AlliedWare™ OS

How To | Use the Allied Telesis GUI Wizard to Create a Site-to-Site VPN

This How To Note describes how to configure a Virtual Private Network (VPN) between LANs at two sites, such as a central office and a branch office. The VPN gives people at each site secure access to the LAN at the other site, without the expense of a dedicated connection between the sites.

In this Note's example, each LAN is connected to the Internet through an Allied Telesis router. The Note gives step-by-step instructions for setting up this example by using the Site-To-Site VPN wizard, which makes VPN configuration simple. 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 pre-shared 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 LANs through a single public IP address on each router. This Internet access does not interfere with the VPN solution.

If one or both routers are connected to the Internet through a NAT gateway device, such as an ADSL modem, see *How To Use the Allied Telesis GUI Wizard to Create a Site-to-Site VPN through a NAT Gateway Device* instead. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

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.

The following Notes are particularly relevant:

- *How To Use The Allied Telesis GUI To Customise The Router And Set Up An Internet Connection*
- *How To Use The Allied Telesis GUI Wizard To Create A Site-to-Site VPN Through A NAT Gateway Device*

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?

This configuration applies to the following routers, running Software Version 2.9.1 or later:

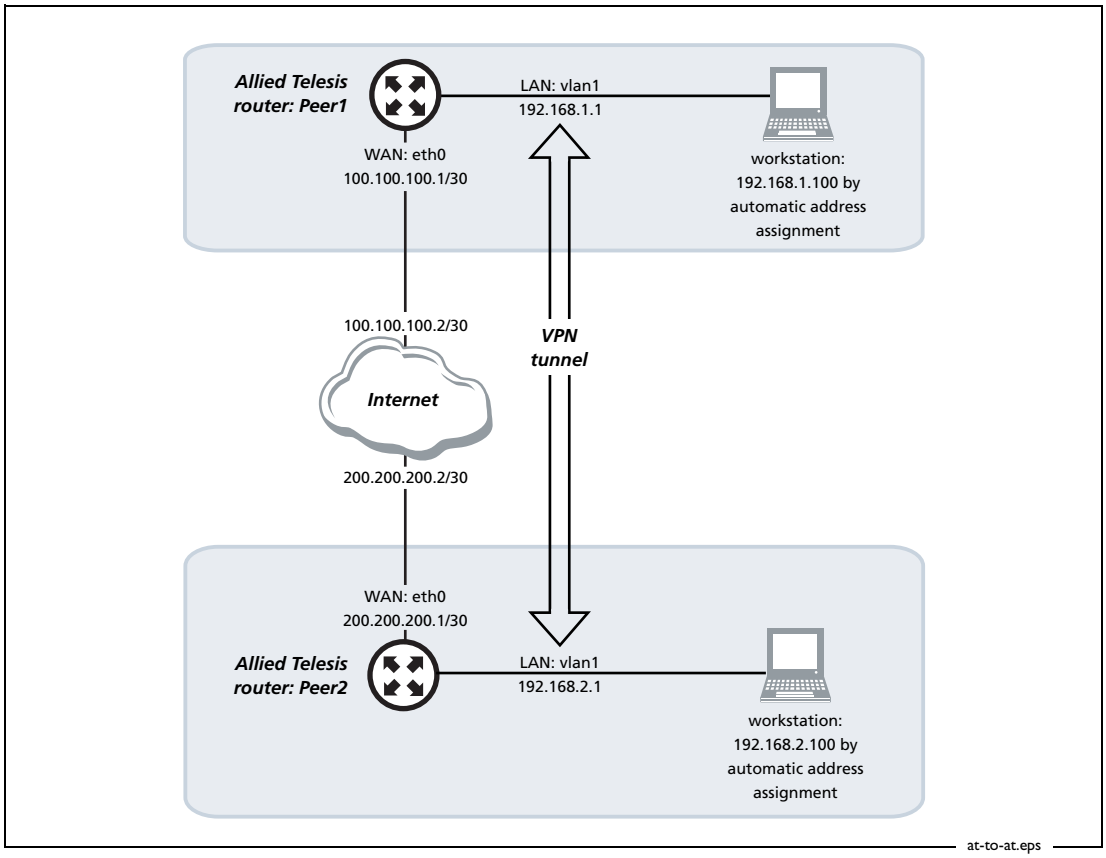
- AR415S
- AR440S
- AR441S
- AR442S

The screenshots in this Note are from an Internet Explorer 6.0 browser running on Windows XP[1].

1. Internet Explorer and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

The network

The following diagram shows the LANs and their interfaces and addresses.



Dynamic IP addresses

In this example both routers have fixed public IP addresses, but this configuration also works when the router at one of the sites has a dynamically-assigned IP address instead.

However, in that case the tunnel can only be initiated from the site with the dynamic address. This is because a router can only initiate communication with a peer if it knows the peer's IP address. When one router has a dynamically assigned address, the other router does not know which address to contact.

For example, if your central office has a fixed public IP address but your branch office does not, this configuration allows users in the branch office to access the central office computers. Users in the central office can access the branch office if someone in the branch office accesses the central office first.

How to configure Peer1

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. This example uses a fixed IP address on the WAN interface—modify it to use an appropriate interface for your network.

The router setup in steps 1-3 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 router Peer1 has the following settings:

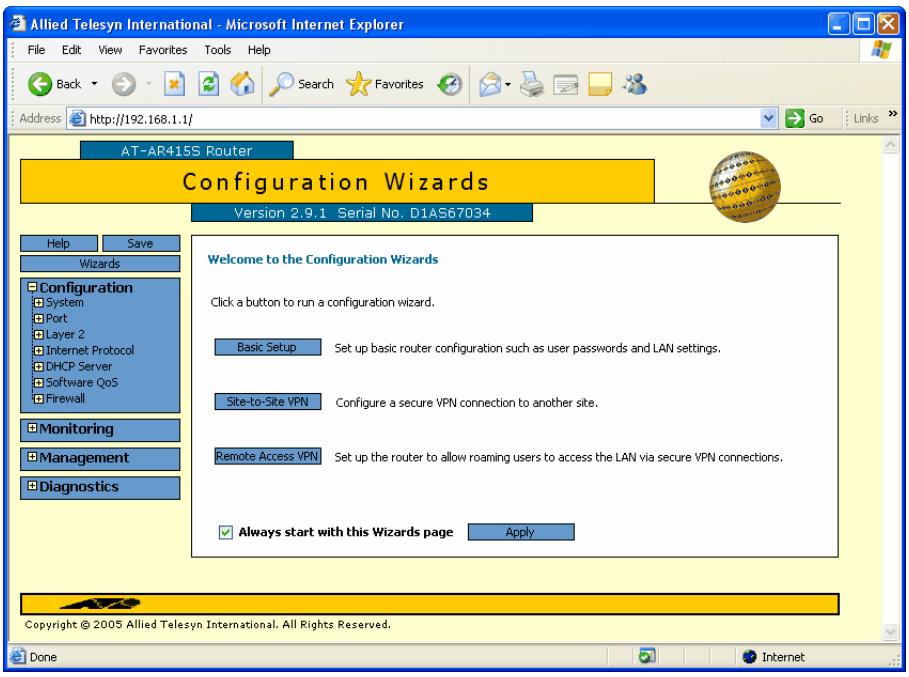
	Interface	Address	Mask
Peer1 LAN	vlan1	192.168.1.1	255.255.255.0
Peer1 WAN	eth0	100.100.100.1	255.255.255.252
Remote site's WAN settings		200.200.200.1	
Remote site's LAN settings		192.168.2.1	255.255.255.0

Create the VPN tunnel

1. Open the Configuration Wizards page

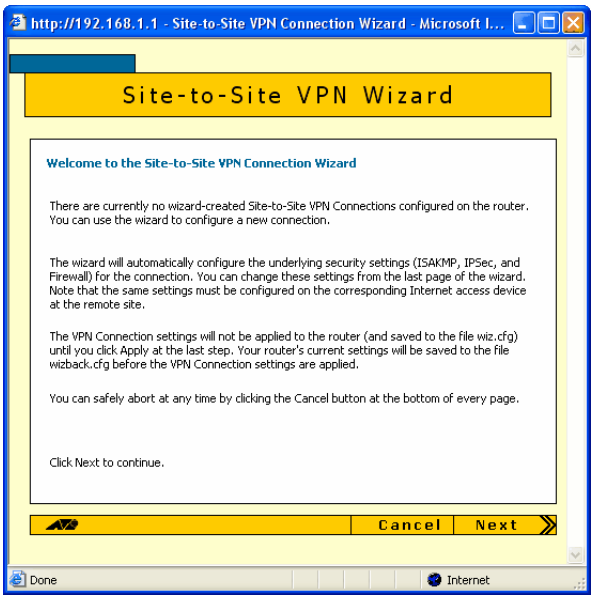
Log in as either the manager or the security officer. If you log in as the manager, the router changes to secure mode when you finish the VPN wizard and at that stage prompts you to log in again as the security officer.

The Site-To-Site VPN wizard is one of the options on the 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.



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.

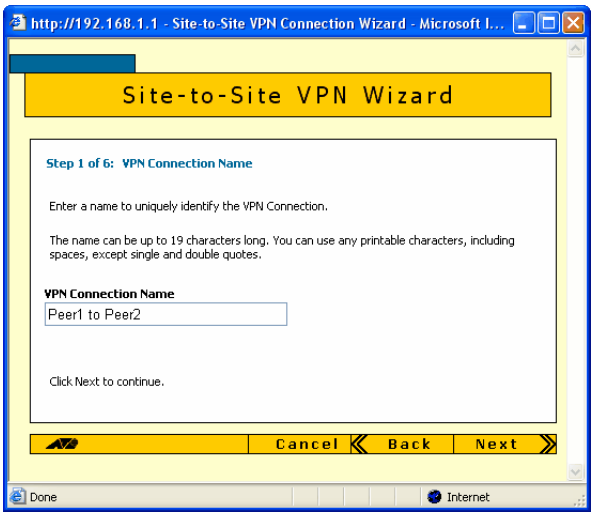
2. Start the Site-to-Site VPN wizard



Click on the Site-to-Site VPN button. The wizard starts by displaying a welcome message.

Click the Next button.

3. Name the VPN connection



Enter an appropriate VPN connection name.

Click the Next button. If you have multiple possible WAN interfaces configured on the router, the wizard next lets you 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.

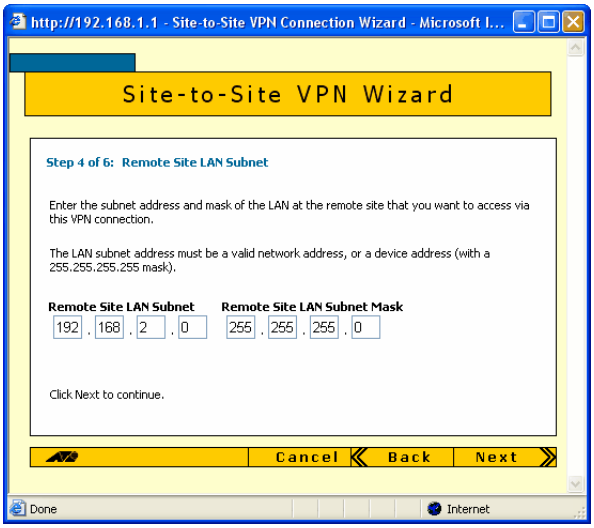
4. Enter the remote site's WAN IP address

Enter the public IP address of the other end of the tunnel. In this example, this is 200.200.200.1, which is the IP address of the Peer2 router's WAN interface.

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

Click the Next button.

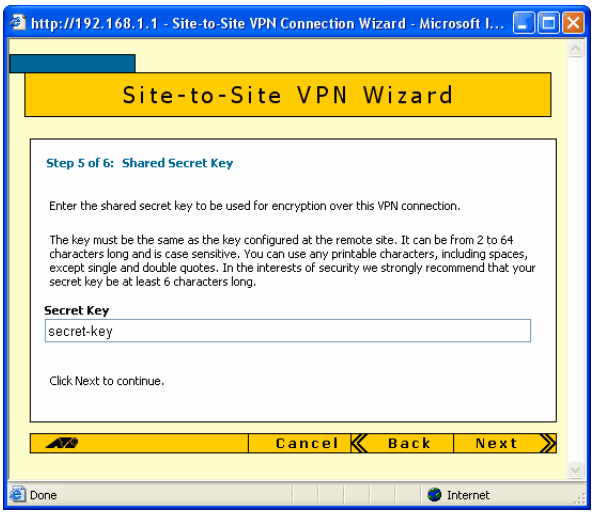
5. Enter the remote site's LAN IP address



Enter the Peer2 router's LAN subnet address and mask. In this example, this is 192.168.2.0 and a mask of 255.255.255.0.

Click the Next button.

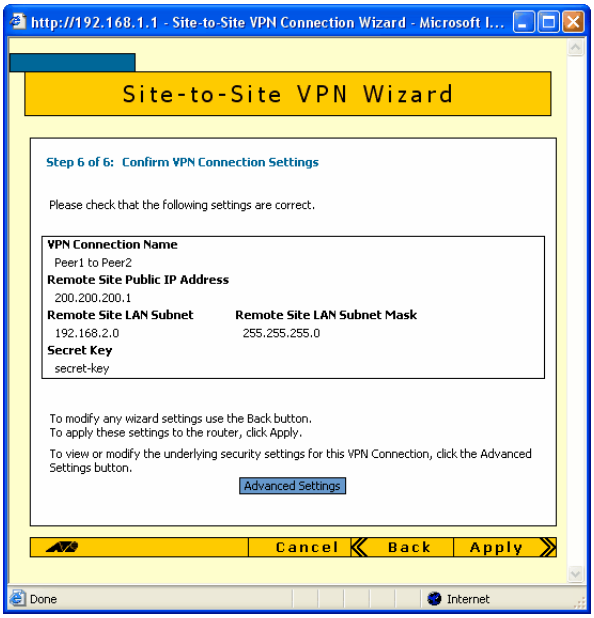
6. Enter the shared secret key



Enter the secret key, which is an alphanumeric string between 2 and 64 characters long. Note that both peer routers must use the same secret key.

Click the Next button.

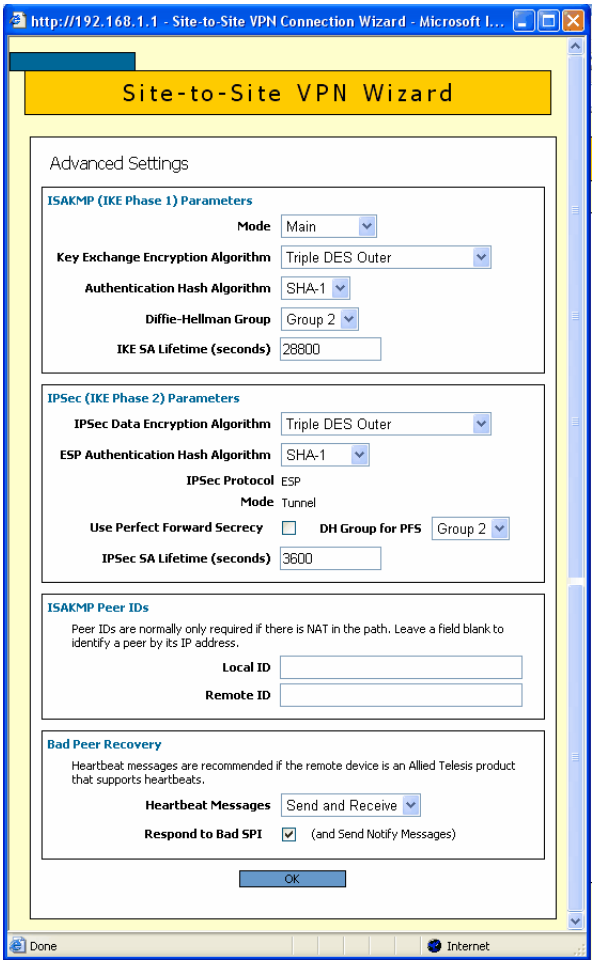
7. Check the settings



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 the Advanced Settings button to modify heartbeat settings.

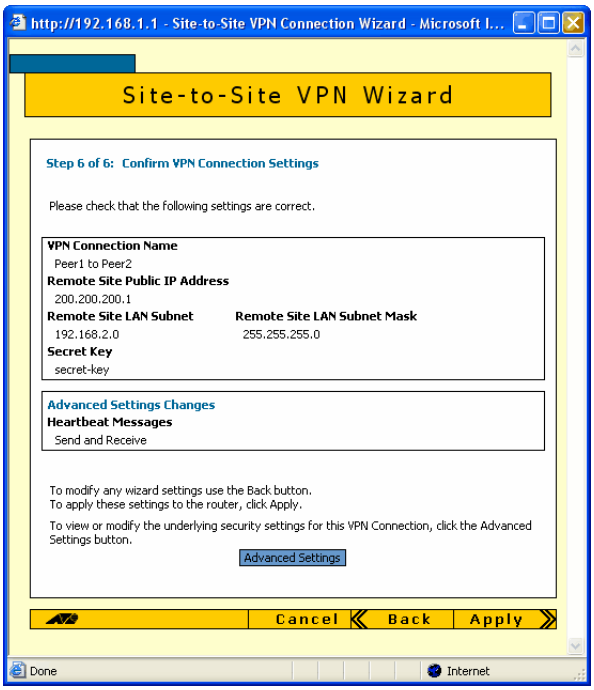
8. Enable heartbeats



Heartbeats are messages that Allied Telesis routers exchange to keep the VPN tunnel open when both peers are available. We recommend that you use them when both peers are Allied Telesis routers.

At the bottom of the Advanced Settings page, set Heartbeat Messages to Send and Receive. Then click the OK button.

9. Check the settings again

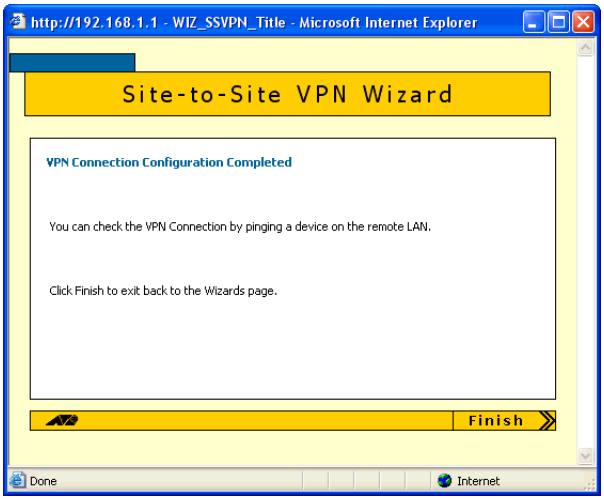


Check the summary. It now includes the Heartbeat settings. If necessary, correct any settings you want to change.

When all the settings are correct, click the Apply button.

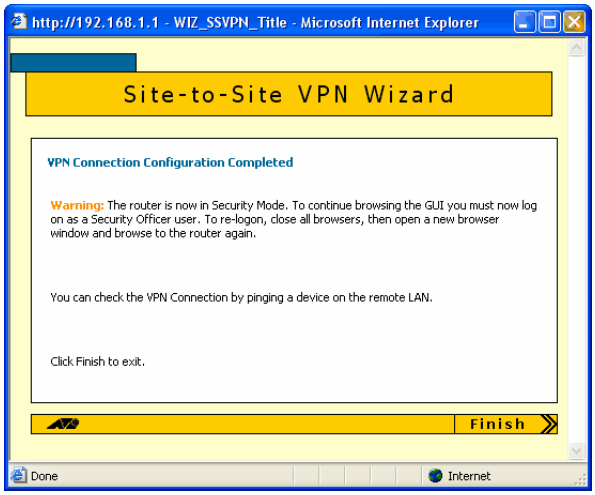
10. Finish the wizard

Security officer



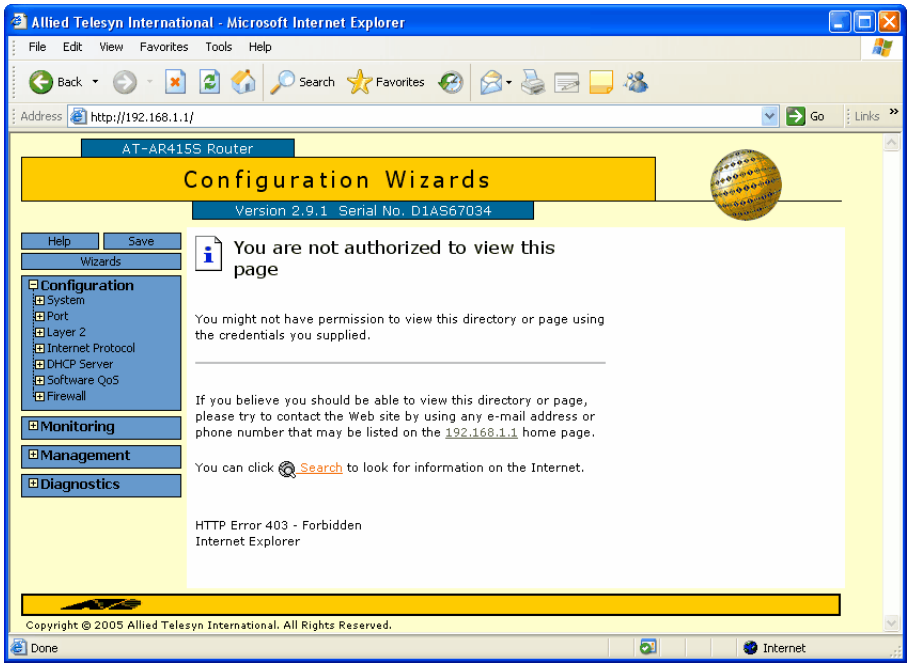
If you are logged in as the security officer, the GUI displays a completion message. Click the Finish button to finish the Wizard and save the VPN settings.

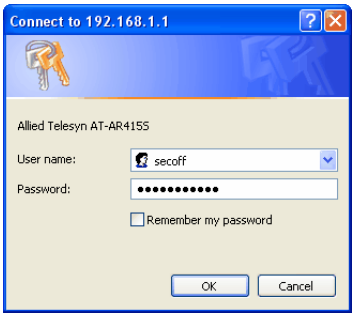
Manager



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





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.

How to configure Peer2

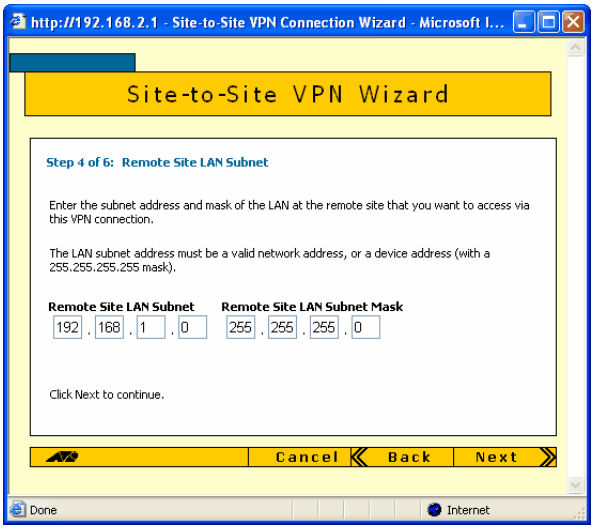
Peer2 has the following settings:

	Interface	Address	Mask
Peer2 LAN	vlan1	192.168.2.1	255.255.255.0
Peer2 WAN	eth0	200.200.200.1	255.255.255.252
Remote site's WAN settings		100.100.100.1	
Remote site's LAN settings		192.168.1.0	255.255.255.0

To create the VPN tunnel, perform the same steps as when configuring Peer1. The only differences are:

- In step 4 "Enter the remote site's WAN IP address", use the IP address of the Peer1 router's WAN interface: 100.100.100.1

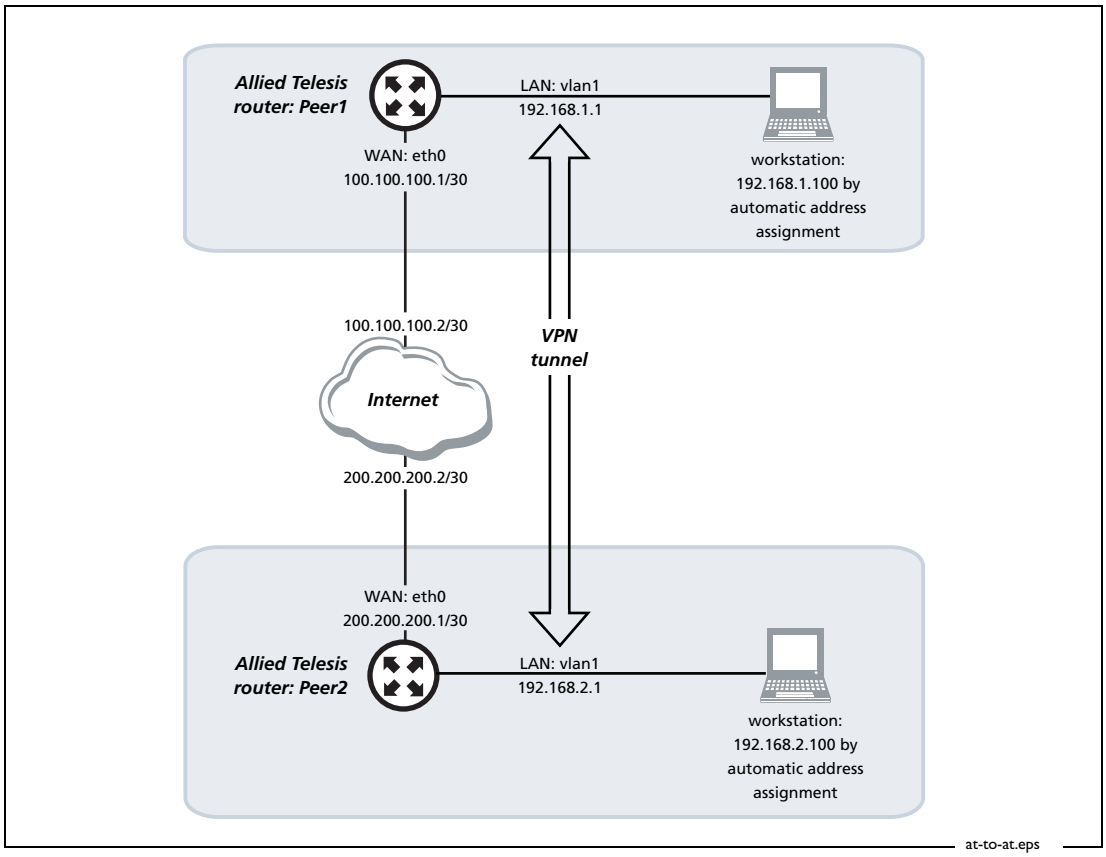
- In step 5 "Enter the remote site's LAN IP address", use the Peer1 router's LAN subnet address and mask: 192.168.1.0 and 255.255.255.0



How to test the tunnel

If the following tests show that your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

The network diagram is repeated here for your convenience.



Check the LANs are reachable

The simplest way to test the tunnel is to ping from one LAN to the other.

From the PC attached to Peer1, ping the PC attached to Peer2. In this example, that means using the following command at the command prompt on the PC attached to Peer1:

```
ping 192.168.2.100
```

If a Microsoft Windows PC's IP address was assigned dynamically, you can find out what it is by using the following command at the command prompt:

```
ipconfig
```

Check traffic goes through the VPN

To tell if traffic passes through the tunnel, perform a traceroute from one LAN to the other—so from a PC attached to one peer, perform a traceroute to a PC attached to the other peer. For example, if the PC attached to Peer2 has an address of 192.168.2.100, that means using the following command at the command prompt on the (Windows) PC attached to Peer1:

```
tracert 192.168.2.100
```

If traffic goes through the tunnel, the traceroute may display IP addresses from one or both peers' private networks and public interfaces. If it shows other public IP addresses, then traffic is not passing through the tunnel.

Check counters

Another way to be certain that the router is encrypting traffic and sending it over the tunnel is to use the IPsec counter command, as follows:

1. In the GUI, select Diagnostics, then Command Line.
2. Enter the command **show ipsec policy counters** and click the Execute button. Note the current values of the outProcessDone counter (in the Outbound Packet Processing Counters section) and the inProcessDone counter (in the Inbound Packet Processing Counters section).
3. From the PC attached to Peer1, ping the PC attached to Peer2. Note that you have to ping from a PC, not from the GUI—the GUI Command Line page does not display the ping response.
4. Enter the command **show ipsec policy counters** again and click the Execute button. The outProcessDone counter should have incremented once for each ping packet sent, and the inProcessDone counter should have incremented once for each echo reply.

How to browse to the GUI securely

Now that the router is in secure mode, you should consider setting it up so that you can browse to the GUI securely. This means using HTTPS instead of HTTP.

1. Access the router's CLI

See the Installation and Safety Guide for instructions about how to access the router's command line interface via a console port.

Log into the router with the username "secoff", by using the command:

```
login secoff
```

2. Configure SSL

Step-by-step instructions for this are given in the Software Reference, in the "Configuration Example" section in the "Secure Sockets Layer (SSL)" chapter. Note the following variations from that example:

- That example begins by creating a new Security Officer user and enabling system security—skip those steps and start at the step that creates an RSA key pair.
- That example ends by configuring an IP address and associated route. You have already done this, so stop at the step that enables SSL.

3. Browse to the GUI

Once you have finished the configuration, to access the router via the GUI, you browse to:

```
https://<router-ip-address>
```

Note that the URL uses HTTPS, not HTTP. For example, to access the Peer2 router in this How To Note, browse to:

```
https://192.168.2.1
```

Log into the router with the username "secoff" and your password.

The router commands

This section lists the configuration commands that the wizard runs when it sets up the VPN.

You can compare your router configuration against the following commands to help with troubleshooting. To display your router configuration, log into its CLI and enter the following command:

```
show config dynamic
```

Peer1

```
# System configuration
set system name="Peer1"

# User configuration
set user=manager pass=your-password priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
add user=secoff pass=your-password 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=150.150.150.1 seco=150.150.150.2

# 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=192.168.1.100 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_Peer1 to Peer2" int=eth0 ac=ipsec key=isakmp bund=0
  peer=200.200.200.1 isa="wiz_Peer1 to Peer2"
set ipsec pol="wiz_Peer1 to Peer2" lad=192.168.1.0 lma=255.255.255.0
  rad=192.168.2.0 rma=255.255.255.0
set ipsec pol="wiz_Peer1 to Peer2" respondbadspi=TRUE
create ipsec pol="eth0allow" int=eth0 ac=permit
enable ipsec

# ISAKMP configuration
create isakmp pol="wiz_Peer1 to Peer2" pe=200.200.200.1 enc=3desouter key=0
  natt=true
set isakmp pol="wiz_Peer1 to Peer2" expirys=28800 gro=2
set isakmp pol="wiz_Peer1 to Peer2" sendd=true sendn=true
set isakmp pol="wiz_Peer1 to Peer2" hear=BOTH
enable isakmp
```

Peer2

```
# System configuration
set system name="Peer2"

# User configuration
set user=manager pass=your-password priv=manager lo=yes
set user=manager telnet=yes desc="Manager Account"
add user=secoff pass=your-password 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=192.168.2.1
add ip int=eth0 ip=200.200.200.1 mask=255.255.255.252
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.200.200.2
add ip dns prim=150.150.150.1 seco=150.150.150.2

# 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=200.200.200.1 gblip=200.200.200.1 gblp=500
add firewall poli="guilan" ru=2 ac=allo int=eth0 prot=udp po=4500
  ip=200.200.200.1 gblip=200.200.200.1 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=192.168.2.1-192.168.2.254
set firewall poli="guilan" ru=4 rem=192.168.1.1-192.168.1.254

# 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=192.168.2.1
add dhcp poli="lan-dhcp" dnss=192.168.2.1
create dhcp ran="standard" poli="lan-dhcp" ip=192.168.2.100 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_Peer1 to Peer2" int=eth0 ac=ipsec key=isakmp bund=0
  peer=100.100.100.1 isa="wiz_Peer1 to Peer2"
set ipsec pol="wiz_Peer1 to Peer2" lad=192.168.2.0 lma=255.255.255.0
  rad=192.168.1.0 rma=255.255.255.0
set ipsec pol="wiz_Peer1 to Peer2" respondbadspi=TRUE
create ipsec pol="eth0allow" int=eth0 ac=permit
enable ipsec

# ISAKMP configuration
create isakmp pol="wiz_Peer1 to Peer2" pe=100.100.100.1 enc=3desouter key=0
  natt=true
set isakmp pol="wiz_Peer1 to Peer2" expirys=28800 gro=2
set isakmp pol="wiz_Peer1 to Peer2" sendd=true sendn=true
set isakmp pol="wiz_Peer1 to Peer2" hear=BOTH
enable isakmp
```

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

C613-16095-00 REV D

Connecting The IP World

Allied Telesis