AlliedWare™ OS

# How To | Create a VPN between an Allied Telesis Router and a Cisco PIX Firewall

## Introduction

Today's network managers often need to incorporate other vendors' equipment into their networks, as companies change and grow. To support this challenge, Allied Telesis routers are designed to inter-operate with a wide range of equipment.

This How To Note details one of the inter-operation solutions from Allied Telesis: creating virtual private networks between Allied Telesis routers and Cisco PIX firewalls. It shows you how to configure a VPN between a local Allied Telesis router and a remote Cisco PIX firewall, step-by-step. On the Allied Telesis router, it uses the Site-To-Site VPN wizard for the VPN configuration.

The wizard runs on selected AR400 Allied Telesis routers from the router's web-based GUI (graphical user interface). It asks you to enter a few details and from those it configures the following settings:

- encryption to protect traffic over the VPN
- ISAKMP with a preshared key to manage the VPN
- the firewall, to protect the LANs and to allow traffic to use the VPN
- Network Address Translation (NAT), so that you can access the Internet from the private LAN through a single public IP address. This Internet access does not interfere with the VPN solution.

You can use the command line to set up an equivalent configuration on AR700 and other AR400 Series routers. See "The Allied Telesis router command script" on page 31 for a complete list of the commands the configuration uses.

## What information will you find in this document?

This How To Note begins with the following information:



Then it describes the configuration, in the following sections:



## Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

## Which products and software version does it apply to?

The VPN wizard is available on the following Allied Telesis routers, running Software Version 2.9.1 or later:

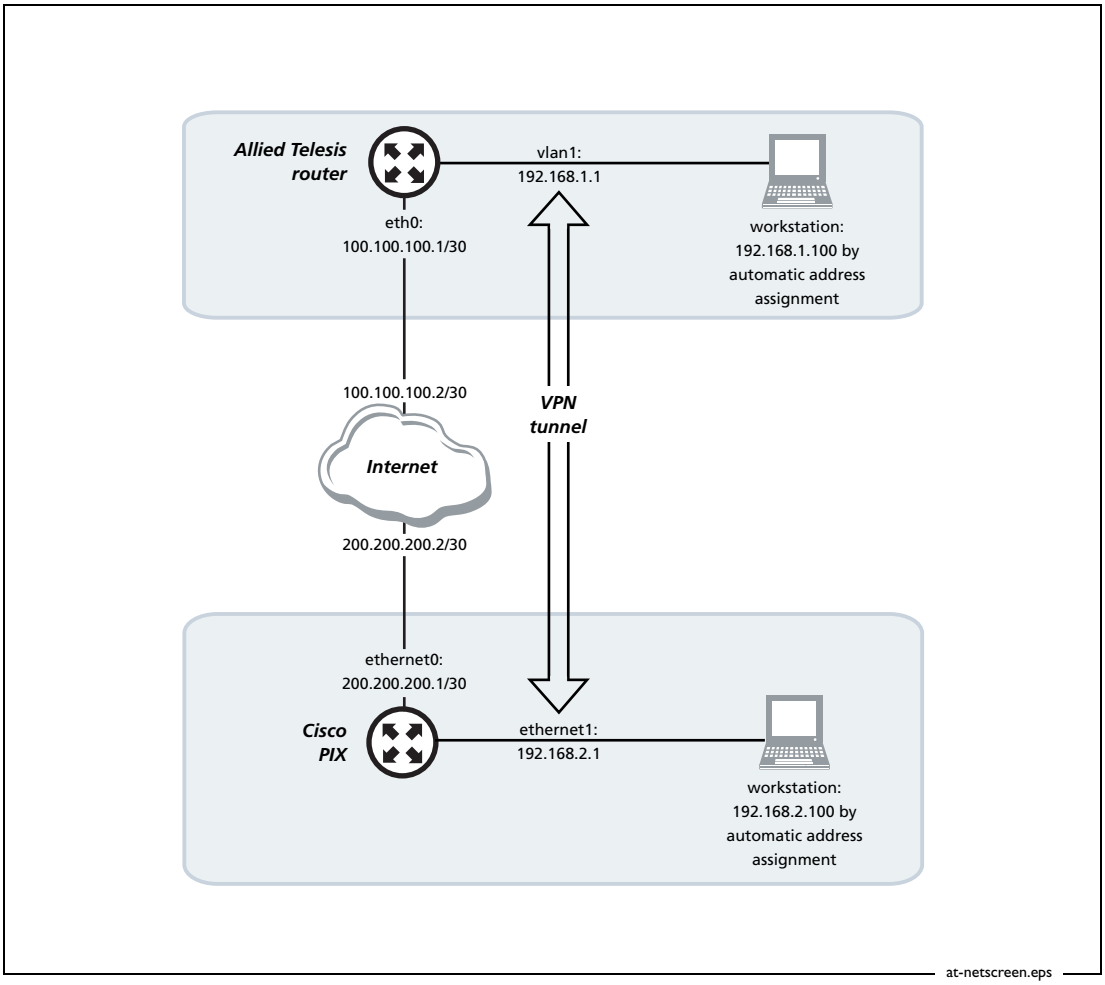
- AR415S
- AR440S, AR441S, AR442S

You can use the command line to set up an equivalent configuration on AR700 and other AR400 Series routers. See "The Allied Telesis router command script" on page 31 for a complete list of the commands that the configuration uses.

We created this example with Cisco PIX Firewall Version 6.3(5).

# The network

The following diagram shows the LANs used in this How To Note's example, and their interfaces and addresses.



# How to configure the Allied Telesis router

**Before you start**

1. Access the router via its GUI.
2. Customise the router and set up vlan1 as the LAN interface. The site-to-site VPN wizard always uses vlan1 as the local LAN for the VPN connection, so you must make sure an IP interface is configured on vlan1 before running the wizard.
3. Create a security officer. If you use the Basic Setup wizard to customise the router, this creates one security officer, with a username of "secoff".
4. Set up the WAN interface appropriately for your connection type. This example shows the steps for a fixed IP address on the WAN interface (as in the figure above).

The router setup of steps 1-4 is described in *How To Use the Allied Telesis GUI to Customise the Router and Set Up An Internet Connection*, which is available from www.alliedtelesis.com/resources/literature/howto.aspx.

In this example, the Allied Telesis router has the following settings:

| | Interface | Address | Mask |
|---|---|---|---|
| Allied Telesis router LAN | vlan1 | 192.168.1.1 | 255.255.255.0 |
| Allied Telesis router WAN | eth0 | 100.100.100.1 | 255.255.255.252 |
| Remote site's WAN settings | | 200.200.200.1 | |
| Remote site's LAN settings | | 192.168.2.1 | 255.255.255.0 |

**Create the VPN tunnel**

### 1. Open the Configuration Wizards page

Log in as either the manager or the security officer. If you log in as the manager, the router changes to secure mode when you finish the VPN wizard and at that stage prompts you to log in again as the security officer.

The Site-To-Site VPN wizard is one of the options on the GUI's Configuration Wizards page. Make sure your browser's pop-up blocker is disabled—the wizard needs to open pop-ups. If you access the Internet through a proxy server, make sure your browser bypasses the proxy for this address.

## Bypass the proxy for the Allied Telesis Router GUI management IP address

If you access the Internet through a proxy, you need to bypass the proxy when browsing to the Allied Telesis router. To do this:

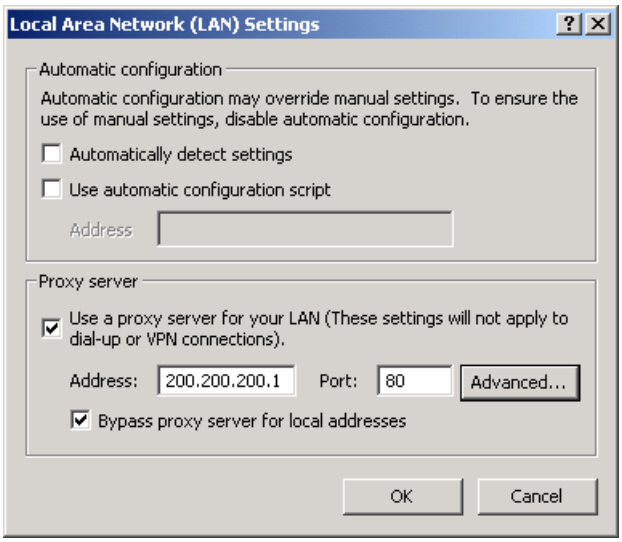
### 1. Open your browser

### 2. Open the browser's options

Use the browser's Tools menu to open its options window. In IE 7, this is called Internet Options.

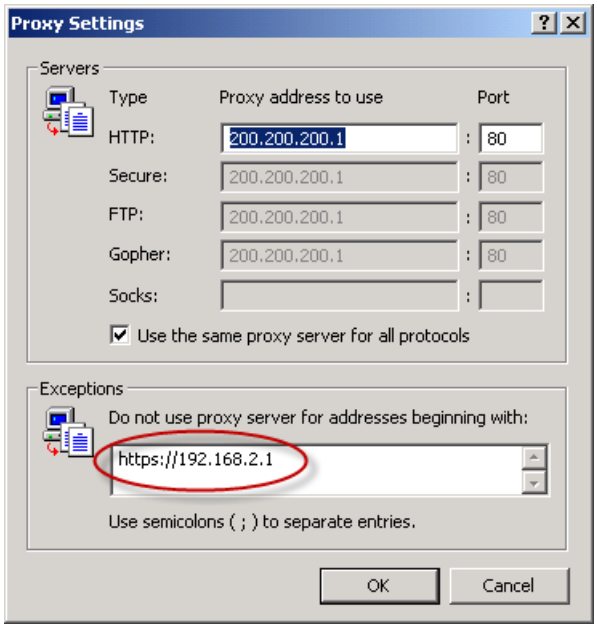
### 3. Edit the proxy settings

Go to the connection settings for the LAN. To do this in IE 7, click the **Connections** tab, then the **LAN** settings button. This opens the following window.

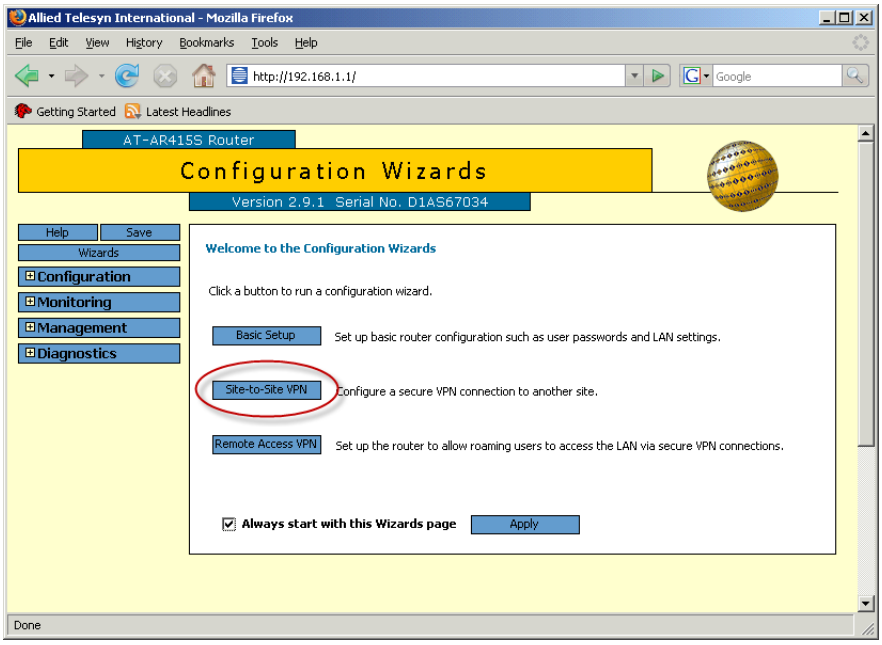



Go to the proxy settings. To do this in IE 7, click the **Advanced** button.

Enter the **Allied Telesis Router** address in the **Exceptions** section.



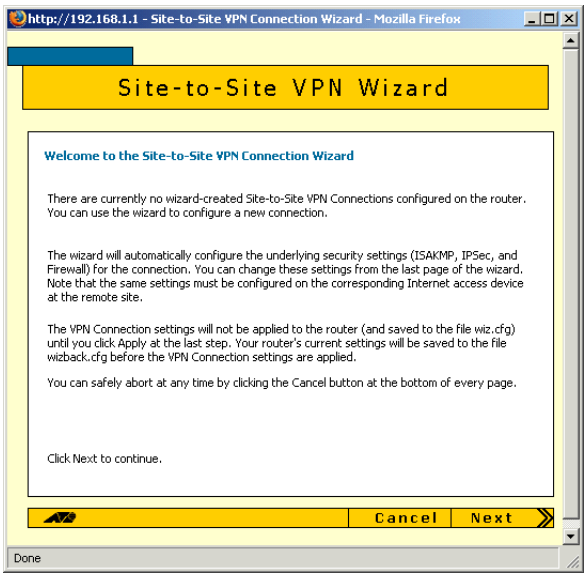

## 4. Browse to the Allied Telesis Router GUI address and log in




The GUI opens at this page the first time you configure your router. After initial configuration it may open at the System Status page instead. If so, click on the **Wizards** button in the left-hand menu to open the **Configuration Wizards** page.

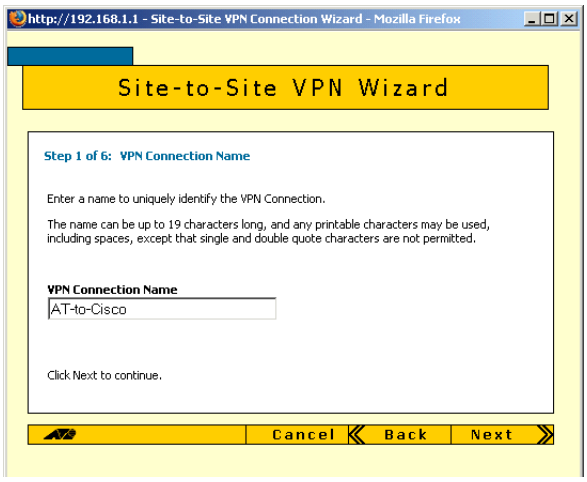
Click on the **Site-to-Site VPN** button.

## 5. Start the Site-to-Site VPN Wizard




The wizard starts by displaying a welcome message.

## 6. Name the VPN connection

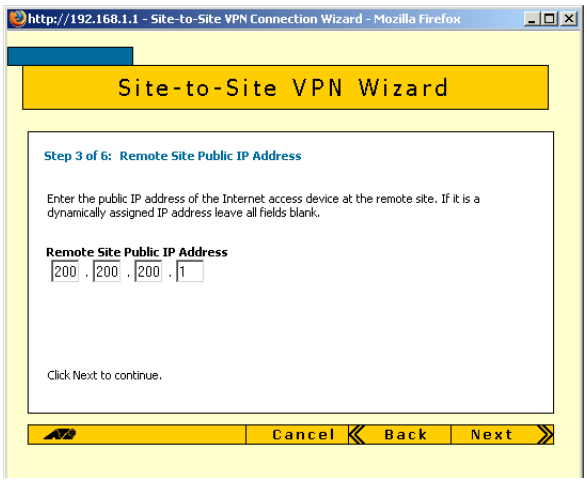



Enter an appropriate **VPN Connection Name**.

Click **Next**.

If you have multiple possible WAN interfaces configured on the router, the wizard allows you to select the appropriate interface. In this example there is only one WAN interface, so the wizard selects it automatically and moves directly to the remote site settings.

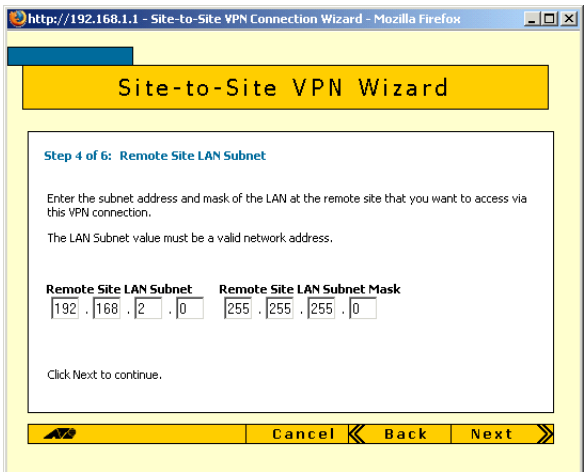
## 7. Enter the remote site's WAN IP address




Enter the public IP address of the other end of the tunnel. In this example, this is 200.200.200.1

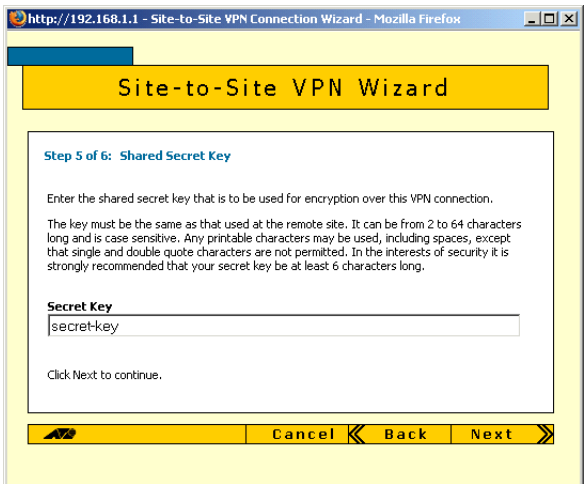
Note that you can use the Tab key to move between fields when entering the address, but you should not use the. key (the period).

## 8. Enter the remote site's LAN IP address



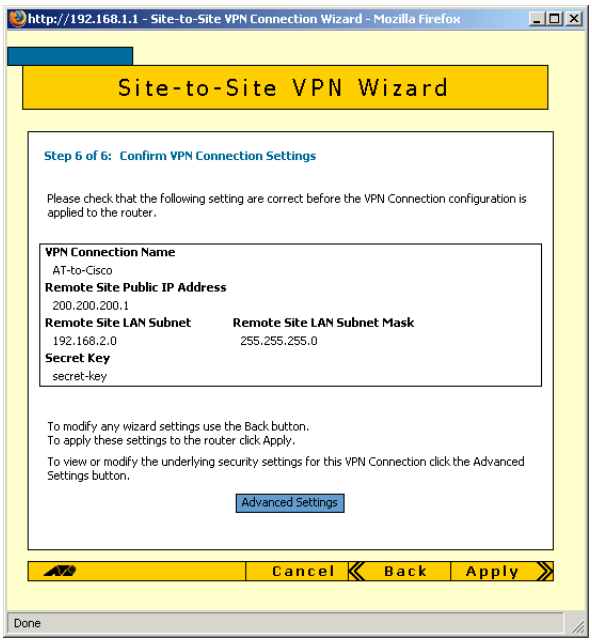

Enter the **Cisco PIX firewall's LAN subnet address and mask**. In this example, this is 192.168.2.0 and a mask of 255.255.255.0.

## 9. Enter the shared secret key




Enter the secret key, which is an alphanumeric string between 2 and 64 characters long. Both routers must use the same secret key. On the Cisco PIX firewall, this is the **Preshared Key**.

## 10. Check the settings

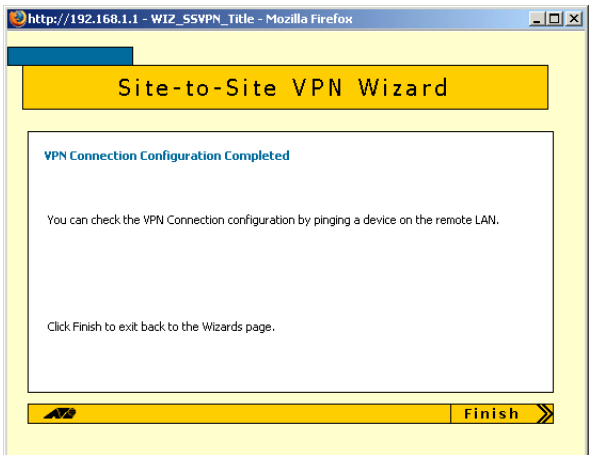



Check the summary. If necessary, use the wizard's Back button to return and correct any settings you want to change.

Once you are happy with the settings, click **Apply**.

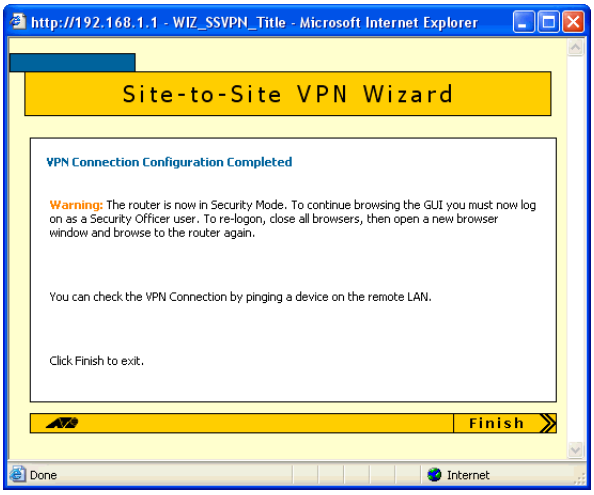
## 11. Finish the wizard

**Security officer**



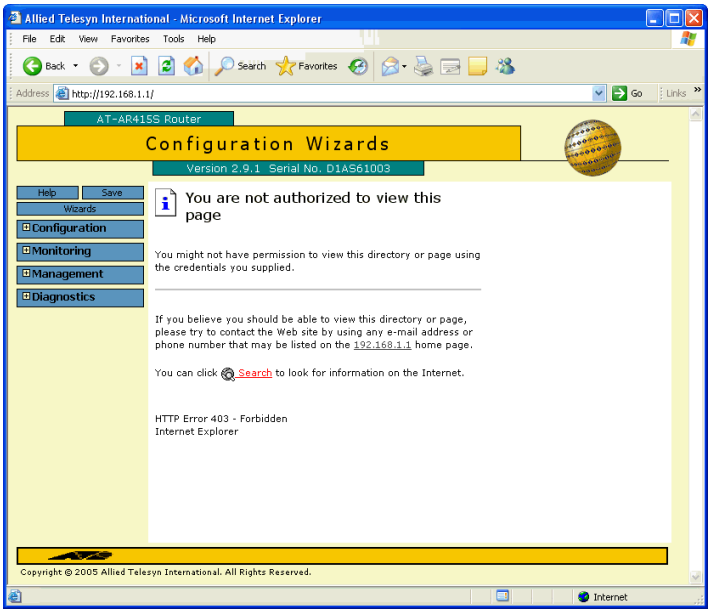

If you are logged in as the security officer, the GUI displays a completion message. Click **Finish** to end the Wizard and save the VPN settings.

**Manager**

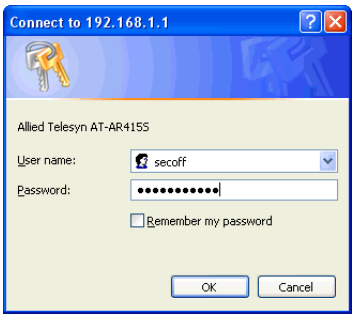



If you are logged in as manager, the GUI displays a message to warn you that you will need to close your browser and re-login as a security officer (see below) once you have finished the wizard.

Click **Finish** to end the Wizard and save the VPN settings. The browser now indicates that you no longer have permission to view the GUI.




This error message occurs because you now need to log in as a security officer.




The router configuration is now complete. If required, you can log in to the router again for further configuration or monitoring. To do this, close your browser, open it again, and browse to the router's IP address.

If you used the Basic Setup wizard to configure the LAN settings, the router will have one security officer, with a username of "secoff".

Login as the security officer.

# Configuring the Cisco PIX

To configure the Cisco PIX, perform the steps in the following sections:

1. "Accessing the Cisco PIX" on page 12
2. "Run the startup wizard" on page 17
3. "Run the VPN wizard" on page 23

## Accessing the Cisco PIX

Before using the PIX GUI for configuration you may need to access the PIX console for initial configuration, so you can reset a few things.

### 1. Configure the PIX console for initial setup

- You will need to connect to the PIX console port using a terminal program such as Hyperterm or Teraterm, at port baud rate 9600 bps. Connect power to the PIX and you should see a Start Up sequence.
- Enter 'enable' at the final prompt to reach privilege exec mode. A password may be required. If you do not know the password, then you will need to follow the Password recover procedure for PIX. Refer to http://www.cisco.com/application/pdf/paws/8529/34.pdf

Enter the command: **write erase**

```
pixfirewall# write erase
```

- The PIX displays a confirmation request. Press **Enter** to confirm.

```
Erase PIX configuration in flash memory? [confirm]
```

### 2. Reboot the PIX

Enter the command: **reload**

```
pixfirewall# reload
```

The PIX displays a confirmation request. Press **Enter** to confirm.

```
Proceed with reload? [confirm]
```

### Pre-configure the PIX

When the PIX boots up, it prompts you to give it a password and IP address for the PIX Device Manager (PDM) and some other settings. After this, you will be able to use the PDM to configure the PIX, by browsing to its IP address. Note that this is called the **Inside IP address** in the pre-configuration dialog.

The following output is an example of this pre-configuration dialog.

```
Pre-configure PIX Firewall now through interactive prompts [yes]?
Cannot select private keyyes
Enable password [<use current password>]: friend
Clock (UTC):
  Year [2007]:
  Month [Mar]:
  Day [20]:
  Time [18:27:07]: 17:32:00
Inside IP address: 192.168.2.1
Inside network mask: 255.255.255.0
Host name: ciscopix
Domain name: alliedtelesis.com
IP address of host running PIX Device Manager: 192.168.2.2

The following configuration will be used:
Enable password: friend
Clock (UTC): 17:32:00 Mar 20 2007
Inside IP address: 192.168.2.1
Inside network mask: 255.255.255.0
Host name: ciscopix
Domain name: alliedtelesis.com
IP address of host running PIX Device Manager: 192.168.2.2

Use this configuration and write to flash? yes
Building configuration...
Cryptochecksum: adf3a755 dec019c1 8378c3df 771a70d2
[OK]

Type help or '?' for a list of available commands.
ciscopix>
```

## Bypass the proxy for the PIX management IP address

If you access the Internet through a proxy, you need to bypass the proxy when browsing to the PIX Device Manager. To do this:

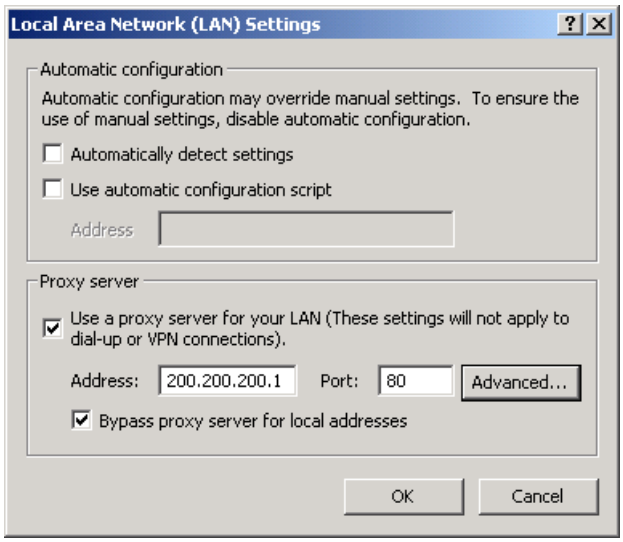
1. Open your browser

2. Open the browser's options

Use the browser's Tools menu to open its options window. In IE 7, this is called Internet Options.

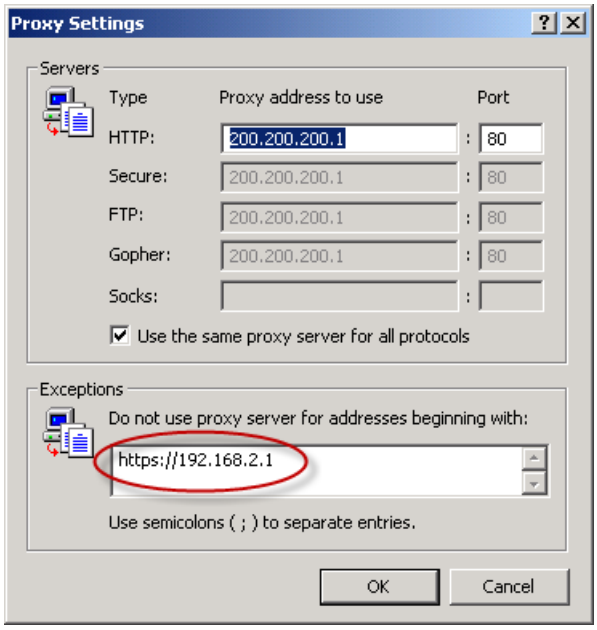
## 3. If necessary, edit the proxy settings

Go to the connection settings for the LAN. To do this in IE 7, click the **Connections** tab, then the **LAN** settings button. This opens the following window.




Go to the proxy settings. To do this in IE 7, click the **Advanced** button.

Enter the PDM address in the **Exceptions** section.

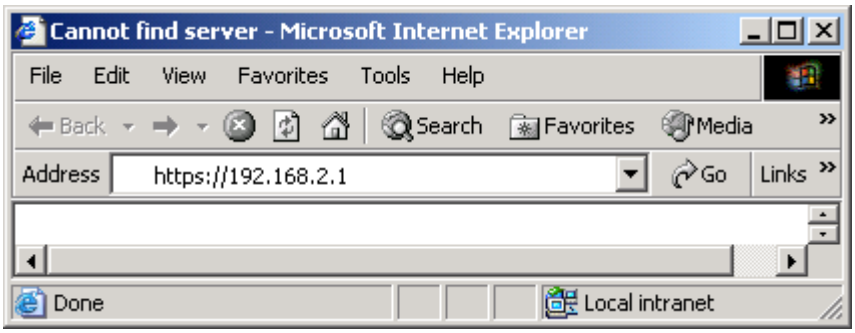


## Browse to the PIX IP address and log in

This section describes how to access the PIX Device Manager (PDM), to configure the PIX.

### 1. Browse to the management address

First, browse to the management address. Note that it is a secure HTTPS address.

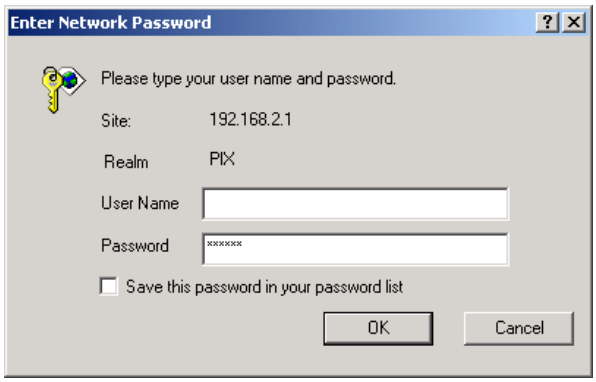



### 2. Accept the certificate

Secure HTTPS addresses require a certificate to be accepted, so click the **Yes** button at the Security Alert.

## 3. Log in

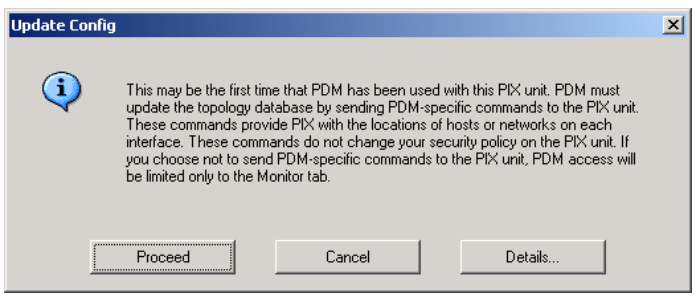
Log in. Note that you do not need a **User Name**. The password is the **Enable password** that you set during the pre-configuration stage.




The PDM starts up.


## 4. Allow PDM to update the topology database

If necessary, PDM will display the following dialog box. Click **Proceed**.



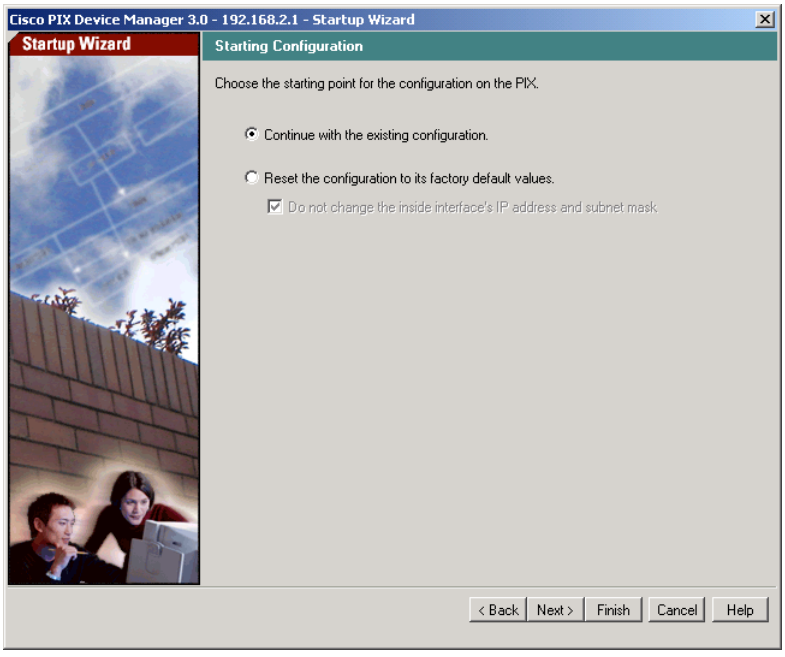
# Run the startup wizard

## 1. Start the startup wizard

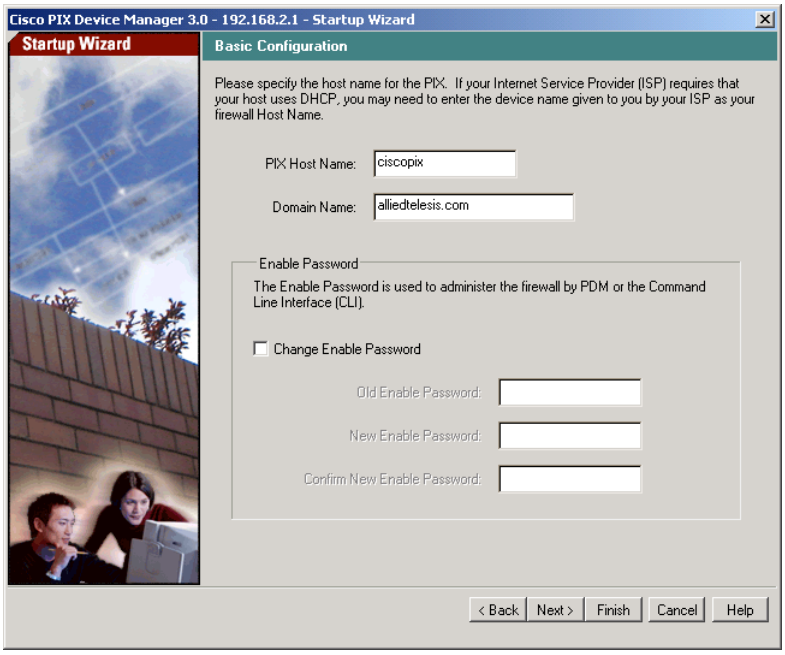
From the Wizards menu, select **Startup Wizard**. The wizard's welcome page displays.


## 2. Choose whether or not to reset the configuration

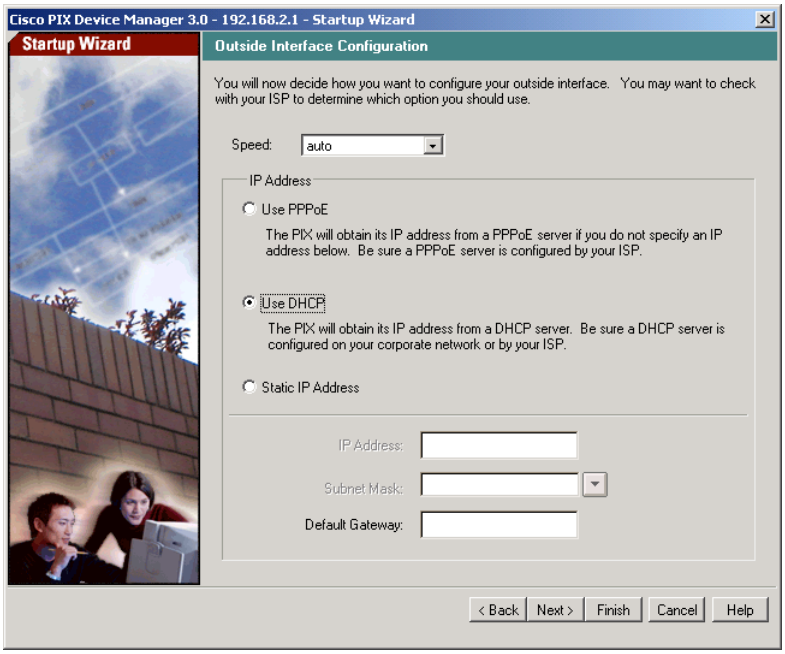
We reset the configuration from the command line, so we do not want to reset it again.



## 3. Enter a name for the PIX and a domain name

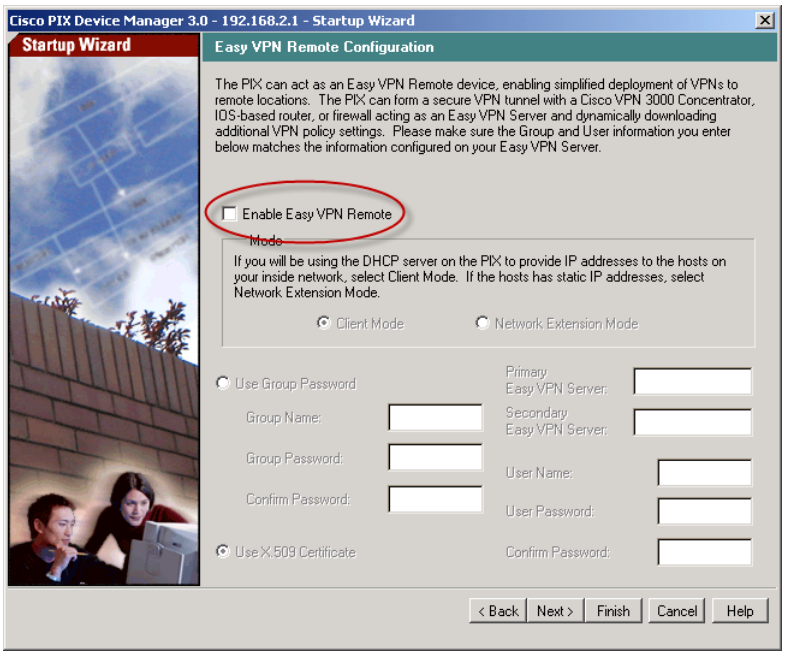



## 4. Specify how the PIX gets its public address from your ISP



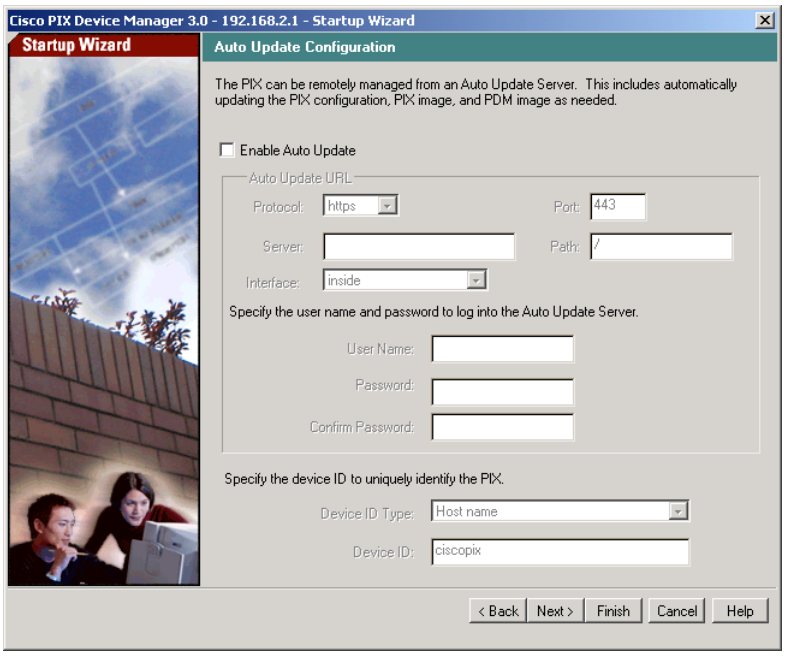
## 5. Do not enable Easy VPN Remote

You cannot use Easy VPN Remote when interoperating with an Allied Telesis router, so make sure that the **Enable Easy VPN Remote** checkbox is **not** selected.



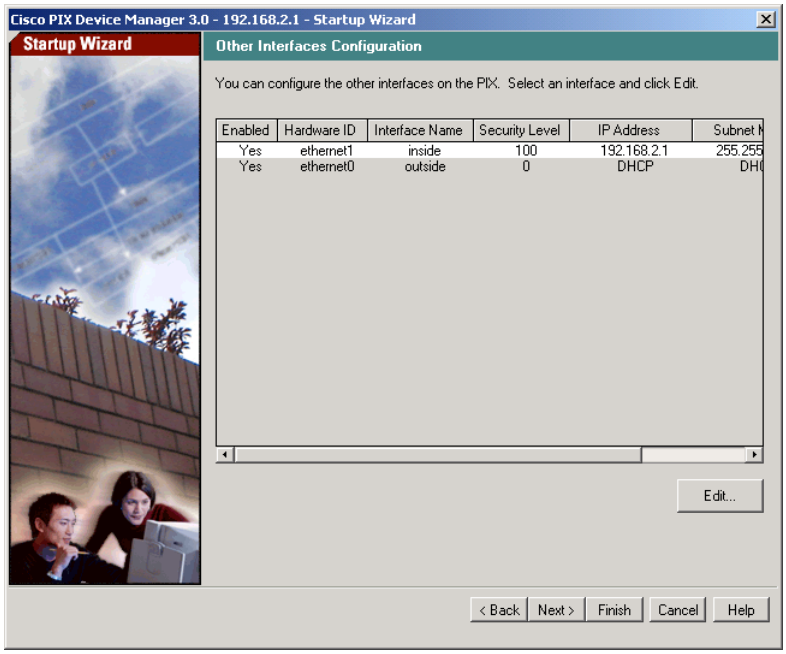

## 6. Configure the Auto Update Server settings, if desired

In this example, we did not use the Auto Update Server.



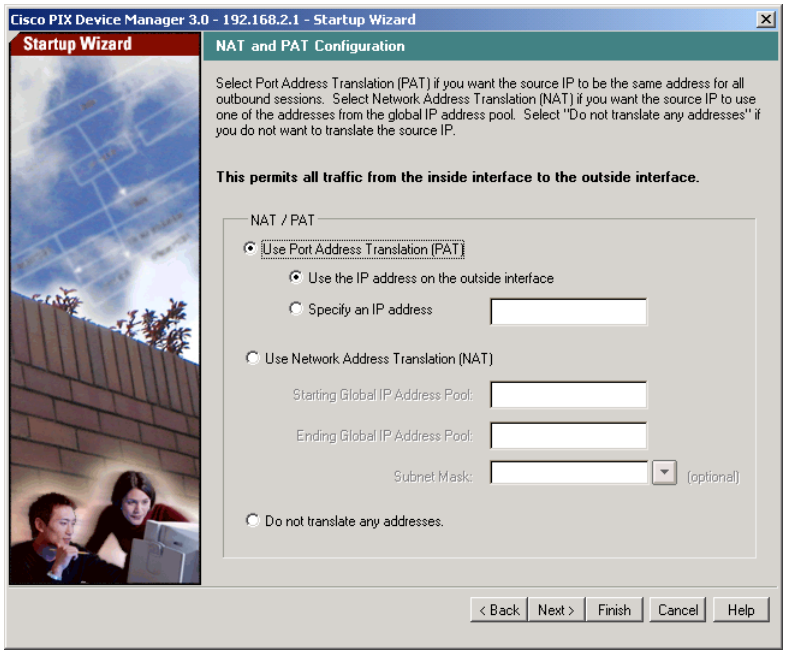
## 7. Edit the interfaces, if necessary

Unless you need to edit an interface, click **Next**.



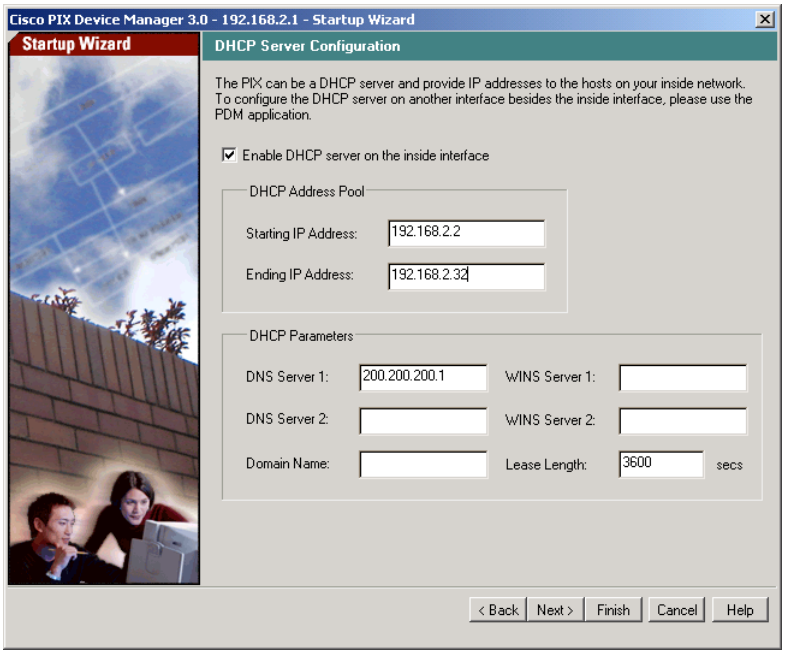

## 8. Set up NAT or PAT

Set up Enhanced NAT, or Network Address and Port Translation (PAT). We used **PAT**.

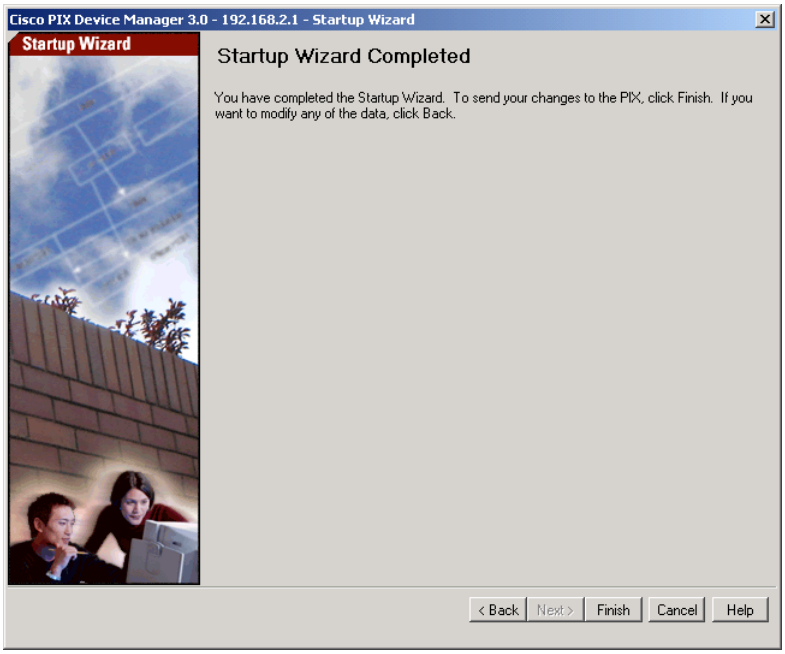


## 9. Configure the DHCP server, if desired

The PIX can act as a DHCP server for clients on the private LAN side.

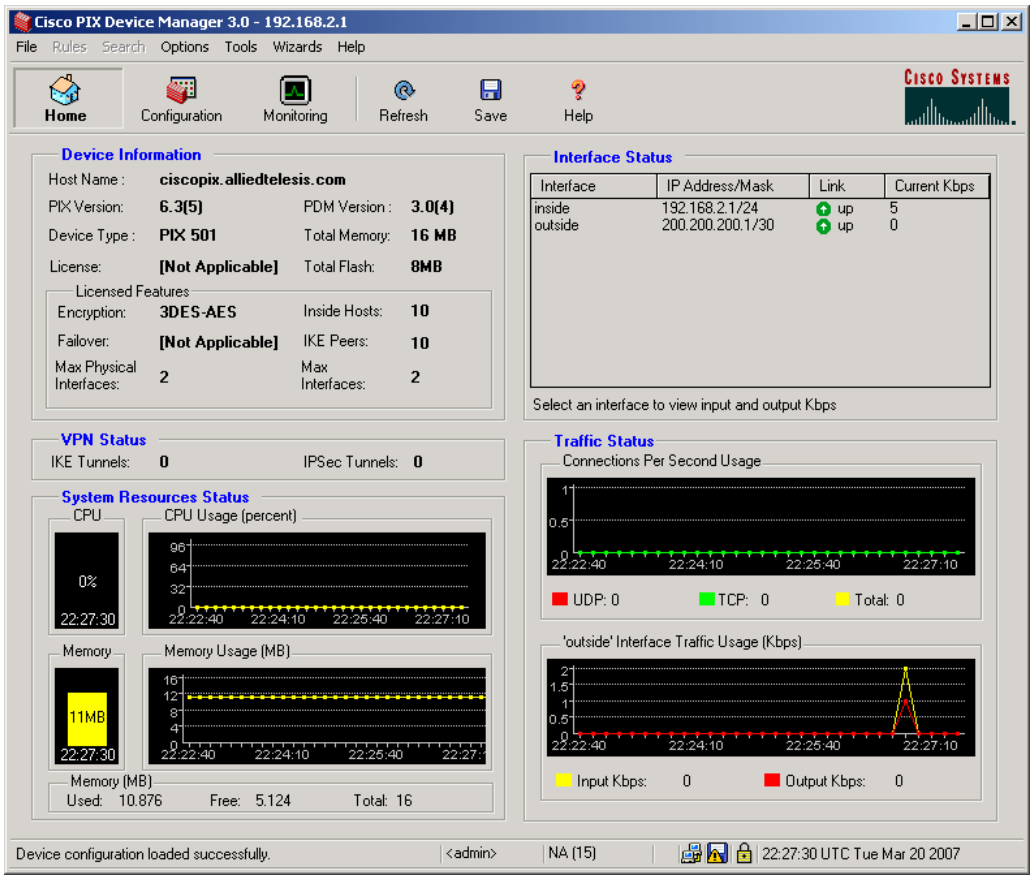



## 10. Complete the wizard



## 11. Check the PIX status

The following screenshot of the PDM's Home summary status page shows the PIX status after completion of the general setup wizard.

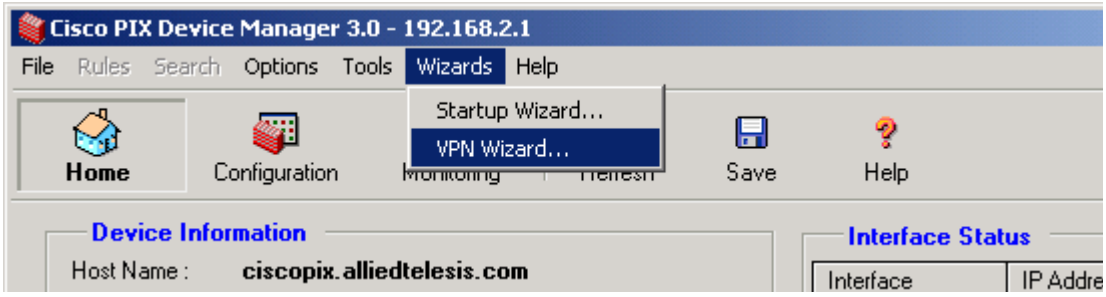


# Run the VPN wizard

This section describes how to set up the VPN to inter-operate with the Allied Telesis router.

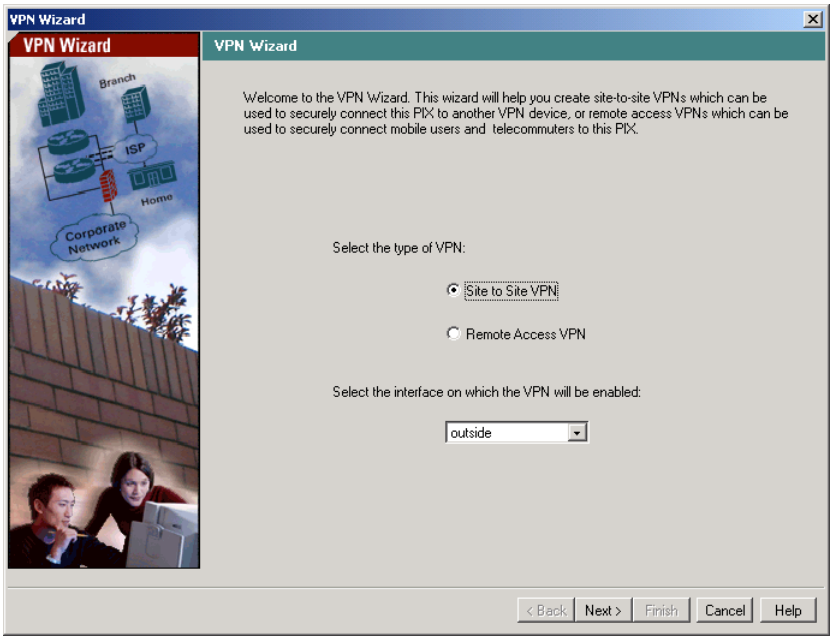
## 1. Start the VPN wizard

Open the VPN wizard by selecting **VPN Wizard** from the **Wizards** menu.



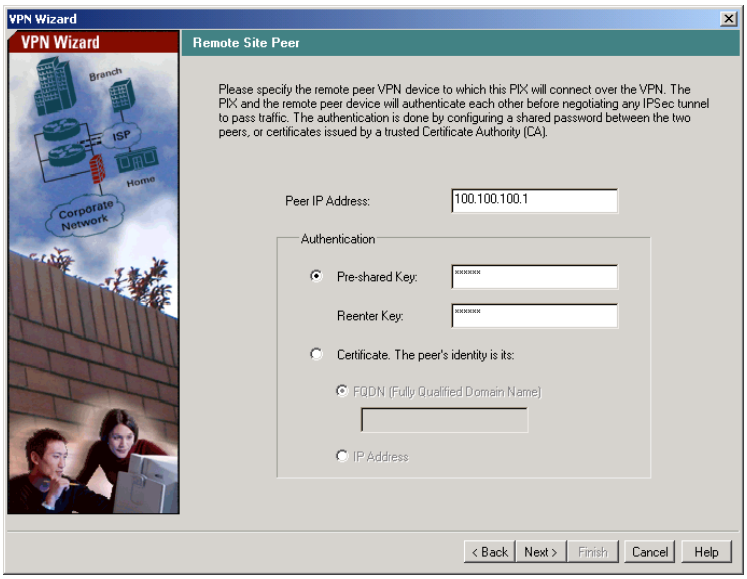

## 2. Select Site to Site VPN

This example is a **Site to Site VPN** because it is connecting to a remote site VPN running on an Allied Telesis device.



## 3. Enter the Allied Telesis router's details

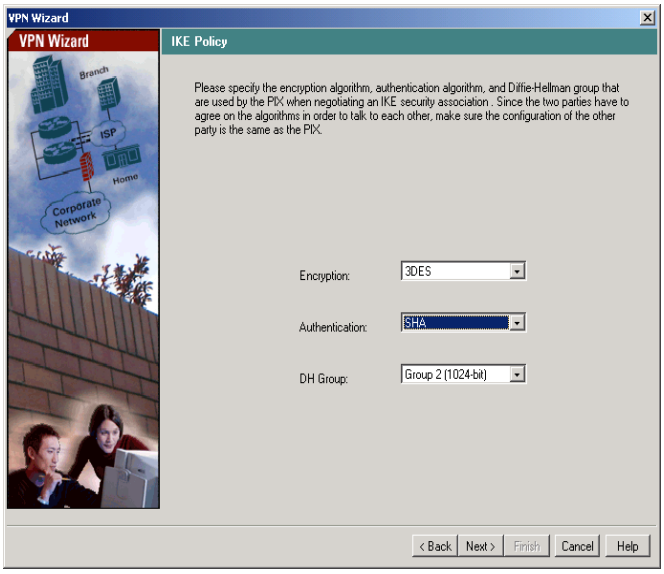
Enter the Allied Telesis router's IP address, and the secret key that is shared by both routers. The IP address is the router's WAN interface address. The key is an alphanumeric string between 2 and 64 characters long. On the Allied Telesis router, this is the **shared secret key**.




## 4. Specify the IKE settings

The IKE settings for inter-operation with an Allied Telesis router are:

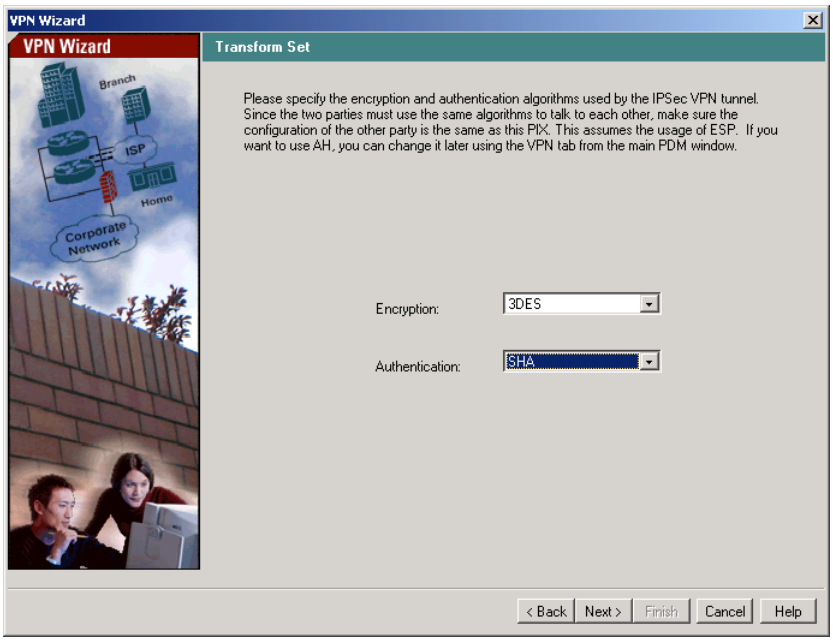
| | |
|---|---|
| Encryption: | 3DES |
| Authentication: | SHA |
| DH Group: | Group 2 (1024-bit) |



## 5. Specify the transform set

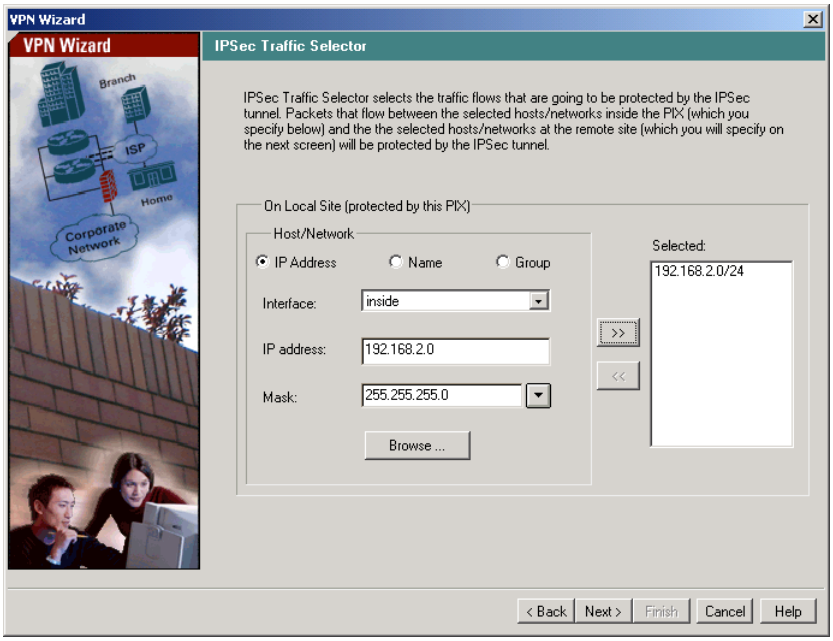
The transform set for inter-operation with an Allied Telesis router is:

Encryption: 3DES
Authentication: SHA




## 6. Specify the VPN traffic's subnet at the PIX end (Local LAN)

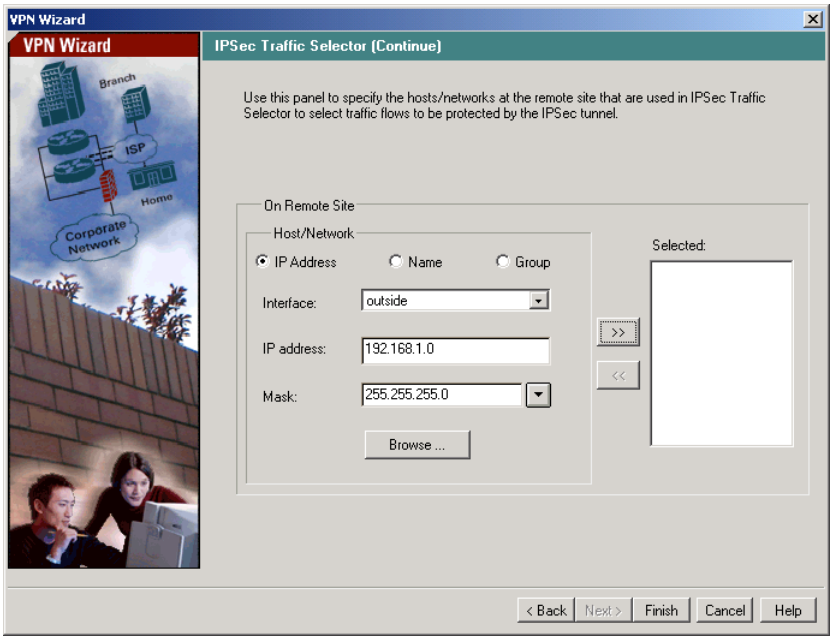
From the **Interface** dropdown box select **inside**, then to select this address, click the right-pointing arrow. The address is displayed in the **Selected** field, as shown in the following screenshot.



## 7. Specify the VPN traffic's subnet at the Allied Telesis router's end (Remote LAN)

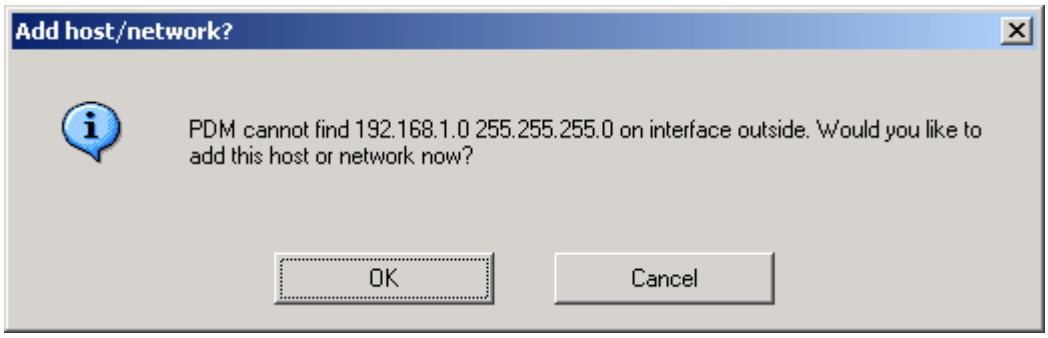
Fill in the IP address and mask for the Allied Telesis peer. Then select that address by clicking the right-pointing arrow.

Click **Finish**.

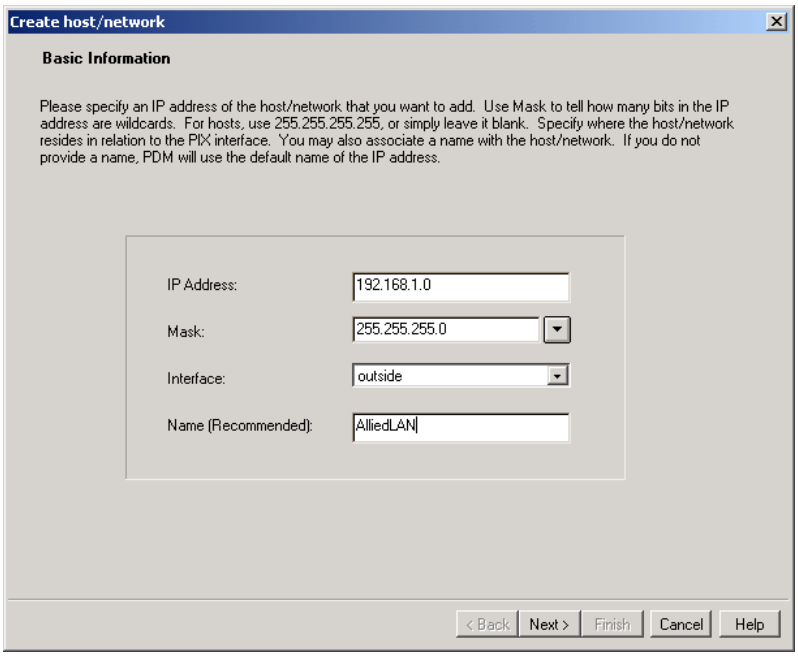



## 8. Set up a route to the remote LAN

The PDM displays a dialog box because it does not have a route to the remote VPN LAN. Therefore, you need to divert to the Create Network wizard to set up a route. To do this, click **OK**.

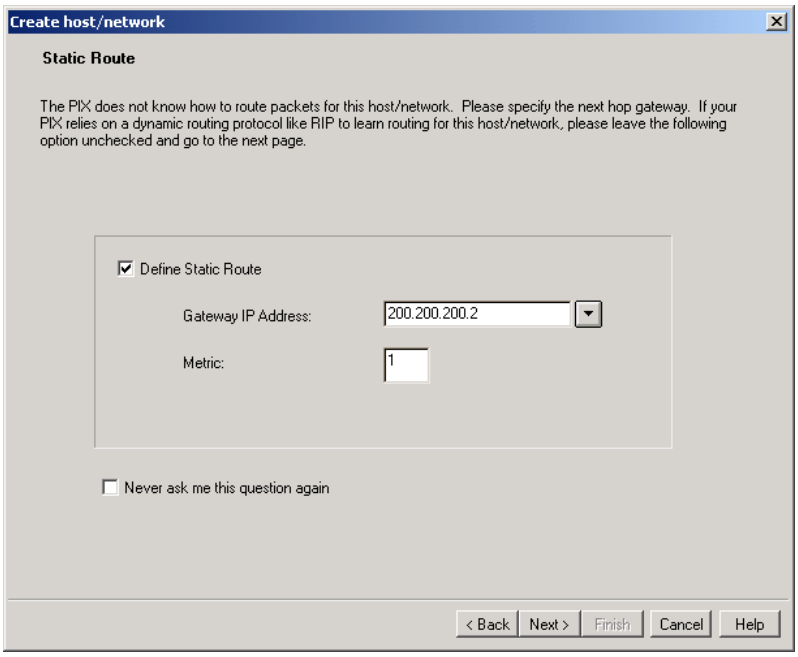


## 9. Specify a name for the remote LAN

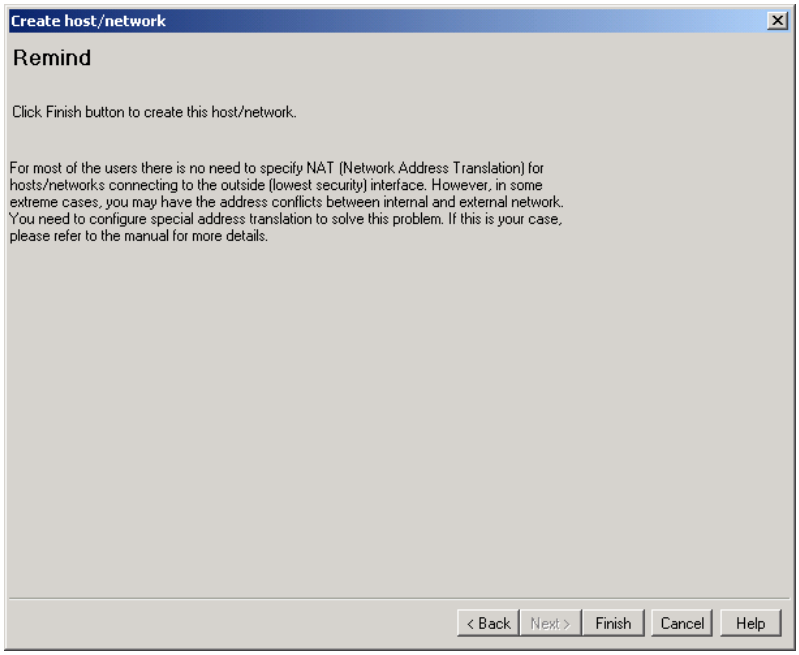



## 10. Specify the next hop

The next hop is the **Gateway IP Address** at the ISP.

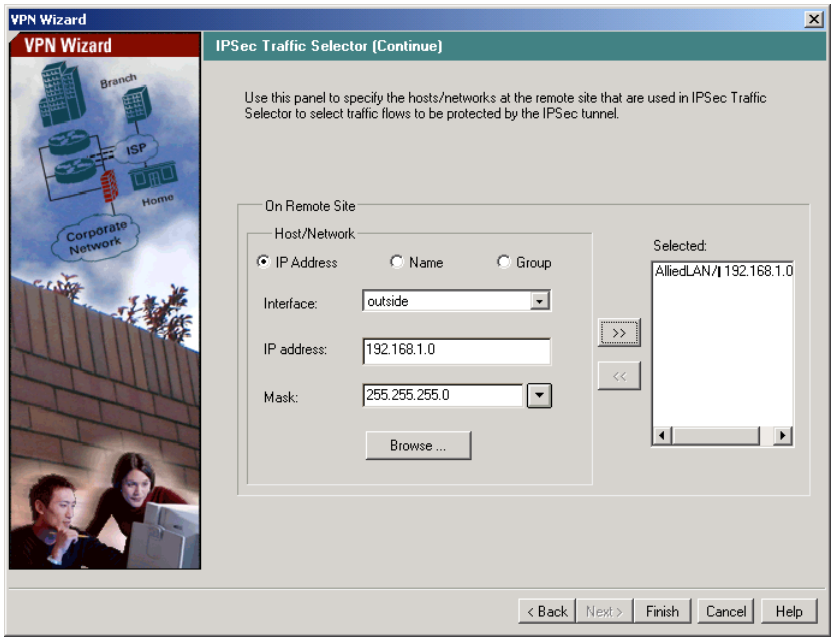


## 11. Click Finish to create the network



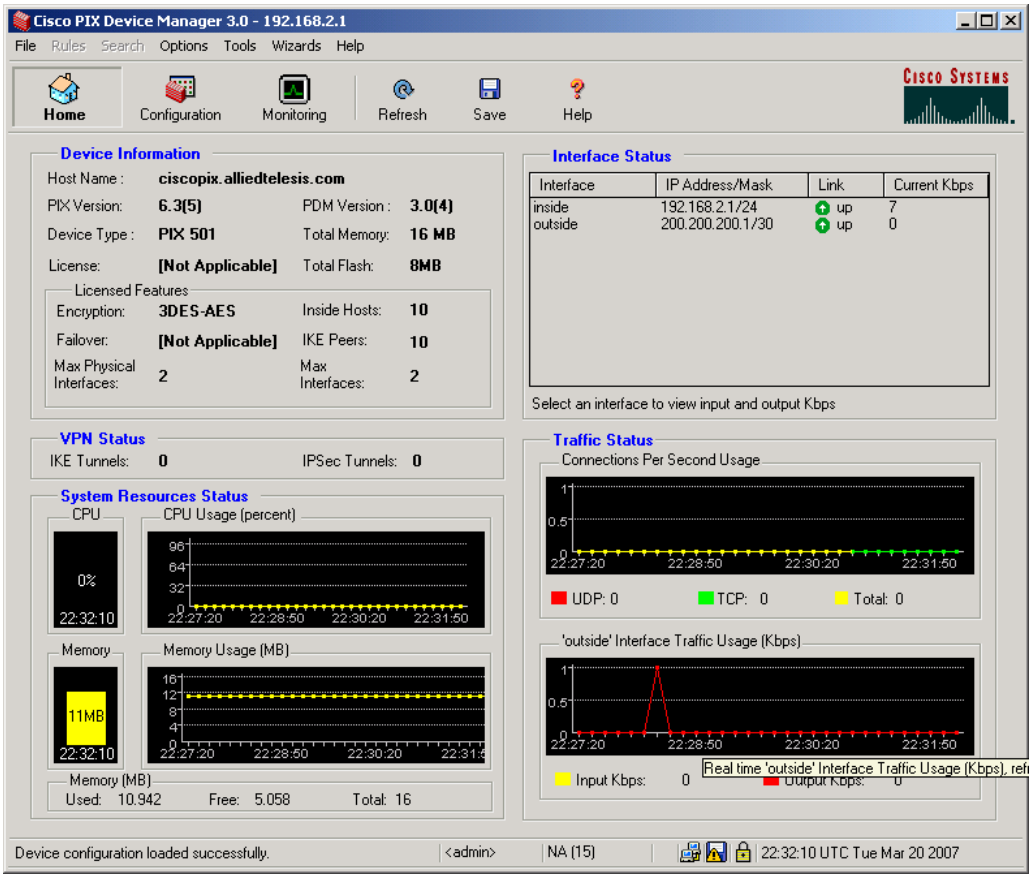

## 12. Confirm the address

The system returns you to the VPN Wizard to confirm the VPN's remote LAN network address. Click the right-pointing arrow to select the defined address. Then click **Finish** to complete the VPN setup wizard.



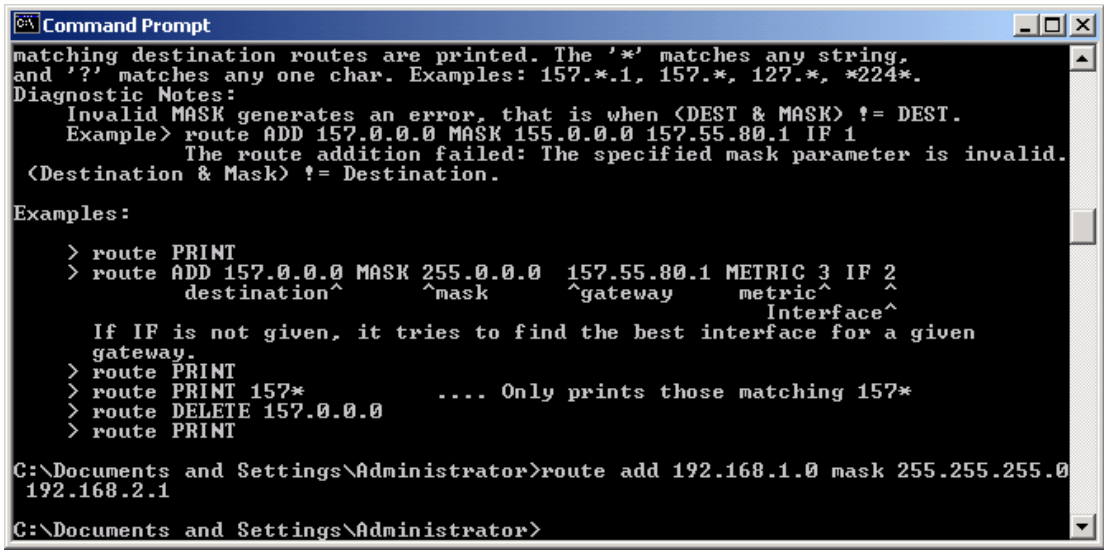
## 13. Check the PIX status

The following screenshot shows the PDM's Home summary status page again. At this stage the **VPN Status** shows zero IKE/IPsec tunnels.



### 14. Ensure appropriate VPN routes are defined on the LAN PCs

The PIX device is probably your default gateway. If you have two gateways, use the command prompt to set up a static route on the PC, to send traffic through the VPN to the remote LAN.




# Testing the tunnel

There are several options for testing the tunnel. If these checks show that your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

### 1. Ping the LAN

The simplest way to test the tunnel is to ping from one LAN to the other. For example, from the PC attached to the Allied Telesis router, ping the PC attached to the PIX.

If the Allied Telesis router has a dynamic IP address, note that you must initiate the tunnel from the Allied Telesis end. This means pinging from a PC attached to the Allied Telesis router, not from a PC attached to the PIX.

### 2. Check the PDM's Home summary status page to see whether the tunnels increment

Start some payload traffic from the PC at the Cisco end of the VPN to the LAN at the Allied Telesis router's end. For example, try to access a web server on the remote LAN.

Then, to confirm that the VPN is up, check the PDM's Home summary status page. The number of IKE/IPsec tunnels should increment.

# The Allied Telesis router command script

This section gives the Allied Telesis router configuration. To display the router configuration, log into its CLI and enter the command **show config dynamic**.

```
# System configuration
set system name="AlliedTelesis"

# User configuration
set user  securedelay=600
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503eff priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
add user=secoff pass=c962b86f3da856a9a67221a7df2038eeff priv=securityOfficer
   lo=yes
set user=secoff telnet=no netmask=255.255.255.255

# IP configuration
enable ip
ena ip dnsrelay
add ip int=vlan1 ip=192.168.1.1
add ip int=eth0 ip=100.100.100.1 mask=255.255.255.252
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=100.100.100.2
add ip dns prim=200.200.200.2

# Firewall configuration
enable firewall
create firewall policy="guilan"
enable firewall policy="guilan" icmp_f=ping
add firewall policy="guilan" int=vlan1 type=private
add firewall policy="guilan" int=eth0 type=public
add firewall poli="guilan" nat=enhanced int=vlan1 gblin=eth0
add firewall poli="guilan" ru=1 ac=allo int=eth0 prot=udp po=500
   ip=100.100.100.1 gblip=100.100.100.1 gblp=500
add firewall poli="guilan" ru=2 ac=allo int=eth0 prot=udp po=4500
   ip=100.100.100.1 gblip=100.100.100.1 gblp=4500
add firewall poli="guilan" ru=3 ac=non int=eth0 prot=ALL enc=ips
add firewall poli="guilan" ru=4 ac=non int=vlan1 prot=ALL
   ip=192.168.1.1-192.168.1.254
set firewall poli="guilan" ru=4 rem=192.168.2.1-192.168.2.254

# DHCP (Post IP) configuration
enable dhcp
create dhcp poli="lan-dhcp" lease=259200
add dhcp poli="lan-dhcp" subn=255.255.255.0
add dhcp poli="lan-dhcp" rou=192.168.1.1
add dhcp poli="lan-dhcp" dnss=192.168.1.1
create dhcp ran="standard" poli="lan-dhcp" ip=192.168.1.2 num=50

# IPSEC configuration
create ipsec sas=0 key=isakmp prot=esp enc=3desouter hasha=sha
set ipsec sas=0 antir=true
create ipsec bund=0 key=isakmp string="0" expirys=3600
create ipsec pol="eth0allowISAKMP" int=eth0 ac=permit
set ipsec pol="eth0allowISAKMP" lp=500 tra=UDP
create ipsec pol="eth0allowISAKMPF" int=eth0 ac=permit
set ipsec pol="eth0allowISAKMPF" lp=4500
create ipsec pol="wiz_AT-to-Cisco" int=eth0 ac=ipsec key=isakmp bund=0
   peer=200.200.200.1 isa="wiz_AT-to-Cisco"
set ipsec pol="wiz_AT-to-Cisco" lad=192.168.1.0 lma=255.255.255.0
   rad=192.168.2.0 rma=255.255.255.0
set ipsec pol="wiz_AT-to-Cisco" respondbadspi=TRUE
create ipsec pol="eth0allow" int=eth0 ac=permit
enable ipsec
```

```
# ISAKMP configuration
create isakmp pol="wiz_AT-to-Cisco" pe=200.200.200.1 enc=3desouter key=0
   natt=true
set isakmp pol="wiz_AT-to-Cisco" expirys=28800 gro=2
set isakmp pol="wiz_AT-to-Cisco" sendd=true sendn=true
enable isakmp
```

# The Cisco PIX command script

This section gives the Cisco PIX configuration. To display the PIX configuration, log into its CLI and enter the command **show run**.

```
:
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password H1T1eAKSC1VRiKB9 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname ciscopix
domain-name alliedtelesis.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
name 192.168.1.0 alliedVPN
access-list inside_outbound_nat0_acl permit ip 192.168.2.0 255.255.255.0
   alliedVPN 255.255.255.0
access-list outside_cryptomap_20 permit ip 192.168.2.0 255.255.255.0
   alliedVPN 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside dhcp setroute
ip address inside 192.168.2.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm location 192.168.2.2 255.255.255.255 inside
pdm location alliedVPN 255.255.255.0 outside
pdm history enable
arp timeout 14400
global (outside) 10 interface
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 10 0.0.0.0 0.0.0.0 0 0
route outside alliedVPN 255.255.255.0 200.200.200.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
```

```
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 192.168.2.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 100.100.100.1
crypto map outside_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp key ******** address 100.100.100.1 netmask 255.255.255.255 no-xauth
   no-config-mode
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.2.2-192.168.2.32 inside
dhcpd dns 200.200.200.1
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable inside
terminal width 80
Cryptochecksum:adf3a755dec019c18378c3df771a70d2
: end
```

# The ISP command script

This section gives the configuration of the Allied Telesis device that we used to represent the ISP between the two ends of the VPN. This script is provided in case you want to set up the scenario in a lab.

```
# SYSTEM configuration
set system name="ISP_DHCP"

# USER configuration
set user=manager pass=3af00c6cad11f7ab5db4467b66ce503eff priv=manager lo=yes
set user=manager desc="Manager Account" telnet=yes

# IP configuration
enable ip
add ip int=eth0 ip=200.200.200.2 mask=255.255.255.252
add ip int=eth1 ip=100.100.100.2 mask=255.255.255.252

# DHCP configuration - Post IP
enable dhcp
create dhcp poli="isp" lease=259200
add dhcp poli="isp" subn=255.255.255.252
add dhcp poli="isp" rou=200.200.200.2
add dhcp poli="isp" dnss=202.80.80.254
create dhcp ran="users" poli="isp" ip=200.200.200.1 num=1
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com



C613-16124-00 REV A