



VPN Installation Procedures

Cisco PIX501 Firewall Router

EbixExchange Confidential and Proprietary

This document and the information contained therein are confidential to and the property of EbixExchange Australia Pty Ltd. This information is made available to Sunrise customers for the sole purpose of conducting the company's business and is not to be disclosed without prior written consent. All rights reserved.

VPN Installation Procedures

Cisco PIX501 Firewall Router

© EbixExchange Australia Pty Ltd 2008

Disclaimer:

Every effort has been made to provide accurate and complete information. However, EbixExchange Australia Pty Ltd assumes no responsibility for any direct, indirect, incidental or consequential damages arising from the use of the information in this document. Data and case-study examples are intended to be fictional.

Copyright:

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means electronic, mechanical photocopying, recording, or otherwise without written permission from EbixExchange Australia Pty Ltd.

This manual was produced using Windows XP Professional and Microsoft Word 2003

Last Updated: 3/10/08

1	Introduction	1
2	Prerequisites	1
3	Installation	1
3.1	Installing the Digital Certificate	1
	Using Static IP Address	5
	Using PPPoE	8
3.2	Testing Connection to the Internet	9
4	Configuring the VPN	10
5	Confirming VPN Access	11
5.1	Is the VPN Working Correctly?	13
5.2	Testing your Sunrise™ Exchange Connection	14
Appendix A	16
Firmware Update for PIX501		16
Requirements		16
Update Procedure		16
Appendix B	18
Upgrade Notes from Cisco		18
Entering Monitor Mode on a PIX 501, 506, 515, 525, 535		18
Upgrading PIX Firewall from Boothelper or Monitor Mode		18
Upgrading PIX Firewall from Version 5.1.1 or Later		21
Using the copy tftp flash Command to Upgrade the PIX		21
Upgrading PIX Devices in a Failover Set with Minimal Downtime		21
Upgrading the Activation Key		23
PIX Devices Running Versions 6.1 and Earlier		23
PIX Devices Running Versions 6.2 and Later		23
Installing PDM		24

1 Introduction

EbixExchange's use of Sunrise™ Exchange uses a Virtual Private Network (VPN). Connecting to a remote corporate server, using a routing infrastructure such as the Internet, the VPN allows connection between insurers and intermediaries to operate in a secure manner.

Other options open to insurers who operate Sunrise™ Exchange independently of EbixExchange, include IP-based intranets and extranets, as well as the public Internet.

The Sunrise™ Exchange VPN is based on the IPSec protocol and takes advantage of the broad availability of the Internet.

IPSec encrypts everything between two computers. Using a VPN connection, data is carried over the public network, but is unreadable to unauthorised clients. It also provides audit records to show access information.

Note:

IP addresses, user names and user passwords used throughout this document are not valid and are displayed for demonstration purposes only. EbixExchange will supply valid IP addresses and user details upon connection to Sunrise™ Exchange.

2 Prerequisites

In this document, PIX501 is configured as a Cisco VPN Client (EzVPN) to set up a VPN for Sunrise Exchange. It is also possible to configure the Pix501 as a LAN-LAN connection, if the internet connection has a static IP address (separate document available). The Pix501 may be connected to the Internet directly via PPPoE, or through an Internet router. The Internet connection may be cable, ADSL or ISDN, which provides a static or dynamic IP address.

Instructions for configuring the PIX501 are provided in this document, along with how to configure the PIX501 to connect to the Internet using PPPoE (using a cable or ADSL modem) or a router (using a static or dynamic IP address).

The PIX501 requires IOS version 6.2 or later, and 16MB of memory to operate as VPN Client as required by this set up.

The PIX501 should have a 3DES activation key.

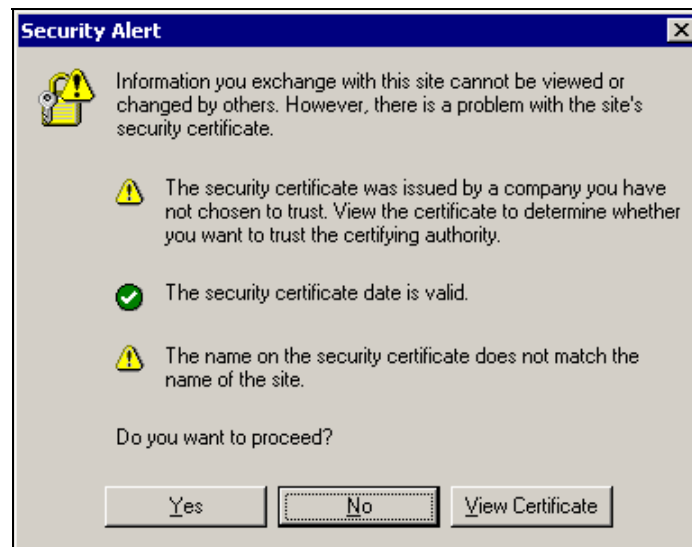
Detailed steps on upgrading the PIX IOS to 6.2.2 are provided in *Appendix A*.

3 Installation

The factory default IP address setting of PIX501 is **192.168.1.1**. DHCP server facility is also enabled by default.

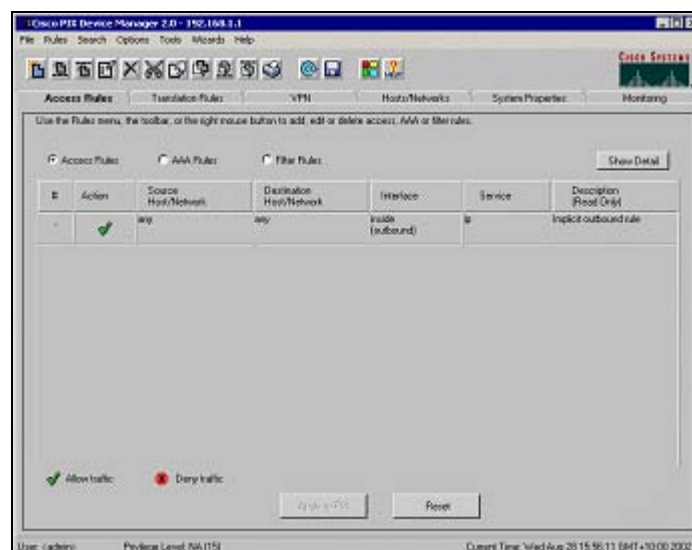
3.1 Installing the Digital Certificate

Enter **https:\\192.168.1.1** into the browser.



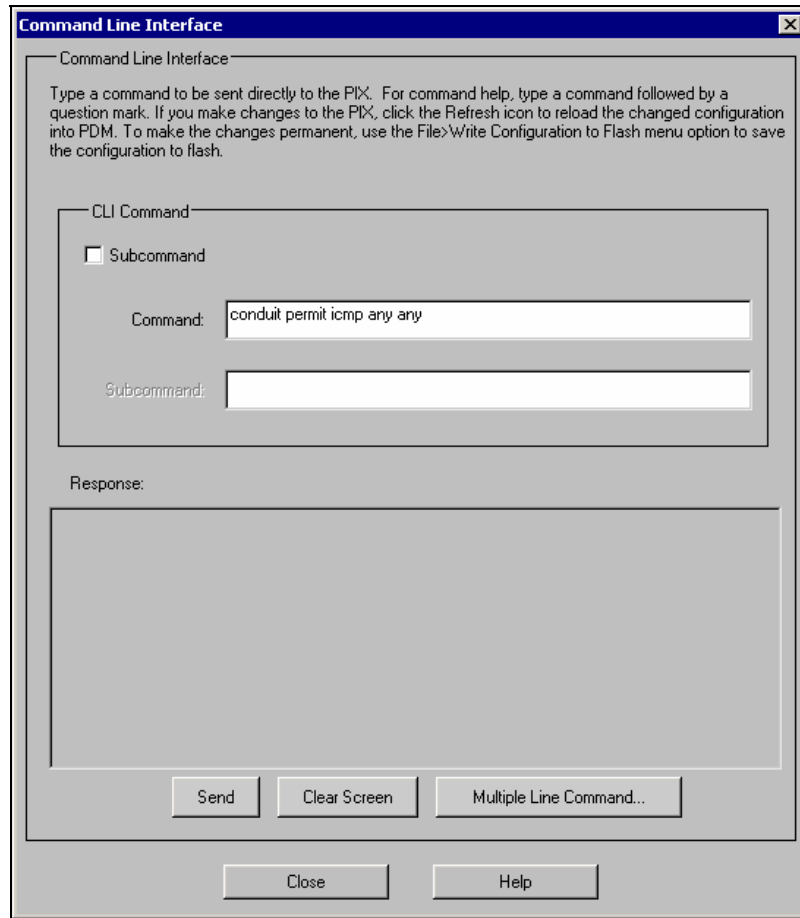
The browser will ask for a digital certificate to be installed.

Select **Y**es.

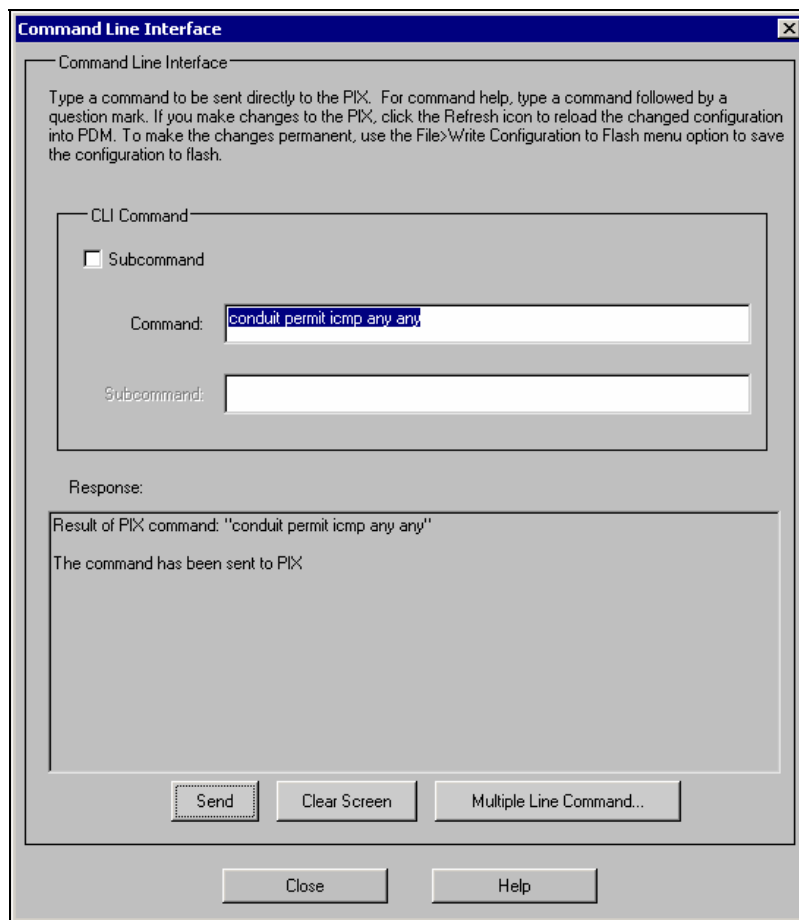


The PIX Device Manager will display.

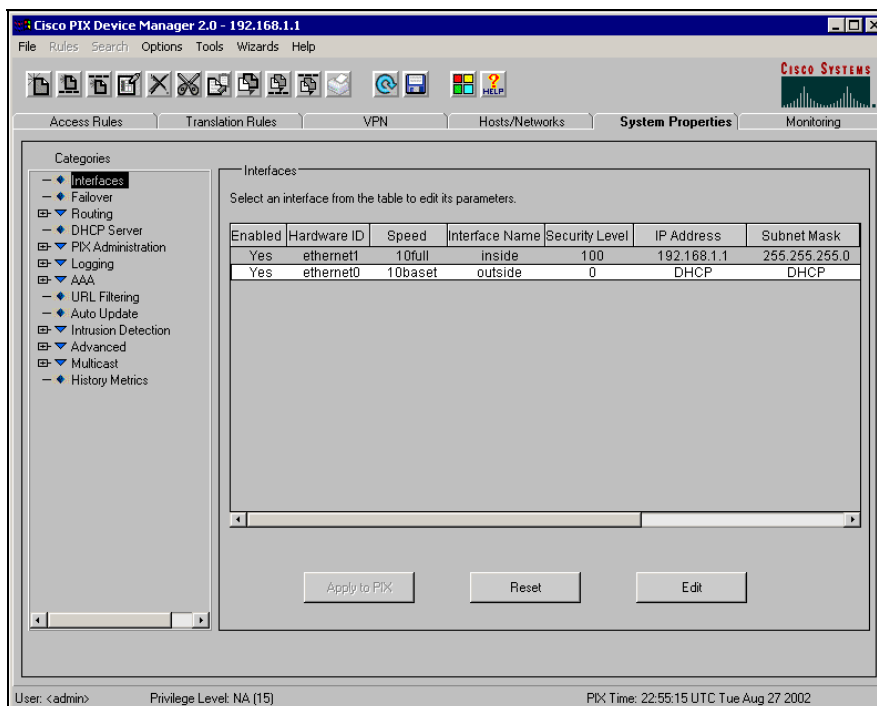
Click **T**ools.



Type **Conduit permit icmp any any** on the command line and click **Send**.



Click **Close**.



Select the **System Properties** tab.

Highlight the outside entry and click **Edit**.

Edit Interface

Hardware ID: **ethernet0**

Enable Interface Speed: 10baset

Interface Name: outside Security Level: 0

IP Address

Static IP Address Use DHCP Use PPPoE

The interface automatically gets its IP address using DHCP.

Obtain default route using DHCP

Retry Count:

OK Cancel Help

If using **DHCP**, click Use DHCP and click **OK**.

Proceed to *Configuring the VPN*.

If using **Static IP Address**, click Static IP Address and proceed to *Using Static IP Address*.

If using **PPPoE**, click Use PPPoE and proceed to *Using PPPoE*.

Using Static IP Address

When using an outside interface, you will need to enter a Static IP Address.

Edit Interface

Hardware ID: **ethernet0**

Enable Interface Speed: 10baset

Interface Name: outside Security Level: 0

IP Address:

Static IP Address Use DHCP Use PPPoE

IP Address: 192.168.0.55

Subnet Mask: 255.255.255.0

OK Cancel Help

Fill in the details for IP address and subnet mask for an outside interface.

Click **OK** to continue.

Cisco PIX Device Manager 2.0 - 192.168.1.1

File Rules Search Options Tools Wizards Help

Access Rules Translation Rules VPN Hosts/Networks **System Properties** Monitoring

Categories:

- Interfaces
- Falover
- Routing
- DHCP Server
- PIX Administration
- Logging
- AAA
- URL Filtering
- Auto Update
- Intrusion Detection
- Advanced
- Multicast
- History Metrics

Interfaces

Select an interface from the table to edit its parameters.

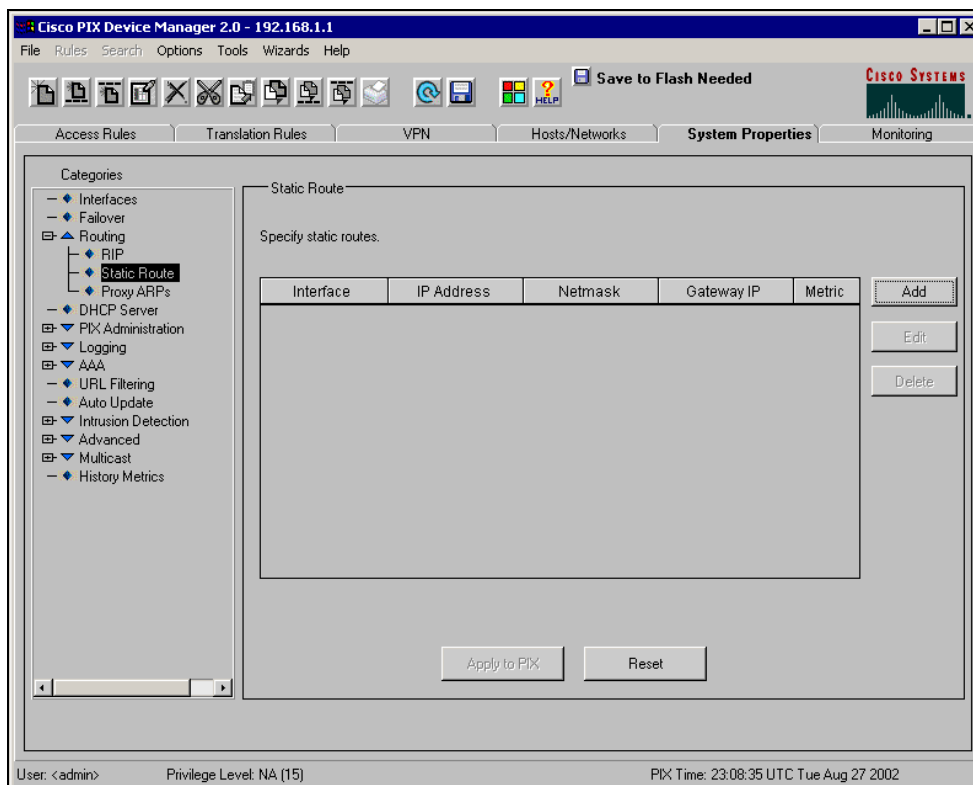
Enabled	Hardware ID	Speed	Interface Name	Security Level	IP Address	Subnet Mask
Yes	ethernet1	10full	inside	100	192.168.1.1	255.255.255.0
Yes	ethernet0	10baset	outside	0	192.168.0.55	255.255.255.0

Apply to PIX Reset Edit

User: <admin> Privilege Level: NA (15) PIX Time: 23:02:05 UTC Tue Aug 27 2002

A default gateway is also required.

Click **Routing** and select **Static Route**.



Click **Add**.

The 'Add Static Route' dialog box is shown with the following fields:

- Interface Name: outside
- IP Address: 0.0.0.0
- Gateway IP: 192.168.0.1
- Mask: 0.0.0.0
- Metric: 1

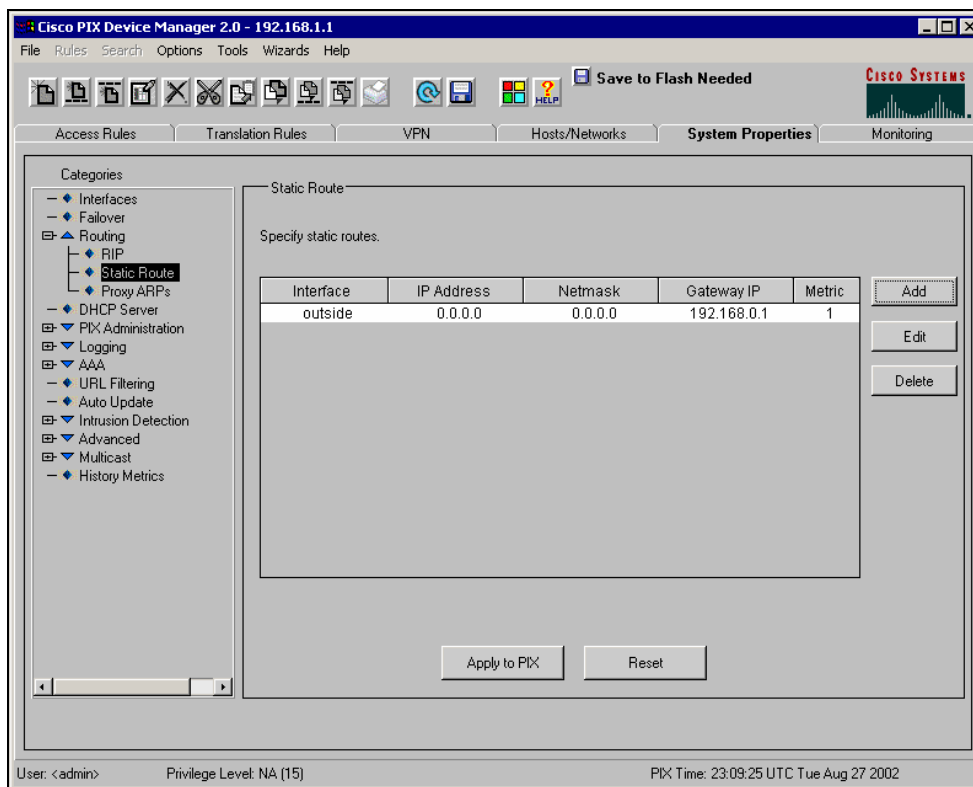
Buttons: OK, Cancel, Help

Enter **0.0.0.0** for the IP Address.

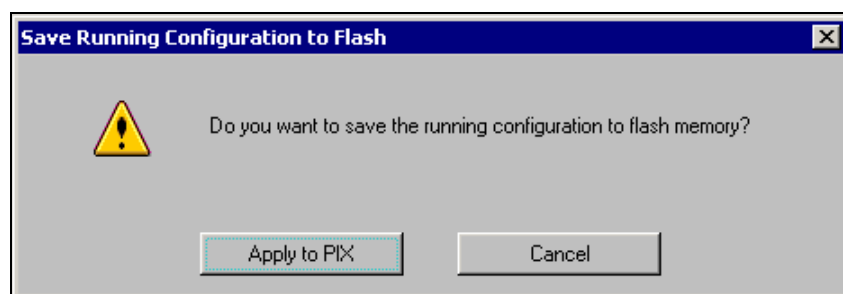
Enter the correct Gateway IP address.

Enter **0.0.0.0** for the Mask.

Click **OK**.

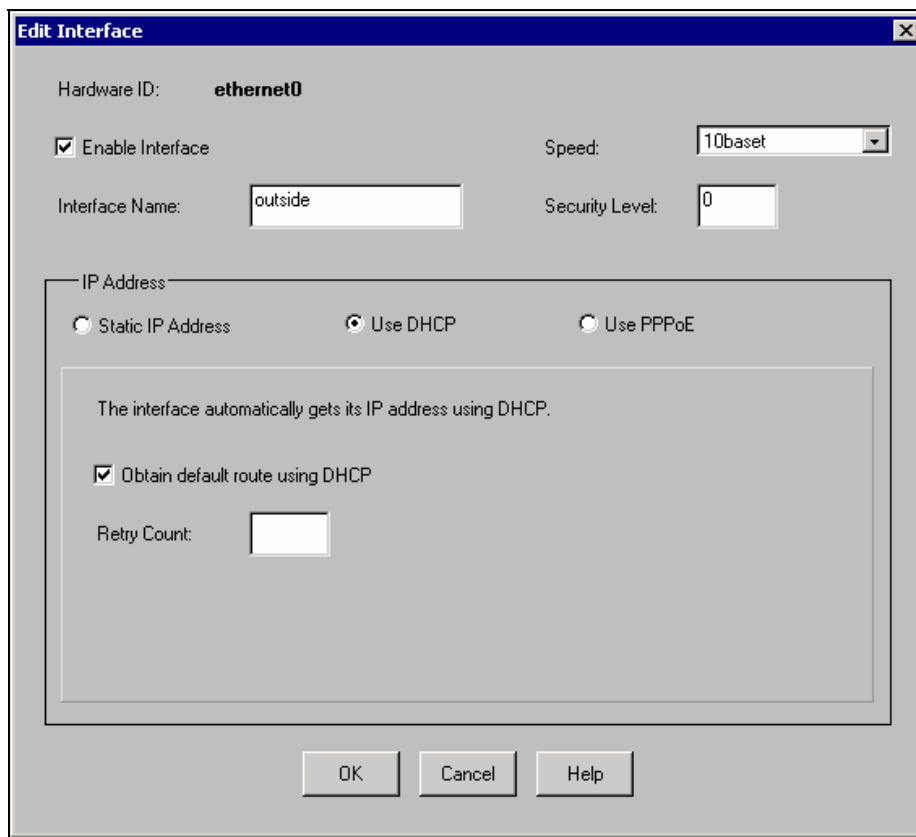


Click **Apply to PIX** to update the configuration.



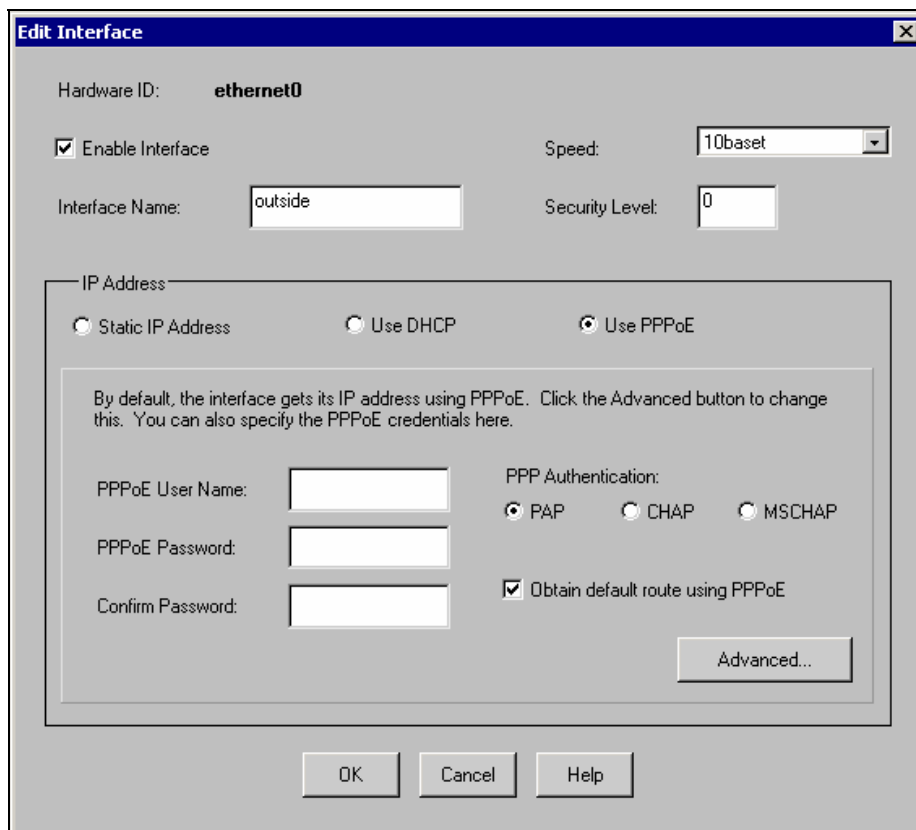
Click **Apply to PIX** again to confirm.

Using PPPoE



The screenshot shows the 'Edit Interface' dialog box for the 'ethernet0' interface. The 'Enable Interface' checkbox is checked. The 'Interface Name' is 'outside'. The 'Speed' is set to '10baset' and the 'Security Level' is '0'. In the 'IP Address' section, the 'Use DHCP' radio button is selected. Below this, a text box states: 'The interface automatically gets its IP address using DHCP.' The 'Obtain default route using DHCP' checkbox is checked, and the 'Retry Count' is set to 1. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

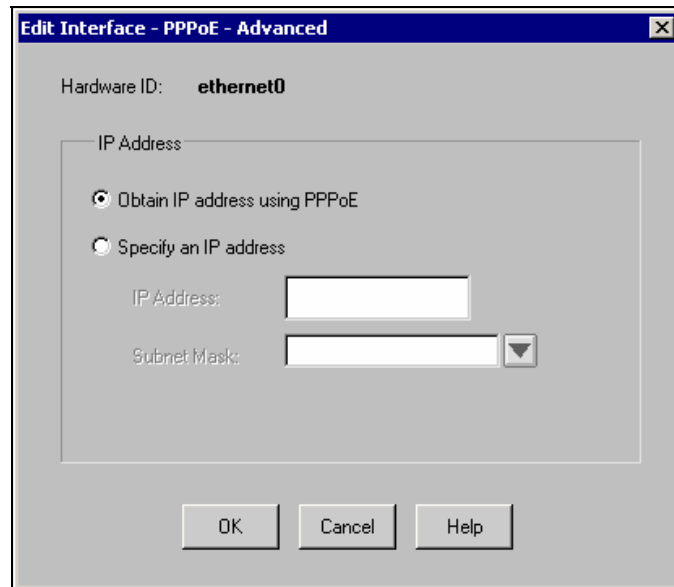
When using PPPoE, select **Use PPPoE**.



The screenshot shows the 'Edit Interface' dialog box for the 'ethernet0' interface. The 'Enable Interface' checkbox is checked. The 'Interface Name' is 'outside'. The 'Speed' is set to '10baset' and the 'Security Level' is '0'. In the 'IP Address' section, the 'Use PPPoE' radio button is selected. Below this, a text box states: 'By default, the interface gets its IP address using PPPoE. Click the Advanced button to change this. You can also specify the PPPoE credentials here.' There are three input fields for 'PPPoE User Name', 'PPPoE Password', and 'Confirm Password'. The 'PPP Authentication' section has 'PAP' selected, with 'CHAP' and 'MSCHAP' also available. The 'Obtain default route using PPPoE' checkbox is checked. An 'Advanced...' button is located at the bottom right of the IP Address section. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Enter the PPPoE User Name, Passwords and PPP Authentication (usually CHAP).

Click Advanced (if required), or click **OK**.



Advanced allows for an IP address to be specified, if required.

3.2 Testing Connection to the Internet

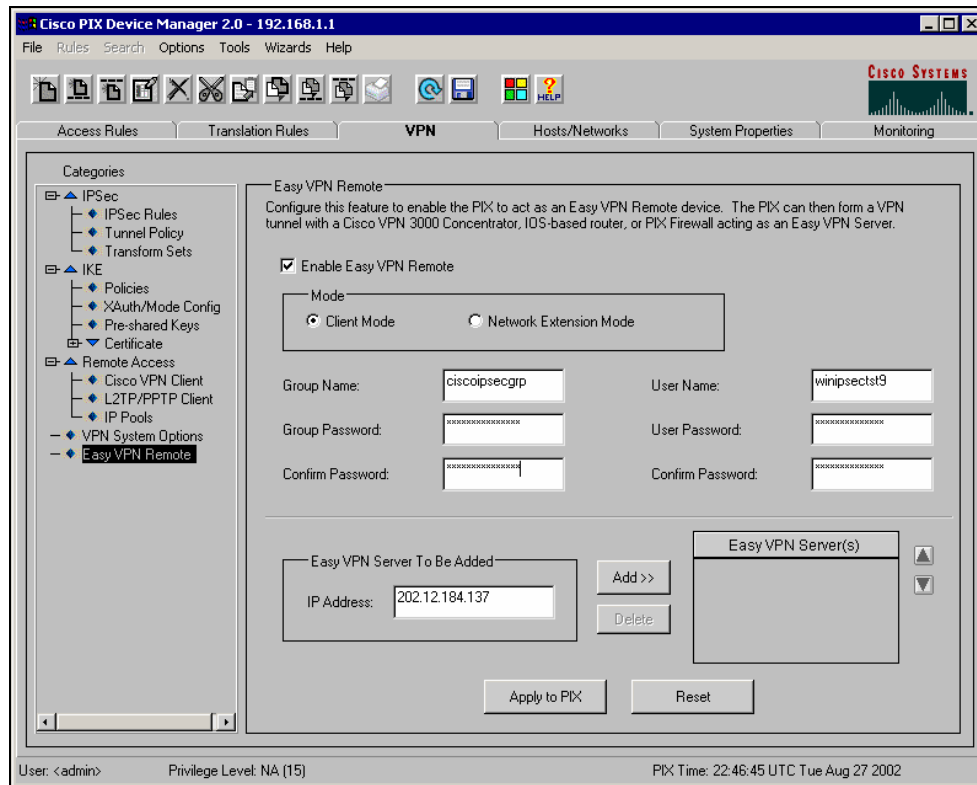
Ping the Internet from a PC; i.e. www.ebix.com.au or 202.12.184.1.

Ping replies should be received confirming that you can browse the Internet. If you are unable to access the Internet, reload the router and try again. Troubleshooting may be required.

When Internet access has been established, proceed to the next section.

4 Configuring the VPN

Whilst still in the Cisco PIX Device Manager, select the **VPN** tab.



Select Enable Easy VPN Remote, and Client Mode.

Enter the following details:

Group Name	Groupname (refer your Sunrise Configuration Sheet)
Group Password and Confirm Password	Password (refer your Sunrise Configuration Sheet)
User Name	Username (refer your Sunrise Configuration Sheet)
User Password and Confirm Password	Password (refer your Sunrise Configuration Sheet)
IP Address	VPN IP Address (refer your Sunrise Configuration Sheet)

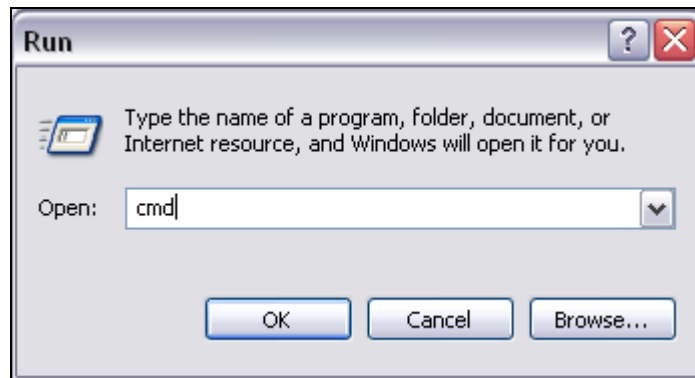
Click **Add >>**.


Click **Apply to PIX** to continue.

5 Confirming VPN Access

To confirm that your VPN Access is established:

Click **S**tart and **R**un.



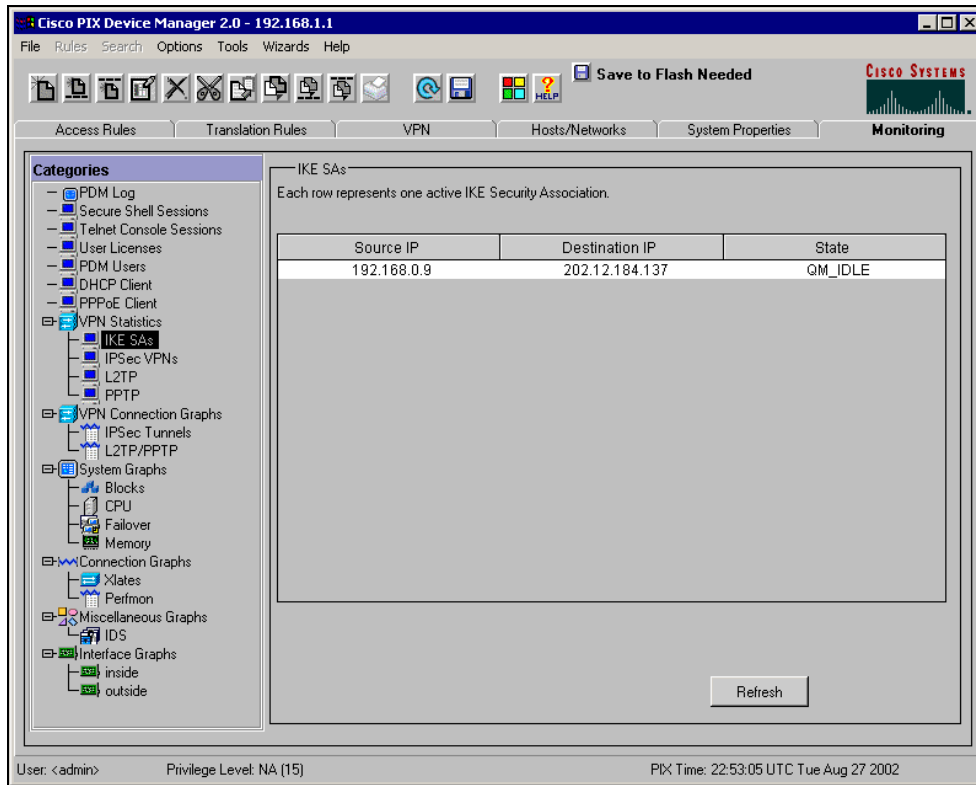
Type **cmd** and click .

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
Copyright 1985-2000 Microsoft Corp.
Z:\>ping 172.27.1.91
Pinging 172.27.1.91 with 32 bytes of data:
Reply from 172.27.1.91: bytes=32 time=3ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254
Reply from 172.27.1.91: bytes=32 time=2ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254
Ping statistics for 172.27.1.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
Z:\>
```

Type **ping 172.27.1.74**

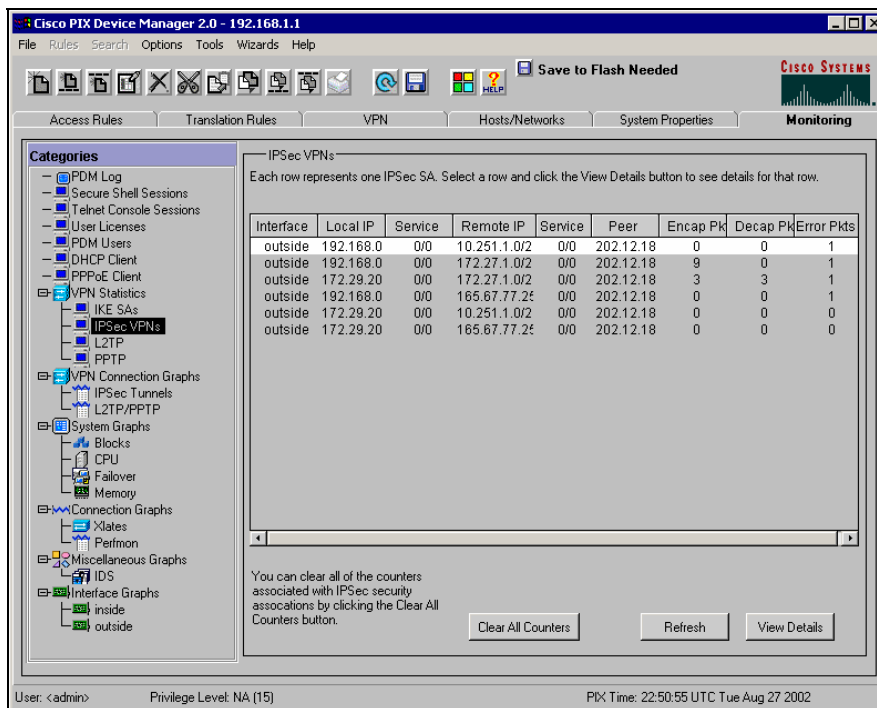
This should establish the VPN connection.

From the Cisco PIX Device Manager, select the Monitoring tab.



Select VPN Statistics, and IKE SAs.

Display of QM_IDLE indicates that ISAKMP tunnel is established.



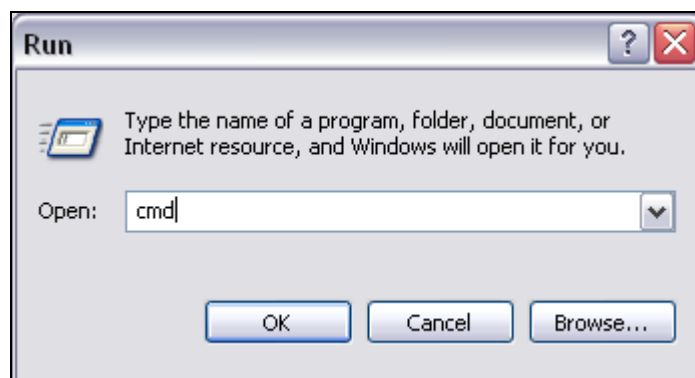
Select IPsec VPNs.


Entries on the screen indicate that the VPN tunnel is established.

5.1 Is the VPN Working Correctly?

To confirm that your VPN Access is working correctly:

Click **S**tart and **R**un.



Type **cmd** and click .

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
Copyright 1985-2000 Microsoft Corp.

Z:\>ping 172.27.1.91

Pinging 172.27.1.91 with 32 bytes of data:

Reply from 172.27.1.91: bytes=32 time=3ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254
Reply from 172.27.1.91: bytes=32 time=2ms TTL=254
Reply from 172.27.1.91: bytes=32 time=1ms TTL=254

Ping statistics for 172.27.1.91:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

Z:\>
```

Type ping **172.27.1.91**

If you see more than one line beginning with **Reply from...** appear on the screen, this indicates the vpn is responding and the test has been successful.

To perform a basic test to check access to web-based insurer products, perform the same test above, typing **ping 10.125.80.50**

Again, if you see more than one line beginning with **Reply from...** appear on the screen, this indicates access to web-based insurer products may be possible.

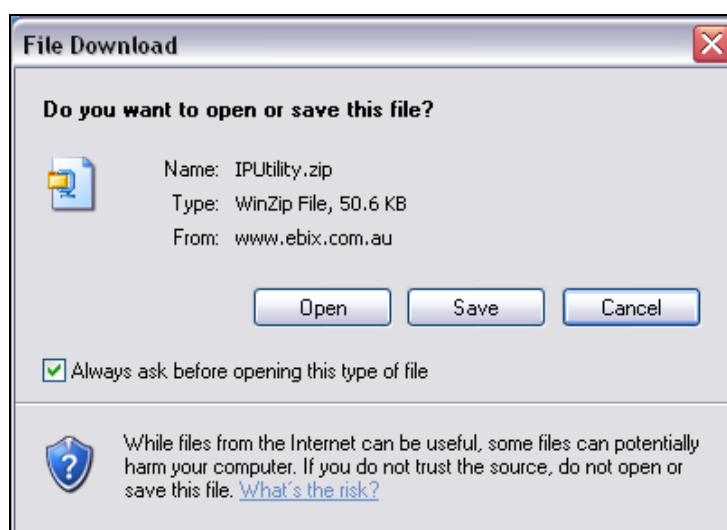
5.2 Testing your Sunrise™ Exchange Connection

Whilst the tests run in 5.1 prove that your VPN Connections is responding correctly, they do not necessarily prove that your PC can load the Sunrise™ Exchange insurer products.

To test that the products will load successfully, you will need to download a program called **IPUtility**.

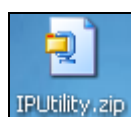
Click on the following link:

<http://www.ebix.com.au/files/zip/IPUtility.zip>

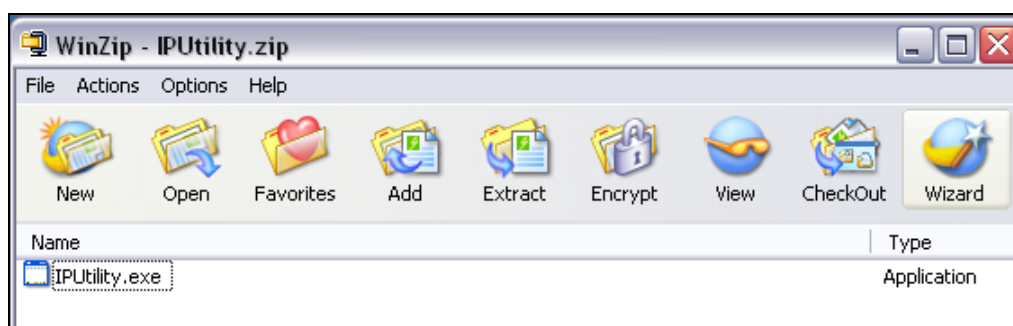


Click **Save** and save IPUtility.zip to a folder on your Desktop.

Double-click on **IPUtility.zip**.



WinZip will display



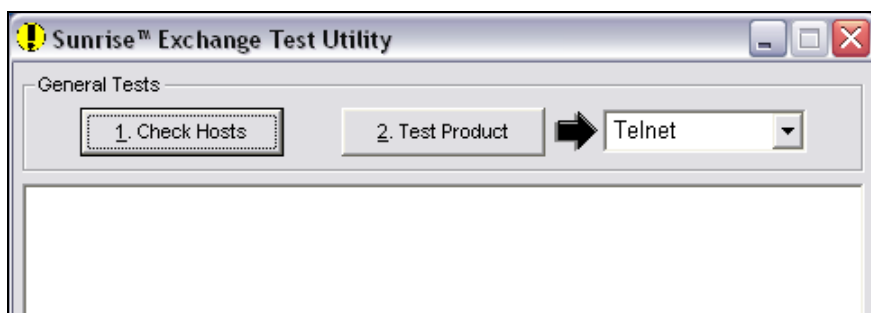
Highlight **IPUtility.exe** and click **E**xtract.

Select Desktop and click **E**xtract.

Double-click on **IPUtility.exe**.



The Sunrise™ Exchange Test Utility window will display



Please refer to the **Sunrise Exchange VPN Tests.pdf** for further instructions to run the Web Product Test.

A **No JVM Error** message indicates you will need to download and install Java. This download is available from <http://java.com/en/download/manual.jsp>.

Download and install the "Windows" file.

Re-run the IPUtility again and make sure it can now load the test product.

Note:

Please contact our Client Service Centre (CSC) on 1800 331 018 to run the Web Product Test and advise them of the successful completion of the installation of your VPN.

```
Installing to flash
```

```
Serial Number: 480380761 (0x1ca20759)
```

```
Activation Key: 760754d0 39f62229 a4a0245f b5b87e80
```

```
Do you want to enter a new activation key? [n]
```

```
Writing 1540152 bytes image into flash...
```

```
The PIX is now ready with Firmware
```

Reload the PIX 501 and type the following command in enable mode. It should display that it is ver 6.2.2 or later.

```
pixfirewall# sh ver
```

You need to update the PIX Device Manager, which provides the graphical interface to 2.0.2 or later.

You can enter the generic command and follow the prompts:

```
pixfirewall# copy tftp:192.168.1.2 pdm202.bin flash:pdm
```

Appendix B

Upgrade Notes from Cisco

The following sections are extracts from the CISCO web site (www.cisco.com) on procedures to upgrade the PIX501 firmware.

Entering Monitor Mode on a PIX 501, 506, 515, 525, 535

PIX devices that do not have an internal floppy drive come with a ROM boot monitor program that is used for upgrading the PIX Firewall's image. Follow the instructions below to enter monitor mode on these PIX devices.

Power cycle or reload the PIX. During boot-up you will be prompted to use BREAK or ESC to interrupt Flash boot. You have 10 seconds to interrupt the normal boot process.

Press the ESC key or send a BREAK character to enter monitor mode.

If you are using Windows HyperTerminal, you can press the ESC key or send a BREAK character by pressing **Ctrl+Break**.

If you are Telnetting through a terminal server to access the console port of the PIX, you will need to press **Ctrl]** to get to the Telnet command prompt. Then enter the **send break** command.

The **monitor>** prompt is displayed.

Proceed to [Upgrading the PIX Firewall from Boothelper or Monitor Mode](#).

Upgrading PIX Firewall from Boothelper or Monitor Mode

If you are upgrading your PIX Firewall from versions 5.0.x or earlier, to versions 5.1.x or later, you will need to use the boothelper, or monitor mode method for the upgrade. This is because before version 5.1, the PIX Firewall Software did not provide a way to TFTP an image directly into the Flash. Starting with PIX Firewall Software version 5.1, the **copy tftp flash** command was introduced to copy a new image directly into the PIX's Flash.

Note:

If you wish to change the PIX Firewall's activation key (to add an additional feature), you must install a new PIX image using the boothelper or monitor mode method. You cannot use the copy tftp flash method to change the activation key on the PIX Firewall.

Copy the PIX Firewall binary image (pix nnn .bin) to the root directory of the TFTP server.

For PIX Classic, 10000, 510 and 520s use the procedure for [Creating a Bootable Diskette](#). Use the boothelper file that most closely corresponds to the PIX image you are upgrading to. Boot the PIX from the boothelper floppy to enter the boothelper mode.

All other PIX devices (501, 506, 515, 525 and 535) do not contain a floppy drive; instead, they have an internal boot monitor mode. Please refer to instructions for [Entering Monitor Mode on a PIX 501, 506, 515, 525 or 535](#).

Once in monitor or boothelper mode, you can use the **?** key to see a list of available options.

```
Type interface number
```

The **interface** command specifies which PIX interface the TFTP server is connected out of. The default is interface 1 (inside).

Note:

The PIX Firewall cannot initialize a Gigabit Ethernet interface from monitor or boothelper mode. Use a Fast Ethernet or Token Ring interface instead.

```
address pix_interface_ip_address
```

The **address** command specifies the IP address of the PIX Firewall unit's interface.

```
server tftp_server_ip_address
```

The **server** command specifies the TFTP server's IP address.

```
file filename
```

The **file** command specifies the filename of the PIX Firewall image.

```
ping tftp_server_ip_address
```

Ping the server to verify accessibility. If this command fails, double-check your cables, IP address of the server and of the PIX, and IP address of the gateway (if needed). The pings must succeed before you can continue.

Note:

Use the gateway command to specify the IP address of a router gateway through which the server is accessible:

```
gateway ip_address of the gateway interface
```

Type **tftp** to start the download of image from the TFTP server.

After the image downloads, you are prompted to install the new image.

Enter **y** to install the image to Flash.

When prompted to enter a new activation key, enter **y** if you wish to enter a new activation key, or **n** to keep your existing activation key. See [Upgrading the Activation Key](#) for more information about the activation key and how to obtain a new one.

If you used the boothelper mode, you are prompted to remove the boothelper diskette. You have 30 seconds to remove the diskette before the PIX automatically reboots.

Please remove the diskette now. Once the PIX reboots it will load the new image from Flash.

This completes the upgrade process.

Once the PIX has been upgraded to 5.1 or later, it is no longer necessary to use a floppy diskette to load new images onto the PIX.

Starting with PIX Software version 5.1, the **copy tftp flash** command allows you to TFTP your new PIX image directly to the PIX from a TFTP server. Refer to the [PIX Command Reference](#) for further details.

Sample Upgrading the PIX Firewall from Boothelper or Monitor Mode

```
monitor> interface 1
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 0002.b945.a23c
monitor> address 172.18.124.154
address 172.18.124.154
monitor> server 172.18.125.3
server 172.18.125.3
monitor> file pix611.bin
file pix611.bin
monitor> ping 172.18.125.3
Sending 5, 100-byte 0xcde2 ICMP Echoes to 172.18.125.3, timeout is 4
seconds:
!!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp pix611.bin@172.18.125.3
Received 2562048 bytes
Cisco Secure PIX Firewall admin loader (3.0) #0: Tue Dec 517:35:46
PST 2000
System Flash=E28F128J3 @ 0xffff00000
BIOS Flash=am29f400b @ 0xd8000
Flash version 6.1.1, Install version 6.1.1
Do you wish to copy the install image into flash? [n] y
Installing to flash
Serial Number: 480380761 (0x1ca20759)
Activation Key: 760754d0 39f62229 a4a0245f b5b87e80
Do you want to enter a new activation key? [n] n
Writing 2469944 bytes image into flash...
```

Upgrading PIX Firewall from Version 5.1.1 or Later

If the PIX Firewall is running PIX Software versions 5.1.1 or later, you can use the **copy tftp flash** command to download a software image with TFTP. The **copy tftp flash** command can be used with any PIX Firewall model running PIX Software versions 5.1.1 or later. The image you download is made available to the PIX Firewall on the next reload (reboot). For more information on this command refer to the [PIX Command Reference](#).

Note:

If you wish to enter a new activation key into the PIX Firewall, you need to follow the instructions for [Upgrading the PIX Firewall from Boothelper or Monitor Mode](#).

Using the copy tftp flash Command to Upgrade the PIX

Copy the PIX Firewall binary image (pix nnn .bin) to the root directory of the TFTP server.

From the PIX prompt, issue the **copy tftp flash** command.

Enter the remote host IP address.

Enter the PIX binary filename (has the pix nnn .bin name format).

Type **yes**.

Sample Upgrading the PIX Firewall with the copy tftp flash Command

```

pixfirewall# copy tftp flash
Address or name of remote host [127.0.0.1]? 172.18.125.3
Source file name [cdisk]? pix611.bin
copying tftp://172.18.125.3/pix611.bin to flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 2562048 bytes.
Erasing current image.
Writing 2469944 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed.
pixfirewall#

```

Upgrading PIX Devices in a Failover Set with Minimal Downtime

To use this procedure, the PIX devices must be running PIX Software versions 5.1.x or later. These instructions are valid for all PIX devices that are capable of running in a failover set. For more information about failover, see [How Failover Works on the Cisco Secure PIX Firewall](#).

Two different options are listed below for upgrading your PIX with minimal downtime. The first option is the safest way to upgrade your failover set. If anything goes wrong

with the upgrade process, you would always have one operational PIX to pass your network traffic. The second option is simpler, but riskier. The risk resides in the possibility that the new image loaded on the PIX devices is corrupt in some way. Both options are presented so that you can choose the best method for your specific network.

Option 1

Copy the PIX Firewall binary image (*pixnnn.bin*) to the root directory of the TFTP server.

Power off the Primary (this causes the Secondary to become active).

Disconnect all cables from the Primary (including failover cable).

Power on the Primary and attach a PC with a TFTP server on it.

Use **copy tftp flash** to upgrade the Primary.

Reload the Primary and verify the new version and configuration.

Power off the Primary.

Reconnect all cables back to the Primary.

Quickly power off the Secondary, and then immediately power on the Primary (Your downtime will occur while the Primary is booting up).

Once the Primary is up, it will be active and passing traffic.

Repeat steps above for the Secondary PIX.

Power on the Secondary; it comes up as Standby.

Both PIX devices are now running the upgraded version and are back to normal operation.

Option 2

Copy the PIX Firewall binary image (*pixnnn.bin*) to the root directory of the TFTP server.

Use the **copy tftp flash** command to copy the new PIX image to the Primary PIX.

Use the **copy tftp flash** command to copy the new PIX image to the Secondary PIX.

Power off both PIX devices.

Power on the Primary PIX.

Wait 10 Seconds (to ensure that the Primary PIX becomes the Active PIX).

Power on the Secondary PIX. It will come up at Standby.

Both PIX devices are now running the upgraded version and are back to normal operation.

Upgrading the Activation Key

There are a couple of reasons that you may need to upgrade the activation key on your PIX.

- Your PIX does not currently have VPN-DES or VPN-3DES encryption enabled.

Note:

VPN-DES encryption must be enabled for you to manage your PIX using PIX Device Manager (PDM). [Registered](#) users may obtain a free 56-bit VPN-DES activation key by completing the [PIX 56-bit License Upgrade Key](#) form. VPN-3DES activation keys must be purchased through your local reseller or Cisco sales representative.

- Your PIX currently does not have failover activated.
- You are upgrading from a connection-based license to a feature-based license.

If you fall into one of the above categories and have obtained a new activation key for your PIX, the next step is to connect to your PIX, issue the **show version** command, and save the output to a text file. The output of the **show version** command contains your existing version, serial number, and activation key. You will need this information if there are any problems upgrading your activation key.

The PIX activation key based on the PIX's serial number and is therefore unique for each PIX. The activation key tells the PIX what features it is licensed for. The serial number of your PIX is saved in Flash, so if you replace the Flash card in your PIX, then your PIX will have a new serial number (different from the number shown on the sticker on the outside of the box). Always use the serial number displayed in the output of the **show version** command.

PIX Devices Running Versions 6.1 and Earlier

If your PIX is currently running version 6.1 or earlier, follow the instructions in [Upgrading the PIX Firewall from Boothelper or Monitor Mode](#).

PIX Devices Running Versions 6.2 and Later

If your PIX is currently running version 6.2 or later, use the **activation-key** command to change your activation key. See the [PIX Command Reference](#) for more information.

Sample Upgrading the Activation Key on a PIX Running Versions 6.2 or Later

```
pixfirewall(config)# activation-key 54bf4b80 b7237e20 05022c63 f09e3302
Updating flash...Done.
Serial Number: 480490644 (0x1ca3b494)
Flash Activation Key: 0x54bf4b80 0xb7237e20 0x05022c63 0xf09e3302
Licensed Features:
Failover:                Enabled
```

```
VPN-DES:           Enabled
VPN-3DES:          Enabled
Maximum Interfaces: 10
Cut-through Proxy: Enabled
Guards:            Enabled
URL-filtering:     Enabled
Inside Hosts:      Unlimited
Throughput:        Unlimited
IKE peers:         Unlimited

The flash activation key has been modified.
The flash activation key is now DIFFERENT from the running key.
The flash activation key will be used when the unit is reloaded.
pixfirewall(config)#
pixfirewall(config)#reload
```

Installing PDM

To install PDM:

Check the PIX Firewall software version running on your PIX Firewall unit. If your PIX Firewall is new and was shipped with PIX Firewall software version 6.0 or higher, then PDM should already be loaded into the Flash memory of your unit, and you can skip the next three steps.

Ensure that you have a TFTP server installed that you can use and that you meet all requirements listed in [Getting Started](#). For example, the PIX Firewall unit must be running PIX Firewall software version 6.0 or higher and have a DES or 3DES activation key to use PDM.

For information on installing and using TFTP, refer [Using a TFTP Server](#).

Set up your PIX Firewall hardware according to the directions provided with your unit.

Ensure that you have a Cisco Connection Online (CCO) account. You need a CCO username and password to download PDM software. If you do not have a CCO account, go to <http://www.cisco.com/register/>, click the word **REGISTER** on the menu bar, and follow the prompts presented.

You can download the PDM software from Cisco Connection Online or by FTP.

Caution:

Ensure that PIX Firewall software version 6.0 or higher is installed on your PIX Firewall before installing PDM. If you do not already have PIX Firewall software version 6.0 or higher installed, stop now and install this first; continue only after PIX Firewall software version 6.0 or higher is installed and running on your PIX Firewall. For Instructions on how to install PIX Firewall software refer [Cisco PIX Firewall Installation Guide](#).

Option 1

To install PDM from Cisco Connection Online (the Web):

Go to <http://www.cisco.com> using a web browser.

On the menu bar, click **LOGIN**.

Enter your CCO username and password and click **OK**.

Enter <http://www.cisco.com/cgi-bin/tablebuild.pl/pix> in the web address area of your web browser and press the **Return** or **Enter** key on your keyboard. (If you are prompted again for a username and password, enter your CCO username and password.)

Find the section titled "Select a File to Download" on the Cisco Secure PIX Firewall Software page (<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>), click **pdmnnn.bin** (where *nnn* represents the PDM software image version that you want to install) and follow the instructions presented.

Option 2

To install PDM using FTP:

Set your FTP client for passive mode.

Start your FTP client and connect to **cco.cisco.com**. Enter your CCO username and password when prompted.

Enter the command **cd cisco**.

Enter **cd internet** and then **cd pix** to access the PIX Firewall software directory.

Copy the **pdmnnn.bin** file (where *nnn* represents the PDM version) to a folder where it can be accessed from your TFTP server. (You can use the **ls** command to view the directory contents.)

To download PIX Firewall and PDM documentation, enter **cd documentation**, locate the .pdf files for the documents you want, and copy the files to your workstation. (Files with the .pdf file extension are viewed with Adobe Acrobat Reader, which is free and available at <http://www.adobe.com/prodindex/acrobat/readstep.html>.)

Enter **quit** to exit.

If you already have a console connection to your PIX Firewall unit, skip to the next step. Otherwise, use the following steps to set up a console connection:

Power off your PIX Firewall unit.

Connect the serial port of a Microsoft Windows workstation to the console port of the PIX Firewall with the serial cable supplied in the PIX Firewall accessory kit.

Power on the PIX Firewall unit. If a failover PIX Firewall unit is present, configure the primary unit first.

Locate the Windows **HyperTerminal** accessory by looking for it on the Windows **Start** menu. It is usually located under **Programs>Accessories>Communications>HyperTerminal**.

Click **HyperTerminal** to open the **New Connection** window; the **Connection Description** dialog box appears in the center of the window.

Enter a name for the connection and click **OK**.

In the **Connect To** dialog box, do not enter an area code or phone number. Leave these boxes blank.

Select **Direct to Com 1** in the **Connect using** field (unless you are using another serial port to connect) and click **OK**.

Next, set the values in the following table:

Field Name	Value to Set
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Click **OK** to continue.

The HyperTerminal window is now ready to receive information from the PIX Firewall console. Wait 30 seconds for the PIX Firewall startup messages to display. These messages should appear similar to the following:

```
booting....
PhoenixPICOBIOS 4.0 version 6.0
Copyright 1985-1998 ABC Technologies Ltd.
All Rights Reserved
Build Time:04/27/01 17:08:34
Polaris BIOS Version 0.09
CPU = Pentium with MMX 600 MHz
640K System RAM Passed
63M Extended RAM Passed
```

```
0512K Cache SRAM Passed
System BIOS shadowed
limit segment address:EFE5
Cisco Secure PIX Firewall BIOS (4.0) #0:Mon Sep 13 13:28:49 PDT 2000
Platform PIX-515
Flash=i28F640J5 @ 0x300
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 2011648 bytes of image from flash.
64MB RAM
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xffffd8000
mcwa i82559 Ethernet at irq 11  MAC:00aa.0000.000f
mcwa i82559 Ethernet at irq 10  MAC:00aa.0000.0010
```

If it takes more than a minute for the PIX Firewall command prompt to appear, press the **Enter** key. If it still does not appear, power off the PIX Firewall and ensure that the serial cable is attached to COM1 and not to COM2, if your computer is so equipped. Power the PIX Firewall back on and try to connect again.

If garbage characters appear, reset the **Bits per second** to 9600 and try to connect again.

If your PIX Firewall unit is being run for the first time, enter the **enable** command. When prompted, enter the enable password if there is one.

Start your TFTP server. If you need to obtain a TFTP server or more information on using one, refer to [Using a TFTP Server](#).

Determine the IP address of the computer running the TFTP server. If you are not sure how to do this, refer to [Determining the IP Address of Your TFTP Server](#) in [Using a TFTP Server](#).

Load the PDM image file into the PIX Firewall by entering the following at the command prompt:

```
pixfirewall# copy tftp://Your_TFTP_Server_IP_Address/Your_pdmfile_name
flash:pdm
```

Or you can enter the generic command and follow the prompts:

```
pixfirewall# copy tftp flash:pdm
```

Enter configuration mode by entering the following at the command prompt:

```
pixfirewall# configure terminal
pixfirewall (config)#
```