Allied Telesis

AlliedWare^{TM} OS

How To | Create a VPN between an Allied Telesis Router and a Microsoft Windows 2000[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 2000 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.

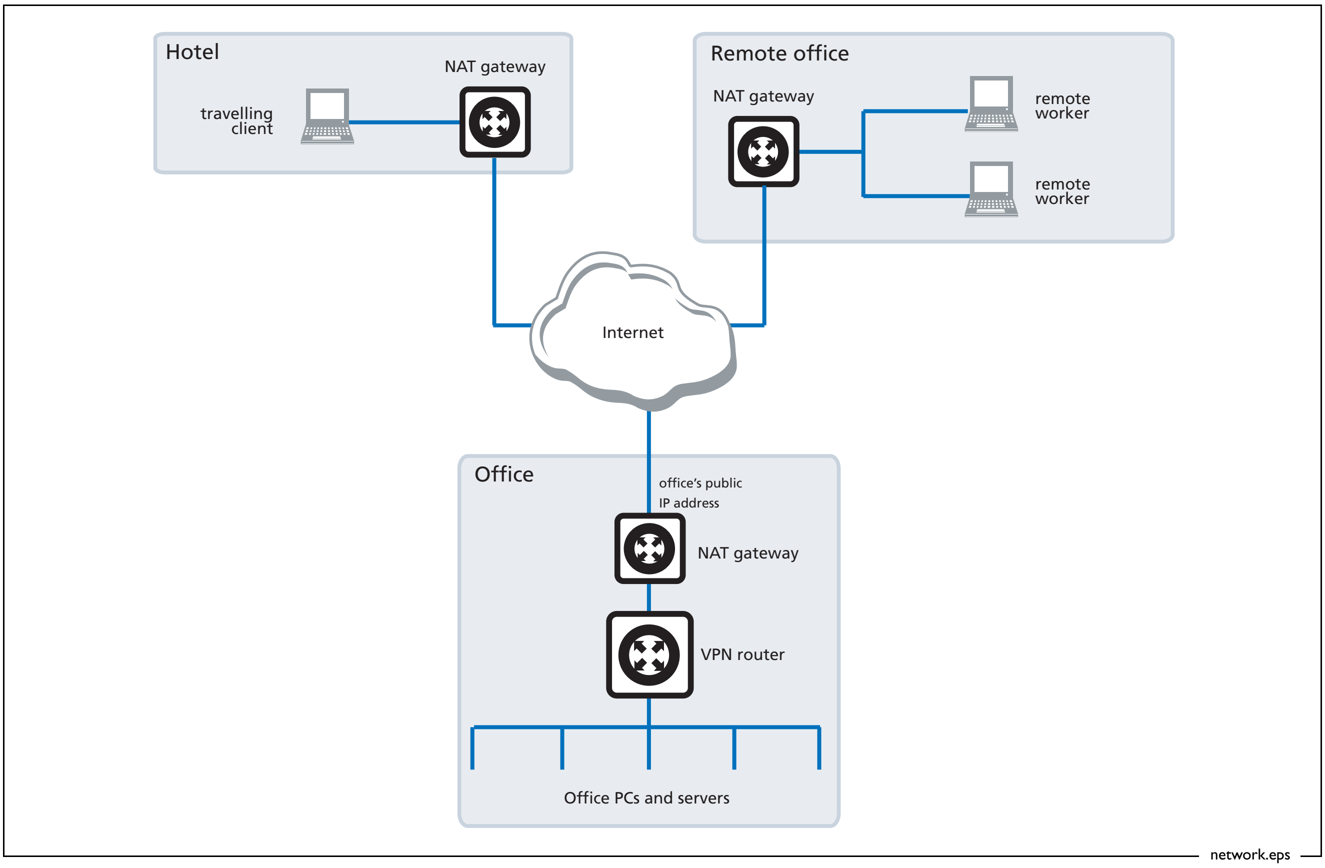
The travelling staff members will get secure remote access from any hotel or location with Internet access through the use of IPSec VPN. Each staff member has a laptop or other portable device with Windows 2000 installed.

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.

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 2000 and NAT-T support

To use NAT-T with Windows 2000 clients, you need:

- Windows 2000 Professional
- Service Pack 3 or 4. We used SP 4.
- the Layer Two Tunnelling Protocol (L2TP) and Internet Protocol security (IPSec) update patch, KB 818043. See "The KB 818043 update patch", on this page.
- to set your router to propose a local port of 1701, not a remote port. See "Port settings for IPsec policy proposal" on page 4.

The KB 818043 update patch

NAT-T support is provided by the Layer Two Tunnelling Protocol (L2TP) and Internet Protocol security (IPSec) update patch, *KB 818043,* for Windows 2000 Service Pack 3 and 4.

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 2000 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 2000 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 2000 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:

- SP 3 or 4 with the KB 808143 patch and 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.
- any service pack (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

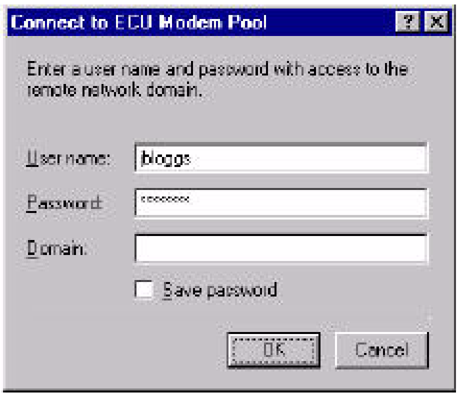
Since this Windows VPN solution is usually used to allow remote access into corporate networks, a common security concern is "what happens if the remote laptop or PC is stolen or falls into unauthorised hands?" This is particularly a concern because the VPN connection is enabled through the standard 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. In other words, do **not** tick the box labelled "Save password" in the following dialog box:



Connect to ECU Modem Pool

Enter a user name and password with access to the remote network domain.

User name: bloggs

Password: ********

Domain:

□ Save password

Some PCs have security modes that can be enabled. There are also numerous tips to be found relating to 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 8. 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 10.
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 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 12
- "Create an IP Security Policy" on page 14
- "Create an IP Security Rule" on page 16
- "Create an IP Filter" on page 19
- "Configure the connection" on page 26

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.

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

   ```
   regedit
   ```

   Then click **OK**.

   This opens the Registry Editor.

2. In the Registry Editor, browse to the following folder: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

3. Right-click on this folder and select **New** > **DWORD Value**. This creates a new entry.

4. Name the new entry “ProhibitIpSec”.

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.

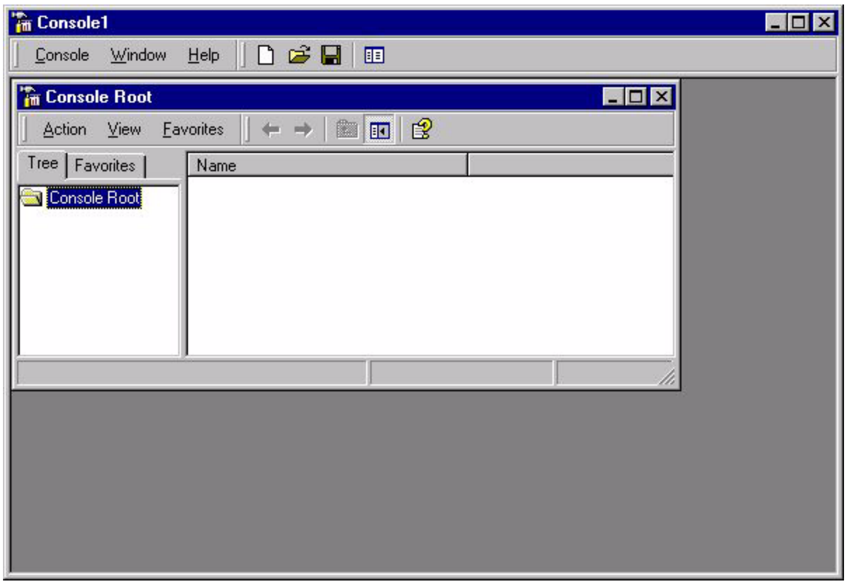
Add the IP Security Policy Management snap-in

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.

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

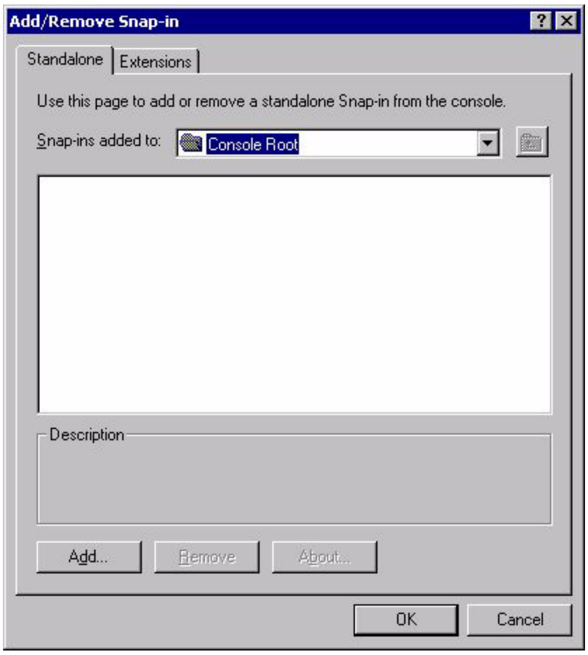
```
mmc
```

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



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

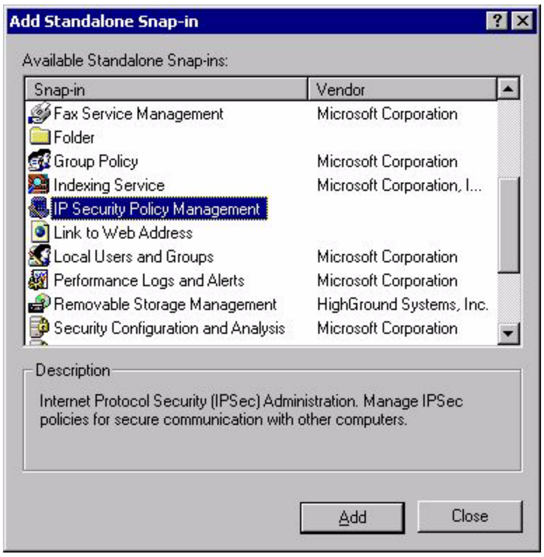
This opens the *Add/Remove Snap-in* window, as shown in the following figure.



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.



Add Standalone Snap-in

Available Standalone Snap-ins:

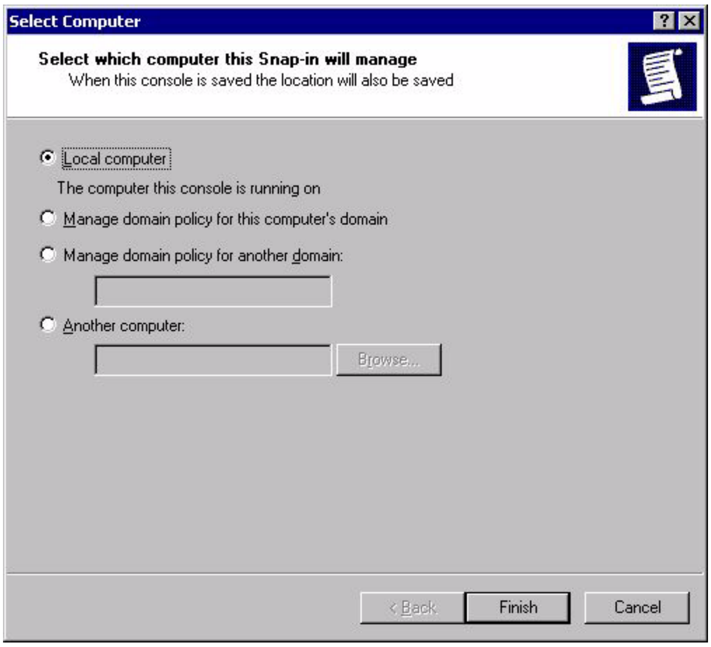
Snap-in	Vendor
Fax Service Management	Microsoft Corporation
Folder	
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
IP Security Policy Management	
Link to Web Address	
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	HighGround Systems, Inc.
Security Configuration and Analysis	Microsoft Corporation

Description

Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with 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.



Select Computer

Select which computer this Snap-in will manage

When this console is saved the location will also be saved

● Local computer

The computer this console is running on

○ Manage domain policy for this computer's domain

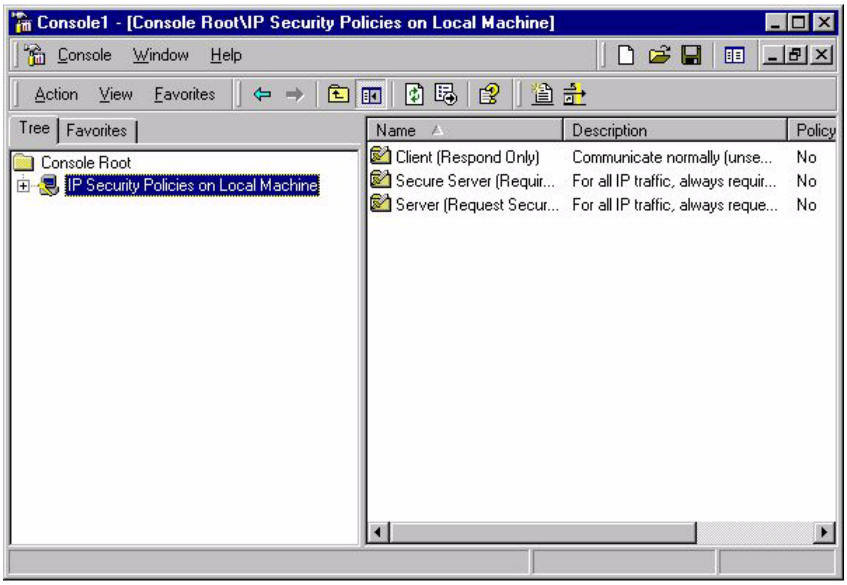
○ Manage domain policy for another domain:

○ Another computer:

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

Create an IP Security Policy

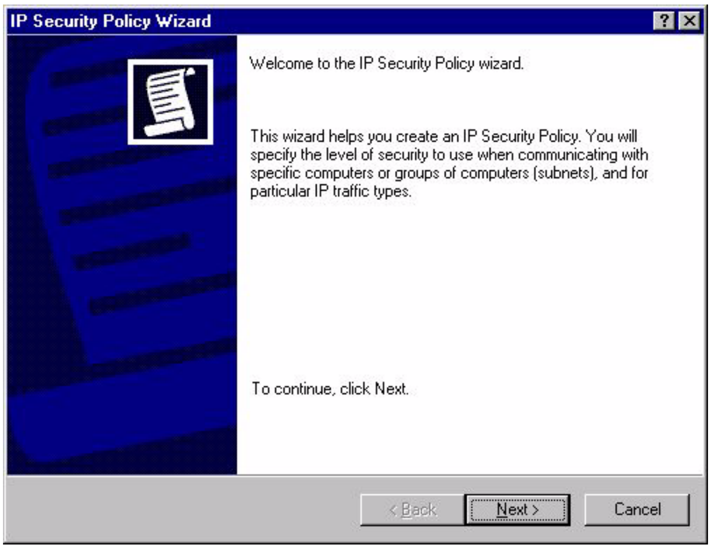
1. On the Console window, **right-click** *IP Security Policies on Local Machine*.


Console1 - [Console Root\IP Security Policies on Local Machine]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
IP Security Policies on Local Machine

Name	Description	Policy
Client (Respond Only)	Communicate normally (unse...	No
Secure Server (Requir...	For all IP traffic, always requir...	No
Server (Request Secur...	For all IP traffic, always reque...	No

2. Select *Create IP Security Policy.*

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

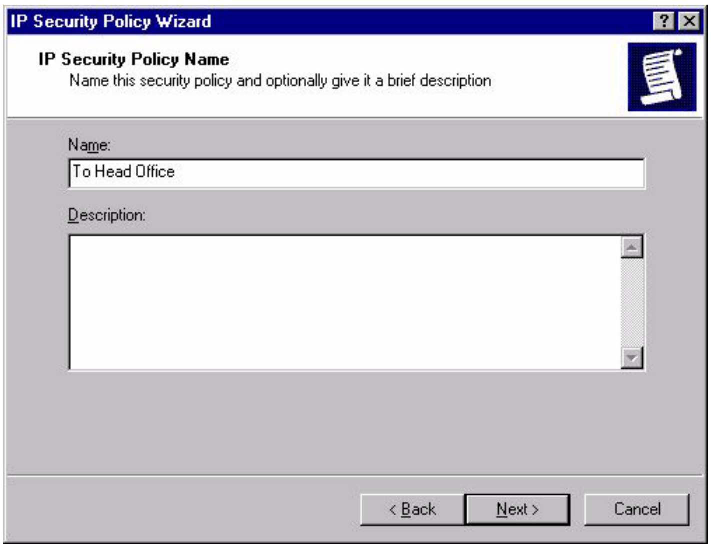


Welcome to the IP Security Policy wizard.

This wizard helps you create an IP Security Policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.

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



IP Security Policy Wizard

IP Security Policy Name

Name this security policy and optionally give it a brief description

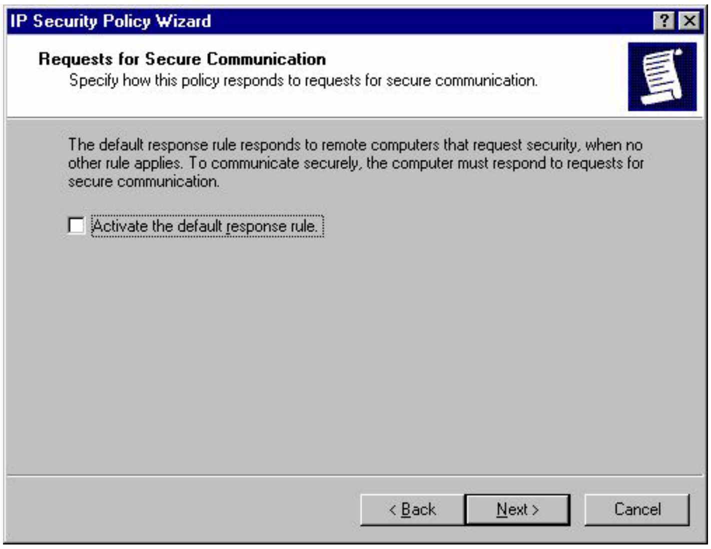
Name:

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.



IP Security Policy Wizard

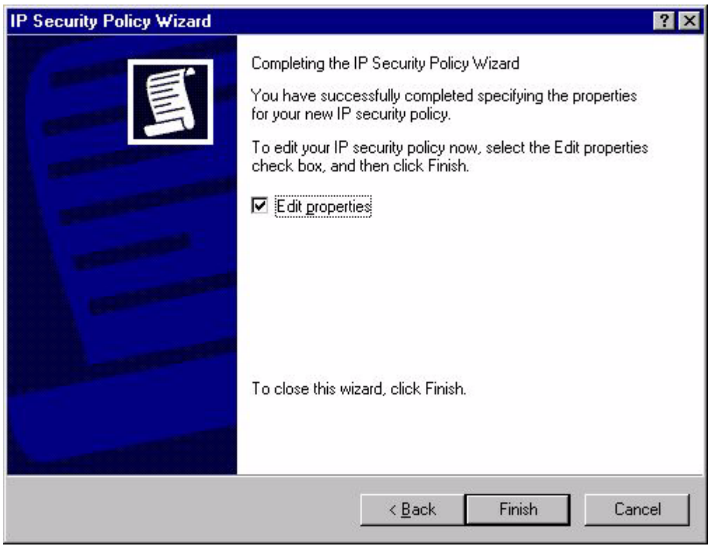
Requests for Secure Communication

Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

□ Activate the default response rule.

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.

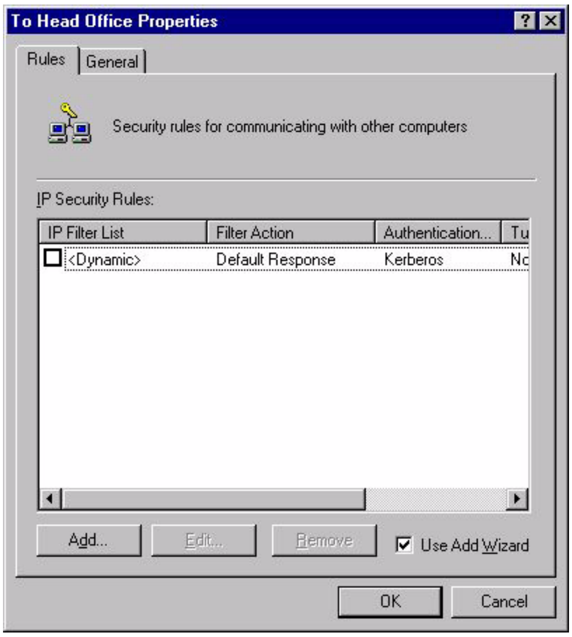
☑ Edit properties

To close this wizard, click Finish.

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

Create an IP Security Rule

1. Clicking Finish in the previous step opens the policy's *Properties* window, as shown in the following figure.



To Head Office Properties

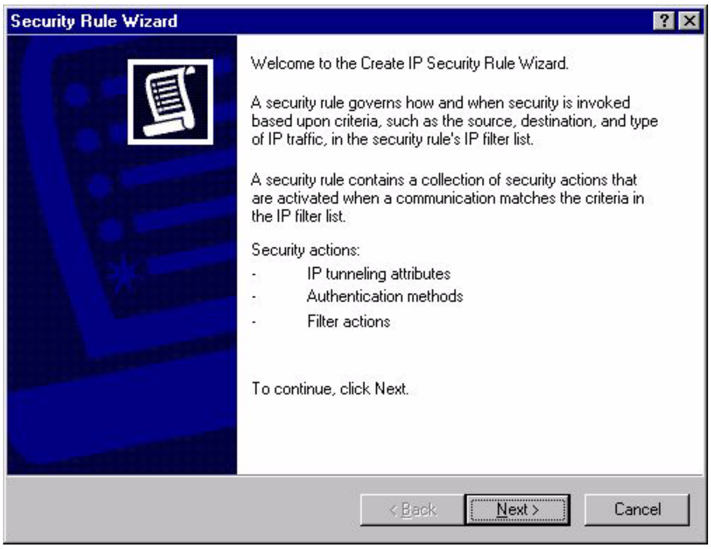
Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	Nc

☑ Use Add Wizard

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



Security Rule Wizard

Welcome to the Create IP Security Rule Wizard.

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

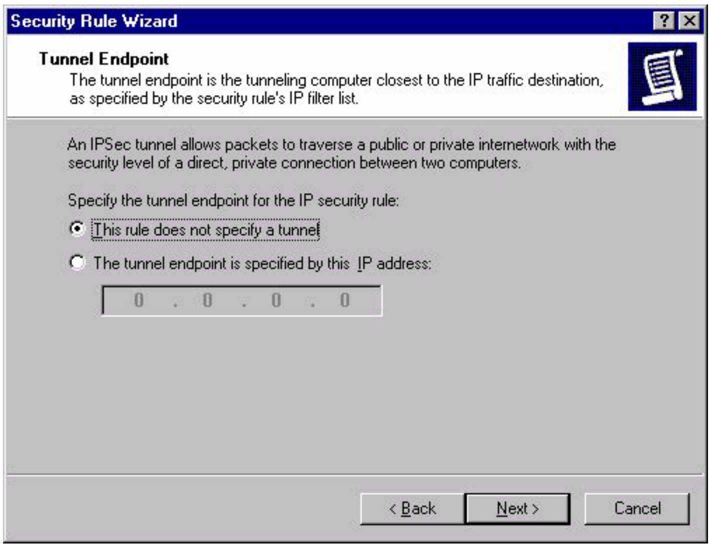
- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

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.



Security Rule Wizard

Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP security rule:

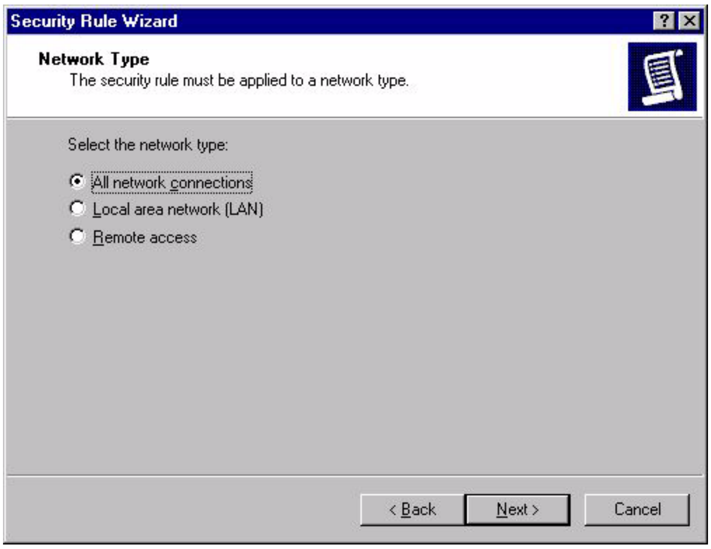
● This rule does not specify a tunnel

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

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.



Security Rule Wizard

Network Type

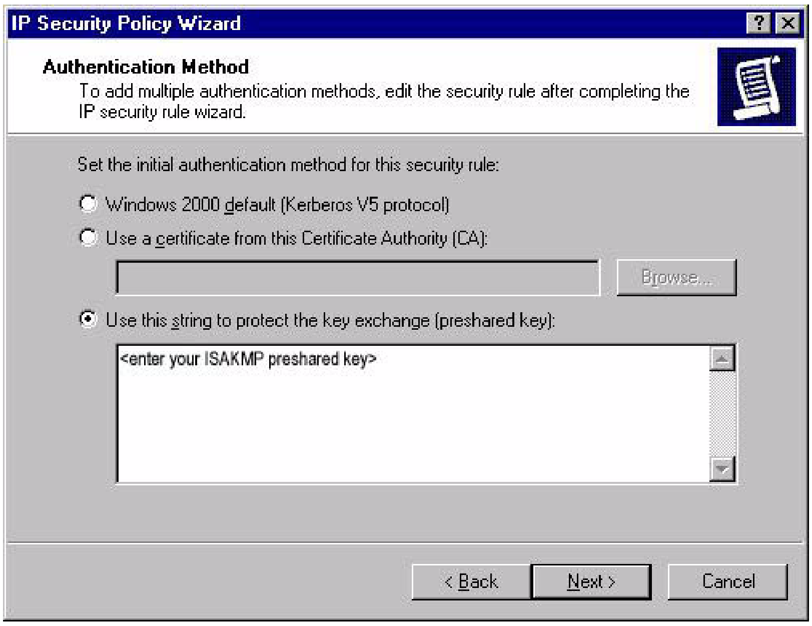
The security rule must be applied to a network type.

Select the network type:

● All network connections
○ Local area network (LAN)
○ Remote access

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.



IP Security Policy Wizard

Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.

Set the initial authentication method for this security rule:

○ Windows 2000 default (Kerberos V5 protocol)
○ Use a certificate from this Certificate Authority (CA):
● Use this string to protect the key exchange (preshared key):

<enter your ISAKMP preshared key>

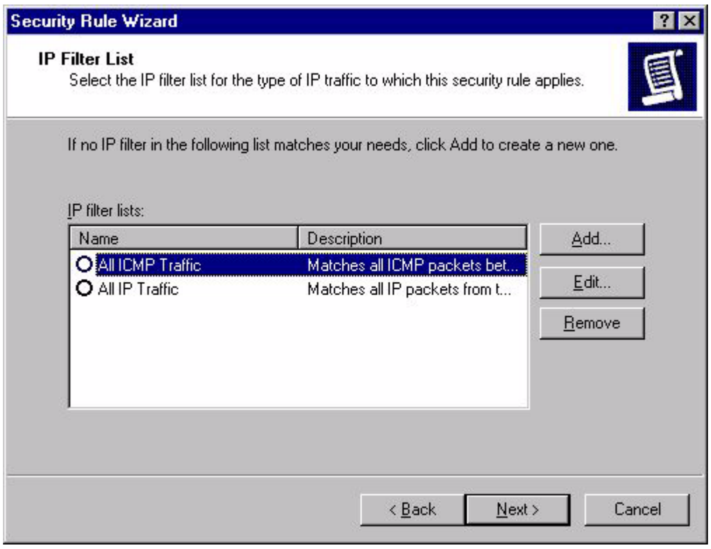
In the text box underneath the option, **enter a preshared key** that is known to both the router and the client.

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 7).

Create an IP Filter

1. 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.



Security Rule Wizard

IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

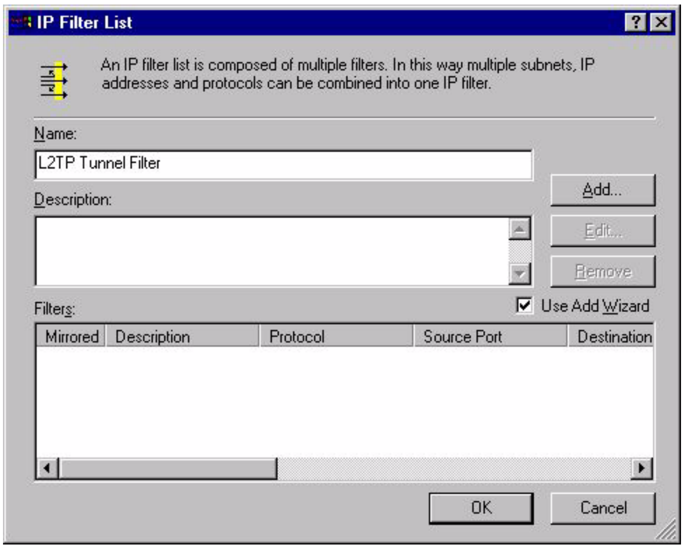
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
● All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

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.



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

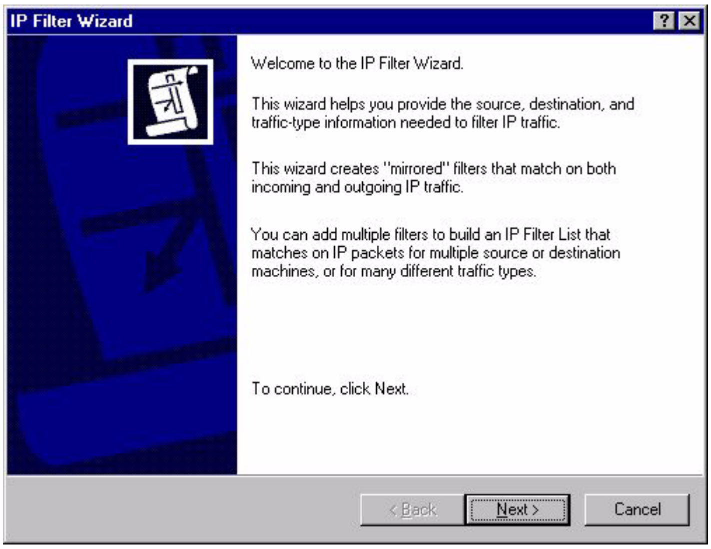
Name: L2TP Tunnel Filter

Description:

Filters: ☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

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



IP Filter Wizard

Welcome to the IP Filter Wizard.

This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

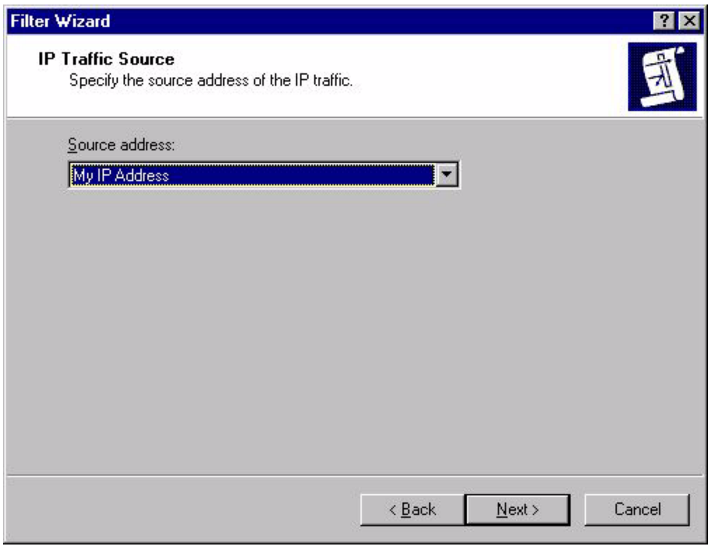
This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP Filter List that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

4. Click **Next**.

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



Filter Wizard

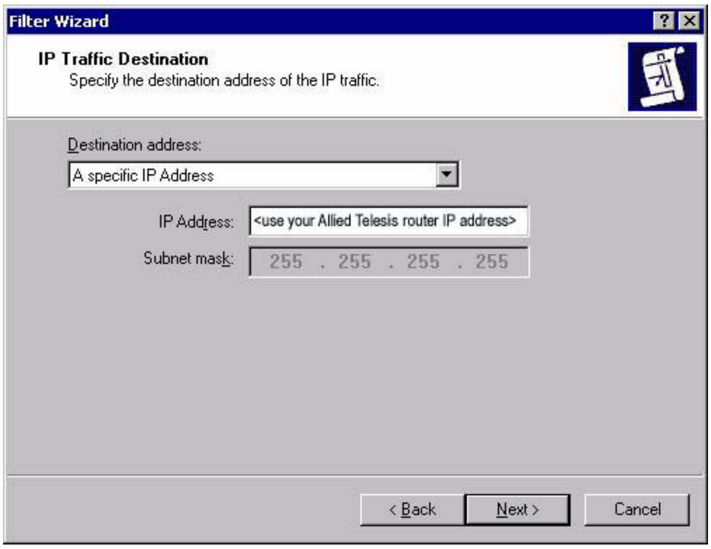
IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

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 Telesis router. This must be a valid Internet address.



Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

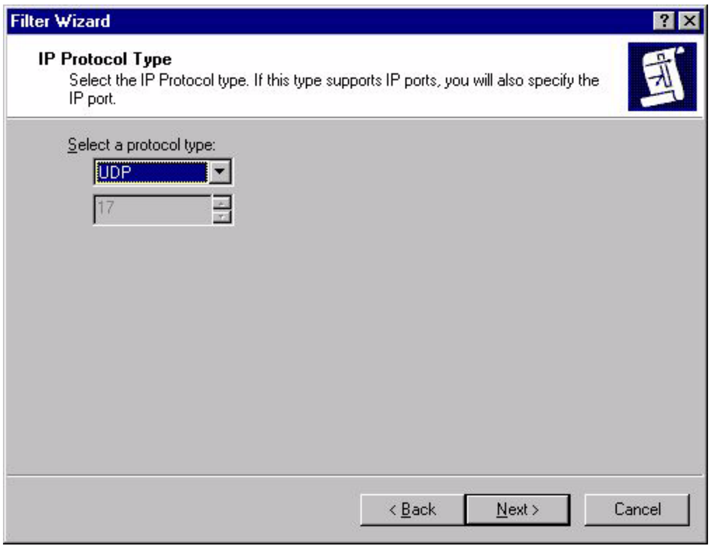
Destination address: A specific IP Address

IP Address: <use your Allied Telesis router IP address>

Subnet mask: 255 . 255 . 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.



Filter Wizard

IP Protocol Type

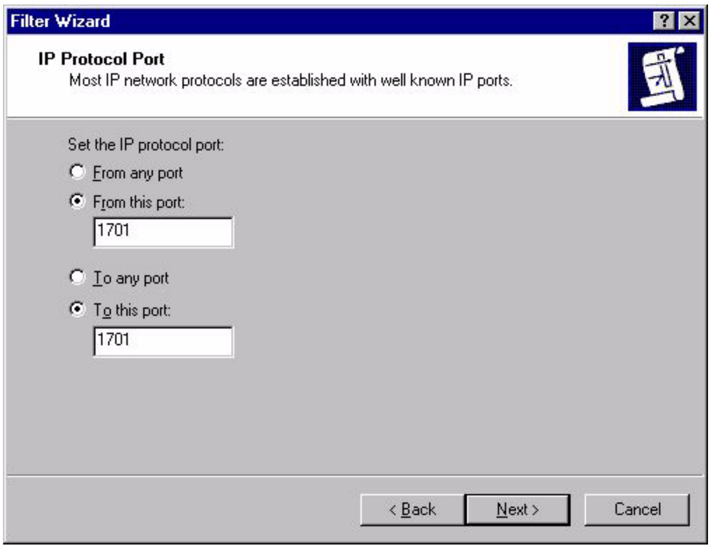
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.

Select a protocol type: UDP

17

7. Click **Next**.

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



Filter Wizard

IP Protocol Port

Most IP network protocols are established with well known IP ports.

Set the IP protocol port:

○ From any port

● From this port:

1701

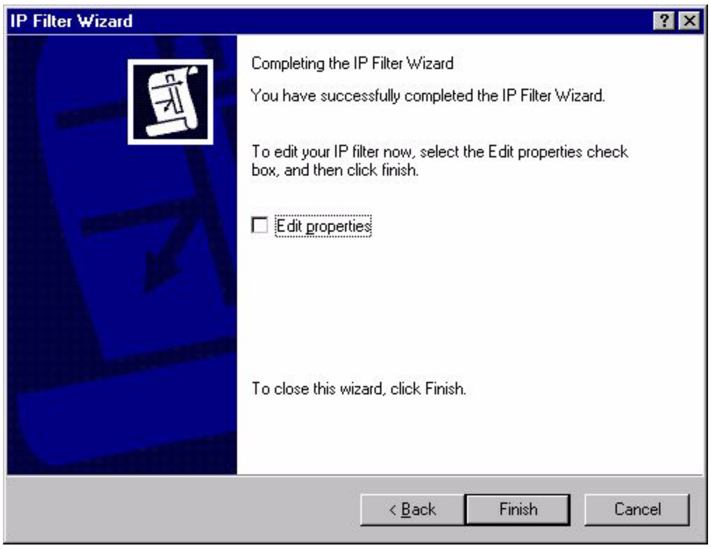
○ To any port

● To this port:

1701

8. Click **Next**.

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



IP Filter Wizard

Completing the IP Filter Wizard

You have successfully completed the IP Filter Wizard.

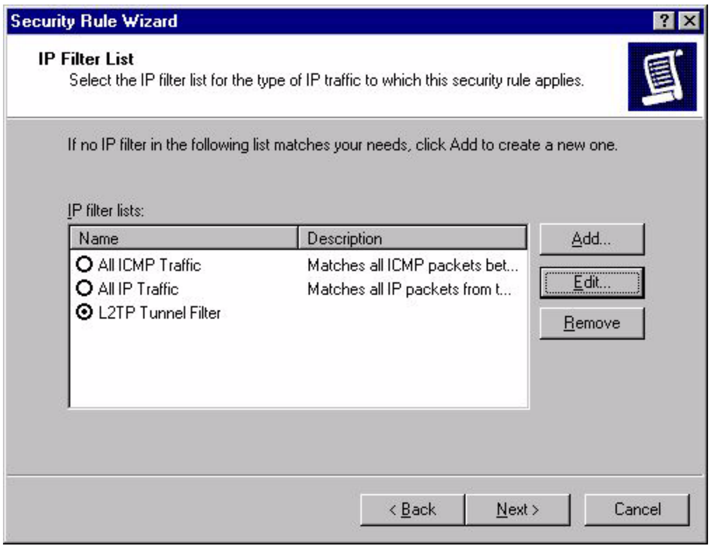
To edit your IP filter now, select the Edit properties check box, and then click finish.

□ Edit properties

To close this wizard, click Finish.

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.



Security Rule Wizard

IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

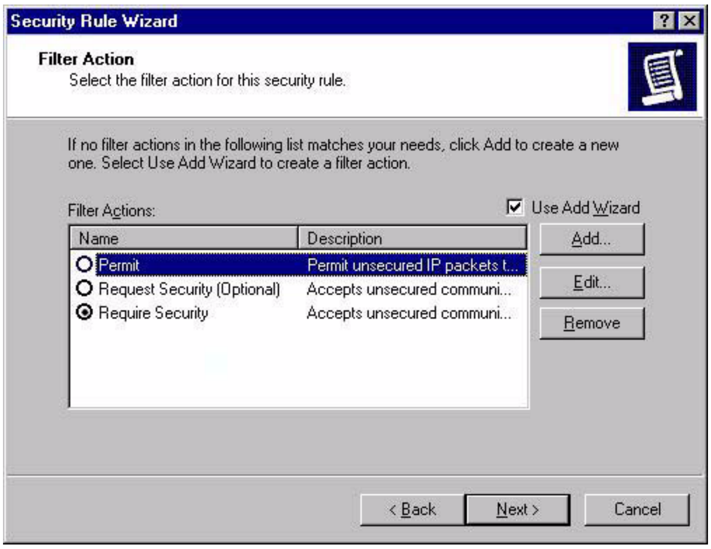
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
● L2TP Tunnel Filter	

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 8).



Security Rule Wizard

Filter Action

Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

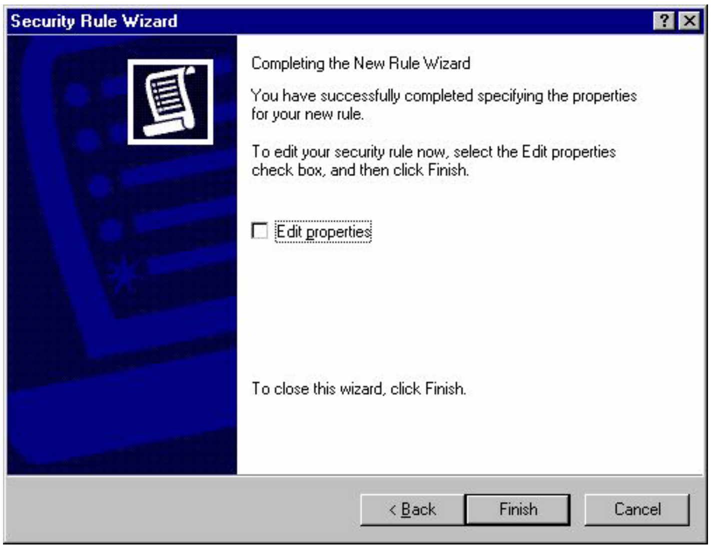
Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
● Require Security	Accepts unsecured communi...

11. Click **Next**.

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



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.

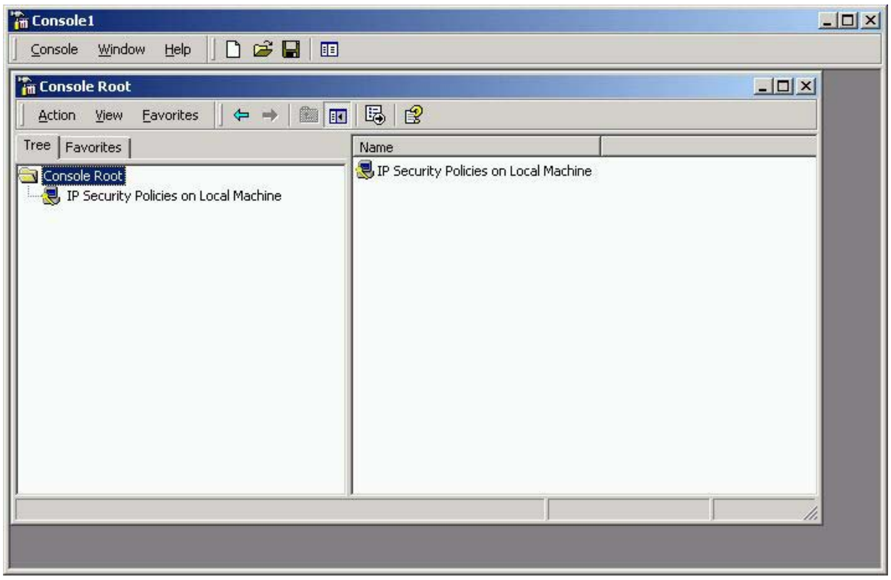
□ Edit properties

To close this wizard, click Finish.

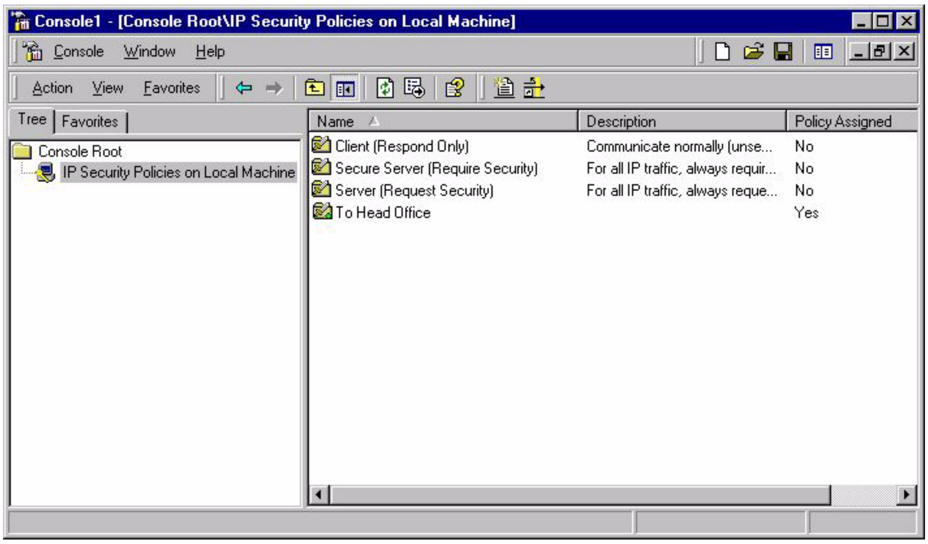
12. Click **Finish**. Then, on the *To Head Office Properties* window, click **Close**.

    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.

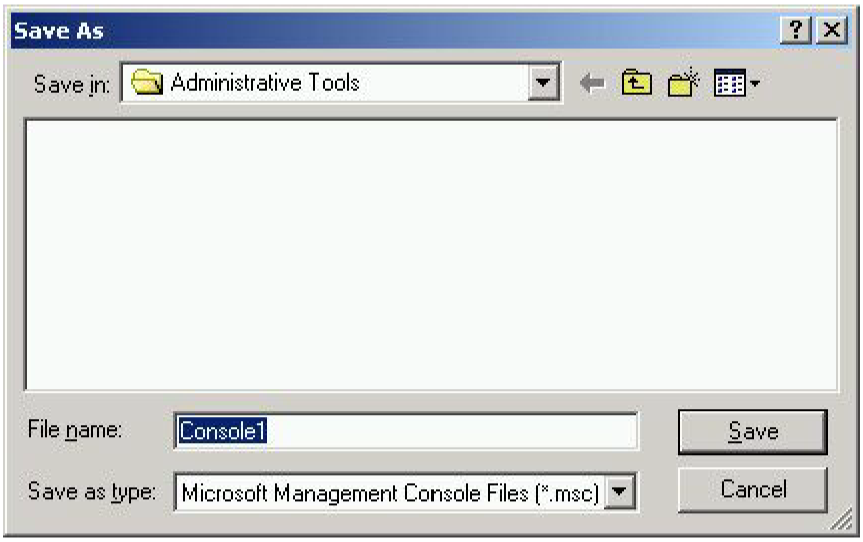


Console1 - [Console Root\IP Security Policies on Local Machine]

Console Root
IP Security Policies on Local Machine

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unse...	No
Secure Server (Require Security)	For all IP traffic, always requir...	No
Server (Request Security)	For all IP traffic, always reque...	No
To Head Office		Yes

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.



Save As

Save in: Administrative Tools

File name: Console1

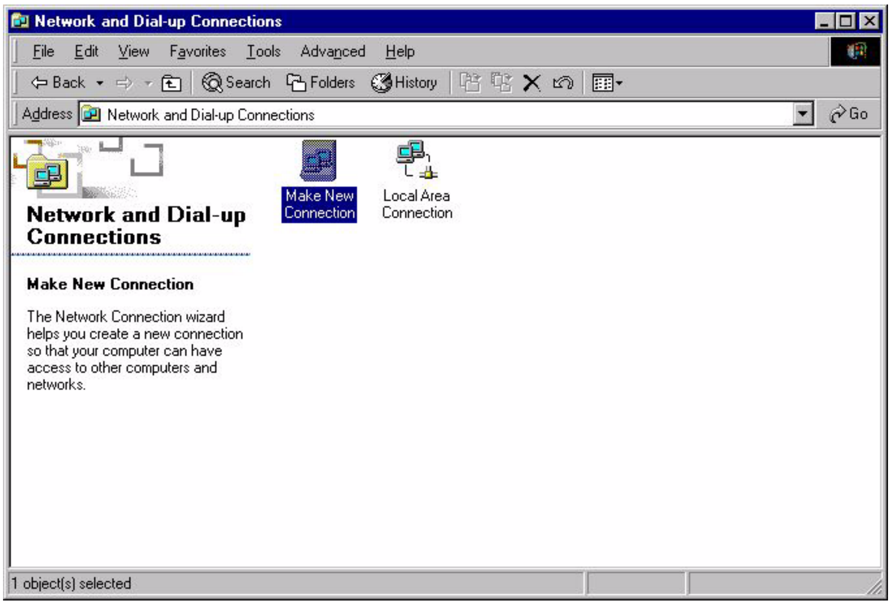
Save as type: Microsoft Management Console Files (*.msc)

Configure the connection

1. 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.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
1 object(s) selected

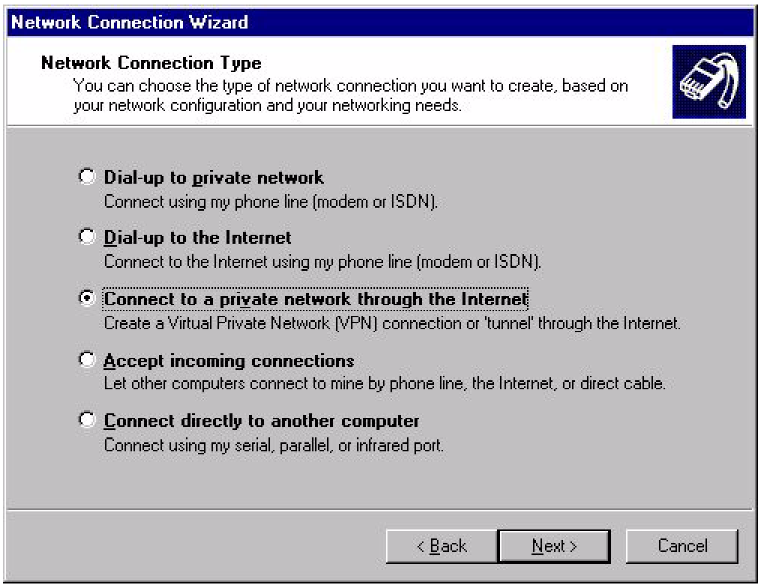
Network and Dial-up Connections

Make New Connection

The Network Connection wizard helps you create a new connection so that your computer can have access to other computers and networks.

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.



Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ Dial-up to private network
Connect using my phone line (modem or ISDN).

○ Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).

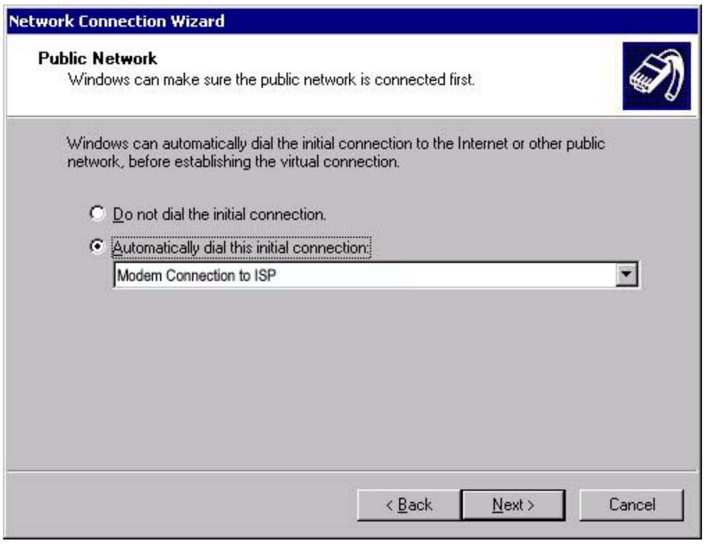
● Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ Connect directly to another computer
Connect using my serial, parallel, or infrared port.

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).



Network Connection Wizard

Public Network
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

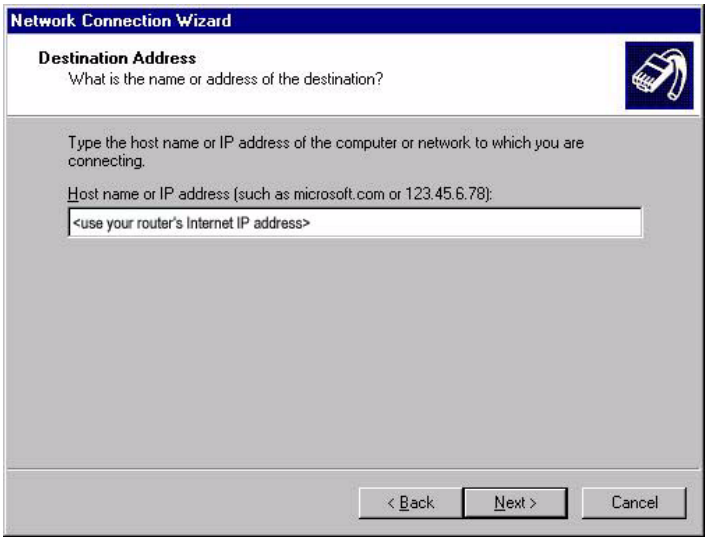
○ Do not dial the initial connection.

● Automatically dial this initial connection:

Modem Connection to ISP

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.



Network Connection Wizard

Destination Address
What is the name or address of the destination?

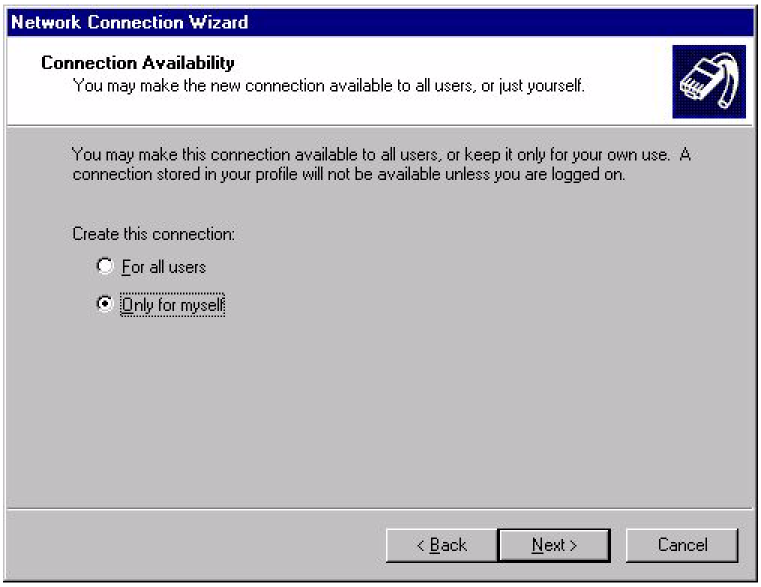
Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

<use your router's Internet IP address>

7. Click **Next**.

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



Network Connection Wizard

Connection Availability

You may make the new connection available to all users, or just yourself.

You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

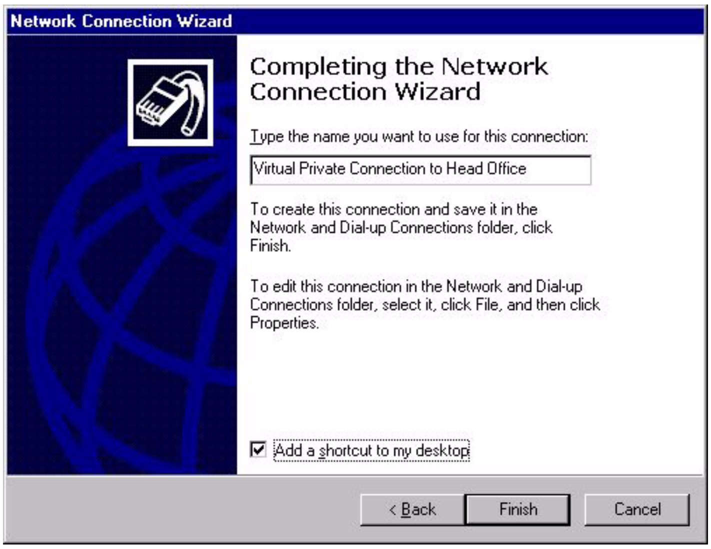
Create this connection:

○ For all users

● Only for myself

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

Completing the Network Connection Wizard

Type the name you want to use for this connection:

Virtual Private Connection to Head Office

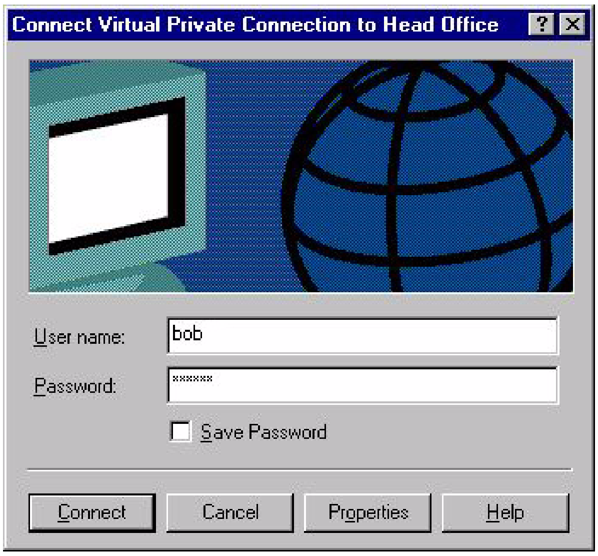
To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

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

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.



Connect Virtual Private Connection to Head Office

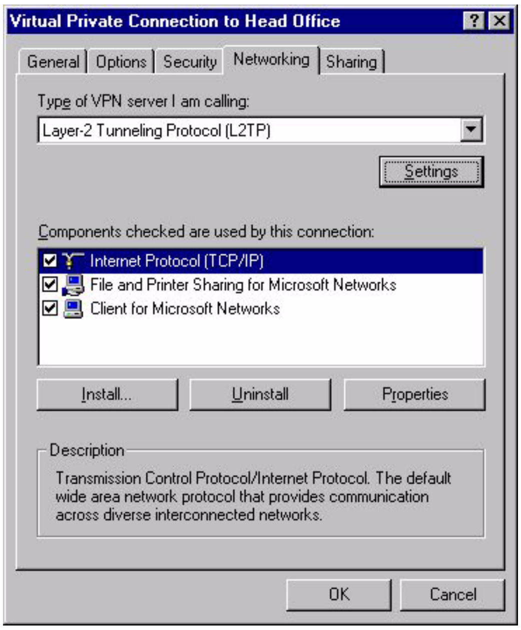
User name: bob

Password: ******

□ Save Password

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.



Virtual Private Connection to Head Office

Type of VPN server I am calling: Layer-2 Tunneling Protocol (L2TP)

Components checked are used by this connection:

☑ Internet Protocol (TCP/IP)
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

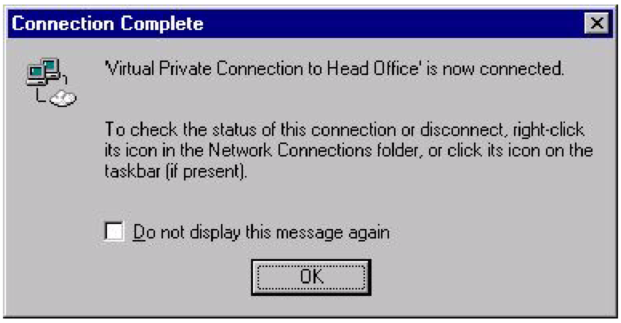
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

11. 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**.



Connection Complete

'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:

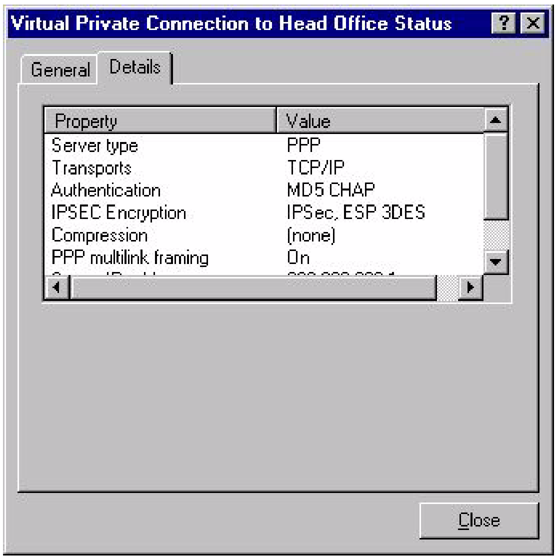
```
tracert <ip-address>
```

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.



Property	Value
Server type	PPP
Transports	TCP/IP
Authentication	MD5 CHAP
IPSEC Encryption	IPSec, ESP 3DES
Compression	(none)
PPP multilink framing	On

Troubleshooting

Check the following points in your Windows 2000 settings:

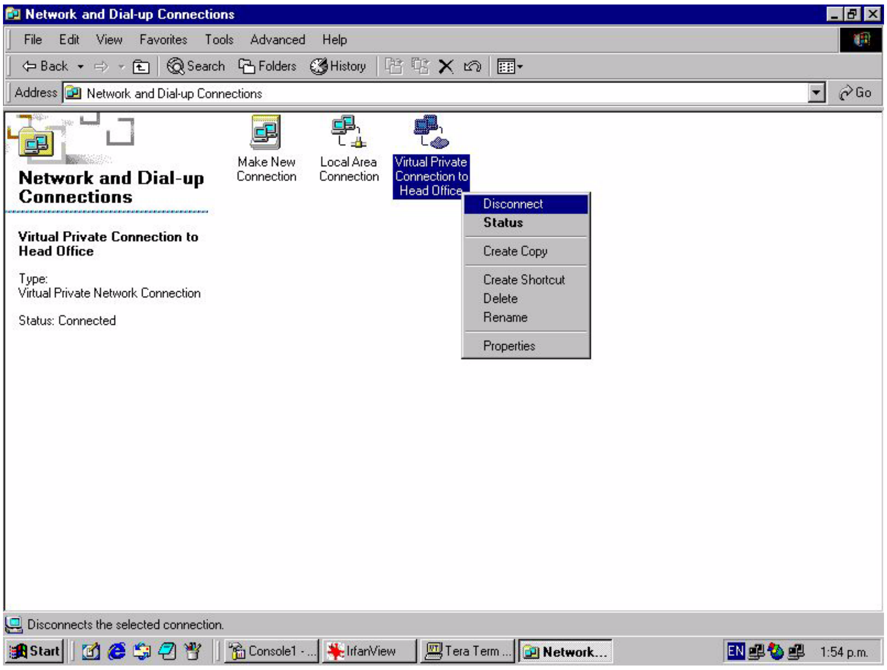
- Make sure the IPsec Policy Agent Service is in automatic mode. You can check this by selecting *Start* > *Settings* > *Control Panel* > *Administrative Tools* > *Services*, then look down the list for "IPsec Policy Agent". This should be in automatic mode, and can be corrected if necessary by right-clicking and choosing "*Properties*" from the pop-up menu.
- Ensure that the security policy has been properly assigned in the MMC console. If you find that the policy says "assigned, but the IPsec policy agent service is not in a running state", then check that the IPsec policy agent is in automatic mode and then unassign and reassign the policy to correct the problem. You may also need to reboot your PC.

  This error state can occur due to various historical installations, such as other VPN clients. You should not have another VPN client installed at the same time as this one.

If your tunnel is not working and the above settings are correct, 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.



Network and Dial-up Connections

Virtual Private Connection to Head Office

Type:
Virtual Private Network Connection

Status: Connected

Disconnects the selected connection.

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Make New Connection
Local Area Connection
Virtual Private Connection to Head Office
Disconnect
Status
Create Copy
Create Shortcut
Delete
Rename
Properties
Start
Console1 - ...
IrfanView
Tera Term ...
Network...
EN
1:54 p.m.

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

Connecting The IP World