the hosts on your inside network. To configure the DHCP server on another interface besides the inside interface, please use the PDM application.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.10.50

Ending IP Address: 192.168.10.250

DHCP Parameters

DNS Server 1: 198.6.1.1 WINS Server 1: []

DNS Server 2: 198.5.1.1 WINS Server 2: []

Domain Name: company.com Lease Length: 3600 secs

< Back Next > Finish Cancel Help

2. Under DHCP Address Pool:

- a. Enter the starting range of the DHCP server pool from line L50A on the LAN Addressing Worksheet.
- b. Enter the ending range of the DHCP server pool from line L51A on the LAN Addressing Worksheet.

3. Under DHCP Parameters:

- a. Enter the IP address of the DNS server from line L4A on the LAN Addressing Worksheet.
- b. Enter the IP address of the alternate DNS server from line L5A on the LAN Addressing Worksheet.
- c. Enter the domain name of the DNS server from line B48 of the Internet Worksheet.

4. Click **Next**.

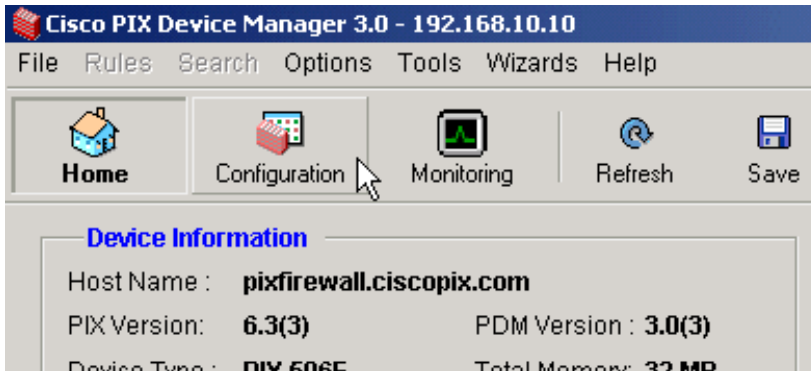
The last panel appears. Click **Finish** to save the configuration to the PIX Security Appliance.

[Back to Top](#)

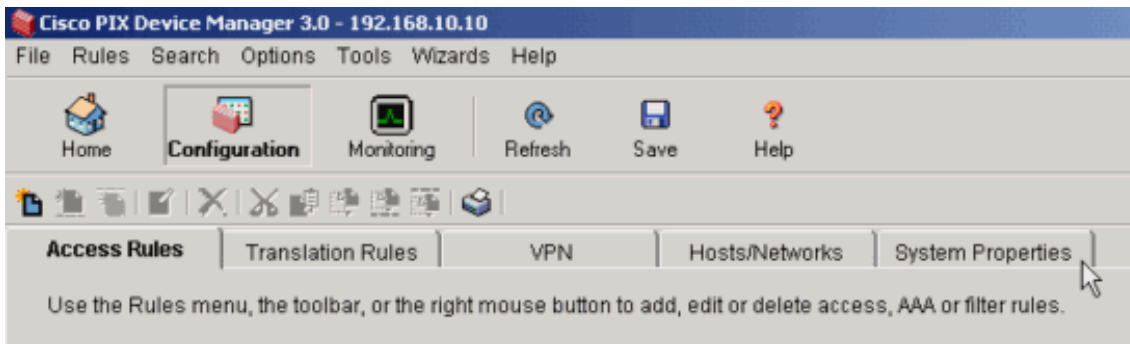
Create an Administrative Account

To create an administrative account to manage the PIX, follow these steps:

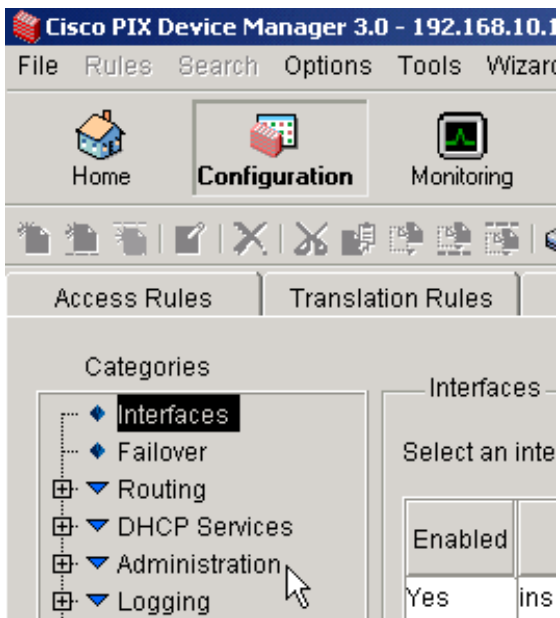
1. Click **Configuration**.



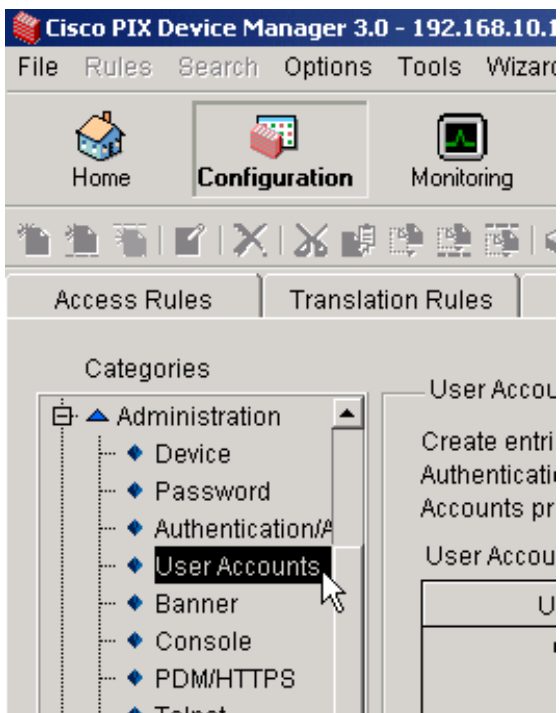
2. Click **System Properties**.



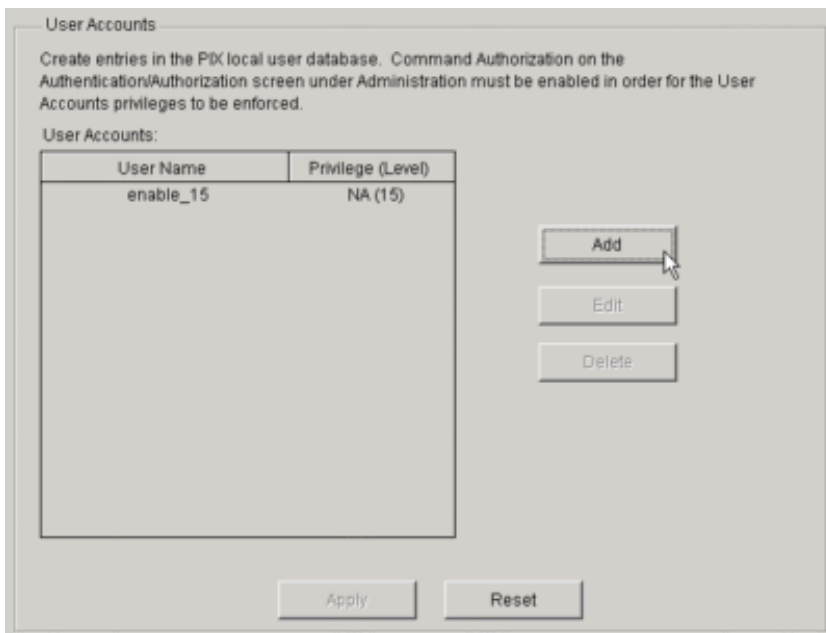
3. Click **Administration**.



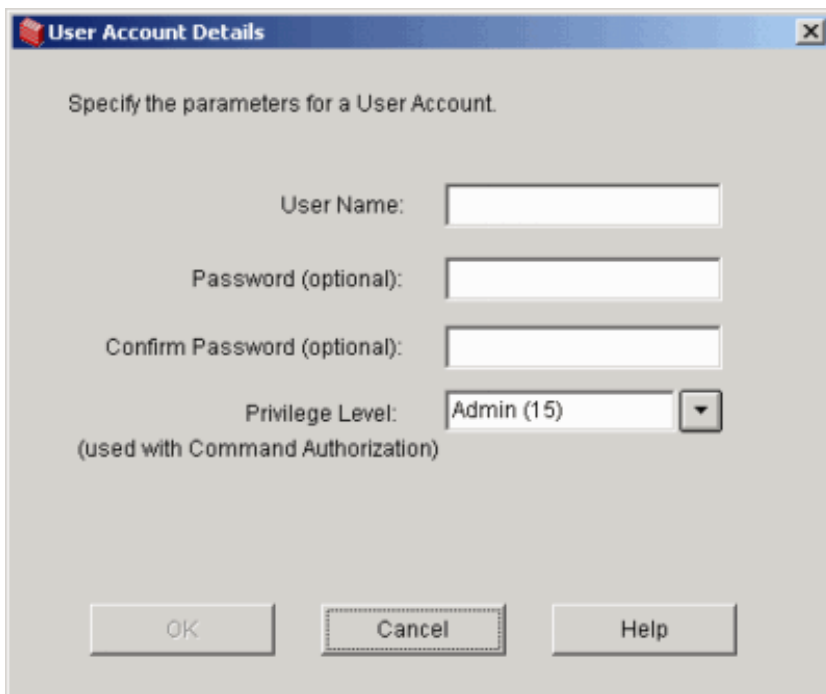
4. Click **User Accounts**.



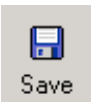
5. Click **Add**.



6. Type **admin** in the User Name field and enter the password that you entered on the Internet Worksheet (B11) in the Password and Confirm Password fields. Ensure that the Privilege Level is set to **15** and click **OK**.



7. Click the **Save** button to save the configuration.



[Back to Top](#)

Next Step

You have completed the initial setup of the PIX Security Appliance.

Refer to [Set Up Internet Security on the PIX Security Appliance](#) to secure your PIX.

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter.

Problem	Condition	Suggested Solution(s)
Browser asks for acceptance of the security certificate again.	The hostname or domain name has changed.	This is normal. Accept the security certificates again. (If you change the hostname or domain of the firewall unit, the browser asks you to accept the new security certificate.)
Browser asks for the password again.	If you change the password on the firewall unit, the browser might ask you to reenter the password for authentication. If you use the Java Plug-in, the browser will prompt you for your username and password twice.	Keep track of new and changed passwords on your worksheets.

<p>Browser cannot access PDM.</p>	<p>When you attempt to access PDM, the message "the page cannot be displayed" appears in Internet Explorer or the message "network connection was refused by the server" appears in Netscape Communicator.</p>	<p>Check that you are using "https" in your connection to "https://<i>inside_interface_ip_address</i>" and not "http." The connection cannot be made using "http," it must be "https."</p>
<p>Help files appear corrupted (on Internet Explorer only).</p>	<p>This can occur because PDM compresses the online Help files and Internet Explorer requires HTTP 1.1 to be enabled to handle compressed files properly.</p>	<p>If you are using a proxy server, select the Use HTTP 1.1 through proxy connections check box.</p>
<p>Some graphics or icons do not display properly.</p>	<p>PDM is being run with a Java Plug-in that is not supported (PDM supports Java Plug-in 1.4.2).</p>	<p>If you have the Java Plug-in installed, confirm that it is your default Java Virtual Machine (JVM). Do the following to ensure that the Java Plug-in is your default JVM:</p> <ol style="list-style-type: none"> 1. In Internet Explorer, click Tools > Internet Options. 2. Click the Advanced tab. Scroll down. Look for a Java (Sun) section. If there is one, confirm that Use Java 2 is selected. <p>In Netscape, click Edit > Preferences. Click Advanced. Make sure the Enable Java Plug-in check box is selected.</p> <p>For more detailed instructions see</p>

PDM launches slowly.	The startup speed of PDM depends on the amount of available RAM in your computer and whether virus scanning software is running on your computer.	<p>You can increase your available RAM by closing other applications.</p> <p>The time required to download the PDM applet can be greatly affected by the speed of the link between your workstation and the firewall unit. A minimum of 56 Kbps link speed is required; however, 3.84 Mbps or higher is recommended. Once the PDM applet is loaded on your workstation, the link speed impact on PDM operation is negligible.</p>
There is access only to the Monitoring tab in PDM.	The use of certain firewall CLI commands, and certain command combinations, limit access in PDM to the Monitoring tab.	For more information on these commands and command combinations, see the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide Release 2.3</i> .
PDM prompts for the username/password and certificate information twice.	This is normal when using Java Plug-in.	You can choose to accept the certificate permanently so that this dialog box does not appear again.

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Set Up Internet Security on the PIX Security Appliance](#)
- [Enable Java and JavaScript on Your PC](#)
- [SMB Technical Assistance Center \(SMB TAC\)](#)



Set Up Your PIX Security Appliance

[Home](#) > [Work With My Security Devices](#) > [Cisco Security Appliances](#) > [Set Up Your PIX Security Appliance](#)

Step 5: Set Up Internet Security on the PIX Security Appliance

- Step 1: [SMB Support Assistant Site Survey](#)
 Step 2: [Set Up Your PIX Security Appliance Hardware](#)
 Step 3: [Prepare to Configure Your PIX Security Appliance](#)
 Step 4: [Configure Your PIX Security Appliance with PIX Device Manager](#)

Step 5: Set Up Internet Security on the PIX Security Appliance

[Introduction](#)

[Requirements](#)

[Connect to the PIX](#)

[Configure Fixup Protocol Rules](#)

[Configure Access Control Lists](#)

[Create an ACL to Control Incoming Traffic](#)

[Create Additional Security Rules](#)

[Create Optional ACL Rules on the Inside Interface](#)

[Create ACL Rules for the Outside Interface](#)

[Configure Network Address Translation](#)

[Set Up NAT with a Dynamic IP Address](#)

[Set Up NAT with a Static IP Address](#)

[Set Up Port Address Translation](#)

[Next Step](#)

[Troubleshoot the Procedure](#)

[Related Information](#)

Introduction

This document describes how to configure a firewall on your PIX Security Appliance. A firewall is a protective barrier made up of rules that regulate the flow of Internet and network traffic that flows in and out of your network. This document is designed to show you how to set up rules to protect your network and to allow necessary traffic to flow in and out.

[Back to Top](#)

Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

Download PDF

[Step 5: Set Up Internet Security on the PIX Security Appliance](#)

[Set Up Your PIX Security Appliance](#)

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

Requirements

To perform the steps described in this document, you need to have these items:

- Ensure that all steps in [Configure the PIX Security Appliance](#) have been completed successfully.
- One of these web browsers, with JavaScript and Java enabled:
 - Netscape version 7.1 or later
 - Internet Explorer version 5.5 or later
- Completed worksheets as instructed in the [Site Survey](#):
 - Completed Remote Networking Assignments worksheet
 - Completed Internet Worksheet
 - Completed Firewall Worksheet
 - Completed LAN Addressing Worksheet

[Back to Top](#)

Connect to the PIX

Complete these steps to access the PIX:

1. Open a browser and type **https://pix_interface_ip_address** into the Address field. Refer to field R12 of the Remote Networking Assignments worksheet.

Note: Ensure that you add the "s" to "https" or the web browser cannot connect. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Security Appliance.

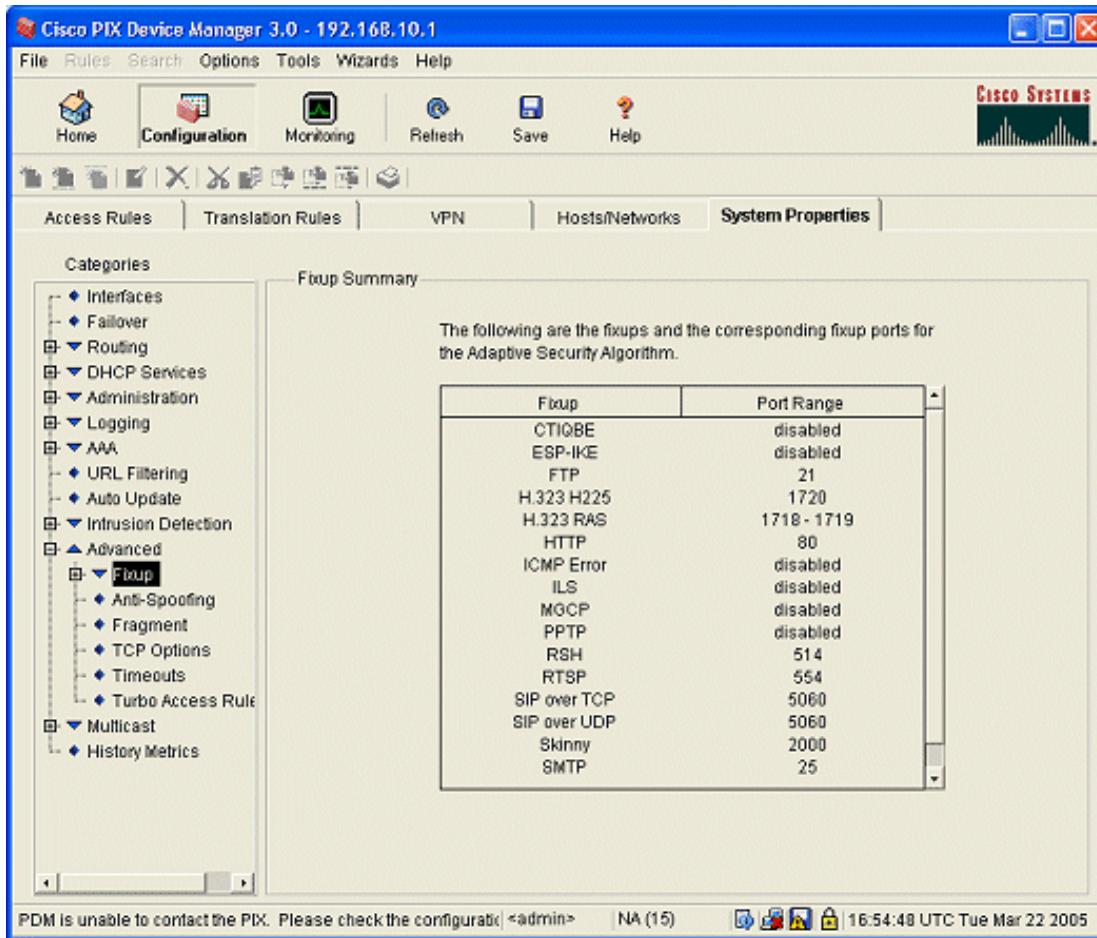
2. Leave the user name blank and enter the enable password found on line B12 of the Internet Worksheet, then press **Enter**.
3. Accept the security certificates (if they appear).
4. When the next logon screen appears, enter the enable password again and click **OK** to continue.
5. When the security warning screen appears, click **Always** to accept the certificates and launch PIX Device Manager (PDM).

[Back to Top](#)

Configure Fixup Protocol Rules

To configure fixup protocol rules on the firewall, follow these steps:

1. Go to **PDM > Configuration > System Properties**.
2. From the PDM home page, click **Configuration**, and then click the **System Properties** tab.
3. From the Categories menu on the left side of the window, click **Advanced > Fixup**.



4. To configure the fixup protocol rule, follow these steps:
 - a. The list of fixup protocols is displayed in the right side of the panel under Fixup Summary. Click **Advanced >**

Fixup > ICMP Error.

- b. Fixup Summary will be replaced with ICMP Error. Check the **Enable NAT for ICMP error messages** box.
- c. Click **Apply**.
- d. Click **MGCP**. The MGCP information appears in the right side of the PDM Configuration panel.

The screenshot shows the 'System Properties' tab in a configuration window. Under the 'MGCP' section, there is a descriptive paragraph: 'Media Gateway Control Protocol (MGCP) is a UDP signaling and session management protocol that media gateway controllers, also known as Call Agents, use to set up or terminate calls between media gateways, such as a Cisco AS5850.' Below this is another paragraph: 'To add an entry, enter the port information in the fields and click Add. To delete an entry, select a row and click Delete. The MGCP default port numbers are 2427 (gateway) and 2727 (Call...'. There is a table with two columns: 'Low Port' and 'High Port'. To the right of the table are buttons for '<< Add' and 'Delete'. Further right is a 'Port(s) To Be Added' section with 'Low Port:' and 'High Port: (optional)' labels and input boxes. The 'Low Port' box contains the value '2427'. At the bottom of this section is a 'Configure MGCP...' button. At the very bottom of the configuration panel are 'Apply' and 'Reset' buttons.

- e. Enter **2427** in the Low Port box under Port(s) To Be Added.
- f. Click **Add**.
- g. Click **Apply**.
- h. Click on **PPTP** in the tree view.

- i. Enter **1723** in the Low Port box under Port(s) To Be Added.
- j. Click **Add**.
- k. On the same panel, enter **47** in the Low Port box under Port(s) To Be Added.
- l. Click **Add**.
- m. Click **Apply**.
- n. Click **SMTP** in the tree view.
- o. Enter **465** in the Low Port box under Port(s) To Be Added.
- p. Click **Add**.
- q. Click **Apply**.

Note: In the Fixup Summary panel, the protocols that you changed will now show the port number or enabled instead of saying disabled.

5. Click the **Save** icon at the top of the panel.
6. When prompted to save the running configuration to flash memory, click **Apply**.

[Back to Top](#)

Configure Access Control Lists

An access control list (ACL) lets you specify what type of traffic to allow into an interface. By default, traffic that is not explicitly permitted is denied.

Create an ACL to Control Incoming Traffic

Complete these steps to create ACLs on your device:

1. Go to **PDM > Configuration**.

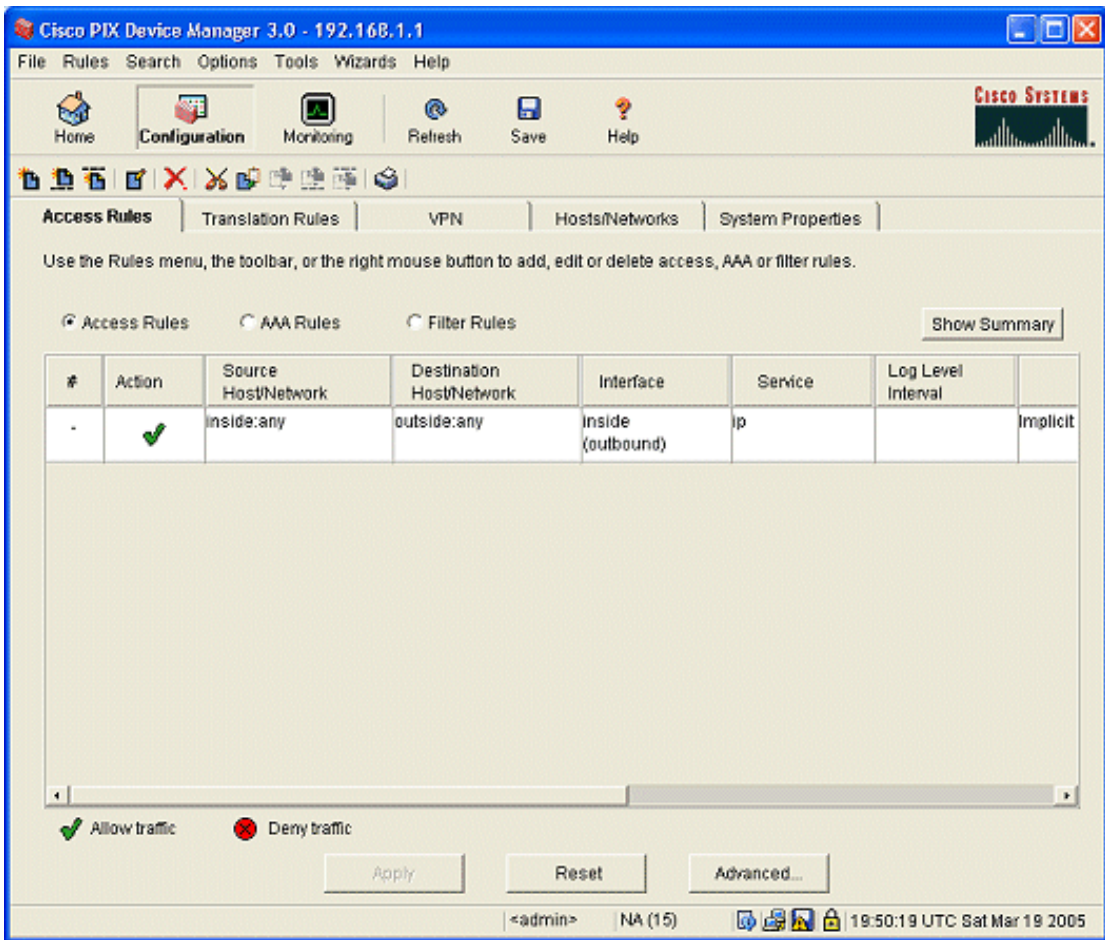
The screenshot displays the Cisco PIX Device Manager 3.0 interface for a device at 192.168.1.1. The interface is divided into several sections:

- Device Information:**
 - Host Name: pixfirewall.ciscopix.com
 - PIX Version: 6.3(3) | PDM Version: 3.0(1)
 - Device Type: PIX 506E | Total Memory: 32 MB
 - License: [Not Applicable] | Total Flash: 8MB
 - Licensed Features:
 - Encryption: 3DES-AES | Inside Hosts: Unlimited
 - Follower: [Not Applicable] | IKE Peers: Unlimited
 - Max Physical Interfaces: 2 | Max Interfaces: 2
- Interface Status:**

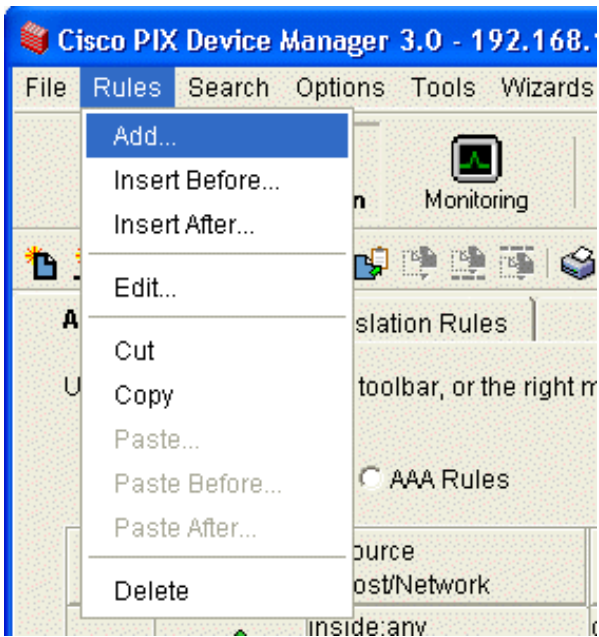
Interface	IP Address/Mask	Link	Current Kbps
inside	192.168.1.1/24	up	8
outside	64.102.40.182/25	up	1
- VPN Status:**
 - IKE Tunnels: 0
 - IPSec Tunnels: 0
- System Resources Status:**
 - CPU:** 0% usage.
 - Memory:** 15MB used (14.973 MB used, 17.027 MB free, 32 MB total).
- Traffic Status:**
 - Connections Per Second Usage: Graph showing a spike at 16:36:12.
 - UDP: 0, TCP: 0, Total: 0.
 - 'outside' Interface Traffic Usage (Kbps): Graph showing input and output traffic.
 - Input Kbps: 1, Output Kbps: 0.

The bottom status bar shows: <admin> | NA (15) | 16:38:02 UTC Fri Mar 18 2005.

- On the PDM home page, click **Configuration**.
- On the Configuration page, ensure that the Access Rules tab is displayed and that the Access Rules radio button is selected.



4. Create an ACL rule to block all incoming traffic that is not sent to the PIX.
 - a. The Rules menu will be accessible from the Configuration view. Click **Rules > Add**.



b. When the Add Rule panel appears, select **permit** from the drop-down list under Action.

Add Rule

Action
Select an action:

Syslog
 Enable Syslog

Source Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Destination Host/Network
 IP Address Name Group
Interface:
IP address:
Mask:

Protocol and Service
 TCP UDP ICMP IP
IP Protocol
IP protocol:

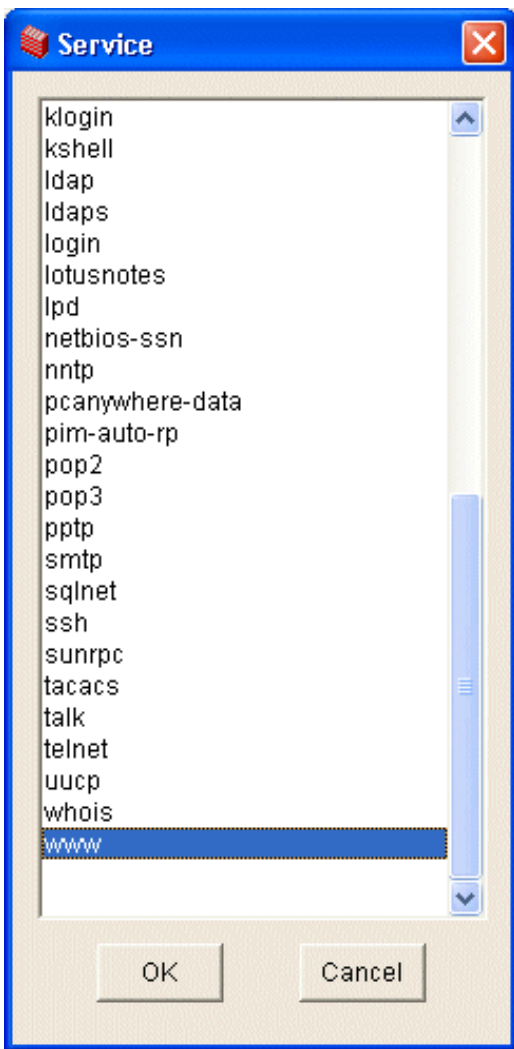
Please enter the description below (optional):

- c. Under Source Host/Network, select **IP Address**.
- d. For the Interface, select **outside**.
- e. Leave the IP address and Mask set to 0.0.0.0.
- f. Under Protocol and Service, select **IP**.
- g. Under IP protocol, select **any**.
- h. For Syslog leave the box unchecked.
- i. Under Destination Host/Network, select **IP Address**.

- j. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
- k. For the Mask, select **255.255.255.255** from the drop-down list.
- l. In the text box at the bottom of the Add Rule panel, enter a descriptive name for this rule.
- m. Click **OK** to save the rule.

5. Create an ACL rule to allow incoming web traffic:

- a. Click **Rules > Insert After**.
- b. Select **permit** from the drop-down list under Action.
- c. Under Source Host/Network, select **IP Address**.
- d. For the Interface, select **outside**.
- e. Leave the IP address and Mask set to 0.0.0.0.
- f. Under Protocol and Service, select **TCP**.
- g. Under Service, select **any**.
- h. For Syslog, leave the box unchecked.
- i. Under Destination Host/Network, select **IP Address**.
- j. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
- k. For the Mask, select **255.255.255.255** from the drop-down list.
- l. In the text box at the bottom of the Add Rule panel, enter a descriptive name for this rule.
- m. Under Destination Port, select **Service**. Click the details button (...) and select **www**.



- n. Click **OK**.
 - o. At the bottom of the Insert After Rule panel, enter a descriptive name for this rule.
 - p. Click **OK** to save this rule.
6. Create an ACL rule to allow incoming secure web traffic.
- a. Click **Rules > Insert After**.
 - b. Select **permit** from the drop-down list under Action.
 - c. Under Source Host/Network, select **IP Address**.
 - d. For the Interface, select **outside**.

- e. Leave the IP address and Mask set to 0.0.0.0.
- f. Under Protocol and Service, select **TCP**.
- g. Under Source Port, select **www**.
- h. Under Destination Host/Network, select **IP Address**.
- i. For the Interface, select **inside**.
- j. Leave IP address and Mask set to 0.0.0.0.
- k. Under Destination Port, select **https**.
- l. At the bottom of the Insert Rule After panel, enter a descriptive name for this rule.
- m. Click **OK** to save this rule.

7. Create an ACL rule to block incoming network broadcast traffic from the Internet.

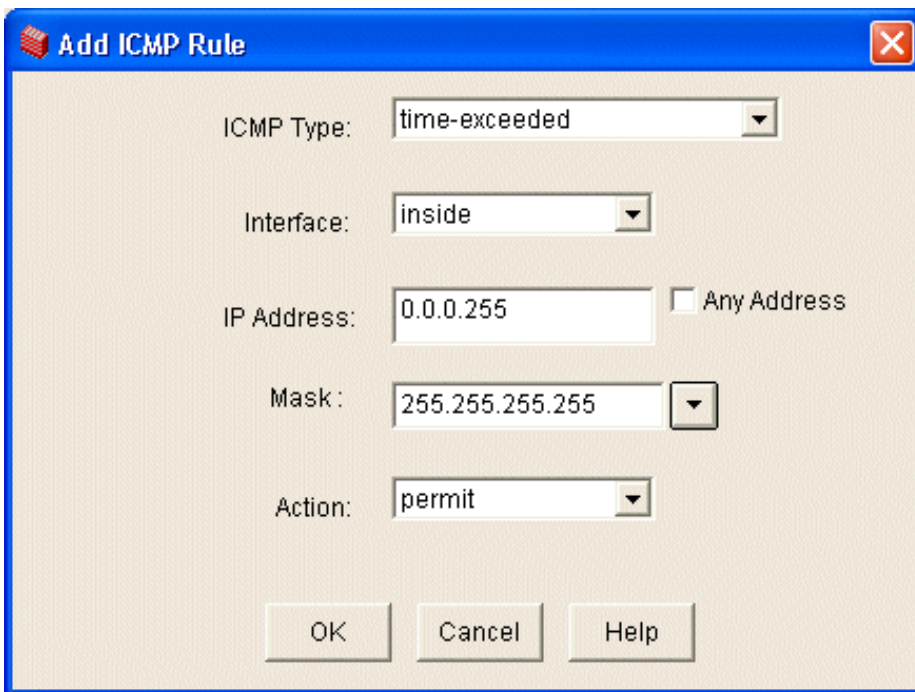
- a. Click **Rules > Insert After**.
- b. Select **deny** from the drop-down list under Action.
- c. Under Source Host/Network, select **IP Address**.
- d. For the Interface, select **outside**.
- e. Leave the IP address and Mask set to 0.0.0.0.
- f. Under Protocol and Service, select **IP**.
- g. Under IP protocol, select **any**.
- h. Under Destination Host/Network, select **IP Address**.
- i. For the Interface, select **inside**.
- j. Leave IP address and Mask set to 255.255.255.255.
- k. At the bottom of the Insert Rule After panel, enter a descriptive name for this rule.
- l. Click **OK** to save this rule.

8. Create an ACL rule to allow incoming Secure Shell (SSH) traffic on TCP.

- a. Click **Rules > Insert After**.
- b. Select **permit** from the drop-down list under Action.

- c. Under Source Host/Network, select **IP Address**.
 - d. For the Interface, select **outside**.
 - e. Leave the IP address and Mask set to 0.0.0.0.
 - f. Under Protocol and Service, select **TCP**.
 - g. Under Source Port select Service. Click the details button (...) and select **ssh**.
 - h. Under Destination Host/Network, select **IP Address**.
 - i. For the Interface, select **inside**.
 - j. For IP address enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
 - k. For the Mask, select **255.255.255.255** from the drop-down list.
 - l. Under Destination Port, select **Service**. Click the details button (...) and select **ssh**.
 - m. At the bottom of the Insert Rule After panel, enter a descriptive name for this rule.
 - n. Click **OK** to save this rule.
9. Click the **Save** icon at the top of the panel.
 10. When prompted to save the running configuration to flash memory, click **Apply**.
 11. Create an ACL rule to allow incoming Network Time Protocol traffic on UCP port 123.
 - a. Click **Rules > Insert After**.
 - b. Select **permit** from the drop-down list under Action.
 - c. Under Source Host/Network, select **IP Address**.
 - d. For the Interface, select **outside**.
 - e. Leave the IP address and Mask set to 0.0.0.0.
 - f. Under Protocol and Service, select **UDP**.
 - g. Under Source Port select Service. Click the details button (...) and select **ntp**.
 - h. Under Destination Host/Network, select **IP Address**.
 - i. For the Interface, select **inside**.
 - j. For IP address enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.

- k. For the Mask, select **255.255.255.255** from the drop-down list.
 - l. Under Destination Port, select **Service**. Click the details button (...) and select **ntp**.
 - m. At the bottom of the Insert Rule After panel, enter a descriptive name for this rule.
 - n. Click **OK** to save this rule.
12. Click the **Save** icon at the top of the panel.
 13. When prompted to save the running configuration to flash memory, click **Apply**.
 14. Create a rule to allow incoming time-exceeded ICMP messages on ICMP Type.
 - a. Click the **System Properties** tab. From the tree view on the left, select **Administration**.
 - b. Select **ICMP**.
 - c. When the ICMP information appears in the right side of the panel, click **Add**.
 - d. When the Add ICMP Rule panel appears, select **time-exceeded** from the ICMP Type drop-down list .



Add ICMP Rule

ICMP Type: time-exceeded

Interface: inside

IP Address: 0.0.0.255 Any Address

Mask: 255.255.255.255

Action: permit

OK Cancel Help

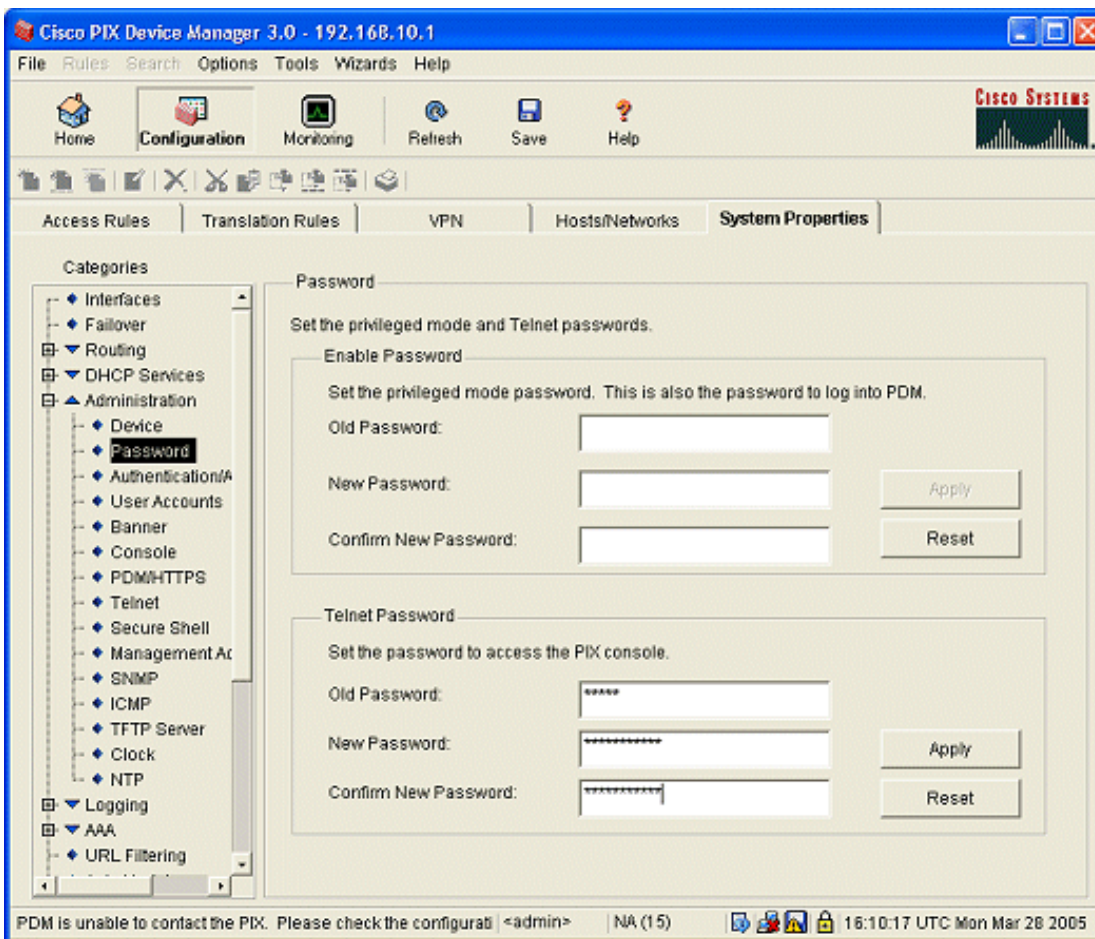
- e. For the Interface, select **inside**.
- f. For IP Address, enter **0.0.0.255**.

- g. For the Mask, select **255.255.255.255** from the drop-down list.
 - h. Select **permit** from the drop-down list under Action.
 - i. Click **OK**.
 15. Create a rule to allow incoming traceroute ICMP messages on ICMP Type.
 - a. Click **Add**.
 - b. For ICMP Type, choose **traceroute**.
 - c. For the Interface, select **inside**.
 - d. For IP Address, enter **0.0.0.255**.
 - e. For the Mask, select **255.255.255.255** from the drop-down list.
 - f. Select **permit** from the drop-down list under Action.
 - g. Click **OK**.
 - h. Click **Apply**.
 16. Click the **Save** icon at the top of the panel.
 17. When prompted to save the running configuration to flash memory, click **Apply**.

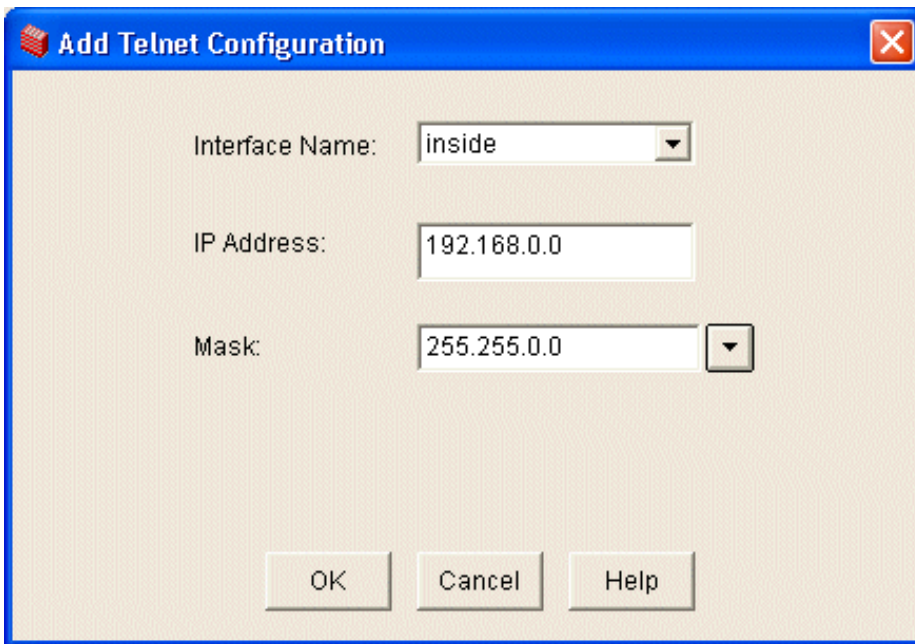
Create Additional Security Rules

Now that you have created the rules for SSH, you need to create rules for the PIX to recognize the sessions. To create the additional security rules, follow these steps:

1. Create a rule for Telnet.
 - a. Click the **System Properties** tab. From the tree view on the left, select **Administration > Password**.



- b. Under Telnet Password, enter **cisco** for the Old Password.
- c. Enter a strong password in the New Password field. For information on how to create strong passwords, refer to [Password Security](#).
- d. Enter the password again to confirm.
- e. Click **Apply**.
- f. From the tree view, click **Telnet**.
- g. In the right side of the panel, click **Add**.
- h. When the Add Telnet Configuration window appears, select **inside** from the Interface Name drop-down list.



Add Telnet Configuration

Interface Name:

IP Address:

Mask:

- i. For the IP Address, enter **192.168.0.0**.
 - j. For the Mask, select **255.255.0.0** from the drop-down list.
 - k. Click **OK**.
 - l. Click **Apply**.
2. Create a rule for SSH.
 - a. In the tree view, click **Secure Shell**.
 - b. For the IP Address, enter **192.168.0.0**.
 - c. For the Mask, select **255.255.0.0** from the drop-down list.
 - d. Click **OK**.
 - e. Click **Apply**.
 3. Create a rule to allow NTP Authentication.
 - a. In the tree view, click **NTP**.
 - b. On the right side of the panel, check **Enable NTP Authentication**.
 - c. Click **Add**.

The screenshot shows a dialog box titled "NTP Server Detail". It has a blue title bar with a close button. The main area is light beige. At the top, there is a text label "IP Address:" followed by a text input field containing "129.6.15.29" and a checked checkbox labeled "Preferred". Below that is a text label "Interface:" followed by a dropdown menu showing "outside". A larger rectangular box contains the "Authentication Key" section. Inside this box, there is a text label "Key Number:" followed by a dropdown menu and an unchecked checkbox labeled "Trusted". Below that are two text input fields, one labeled "Key Value:" and one labeled "Reenter Key Value:". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- d. When the NTP Server Detail window appears, enter **129.6.15.28** for the IP Address.
- e. For the Interface select **outside**.
- f. Check the Preferred box.
- g. Click OK.
- h. Click Add.
- i. For the IP Address enter **129.6.15.28**.
- j. Select **outside** from the Interface drop-down list.
- k. Check the **Preferred** check box.
- l. Click **OK**.
- m. Click **Apply**.

4. Click the **Save** icon at the top of the panel.

5. When prompted to save the running configuration to flash memory, click **Apply**.

Create Optional ACL Rules on the Inside Interface

If you need to allow certain types of VPN and email traffic through the firewall, you can create additional ACL rules. Each ACL rule in this section is optional. If you do not use VPN or have SMTP email traffic, you can skip this section.

Note: The firewall denies all network traffic by default unless an ACL rule explicitly permits traffic on a certain IP address or port.

1. If you use an SMTP email server, follow these steps to create an ACL rule to allow email traffic:
 - a. On the Configuration page, click the **Access Rules** tab, and then click the **Access Rules** radio button.
 - b. Click **Rules > Insert After**.
 - c. Select **permit** from the drop-down list under Action.
 - d. Under Source Host/Network, select **IP Address**.
 - e. For the Interface, select **inside**.
 - f. Leave IP address and Mask set to 0.0.0.0.
 - g. Under Protocol and Service, select **TCP**.
 - h. Under Source Port, click the details button (...) and select **smtp**.
 - i. Under Destination Host/Network, select **IP Address**.
 - j. For the Interface, select **outside**.
 - k. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
 - l. For the Mask, select **255.255.255.255** from the drop-down list.
 - m. Under Destination Port, select **Service**, click the details button (...), and then select **smtp**.
 - n. In the text box at the bottom of the panel, enter a descriptive name for this rule.
 - o. Click **OK** to save the rule.
2. Check the Firewall Worksheet line F5, if you have PPTP VPN create two rules to allow PPTP VPN traffic. Follow these steps for the first rule:
 - a. On the Configuration page, click the **Access Rules** tab, and then click the **Access Rules** radio button.
 - b. Click **Rules > Insert After**.
 - c. Select **permit** from the drop-down list under Action.

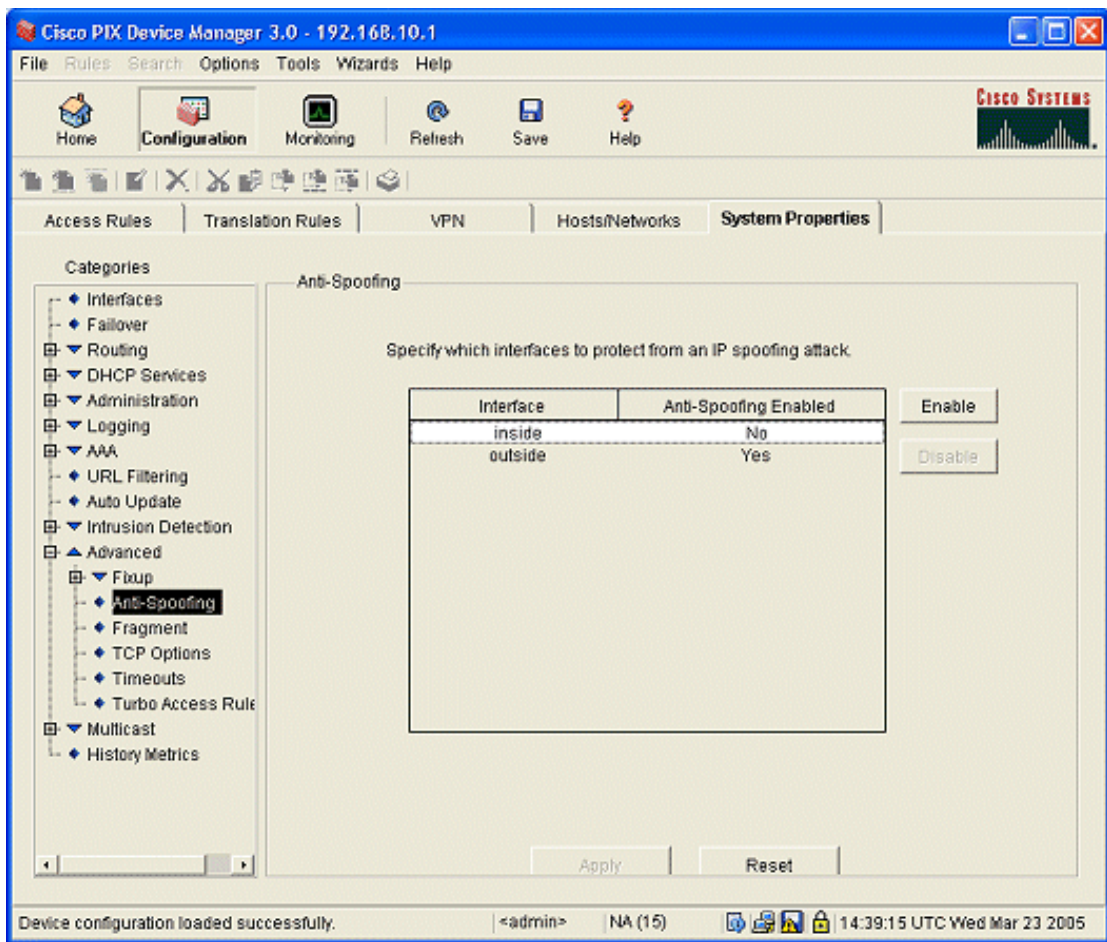
- d. Under Source Host/Network, select **IP Address**.
 - e. For the Interface, select **inside**.
 - f. Leave IP address and Mask set to 0.0.0.0.
 - g. Under Protocol and Service, select **TCP**.
 - h. Under Source Port, click the details button (...) and select **pptp**.
 - i. Under Destination Host/Network, select **IP Address**.
 - j. For the Interface, select **outside**.
 - k. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
 - l. For the Mask, select **255.255.255.255** from the drop-down list.
 - m. Under Destination Port, select **Service**, click the details button (...), and then select **pptp**.
 - n. In the text box at the bottom of the panel, enter a descriptive name for this rule.
 - o. Click **OK** to save the rule.
3. Follow these steps to create the second PPTP rule:
- a. On the Configuration page, click the **Access Rules** tab, and then click the **Access Rules** radio button.
 - b. Click **Rules > Insert After**.
 - c. Select **permit** from the drop-down list under Action.
 - d. Under Source Host/Network, select **IP Address**.
 - e. For the Interface, select **inside**.
 - f. Leave IP address and Mask set to 0.0.0.0.
 - g. Under Protocol and Service, select **IP**.
 - h. Under Source Port, click the details button (...) and select **pptp**.
 - i. Under Destination Host/Network, select **IP Address**.
 - j. For the Interface, select **outside**.
 - k. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.

- I. For the Mask, select **255.255.255.255** from the drop-down list.
 - m. Under Destination Port, select **Service**, click the details button (...), and select **pptp**.
 - n. In the text box at the bottom of the panel, enter a descriptive name for this rule.
 - o. Click **OK** to save the rule.
4. Click **Apply**.
5. Click the **Save** icon at the top of the panel.
6. When prompted to save the running configuration to flash memory, click **Apply**.

Create ACL Rules for the Outside Interface

To create an ACL on the outside interface to limit unsolicited internet traffic, follow these steps:

1. Click the **System Properties** tab.
2. From the tree view on the left, click **Administration**.
3. Click **Anti-Spoofing**.
4. In the Anti-Spoofing area, select the inside interface.



5. Click **Enable**.
6. Select the outside interface, and then click **Enable**.
7. Click **Apply**.
8. Click the **Save** icon at the top of the panel.
9. When prompted to save the running configuration to flash memory, click **Apply**.

[Back to Top](#)

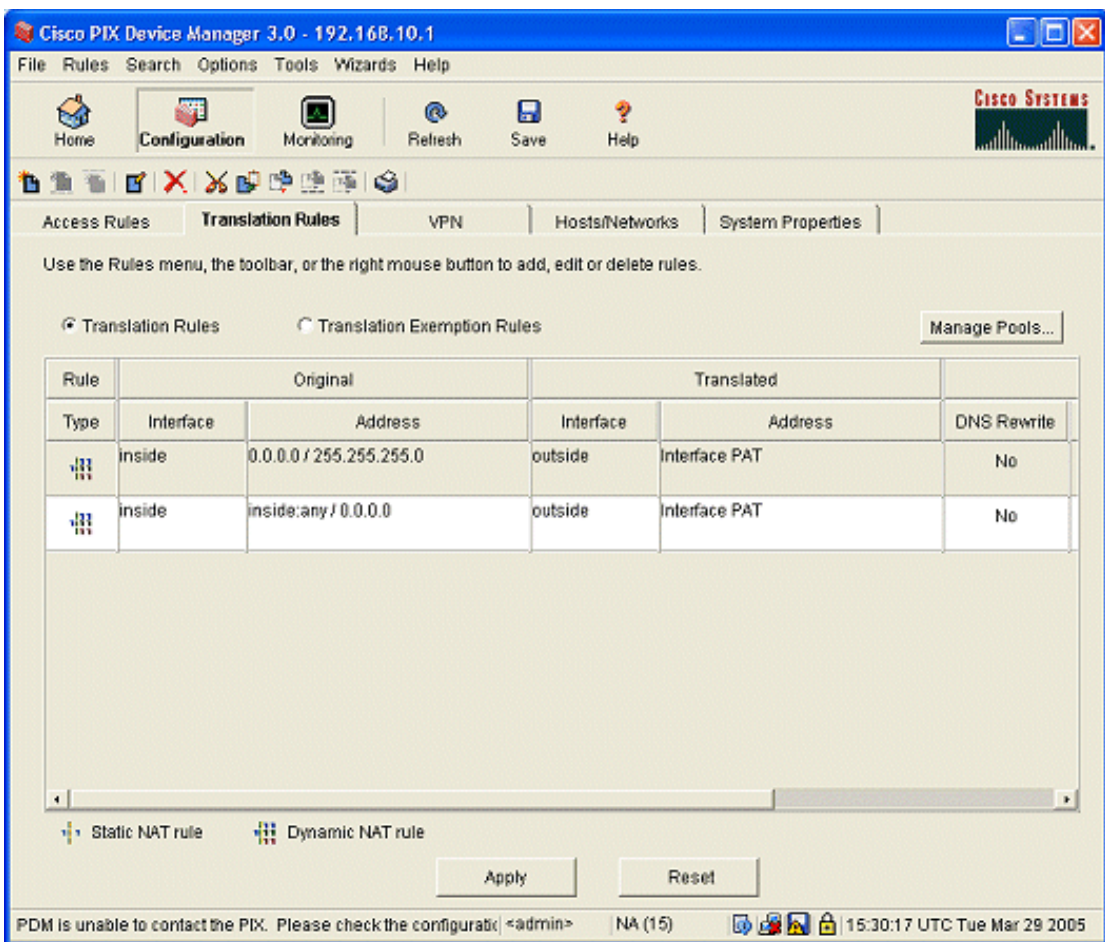
Configure Network Address Translation

Network Address Translation (NAT) uses an internal address scheme to provide additional security for your network. In order to set up NAT, you need to know whether your connection uses a static or dynamic IP address. Refer to the Internet Worksheet (B45, B46) for this information.

Set Up NAT with a Dynamic IP Address

If your connection uses a dynamic address, follow these steps to set up NAT with a dynamic IP address:

1. Click the **Translation Rules** tab.
2. Click the **Translation Rules** button.



3. Click **Rules > Add**.
4. Under Original Host/Network, select **inside** from the Interface drop-down list.

Add Address Translation Rule

Original Host/Network

Interface:

IP address: Mask:

Translate address on interface:

Translate Address to

Static IP address:

Redirect port

TCP Original port: Translated port:

UDP

Dynamic Address pool:

Pool ID	Address
1	Interface PAT

5. For the IP Address, enter **0.0.0.0**.
6. For the Mask, select **0.0.0.0** from the drop-down list.
7. In the Translate address on interface, select **outside**.
8. In the Translate Address To section, click **Dynamic**.
9. In the Address Pool box, select the address pool you created on your worksheet.
10. Click **OK**.

11. Click **Apply**.
12. Click the **Save** icon at the top of the panel.
13. When prompted to save the running configuration to flash memory, click **Apply**.

Set Up NAT with a Static IP Address

To set up NAT with a static IP address, follow these steps:

1. Click **Rules > Add**.
2. Under Original Host/Network, select **inside** from the Interface drop-down list.

Add Address Translation Rule

Original Host/Network

Interface:

IP address: Mask:

Translate address on interface:

Translate Address to

Static IP address:

Redirect port

TCP Original port: Translated port:

UDP

Dynamic Address pool:

Pool ID	Address
---------	---------

3. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
4. For the Mask, select **255.255.255.255** from the drop-down list.
5. In the Translate address on interface, select **outside**.
6. In the Translate Address To section, click **Static**.
7. For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
8. Click **OK**.
9. Click **Apply**.
10. Click the **Save** icon at the top of the panel.
11. When prompted to save the running configuration to flash memory, click **Apply**.

[Back to Top](#)

Set Up Port Address Translation

If you have servers in your network that users outside of your network need to access, you must set up Port Address Translation (PAT).

You can set up PAT for a variety of internal servers. Remember that PAT is only needed if the server is *physically located inside your network*. Use the table to find the worksheet reference you need to verify if you have each type of server.

Server Type	Worksheet Reference
Internal email server	Firewall Worksheet line F1
Internal web server	Firewall Worksheet line F4
Microsoft PPTP VPN server	Firewall Worksheet line F5

You need to create one PAT rule for each server that you want to make available outside of your network.

You also need to ensure that you have set up the appropriate access rules to allow traffic from the server to leave the network. See [Create Optional ACL Rules on the Inside Interface](#) for more information.

To set up a new PAT rule, follow these steps:

1. From the Translation Rules tab, click **Rules > Add**.

Add Address Translation Rule

Original Host/Network

Interface:

IP address: Mask:

Translate address on interface:

Translate Address to

Static IP address:

Redirect port

TCP Original port: Translated port:

UDP

Dynamic Address pool:

Pool ID	Address
---------	---------

2. Under Original Host/Network, select **inside** from the Interface drop-down list.
3. For the IP address, enter the IP Address for the server. See the appropriate line on the Firewall Worksheet indicated in the [table of server types](#).
4. For the Mask, select **255.255.255.255** from the drop-down list.

- In the Translate address on interface, select **outside**.
- In the Translate Address To section, click **Static**.
- For IP address, enter the IP address of the PIX found on line R12 of the Remote Network Addressing worksheet.
- Check the **Redirect Port** check box.
- Choose **TCP** or **UDP** and enter the port number in the Original Port and Translated Port fields. Refer to the table for a listing of common ports.

Service	Port Type	Port Number (s)
HTTP (Internet)	TCP	80
HTTPS	TCP	443
SMTP	TCP	25, 465
PPTP VPN	TCP	1723
PPTP VPN	IP	47

- Click **OK**.
- Click **Apply**.
- Repeat these steps for each internal server that needs to be accessed from the outside.
- Click the **Save** icon at the top of the panel.
- When prompted to save the running configuration to flash memory, click **Apply**.

[Back to Top](#)

Next Step

You have completed the set up of the firewall on your PIX.

To configure a VPN on the PIX, proceed to [Configure VPN on the PIX Security Appliance](#).

To make further changes to your PIX, refer to the [PIX Support Page](#).

To configure other devices in your network, refer to the [Configuration Overview Page](#).

[Back to Top](#)

Troubleshoot the Procedure

This section provides information about common problems that you may encounter. If this information does not solve your problem, contact the [SMB Technical Assistance Center \(SMB TAC\)](#) for assistance.

Problem	Cause(s) and Suggested Solution(s)
I added a new rule to the firewall, and now I cannot access the PIX Security Appliance.	Contact the SMB TAC for assistance.

[Back to Top](#)

Related Information

- [Site Survey](#)
- [Configure VPN on the PIX Security Appliance](#)
- [Configure the PIX Security Appliance](#)
- [Password Security](#)