

# AlliedWare<sup>TM</sup> OS

How To | Create a VPN between an Allied Telesis Router and a Microsoft Windows 2000<sup>1</sup> Client, Without Using 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 staff who work from home.

You should use the companion Note How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows 2000 Client, Over NAT-T instead, if:

- the Allied Telesis router is connected to the Internet through a NAT gateway device, such as an ADSL modem, and/or
- you want to let travelling staff connect to your office from such places as hotel rooms.

This companion How To Note is available from www.alliedtelesis.com/resources/literature/ howto.aspx.

### 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 people who sometimes work from home. 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.

Each staff member has a laptop or PC with Windows 2000 installed.

C613-16004-00 REV D

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

This document describes how to configure the Windows system to use IPSec VPN to connect to your office through the AR415S router.

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

## 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 2.3.1 and was tested using a PC running Microsoft Windows 2000 Professional, Service Pack 4.

### **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.

Page 2 | AlliedWare<sup>™</sup> OS How To Note: VPNs with Windows 2000 clients, without NAT-T

## **Security issue**

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, refer to Microsoft Knowledge Base article 172430 by following this link: support.microsoft.com/default.aspx?scid=172430.

This solution works on both Windows 2000 and Windows XP.

## **Example network**

The following figure shows an example of a network that could use this configuration.



## **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 5. 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 or TFTP.
- 5. "Set the router to use the configuration" on page 7.
- 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.

I. 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.

### 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 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
# 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.
add user=dialin1 pass=friend1 login=no
add user=dialin2 pass=friend2 login=no
add user=dialin3 pass=friend3 login=no
add user=dialin4 pass=friend4 login=no
add user=secoff pass=<your-password> priv=securityOfficer login=yes
set user=secoff description="Security Officer Account"
# If RADIUS server support is needed, use a line such as this:
# add radius server=<your-RADIUS-server-address> secret=<secret-key>
# All dynamic incoming L2TP calls will associate with this PPP template
# as indicated below.
create ppp template=1 bap=off ippool="ip" authentication=chap echo=10
   lqr=off
# To cater for dynamic creation of incoming L2TP calls enter the
# following commands.
enable 12tp
enable 12tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
# The IP address allows for any valid Internet address.
enable ip
add ip int=vlan1 ip=<office-private-LAN-address>
add ip int=eth0 ip=<office-Internet-address> mask=<appropriate-mask>
# The default route to the Internet.
add ip route=0.0.0.0 mask=0.0.0.0 int=eth0
  next=<your-Internet-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).
create ip pool=ip ip=<pool-range>
```

```
# Firewall
enable fire
create fire poli=main
create fire poli=main dy=dynamic
add fire poli=main dy=dynamic user=ANY
add fire poli=main int=vlan1 type=private
# Dynamic private interfaces are accepted from L2TP, which are from
# IPSec only.
add fire poli=main int=dyn-dynamic type=private
add fire poli=main int=eth0 type=public
# The firewall allows for internally generated access to the Internet
# through the following NAT definition.
add fire poli=main nat=enhanced int=vlan1 gblint=eth0
# This NAT definition allows Internet access for remote VPN users by
# providing address translation.
add fire poli=main nat=enhanced int=dyn-dynamic gblint=eth0
add fire poli=main rule=1 int=eth0 action=allow prot=udp
   ip=<office-Internet-address> port=500
   gblip=<office-Internet-address> gblpo=500
# Rule 2 becomes the L2TP tunnel allow rule. Additional security is
# provided by only allowing traffic from IPSec tunnels.
add fire poli=main rule=2 int=eth0 action=allow prot=udp
   ip=<office-Internet-address> port=1701
   gblip=<office-Internet-address> gblpo=1701 encap=ipsec
create ipsec sas=1 key=isakmp prot=esp encalg=3desouter hashalg=sha
  mode=transport
create ipsec sas=2 key=isakmp prot=esp encalg=3desouter hashalg=md5
  mode=transport
create ipsec sas=3 key=isakmp prot=esp encalg=des hashalg=sha
   mode=transport
create ipsec sas=4 key=isakmp prot=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"
create ipsec policy=isakmp int=eth0 action=permit lport=500 rport=500
# This is a generic IPSec policy that multiple IPSec remote PC clients
# can connect through.
create ipsec policy=to HQ int=eth0 action=ipsec key=isakmp bundle=1
   peer=any isa=keys
set ipsec policy=to_HQ transport=udp rport=1701
# The following policy allows for internally generated Internet access.
create ipsec policy=Internet int=eth0 act=permit
enable ipsec
create isakmp policy=keys peer=any key=1
set isakmp policy=keys sendd=true
enable isakmp
```

### 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 2000 VPN client involves the following stages:

- "Add a new registry entry", on this page
- "Add the IP Security Policy Management snap-in" on page 9
- "Create an IP Security Policy" on page 11
- "Create an IP Security Rule" on page 13
- "Create an IP Filter" on page 16
- "Configure the connection" on page 23

### Add a new registry entry

To ensure compatibility, you need to make a change to the registry. This Windows registry change allows the Windows client to bypass the default encryption scheme, and allows for user defined encryption parameters, or no encryption.

I. On your desktop, select **Start > Run** and enter the following command:

regedit

Then click **OK**.

This opens the Registry Editor.

- In the Registry Editor, browse to the following folder: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- Right-click on this folder and select New > DWORD Value. This creates a new entry.
- 4. Name the new entry "ProhibitlpSec".
- 5. Double-click on the **ProhibitIpSec** entry. This opens a dialog box with the entry's settings.
- 6. In the Value data field, enter 1. Click OK.
- 7. Restart Windows 2000 so that the changes take effect.

## Add the IP Security Policy Management snap-in

- **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.
- I. On your desktop, select **Start > Run** and enter the following command:

mmc

This opens the Console window, as shown in the following figure.

🚡 Console1	_ 🗆 🗙
📙 Console 🔟 indow Help 📙 🗅 😂 🔚 💷	1 a -
Console Root	
Action ⊻iew Eavorites ← →   📾 📧   😤	
Tree Favorites Name	
Console Root	

2. Select Console Root > Add/Remove Snap-In.

This opens the Add/Remove Snap-in window, as shown in the following figure.

Add/Remove Snap-i	n	? ×
Standalone Extensi	ons	
Use this page to ad	d or remove a standalone Snap-in from the consol	e.
<u>Snap-ins added to:</u>	Console Root	
		_
		- 1
Description		
<u>Add</u>	<u>Remove</u> <u>About</u>	
	OK	Cancel
		110

3. Click Add.

This opens the Add Standalone Snap-In window.

Scroll down the list of Available Standalone Snap-ins and select IP Security Policy Management, as shown in the following figure.

Snap-in	Vendor	-
∯Fax Service Management ■Folder	Microsoft Corporation	
😼 Group Policy	Microsoft Corporation	
😫 Indexing Service	Microsoft Corporation, I	
IP Security Policy Management Link to Web Address		
🕼 Local Users and Groups	Microsoft Corporation	
🗱 Performance Logs and Alerts	Microsoft Corporation	
Pemovable Storage Management	HighGround Systems, Inc.	
Security Configuration and Analysis	Microsoft Corporation	-
Description Internet Protocol Security (IPSec) Admir	nistration. Manage IPSec	
policies for secure communication with o	other computers.	

### 4. Click Add.

This opens the Select Computer window, which lets you select the computer or domain that the snap-in will manage. Select Local computer, as shown in the following figure.

lect Computer			?
Select which computer this Snap-in When this console is saved the location	will manage on will also be saved		
Local computer     The computer this console is upping on			
Manage domain policy for this computer	r's domain		
O Manage domain policy for another dom	ain:		
	-		
O Another computer:			
	Blowse		
	2 Beach	Circle 1	Consol

5. Click Finish, then Close, then OK, to return to the Console window.

Page 10 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

## **Create an IP Security Policy**

1. On the Console window, **click**, then **right-click** IP Security Policies on Local Machine.

http://www.comsole.com/active.com	licies on Local Machine]		
📔 🔓 Console 🛛 Window Help		🗋 🖨 🖬 🔳	Ð×
	🖬 🗗 🗛 🔮 📋	<u>≞</u>	
Tree Favorites	Name A	Description	Policy
Console Root	<ul> <li>☑ Client (Respond Only)</li> <li>☑ Secure Server (Requir</li> <li>☑ Server (Request Secur</li> </ul>	Communicate normally (unse For all IP traffic, always requir For all IP traffic, always reque	No No

### 2. Select Create IP Security Policy.

This opens the IP Security Policy Wizard, as shown in the following figure.



Page II | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

3. Click **Next**, then enter a name for your security policy (e.g. "To Head Office"), as shown in the following figure.

Security Policy Name	and optionally aire	it a brief deserie	tion	
Name this security policy	anu optionally give	en a brier descrip	NION	
Na <u>m</u> e:				
To Head Office				
Description:				
				*
				-
·				

#### 4. Click Next.

This opens the Requests for Secure Communication window. Clear the Activate the default response rule checkbox, as shown in the following figure.

Security Policy Wizard		1
Requests for Secure Communicatio	)n	
Specily now this policy responds to h	equests for secure communicat	lion.
The default response rule responds to other rule applies. To communicate s secure communication.	o remote computers that reque: ecurely, the computer must res	st security, when no pond to requests for
Activate the default response rule		

Page 12 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

5. Click **Next.** You have now completed the IP Security Policy Wizard, as shown in the following figure.

IP Security Policy Wizard	? ×
	Completing the IP Security Policy Wizard You have successfully completed specifying the properties for your new IP security policy. To edit your IP security policy now, select the Edit properties check box, and then click Finish. Edit properties To close this wizard, click Finish.
	< <u>B</u> ack Finish Cancel

6. Leave the Edit properties checkbox checked. Click Finish.

## **Create an IP Security Rule**

1. Clicking Finish in the previous step opens the *IP Security Policy Properties* window, as shown in the following figure.

Head Office Prope	rties	?
Rules General		
🥿 🛋 Security ru	les for communicating with	other computers
IP Security Rules:	Filter Action	Authentication Tu
Oynamic>	Default Response	Kerberos Nc
A <u>d</u> d	Edit	Use Add <u>W</u> izard
		OK Cancel

Page 13 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

2. Click Add. This opens the Security Rule Wizard, as shown in the following figure.



#### 3. Click Next.

The next window lets you specify the tunnel endpoint for the IP Security rule, if required.

A tunnel endpoint is not required for this example. Therefore, make sure This rule does not specify a tunnel is selected, as shown in the following figure.

curity Rule	Wizard						?
Tunnel En The tun as spec	<b>dpoint</b> nel endpoint is l ified by the sect	he tunneling c urity rule's IP fi	computer Iter list.	closest to t	he IP traffic (	destination,	
An IPSe security	c tunnel allows level of a direct	packets to tra , private conne	verse a p ection be	ublic or pri tween two	vate interneti computers.	work with th	ne
Specify	the tunnel endp	oint for the IP	security r	ule:			
This	rule does not s	pecify a tunne	ļ				
C The	tunnel endpoin	t is specified b	ythis <u>I</u> P	address:			
	0.0	. 0 .	0	7			
J.,							
				< Back	Next	<u>_</u>	Cancel
				( Dack	<u>H</u> ent		Carloer

Page 14 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

### 4. Click Next.

The next window lets you specify the network type the IP Security rule applies to. Make sure the *All network connections* option is selected, as shown in the following figure.

curity Rule Wizard			? 2
Network Type The security rule must be applied to a n	etwork type.		Ē
Select the network type:			
All network connections			
Local area network (LAN)			
C <u>R</u> emote access			
		r	
	< Back	Next>	Cancel

#### 5. Click Next.

The next window lets you specify the authentication method for the IP Security rule. Select the Use this string to protect the key exchange (preshared key) option, as shown in the following figure.

Security Policy Wizard		?
Authentication Method To add multiple authentication methods, ed IP security rule wizard.	it the security rule after com	oleting the
Set the initial authentication method for this	security rule:	
O Windows 2000 default (Kerberos V5 pro	tocol)	
O Use a certificate from this Certificate Au	hority (CA):	
		Browse
<ul> <li>Use this string to protect the key exchange</li> </ul>	nge (preshared key):	
<enter isakmp="" key="" preshared="" your=""></enter>		
		*
	<back next=""></back>	Cancel
		<b></b>

In the text box underneath the option, **enter a preshared key** that is known to both the router and the client.

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 4).

## **Create an IP Filter**

I. Click Next.

The next window, shown in the following figure, lets you specify the IP filter for the type of IP traffic the IP Security rule applies to.

f no IP filter in the followin	ig list matches your needs, click Add to create	e a new one.
P filter lists: Name	Description	<u>A</u> dd
O All ICMP Traffic O All IP Traffic	Matches all ICMP packets bet Matches all IP packets from t	<u>E</u> dit
		<u>R</u> emove

2. Click Add to start creating a new filter.

This opens the IP Filter List Name window. Enter a *name* (e.g. "L2TP Tunnel Filter"), as shown in the following figure.

ame: 2TP Tu	nnal Filter			
escriptio	n:			<u>A</u> dd
			<u> </u>	<u>E</u> dit
			*	<u>B</u> emove
ilter <u>s</u> :				Use Add <u>W</u> izard
Mirrored	Description	Protocol	Source Port	Destination

Page 16 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

3. Click Add. This starts the IP Filter Wizard, as shown in the following figure.



#### 4. Click Next.

This opens the IP Traffic Source window. Select My IP Address from the Source address dropdown box, as shown in the following figure.

Filter Wizard	? ×
IP Traffic Source Specify the source address of the IP traffic.	Ē
Source address:	
My IP Address	
< <u>B</u> ack <u>N</u> ext >	Cancel

### 5. Click Next.

This opens the *IP Traffic Destination* window. Select A specific *IP* Address from the Destination address drop-down box, as shown in the following figure. Enter the destination *IP* address of your Allied Telesyn router. This must be a valid Internet address.

Destination	n address:					Ţ		
Tropoone	IP Address:	<use th="" you<=""><th>r Allied 1</th><th>elesyr</th><th>n router</th><th>IP ad</th><th>idress&gt;</th><th></th></use>	r Allied 1	elesyr	n router	IP ad	idress>	
	Subnet mas <u>k</u> :	255	. 25	5.	255		255	

#### 6. Click Next.

This opens the *IP Protocol Type* window. Select *UDP* from the drop-down box, as shown in the following figure.

er Wizard			?
IP Protocol Type Select the IP Protocol type. If this type su IP port.	pports IP ports, you	ı will also specify the	1 T
Select a protocol type:			
<u>*</u>			
	< Back	Next >	Cancel

### 7. Click Next.

This opens the *IP Protocol Port* window. Select *From this port* and enter **1701**, as shown in the following figure.

_			
	_	_	

### 8. Click Next.

This completes the IP Filter wizard. Leave the *Edit properties* box unchecked, as shown in the following figure.



9. Click **Finish**, then on the IP Filter List window, click **Close**.

This returns you to the Security Rule Wizard IP Filter List window. The filter list now includes your new L2TP Tunnel Filter filter, as shown in the following figure.

n no ir niterin tile tollowing is	st matches your needs, CICK AUU (U Crea	te a new one.
IP filter lists: Name	Description	<u>A</u> dd
O All ICMP Traffic O All IP Traffic O L2TP Tunnel Filter	Matches all ICMP packets bet Matches all IP packets from t	<u>E</u> dit <u>R</u> emove

#### 10. Select L2TP Tunnel Filter and click **Next**.

This opens the *Filter Action* window. Select *Require Security*, as shown in the following figure. This option forces the VPN client to use strong security. Microsoft Windows will not accept any incoming calls by default. All outgoing calls to your Allied Telesis router will be required to use IPSec encryption (assuming you use the router configuration from "The configuration script" on page 5).

Security Rule Wizard		? >
Filter Action Select the filter action for this sect	urity rule.	
If no filter actions in the following I one. Select Use Add Wizard to cr	ist matches your needs, click Add to eate a filter action.	o create a new
Filter Actions:		Use Add <u>W</u> izard
Name	Description	Add
O Permit O Request Security (Optional)	Permit unsecured IP packets t Accepts unsecured communi	<u>E</u> dit
Require Security	Accepts unsecured communi	<u>R</u> emove
	2. <u>2</u>	
	< <u>B</u> ack <u>N</u> ex	t > Cancel

Page 20 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

### II. Click Next.

This completes the Rule wizard. Leave the *Edit properties* box unchecked, as shown in the following figure.

Security Rule Wizard		? ×
	Completing the New Rule Wizard You have successfully completed specifying the properties for your new rule. To edit your security rule now, select the Edit properties check box, and then click Finish.	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cano	cel

12. Click Finish, then on the To Head Office Properties window, click Close.

This returns you to the Console Root window, as shown in the following figure. Click *IP Security Policies on Local Machine*.



13. Click and then right-click on To Head Office, and select Assign. The policy is now assigned or enabled on your PC host, indicated by Yes in the Policy Assigned column, as shown in the following figure.

http://www.comsole.com/active-securit	y Policies on Local Machine]		_ 🗆 🗵
Console <u>W</u> indow <u>H</u> elp		🗅 🖨 🖥	. <u>-</u> 8×
] <u>A</u> ction <u>V</u> iew <u>F</u> avorites   ⇐ ⇒	🗈 📧 🔯 🗟 🔂 🔁 🏪		
Tree Favorites	Name 🔺	Description	Policy Assigned
Console Root	🖄 Client (Respond Only)	Communicate normally (unse	No
	Secure Server (Require Security)	For all IP traffic, always requir	No
1.77	🖾 Server (Request Security)	For all IP traffic, always reque	No
	🖾 To Head Office		Yes
	<b>[1</b> ]		•

14. Select Exit from the Console menu, to close and save the console window to your local hard drive. This uses the default name of Console1, as shown in the following figure.



### **Configure the connection**

- I. On your desktop, click Start > Settings > Control Panel.
- 2. Double-click the Network and Dial-Up Connection folder.

This opens the window shown in the following figure. Double-click the *Make New Connection* icon.



- 3. This opens the New Connection Wizard. Click Next.
- 4. Select Connect to a private network through the internet, as shown in the following figure.



### 5. Click Next.

The next window lets you 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).

work Con	nection Wizard		
Public N Wind	etwork ows can make sure the public network is connected f	irst.	a de la comercia de l
Windo netwo	ows can automatically dial the initial connection to the ork, before establishing the virtual connection.	Internet or other public	
c	Do not dial the initial connection.		
۲	Automatically dial this initial connection;		
	Modem Connection to ISP		•
	< <u>B</u> ack	<u>N</u> ext >	Cancel
			Carlcer

6. 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.

What is the name or address	s of the destination?
Type the host name or IP ad connecting.	dress of the computer or network to which you are
Host name or IP address (su	ich as microsoft.com or 123.45.6.78):
<use internet="" ip<="" router's="" td="" your=""><td>address&gt;</td></use>	address>

Page 24 | AlliedWare™ OS How To Note: VPNs with Windows 2000 clients, without NAT-T

### 7. Click Next.

This opens the *Connection Availability* window. Select *Only for myself*, as shown in the following figure.

twork Connection Wizard	
Connection Availability You may make the new connection ava	ailable to all users, or just yourself.
You may make this connection available connection stored in your profile will not	e to all users, or keep it only for your own use. A be available unless you are logged on.
Create this connection:	
O Eor all users	
Only for myself	
	< <u>B</u> ack <u>N</u> ext > Cancel

#### 8. Click Next.

Enter the name for your connection (e.g. Virtual Private Connection to Head Office), as shown in the following figure. If you want to, check the *Add a shortcut to this connection to my desktop* check box.

Network Connection Wizard	
Ś	Completing the Network Connection Wizard Iype the name you want to use for this connection:
VAR)	Virtual Private Connection to Head Office
K	To create this connection and save it in the Network and Dial-up Connections folder, click Finish. To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.
	Add a shortcut to my desktop Add a shortcut to my desktop           < Back         Finish         Cancel

### 9. Click Finish.

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

-	1 APR
User name:	bob
Password:	Save Password
<u>C</u> onnect	Cancel Pr <u>o</u> perties <u>H</u> elp

#### **10.** Click **Properties**.

This opens the Virtual Private Connection to Head Office window. Click the Networking Tab. Select Layer-2 Tunneling Protocol (L2TP) in the drop-down box, as shown in the following figure.

tual Private Connec	tion to Head Office	? >
General   Options   Sec	curity Networking Sharin	ng
Type of VPN server I a	m calling:	
Layer-2 Tunneling Pro	itocol (L2TP)	•
		<u>S</u> ettings
		-
Components checked	are used by this connectio	n:
🗹 🏹 Internet Protoc	ol (TCP/IP)	
🗹 📇 File and Printer	Sharing for Microsoft Netv	vorks
Client for Micro	soft Networks	
Client for Micro	soft Networks	
Client for Micro	soft Networks	Properties
Client for Micro	soft Networks	Properties
Client for Micro	soft Networks	Properties
Client for Micro	I Protocol/Internet Protoco	Properties
Client for Micro	Uninstall	Properties
Client for Micro	soft Networks	Properties
Client for Micro	soft Networks	Properties

### II. 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.

If the connection succeeds, the following dialog box displays. Click **OK**.

Connecti	ion Complete 🗙
Ð	Virtual Private Connection to Head Office' is now connected.
	To check the status of this connection or disconnect, right-click its icon in the Network Connections folder, or click its icon on the taskbar (if present).
	Do not display this message again

### **Testing the tunnel**

The simplest way to tell if traffic is passing through the tunnel is to perform a traceroute from the Windows 2000 client to a PC in the router's LAN. To do this, use the following command at the command prompt on the Windows 2000 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 (e.g. Virtual Private Connection to Head Office) 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

© 2007 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. Allied Telesis is a trademark or registered trademark of Allied Telesis, Inc. in the United States and other countries. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

C613-16004-00 REV D





Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com