TheGreenBow IPSec VPN Client

Configuration Guide

Windows 2000 Server

WebSite:	http://www.thegreenbow.com
Contact:	support@thegreenbow.com

Table of contents

1 Goal of this document

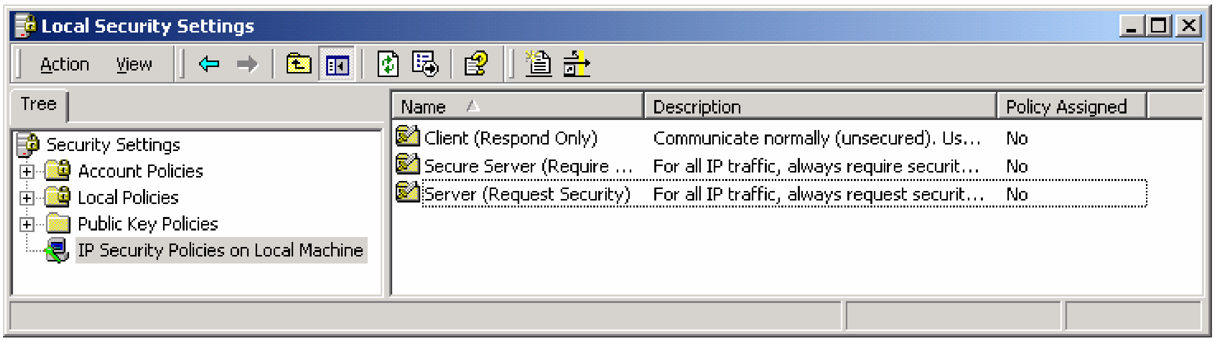
This document describes VPN configuration of TheGreenBow IPSec VPN client and a host server with Microsoft Windows 2000 server. The two computers belong to the same local network. TheGreenBow VPN Client IP address is 192.168.1.3 and Windows 2000 Server IP address is 192.168.1.2.

This configuration is given as an example.

2 Windows 2000 Server VPN Configuration

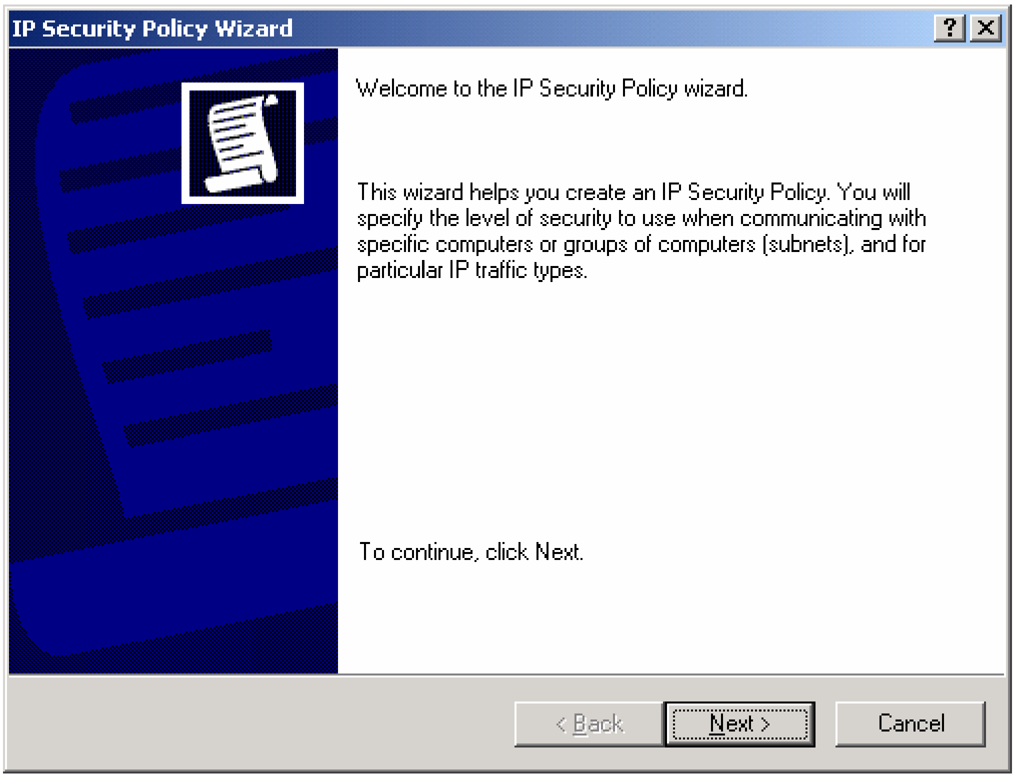
2.1 Windows 2000 Server IP Security Policies

- For changing IPSec VPN configuration, click on Start , Programs, Administration tools, Local security settings.



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecured). Us...	No
Secure Server (Require ...	For all IP traffic, always require securit...	No
Server (Request Security)	For all IP traffic, always request securit...	No

- Right-click on « IP Security Policies on Local Machine ». Then left-click on « Create IP Security Policy ». The Security Policy wizard starts. Click on « Next ».

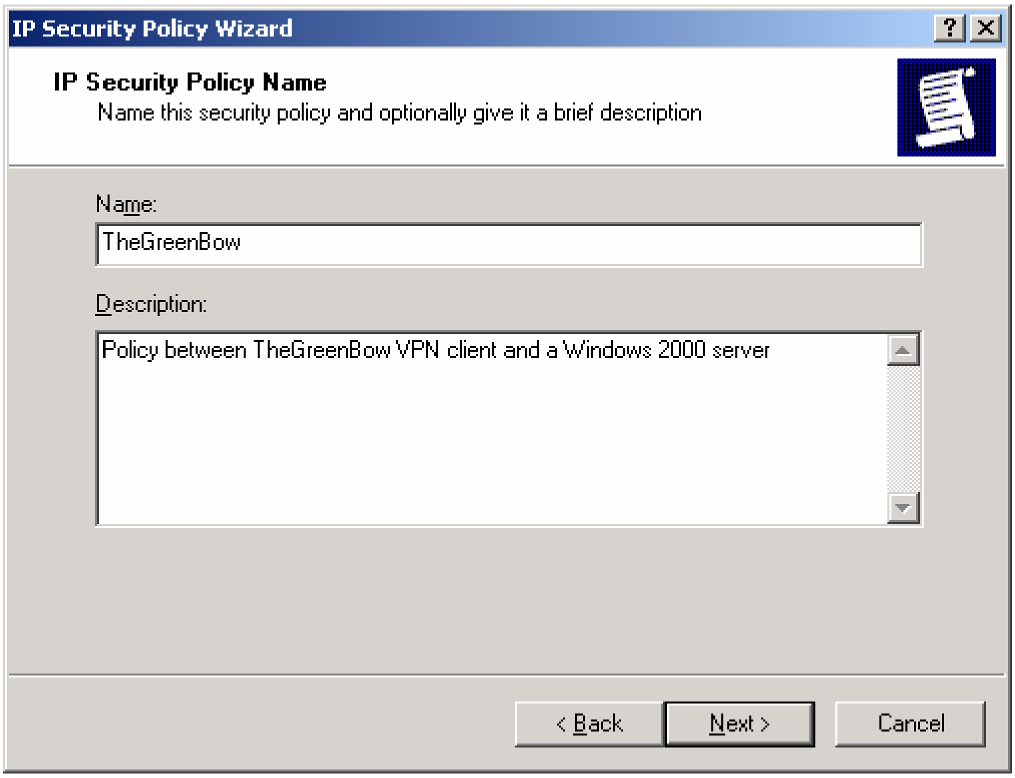


Welcome to the IP Security Policy wizard.

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.

- Give a name to your Security rule and a description. Then click on « Next ».



IP Security Policy Wizard

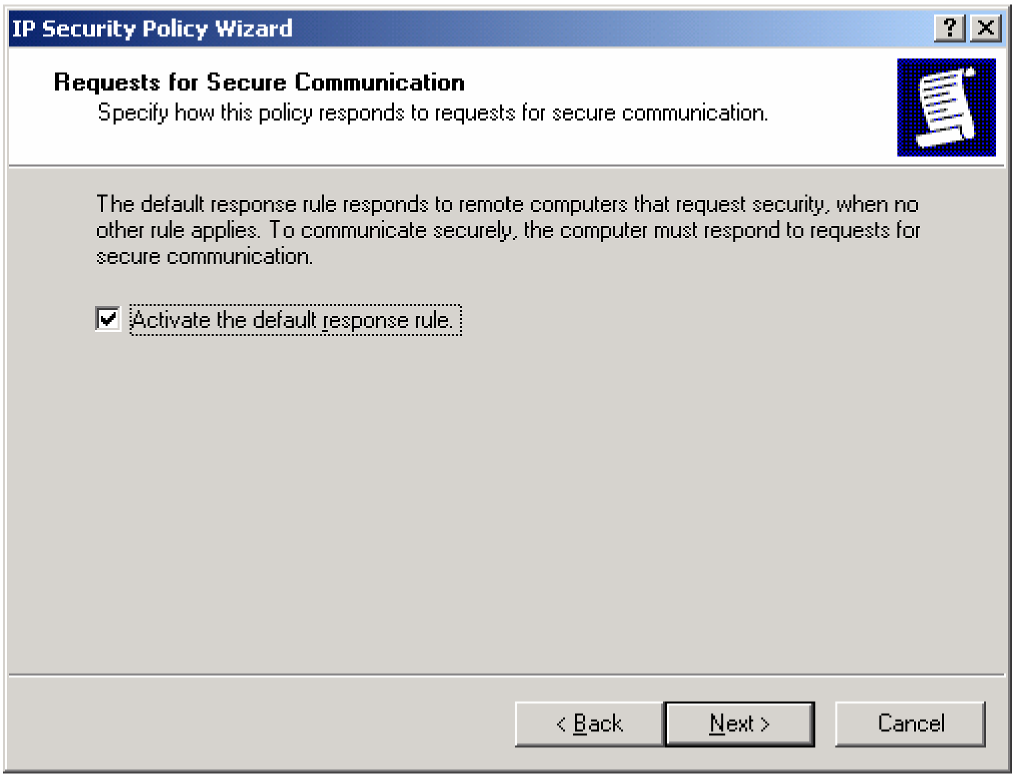
IP Security Policy Name

Name this security policy and optionally give it a brief description

Name: TheGreenBow

Description: Policy between TheGreenBow VPN client and a Windows 2000 server

- Click on « Next ».



IP Security Policy Wizard

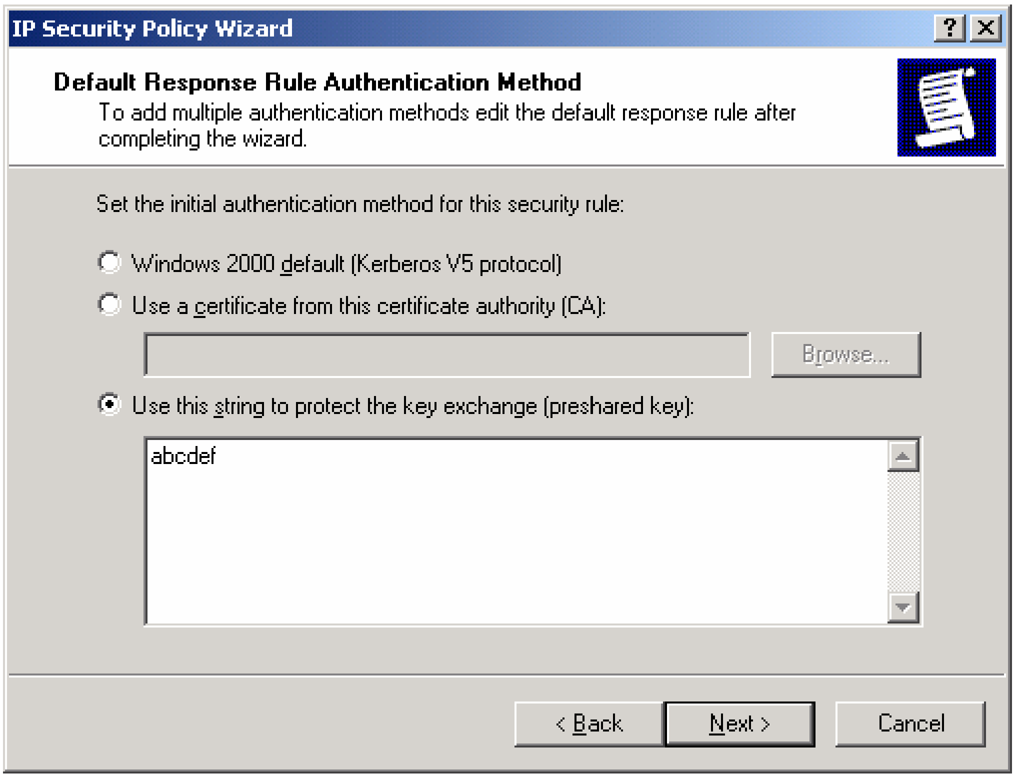
Requests for Secure Communication

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.

- Click on « Use this string to protect the key exchange » and fill the form with a preshared key. This value will be used by the VPN client. Then click on « Next ».



Default Response Rule Authentication Method

To add multiple authentication methods edit the default response rule after completing the wizard.

Set the initial authentication method for this security rule:

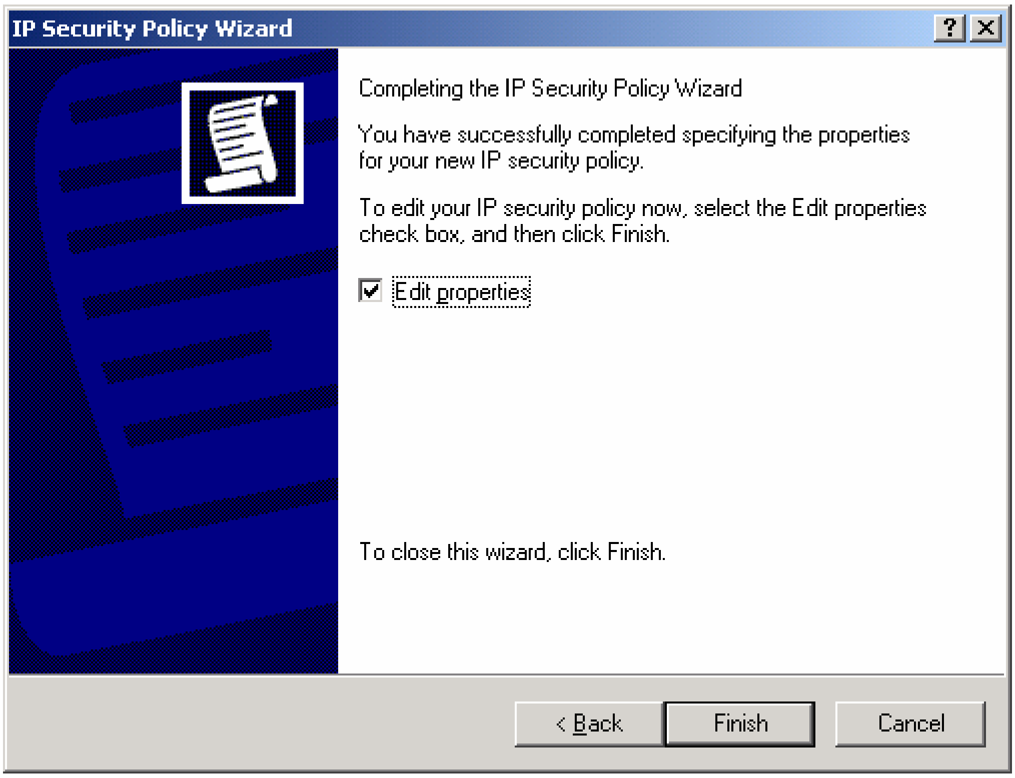
○ Windows 2000 default (Kerberos V5 protocol)

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

● Use this string to protect the key exchange (preshared key):

abcdef

- Click on « Next ».



Completing the IP Security Policy Wizard

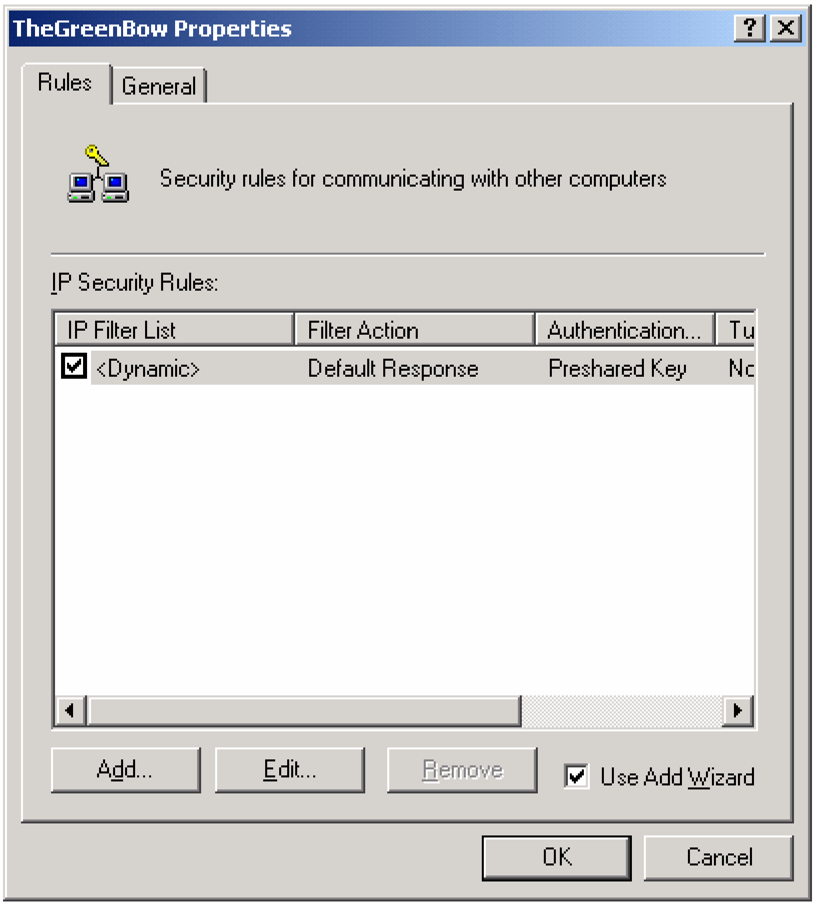
You have successfully completed specifying the properties for your new IP security policy.

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.

- Unchecked « **default response** » then click on « **Add** ». We will add a security rule for the Windows 2000 server.



TheGreenBow Properties

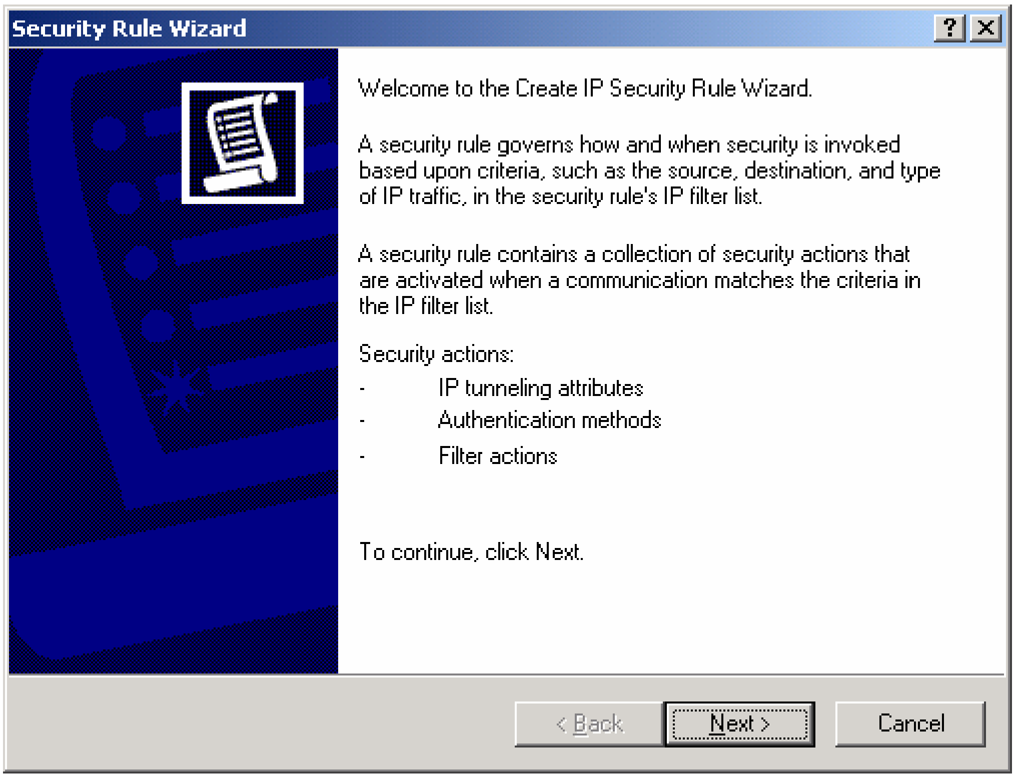
Rules | General

Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ <Dynamic>	Default Response	Preshared Key	Nc

- Click on « Next ».



Security Rule Wizard

Welcome to the Create IP Security Rule Wizard.

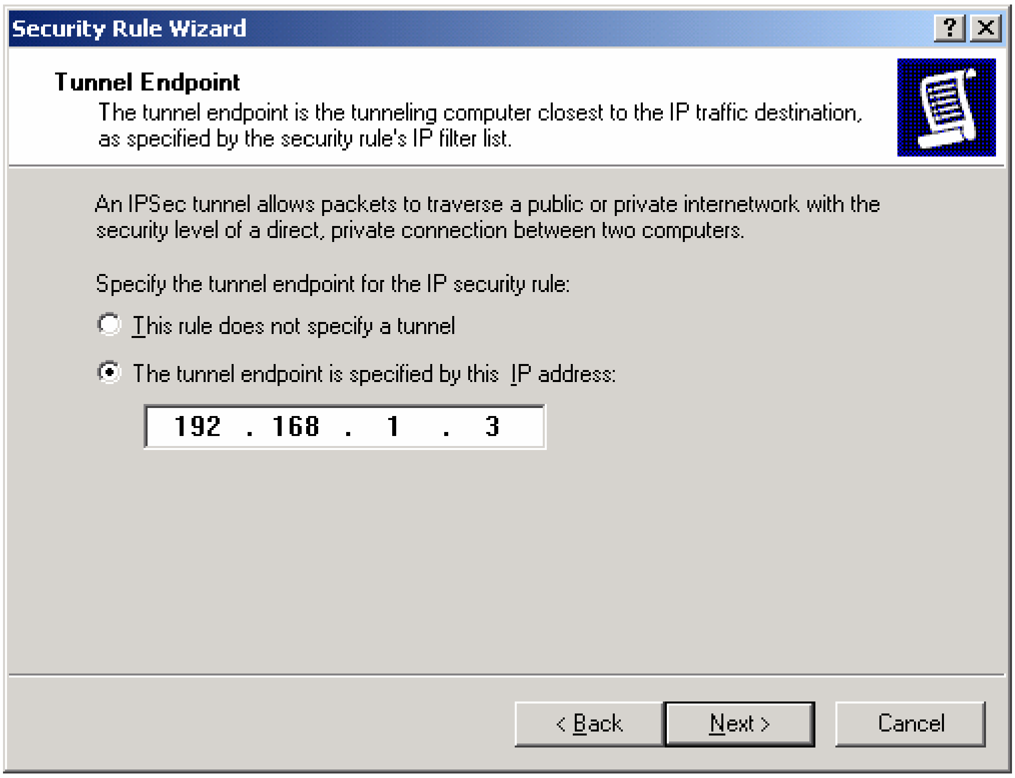
A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

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.

- This security rule concerns a tunnel between the Microsoft Windows 2000 Server and TheGreenBow VPN client. VPN client is the remote endpoint and has IP address 192.168.1.3. Use this address and click on « Next »



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.

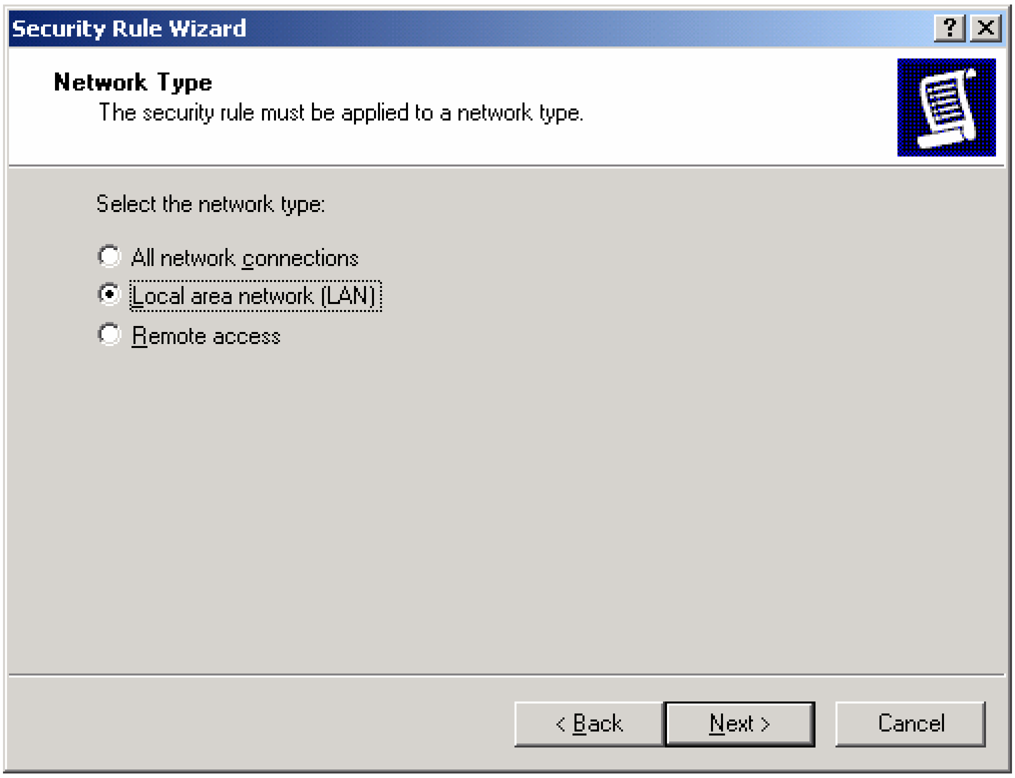
Specify the tunnel endpoint for the IP security rule:

○ This rule does not specify a tunnel

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 3

- In our example, the computers belong to the same local area network. Click on « **Local area network** » then on « **Next** ».



Security Rule Wizard

Network Type

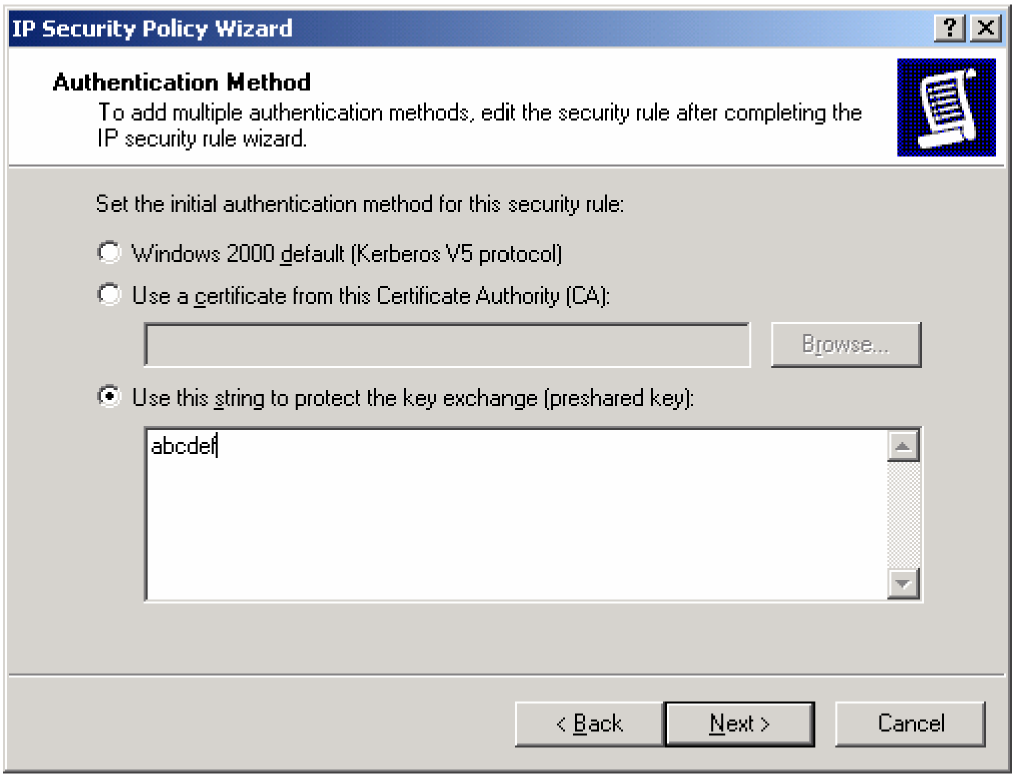
The security rule must be applied to a network type.

Select the network type:

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

2.2 Windows 2000 Server Pre Shared key

- Communication between the IPsec client and the server is protected by a preshared key. Click on « **Use this string to protect the key exchange (preshared key)** » and fill the form with the preshared key value. Click on « **Next**».



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)

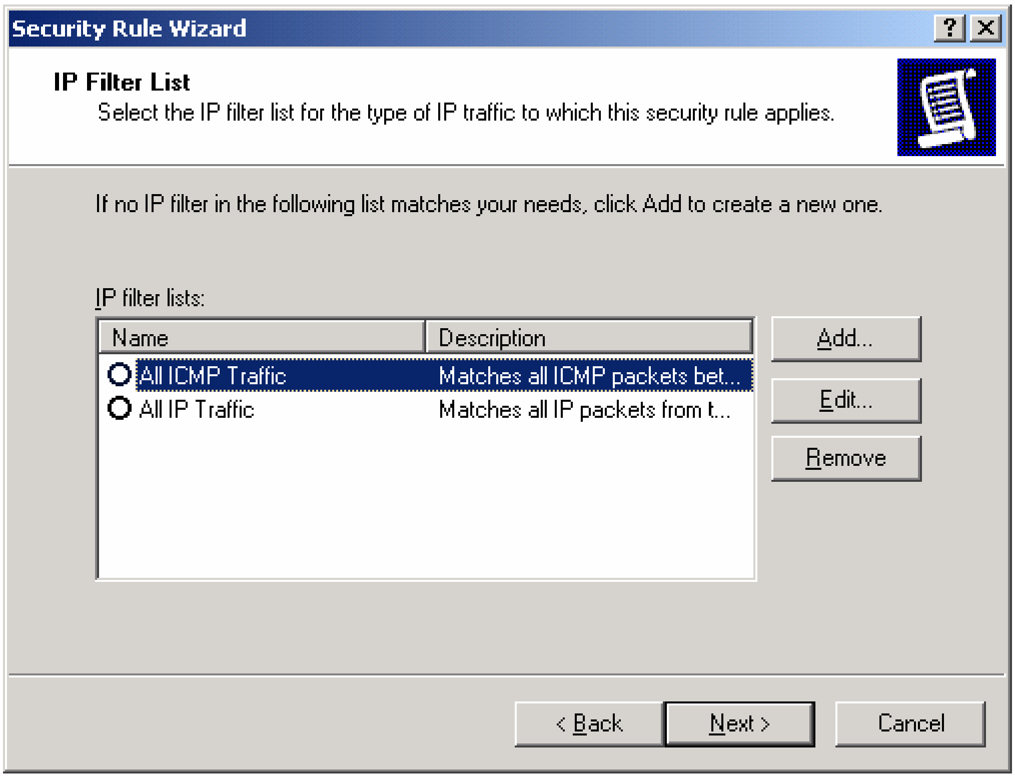
○ Use a certificate from this Certificate Authority (CA):

● Use this string to protect the key exchange (preshared key):

abcdef

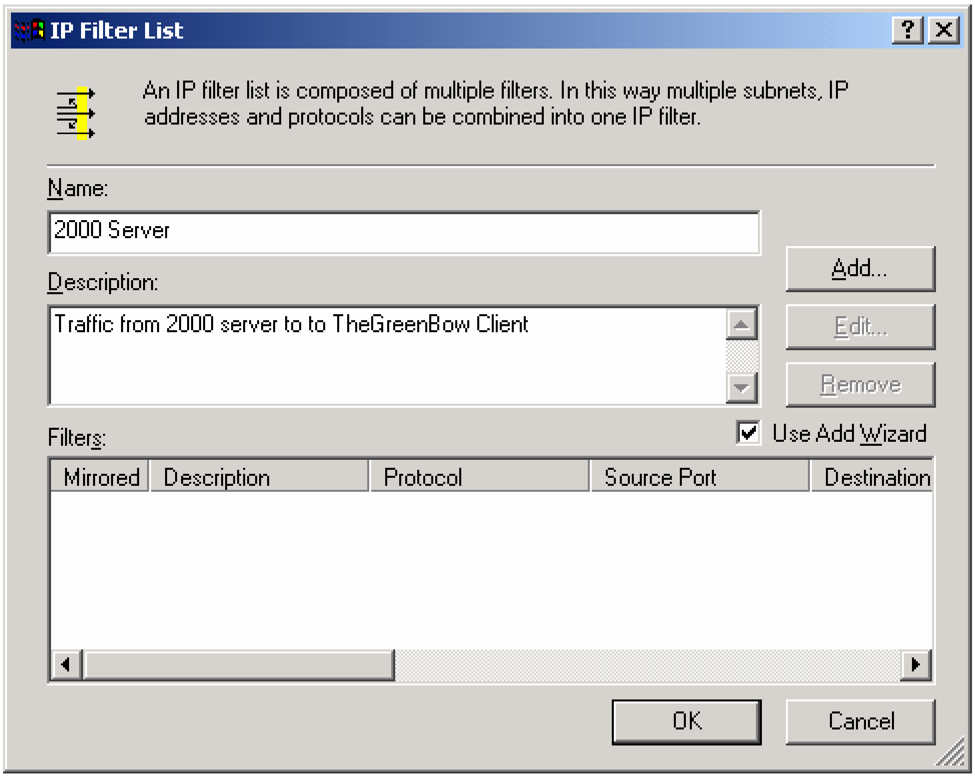
2.3 Windows 2000 Server IP Filter

- Now, we must link our security rule with a IP filter. Click on « **Add** ».


Security Rule Wizard
?
X
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:
Add...
Edit...
Remove
< Back
Next >
Cancel

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

- Give a name to your IP filter and a description. Then click on « **Add** ».

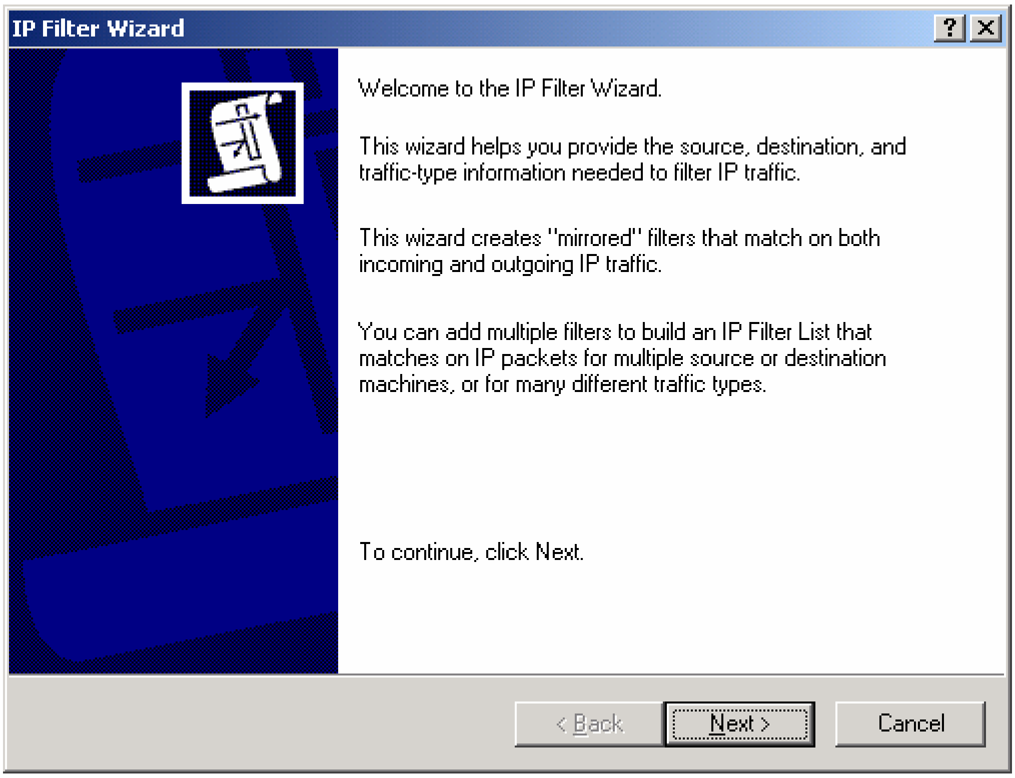

IP Filter List
?
X
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Add...
Edit...
Remove
☑ Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel

Name: 2000 Server

Description: Traffic from 2000 server to to TheGreenBow Client

Filters:

- Configuration wizard begins. Click on « Next ».



IP Filter Wizard

Welcome to the IP Filter Wizard.

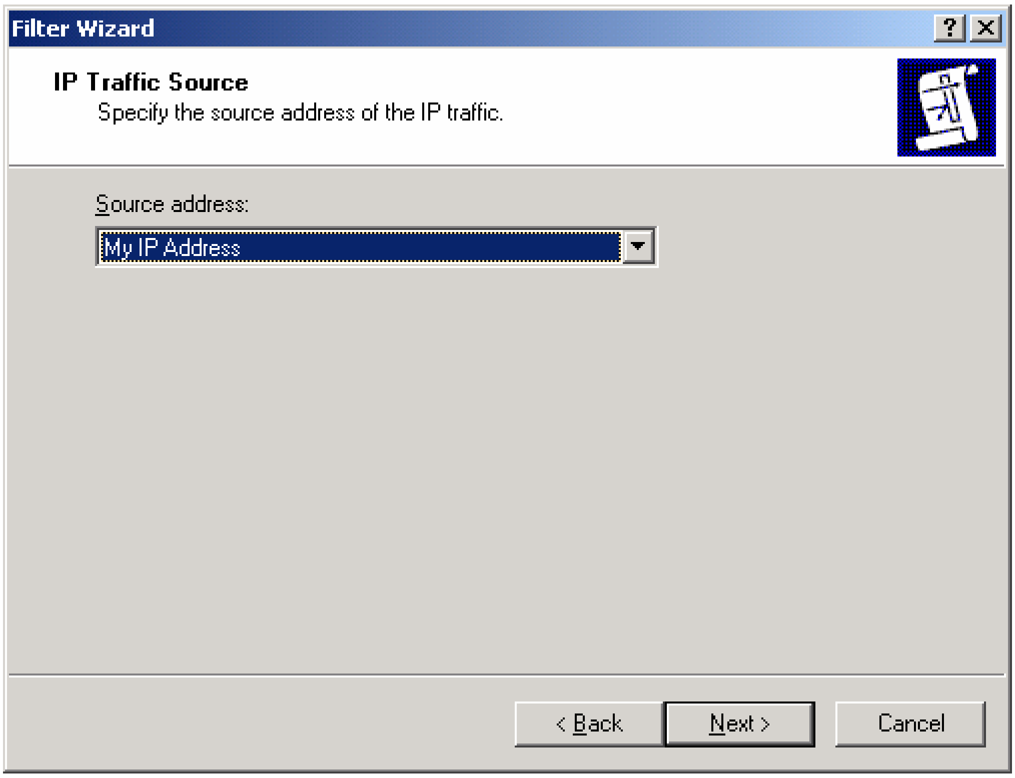
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

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.

- Give starting endpoint IP address of the VPN tunnel (Microsoft Windows 2000 Server). Then click on « Next ».



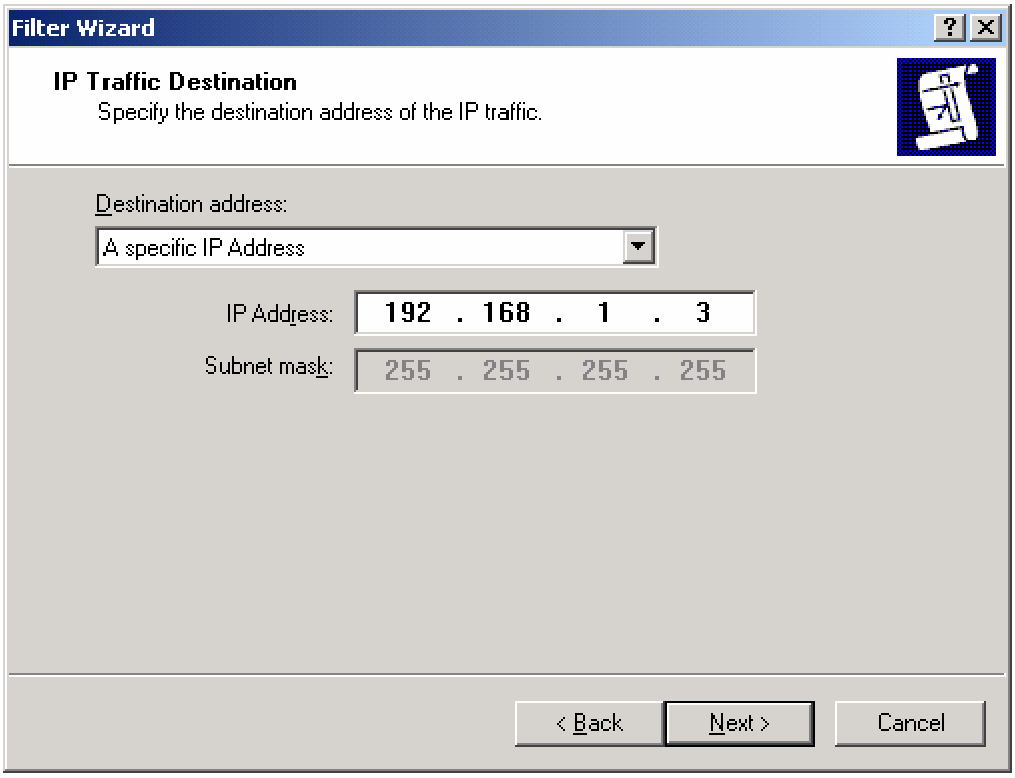
Filter Wizard

IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

- Give final endpoint IP address of the VPN tunnel (TheGreenBow VPN client). Then click on « Next »



Filter Wizard

IP Traffic Destination

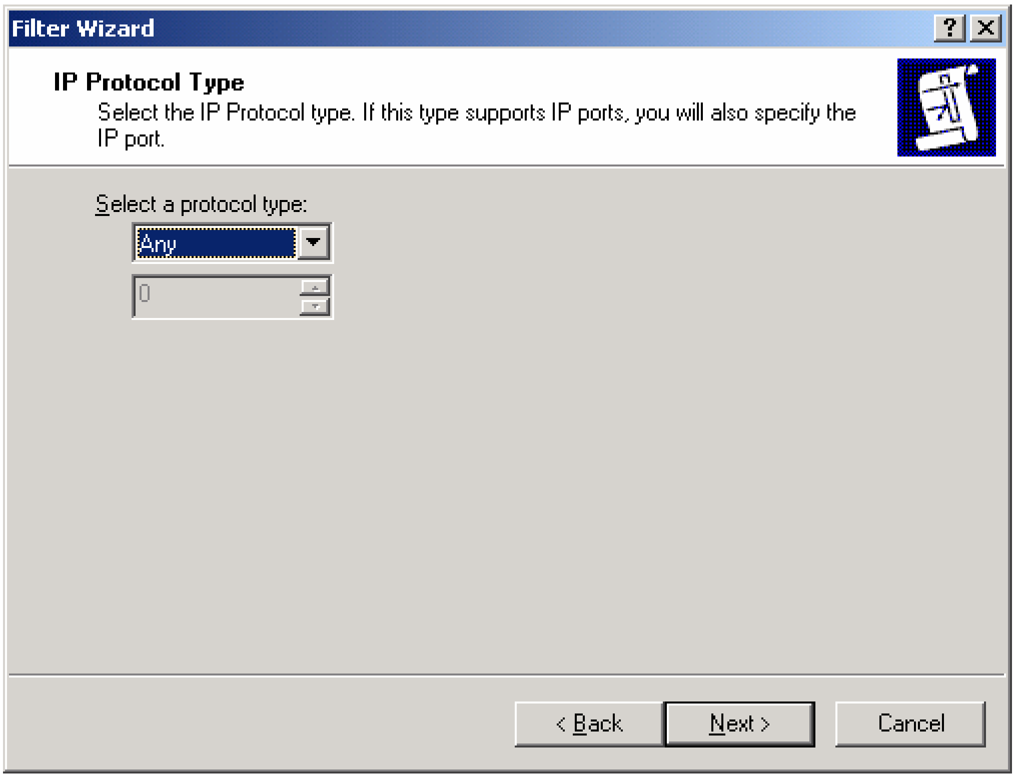
Specify the destination address of the IP traffic.

Destination address: A specific IP Address

IP Address: 192 . 168 . 1 . 3

Subnet mask: 255 . 255 . 255 . 255

- Select protocol type and then click on « Next ».



Filter Wizard

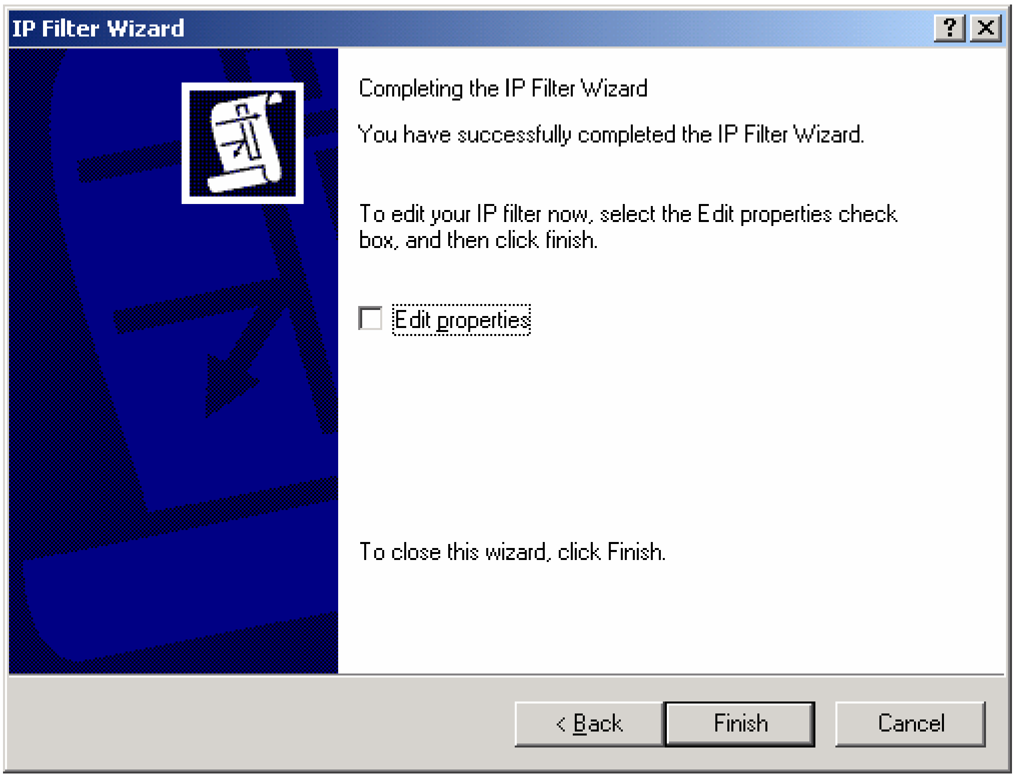
IP Protocol Type

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

Select a protocol type: Any

0

- Click on « **Finish** » for ending IP filter creation.



IP Filter Wizard

Completing the IP Filter Wizard

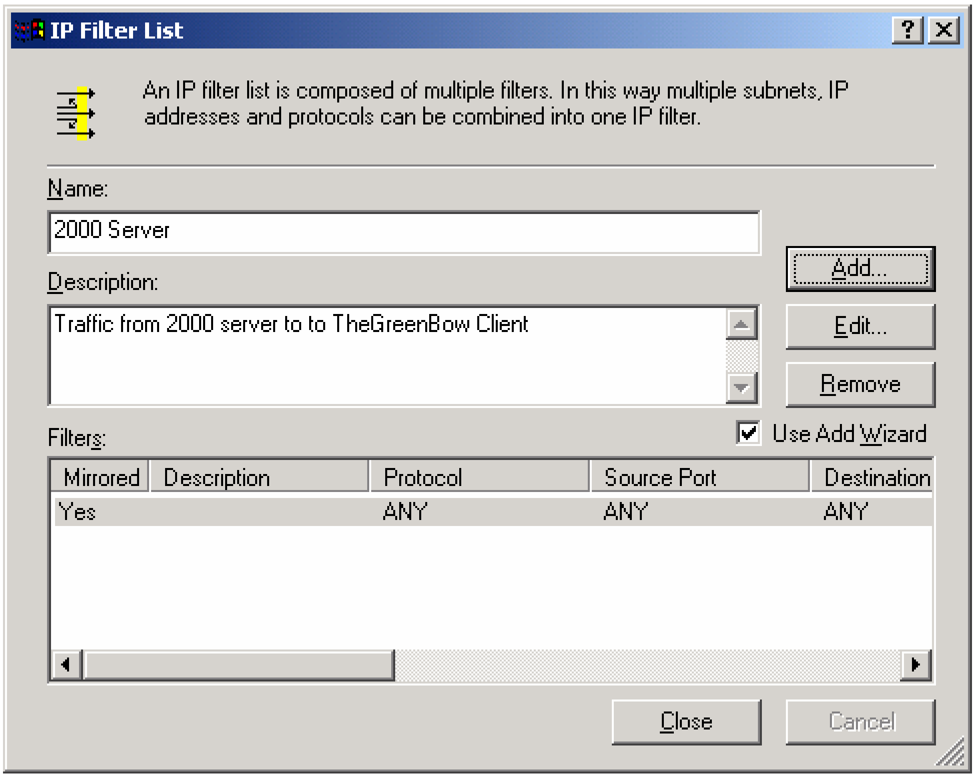
You have successfully completed the IP Filter Wizard.

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

□ Edit properties

To close this wizard, click Finish.

- IP filter was added. Click on « **Close** »



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:

2000 Server

Description:

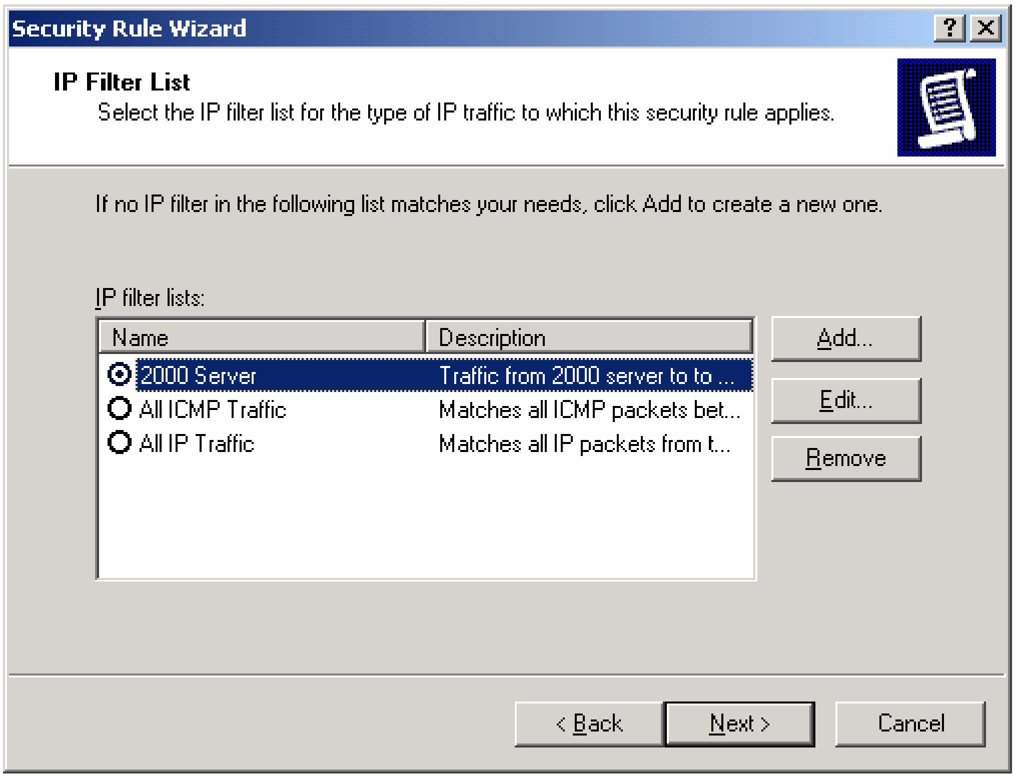
Traffic from 2000 server to to TheGreenBow Client

Filters:

☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

- Select in the list the IP filter you have just created, then click on « Next ».



Security Rule Wizard

IP Filter List

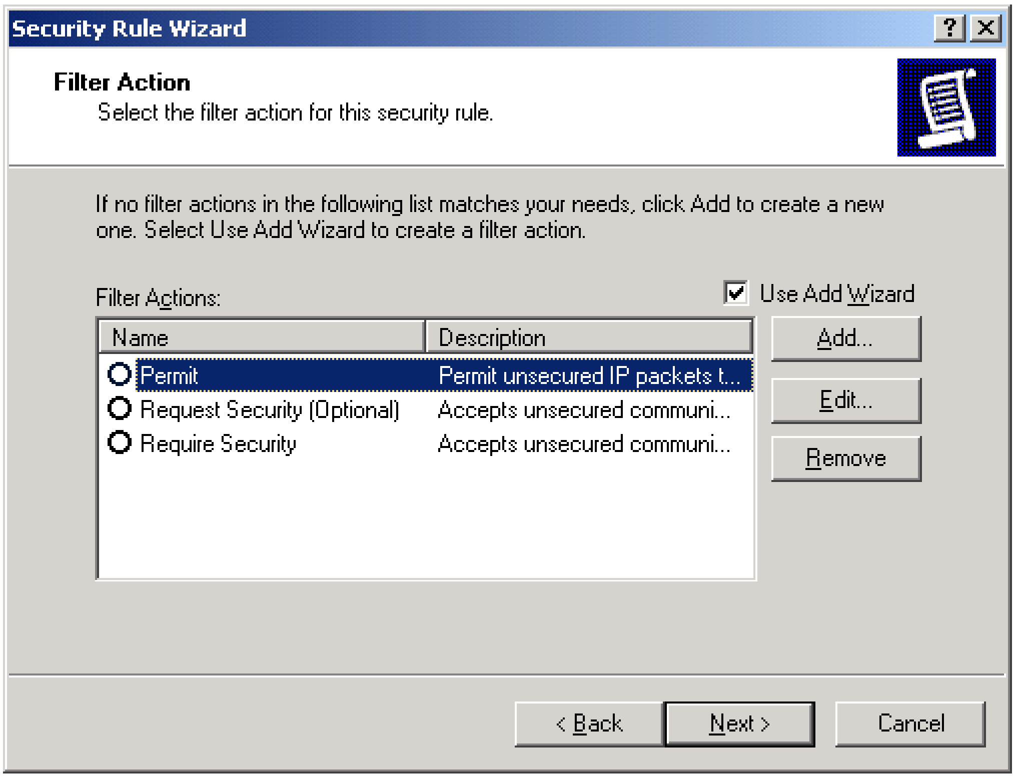
Select the IP filter list for the type of IP traffic to which this security rule applies.

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

IP filter lists:

Name	Description
● 2000 Server	Traffic from 2000 server to to ...
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

- You must associate a filter action with a security rule. Click on « Add ».



Security Rule Wizard

Filter Action

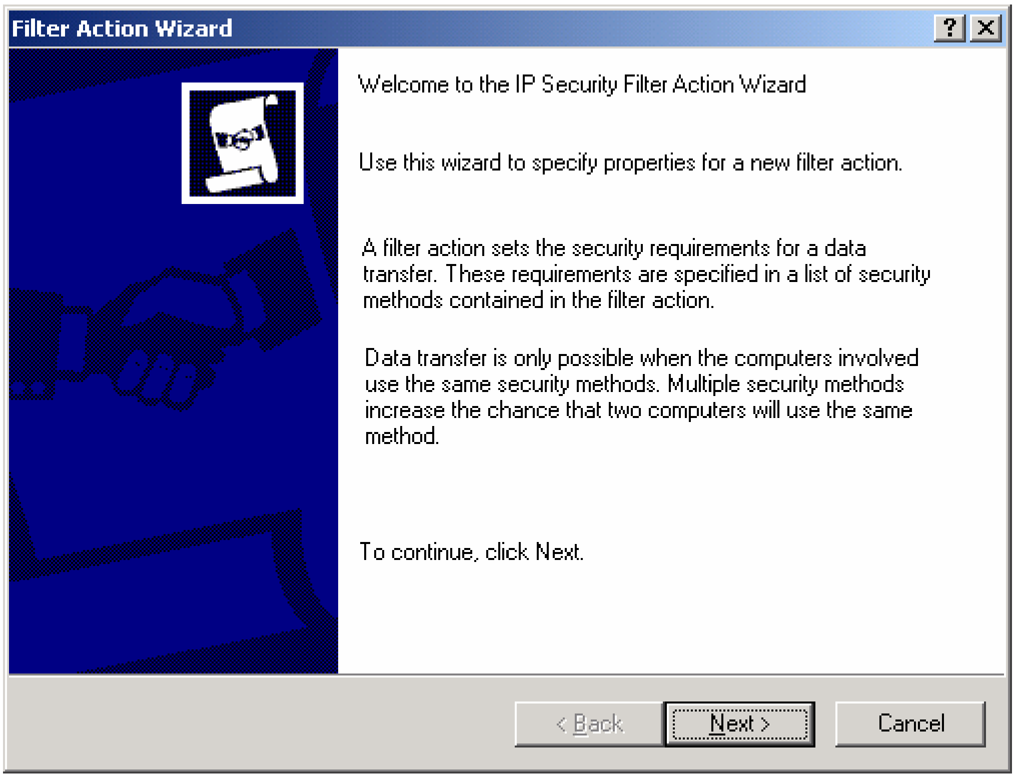
Select the filter action for this security rule.

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...

- Click on « Next ».



Filter Action Wizard

Welcome to the IP Security Filter Action Wizard

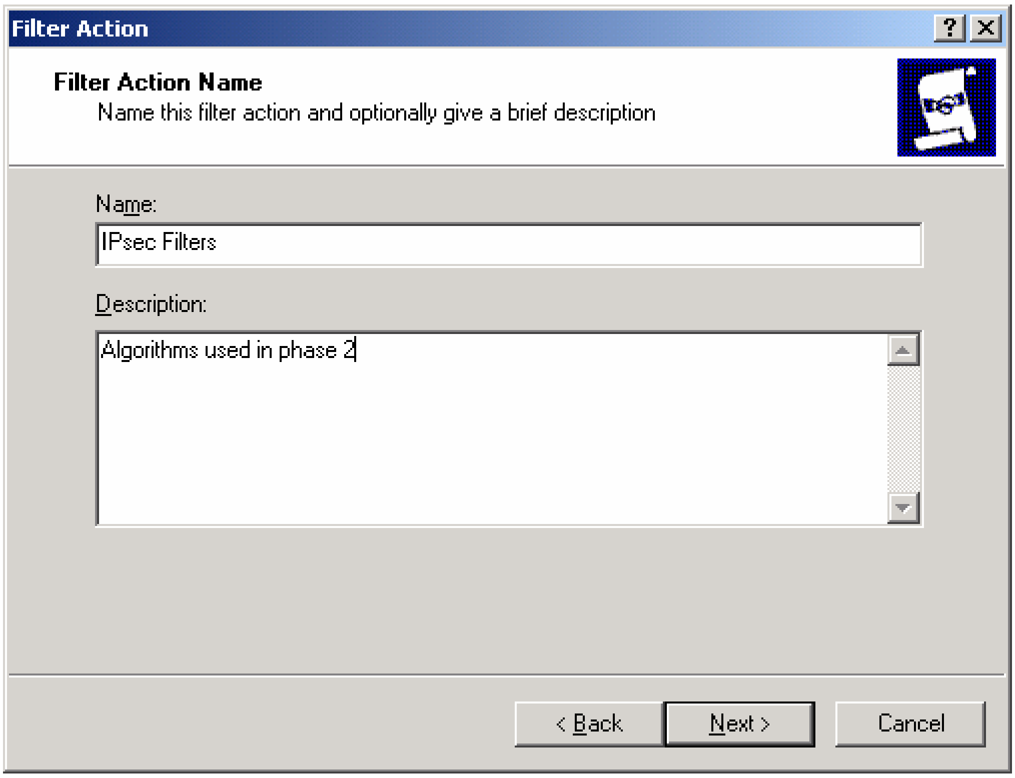
Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

- Give a name for your Filter Action then click on « Next ».



Filter Action

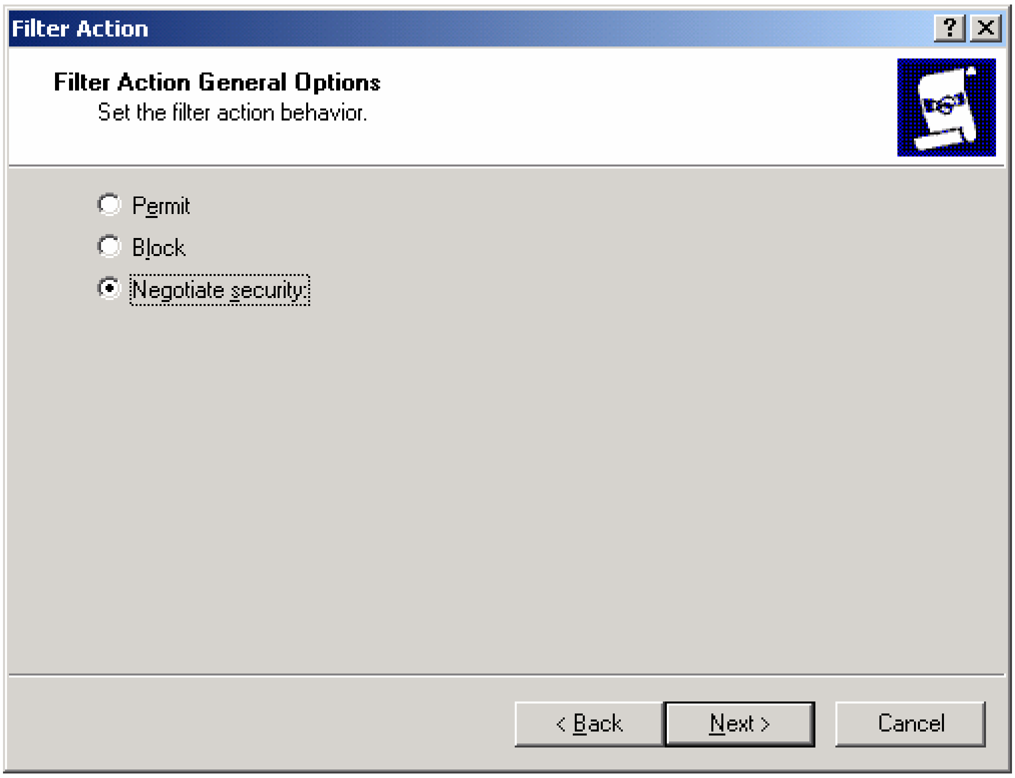
Filter Action Name

Name this filter action and optionally give a brief description

Name:
IPsec Filters

Description:
Algorithms used in phase 2

- Click on « Negotiate security » then on « Next ».



Filter Action

Filter Action General Options

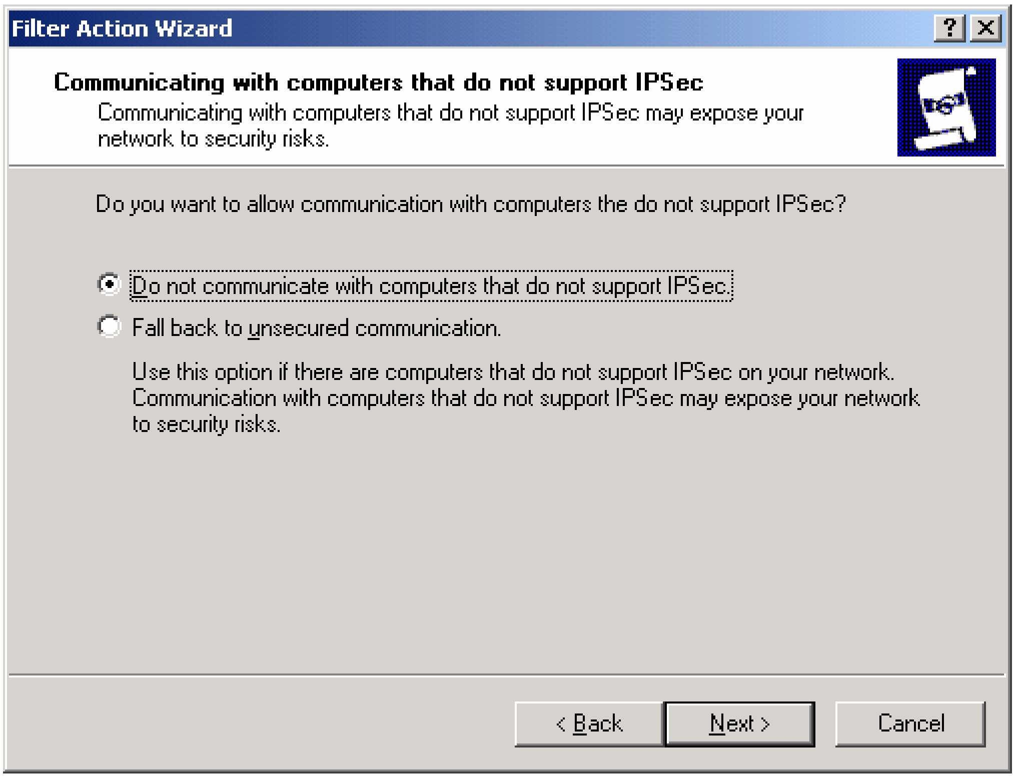
Set the filter action behavior.

○ Permit

○ Block

● Negotiate security:

- Click on « Do not communicate with computers that do not support IPSec » if you want every communication between the client and the server to be secured. Then click on « Next ».



Filter Action Wizard

Communicating with computers that do not support IPSec

Communicating with computers that do not support IPSec may expose your network to security risks.

Do you want to allow communication with computers the do not support IPSec?

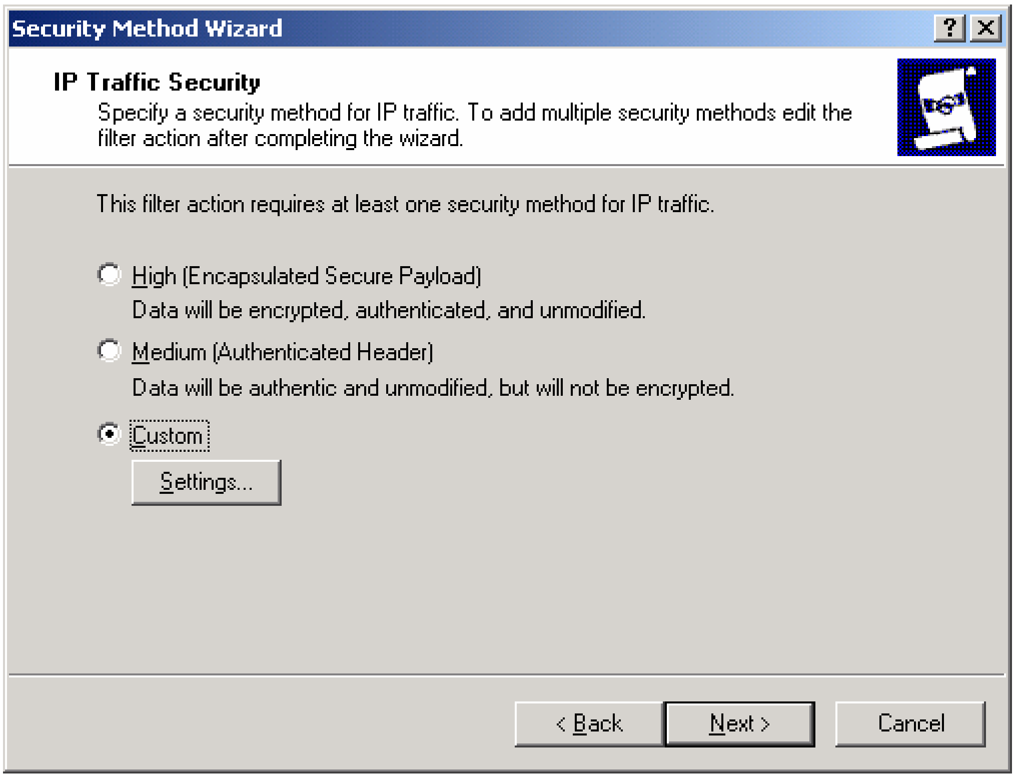
● Do not communicate with computers that do not support IPSec.

○ Fall back to unsecured communication.

Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.

2.4 Windows 2000 Server IPSec algorithms

- Select « Custom » and click on « Settings ».



IP Traffic Security

Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.

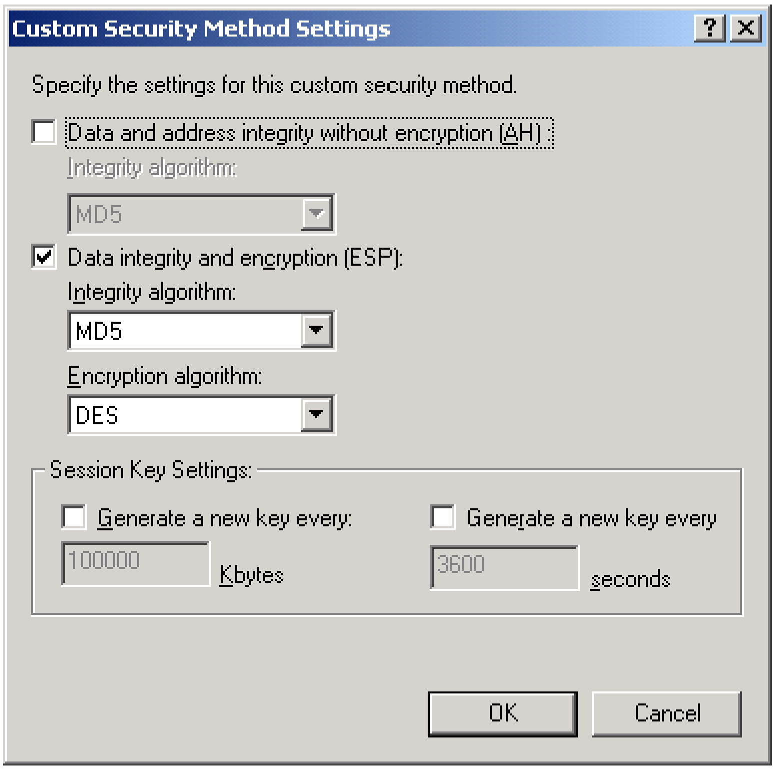
This filter action requires at least one security method for IP traffic.

○ High (Encapsulated Secure Payload)
Data will be encrypted, authenticated, and unmodified.

○ Medium (Authenticated Header)
Data will be authentic and unmodified, but will not be encrypted.

● Custom

- In our example, we are using MD5 and DES with ESP. Click on « OK » and on « Next ».



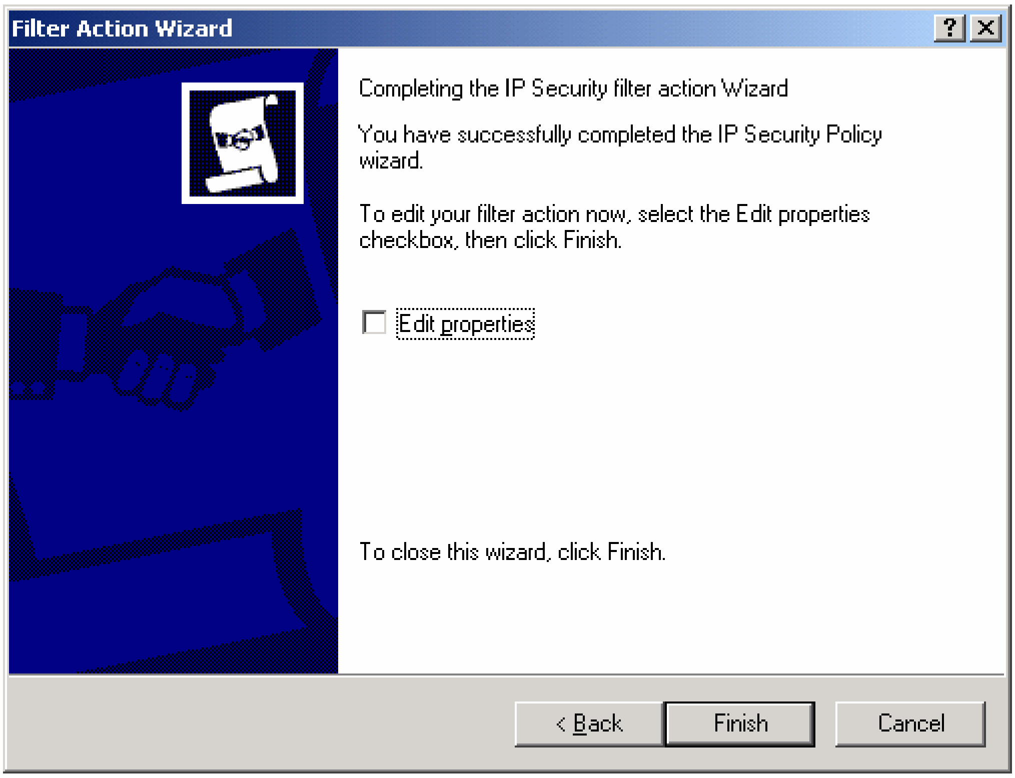
Specify the settings for this custom security method.

□ Data and address integrity without encryption (AH) :
Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):
Integrity algorithm: MD5
Encryption algorithm: DES

Session Key Settings:
□ Generate a new key every: 100000 Kbytes
□ Generate a new key every 3600 seconds

- For finishing Filter Action configuration, click on « **Finish** ».



Filter Action Wizard

Completing the IP Security filter action Wizard

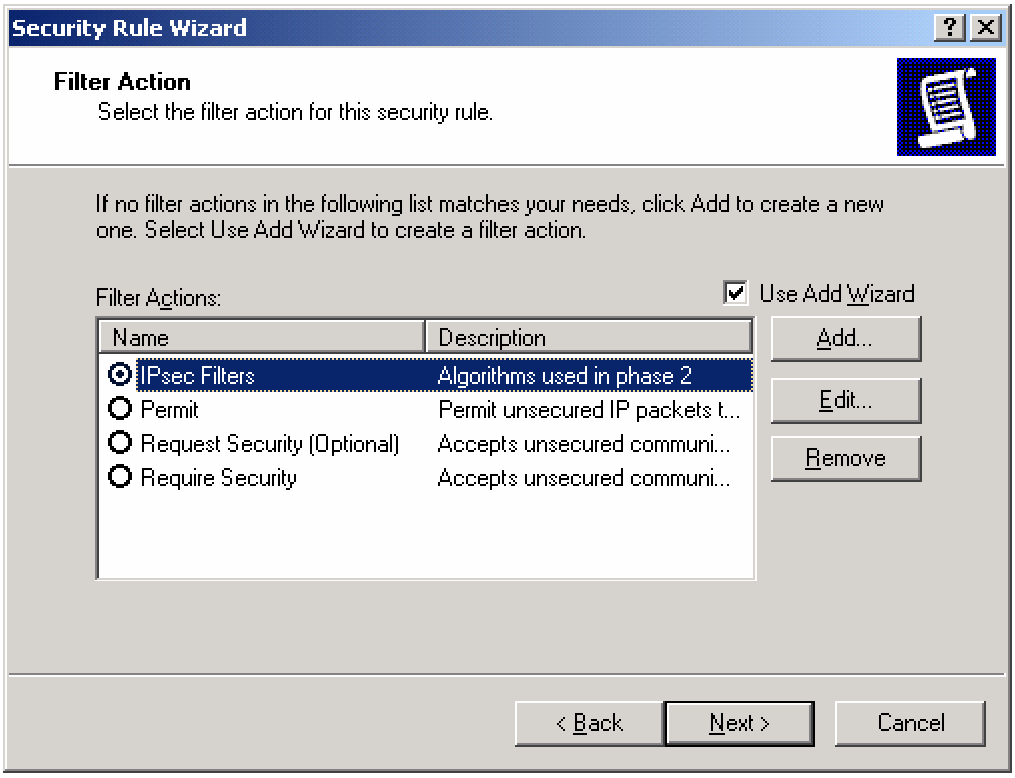
You have successfully completed the IP Security Policy wizard.

To edit your filter action now, select the Edit properties checkbox, then click Finish.

☐ Edit properties

To close this wizard, click Finish.

- The new IP filter action is shown in the list. Click on « **Next** ».



Security Rule Wizard

Filter Action
Select the filter action for this security rule.

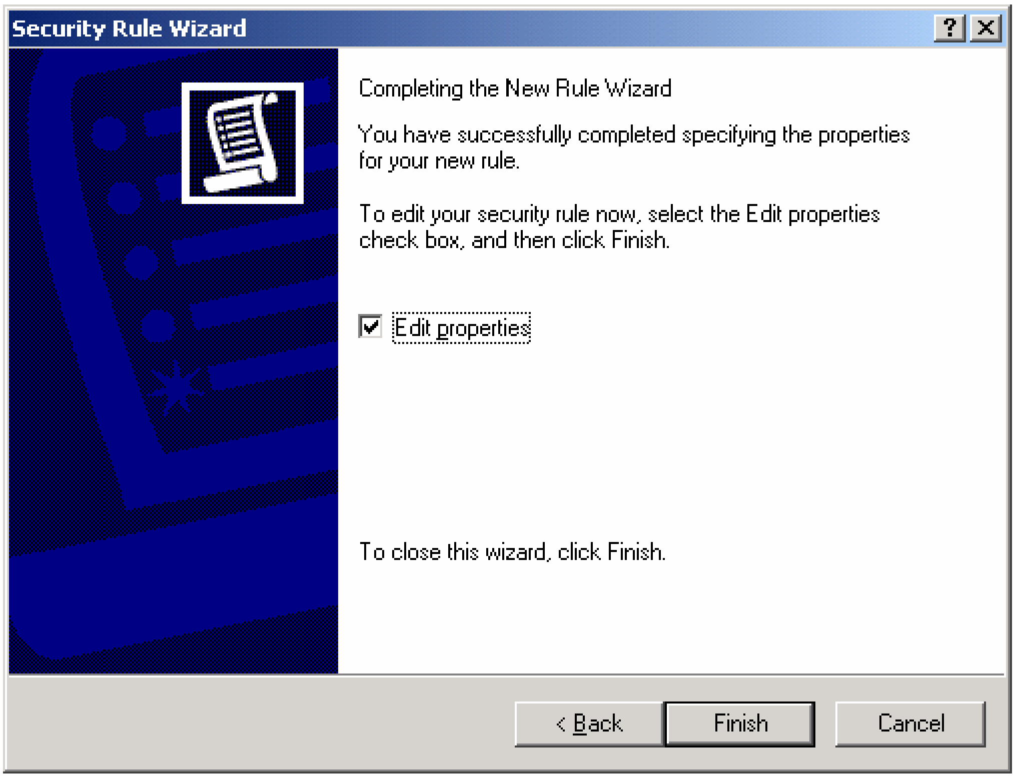
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

Filter Actions:

☑ Use Add Wizard

	Name	Description
●	IPsec Filters	Algorithms used in phase 2
○	Permit	Permit unsecured IP packets t...
○	Request Security (Optional)	Accepts unsecured communi...
○	Require Security	Accepts unsecured communi...

- Click on « Finish ».



Completing the New Rule Wizard

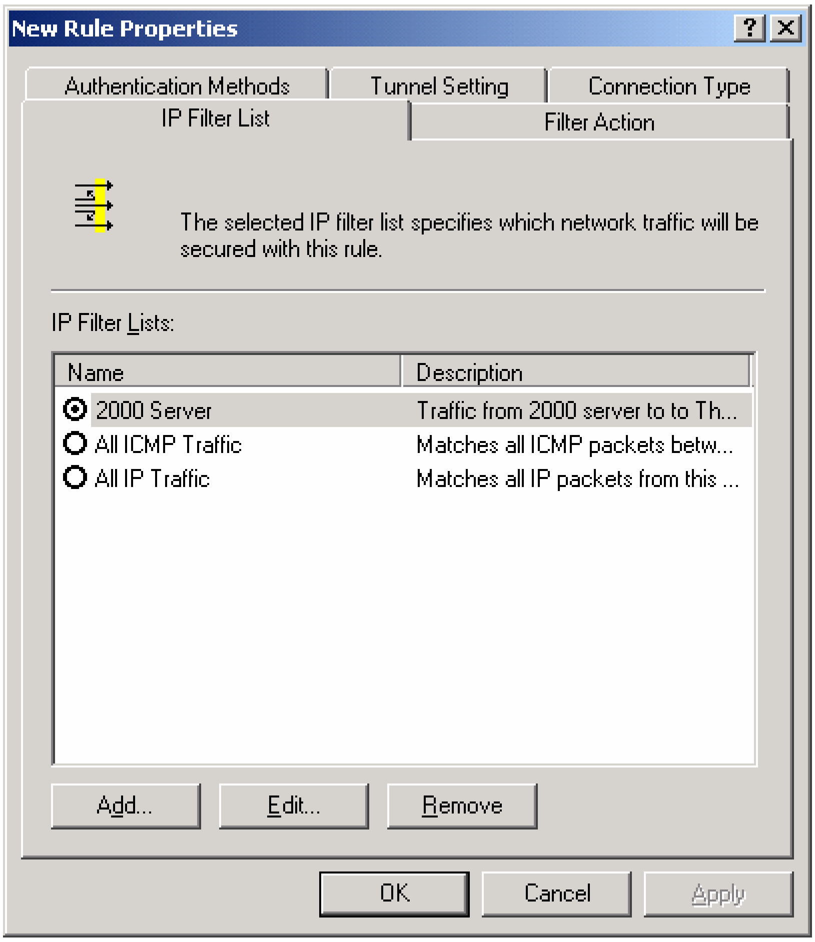
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

- IP filter we have just created is shown in IP filter list. Click on « OK ».

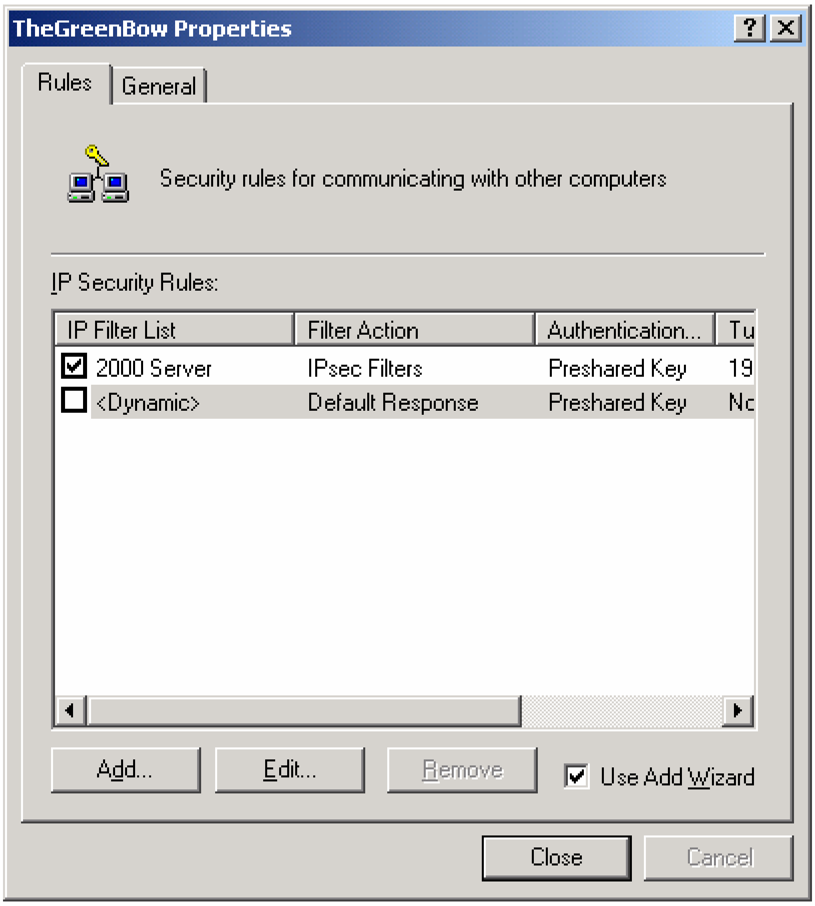


The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
● 2000 Server	Traffic from 2000 server to to Th...
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

- We must create another Security Rule that deals with communication from TheGreenBow VPN client to Microsoft Windows 2000 Server. Click on « Add »



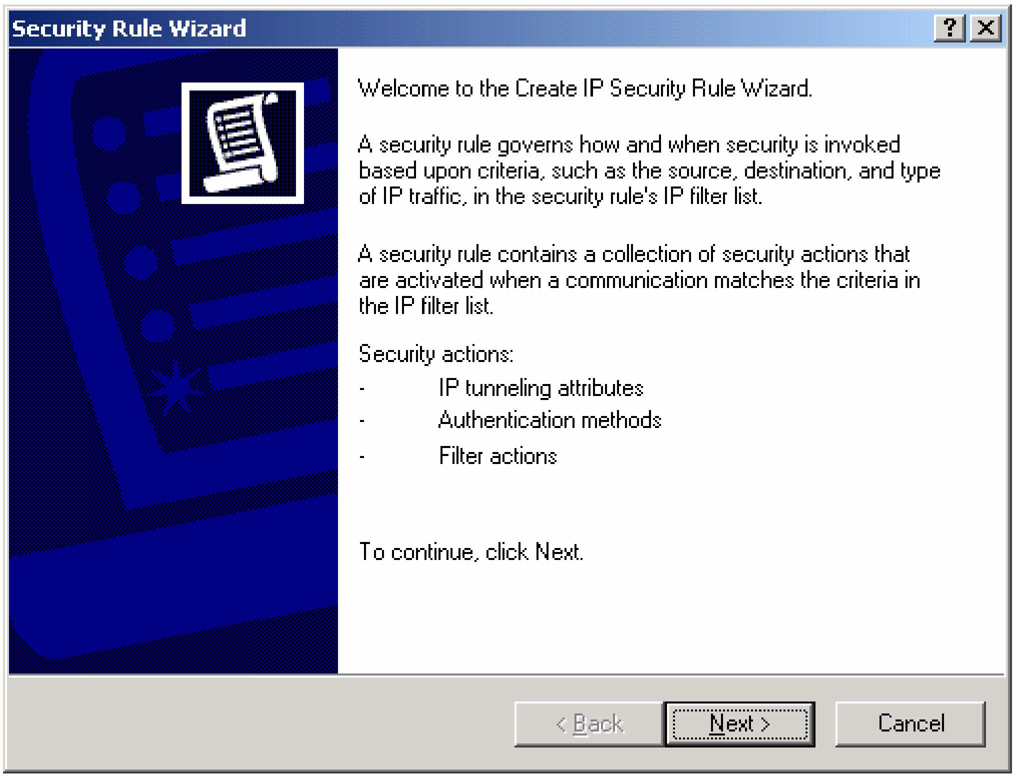
Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ 2000 Server	IPsec Filters	Preshared Key	19
□ <Dynamic>	Default Response	Preshared Key	Nc

☑ Use Add Wizard

- Click on « Next ».



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.

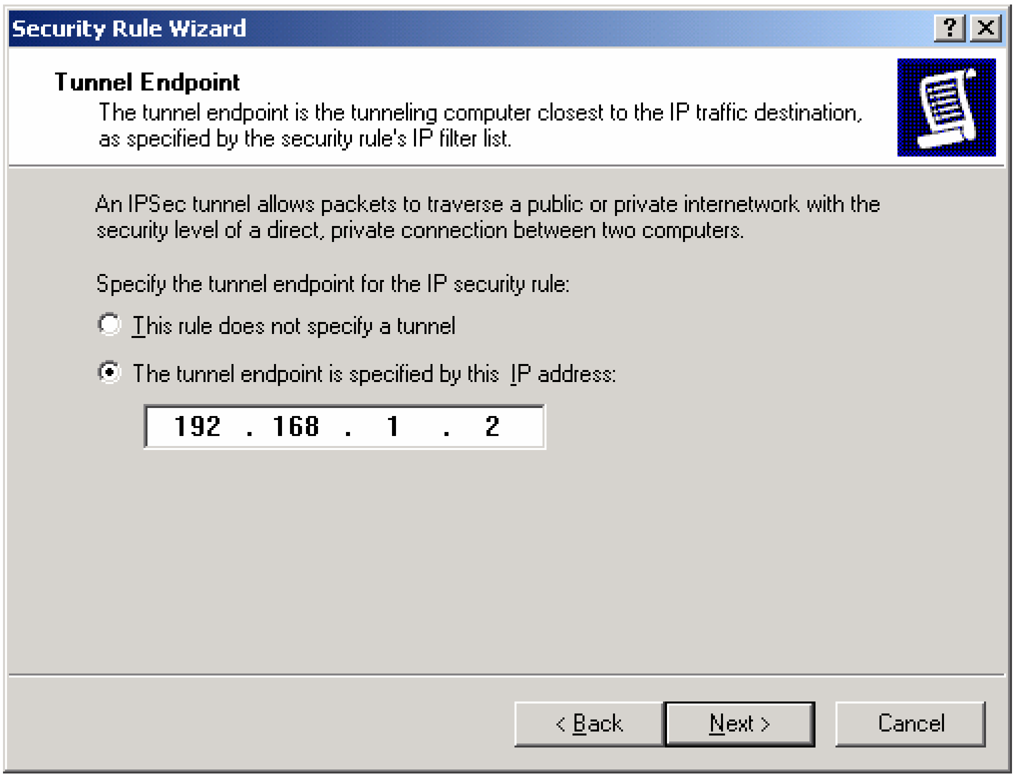
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

- Give IP address of VPN tunnel final endpoint (here Microsoft Windows 2000 Server) then click on « Next ».



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.

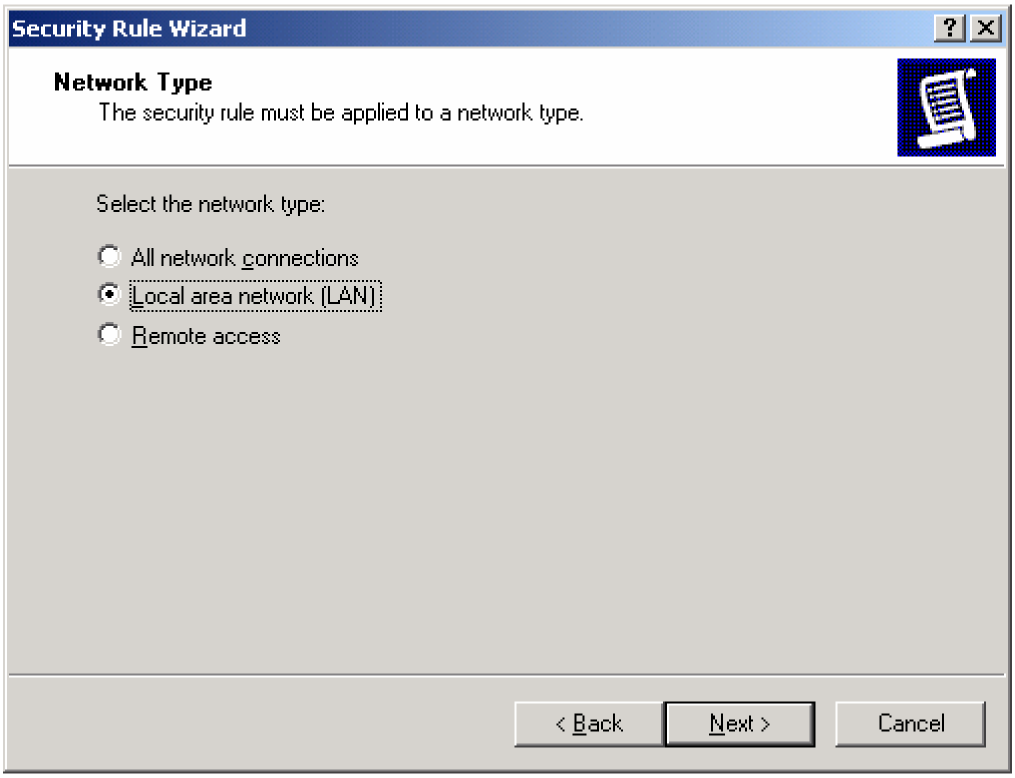
Specify the tunnel endpoint for the IP security rule:

○ This rule does not specify a tunnel

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 2

- In our example, the computers belong to the same local area network. Click on « Local area network » then on « Next ».



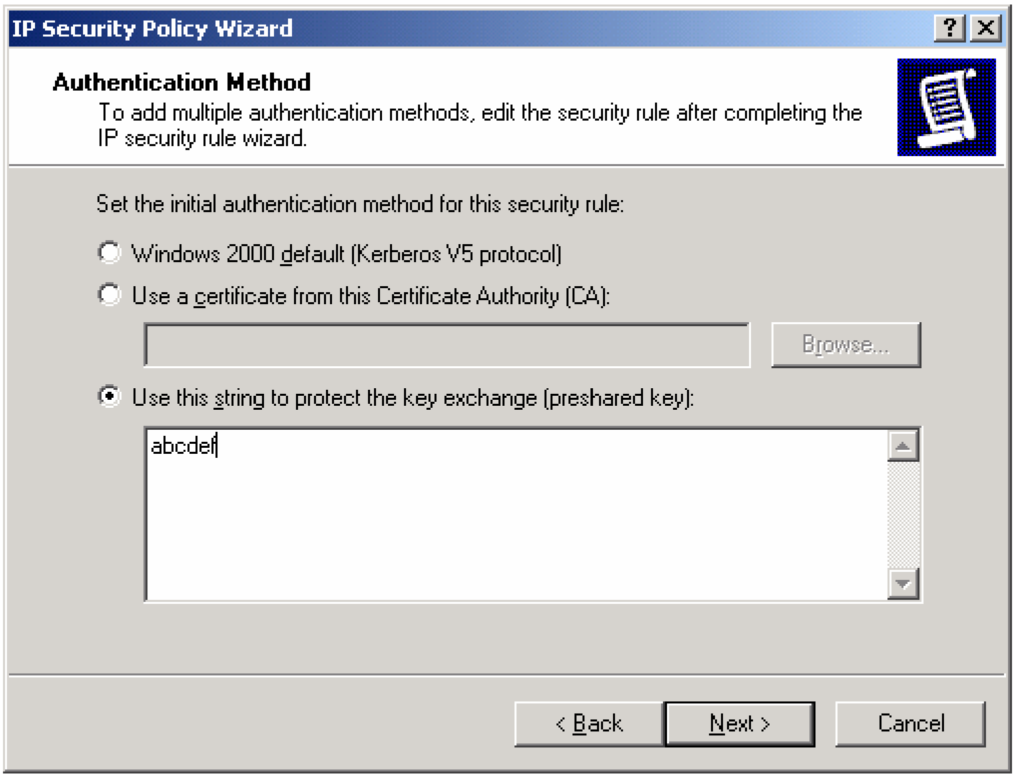
Security Rule Wizard

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

- Traffic between the VPN client and the server is protected by a preshared key. Click on « Use this string to protect the key exchange (preshared key) » and fill the form with the preshared key. Click on « Next ».



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:

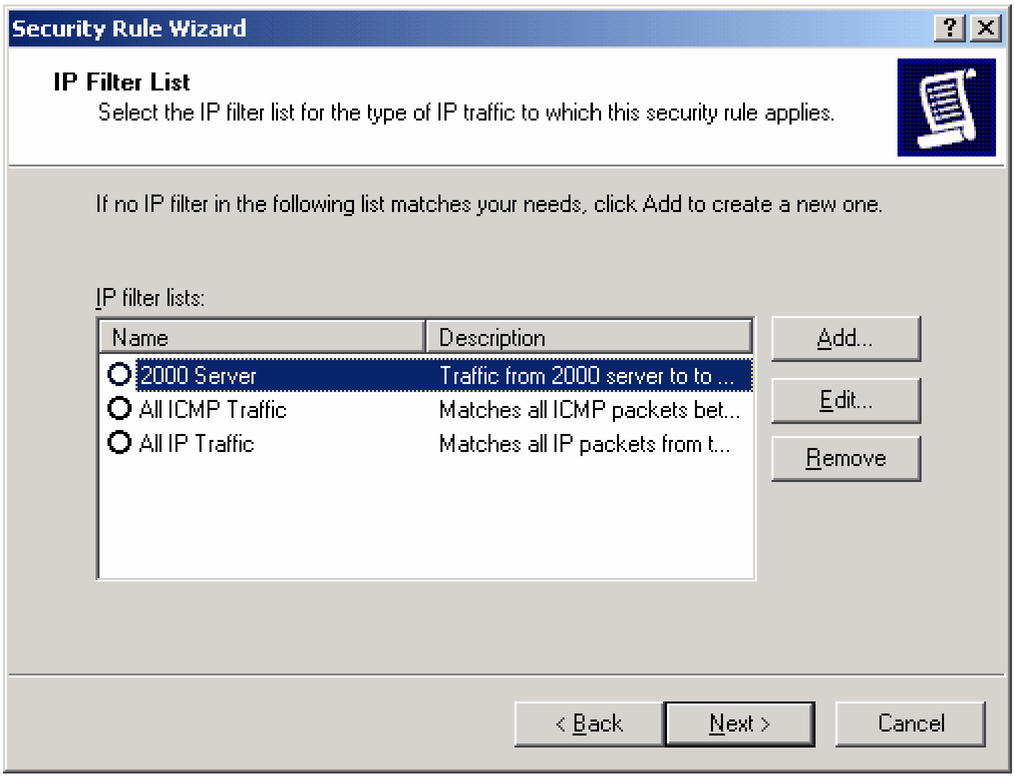
○ Windows 2000 default (Kerberos V5 protocol)

○ Use a certificate from this Certificate Authority (CA):

● Use this string to protect the key exchange (preshared key):

abcdef

- Click on « Add » in order to insert a specific IP filter to our new security rule.



Security Rule Wizard

IP Filter List

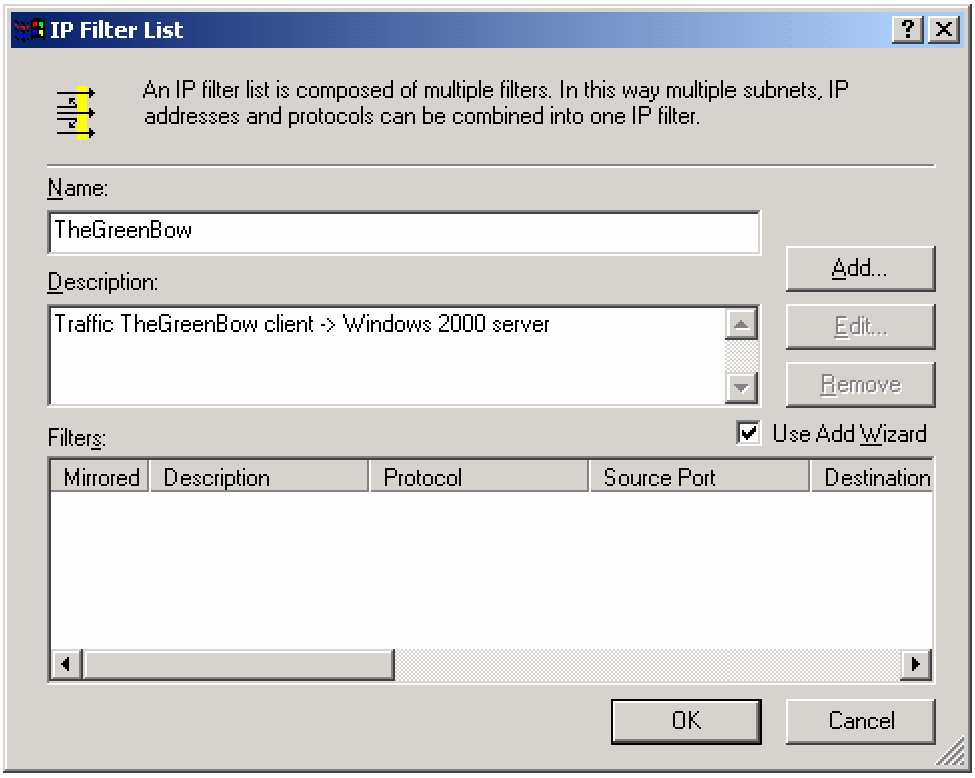
Select the IP filter list for the type of IP traffic to which this security rule applies.

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

IP filter lists:

Name	Description
○ 2000 Server	Traffic from 2000 server to to ...
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...

- Give a name to the new IP filter then click on « Add ».



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: TheGreenBow

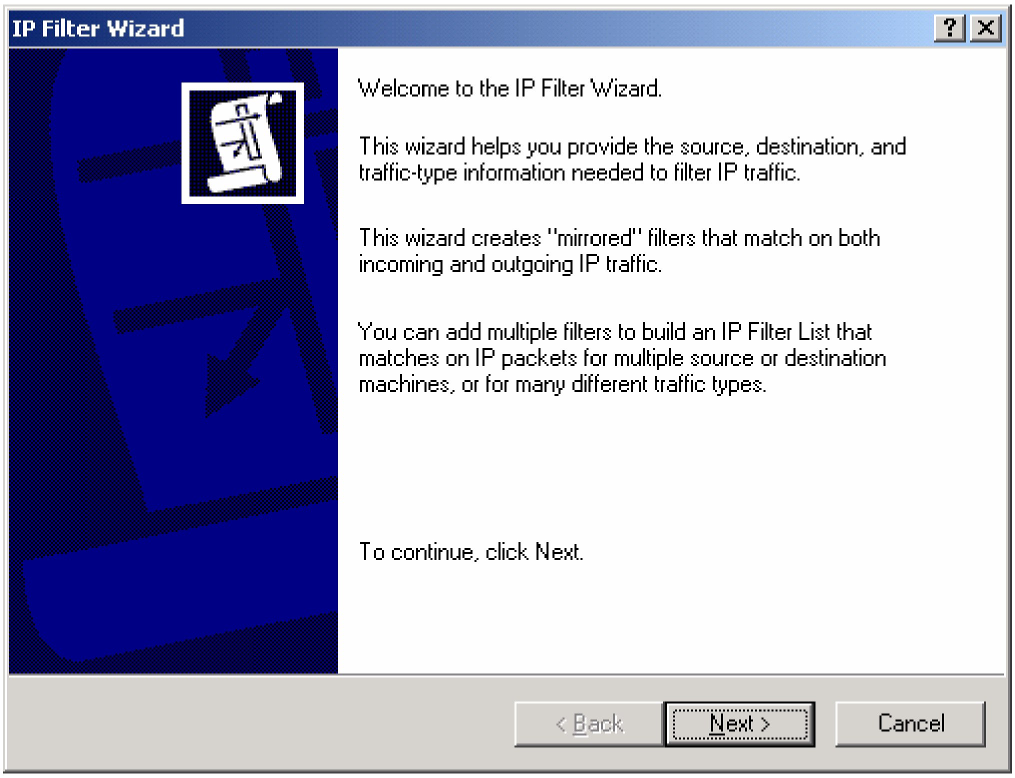
Description: Traffic TheGreenBow client -> Windows 2000 server

Filters:

☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

- Click on « Next ».



Welcome to the IP Filter Wizard.

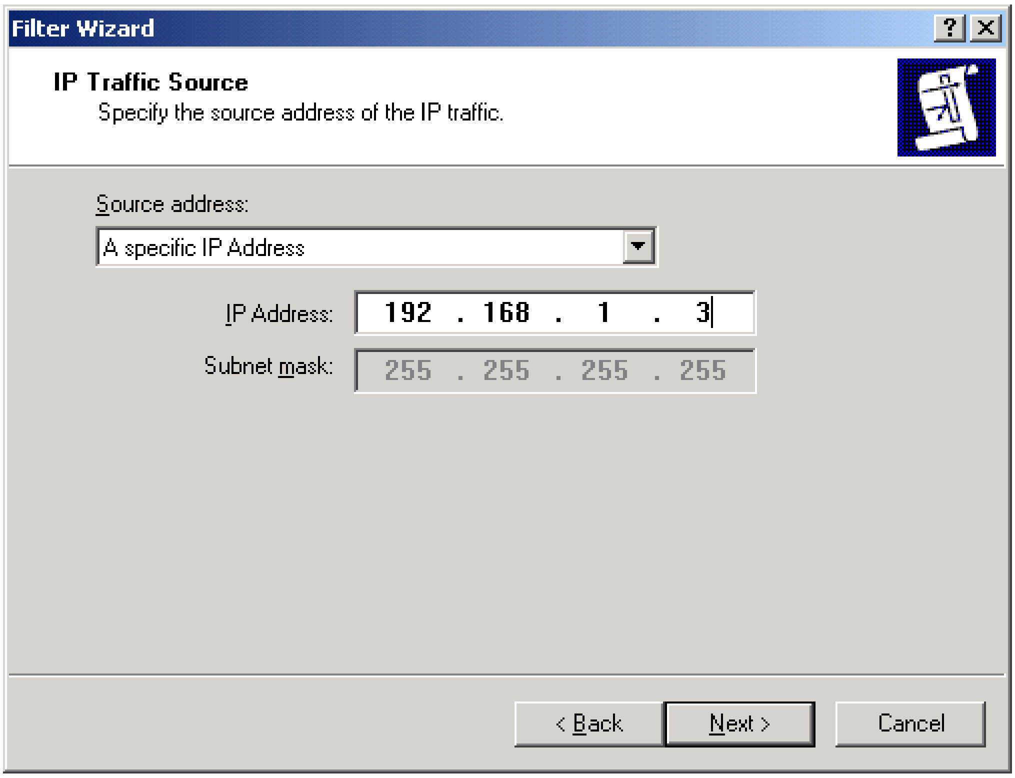
This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

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.

- Select « **A specific IP address** » and give TheGreenBow client IP address. Then click on « **Next** ».



Filter Wizard

IP Traffic Source

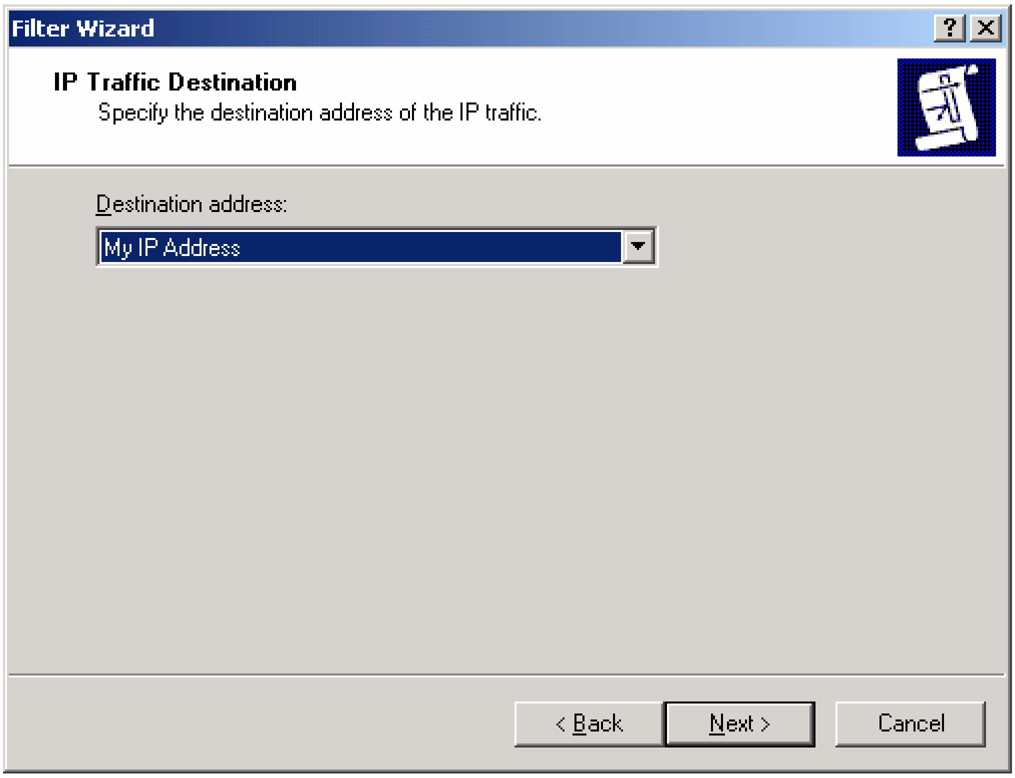
Specify the source address of the IP traffic.

Source address: A specific IP Address

IP Address: 192 . 168 . 1 . 3

Subnet mask: 255 . 255 . 255 . 255

- Select « **My IP address** » as remote destination address, then click on « **Next** ».



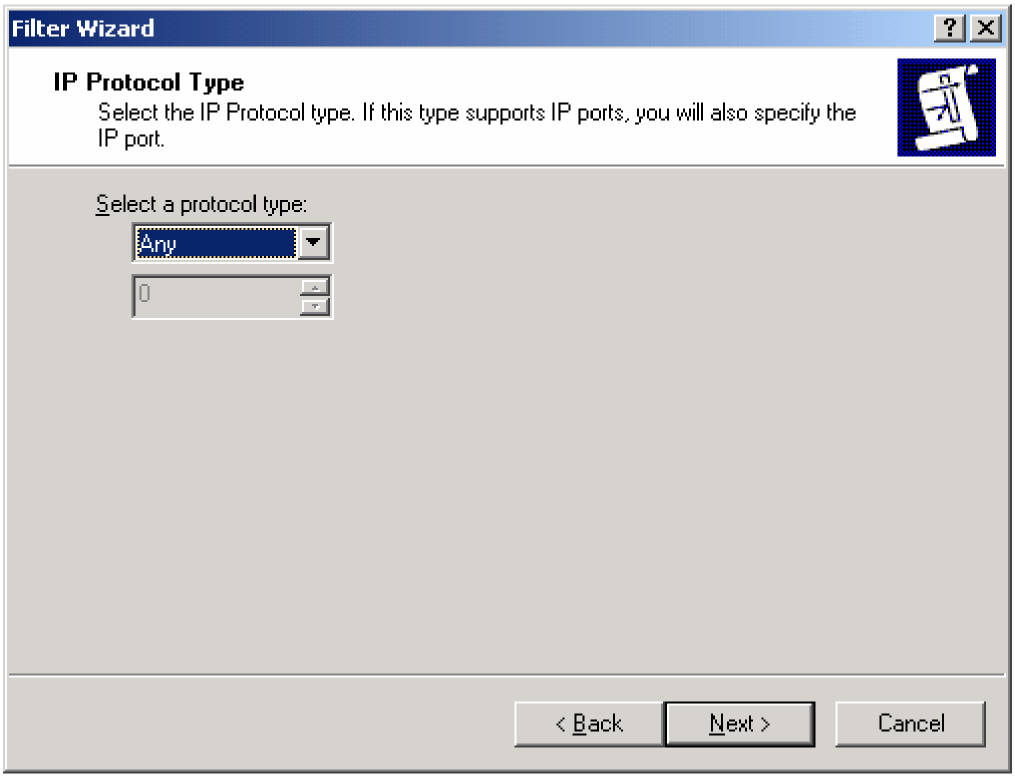
Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

Destination address: My IP Address

- Set protocol type then click on « Next ».



Filter Wizard

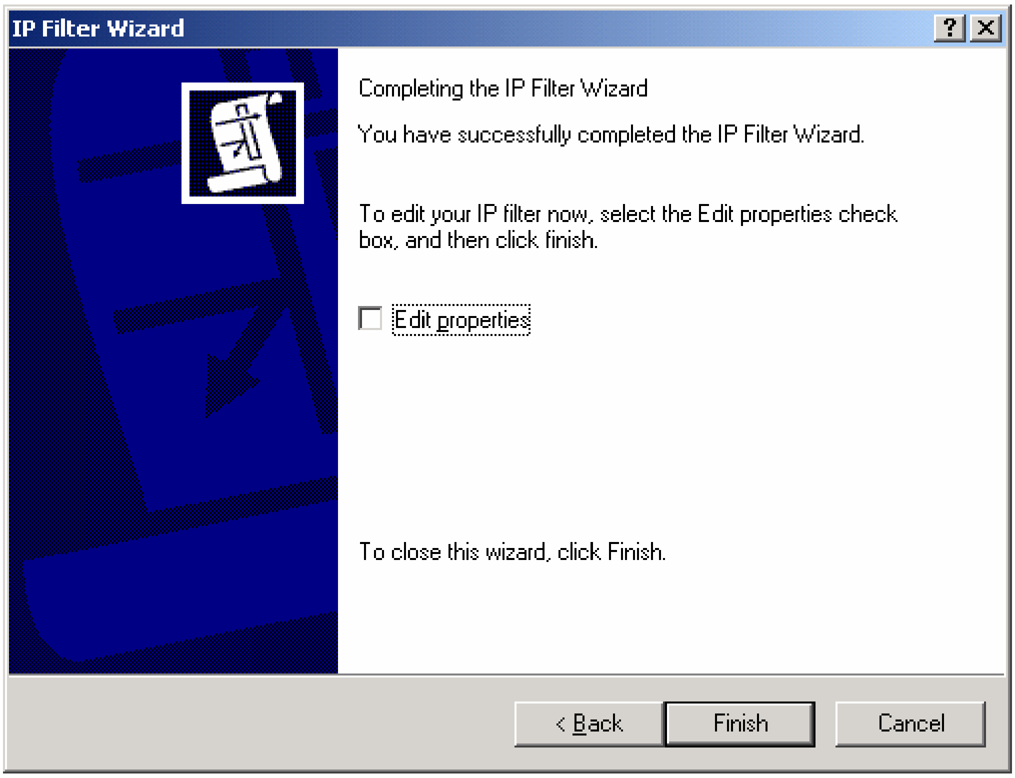
IP Protocol Type

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

Select a protocol type: Any

0

- Click on « Finish »



IP Filter Wizard

Completing the IP Filter Wizard

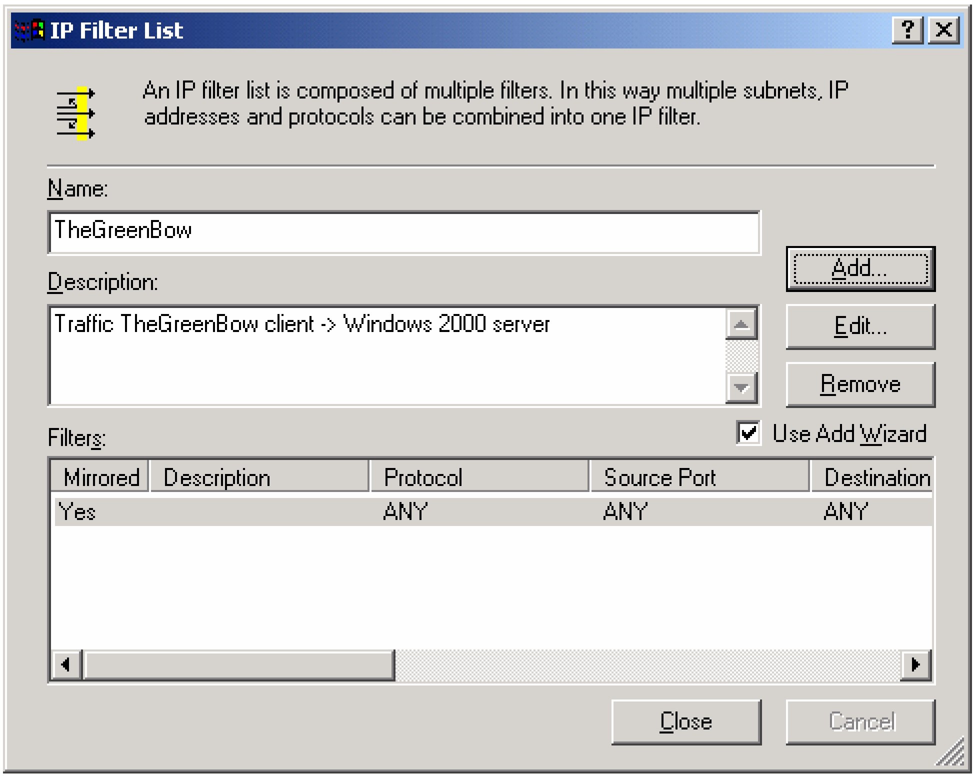
You have successfully completed the IP Filter Wizard.

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

☐ Edit properties

To close this wizard, click Finish.

- Click on « **Close** ».



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.

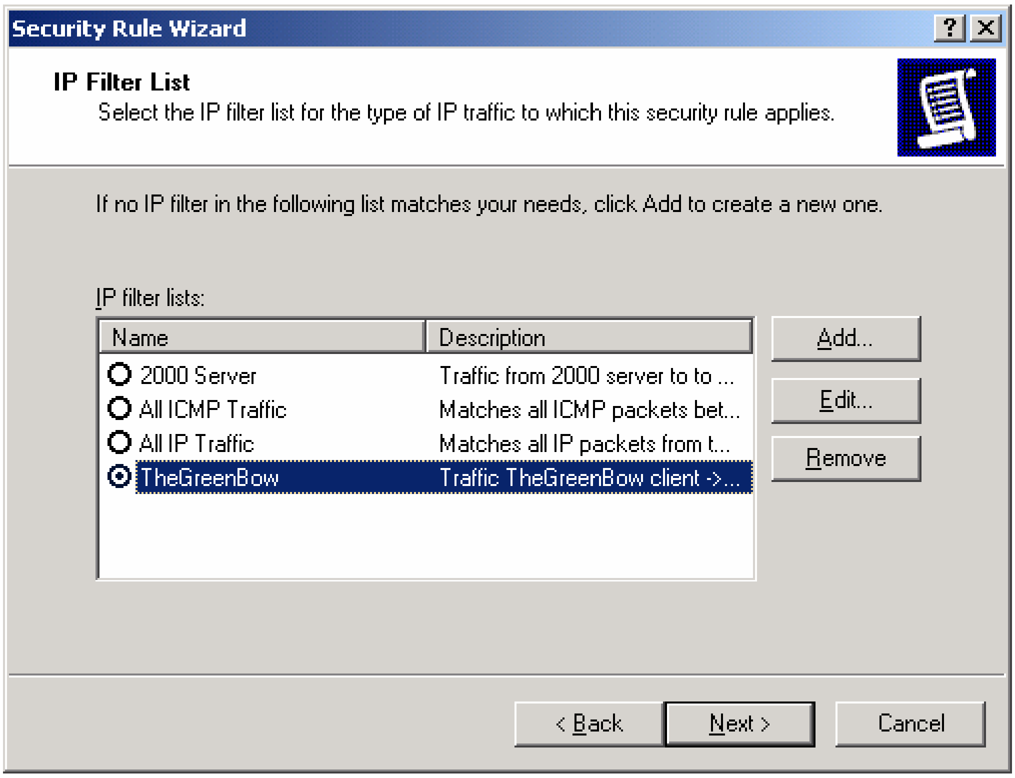
Name: TheGreenBow

Description: Traffic TheGreenBow client -> Windows 2000 server

Filters: ☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

- Select IP filter « **TheGreenBow** » then click on « **Next** ».



Security Rule Wizard

IP Filter List

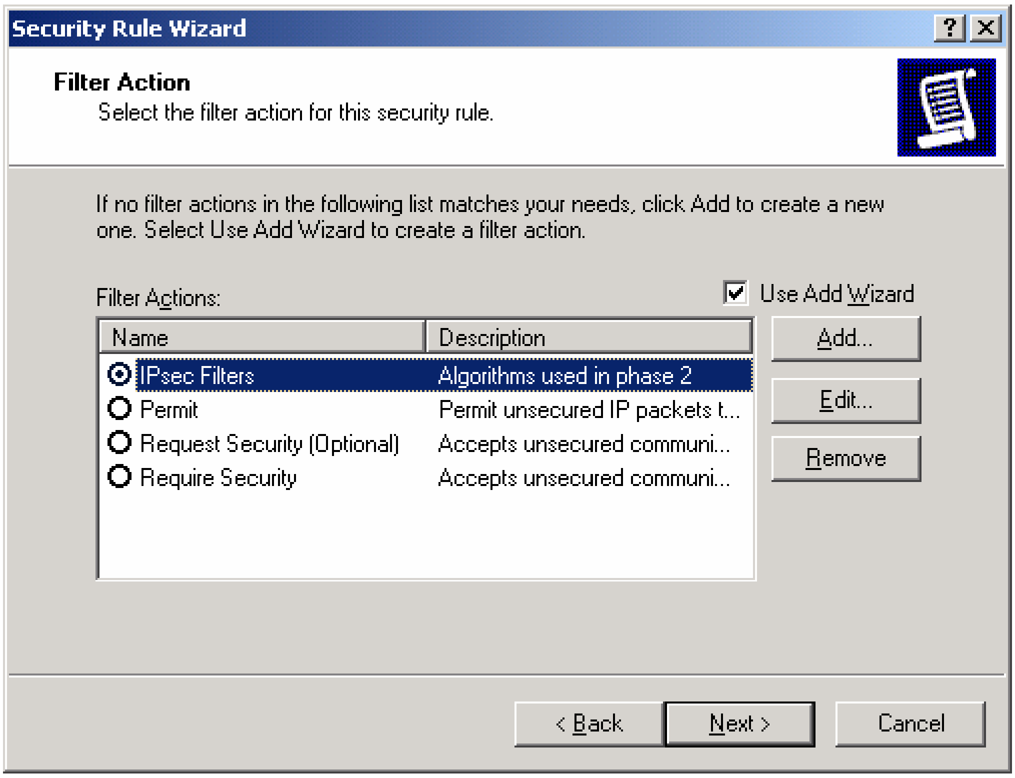
Select the IP filter list for the type of IP traffic to which this security rule applies.

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

IP filter lists:

Name	Description
○ 2000 Server	Traffic from 2000 server to to ...
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
● TheGreenBow	Traffic TheGreenBow client ->...

- Select filter action « IpSec Filters » then click on « Next ».



Security Rule Wizard

Filter Action

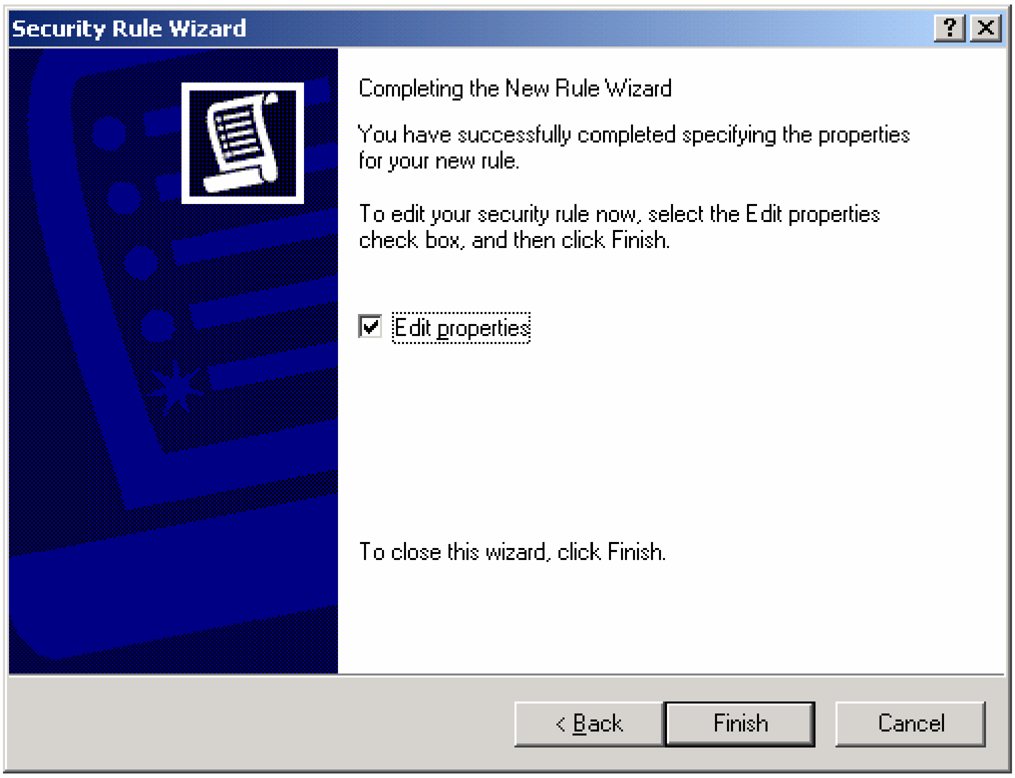
Select the filter action for this security rule.

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
● IPsec Filters	Algorithms used in phase 2
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...

- Click on « Finish ».



Security Rule Wizard

Completing the New Rule Wizard

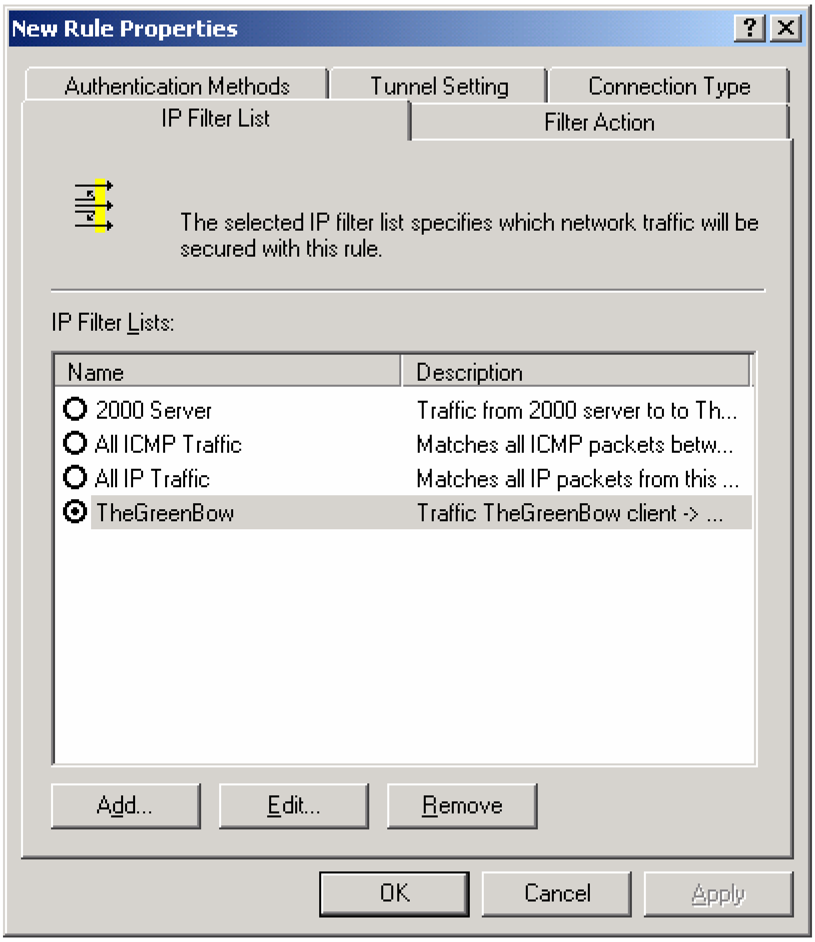
You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

- Select « TheGreenBow » in the IP Filter lists then click on « OK ».

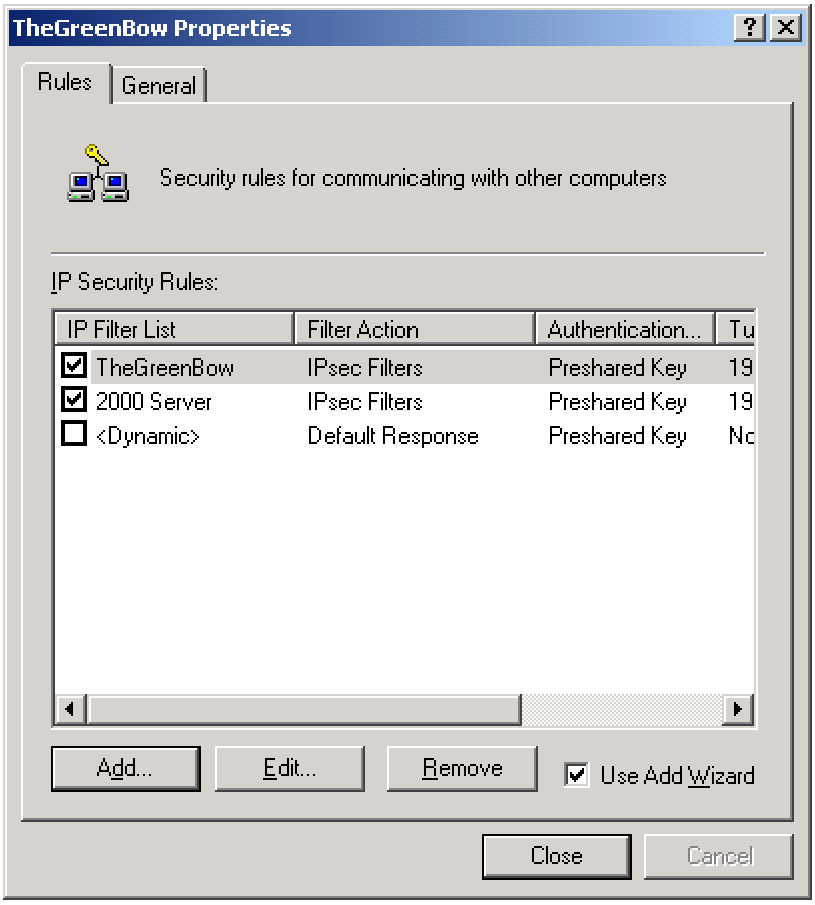


The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ 2000 Server	Traffic from 2000 server to to Th...
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● TheGreenBow	Traffic TheGreenBow client -> ...

- Click on « **Close** ».



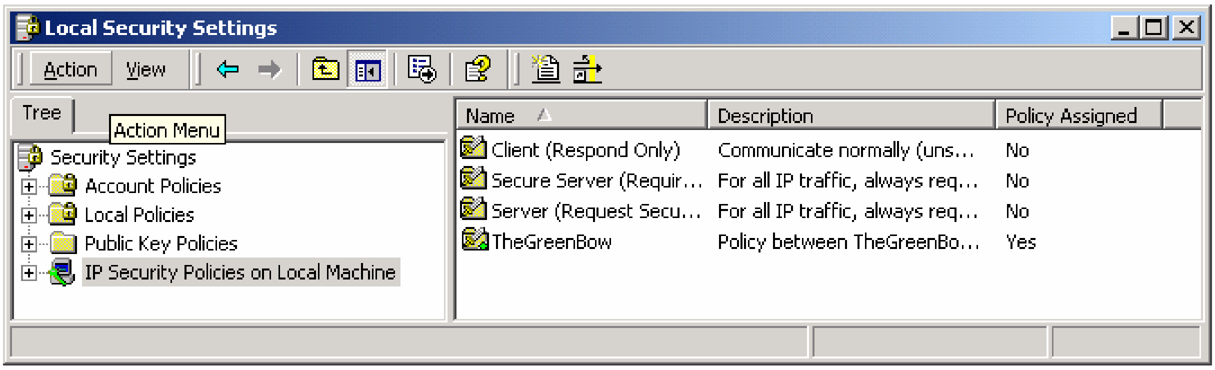
TheGreenBow Properties

Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ TheGreenBow	IPsec Filters	Preshared Key	19
☑ 2000 Server	IPsec Filters	Preshared Key	19
□ <Dynamic>	Default Response	Preshared Key	Nc

- For activating the new Security policy, right-click « **TheGreenBow** » policy, and left-click on « **Assign** ». A green point is shown on icon « **TheGreenBow** ».



Local Security Settings

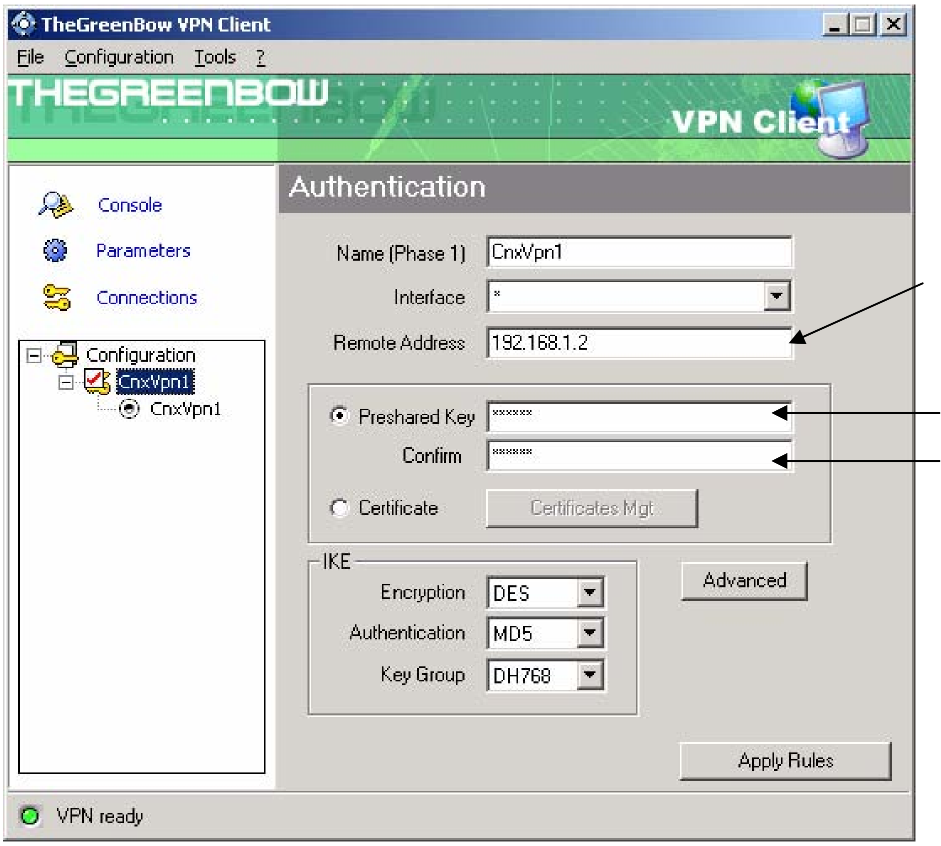
Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
TheGreenBow	Policy between TheGreenBo...	Yes

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

In « **Interface** » field, you can select a star (« ***** ») if the VPN Client gets a dynamic IP address.

In « **Remote address** », set remote server IP address.



Name (Phase 1): CnxVpn1

Interface: *

Remote Address: 192.168.1.2

● Preshared Key: ******

Confirm: ******

○ Certificate

IKE

Encryption: DES

Authentication: MD5

Key Group: DH768

Remote VPN gateway address can be an IP address or a DNS address.

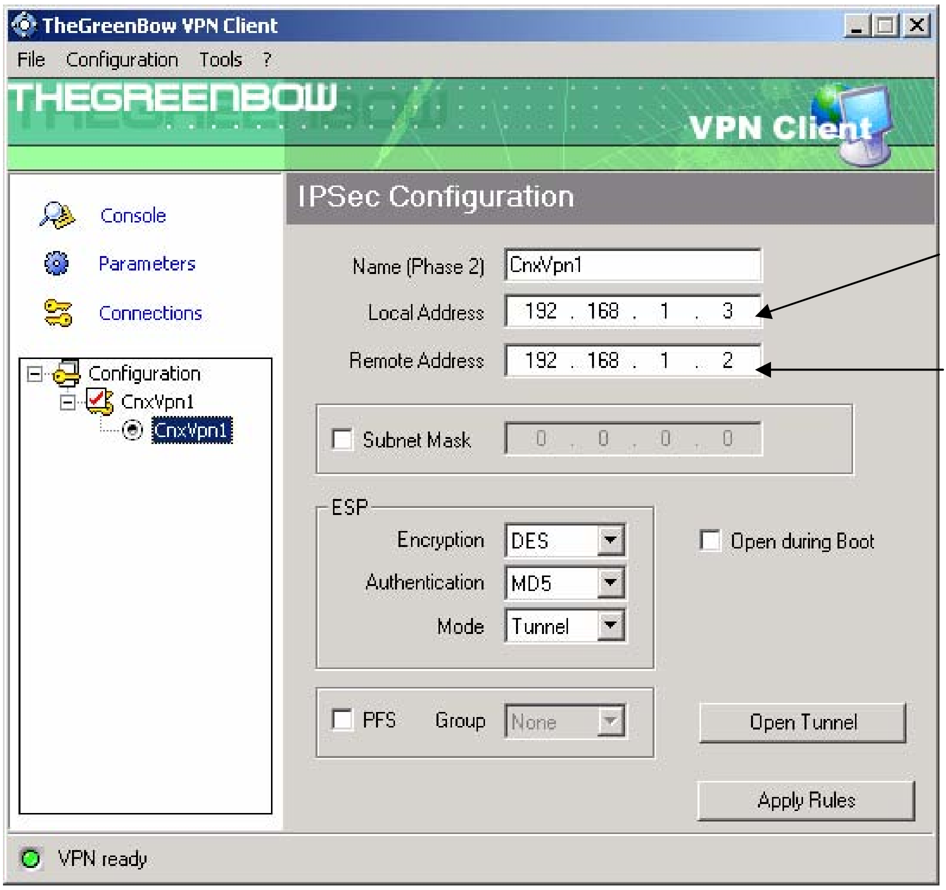
abcdef

abcdef

Configuration Phase 1

3.2 VPN Client Phase 2 (IPSec) Configuration

In this window, you set up IPSec VPN configuration.
« **Local adress** » field is virtual IP address of the client inside remote network.



Name (Phase 2): CnxVpn1
Local Address: 192 . 168 . 1 . 3
Remote Address: 192 . 168 . 1 . 2
☐ Subnet Mask: 0 . 0 . 0 . 0
ESP
Encryption: DES
Authentication: MD5
Mode: Tunnel
☐ Open during Boot
☐ PFS Group: None

You must define a virtual static IP address here.

Remote private IP address of the server.

Configuration Phase 2

3.3 Open IPSec VPN tunnels

Once both Windows Server and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.
1. Click on "**Save & Apply**" to take into account all modifications we've made on your VPN Client configuration
2. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)
3. Select "**Connections**" to see opened VPN Tunnels
4. Select "**Console**" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging.

4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

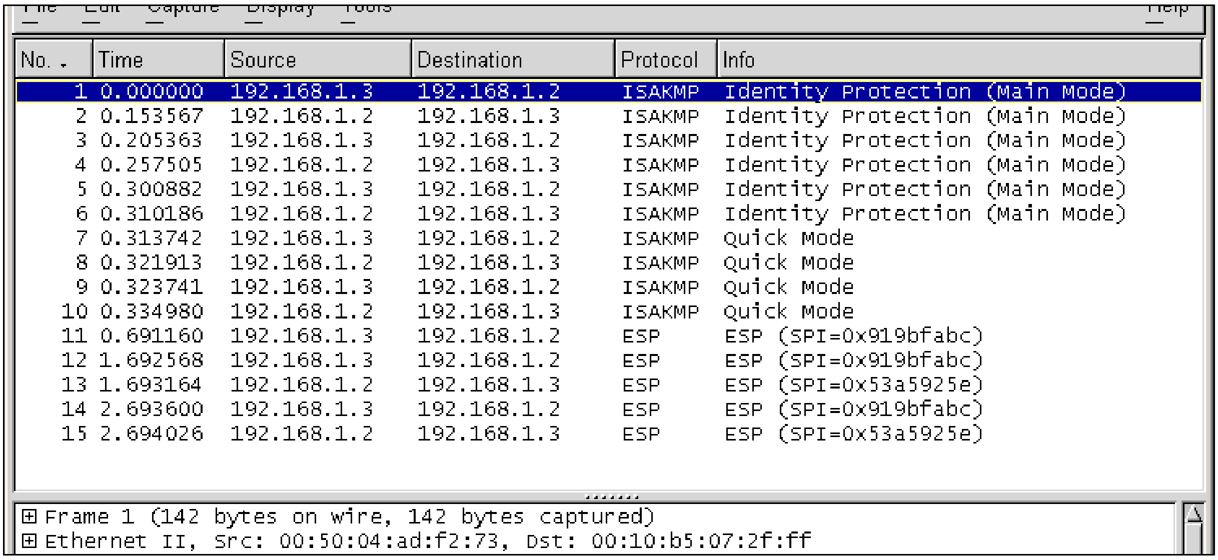
Concerning Microsoft Windows 2000 Server, read in case of trouble document Q257225 in Microsoft Knowledge base :

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q257225

4.1 A good network analyser : ethereal

Ethereal is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tools is available on website http://www.ethereal.com/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

The following example shows a successful connection between TheGreenBow VPN client and a Microsoft Windows 2000 Server.



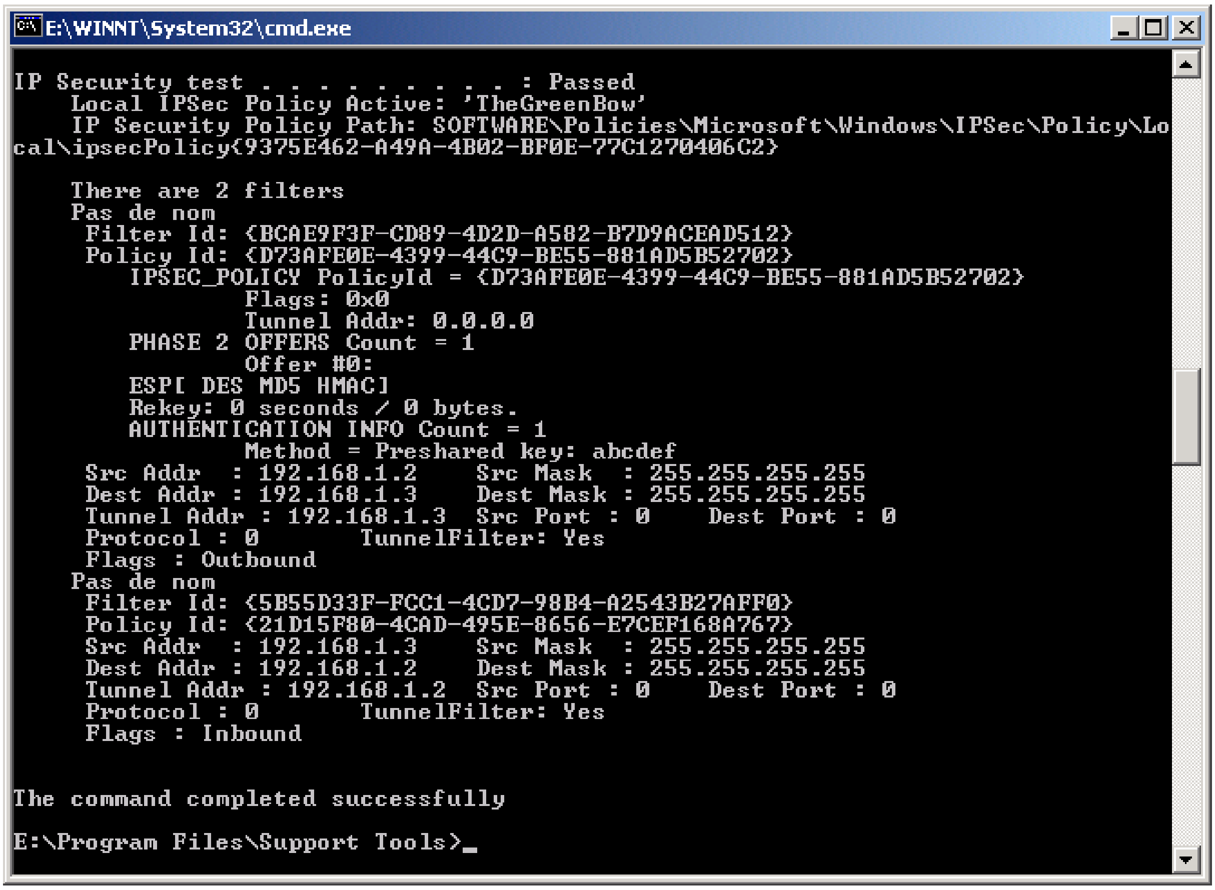
```
No. .  Time      Source        Destination   Protocol  Info
    1 0.000000  192.168.1.3   192.168.1.2   ISAKMP    Identity Protection (Main Mode)
    2 0.153567  192.168.1.2   192.168.1.3   ISAKMP    Identity Protection (Main Mode)
    3 0.205363  192.168.1.3   192.168.1.2   ISAKMP    Identity Protection (Main Mode)
    4 0.257505  192.168.1.2   192.168.1.3   ISAKMP    Identity Protection (Main Mode)
    5 0.300882  192.168.1.3   192.168.1.2   ISAKMP    Identity Protection (Main Mode)
    6 0.310186  192.168.1.2   192.168.1.3   ISAKMP    Identity Protection (Main Mode)
    7 0.313742  192.168.1.3   192.168.1.2   ISAKMP    Quick Mode
    8 0.321913  192.168.1.2   192.168.1.3   ISAKMP    Quick Mode
    9 0.323741  192.168.1.3   192.168.1.2   ISAKMP    Quick Mode
   10 0.334980  192.168.1.2   192.168.1.3   ISAKMP    Quick Mode
   11 0.691160  192.168.1.3   192.168.1.2   ESP       ESP (SPI=0x919bfabc)
   12 1.692568  192.168.1.3   192.168.1.2   ESP       ESP (SPI=0x919bfabc)
   13 1.693164  192.168.1.2   192.168.1.3   ESP       ESP (SPI=0x53a5925e)
   14 2.693600  192.168.1.3   192.168.1.2   ESP       ESP (SPI=0x919bfabc)
   15 2.694026  192.168.1.2   192.168.1.3   ESP       ESP (SPI=0x53a5925e)

⊞ Frame 1 (142 bytes on wire, 142 bytes captured)
⊞ Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff
```

4.2 Netdiag.exe

Netdiag.exe can be find in Microsoft Windows 2000 Server Support Tools. Read Knowledge base article Q257225 for more details.

In a window CMD.EXE, type “select netdiag /test :ipsec /debug”. Output will be :



```
IP Security test . . . . . . . . . : Passed
    Local IPSec Policy Active: 'TheGreenBow'
    IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Lo
cal\ipsecPolicy{9375E462-A49A-4B02-BF0E-77C1270406C2}

    There are 2 filters
    Pas de nom
     Filter Id: {BCAE9F3F-CD89-4D2D-A582-B7D9ACEAD512}
     Policy Id: {D73AFE0E-4399-44C9-BE55-881AD5B52702}
        IPSEC_POLICY PolicyId = {D73AFE0E-4399-44C9-BE55-881AD5B52702}
                Flags: 0x0
                Tunnel Addr: 0.0.0.0
        PHASE 2 OFFERS Count = 1
                Offer #0:
        ESP[ DES MD5 HMAC]
        Rekey: 0 seconds / 0 bytes.
        AUTHENTICATION INFO Count = 1
                Method = Preshared key: abcdef
     Src Addr  : 192.168.1.2    Src Mask  : 255.255.255.255
     Dest Addr : 192.168.1.3    Dest Mask : 255.255.255.255
     Tunnel Addr : 192.168.1.3  Src Port : 0    Dest Port : 0
     Protocol : 0       TunnelFilter: Yes
     Flags : Outbound
    Pas de nom
     Filter Id: {5B55D33F-FCC1-4CD7-98B4-A2543B27AFF0}
     Policy Id: {21D15F80-4CAD-495E-8656-E7CEF168A767}
     Src Addr  : 192.168.1.3    Src Mask  : 255.255.255.255
     Dest Addr : 192.168.1.2    Dest Mask : 255.255.255.255
     Tunnel Addr : 192.168.1.2  Src Port : 0    Dest Port : 0
     Protocol : 0       TunnelFilter: Yes
     Flags : Inbound


The command completed successfully

E:\Program Files\Support Tools>_
```

5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

5.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.
Check « Phase 1 » algorithms if you have this:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.
Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

5.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

5.8 The VPN tunnel is up but I can’t ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.

6 Contacts

News and updates on TheGreenBow web site : http://www.thegreenbow.com
Technical support by email at support@thegreenbow.com
Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com