AlliedWareTM OS

How To | Configure an IPsec VPN between Microsoft ISA Server 2004 and an Allied Telesis Router Client

Introduction

Both Microsoft Internet Security and Acceleration (ISA) Server 2004 and Allied Telesis routers enable you to define Virtual Private Networks (VPNs) for secure remote access to private LANs. This How To note describes how to configure a VPN in which an Allied Telesis router is the private office access gateway connected to a Microsoft ISA Server as the access concentrator.

What information will you find in this document?

This document first describes the network example in the following section:

Then it describes the configuration in the following sections. You must do all of these steps:

Then it describes how to test the configuration in the final section:

This How To Note assumes you have already installed Microsoft ISA Server 2004 and are familiar with its basic functionality.

Which products and software version does it apply to?

We created this configuration using an AR440S router and Software Version 2.7.5. However, the configuration applies to the following products:

- AR415S, AR440S, AR441S and AR442S routers
- AR750S, AR750S-DP and AR770S routers
- Rapier 16fi and Rapier 24i switches
- AT-8824 and AT-8848 switches
- older routers such as AR720, AR740, AR745, AR725, AR300 series, AR450S, and AR410 series
- older switches such as earlier Rapier series switches

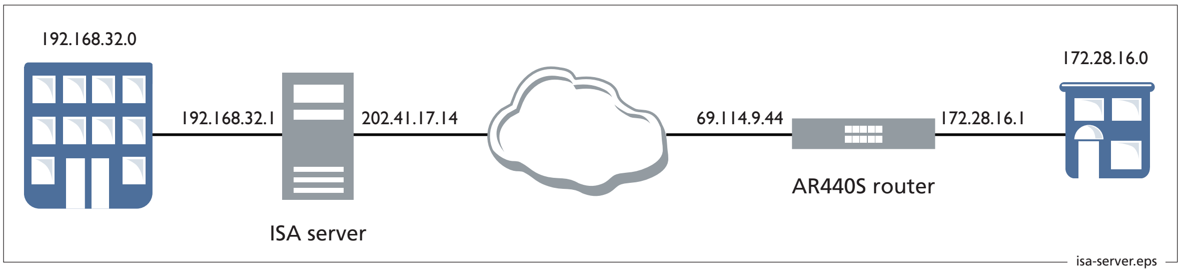
Related How To Notes

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 network

The network configuration for this example is shown in the following figure.



Configure the router

You need a 3DES licence for this example. See your authorised distributor or reseller for more information. Alternatively, you can use single DES.

1. Make the router secure

```
set system name=440_vpn_client
add user=secoff password=secret privilege=securityOfficer login=yes
enable system security
create config=vpn_client.cfg
set config=vpn_client.cfg
```

Log into the router as the security officer, `secoff`.

2. Define the connection to the private client LAN

The AR440S, and some other routers, have an IP address assigned to them by default. Some other routers and switches do not.

For routers and switches that already have an IP address, use the following command:

```
set ip interface=vlan1 ipaddress=172.28.16.1 mask=255.255.255.0
```

For routers and switches without an IP address, use the following commands:

```
enable ip
add ip interface=vlan1 ipaddress=172.28.16.1 mask=255.255.255.0
```

3. Define the connection to the Internet

The router connects to the Internet via port 1 which is in VLAN2. Note that you must give VLAN2 a legal public IP address. Use the following commands:

```
create vlan=vlan2 vid=2
add vlan=2 port=1
add ip interface=vlan2 ipaddress=69.114.9.44 mask=255.255.255.0
add ip route=0.0.0.0 mask=0.0.0.0 int=vlan2 next=69.114.9.45
```

4. Create an encryption key for the VPN to use

```
create enco key=1 type=general value=123456
```

Whenever you configure a VPN through the Internet, we recommend you use a key value that cannot be easily guessed. All printable characters are valid.

5. Configure ISAKMP for key management

```
create isakmp policy=tunnel peer=202.41.17.14 encalg=3desouter key=1
  expirys=28800 group=2

enable isakmp
```

6. Configure IPsec

This step defines a set of IPsec policies to:

- allow the router to forward ISAKMP negotiation traffic without encryption—the *isakmp* policy
- tunnel traffic between the remote LAN and the local LAN—the *tunnel* policy
- allow the router to forward web-browsing traffic without encryption—the *internet* policy

Use the following commands to configure IPsec:

```
create ipsec sas=1 keyman=isakmp prot=esp encalg=3desouter hasha=sha

create ipsec bundle=1 keyman=isakmp string="1" expirys=3600

create ipsec policy=isakmp int=vlan2 action=permit lport=500 rport=500

create ipsec policy=tunnel int=vlan2 action=ipsec keyman=isakmp
  bundle=1 peer=202.41.17.14 isakmp=tunnel laddress=172.28.16.0
  lmask=255.255.255.0 raddress=192.168.32.0 rmask=255.255.255.0

set ipsec policy=tunnel usepfsk=true group=2

create ipsec policy=internet int=vlan2 action=permit

enable ipsec
```

7. Set up the firewall

```
enable firewall

create firewall policy=lan

enable firewall policy=lan icmp_forwarding=ping

add firewall policy=lan interface=vlan1 type=private

add firewall policy=lan interface=vlan2 type=public

add firewall policy=lan nat=enhanced interface=vlan1 gblint=vlan2
```

The firewall uses NAT to translate private-side client IP addresses to a single global public IP address.

8. Create firewall rules

The router uses firewall rules to:

- allow ISAKMP packets to pass through the firewall
- pass VPN traffic through the firewall without applying NAT to it.

Use the following commands:

```
add firewall policy=lan rule=1 interface=vlan2 action=allow
  ip=69.114.9.44 protocol=udp port=500 gblip=69.114.9.44 gblport=500

add firewall policy=lan rule=2 interface=vlan2 action=nonat
  protocol=all ip=172.28.16.1-172.28.16.254 encap=ipsec

add firewall policy=lan rule=3 interface=vlan1 action=nonat
  protocol=all ip=172.28.16.1-172.28.16.254
  remoteip=192.168.32.1-192.168.32.254
```

9. Save the configuration

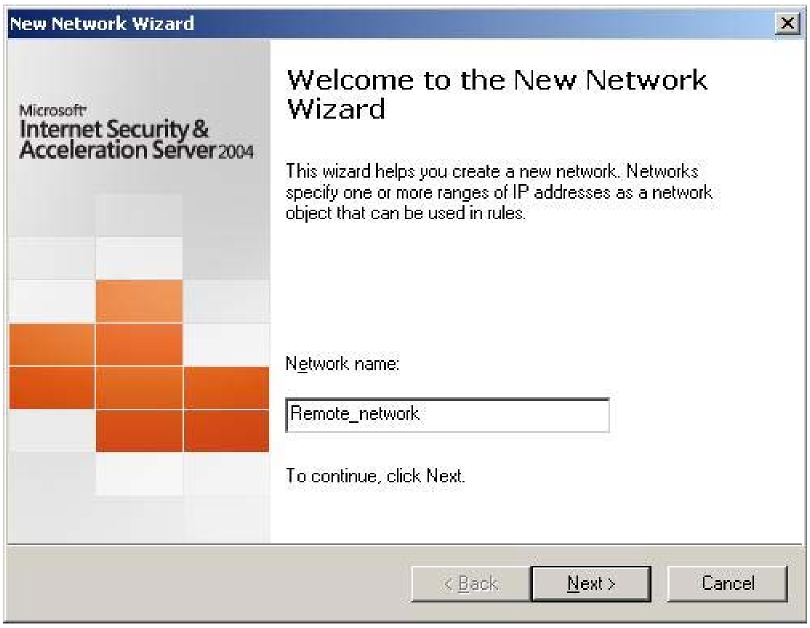
```
create config=vpn_client.cfg
```

Configure the ISA Server—remote network

This section describes how to specify the remote network to which the secure tunnel links.

1. Start the New Network Wizard

Start the ISA server management console, right-click on Networks from the left-hand menu, and select New > Network. The New Network Wizard opens:



Welcome to the New Network Wizard

This wizard helps you create a new network. Networks specify one or more ranges of IP addresses as a network object that can be used in rules.

Network name:

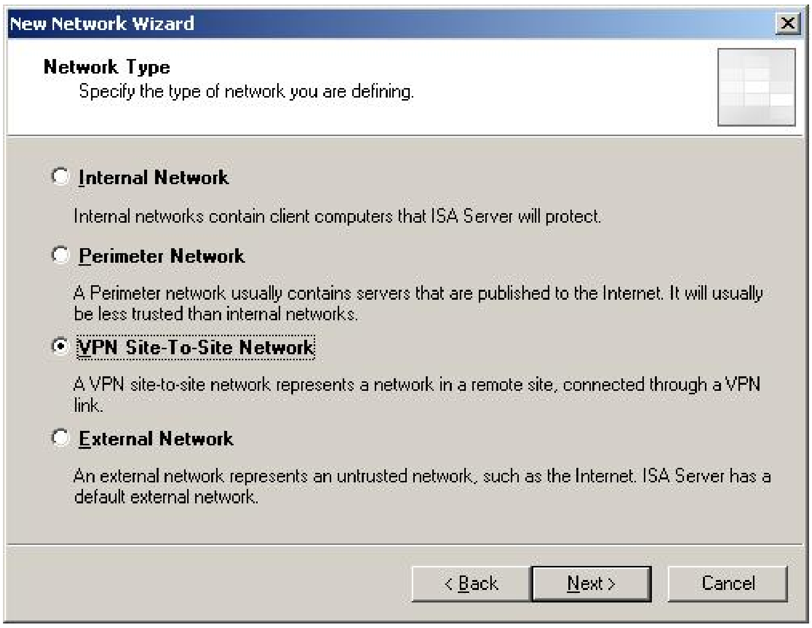
Remote_network

To continue, click Next.

Enter a name such as “Remote_network” and click the Next button to move to the Network Type dialog.

2. Specify the network type

Select "VPN Site-To-Site Network".



New Network Wizard

Network Type

Specify the type of network you are defining.

○ **Internal Network**

Internal networks contain client computers that ISA Server will protect.

○ **Perimeter Network**

A Perimeter network usually contains servers that are published to the Internet. It will usually be less trusted than internal networks.

● **VPN Site-To-Site Network**

A VPN site-to-site network represents a network in a remote site, connected through a VPN link.

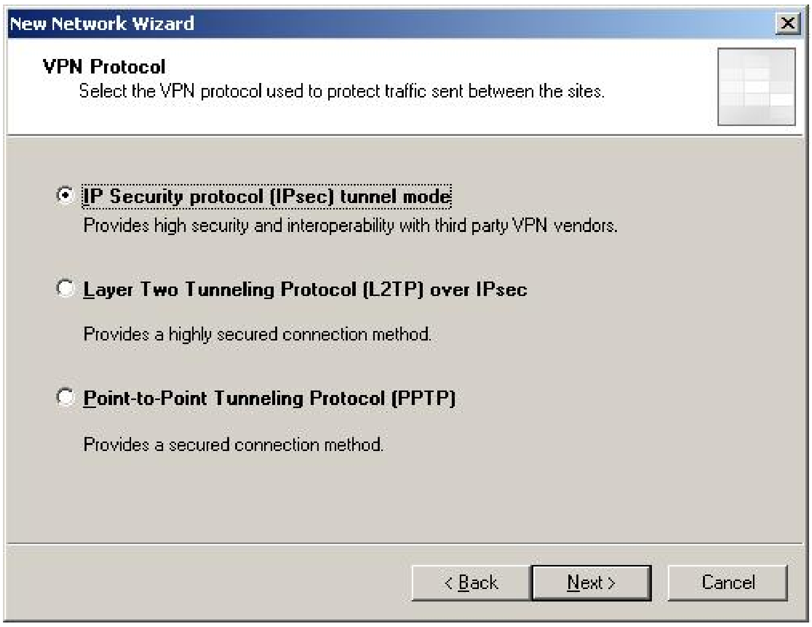
○ **External Network**

An external network represents an untrusted network, such as the Internet. ISA Server has a default external network.

Then click the Next button to move to the VPN Protocol dialog.

3. Specify the VPN protocol

Select "IP Security protocol (IPsec) tunnel mode".



New Network Wizard

VPN Protocol

Select the VPN protocol used to protect traffic sent between the sites.

● **IP Security protocol (IPsec) tunnel mode**

Provides high security and interoperability with third party VPN vendors.

○ **Layer Two Tunneling Protocol (L2TP) over IPsec**

Provides a highly secured connection method.

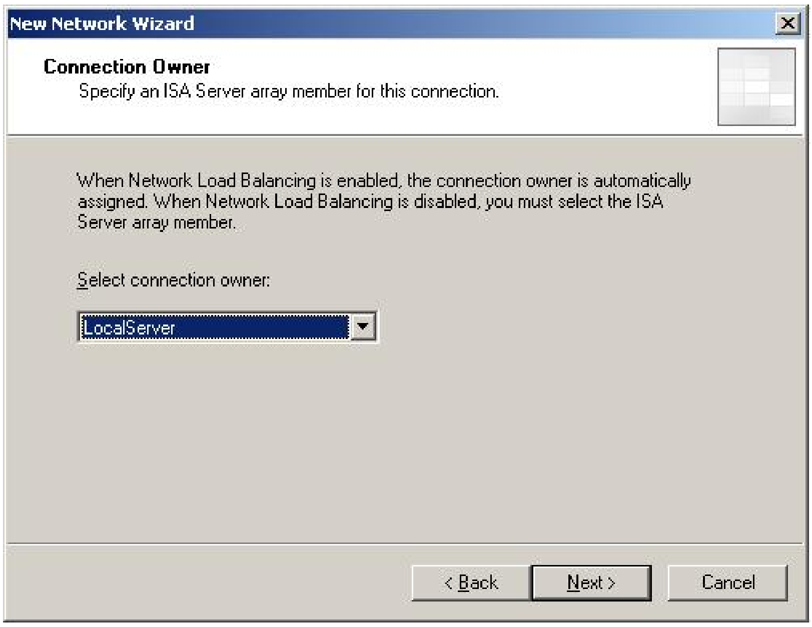
○ **Point-to-Point Tunneling Protocol (PPTP)**

Provides a secured connection method.

Then click the Next button to move to the Connection Owner dialog.

4. Select the connection owner

Select the ISA server array member that you wish to use for this connection (LocalServer in this example). There must be at least one array member defined in the ISA server before this step.



Connection Owner

Specify an ISA Server array member for this connection.

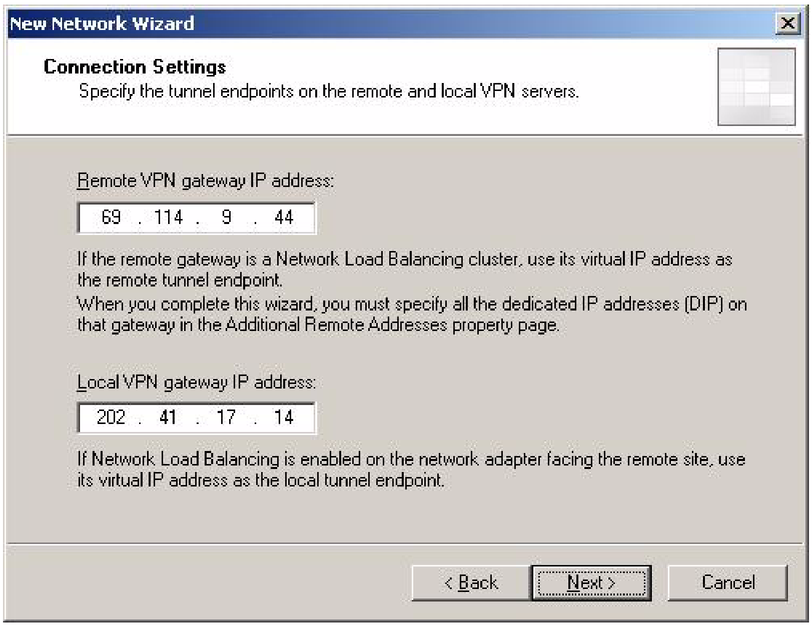
When Network Load Balancing is enabled, the connection owner is automatically assigned. When Network Load Balancing is disabled, you must select the ISA Server array member.

Select connection owner: LocalServer

Then click the Next button to move to the Connection Settings dialog.

5. Specify the connection settings

Enter the IP addresses of the tunnel endpoints.



Connection Settings

Specify the tunnel endpoints on the remote and local VPN servers.

Remote VPN gateway IP address: 69 . 114 . 9 . 44

If the remote gateway is a Network Load Balancing cluster, use its virtual IP address as the remote tunnel endpoint.
When you complete this wizard, you must specify all the dedicated IP addresses (DIP) on that gateway in the Additional Remote Addresses property page.

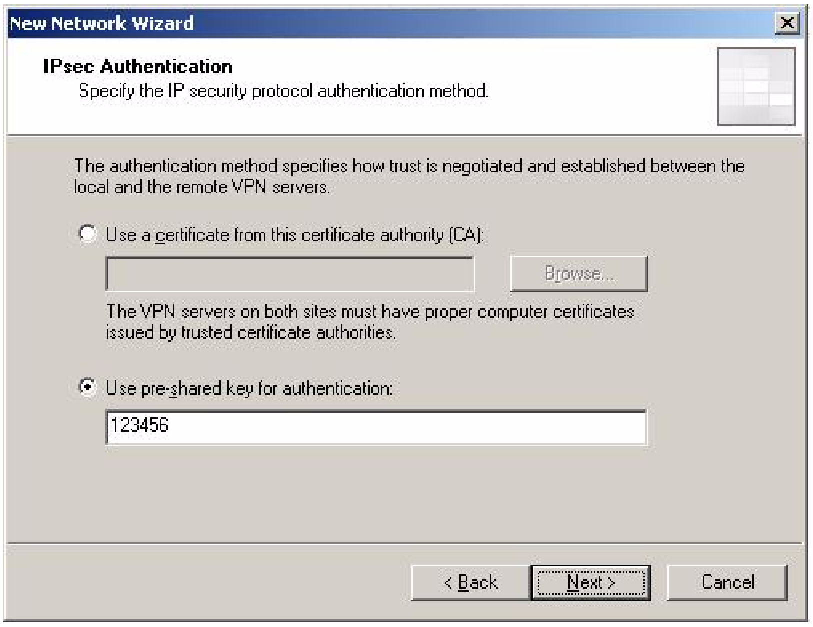
Local VPN gateway IP address: 202 . 41 . 17 . 14

If Network Load Balancing is enabled on the network adapter facing the remote site, use its virtual IP address as the local tunnel endpoint.

Then click the Next button to move to the IPsec Authentication dialog.

6. Specify the IPsec authentication method

Select “Use pre-shared key for authentication” and enter the same key value as you specified on the router in "Create an encryption key for the VPN to use" on page 3.



New Network Wizard

IPsec Authentication

Specify the IP security protocol authentication method.

The authentication method specifies how trust is negotiated and established between the local and the remote VPN servers.

○ Use a certificate from this certificate authority (CA):

The VPN servers on both sites must have proper computer certificates issued by trusted certificate authorities.

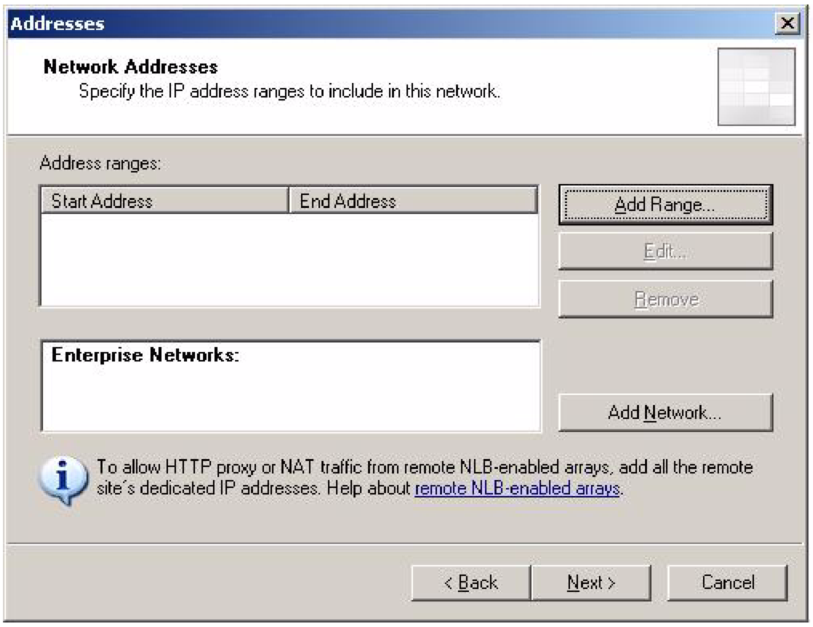
● Use pre-shared key for authentication:

123456

Then click the Next button to move to the Network Addresses dialog.

7. Add network address ranges

On the Network Addresses dialog, click the Add Range button:



Addresses

Network Addresses

Specify the IP address ranges to include in this network.

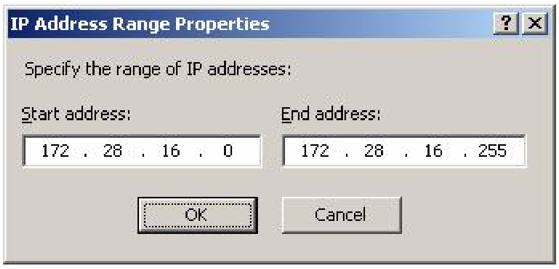
Address ranges:

Start Address	End Address

Enterprise Networks:

To allow HTTP proxy or NAT traffic from remote NLB-enabled arrays, add all the remote site's dedicated IP addresses. Help about remote NLB-enabled arrays.

The IP Address Range Properties dialog opens. Enter the address range of the router's private network:



IP Address Range Properties

Specify the range of IP addresses:

Start address: 172 . 28 . 16 . 0

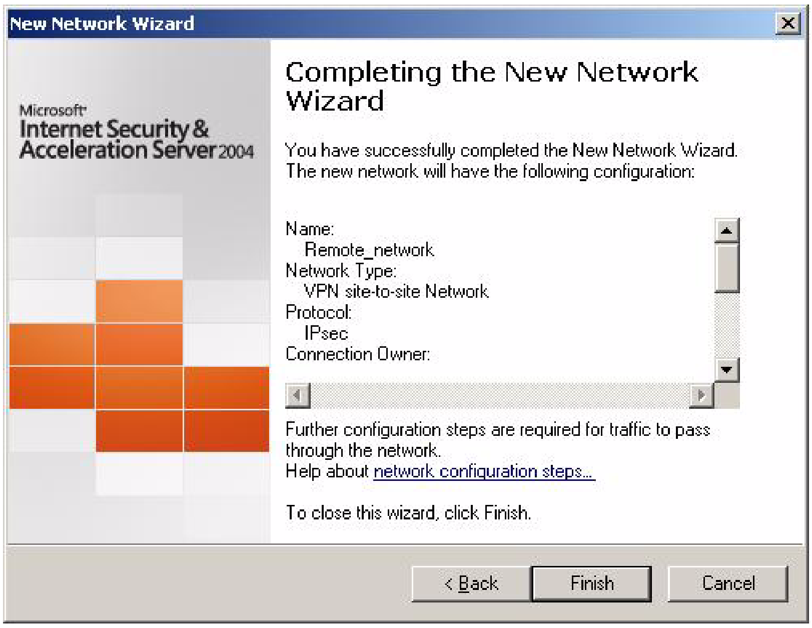
End address: 172 . 28 . 16 . 255

Then click the OK button to return to the Network Addresses dialog.

If necessary, repeat this step to define other address ranges for the remote end's private network. When you have added all the required ranges, click the Next button to move to the Completing the New Network Wizard dialog.

8. Check your network's settings

Review your settings and if necessary use the Back button to backtrack and change them.



New Network Wizard

Completing the New Network Wizard

You have successfully completed the New Network Wizard. The new network will have the following configuration:

Name:
Remote_network
Network Type:
VPN site-to-site Network
Protocol:
IPsec
Connection Owner:

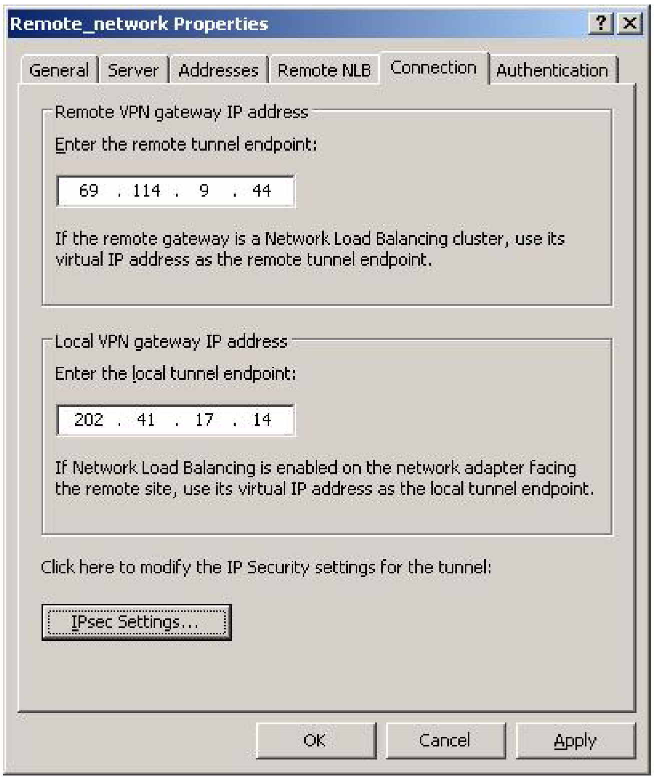
Further configuration steps are required for traffic to pass through the network.
Help about network configuration steps...

To close this wizard, click Finish.

Once the settings are correct, click the Finish button.

9. Access the network’s IPsec settings

From the left-hand menu of the ISA Server, select Virtual Private Networks (VPN). Click the Remote Sites tab, then double-click on Remote_network to open its Properties dialog. Click the Connection tab to display the following dialog:



Remote_network Properties

Remote VPN gateway IP address

Enter the remote tunnel endpoint: 69 . 114 . 9 . 44

If the remote gateway is a Network Load Balancing cluster, use its virtual IP address as the remote tunnel endpoint.

Local VPN gateway IP address

Enter the local tunnel endpoint: 202 . 41 . 17 . 14

If Network Load Balancing is enabled on the network adapter facing the remote site, use its virtual IP address as the local tunnel endpoint.

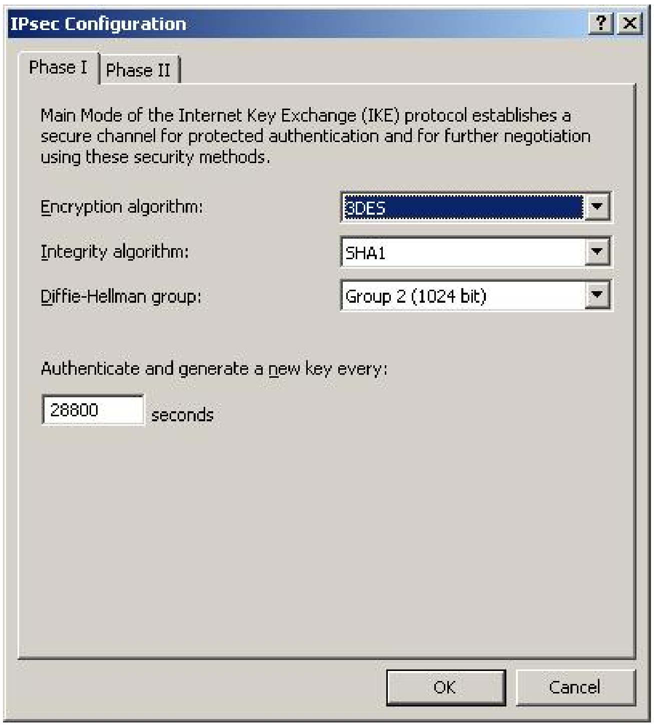
Click here to modify the IP Security settings for the tunnel:

Then click the IPsec Settings button to open the IPsec Configuration dialog.

10. Specify the network's Phase I settings

Specify the following Phase I settings:

Encryption algorithm:	3DES
Integrity algorithm:	SHA1
Diffie-Hellman group:	Group 2 (1024 bit)
Authenticate and generate a new key every:	28800



Main Mode of the Internet Key Exchange (IKE) protocol establishes a secure channel for protected authentication and for further negotiation using these security methods.

Encryption algorithm: 3DES

Integrity algorithm: SHA1

Diffie-Hellman group: Group 2 (1024 bit)

Authenticate and generate a new key every:

28800 seconds

Then click the Phase II tab.

11. Specify the network's Phase II settings

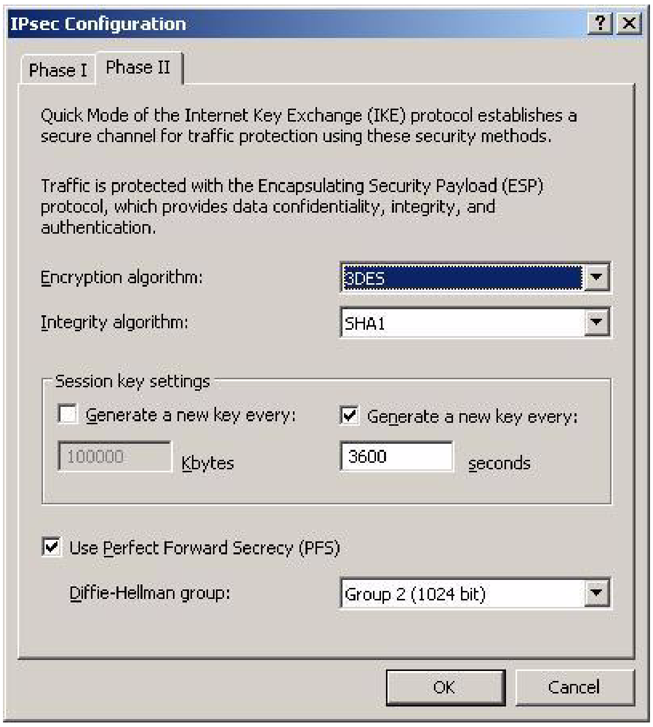
Specify the following Phase II settings:

Encryption algorithm:	3DES
Integrity algorithm:	SHA1

Select the "Generate a new key every:" checkbox and enter 3600 seconds.

Select the "Use Perfect Forward Secrecy (PFS)" checkbox and select:

Diffie-Hellman group:	Group 2 (1024 bit)



Quick Mode of the Internet Key Exchange (IKE) protocol establishes a secure channel for traffic protection using these security methods.

Traffic is protected with the Encapsulating Security Payload (ESP) protocol, which provides data confidentiality, integrity, and authentication.

Encryption algorithm: 3DES

Integrity algorithm: SHA1

Session key settings

□ Generate a new key every: 100000 Kbytes

☑ Generate a new key every: 3600 seconds

☑ Use Perfect Forward Secrecy (PFS)

Diffie-Hellman group: Group 2 (1024 bit)

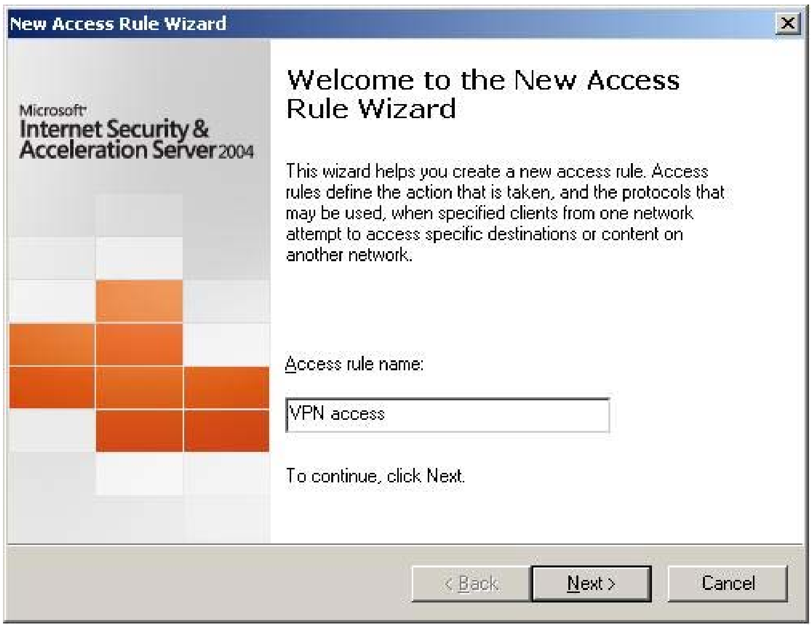
Then click the OK button. This completes the Remote_network configuration.

Configure the ISA Server—access rules

This section describes how to create access rules. These rules define the secure tunnel.

1. Start the New Access Rule Wizard

Right-click on Firewall Policy from the ISA server left-hand menu, and select New > Access Rule. The New Access Rule Wizard opens:



Welcome to the New Access Rule Wizard

This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on another network.

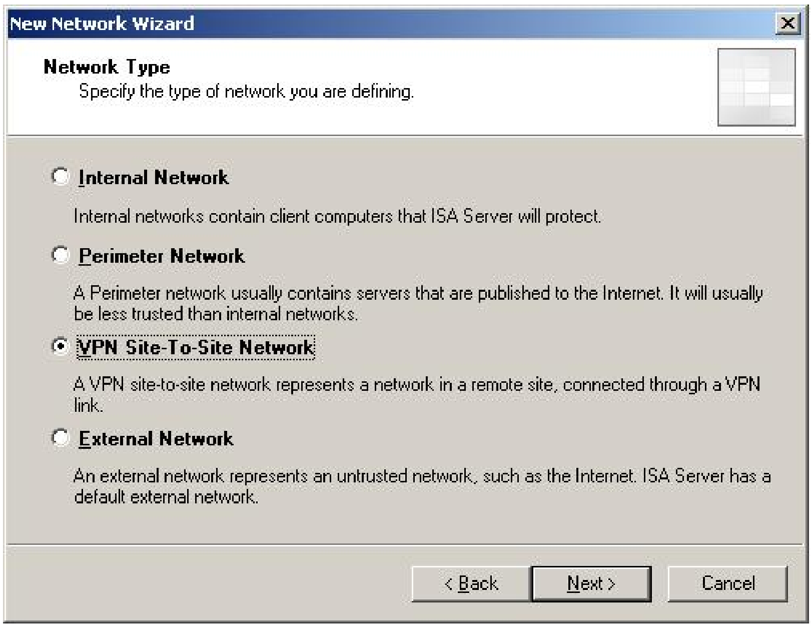
Access rule name: VPN access

To continue, click Next.

Enter a name such as "VPN access" and click the Next button to move to the Rule Action dialog.

2. Specify the action taken on matching traffic

Select "Allow".



Network Type
Specify the type of network you are defining.

○ **Internal Network**
Internal networks contain client computers that ISA Server will protect.

○ **Perimeter Network**
A Perimeter network usually contains servers that are published to the Internet. It will usually be less trusted than internal networks.

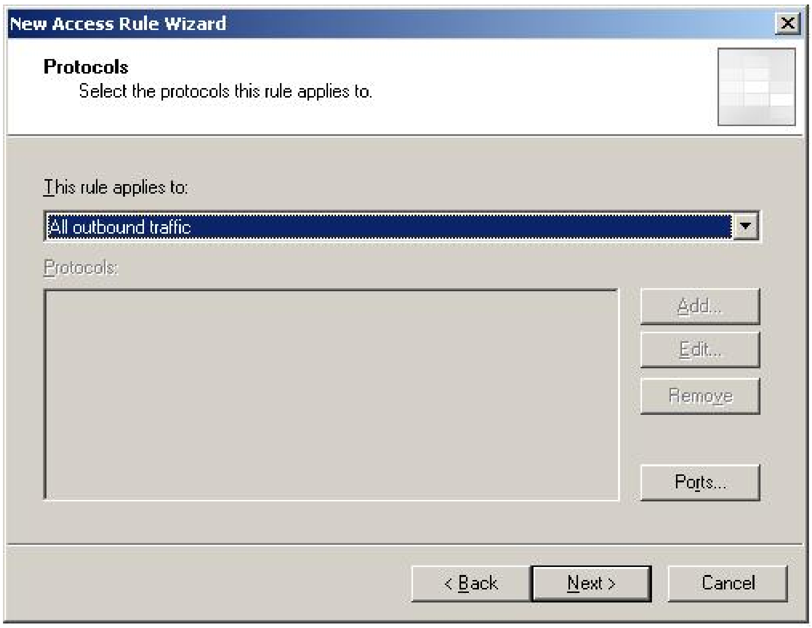
● **VPN Site-To-Site Network**
A VPN site-to-site network represents a network in a remote site, connected through a VPN link.

○ **External Network**
An external network represents an untrusted network, such as the Internet. ISA Server has a default external network.

Then click the Next button to move to the Protocols dialog.

3. Specify the protocols to which the rule applies

In "This rule applies to", select "All outbound traffic". This rule applies to outbound traffic because it applies to traffic that is outbound from the **source**, not the ISA server. For this rule, the source (which you select in the next step) is the remote network.



New Access Rule Wizard

Protocols

Select the protocols this rule applies to.

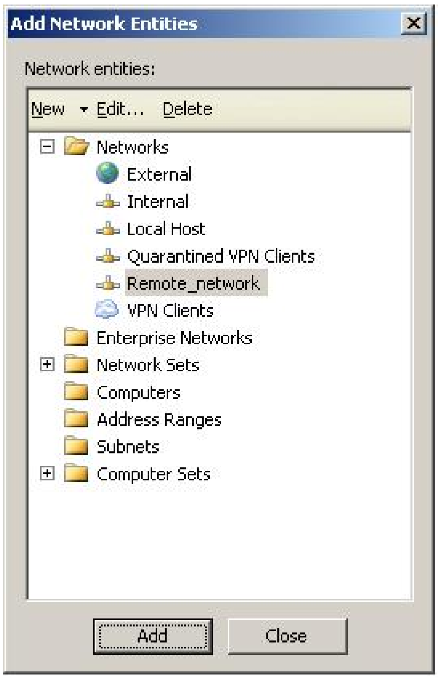
This rule applies to: All outbound traffic

Then click the Next button to move to the Access Rule Sources dialog.

4. Specify the source network for traffic to which the rule applies

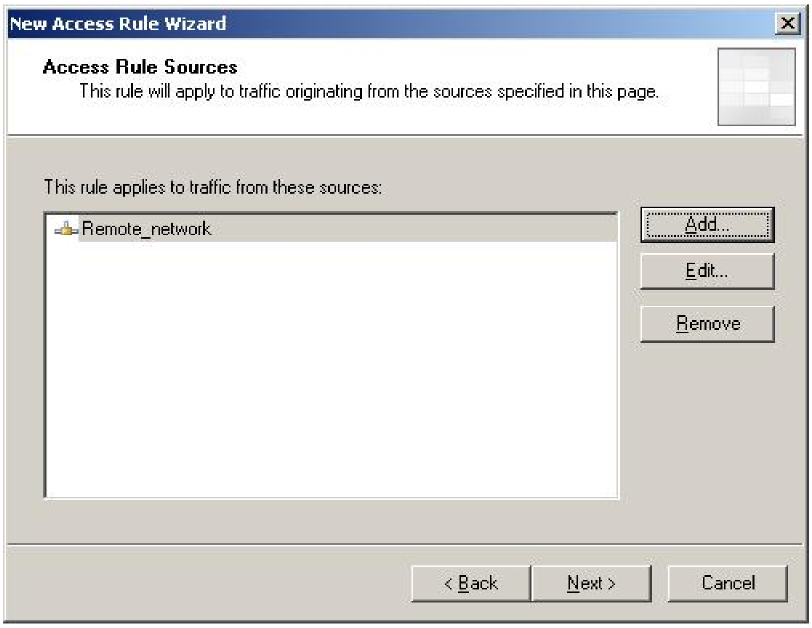
On the Access Rule Sources dialog, click the Add button to open the Add Network Entities dialog.

On the Add Network Entities dialog, select Remote_network. Click the Add button.



Then click the Close button to return to the Access Rule Sources dialog.

Check that the dialog now lists Remote_network.


New Access Rule Wizard

Access Rule Sources

This rule will apply to traffic originating from the sources specified in this page.

This rule applies to traffic from these sources:

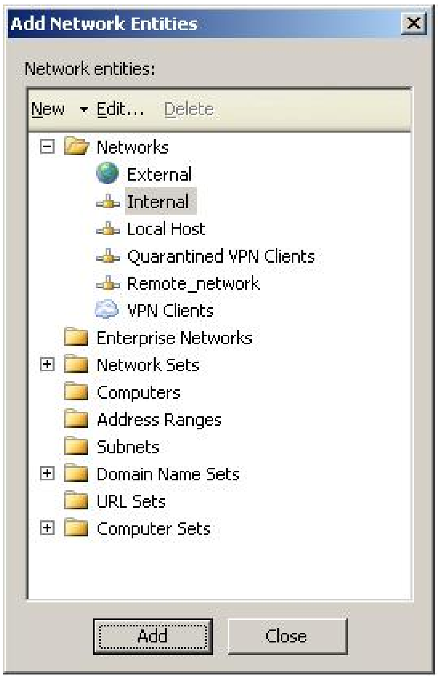
Remote_network

Then click the Next button to move to the Access Rule Destinations dialog.

5. Specify the destination network for traffic to which the rule applies

On the Access Rule Destinations dialog, click the Add button to open the Add Network Entities dialog.

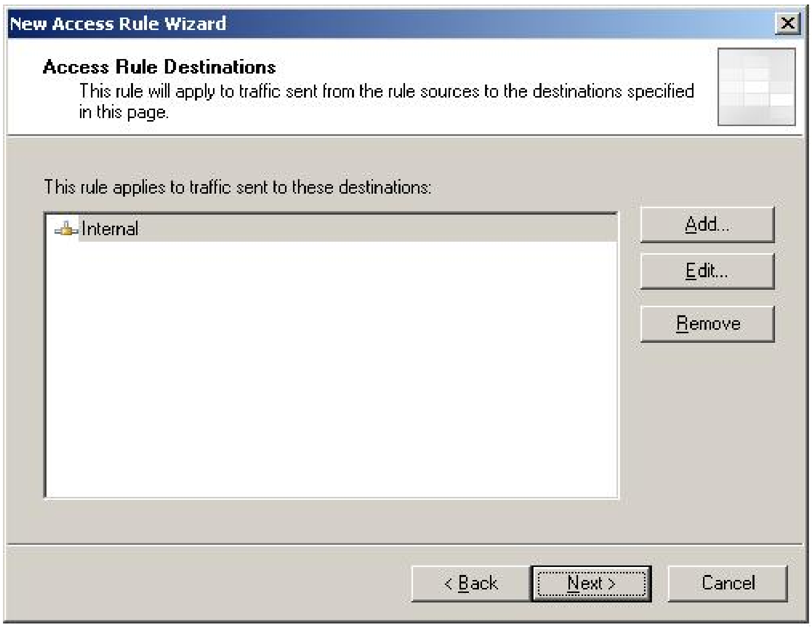
On the Add Network Entities dialog, select Internal. Click the Add button.


Add Network Entities

Network entities:

Then click the Close button to return to the Access Rule Destinations dialog.

Check that the dialog now lists Internal.



New Access Rule Wizard

Access Rule Destinations

This rule will apply to traffic sent from the rule sources to the destinations specified in this page.

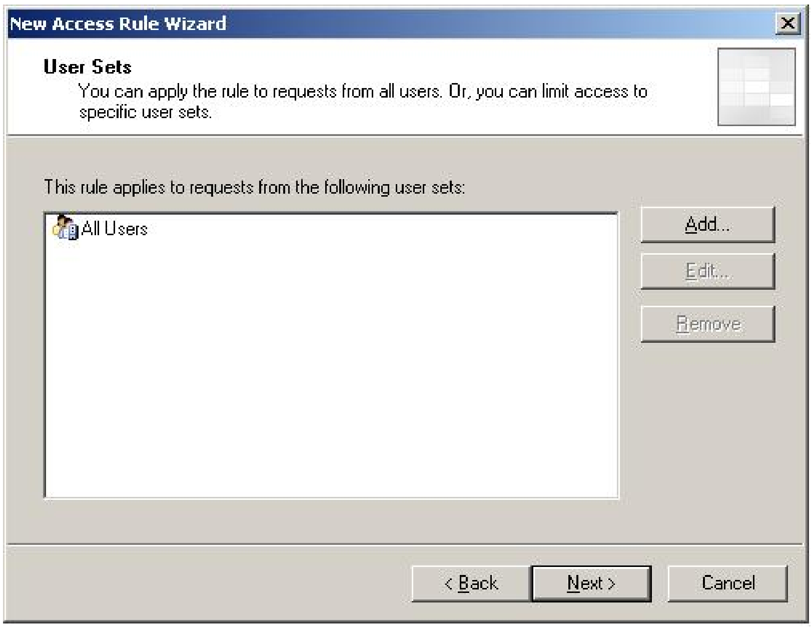
This rule applies to traffic sent to these destinations:

Internal

Then click the Next button to move to the User Sets dialog.

6. Specify the set of users to which the rule applies

Leave this set to the default “All Users”.



New Access Rule Wizard

User Sets

You can apply the rule to requests from all users. Or, you can limit access to specific user sets.

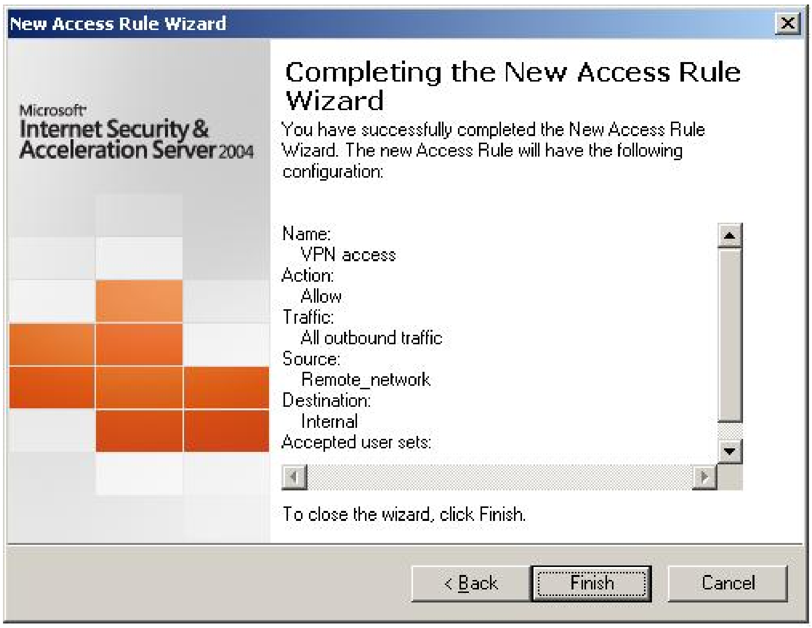
This rule applies to requests from the following user sets:

All Users

Click the Next button to move to the Completing the New Access Rule Wizard dialog.

7. Check your rule's settings

Review your settings and if necessary use the Back button to backtrack and change them.



Completing the New Access Rule Wizard

You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:

Name:
VPN access
Action:
Allow
Traffic:
All outbound traffic
Source:
Remote_network
Destination:
Internal
Accepted user sets:

To close the wizard, click Finish.

Once the settings are correct, click the Finish button.

8. Create a rule for traffic in the other direction

Repeat the steps from this section to create another access rule, for traffic in the reverse direction. Use the settings:

Rule Action:	Allow
Protocols:	All outbound traffic
Access Rule Sources:	Internal
Access Rule Destinations:	Remote_network
User Sets:	All Users

Like the first rule, this rule applies to outbound traffic because it applies to traffic that is outbound from the source. For this rule, the source is the internal network.

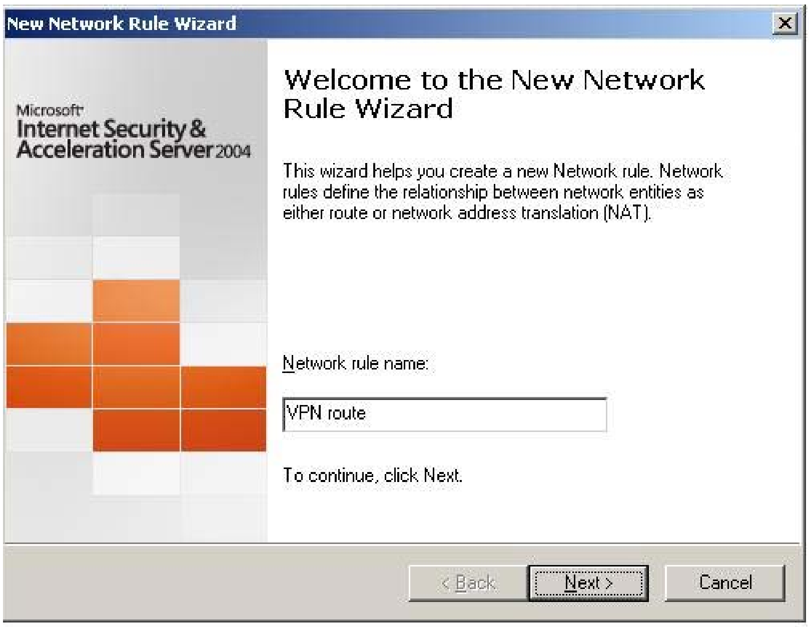
Note that the Microsoft ISA Server processes rules in the order in which they appear on the Firewall Policy list. Once it finds a match, the ISA Server does not look at any rules that are further down the list.

Configure the ISA Server—network rules

This section describes how to create a network rule. This rule stops the ISA server from applying NAT on tunneled traffic.

1. Start the New Network Rule Wizard

Right-click on Networks from the ISA server left-hand menu, and select New > Network Rule. The New Network Rule Wizard opens:



Welcome to the New Network Rule Wizard

This wizard helps you create a new Network rule. Network rules define the relationship between network entities as either route or network address translation (NAT).

Network rule name: VPN route

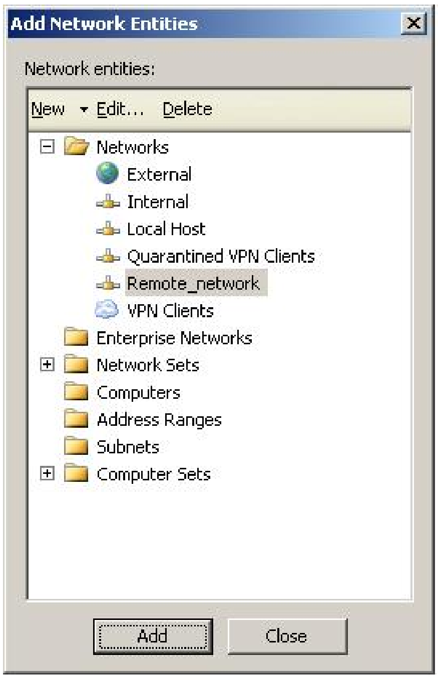
To continue, click Next.

Enter a name such as "VPN route" and click the Next button to move to the Network Traffic Sources dialog.

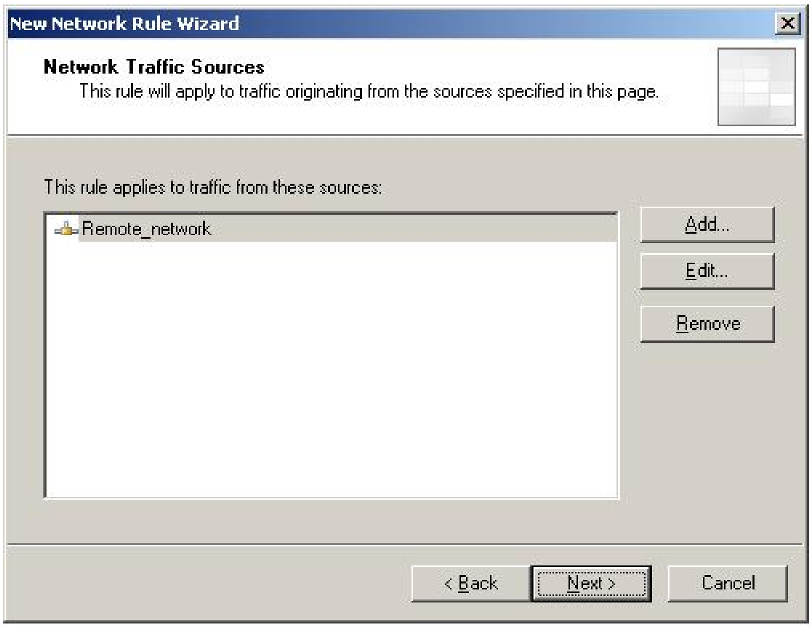
2. Specify the source network

On the Network Traffic Sources dialog, click the Add button to open the Add Network Entities dialog.

On the Add Network Entities dialog, select Remote_network. Click the Add button.



Then click the Close button to return to the Network Traffic Sources dialog. Check that the dialog now lists Remote_network.



Network Traffic Sources

This rule will apply to traffic originating from the sources specified in this page.

This rule applies to traffic from these sources:

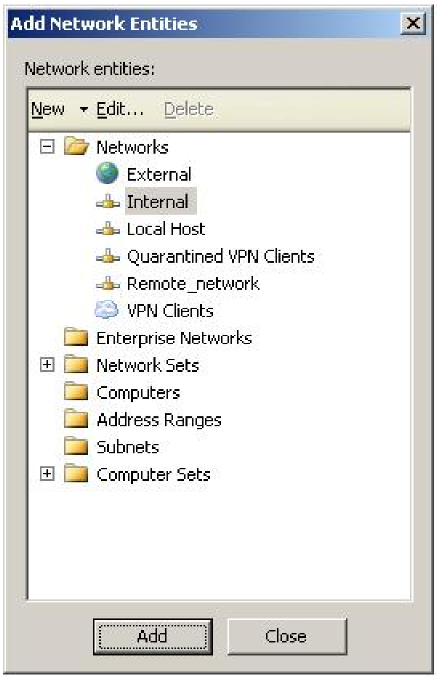
Remote_network

Then click the Next button to move to the Network Traffic Destinations dialog.

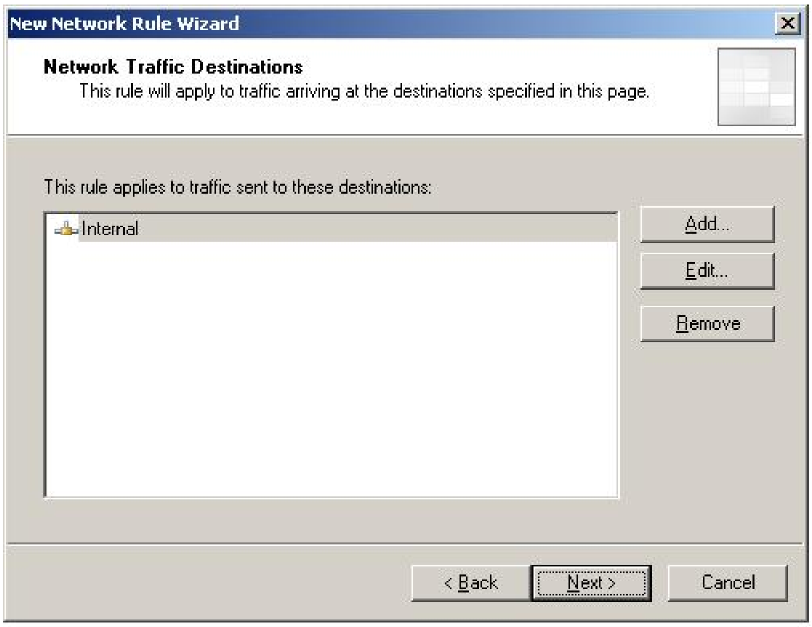
3. Specify the destination network

On the Network Traffic Destinations dialog, click the Add button to open the Add Network Entities dialog.

On the Add Network Entities dialog, select Internal. Click the Add button.



Then click the Close button to return to the Network Traffic Destinations dialog. Check that the dialog now lists Internal.


New Network Rule Wizard

Network Traffic Destinations

This rule will apply to traffic arriving at the destinations specified in this page.

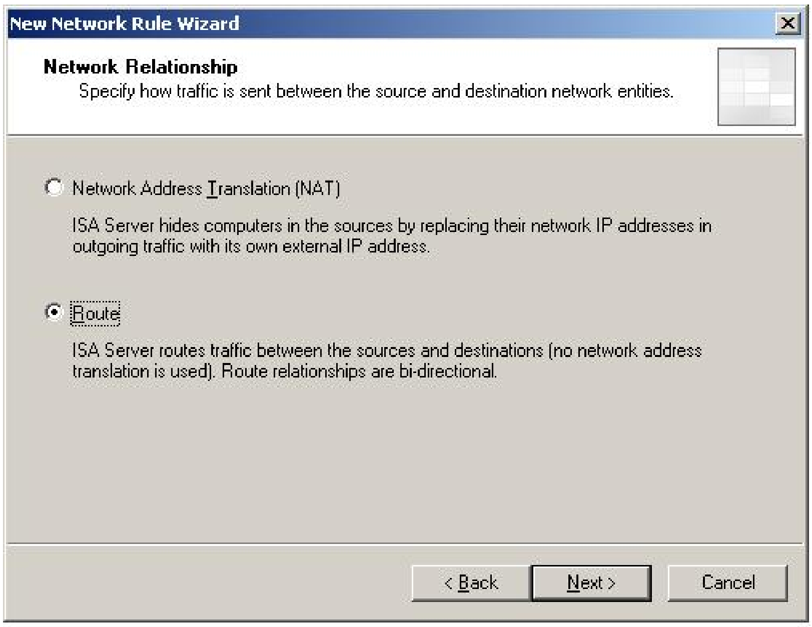
This rule applies to traffic sent to these destinations:

Internal

Then click the Next button to move to the Network Relationship dialog.

4. Specify to not apply NAT to the traffic

Select “Route”.



New Network Rule Wizard

Network Relationship

Specify how traffic is sent between the source and destination network entities.

○ Network Address Translation (NAT)

ISA Server hides computers in the sources by replacing their network IP addresses in outgoing traffic with its own external IP address.

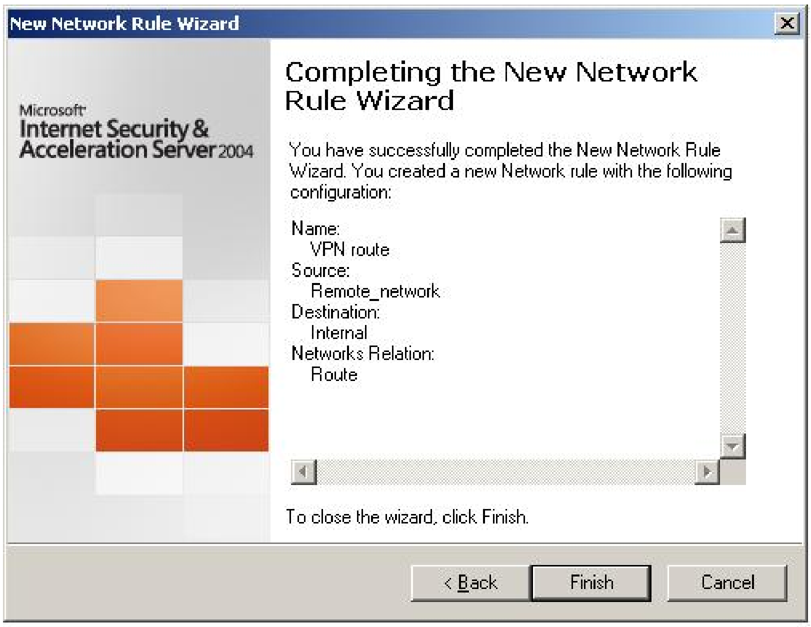
● Route

ISA Server routes traffic between the sources and destinations (no network address translation is used). Route relationships are bi-directional.

Then click the Next button to move to the Completing the New Network Rule Wizard dialog.

5. Check your rule’s settings

Review your settings and if necessary use the Back button to backtrack and change them.



New Network Rule Wizard

Completing the New Network Rule Wizard

You have successfully completed the New Network Rule Wizard. You created a new Network rule with the following configuration:

```
Name:
    VPN route
Source:
    Remote_network
Destination:
    Internal
Networks Relation:
    Route
```

To close the wizard, click Finish.

Once the settings are correct, click the Finish button.

6. Move the rule into the correct position

If you have other rules which apply NAT to traffic, this rule must be processed first. To ensure this:

1. Open the Network Rules tab of the Network dialog, The Microsoft ISA Server processes rules in the order in which they appear on this tab. Once it finds a match, the ISA Server does not look at any rules that are further down the list.
2. Right-click on the new rule and select Move Up.
3. Keep selecting Move Up until the rule is above all rules that have NAT as their network relationship.

7. Save the configuration

In the main ISA Server window, click Apply to save and apply the configuration you have created.

Test the tunnel

This section describes how to check that the VPN tunnel is correctly configured.

1. Ping the private side of the ISA server

Initiate a ping from a device on the private side of the client router to a device on the private side of the ISA server. The ping should be successful.

2. Check the SAs

On the router, check that the ISAKMP and IPSEC SAs (Security Associations) have been established, by using the commands:

```
show isakmp sa

show ipsec sa
```

If the SAs have been established, this proves that the VPN tunnel has come up and that the two private networks can communicate.

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