

AlliedWare™ OS

How To | Create a VPN between an Allied Telesis Router and a Microsoft Windows 7 Client, with or without NAT-T

Introduction

This document describes how to provide secure remote access through IP security (IPsec) Virtual Private Networks (VPNs), with an emphasis on using an Allied Telesis router at a head office and roaming Windows 7 clients. 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 your 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.

What information will you find in this How To Note?

This How To Note starts with the configuration for a head office router on [page 4](#). This configuration allows the head office to create concurrent VPN tunnels with:

- Windows 7 roaming clients. The configuration for these starts on [page 9](#).
- Windows XP, Vista and 2000 roaming clients. This Note does not include the configuration for these. See the How To Notes *How To Create a VPN between an Allied Telesis Router and a Microsoft Windows XP Client, over NAT-T*; and *How to Create Concurrent VPNs with Remote Routers, Microsoft Windows Vista Clients and XP Clients, over NAT-T*.

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.

Which products and software version does this apply to?

This How To Note applies to the following routers and switches, running AlliedWare software version 291-08 or later:

- AR400 Series routers
- AR750S and AR770S routers
- Rapier i Series switches
- AT-8800 Series switches

It requires firewall and 3DES licenses. If these licenses are not already installed on your device, you can purchase them from your Allied Telesis distributor.

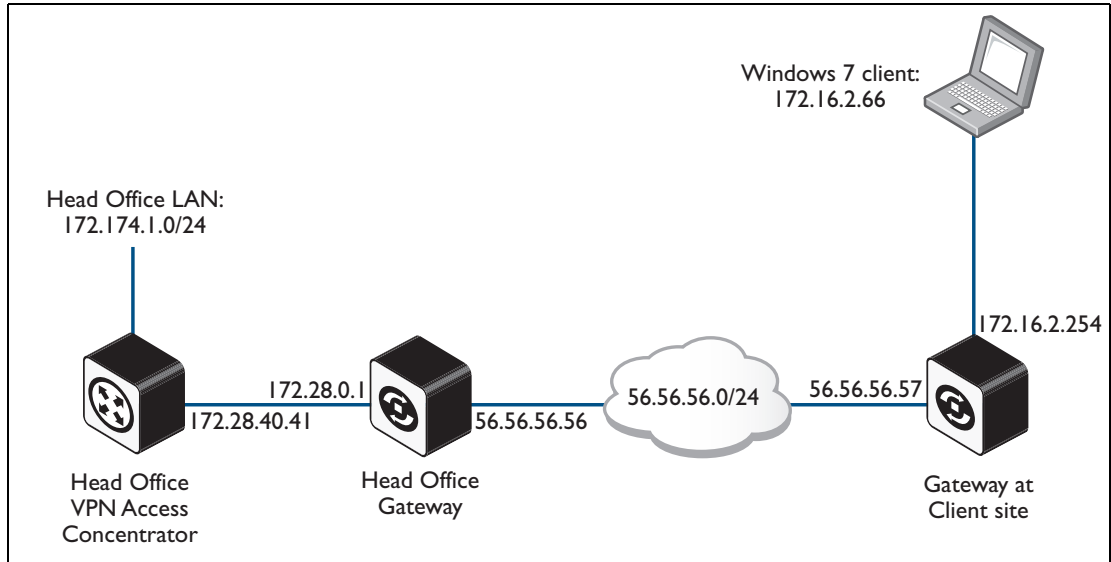
Contents

Introduction	1
What information will you find in this How To Note?	1
Related How To Notes	2
Which products and software version does this apply to?	2
The network	3
Network diagram	3
Configure the head office router	4
Initial security setup	4
Configuration template	6
Configure a Microsoft Windows 7 client	9
Create the connection	9
Modify the connection	14
Connect	19
Introducing NAT into the path between the client and the router	20
Appendix	21

The network

Network diagram

We set up the solution in a lab, using the network shown in the following diagram:



The diagram shows a head office and a remote client.

Configure the head office router

Initial security setup

Before adding the ISAKMP and IPsec configuration, set up the router with the following important details.

1. Create two keys to use for Secure Shell (SSH).

Use the commands:

```
create enco key=1 description="Server Key" type=rsa length=768 format=ssh
create enco key=2 description="Host Key" type=rsa length=1024 format=ssh
```

After each of these commands, the router displays the following information:

```
Info (1073278): RSA Key Generation process started.
Manager >
Info (1073279): RSA Key generation process completed.
```

2. Create a third key for ISAKMP to use as a preshared key.

For security reasons, **do not use the same value as this example.**

Use the command:

```
create enco key=3 description="ISAKMP PSK" type=general value=secret
```

We use this encryption key on the Windows 7 client (see [step 4 on page 17](#)).

3. Check the key configuration.

Use the command:

```
show enco key
```

This results in the following output:

ID	Type	Length	Digest	Description	Mod	IP
1	RSA-PRIVATE	768	A40EB1F4	Server Key	-	-
2	RSA-PRIVATE	1024	2BB712B4	Host Key	-	-
3	GENERAL	6	EE635A9D	ISAKMP PSK	-	-

4. Check feature licences.

Check that you have a 3DES feature licence for the ISAKMP policy.

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor.

If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

5. Add a security officer.

Add a security officer. This step is important because a security officer must exist before you enable system security (which you do in the next step).

```
add user=secoff pass=<password> priv=securityOfficer telnet=yes login=yes
```

After this command, the router displays the following information.

```
Number of Radius-backup users..... 0

User Authentication Database
-----
Username: secoff ()
  Status: enabled   Privilege: Sec Off  Telnet: yes  Login: yes  RBU: no
  Logins: 0         Fails: 0       Sent: 0     Rcvd: 0
  Authentications: 0 Fails: 0
-----
```

6. Enable system security.

Enable system security so that the newly created keys will be stored permanently. They would otherwise be deleted if the router restarted.

```
enable system security
```

Once security mode is enabled, you need to log in as the security officer to enter most configuration-altering commands.

7. Save the configuration and set the router to use it at startup.

Use the command:

```
create config=vpn.cfg set
```

Configuration template

This section contains a configuration script for the head office. You can copy and paste the script to an editor on your PC, modify addresses, passwords and any other requirements for all your individual sites, and then use TFTP, HTTP or ZMODEM to transfer the files to your routers.

Please refer to the “Managing Configuration Files and Software Versions” chapter in the *Software Reference* for more information about loading files onto the router.

For detailed explanations about the CLI configuration, see the *How To Note How To Configure VPNs In A Corporate Network, With Optional Prioritisation Of VoIP*.

```
set system name="Head Office"

# User configuration
add user=secoff pass=<your-secoff-password> priv=securityOfficer lo=yes
set user=secoff telnet=yes netmask=255.255.255.255
add user=win7_user pass=<user-password> lo=no

# PPP templates configuration
create ppp template=1
set ppp template=1 bap=off ippool="myippool" authentication=chap
  mssheader=120 echo=30

# L2TP configuration
enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 pptemplate=1

# VLAN general configuration
create vlan="vlan100" vid=100

# VLAN port configuration
add vlan="100" port=1-5

# IP configuration
enable ip
add ip int=eth0 ip=172.28.40.41
add ip int=vlan100 ip=172.174.1.254 mask=255.255.255.0
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=172.28.0.1
create ip pool="myippool" ip=192.168.66.66-192.168.66.77
add ip dns prim=10.32.16.105 seco=202.49.72.50
```

```

# Firewall configuration
enable firewall
enable firewall notify=mail to=<administrator-email-address>
create firewall policy="fw"
create firewall policy="fw" dy=dynamic
add firewall policy="fw" dy=dynamic us=ANY
enable firewall policy="fw" icmp_f=all
add firewall policy="fw" int=vlan100 type=private
add firewall policy="fw" int=dyn-dynamic type=private
add firewall policy="fw" int=eth0 type=public

# NAT for local users
add firewall poli="fw" nat=enhanced int=vlan100 gblin=eth0

# NAT for the IPsec users
add firewall poli="fw" nat=enhanced int=dyn-dynamic gblin=eth0

# Permit incoming SSH
add firewall poli="fw" ru=1 ac=allo int=eth0 prot=tcp po=22 ip=172.28.40.41
  gblip=172.28.40.41 gblp=22

# Permit incoming ISAKMP
add firewall poli="fw" ru=2 ac=allo int=eth0 prot=udp po=500 ip=172.28.40.41
  gblip=172.28.40.41 gblp=500

# Permit ESP over UDP (for IPsec NAT-T)
add firewall poli="fw" ru=3 ac=allo int=eth0 prot=udp po=4500 ip=172.28.40.41
  gblip=172.28.40.41 gblp=4500

# Permit L2TP specifically over IPsec
add firewall poli="fw" ru=4 ac=allo int=eth0 prot=udp po=1701 ip=172.28.40.41
  gblip=172.28.40.41 gblp=1701 encap=ipsec

# Do not apply NAT on incoming traffic destined for private LAN addresses if
  that traffic has come in encapsulated in IPSEC
add firewall poli="fw" ru=5 ac=non int=eth0 prot=ALL ip=172.174.1.0-
  172.174.1.254 enc=ips

# SSH configuration
enable ssh server serverkey=1 hostkey=2 expirytime=0 logintimeout=60
add ssh user=secoff password=secoff

# IPSEC configuration
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hash=sha
set ipsec sas=1 mod=transport
create ipsec sas=2 key=isakmp prot=esp enc=3desouter hash=md5
set ipsec sas=2 mod=transport
create ipsec sas=3 key=isakmp prot=esp enc=des hash=sha
set ipsec sas=3 mod=transport
create ipsec sas=4 key=isakmp prot=esp enc=des hash=md5
set ipsec sas=4 mod=transport
create ipsec bund=1 key=isakmp string="1 or 2 or 3 or 4"

```

```
# ISAKMP and NAT-T encapsulated data are permitted in/out, without being
  processed by IPsec
create ipsec pol="isakmp" int=eth0 ac=permit lp=500 rp=500
create ipsec pol="natt_udp" int=eth0 ac=permit lp=4500
# The Windows client will match the following policy
create ipsec pol="windows_warriors" int=eth0 ac=ipsec key=isakmp bund=1
  peer=ANY isa="windows_isakmp" lp=1701 tra=UDP
# All other traffic is defined here.
create ipsec pol="internet" int=eth0 ac=permit
enable ipsec

# ISAKMP configuration
create isakmp pol="windows_isakmp" pe=any enc=3desouter key=3 natt=true gro=2
enable isakmp
```


Configure a Microsoft Windows 7 client

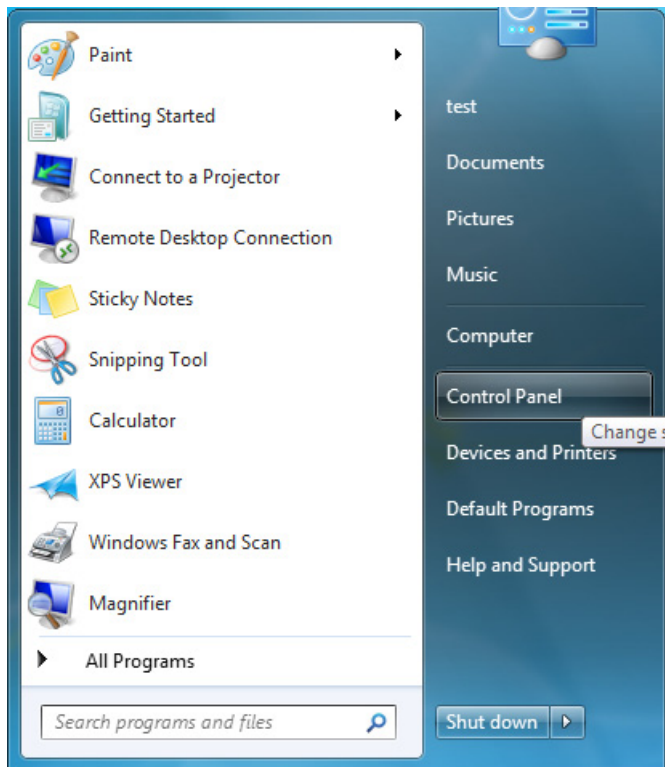
This section describes how to set up a VPN between a Windows 7 client and the Head Office.

Note: No special patches or service packs are required. A registry change is required in one specific circumstance, which is described towards the end.

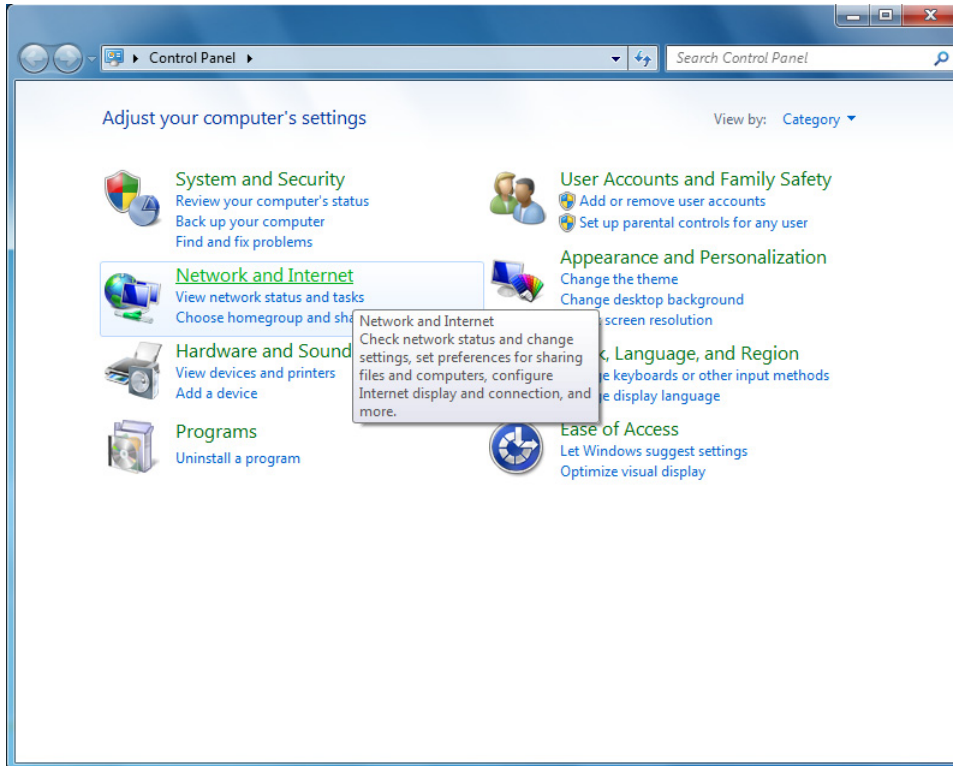
Create the connection

I. Open the Network and Sharing Center.

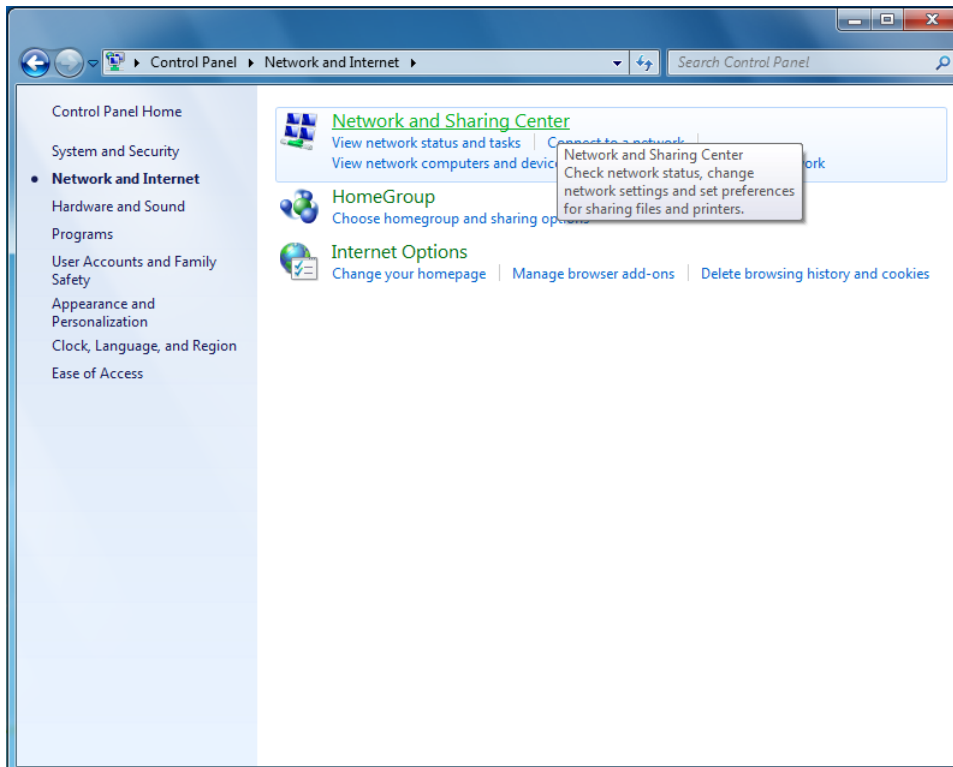
Open the **Start** menu and click **Control Panel**.



Within the Control Panel, select **Network and Internet**.

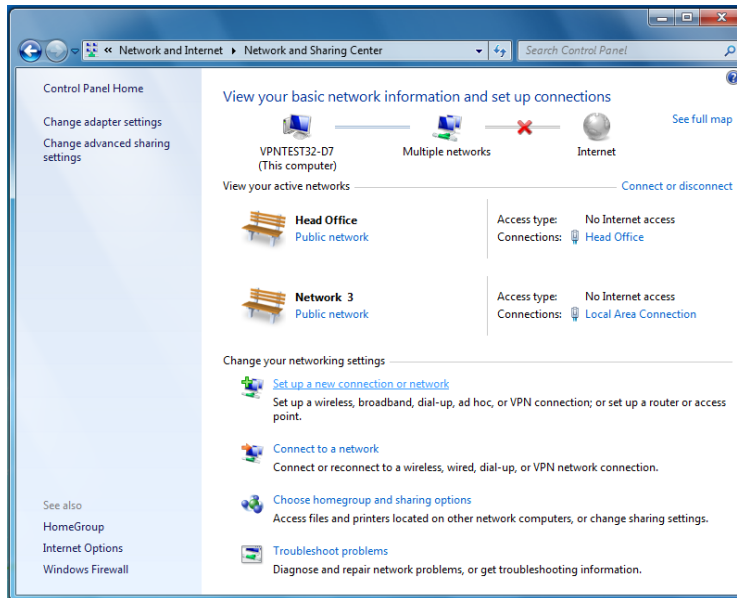


Now choose **Network and Sharing Center**.



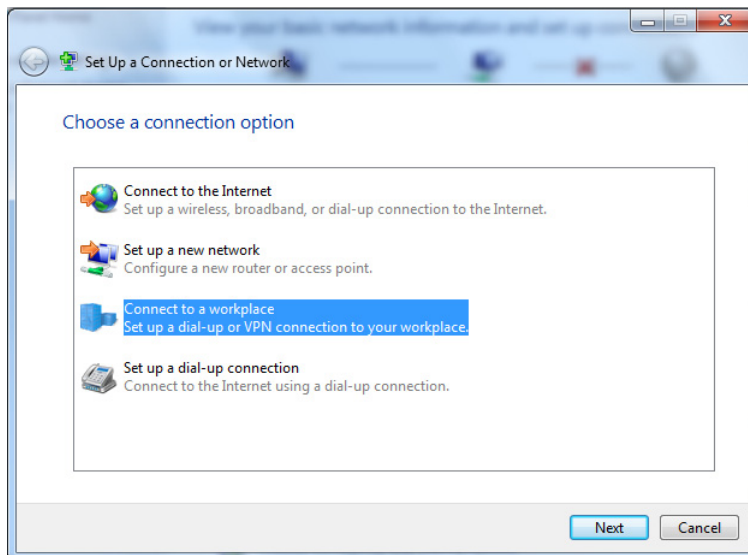
2. Set up a new connection.

In the **Network and Sharing Center**, click **Set up a new connection or network**.



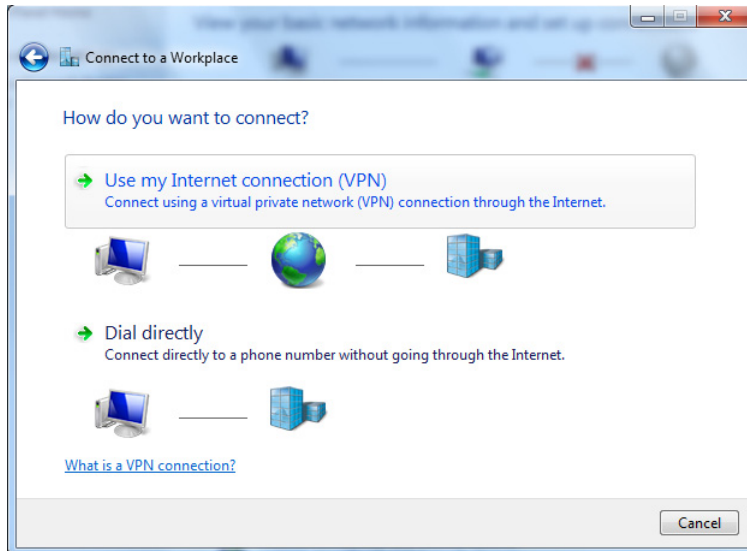
3. Select the connection option.

On the first page of the wizard, select **Connect to a workplace** and click **Next**:



4. Select to connect through a VPN.

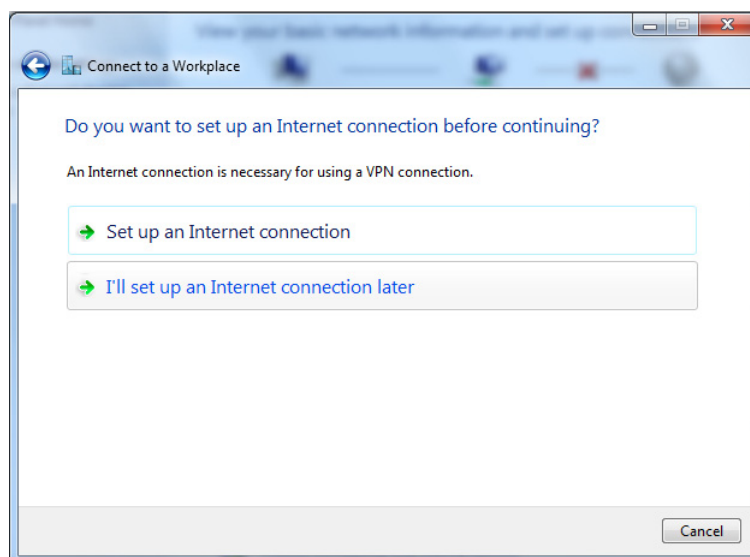
Select **Use my Internet connection (VPN)** and click **Next**.



5. Choose not to set up an Internet connection.

Select **I'll set up an Internet connection later** and click **Next**.

In this example, we assume that the VPN will be initiated over the user's cable modem at home or (when the user is travelling) from a hotel local area network. Therefore the VPN will be initiated over a connection that is already up. If you are instead connecting via dial-up, you might need to set up a dial-up connection. You can do that at this stage, or later.

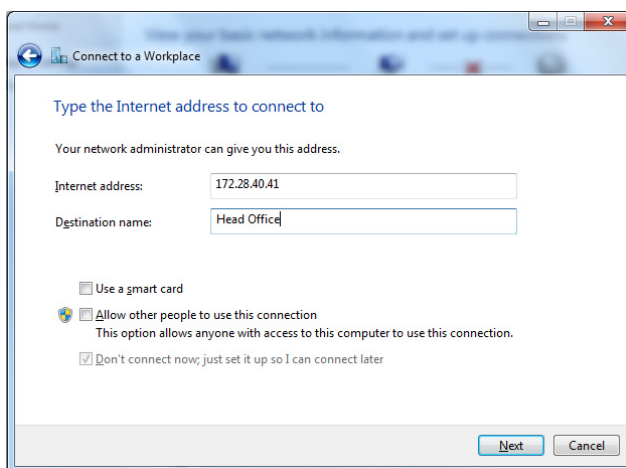


6. Type in the Internet address to connect to.

- In the **Internet address** field, type in the IP address of the Head Office. In the example shown below, the IP is 172.28.40.41.
- In the **Destination name** field, give the connection a meaningful name. The name has no effect on the operation of the VPN, it is just the connection name that appears in the list of network connections.

In this example, we do not use the smart card option. As administrator, you need to decide whether to use the smart card, and whether to allow other people who use this Windows 7 PC to access this VPN connection.

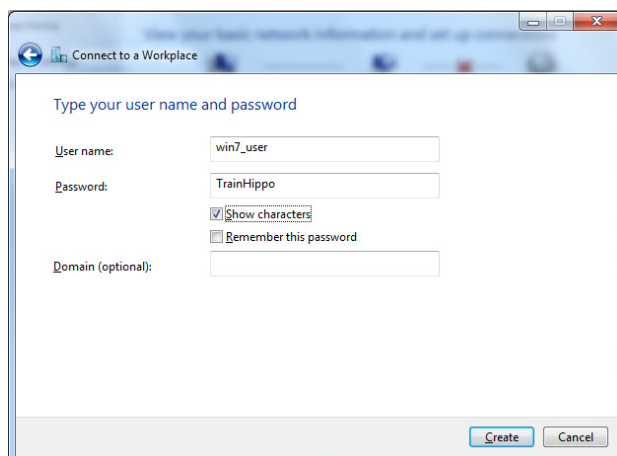
Click **Next**.



7. Choose a user name and password.

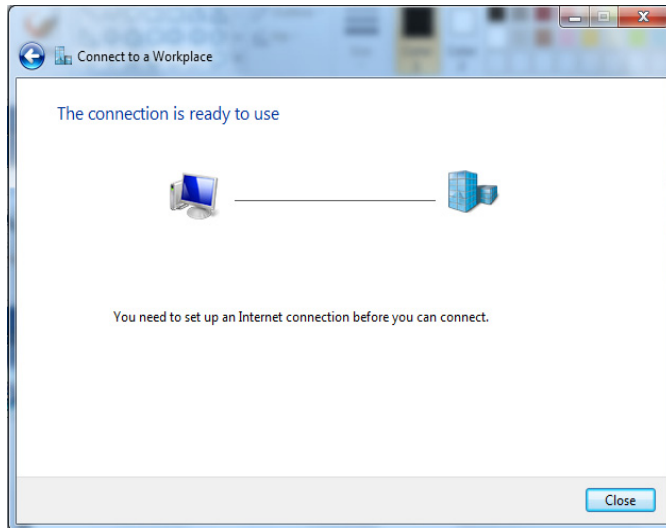
Enter a user name and password, and choose whether to have Windows 7 remember the password. We recommend **not** letting Windows 7 remember passwords, particularly on a laptop. If the laptop is stolen, the VPN connection could be initiated by the thieves.

Then click **Create**.



8. Close the wizard.

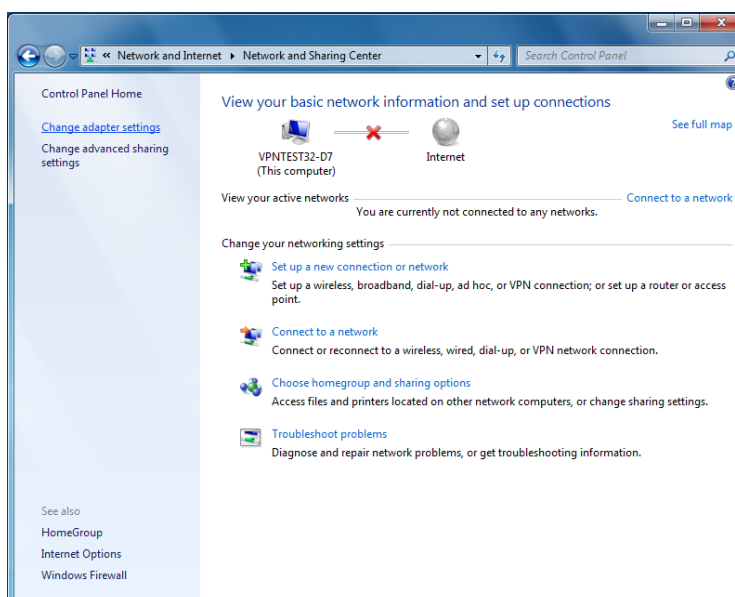
Windows 7 informs you that the connection is ready to use, but it is **not** yet ready. Ignore the message about setting up an Internet connection and click **Close**.



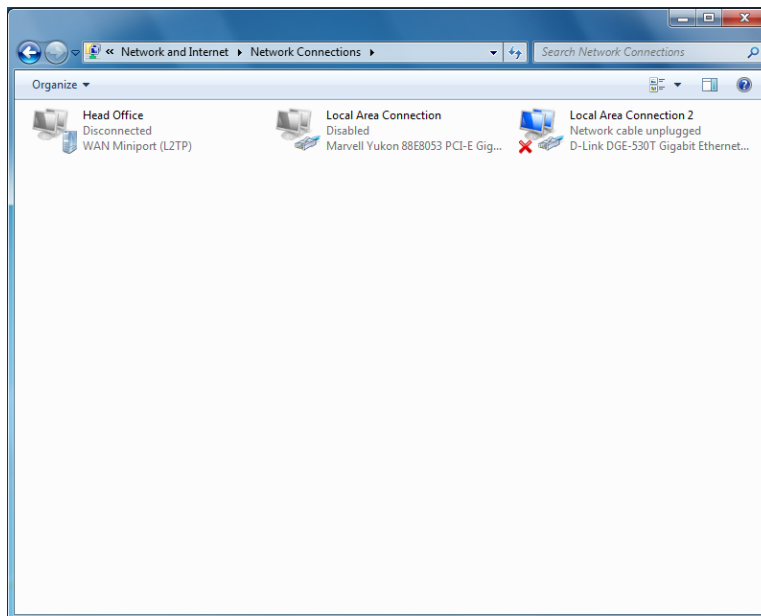
Modify the connection

1. Open the Head office connection properties.

From the **Networking and Sharing Center**, click **Change adapter settings**.



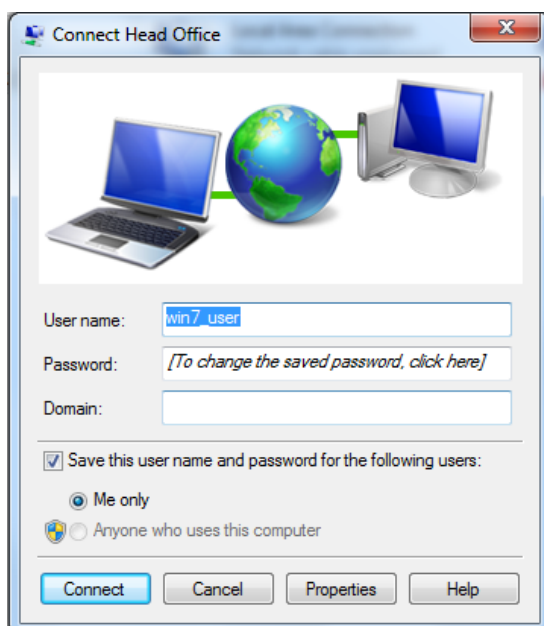
From the resulting window, choose **Head Office**.



Open the Head Office properties by either:

- double-clicking on it. This is possible if there is network connectivity, which you can see by looking for a PC shaped icon to the right of the connection name.
- right-clicking on it and choosing **Properties**. If there is no connectivity, you have to do this.

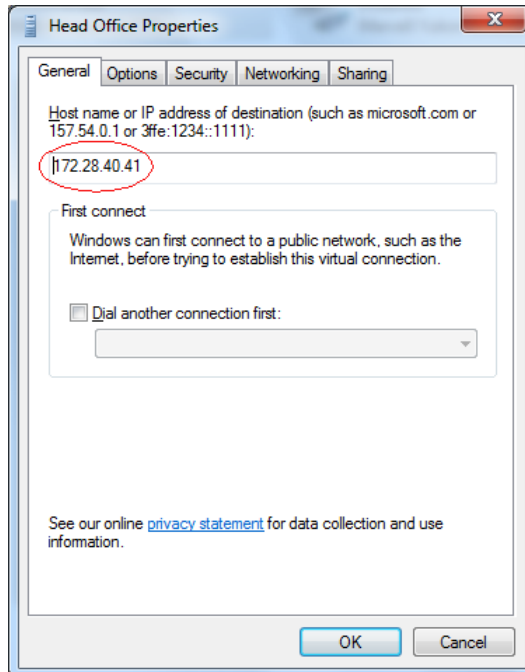
In this example, the connection is present, so you can double-click. This displays the following window:



Click **Properties**.

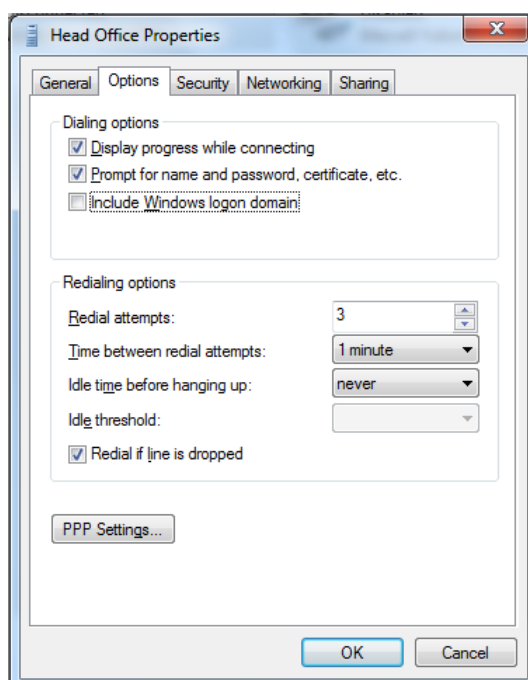
2. Check the destination address.

On the **General** tab, the destination address should be the IP address of the Head Office router.



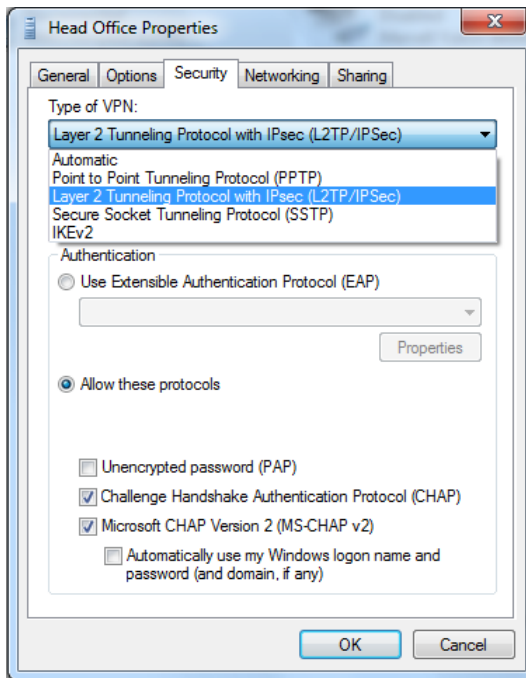
3. Configure the options settings.

On the **Options** tab, deselect the **Include Windows logon domain** checkbox if you do not need it or do not know what it is.



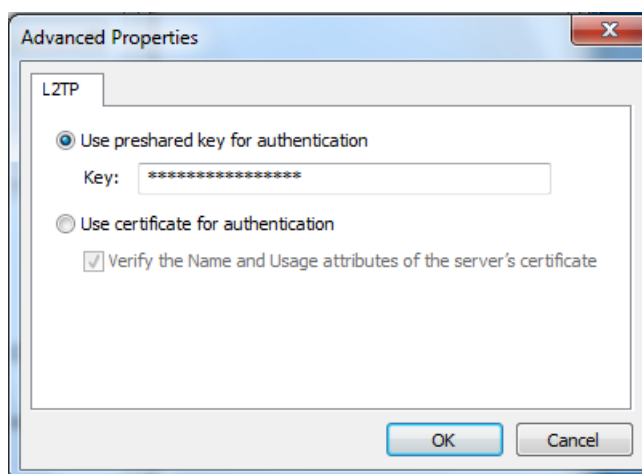
4. Configure the security settings.

On the **Security** tab, set the **Type of VPN** to **L2TP/IPSec**.



Click **Advanced Settings** and enter the preshared key into the resulting window.

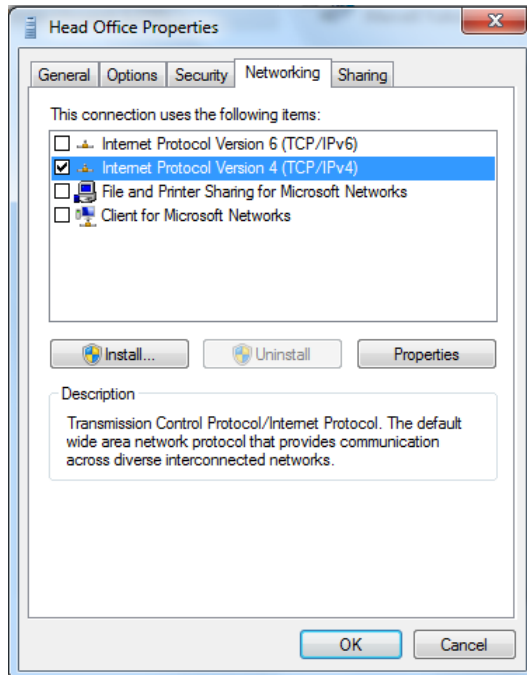
Click **OK**.



Under **Allow these protocols**, deselect **Automatically use my Windows logon name and password (and domain, if any)**, because this example does not use this option. CHAP v2 is also unnecessary so you can optionally deselect it.

5. Configure the networking settings.

On the **Networking** tab, you may also deselect any of the protocols and networks in the box below except for **Internet Protocol Version 4 (TCP/IPv4)**. The IPsec tunnel will complete faster if you turn **off** unnecessary protocols and networks.



Connect

1. If necessary, start the connection that the VPN will initiate over.

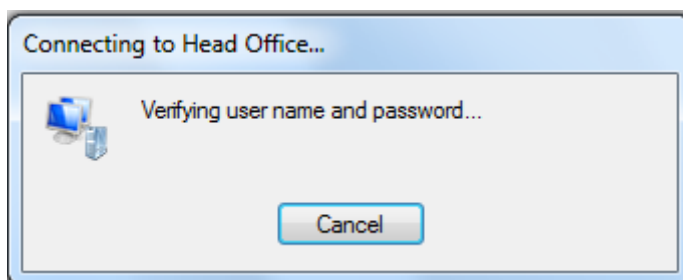
If you are not connected to a LAN, start the connection that the VPN will initiate over (such as dialup).

2. Start the VPN.

Open the **Connect Head Office** window and enter the username and password. Click **Connect**.



You will see a process dialog as the VPN tunnel is negotiated.



Introducing NAT into the path between the client and the router

If one or both of the gateway routers that are present in the path between the client PC and the router are performing NAT, then the VPN connection will need to use NAT-T.

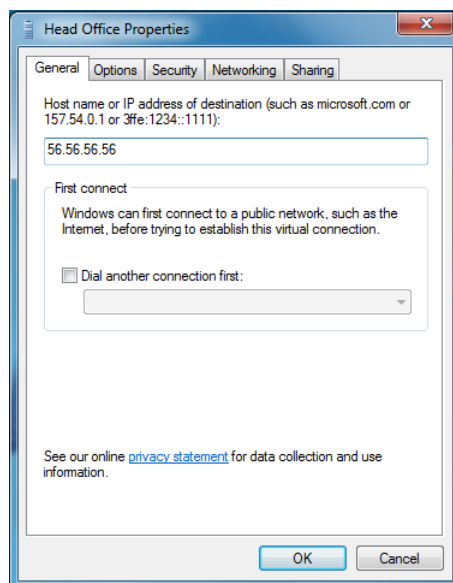
The configuration described in the preceding pages was tested in each of the following scenarios:

- **Scenario 1**
With the gateway at the client site performing NAT.
- **Scenario 2**
With both the gateway at the client site and the gateway at the server site performing NAT.

In **scenario 1**, the VPN connection was successfully established without needing to make any configuration changes to the Windows 7 client or the VPN router.

In **scenario 2**, it was necessary to make two changes to the client PC's configuration:

1. The target IP address of the VPN connection was changed to point to the public IP address of the gateway router at the server end. This is because the LAN at the server site is now "hidden" behind this public IP address.



2. Also necessary was the registry change described in the Microsoft knowledge base article at: <http://support.microsoft.com/kb/926179> - *How to configure an L2TP/IPsec server behind a NAT-T device in Windows Vista and in Windows Server 2008*. Although this article is written for Vista and Server 2008, it applies equally to Windows 7.

This change was necessary because the default setting for Windows, for security reasons, is to not allow VPN connections to VPN servers that reside behind a NATing gateway.

Appendix

The configurations used on the gateway routers are:

1. Gateway at client site.

```
enable ip
add ip int=eth0 ip=172.16.2.254
add ip int=eth1 ip=56.56.56.57
add ip route=172.28.0.0 mask=255.255.0.0 int=eth1 next=56.56.56.56
```

```
enable firewall
create firewall policy=nat
enable firewall policy=nat icmp_forward=all
add firewall policy=nat int=eth0 type=private
add firewall policy=nat int=eth1 type=public
add firewall policy=nat nat=enhanced int=eth0 gblint=eth1
```

2. Gateway at server site.

```
enable ip
add ip int=eth0 ip=56.56.56.56
add ip int=vlan1 ip=172.28.0.1
add ip route=172.16.0.0 mask=255.255.0.0 int=eth0 next=56.56.56.57
```

```
enable firewall
create firewall policy=nat
enable firewall policy=nat icmp_forward=all
add firewall policy=nat int=vlan1 type=private
add firewall policy=nat int=eth0 type=public
add firewall policy=nat nat=enhanced int=vlan1 gblint=eth0
add firewall poli=nat rule=1 act=allow int=eth0 prot=udp port=500
    ip=172.28.40.41 gblip=56.56.56.56 gblport=500
add firewall poli=nat rule=2 act=allow int=eth0 prot=udp port=4500
    ip=172.28.40.41 gblip=56.56.56.56 gblport=4500
```