AlliedWare™ OS

How To | Create a VPN between an Allied Telesis Router and a Microsoft Windows XP[1] Client, over NAT-T

Introduction

This document describes how to provide secure remote access through IP security (IPSec) Virtual Private Networks (VPN).

This VPN solution is suitable for any business deployment and provides your office with secure internet access and firewall protection, plus remote encrypted VPN access for travelling staff.

The solution allows for IPsec NAT Traversal, which permits VPN clients to communicate through Network Address Translation (NAT) gateways over the Internet. For example, business travellers (road warriors) commonly use IPsec on their laptop to gain remote VPN access to the central office. When working off-site, these users sometimes need to connect to the Internet through a NAT gateway such as from a hotel. Also, NAT gateways are often part of a company's firewall and let its Local Area Network (LAN) appear as one IP address to the world.

For more information about NAT gateways, see RFC 1631 *The IP Network Address Translator (NAT)*, and the Network Address Translation section in the Firewall chapter of your device's Software Reference.

If you do not want to enable NAT-T support, use the companion Note *How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows XP Client, Without Using NAT-T* instead. This companion How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

1. Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Consider the following typical scenario:

You are the manager of a small business and you have purchased an AR415S for your small office premises. You have five PCs networked together with a server in your office. You intend to use your AR415S as your Internet gateway and for it to provide firewall protection.

You also have a team of five sales people who travel widely around the globe. You would like these staff members to have secure (encrypted) remote access through the Internet to the servers in your office, to allow them to access files, the private Intranet, and business email.

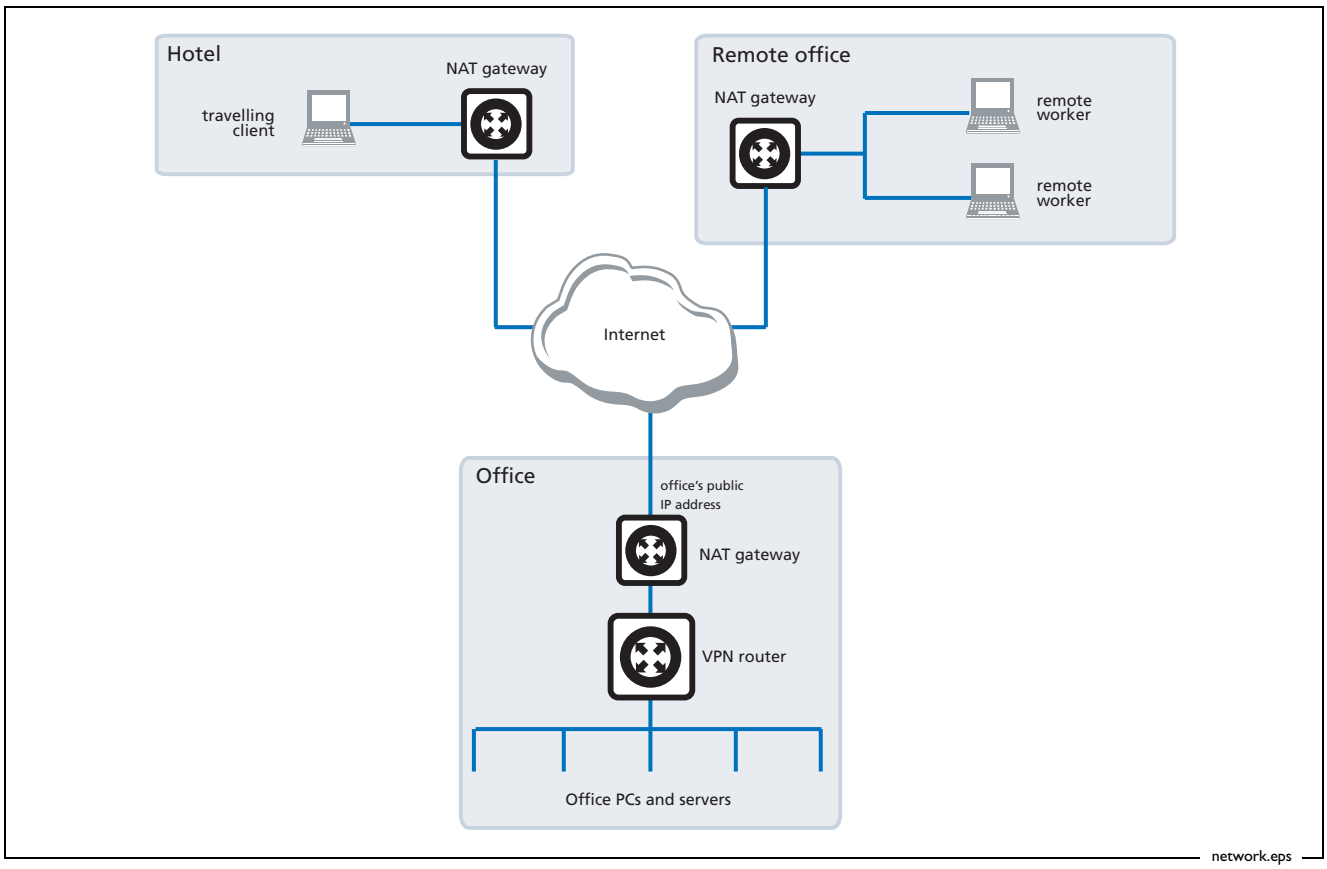
The travelling staff members will get secure remote access from any hotel or location with Internet access through the use of IPSec VPN. Each staff member has a laptop or other portable device with Windows XP installed.

This document describes how to configure the Windows system to use IPSec VPN to connect to your office through the AR415S router. The solution uses NAT-T, so your IPsec VPN will still work even if the remote location uses a NAT gateway or firewall for Internet access. It would also work if your office router used a separate NAT gateway, such as an ADSL modem.

When your staff want to connect to the office they simply use the VPN icon on their desktop to initiate the IPSec VPN connection.

Example Network

The following figure shows three possible scenarios that need NAT-T: travelling workers behind a NAT gateway, a remote office behind a NAT gateway, and the main office behind a NAT gateway.



Which products and releases does it apply to?

The following Allied Telesis routers are most suitable as VPN gateways because they have fast hardware encryption support and high performance:

- AR415S, AR44xS series, and AR450S
- AR750S and AR770S

The AR415S achieves up to 90 Mbps throughput with 3DES or AES encryption.

You can also use older routers as VPN gateways, but they will not have as high performance. The older routers depend on either the Encryption Mini Accelerator Card (EMAC) or the Encryption PCI Accelerator Card (EPAC) to perform encryption. They include:

- AR725, AR745, AR720 and AR740 routers
- AR410 series routers
- AR300 series routers

Finally, you can also use the Rapier 24 and Rapier 24*i* switches as VPN gateways, but this is usually not a recommended practice. Doing so means you will lose wire-speed switching of data, because all traffic needs to be inspected by the firewall and IPSec at CPU processing speed.

Encryption algorithms such as 3DES and AES require a feature licence. This is included on some models. See your Allied Telesis representative for more information.

The configuration is supported on all AlliedWare versions since 2.6.4 and was tested using a PC running Microsoft Windows XP Professional, Service Pack 1a.

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.

The collection includes Notes that describe how to interoperate with Windows 2000, XP and Vista clients.

Windows XP and NAT-T support

To use NAT-T with Windows XP clients, you need:

- Windows XP Professional or Home
- either:
  - Service Pack 2. If you have a separate NAT gateway between the router and the Internet, you also need to change a registry key value, as described in the Microsoft article KB 885407. See "Support for NAT device at the responder VPN gateway end of link", on this page.
  - an earlier service pack or no service pack, with the Layer Two Tunnelling Protocol (L2TP) and Internet Protocol security (IPSec) update patch, KB 818043. See "The KB 818043 update patch" on page 4.
- to set your router to propose a local port of 1701, not a remote port. See "Port settings for IPsec policy proposal" on page 5.

Support for NAT device at the responder VPN gateway end of link

Service Pack 2 does not support NAT devices at the VPN responder end of the link.

To overcome this issue, you need to change the value of a registry key, as described in Knowledge Base article 885407 at support.microsoft.com/kb/885407.

The registry key can be set for different values depending on your NAT circumstances:

- value 0 (default): does not permit IPSec when responders are behind NAT.
- value 1: XP SP2 can initiate IPSec to responders behind NAT (you will target the public side of the NAT device and that device will need pinholes).
- value 2: XP SP2 can initiate IPSec when both initiator and responder and behind NAT.

As well as describing the required change, the article outlines some security issues with it.

The KB 818043 update patch

Prior to Service Pack 2, NAT-T support is provided by the Layer Two Tunnelling Protocol (L2TP) and Internet Protocol security (IPSec) update patch, *KB 818043*.

For details about the update patch and how to download it, see support.microsoft.com/kb/818043.

Note: If you do not have the KB 818043 update patch, then the router or switch log will not proceed beyond “ISAKMP MAIN Phase 1 (resp) started with peer x.x.x.x” and “Exch xx: Failed” when a user attempts to connect. If you have ISAKMP debugging enabled, this condition will show as “Remote ID different to expected”.

Port settings for IPsec policy proposal

NAT-T support resulted in a change to the way Windows XP clients make their IPsec policy proposals—clients now need to propose a **remote** port (from their point of view) of 1701 instead of a **local** port of 1701.

This change was necessary because the Microsoft VPN implementation uses the L2TP payload inside IPSec transport mode. With transport mode, IPSec does not insert an independent new IP header. Instead it reuses the L2TP header. So, if the Windows XP VPN client is behind a local NAT gateway, then the local port value of 1701 will change as it transits the NAT gateway.

Therefore, when Microsoft introduced support for NAT-T, they had to change the way that the VPN client made its IPSec policy proposal. The client could no longer propose a local port of 1701, because the NAT gateway would change this value, so the proposal would fail at the responding peer. Instead, the client proposes a remote port of 1701.

This change needs to be reflected in the configuration of the IPsec policy on the Allied Telesis router. In this How To Note, the router configuration includes the following command:

```
set ipsec policy="all roaming" transport=udp lport=1701
```

In contrast, the non-NAT-T version (*How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows XP Client, Without Using NAT-T*) uses the following command instead:

```
set ipsec policy=to_HQ transport=udp rport=1701
```

The solution over NAT-T uses **lport** instead of **rport**.

If you do not need NAT-T functionality, you can either use:

- the NAT-T How To Note solution. NAT-T automatically drops back to non-NAT-T behaviour when it detects no NAT gateways in the path.
- no service pack or a service pack earlier than SP2, without the KB 808143 patch, with the non-NAT-T How To Note solution and your router proposing **rport**.

Other solution requirements and things to consider

- For the VPN client solution given in this document to work, your office must have a fixed Internet address. This is the target address for the VPN client. Depending on whether the office uses a NAT gateway device or not, this Internet address will either belong to the NAT gateway or the router.

  Many ISPs assign dynamic addresses as standard practice, and these addresses can change periodically. It is likely you will need to specifically ask for a fixed address for your office.
- Other utilities sometimes conflict with the Windows IPSec policy agent, and may need to be uninstalled, such as another VPN client installation, or perhaps a firewall utility. In some cases, uninstalling these utilities may not properly restore the Windows IPSec policy agent, in which case you may need to check your Windows services listing to see that the agent is in "automatic" mode.
- If the office uses a NAT gateway device, that device must be configured with allow rules ("pinholes") for UDP 500 and UDP 4500 traffic.
- If your office router is behind an external gateway that does not use NAT—perhaps a firewall or IP filtering device—then the external gateway will need a protocol 50 permit rule in addition to the UDP 500 and UDP 4500 permit rules. This will allow NAT-T to work in all situations.
- Your ISAKMP pre-shared key needs to be alphanumeric only, to ensure interoperation with Windows.
- You need to define a PPP DNS server address on the router that will be assigned to the incoming VPN users. The DNS address needs to be valid for the network being connected to via VPN.
- Internet Explorer browser users may need to define a proxy definition against the VPN dial-up link, valid for the network being connected to via VPN.
- You should use Secure Shell for remote management. You should not use telnet for a secure gateway.

Security issues

Since this Windows VPN solution is usually used to allow remote access into corporate networks, a common security concern is "what happens if the remote laptop or PC is stolen or falls into unauthorised hands?" This is particularly a concern because the VPN connection is enabled through the standard dial-up networking window that allows username and passwords to be saved.

A solution to this security concern is to disable the standard behaviour that allows passwords to be saved. VPN users will then have to enter their password each time they connect.

If you would like to implement this security measure, see Microsoft Knowledge Base article 172430 by following this link: support.microsoft.com/default.aspx?scid=172430.

To make portable PCs and laptops more secure:

- never leave access numbers or passwords in your carrying case
- carry your laptop with you
- avoid using computer bags, because they advertise the fact that you have a laptop
- encrypt your data
- buy a laptop security device, e.g. a security cable to securely attach it to a heavy chair, table, or desk
- **do not** use the **Save Password** feature that Windows offers during dial-up.

Some PCs have security modes that can be enabled. There are also numerous tips about laptop security available on the Web.

Configuring the router

This section contains a script file for running IPSec encapsulating L2TP on a Head Office AR400 series router, configured to support IPSec remote PC clients.

Using this script involves the following steps:

1. "Perform initial security configuration on the router", on this page.
2. Make a copy the script, which starts on page 9. Name it (for example) *vpn.cfg*.
3. Personalise IP addresses, passwords etc in the script, so that they apply to your network. Placeholders for these are indicated in the script by text within < >.
4. Load the script onto the router using ZMODEM, HTTP or TFTP.
5. "Set the router to use the configuration" on page 11.
6. Restart the router or activate the script.

Perform initial security configuration on the router

Before loading the configuration, you need to do the following steps.

1. Define a security officer.

   ```
   add user=secoff password=<your-password> priv=securityofficer
   ```

   This command must be in the configuration script as well.

2. Enable system security. Unless you do this, rebooting the router destroys encryption keys.

   ```
   enable system security
   ```

3. Log in as the security officer.

   ```
   login secoff
   ```

4. Generate a random key.

   ```
   create enco key=1 type=general value=<alphanumeric-string>
   ```

   Note the value of the string you have entered so that you can load it on the PC clients. This shared key will be used to encrypt ISAKMP negotiation.

5. Create additional keys for SSH if you want remote access to the router. Refer to the Secure Shell chapter and example in your router's Software Reference for more information.

   ```
   create enco key=2 description="Server Key" type=rsa length=768
      format=ssh
   create enco key=3 description="Host Key" type=rsa length=1024
      format=ssh
   ```

The configuration script

Note: Comments are indicated in the script below using the # symbol.
Placeholders for IP addresses, passwords, etc are indicated by text within < >

```
set system name="IPSec Gateway"

#  The first command below shows the Security Officer inactive timeout delay.
#  The default is 60 seconds. During setup you can instead use 600 seconds
#  if desired.
set user securedelay=600
add user=secoff pass=<password> privilege=securityOfficer login=yes
set user=secoff description="Security Officer Account"

#  The incoming L2TP calls will be CHAP authenticated. They may be
#  authenticated against the router's user database as configured below,
#  or against a RADIUS server if configured. You also have the option of
#  assigning individual addresses to individual users using the router user
#  database or your Radiusserver. IP addresses defined in the user database
#  take precedence over the IP pool addresses.
add user=dialin1 password=friend1 login=no ip=192.168.8.50
add user=dialin2 password=friend2 login=no
add user=dialin3 password=friend3 login=no ip=192.168.8.51
add user=dialin4 password=friend4 login=no

#  If RADIUS server support is needed, use a command such as this:
#  add radius server=<RADIUS-server-address> secret=<secret-key>

#  All dynamic incoming L2TP calls will associate with this PPP template.
create ppp template=1 bap=off ippool="myippool" authentication=chap echo=30
   lqr=off

#  PPP may need to give out the site's private DNS server address so the
#  client can do DNS lookups.
set ppp dnsprimary=<your private DNS server address if applicable>

#  Cater for dynamic creation of incoming L2TP calls.
enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
enable ip
add ip int=vlan1 ip=<office private LAN address>
add ip int=eth0 ip=<interconnect LAN address> mask=<mask>

#  The default route to the Internet.
add ip route=0.0.0.0 mask=0.0.0.0 int=eth0
   next=<your NAT gateway or ISP next-hop address>

#  The IP pool addresses are the internal address ranges you want to allocate
#  to your IPSec remote PC clients (e.g. ip=192.168.8.1-192.168.8.254).
#  Although, addresses defined in the user database will take precedence.
create ip pool=myippool ip=<pool-range>

#  Firewall configuration
enable fire
create fire policy=main
create fire policy=main dy=dynamic
add fire policy=main dy=dynamic user=ANY
add fire policy=main int=vlan1 type=private
```

```
#  Dynamic private interfaces are accepted from L2TP, which are from IPSec
#  only.
add fire policy=main int=dyn-dynamic type=private
add fire policy=main int=eth0 type=public

#  The firewall allows for internally generated access to the Internet
#  through the following NAT definition.
add fire policy=main nat=enhanced int=vlan1 gblinterface=eth0

#  The following NAT definition allows Internet access for remote VPN users by
#  providing address translation.
add fire policy=main nat=enhanced int=dyn-dynamic gblinterface=eth0

#  Rules 1 and 2 allow for ISAKMP and the "port floated" IKE/ISAKMP that NAT-T
#  uses.
add fire policy=main rule=1 int=eth0 action=allow protocol=udp
   ip=<office Internet address> port=500 gblip=<office Internet address>
   gblport=500
add fire policy=main rule=2 int=eth0 action=allow protocol=udp
   ip=<office Internet address> port=4500 gblip=<office Internet address>
   gblport=4500

#  Rule 3 becomes the L2TP tunnel allow rule. Additional security is provided
#  by only allowing traffic from IPSec tunnels.
add fire policy=main rule=3 int=eth0 action=allow prot=udp
   ip=<office Internet address> port=1701 gblip=<office Internet address>
   gblport=1701 encap=ipsec

#  We recommend you use Secure Shell for remote management. Telnet should not
#  be used to a secure gateway.
enable ssh server serverkey=2 hostkey=3 expirytime=12 logintimeout=60
add ssh user=secoff password=<secoff password> ipaddress=<trusted remote ip>

#  IPSEC configuration
create ipsec saspecification=1 key=isakmp protocol=esp encalg=3desouter
   hashalg=sha mode=transport
create ipsec saspecification=2 key=isakmp protocol=esp encalg=3desouter
   hashalg=md5 mode=transport
create ipsec saspecification=3 key=isakmp protocol=esp encalg=des hashalg=sha
   mode=transport
create ipsec sas=4 key=isakmp protocol=esp encalg=des hashalg=md5
   mode=transport

#  The ORDER of proposals is important. You should propose the strongest
#  encryption first.
create ipsec bundle=1 key=ISAKMP string="1 or 2 or 3 or 4"

#  The first two IPSec permit rules allow for IKE /ISAKMP and the "port
#  floated" IKE plus NAT-T traffic port.
create ipsec policy="isakmp" int=eth0 ac=permit
set ipsec policy="isakmp" lp=500
create ipsec policy="isakmp_float" int=eth0 action=permit
set ipsec policy="isakmp_float" lport=4500

#  This is a generic IPSec policy. Using the peer=any options allows multiple
#  IPSec remote PC clients to connect through this same policy.
create ipsec policy="all_roaming" int=eth0 action=ipsec key=isakmp
   bundlespecification=1 isakmppolicy="roaming1" peer=any
set ipsec policy="all_roaming" transport=udp lport=1701
```

```
#  If you need both VPN and internet-browsing access, use the following
#  internet policy. Do not use this policy for VPN only.
#  If you use this "internet" permit policy, then the "isakmp" and
#  "isakmp_float" permit policies are actually optional.
create ipsec policy="internet" int=eth0 action=permit
enable ipsec

#  ISAKMP configuration
create isakmp policy="roaming1" peer=any key=1
set isakmp policy="roaming1" senddeletes=true localid=local natt=on
enable isakmp

#  You may find the following alias commands (shortcuts) handy if you need to
#  turn on debugging
add alias=ed string="enable isa debug"
add alias=ed2 string="enable ipsec poli debug=all"
add alias=dd string="dis isa debug"
add alias=dd2 string="dis ipsec poli debug=all"
```

Set the router to use the configuration

After loading the configuration onto the switch, set the router to use the script after a reboot. If you named the script vpn.cfg, enter the command:

```
set conf=vpn.cfg
```

If you entered the configuration directly into the command line instead of loading the script, save the configuration by entering the commands:

```
create conf=vpn.cfg
```

```
set conf=vpn.cfg
```

Configuring the VPN client

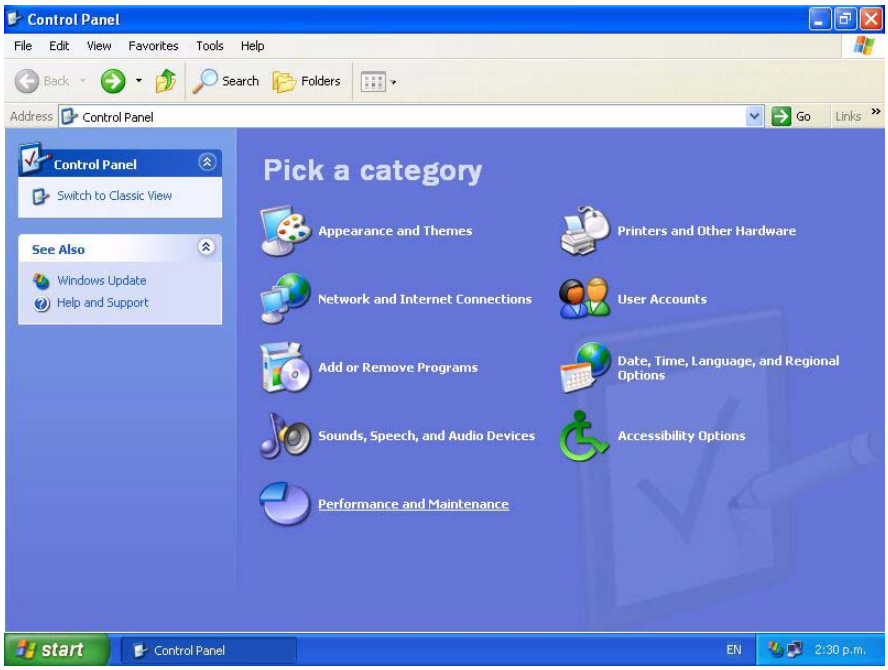
Configuring the Windows XP VPN client involves the following two stages:

Create a VPN tunnel from the PC host to the router

Note: You need to know the public IP address for the router from your Internet Service Provider (ISP) for this configuration.
This example assumes that you have already set up your internet connection.

1. On your desktop, click *Start* > *Control Panel*.

   Make sure you are in *Category View*, as shown in the following figure. If your computer is in Classic View, click **Switch to Category View** in the Control Panel Menu on the left of your screen.



2. Click *Network and Internet Connections* > *Create a connection to the network at your workplace*.

   This starts up the New Connection Wizard.

   Select *Virtual Private Network Connection* as shown in the following figure.

3. Click **Next**.

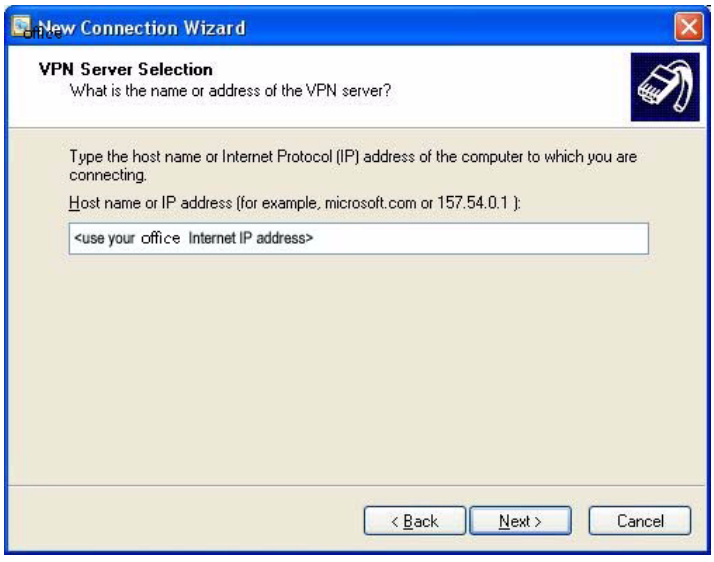
   Type in a name for the connection (e.g. VPN Connection To Head Office) as shown in the following figure.

4. Click **Next**.

   Assign an associated dialled call or select *Do not dial the initial connection*. Selecting *Do not dial the initial connection* is appropriate if you will have LAN access available before initiating the VPN call (for example, if you have a cable modem).

5. Click **Next**.

   Enter the name or IP address of the office router. This will be its Public Internet address, which the ISP will have allocated you.



6. Click **Next**.

   You have now completed creating the connection, as shown in the following figure. If you want to, check the *Add a shortcut to this connection to my desktop* check box. Then click **Finish**.

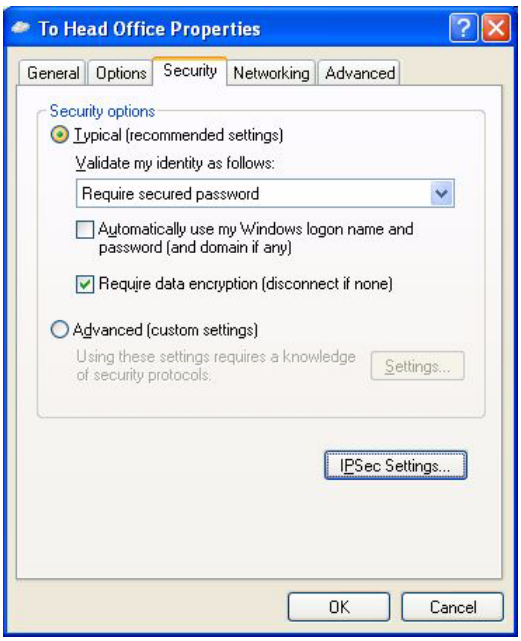
Connect to the Head Office

1. Double-click the new *Head Office* icon on your desktop or in "Network Connections" in the control panel.

2. Enter your **user name** and **password** as shown in the following figure. These are the user name and password that is (or will be) configured on the router's user database or RADIUS server.

3. Click **Properties**.

   This opens the *Head Office Properties* window. Click the **Security Tab,** as shown in the following figure.



4. Click the **IPSec Settings** button.

   This opens the *IPSec Settings* window, as shown in the following figure. Select the *Use pre-shared key for authentication* checkbox and enter your **pre-shared key**. The pre-shared key needs to be the same ISAKMP pre-shared key as is defined on the router ("Generate a random key." on page 8).

5. Click **OK**.

   This returns you to the *Head Office Properties* window.

6. Click the **Networking Tab**, as shown in the following figure. In the *Type of VPN* drop-down box, select *L2TP IPSec VPN*.

7. Click **OK.** This completes the configuration of the L2TP client. To connect to the office, click **Connect**. Note that the connection will fail if the router has not yet been configured.

Testing the tunnel

The simplest way to tell if traffic is passing through the tunnel is to perform a traceroute from the Windows XP client to a PC in the router's LAN. To do this, use the following command at the command prompt on the Windows XP client:

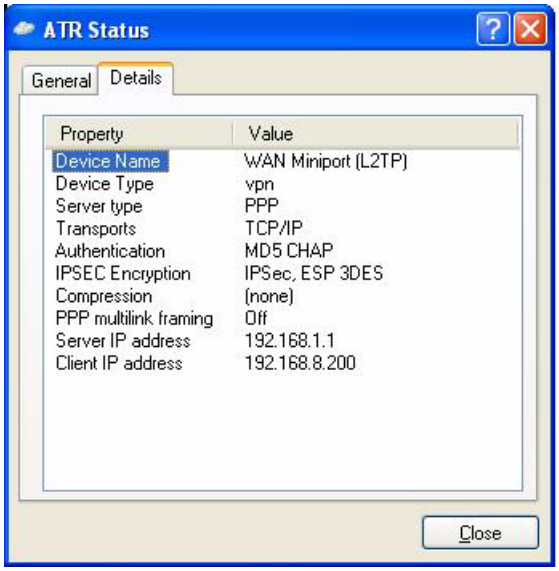
```
tracert <ip-address>
```

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.

Checking the connection from the Windows client

To check your connection details, right-click on your connection icon (e.g. Virtual Private Connection to Head Office) in the Network Connections folder, or on your desktop.

Click **Status**. Then click the **Details** tab to check your connection information, as shown in the following figure.



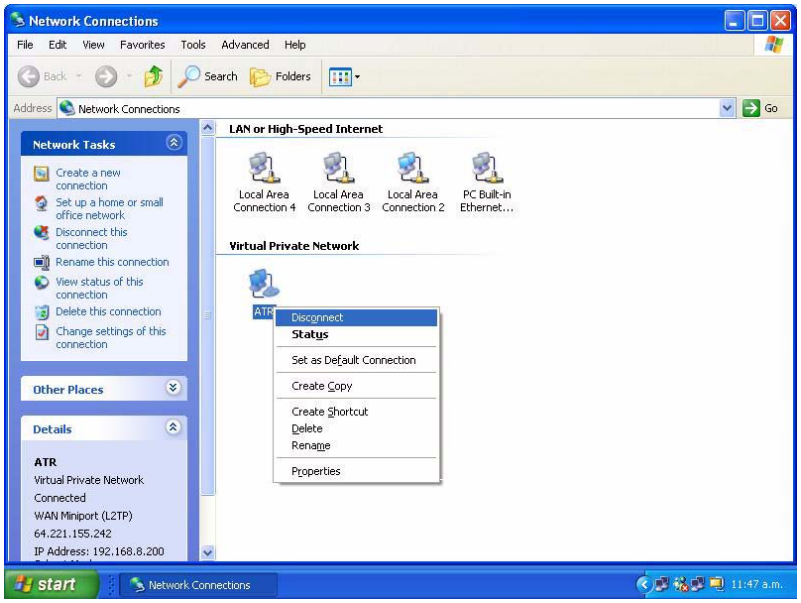
Troubleshooting

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

This How To Note has detailed information about testing and troubleshooting VPNs on the router.

Closing the connection

To close your connection, right-click on your connection icon and click **Disconnect**. The following figure shows this.



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

C613-16034-00 REV E

Connecting The IP World

Allied Telesis