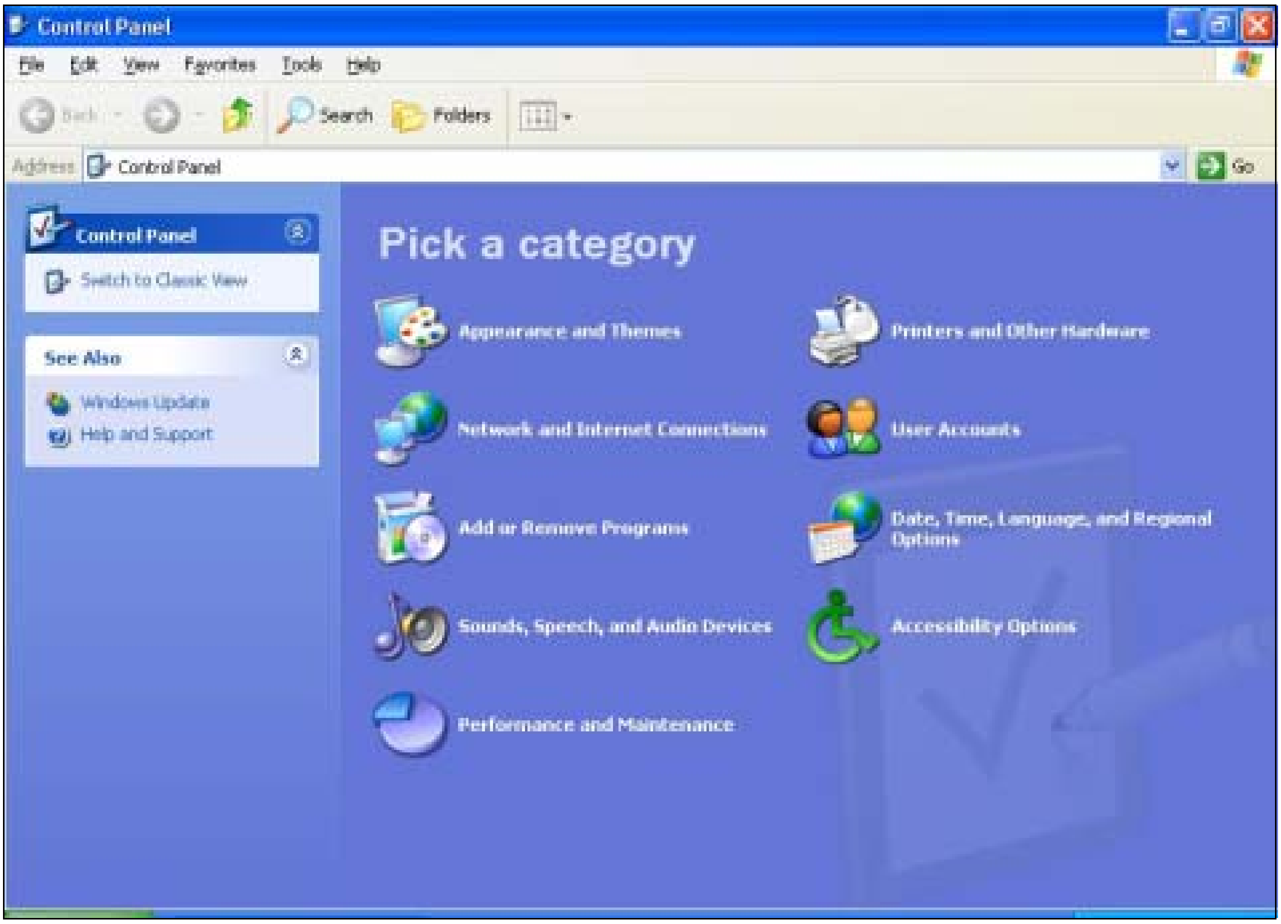
Charlie 20030401

Appendix B Win 2000/XP IPSEC Setting guide

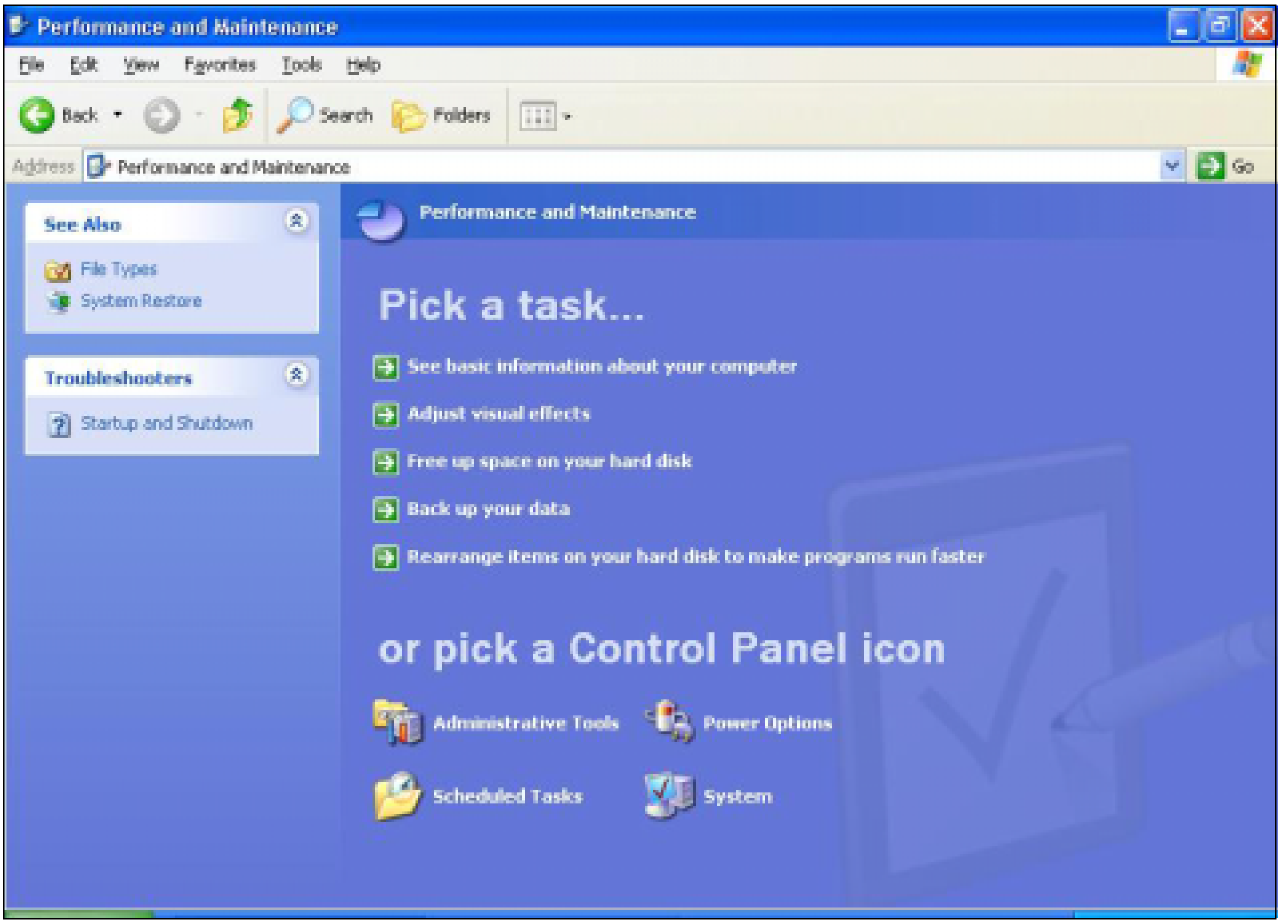
Example: Win XP/2000 →VPN Router
(Configuration on WIN 2000 is similar to XP)

1. On Win 2000/XP, click **[Start]** button, select **[Run]**, type **secpol.msc** in the field, then click **[Run]**→ Goto ****Local Security Policy Settings**** page

2. Or in Win XP, Click **[Control Pannel]**



Double-click **[Performance and Maintenance]**

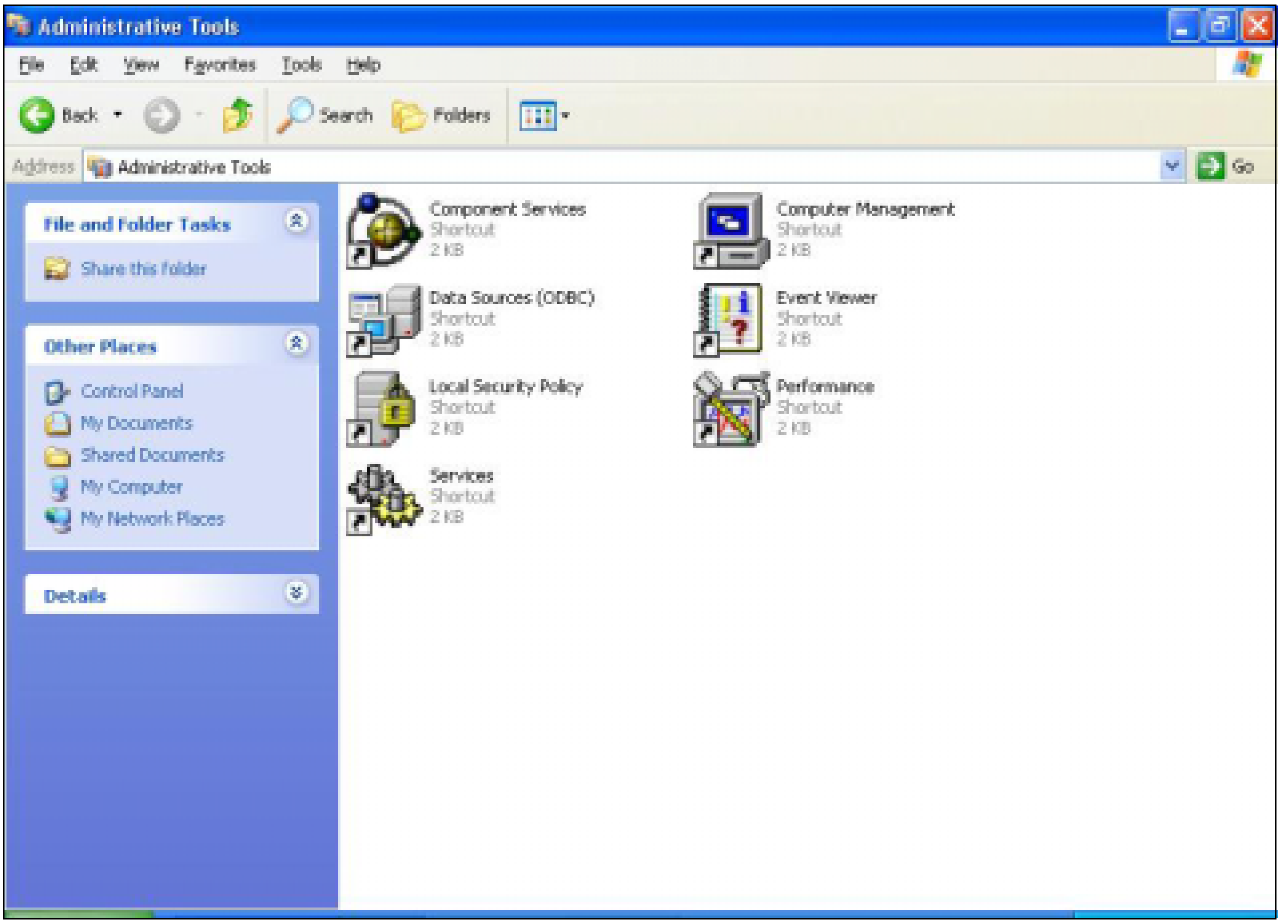


Pick a task...

- See basic information about your computer
- Adjust visual effects
- Free up space on your hard disk
- Back up your data
- Rearrange items on your hard disk to make programs run faster

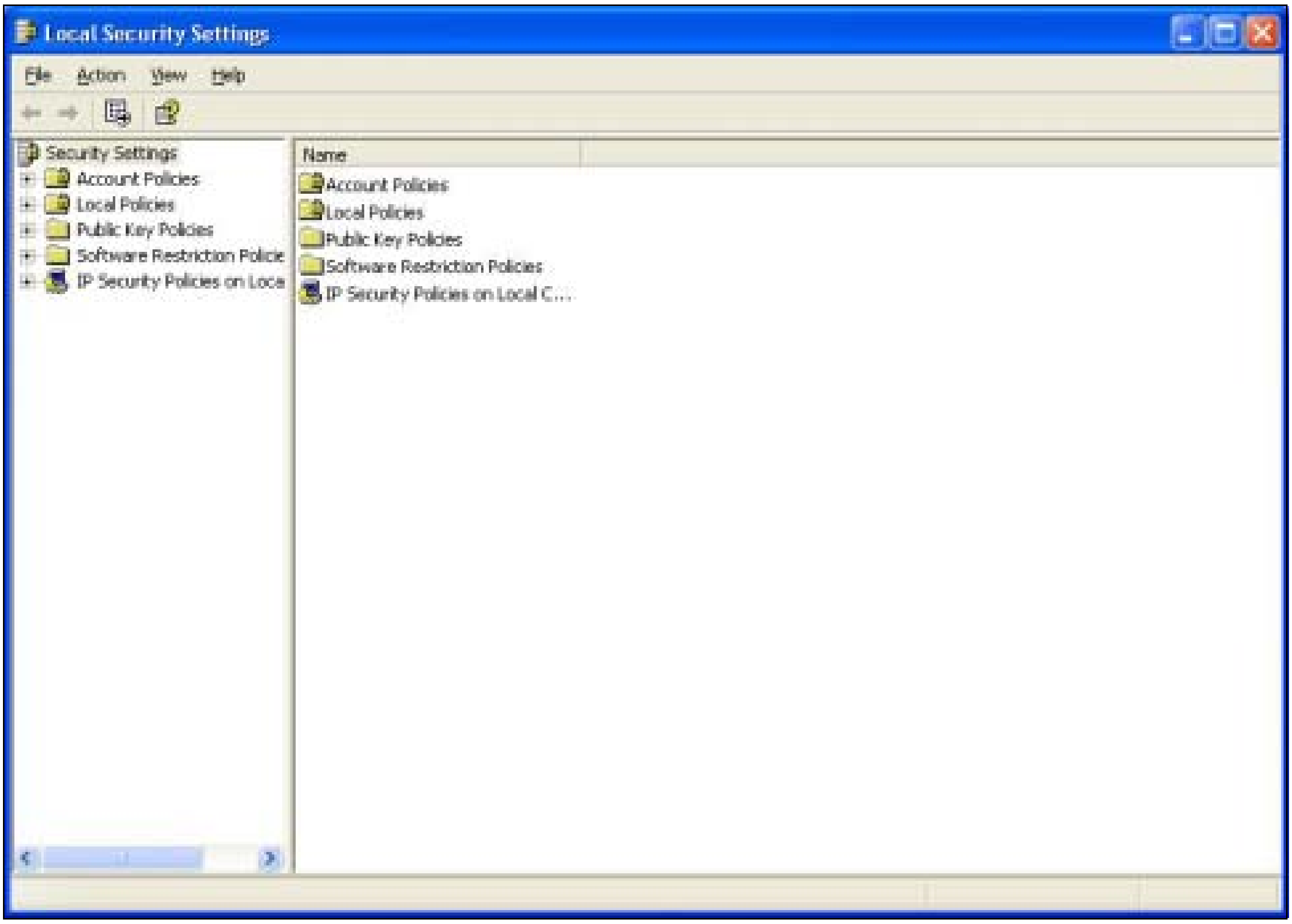
or pick a Control Panel icon

Double-click **[Administrative Tools]**



Local Security Policy Settings

Double-click **[Local Security Policy]**

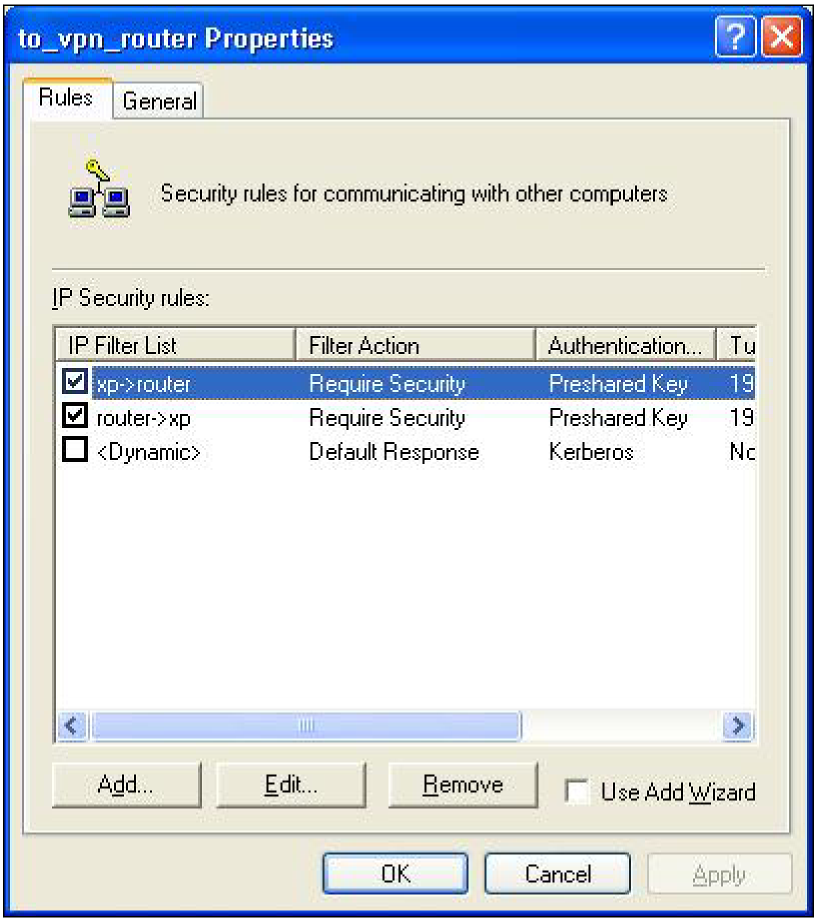


Right-click **[IP Security Policies on Local Computer]**, and click **[Create IP Security Policy]**.

Click the **[Next]** button, enter your policy’s name (Here it is **to_vpn_router**). Then, click **[Next]**.

Dis-select the **[Activate the default response rule]** check box, and click **[Next]** button.

Click **[Finish]** button, make sure **[Edit]** check box is checked.



Security rules for communicating with other computers

IP Security rules:

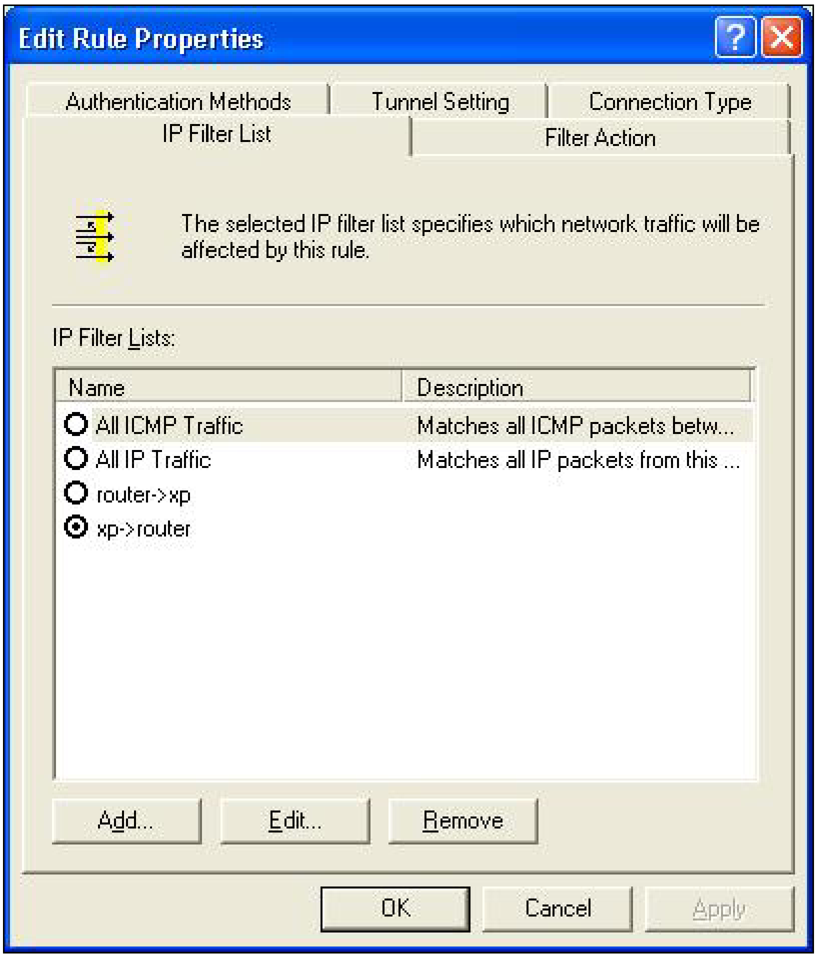
IP Filter List	Filter Action	Authentication...	Tu
☑ xp->router	Require Security	Preshared Key	19
☑ router->xp	Require Security	Preshared Key	19
☐ <Dynamic>	Default Response	Kerberos	Nc

☐ Use Add Wizard

Build 2 Filter Lists: “xp->router” and “router->xp”

Filter List 1: xp-> router

In the “**new policy’s properties**” screen, disselect **[Use Add Wizard]** check box, and then click **[Add]** button to create a new rule.

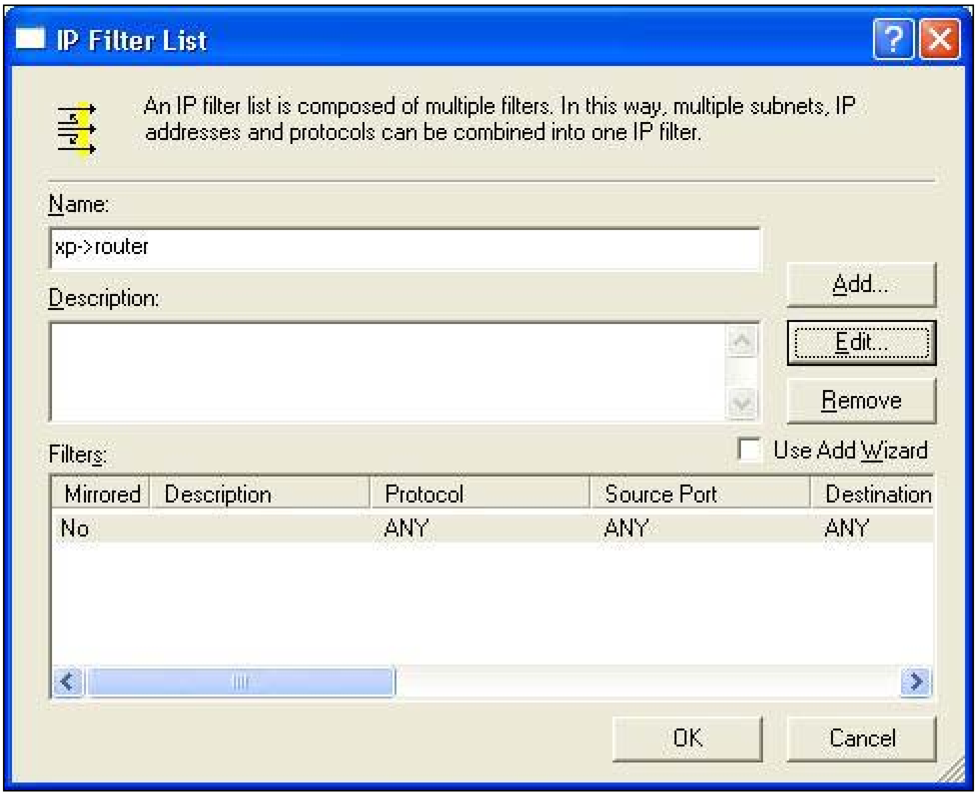


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ router->xp	
● xp->router	

click **[Add]** button



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:
xp->router

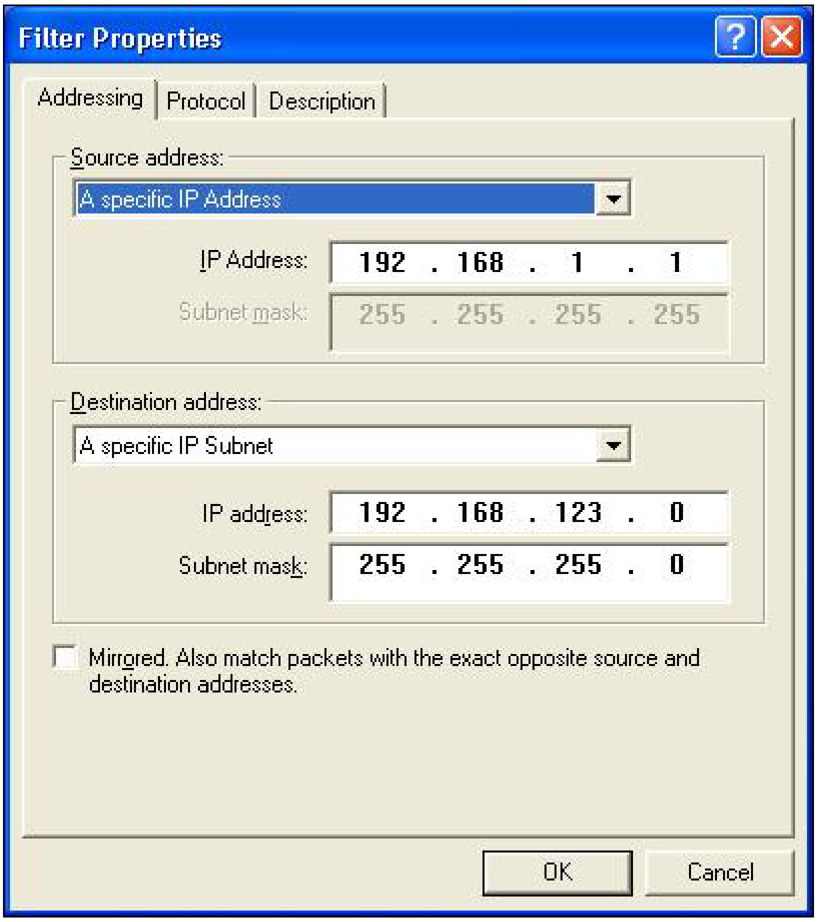
Description:

□ Use Add Wizard

Filters:

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Enter a name, for example: **xp->router**
and dis-select **[Use Add Wizard]** check box. Click **[Add]** button.



Filter Properties

Source address:
A specific IP Address
IP Address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 255

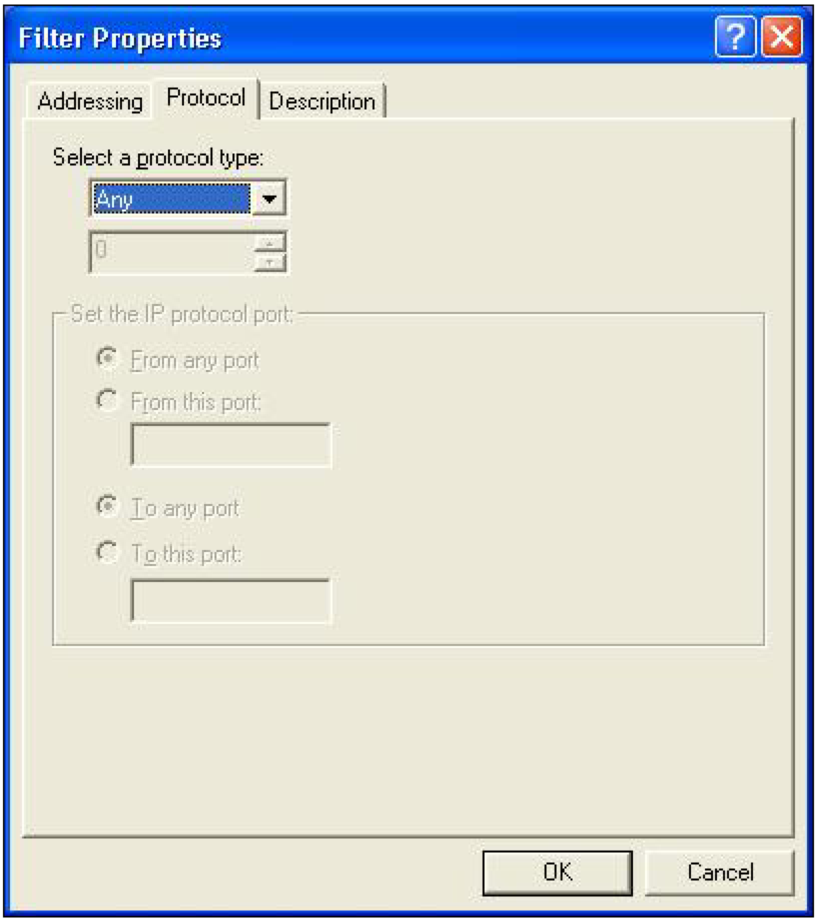
Destination address:
A specific IP Subnet
IP address: 192 . 168 . 123 . 0
Subnet mask: 255 . 255 . 255 . 0

□ Mirrored. Also match packets with the exact opposite source and destination addresses.

In the Source address field, select **[A specific IP Address]**.
and fill in IP Address: **192.168.1.1**

In the Destination address field, select **[A specific IP Subnet]**, fill in IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

If you want to select a protocol for your filter, click **[Protocol]** page.



Select a protocol type: Any

0

Set the IP protocol port:

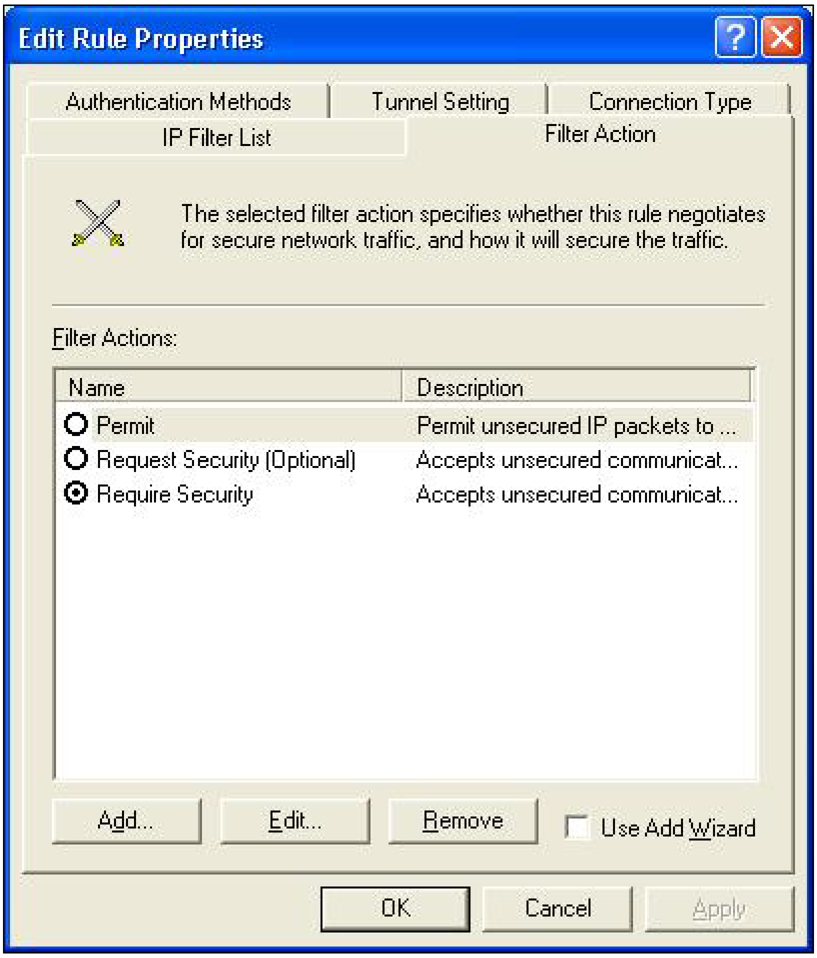
● From any port

○ From this port:

● To any port

○ To this port:

Click **[OK]** button. Then click **[OK]** button on the "**IP Filter List**" page.



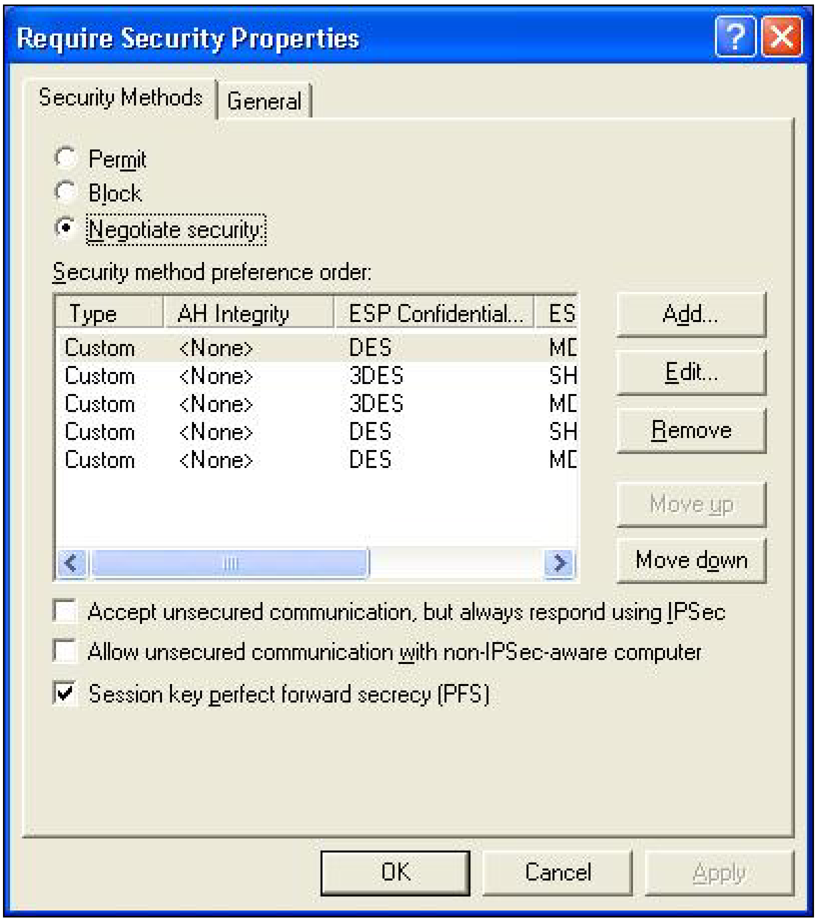
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

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

□ Use Add Wizard

select **[Filter Action]**, select **[Require Security]**, then click **[Edit]** button.



Require Security Properties

Security Methods | General

○ Permit
○ Block
● Negotiate security:

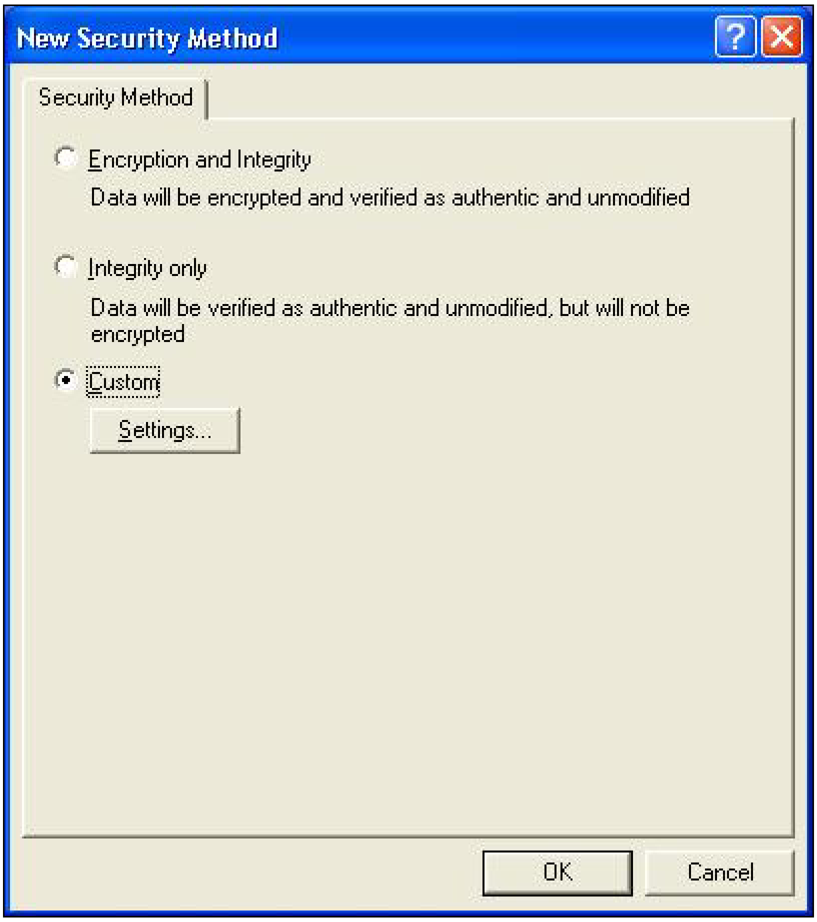
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	DES	MD
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

select **[Negotiate security],** Select **[Session key Perfect Forward Secrecy (PFS)]**

click **[Edit]** button.



New Security Method

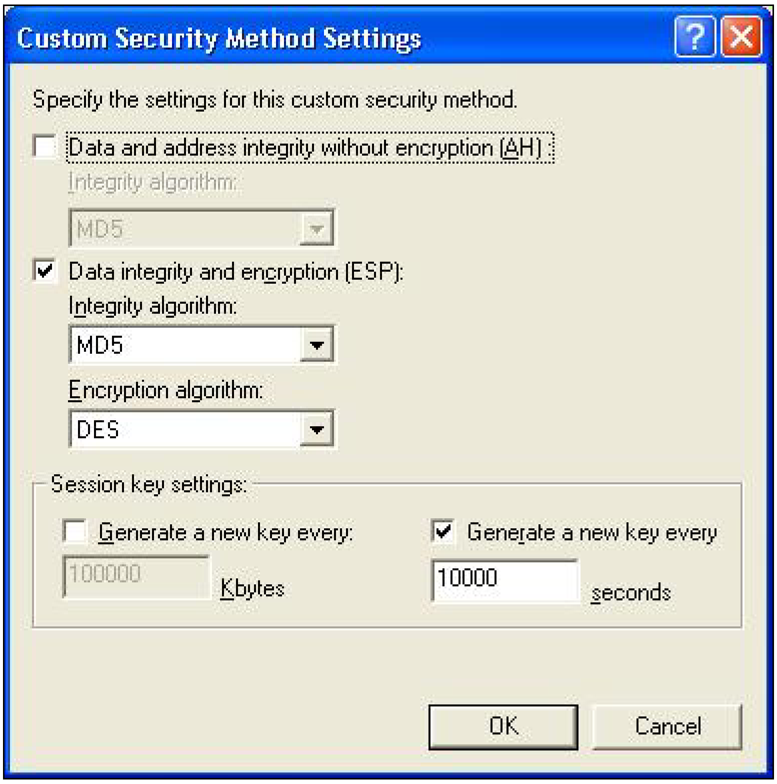
Security Method

○ Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified

○ Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted

● Custom

select **[Custom]** button



Custom Security Method Settings

Specify the settings for this custom security method.

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

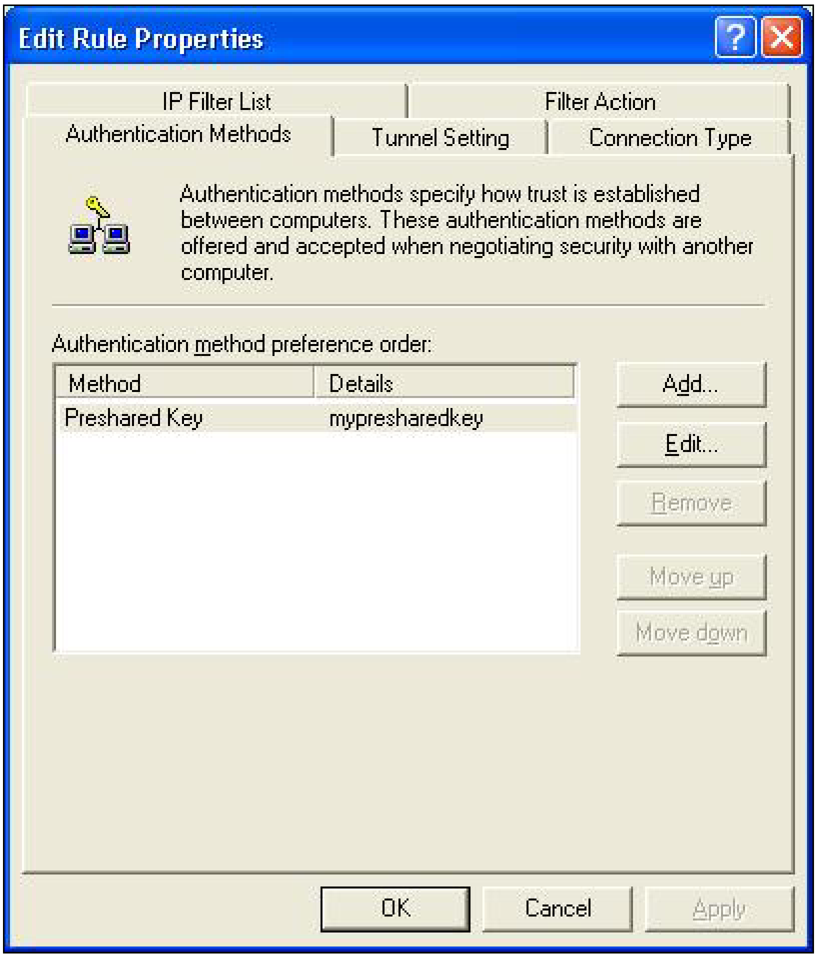
☑ Data integrity and encryption (ESP):
Integrity algorithm:
MD5
Encryption algorithm:
DES

Session key settings:

□ Generate a new key every:
100000 Kbytes

☑ Generate a new key every
10000 seconds

Select **[Data integrity and encryption (ESP)]**
Configure "**Integrity algorithm**": **[MD5]**
Configure "**Encryption algorithm**": **[DES**]
Configure "**Generate a new key every [10000] seconds**"
Click **[OK]** button



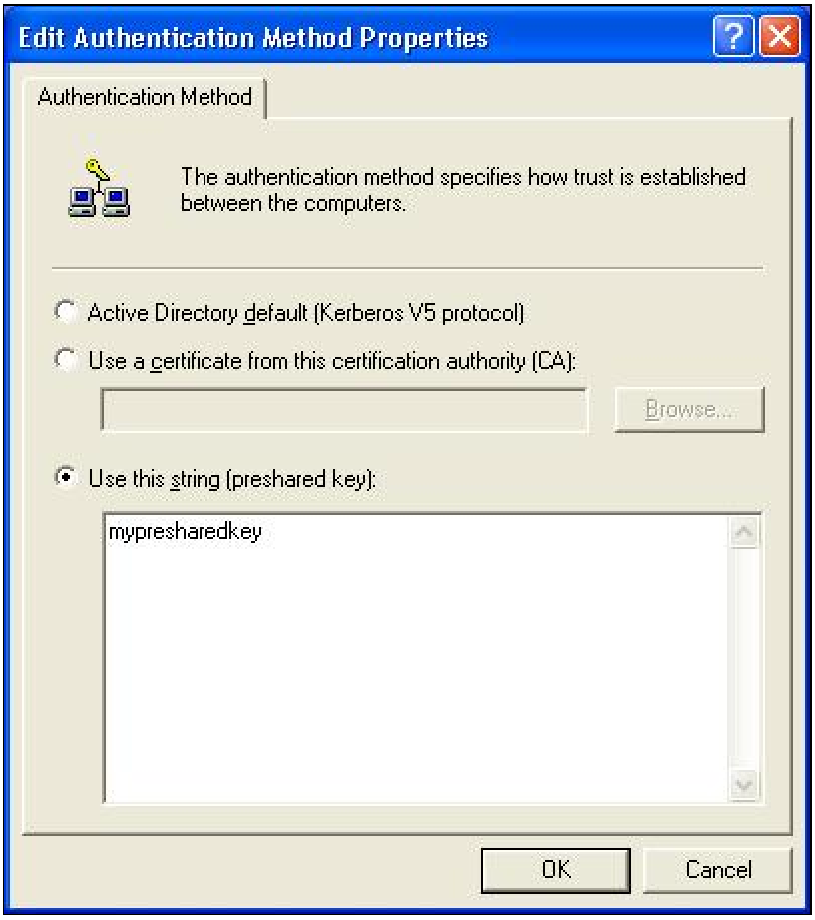
Edit Rule Properties

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	mypresharedkey

select **[Authentication Methods]** page, click **[Add]** button.



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

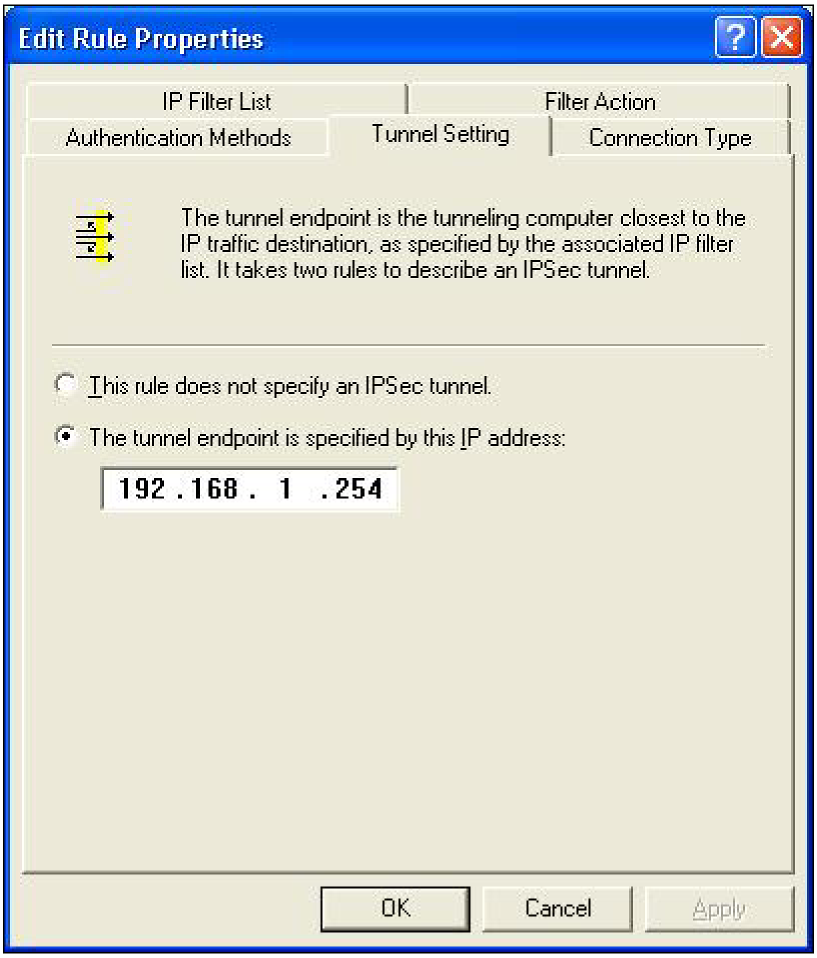
○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

mypresharedkey

select **[Use this string to protect the key exchange (preshared key)]**, and enter your preshared key string, such as **mypresharedkey**. Click [**OK]** button.
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

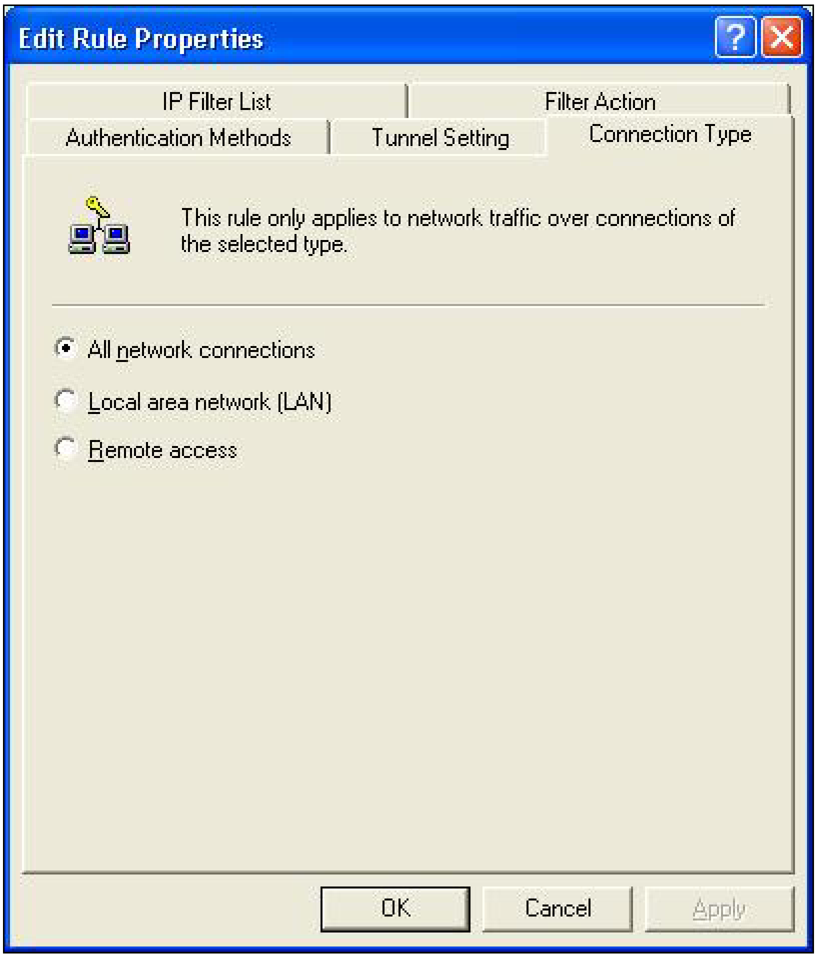
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 254

configure **[The tunnel endpoint is specified by this IP address]**: **192.168.1.254**

Select **[Connection Type]**



This rule only applies to network traffic over connections of the selected type.

● All network connections

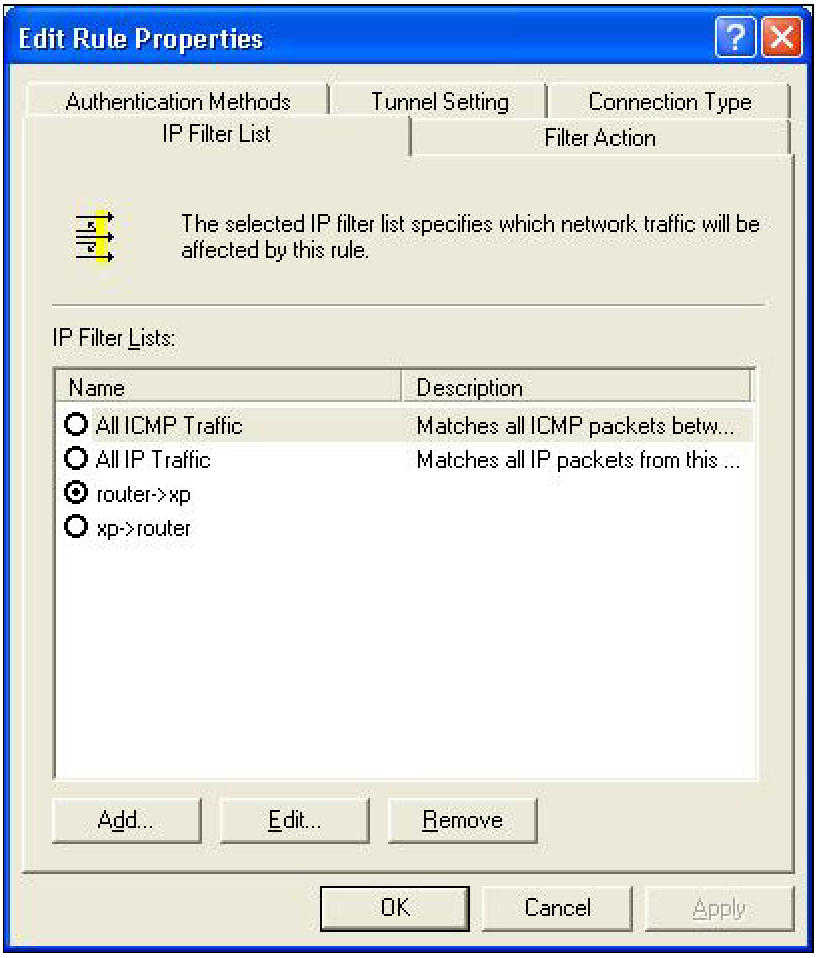
○ Local area network (LAN)

○ Remote access

select **[All network connections]**

Tunnel 2: router->xp

In the “**new policy’s properties**” page, dis-select [**Use Add Wizard]** check box, and then click **[Add]** button to create a new rule.

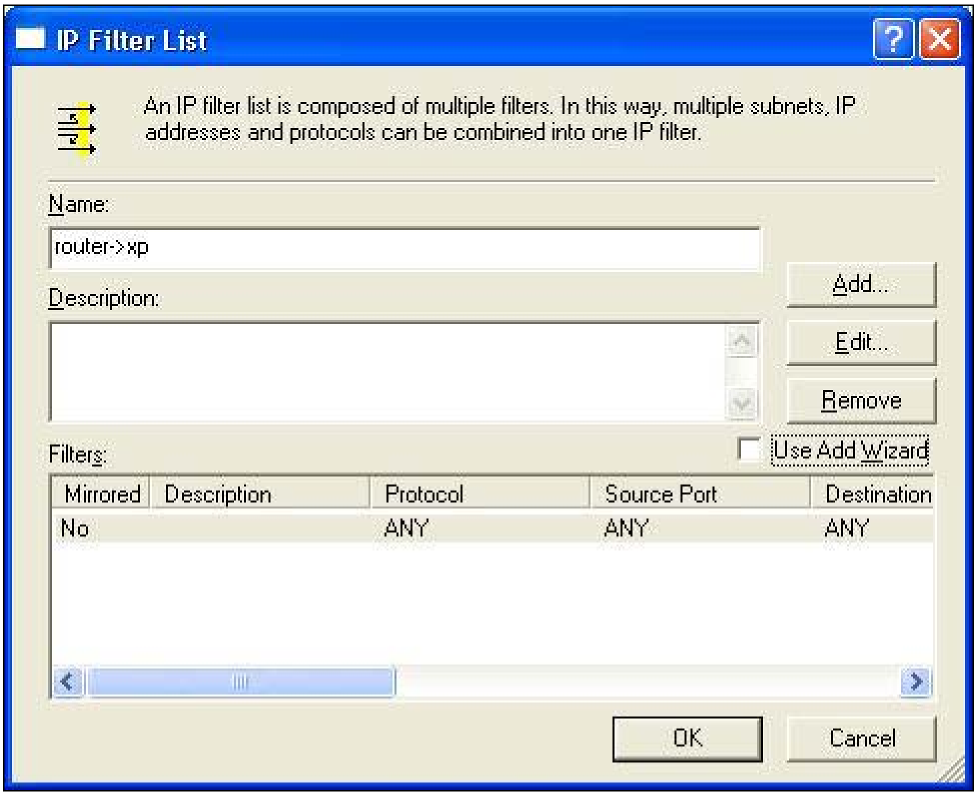


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● router->xp	
○ xp->router	

click **[Add]** button



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:
router->xp

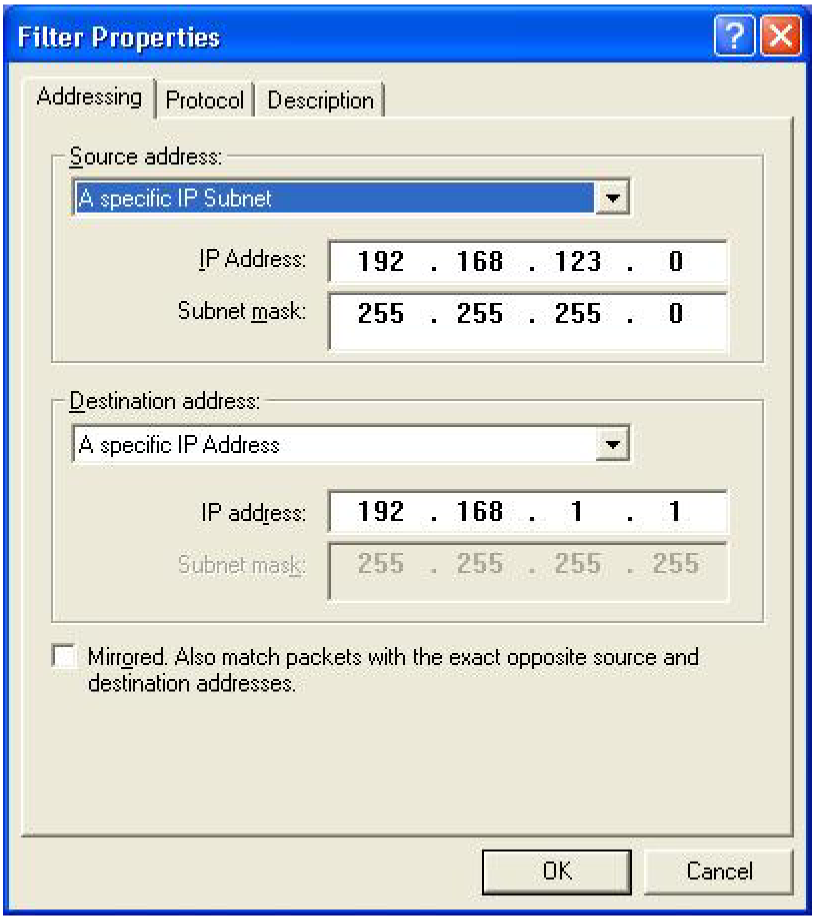
Description:

Filters:

□ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Enter a name, such as **router->xp**
and dis-select **[Use Add Wizard]** check box. Click **[Add]** button.



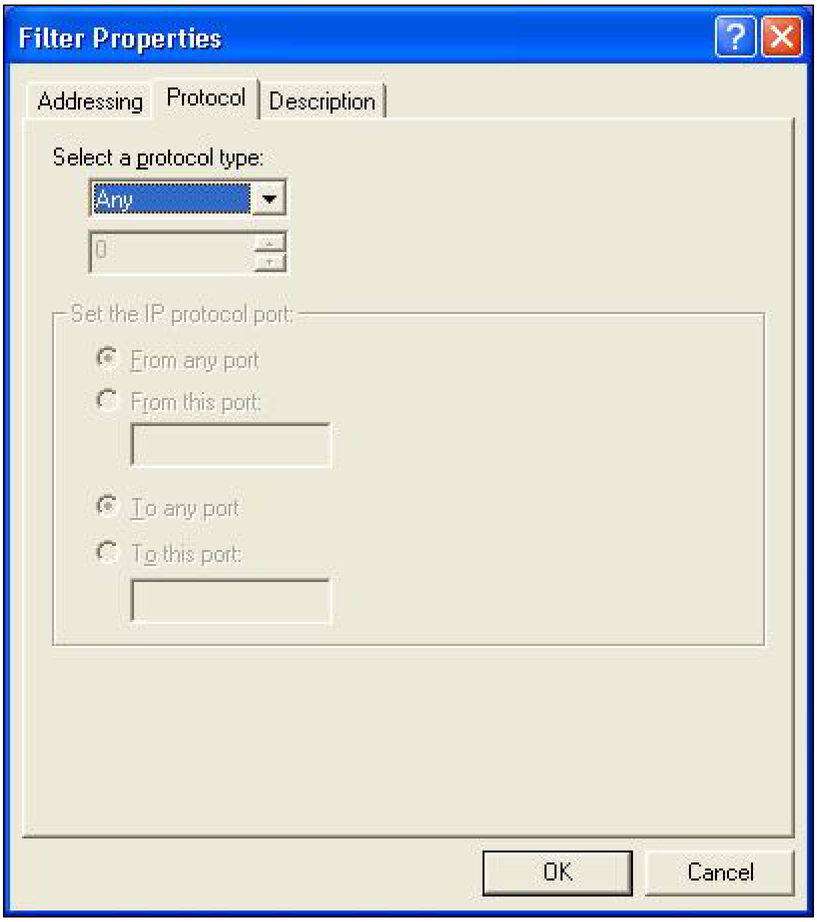
Source address:
A specific IP Subnet
IP Address: 192 . 168 . 123 . 0
Subnet mask: 255 . 255 . 255 . 0

Destination address:
A specific IP Address
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 255

□ Mirrored. Also match packets with the exact opposite source and destination addresses.

In the Source address field, select **[A specific IP Subnet]**. fill in
IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

In the Destination address field, select [**A specific IP Address]**,
and fill in IP Address: **192.168.1.1**
If you want to select a protocol for your filter, click **[Protocol]** page.



Select a protocol type: Any

0

Set the IP protocol port:

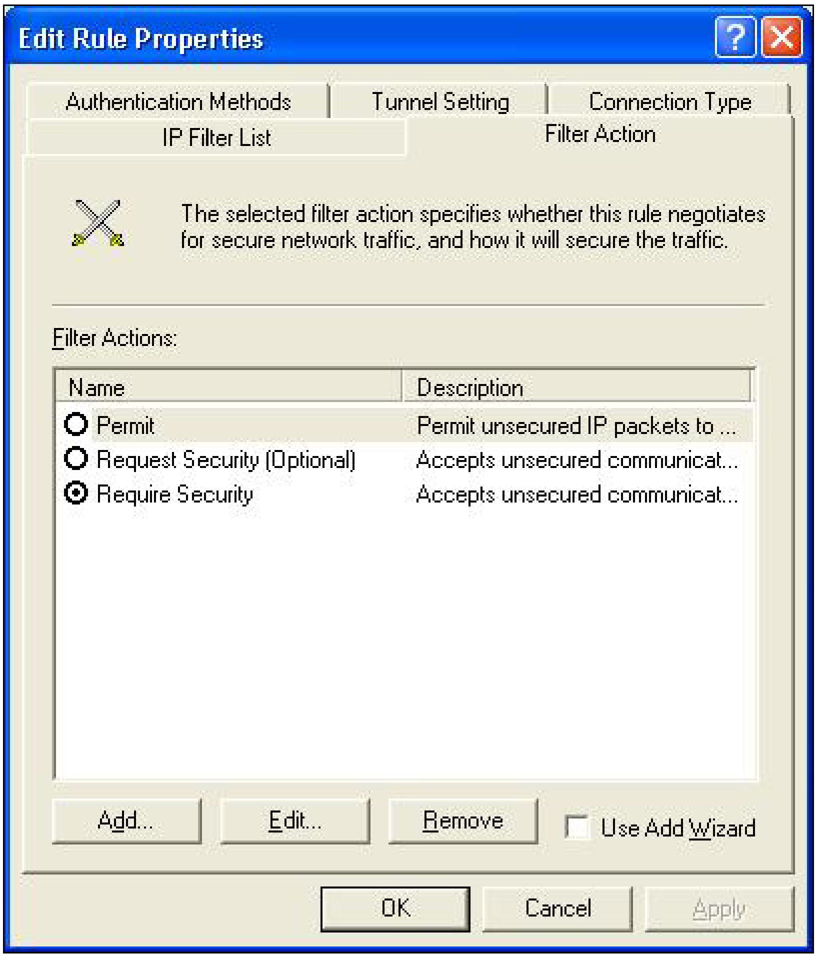
● From any port

○ From this port:

● To any port

○ To this port:

Click **[OK]** button. Then click **[OK]** button on **[IP Filter List]** window.



Edit Rule Properties

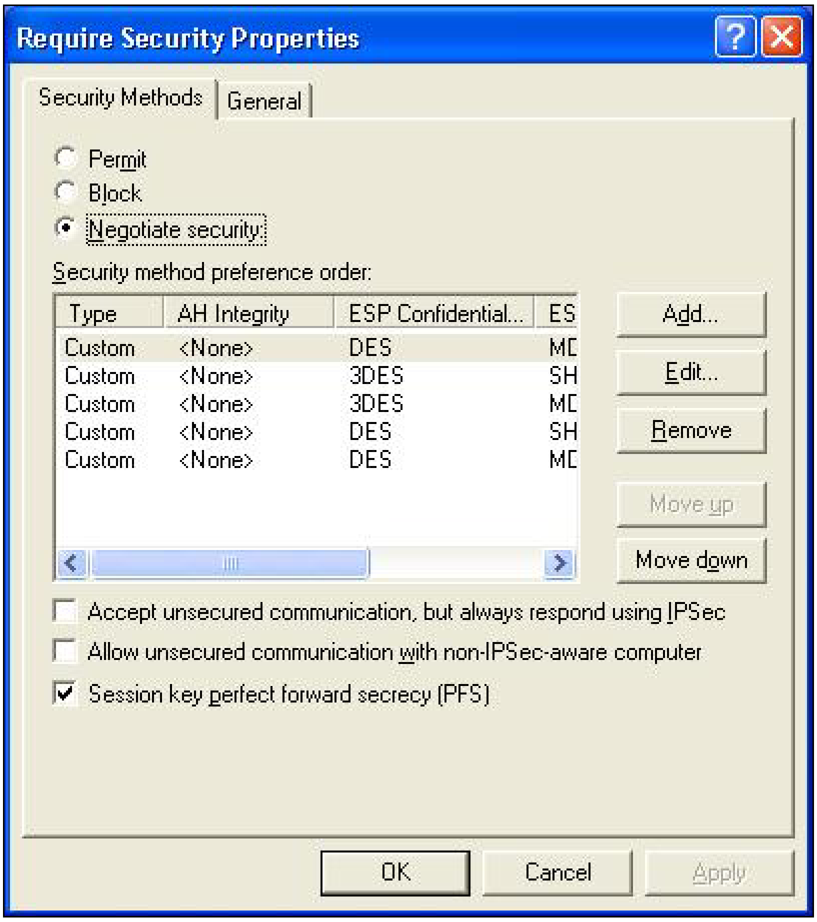
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

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

□ Use Add Wizard

select **[Filter Action tab]**, select **[Require Security]**, then click **[Edit]** button.



○ Permit

○ Block

● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	DES	MD
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

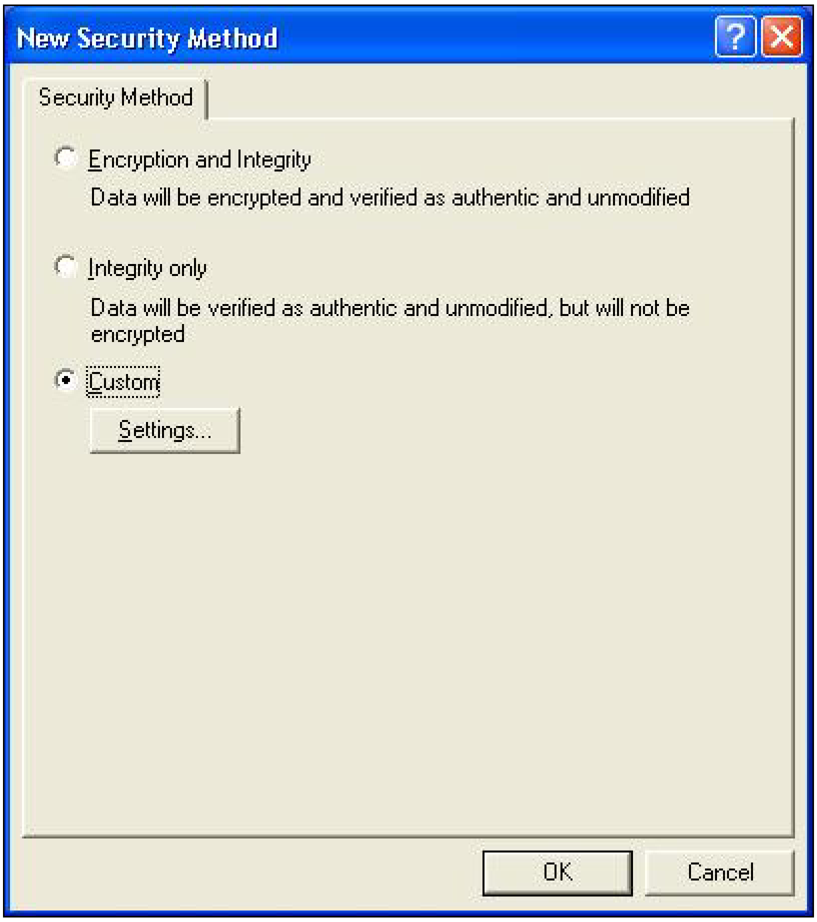
□ Accept unsecured communication, but always respond using IPSec

□ Allow unsecured communication with non-IPSec-aware computer

☑ Session key perfect forward secrecy (PFS)

select **[Negotiate security],** Select **[Session key Perfect Forward Secrecy (PFS)]**

click **[Edit]** button.



New Security Method

Security Method

○ Encryption and Integrity

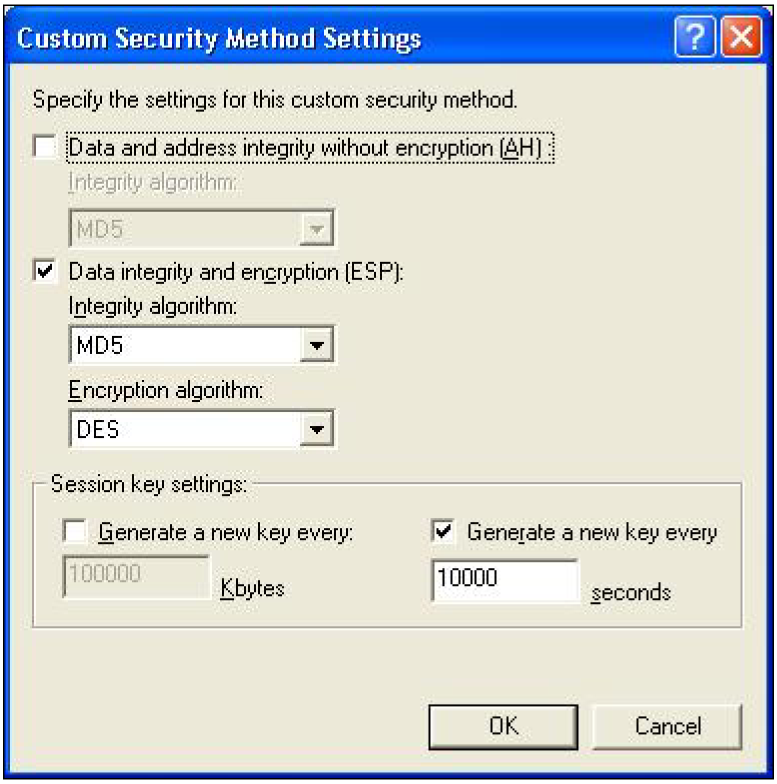
Data will be encrypted and verified as authentic and unmodified

○ Integrity only

Data will be verified as authentic and unmodified, but will not be encrypted

● Custom

select **[Custom]** button



Custom Security Method Settings

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

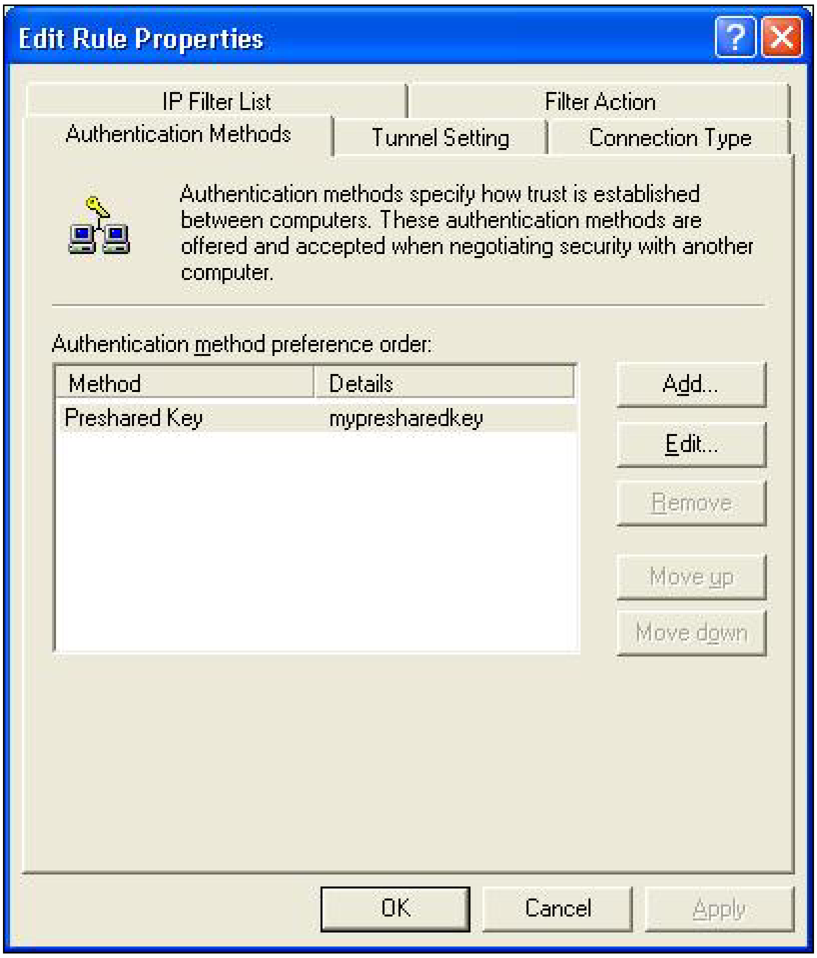
Encryption algorithm: DES

Session key settings:

□ Generate a new key every: 100000 Kbytes

☑ Generate a new key every 10000 seconds

Select **[Data integrity and encryption (ESP)]**
Configure “**Integrity algorithm**”: **[MD5]**
Configure “**Encryption algorithm**”: **[DES]**
Configure “**Generate a new key every [10000] seconds**”
Click **[OK]** button

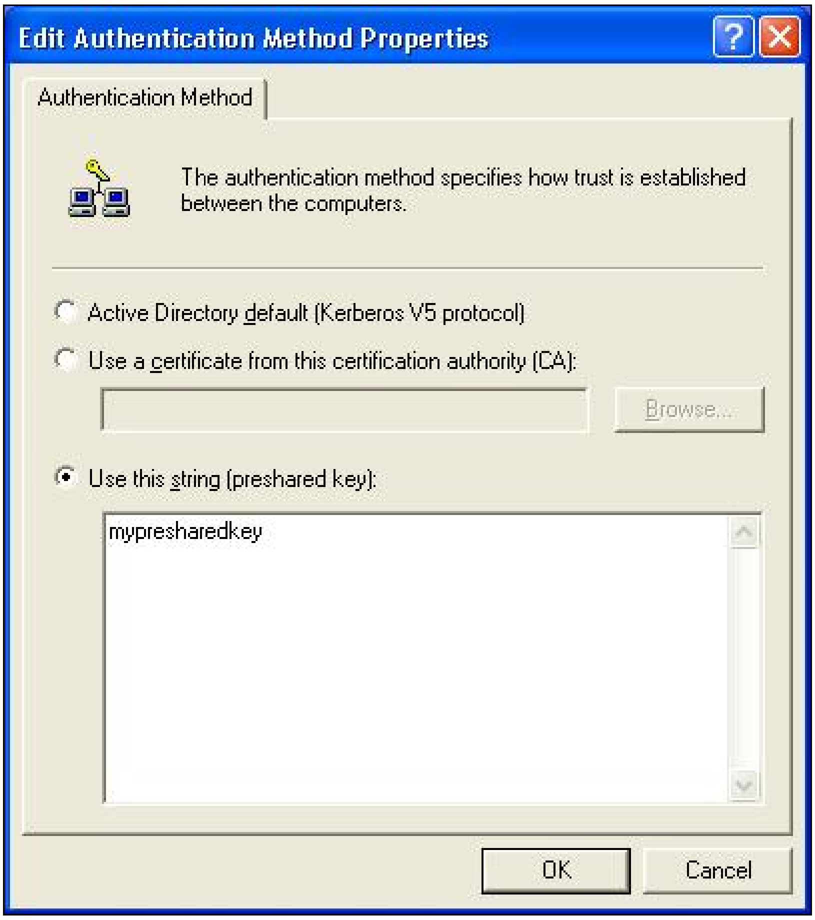


Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	mypresharedkey

select **[Authentication Methods]** page, click **[Add]** button.



The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

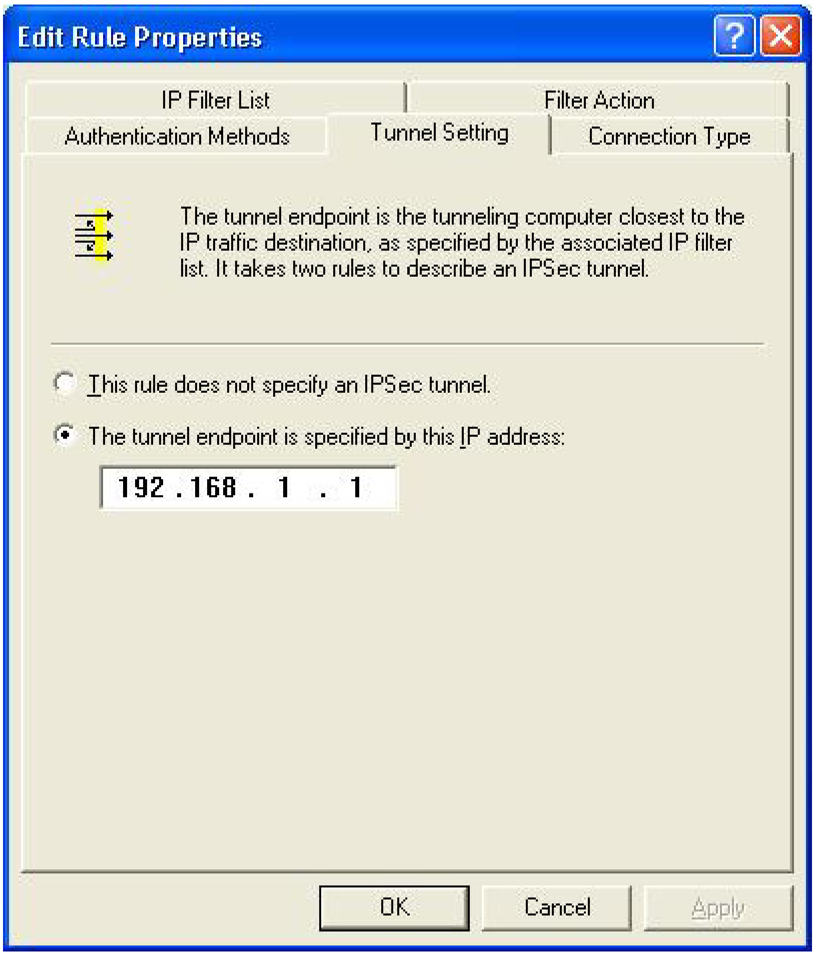
○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

mypresharedkey

select **[Use this string to protect the key exchange (preshared key)]**, and enter the preshared key string, such as **mypresharedkey**. Click **[OK]** button.
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

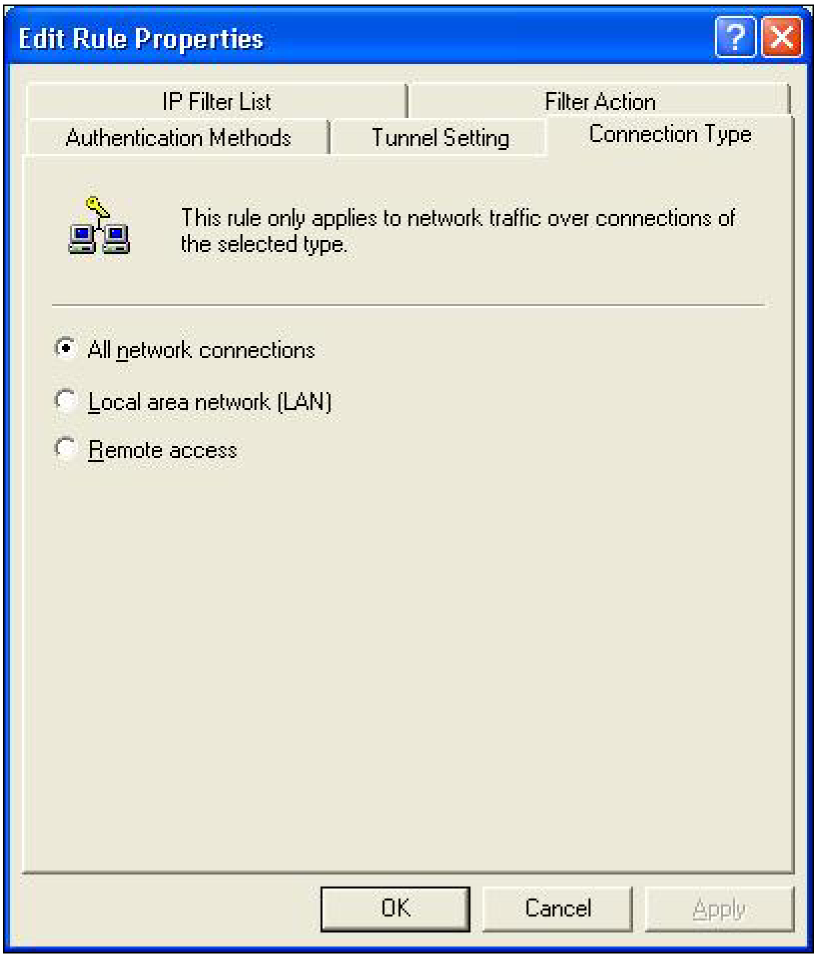
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 1

Configure **[The tunnel endpoint is specified by this IP address]**: **192.168.1.1**

Select **[Connection Type]**



Edit Rule Properties

This rule only applies to network traffic over connections of the selected type.

● All network connections

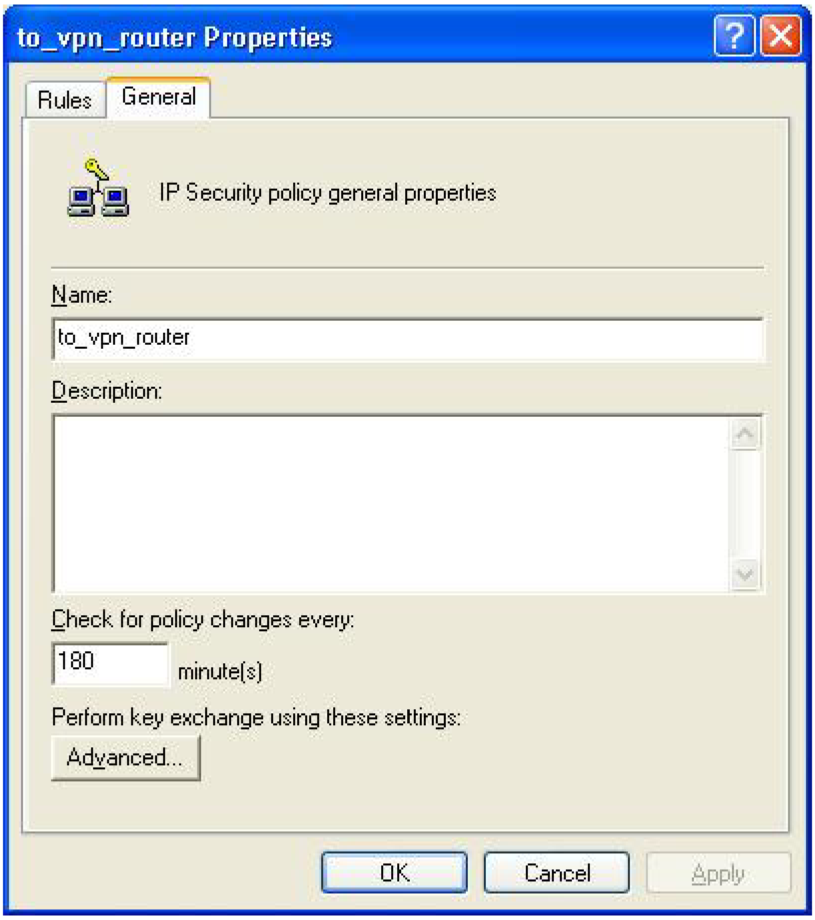
○ Local area network (LAN)

○ Remote access

select **[All network connections]**

Configure IKE properties

Select **[General]**



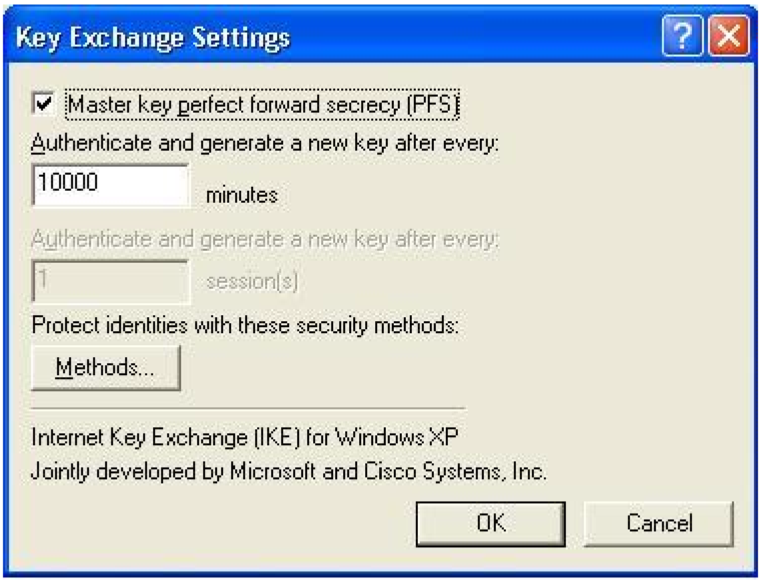
Name:
to_vpn_router

Description:

Check for policy changes every:
180 minute(s)

Perform key exchange using these settings:

Click **[Advanced…]**



☑ Master key perfect forward secrecy (PFS)

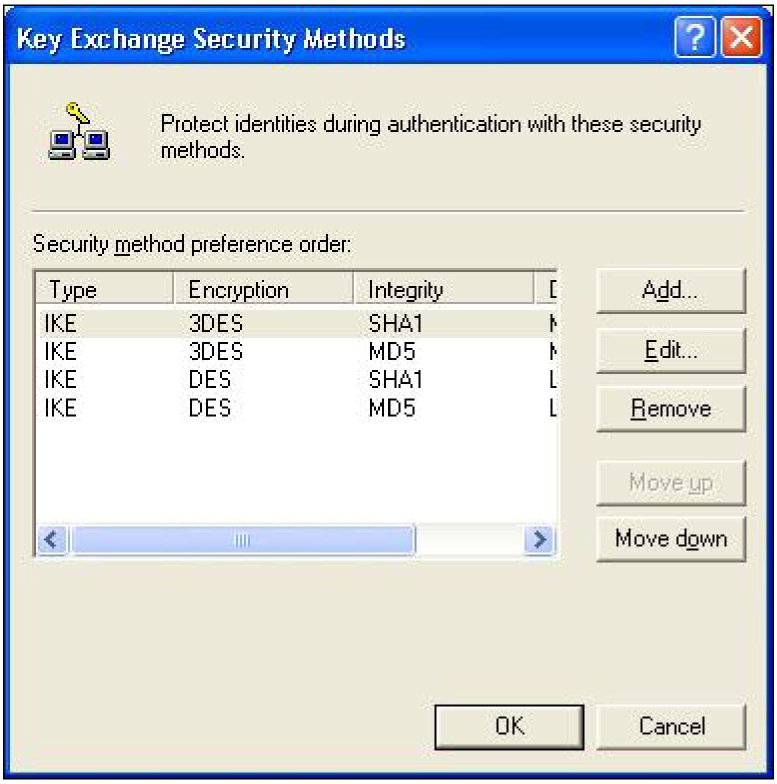
Authenticate and generate a new key after every:
10000 minutes

Authenticate and generate a new key after every:
1 session(s)

Protect identities with these security methods:

Internet Key Exchange (IKE) for Windows XP
Jointly developed by Microsoft and Cisco Systems, Inc.

enable “**Master key perfect forward security (PFS)**”
configure “**Authenticate and generate a new key after every [10000] seconds**”
click **[Methods…]**



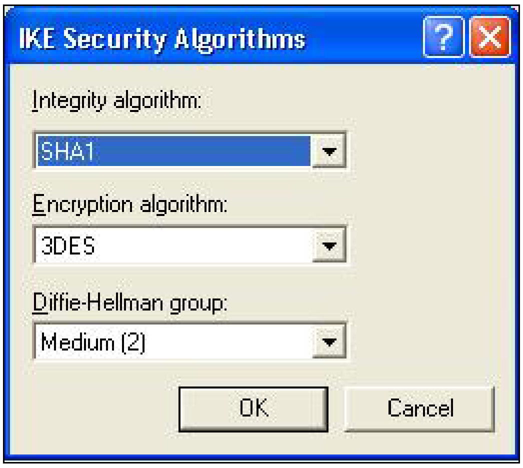
Key Exchange Security Methods

Protect identities during authentication with these security methods.

Security method preference order:

Type	Encryption	Integrity	D
IKE	3DES	SHA1	M
IKE	3DES	MD5	M
IKE	DES	SHA1	L
IKE	DES	MD5	L

click **[Add]** button



IKE Security Algorithms

Integrity algorithm: SHA1

Encryption algorithm: 3DES

Diffie-Hellman group: Medium (2)

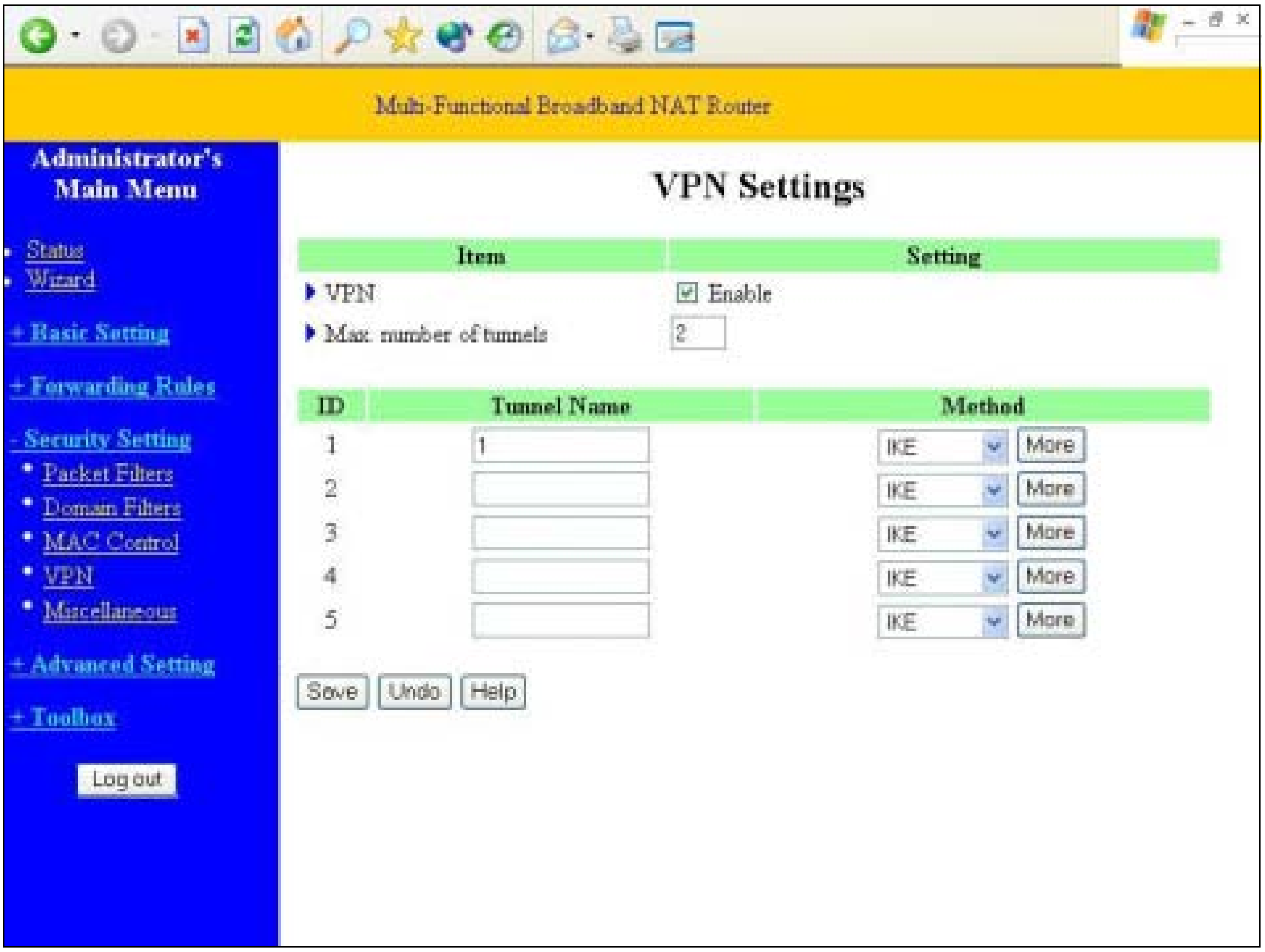
Configure “**Integrity algorithm**”: **[SHA1]**
Configure “**Encryption algorithm**”: **[3DES]**
Configure “**Diffie-Helman group**”: **[Medium (2)]**

Settings on VPN router

VPN Router: Wan IP address:192.168.1.254

Lan IP address:192.168.123.254

PC: 192.168.123.123



VPN Settings

Item	Setting
VPN	☑ Enable
Max. number of tunnels	2

ID	Tunnel Name	Method	
1	1	IKE	More
2		IKE	More
3		IKE	More
4		IKE	More
5		IKE	More

VPN Settings:

VPN: Enable

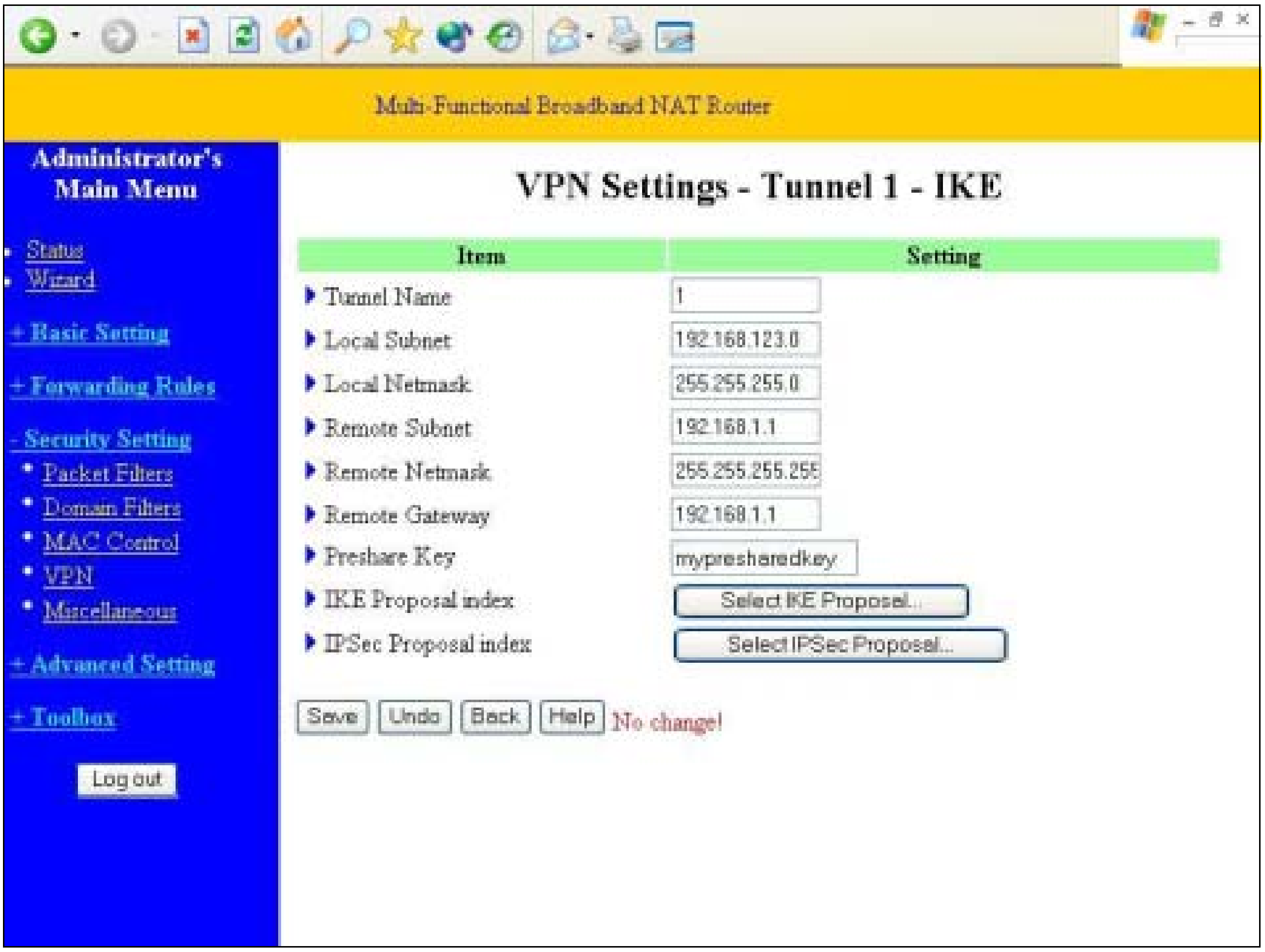
Max. number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Press “**More**”→



VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	1
Local Subnet	192.168.123.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.1.1
Remote Netmask	255.255.255.255
Remote Gateway	192.168.1.1
Preshare Key	mypresharedkey
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

VPN Settings - Tunnel 1 – IKE

Tunnel:1

Local Subnet:192.168.123.0

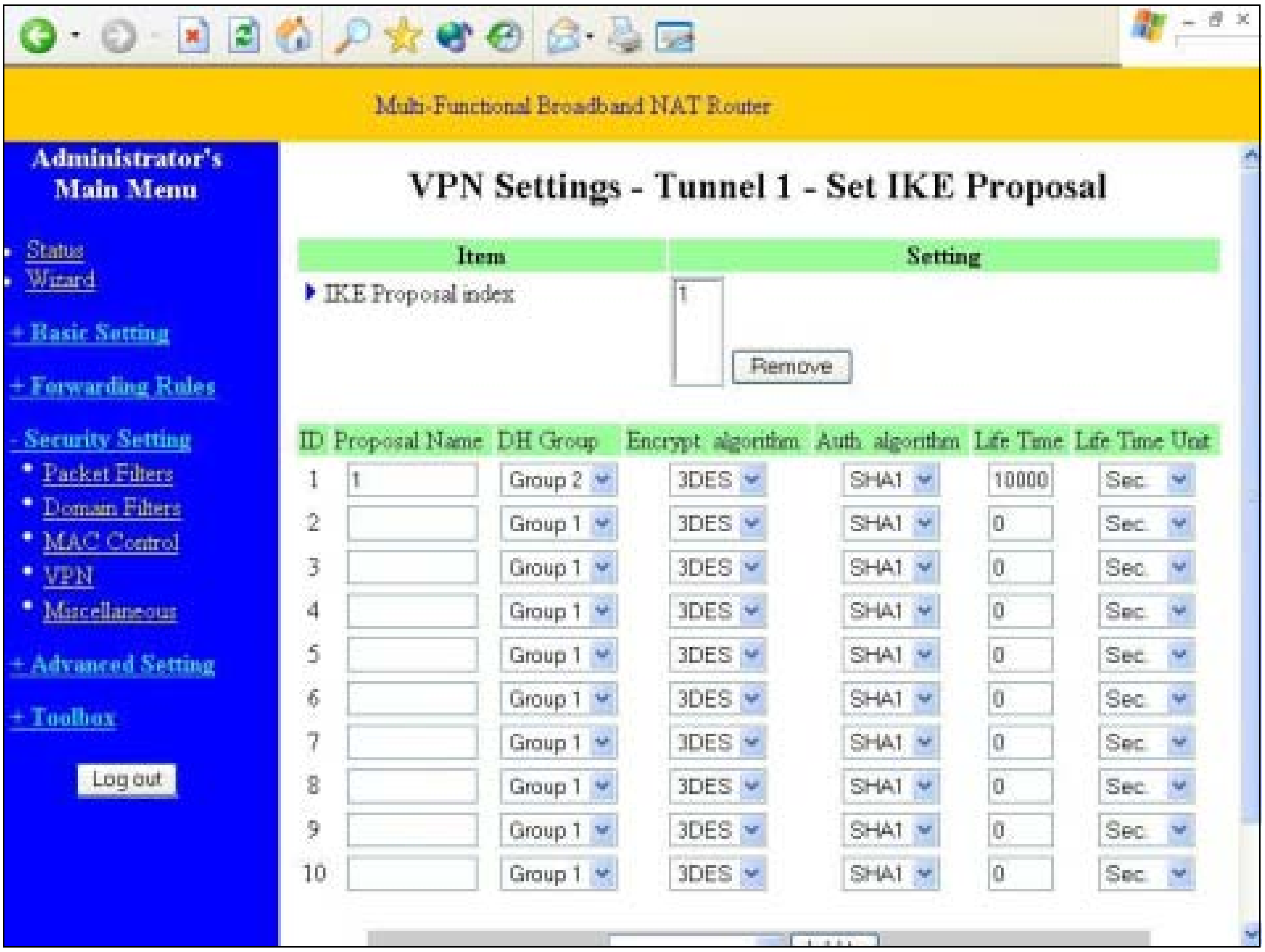
Local Netmask:255.255.255.0

Remote Subnet:192.168.1.1

Remote Netmask:255.255.255.255

Remote Gateway:192.168.1.1

Preshare Key: mypresharedkey



VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
IKE Proposal index	1

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	1	Group 2	3DES	SHA1	10000	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

VPN Settings - Tunnel 1 - Set IKE Proposal

ID: 1

Proposal Name: 1

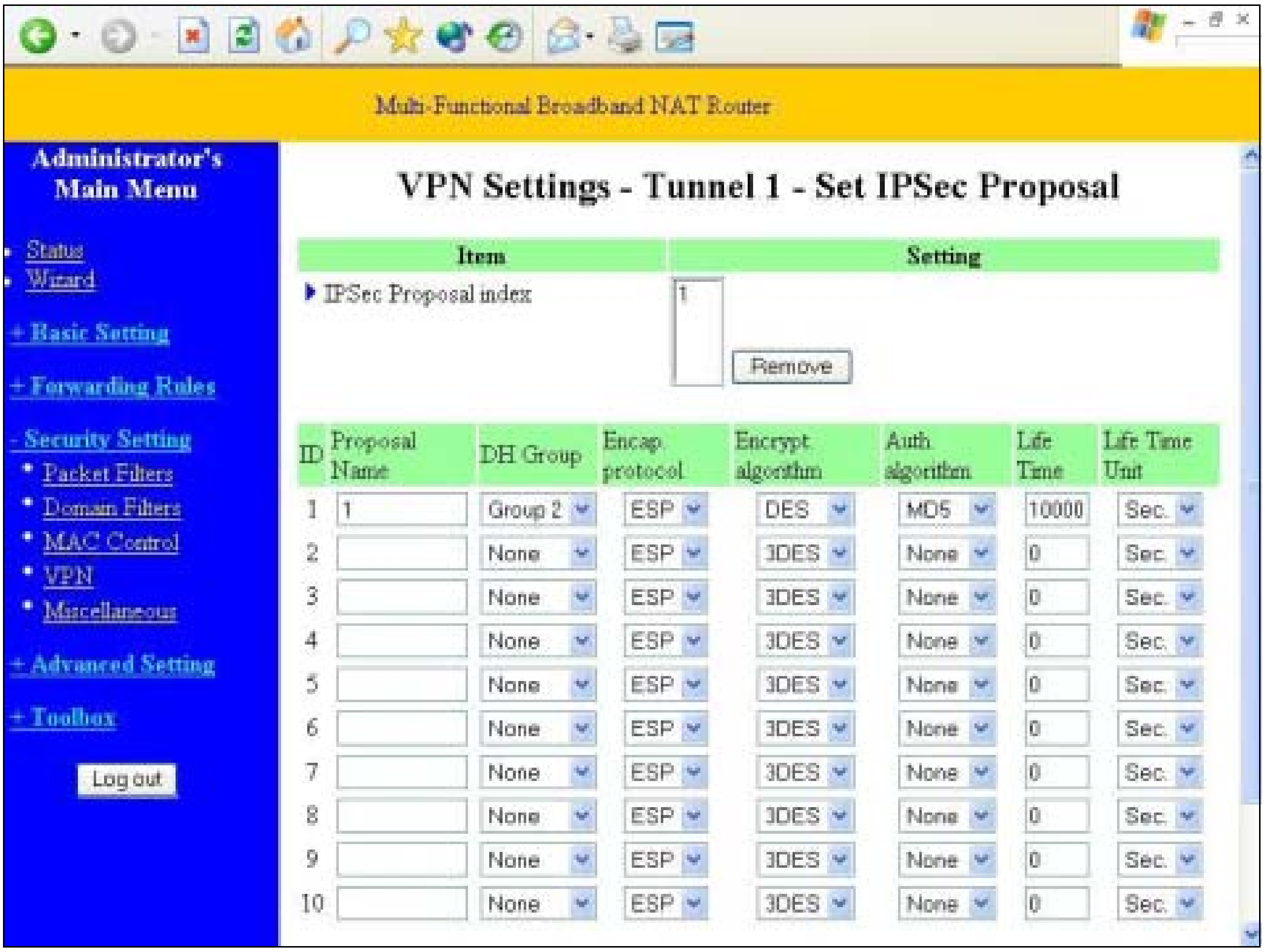
DH Group: Group2

Encrypt. Algorithm: 3DES

Auth. Algorithm: SHA1

Life Time: 10000

Life Time Unit: Sec.



VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
IPSec Proposal index	1

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	1	Group 2	ESP	DES	MD5	10000	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

VPN Settings - Tunnel 1 - Set IPSec Proposal

ID: 1

Proposal Name: proposal1

DH Group: Group2

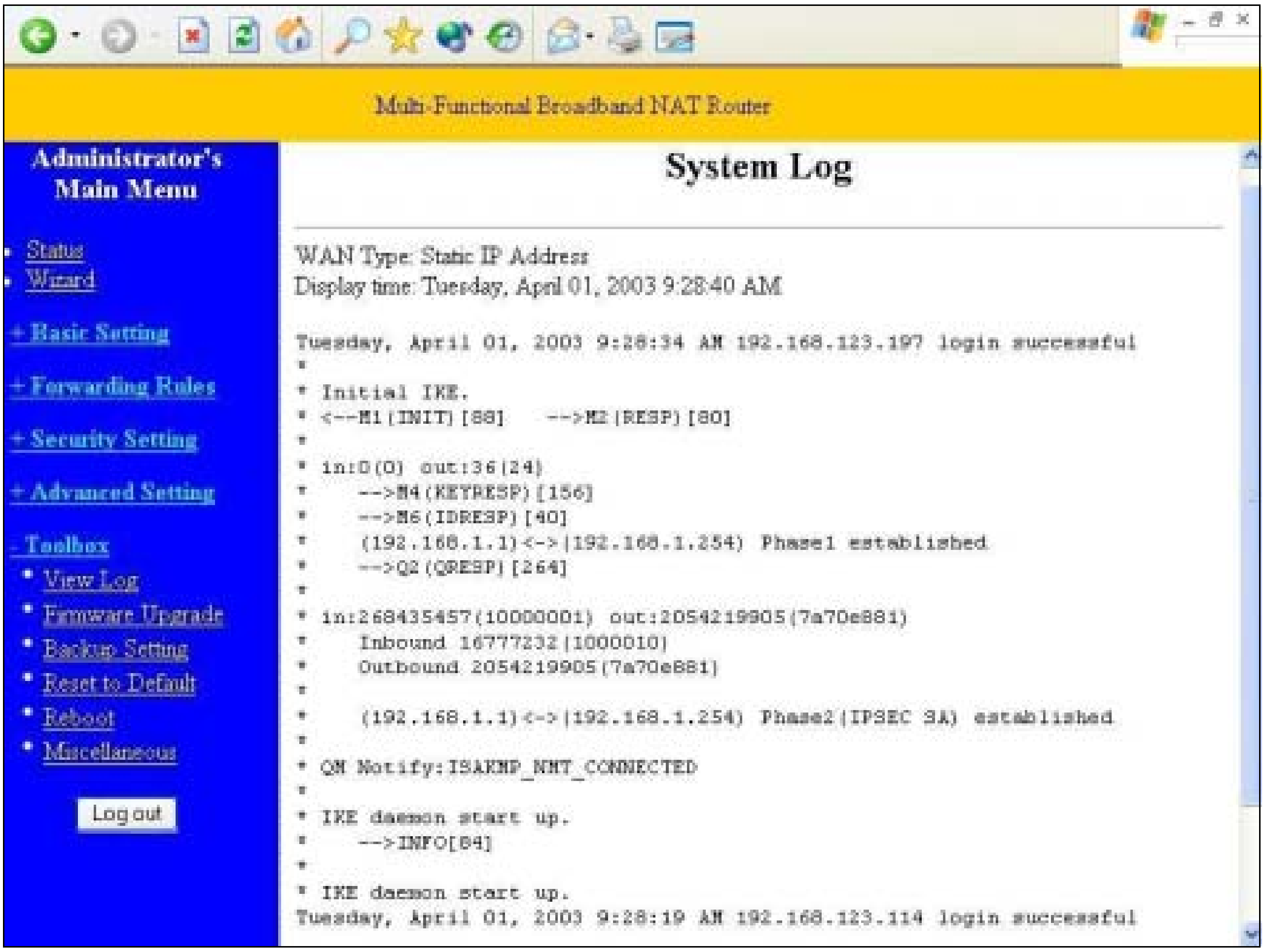
Encap. Protocol: ESP

Encrypt. Algorithm: DES

Auth. Algorithm:MD5

Life Time: 10000

Life Time Unit: Sec.



System Log

WAN Type: Static IP Address
Display time: Tuesday, April 01, 2003 9:28:40 AM

```
Tuesday, April 01, 2003 9:28:34 AM 192.168.123.197 login successful
*
* Initial IKE.
* <--M1(INIT)[88]    -->M2(RESP)[80]
*
* in:0(0) out:36(24)
*     -->M4(KEYRESP)[156]
*     -->M6(IDRESP)[40]
*     (192.168.1.1)<->(192.168.1.254) Phase1 established
*     -->Q2(QRESP)[264]
*
* in:268435457(10000001) out:2054219905(7a70e881)
*     Inbound 16777232(1000010)
*     Outbound 2054219905(7a70e881)
*
*     (192.168.1.1)<->(192.168.1.254) Phase2(IPSEC SA) established
*
* QM Notify:ISAKMP_NMT_CONNECTED
*
* IKE daemon start up.
*     -->INFO[84]
*
* IKE daemon start up.
Tuesday, April 01, 2003 9:28:19 AM 192.168.123.114 login successful
```

User can view VPN connection process in “**System Log**” page, and correct their settings. Phase1 is related to **IKE** settings, Phase2 is related to **IPSEC** settings.

Appendix C Console Mode (optional)

When you forget the system password or the IP address of this product, you need enter console mode to reset them.

Before invoking the console program, be sure to find a null modem cable and use it to connect from this product's COM port to your computer's COM port. Then, execute a terminal program, such as the ***Hyper Terminal*** of MS Windows 95. The connection parameters should be set to **19200 8-N-1**. And, reboot this product. When the M1 indicator starts flashing regularly, you can press the "***Enter***" key of the keyboard several times, there should be some messages and console prompt "**>**" appeared in the terminal.

In the console mode, you may reset the IP address and the system password of this product. Please remember to execute the **SR** command to save the changes you have made. For example,

```
IP 192.168.123.254
PW admin
SR
```