

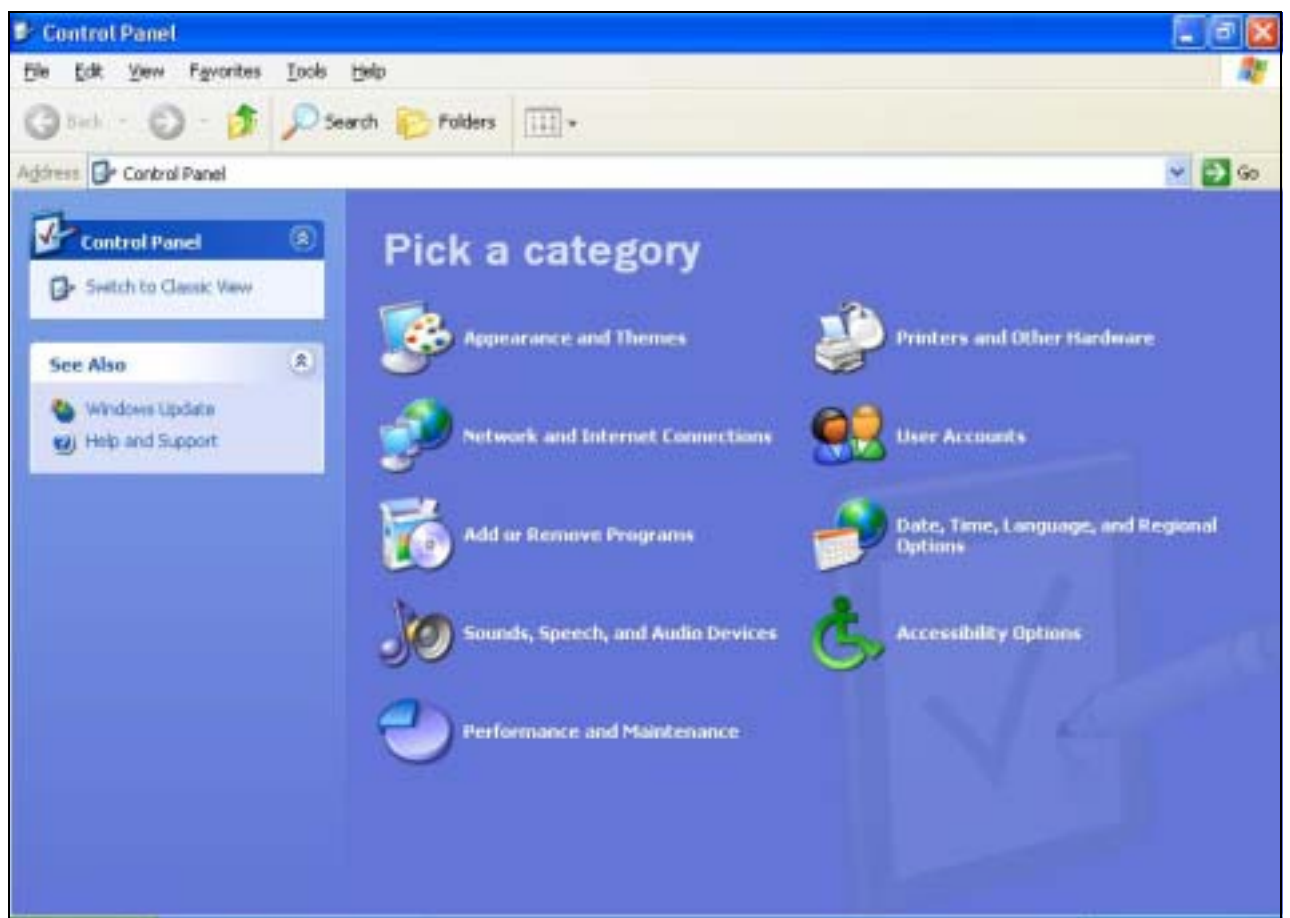
## Appendix B Win 2000/XP IPSEC Setting guide

### Example: Win XP/2000 →VPN Router

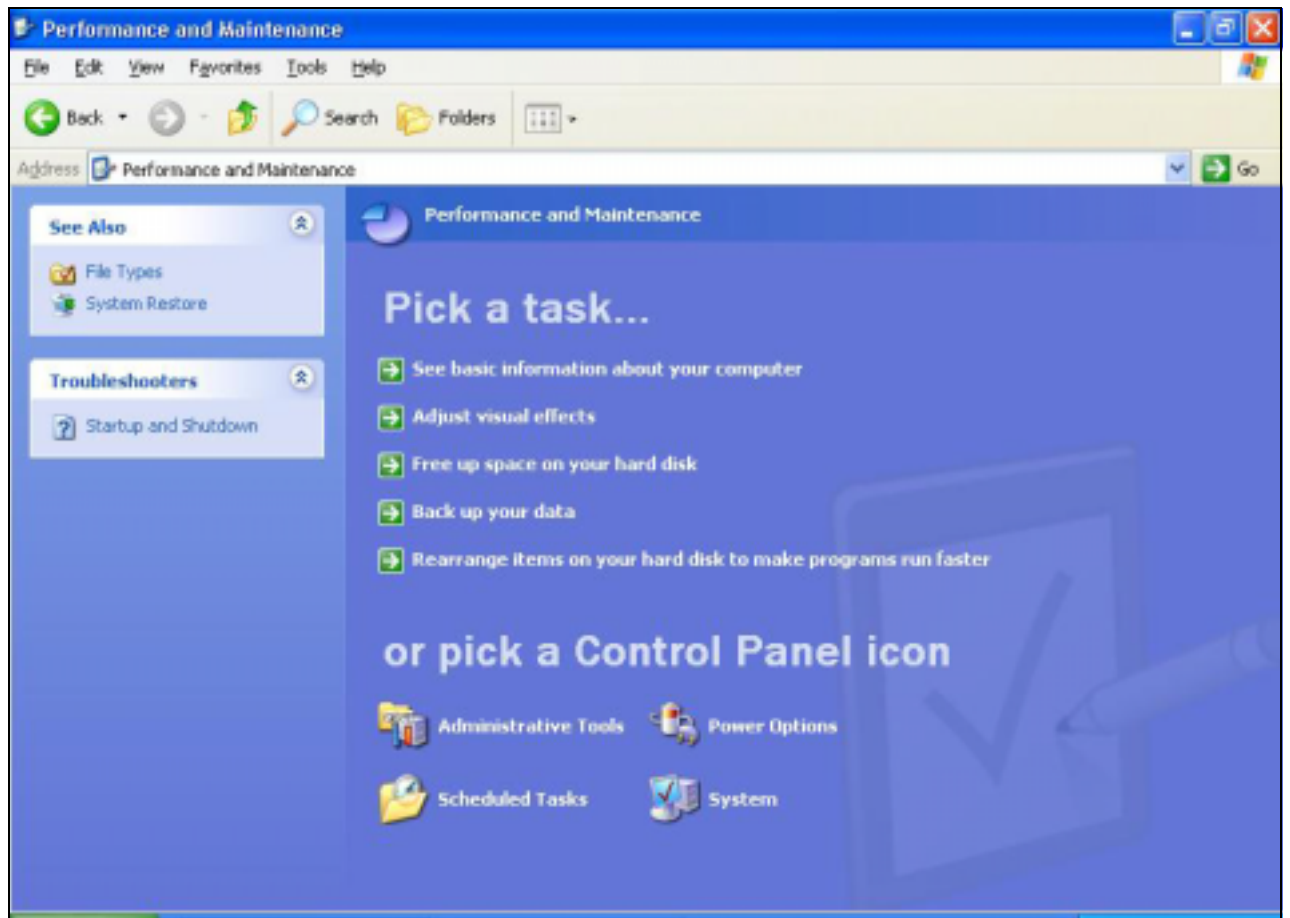
(Configuration on WIN 2000 is similar to XP)

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

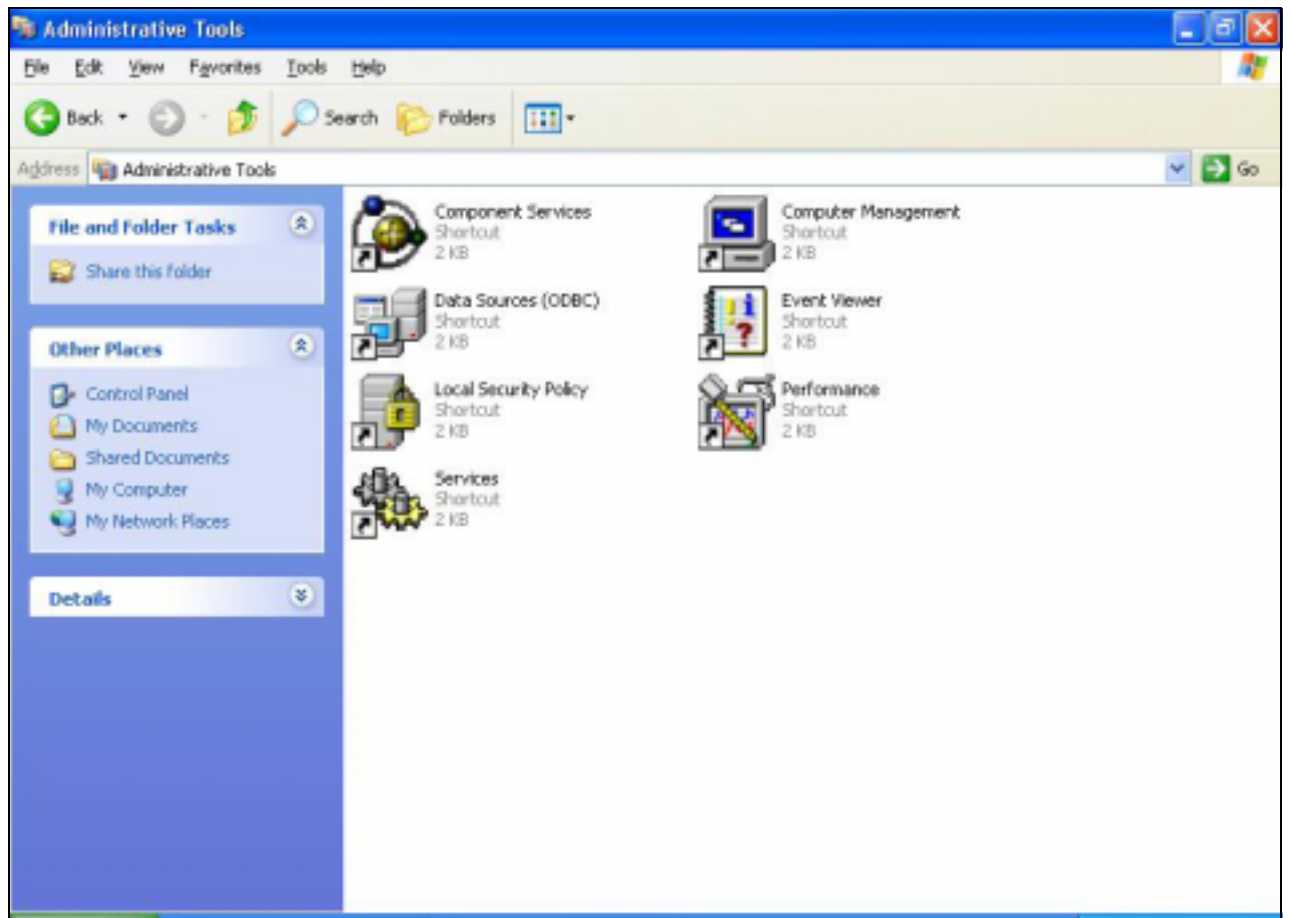
2. Or in Win XP, Click [Control Panel]



Double-click [Performance and Maintenance]

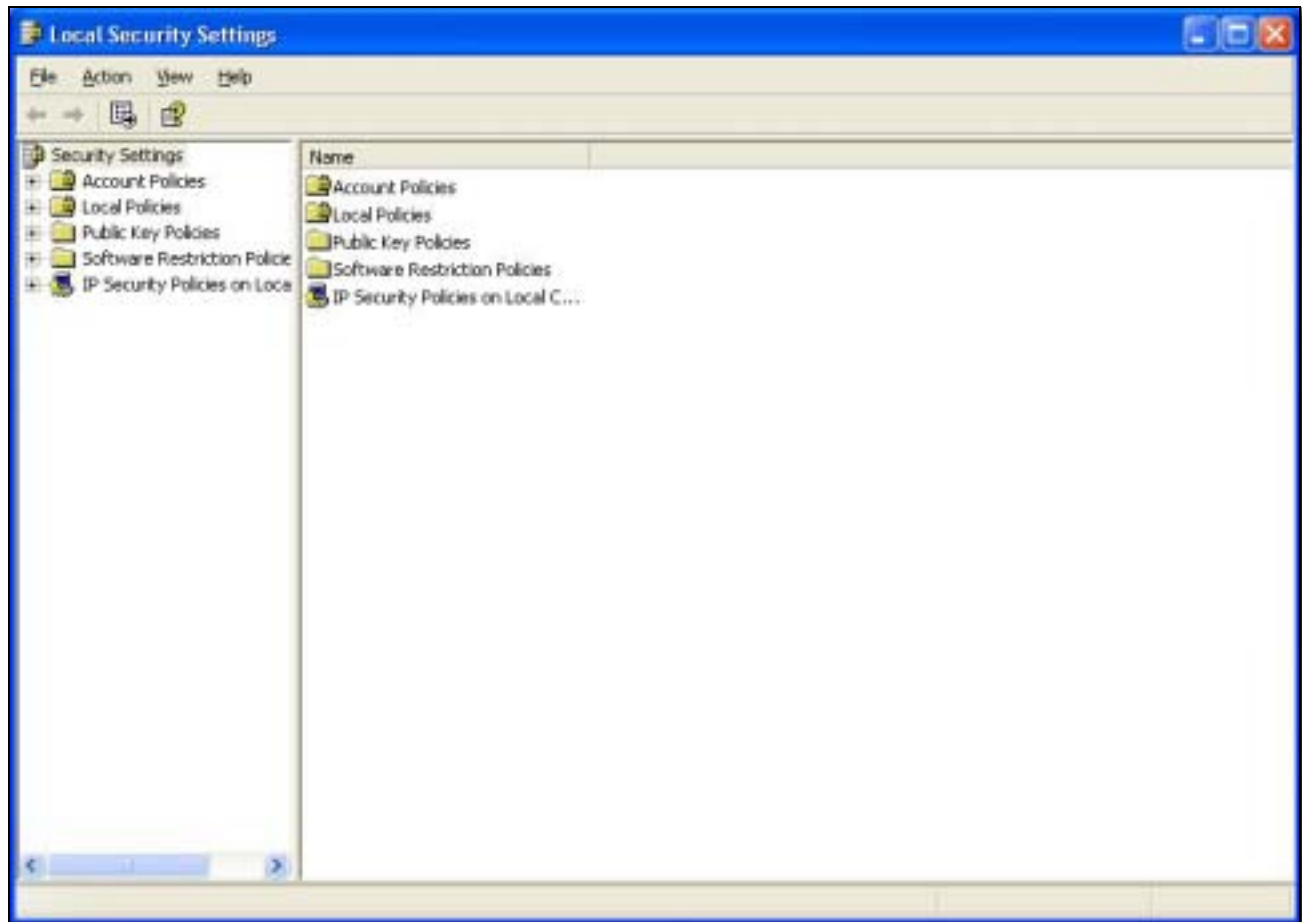


Double-click [Administrative Tools]



## Local Security Policy Settings

Double-click [Local Security Policy]

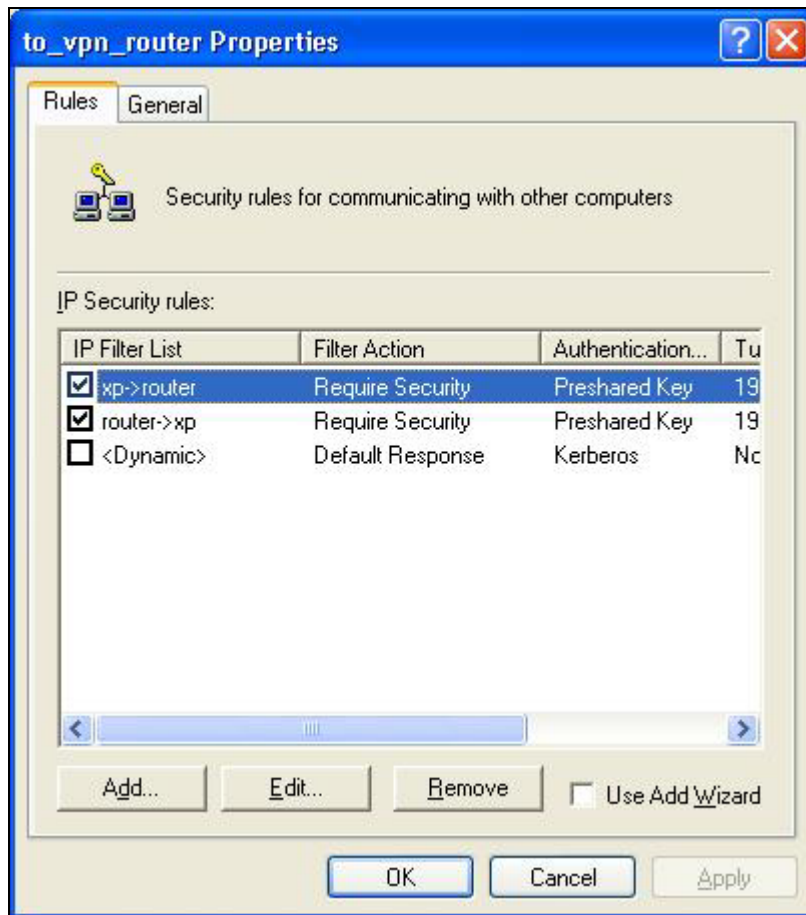


Right-click **[IP Security Policies on Local Computer]**, and click **[Create IP Security Policy]**.

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.

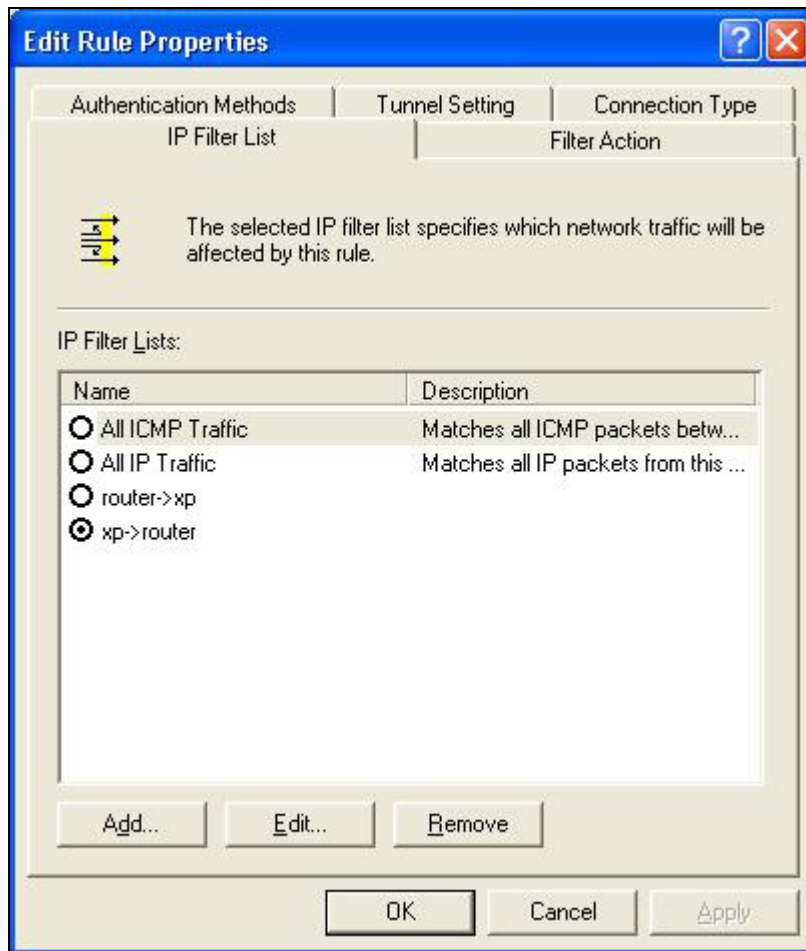
Click **[Finish]** button, make sure **[Edit]** check box is checked.



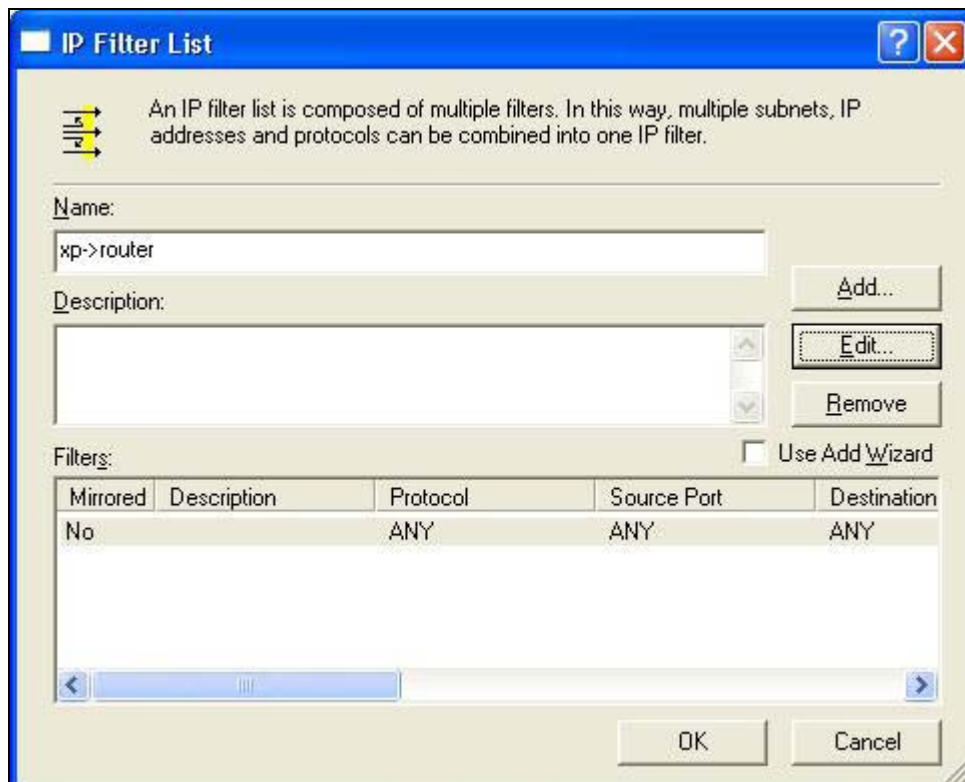
## Build 2 Filter Lists: “xp->router” and “router->xp”

### Filter List 1: xp-> router

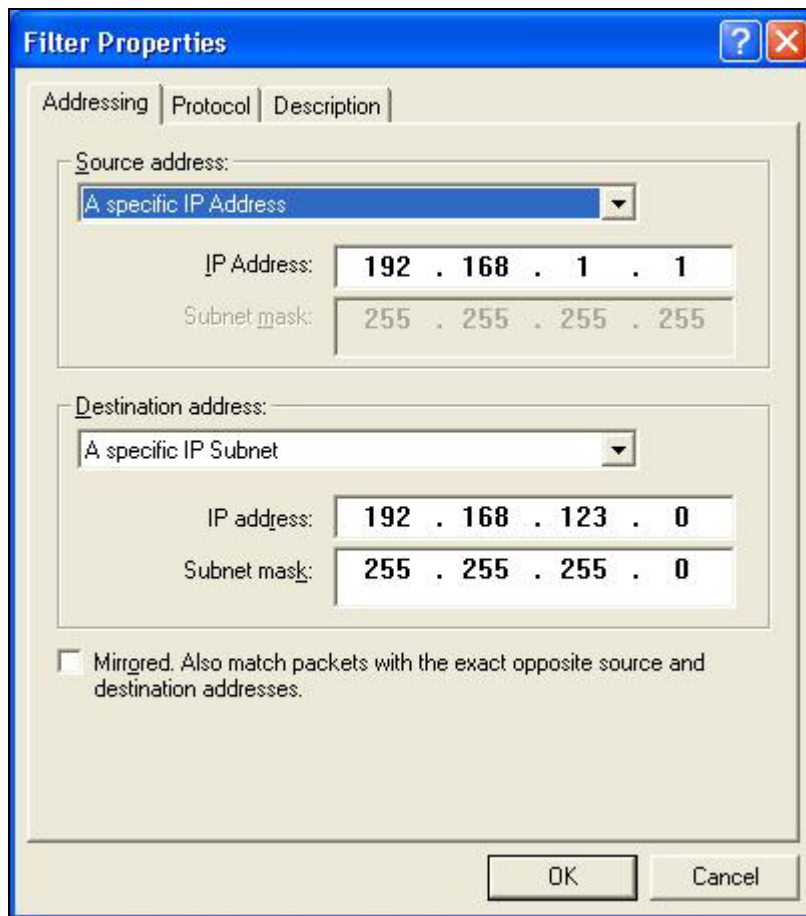
In the “new policy’s properties” screen, disselect [Use Add Wizard] check box, and then click [Add] button to create a new rule.



click **[Add]** button



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

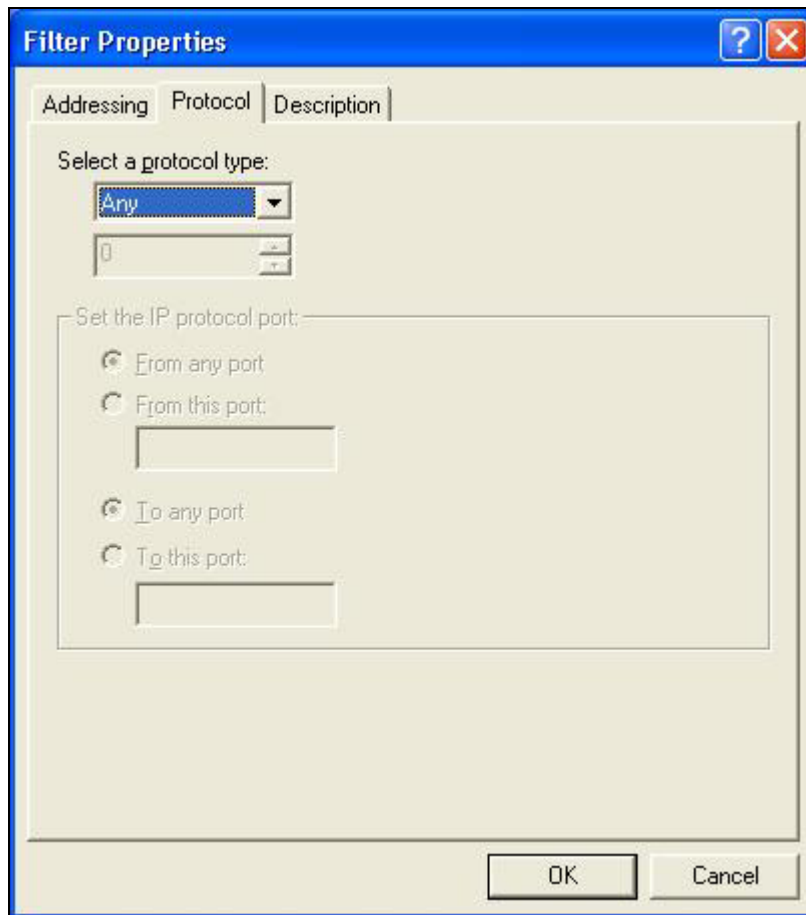


The image shows a Windows-style dialog box titled "Filter Properties". It has three tabs: "Addressing", "Protocol", and "Description". The "Addressing" tab is selected. Inside the dialog, there are two main sections. The first section is for "Source address:" and contains a dropdown menu with "A specific IP Address" selected, and two input fields: "IP Address" with the value "192 . 168 . 1 . 1" and "Subnet mask" with the value "255 . 255 . 255 . 255". The second section is for "Destination address:" and contains a dropdown menu with "A specific IP Subnet" selected, and two input fields: "IP address" with the value "192 . 168 . 123 . 0" and "Subnet mask" with the value "255 . 255 . 255 . 0". At the bottom of the dialog, there is a checkbox labeled "Mirrored. Also match packets with the exact opposite source and destination addresses." which is currently unchecked. At the very bottom are "OK" and "Cancel" buttons.

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.



The image shows a Windows-style dialog box titled "Filter Properties". It has a blue title bar with a question mark icon and a close button (X). The dialog contains three tabs: "Addressing", "Protocol", and "Description". The "Protocol" tab is currently selected. Inside the "Protocol" tab, there is a section titled "Select a protocol type:" with a dropdown menu showing "Any" and a small arrow button. Below this is a text box containing the number "0". Further down is a section titled "Set the IP protocol port:" which contains four radio button options: "From any port" (selected), "From this port:", "To any port", and "To this port:". Each of the last three options has an associated empty text box. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Filter Properties

Addressing Protocol Description

Select a protocol type:

Any

0

Set the IP protocol port:

☒ From any port

☐ From this port:

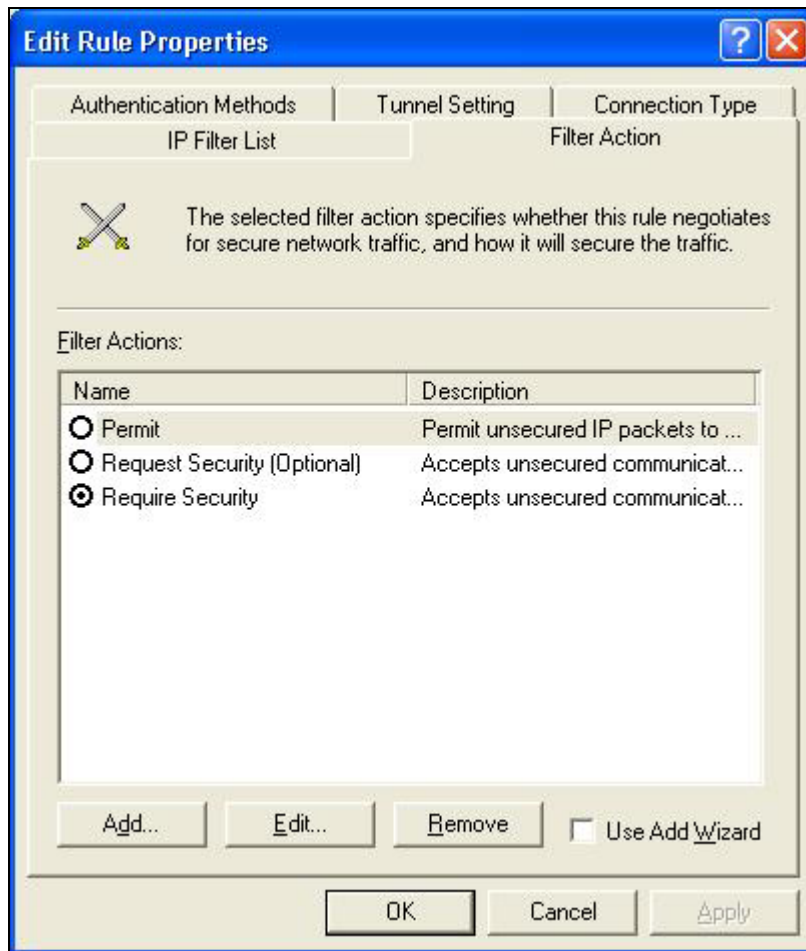
☐ To any port

☐ To this port:

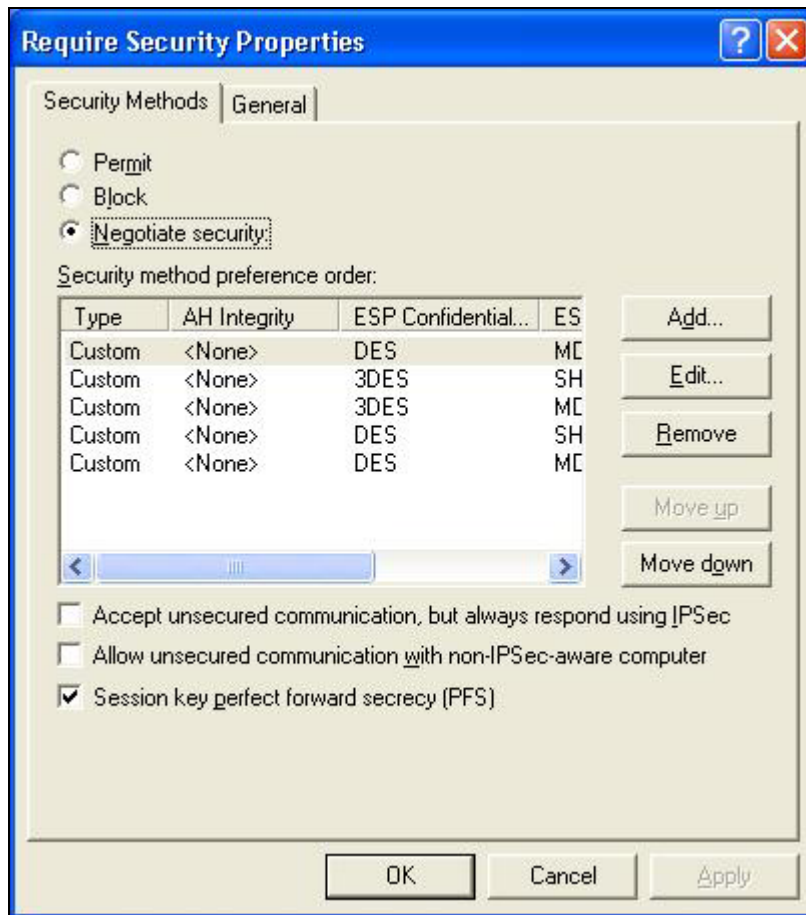
OK Cancel

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



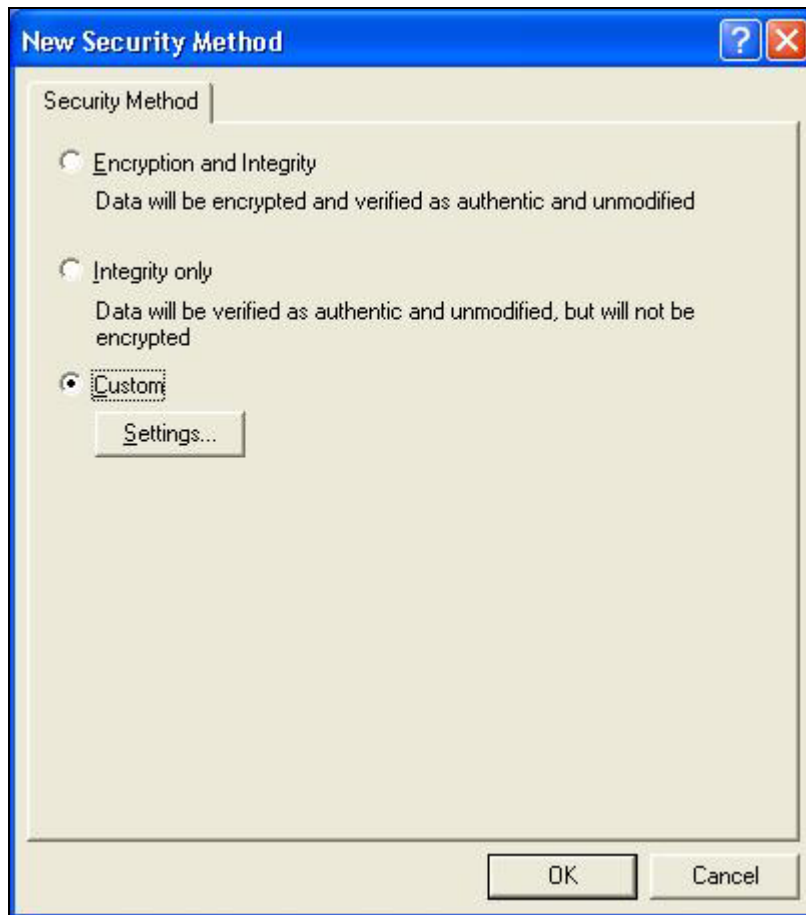


select **[Filter Action]**, select **[Require Security]**, then click **[Edit]** button.

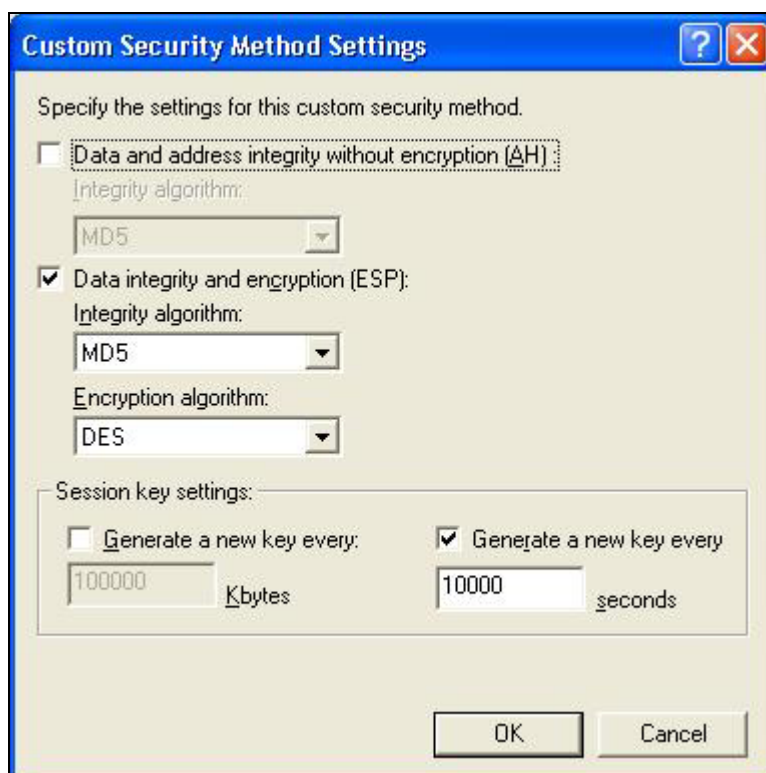


select **[Negotiate security]**, Select **[Session key Perfect Forward Secrecy (PFS)]**

click **[Edit]** button.



select [Custom] button



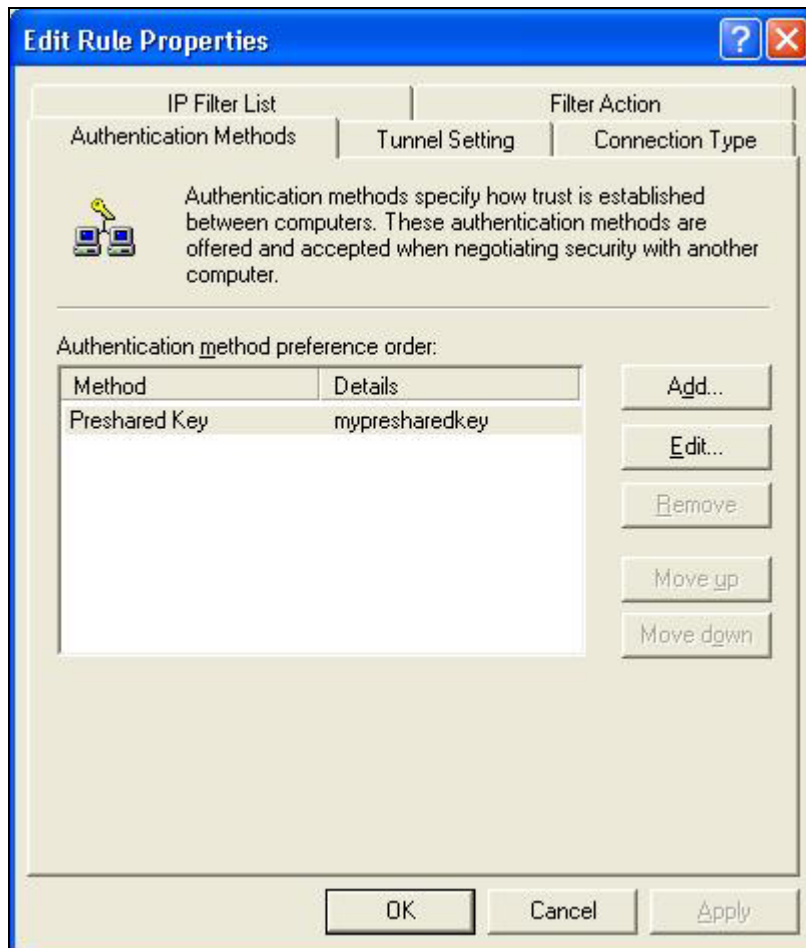
Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

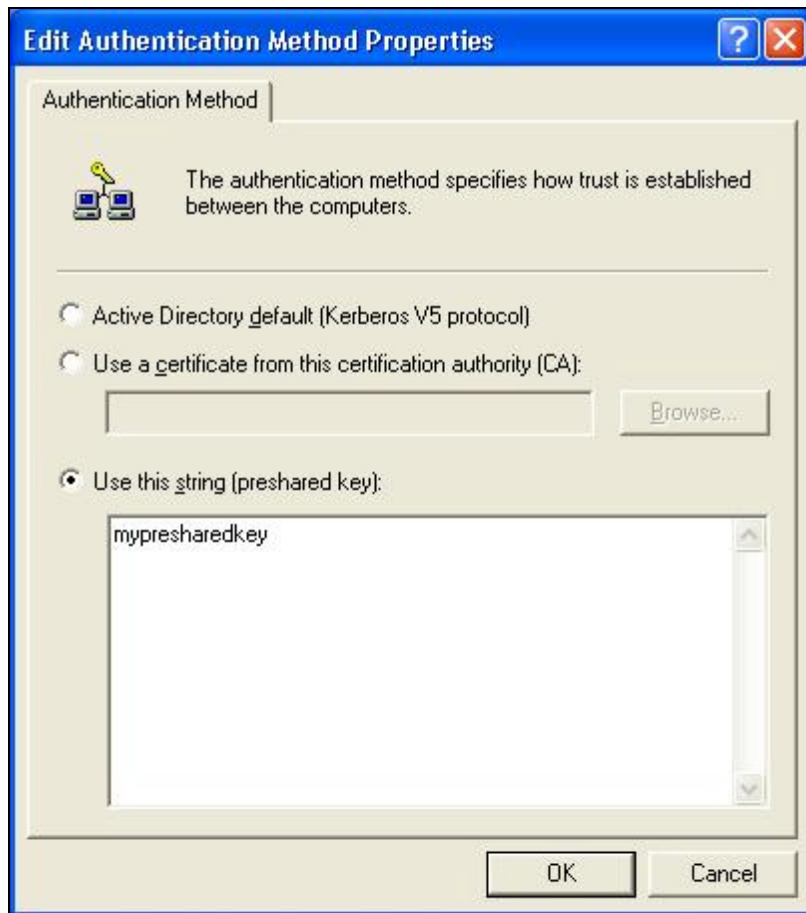
Configure “**Encryption algorithm**”: **[DES]**

Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button

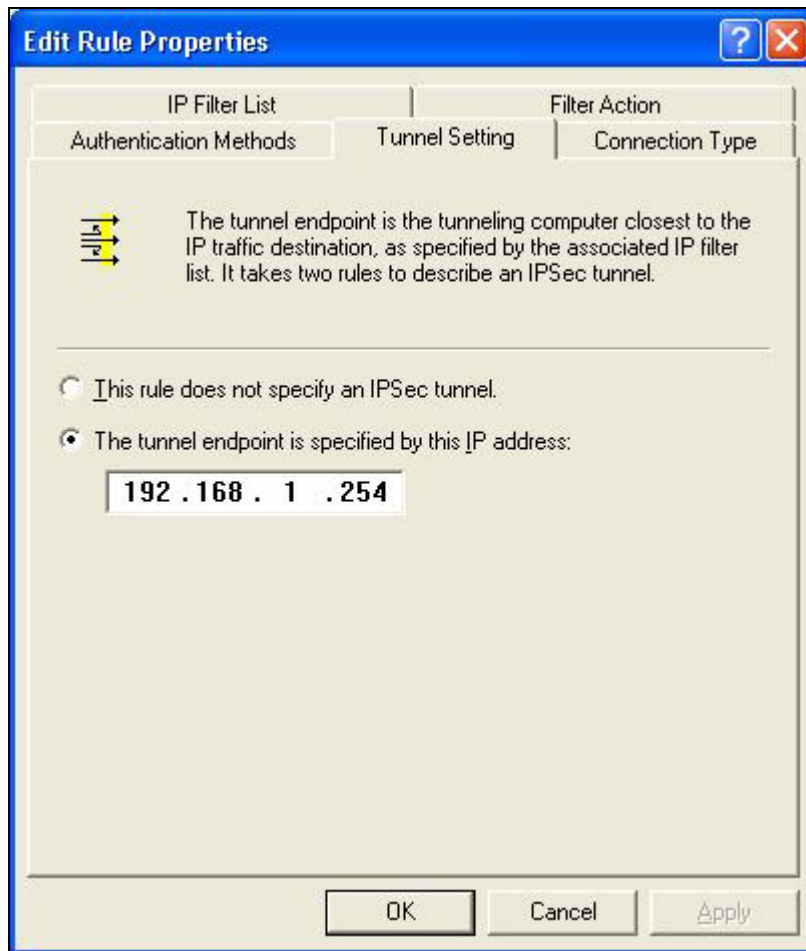


select **[Authentication Methods]** page, click **[Add]** button.



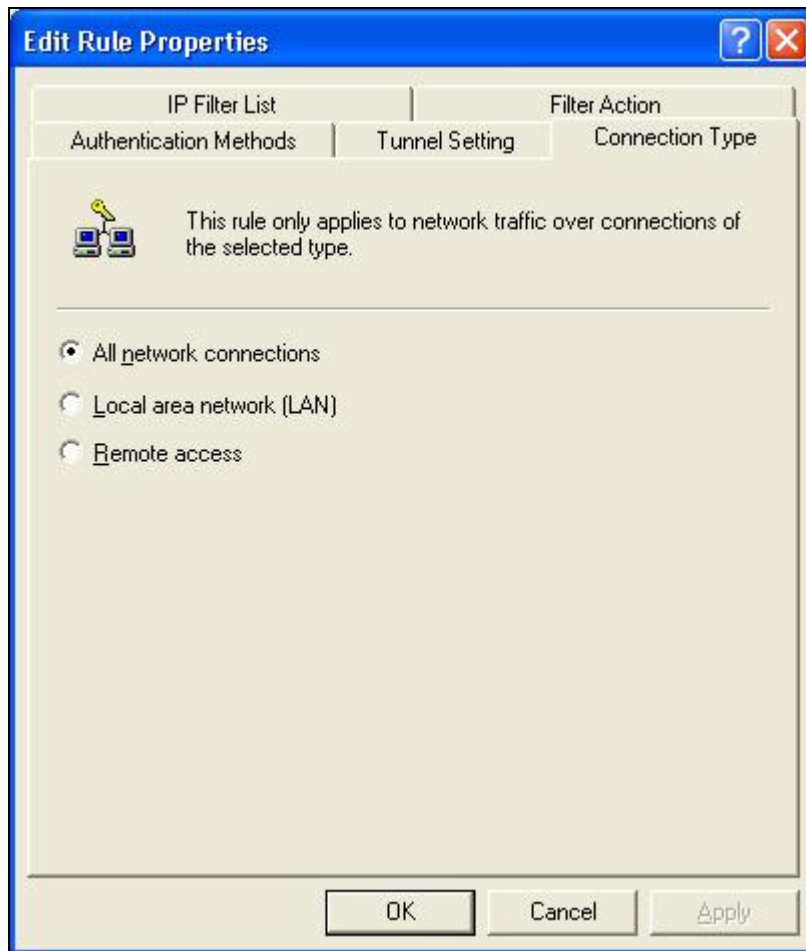
select **[Use this string to protect the key exchange (preshared key)]**, and enter your preshared key string, such as **mypresharedkey**. Click **[OK]** button. Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



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

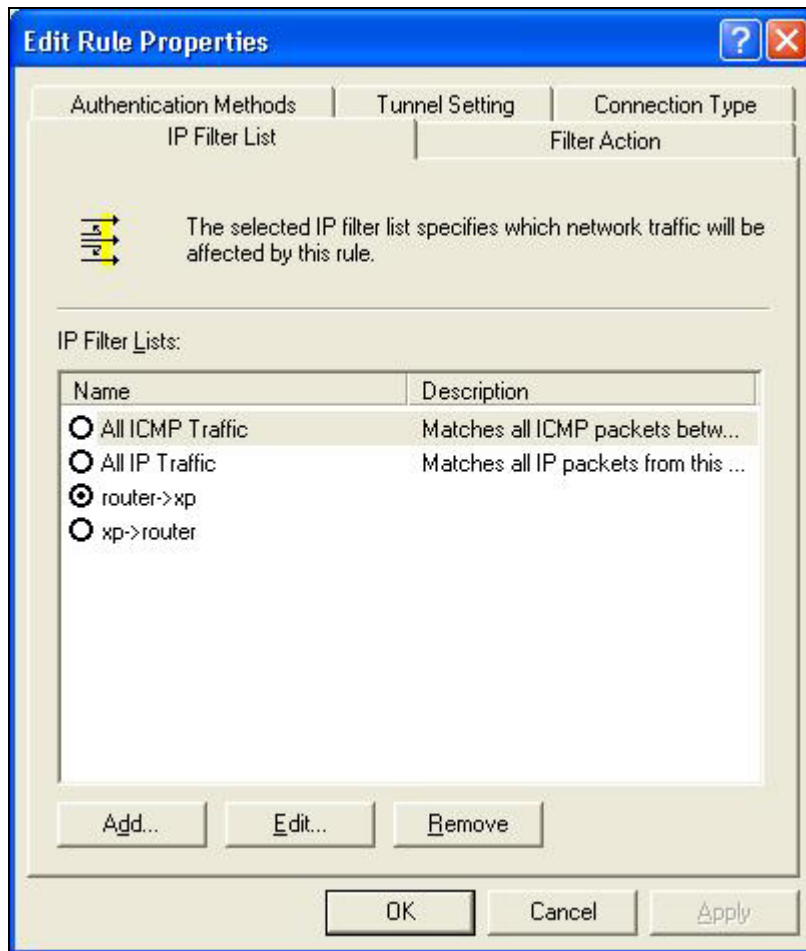
Select [Connection Type]



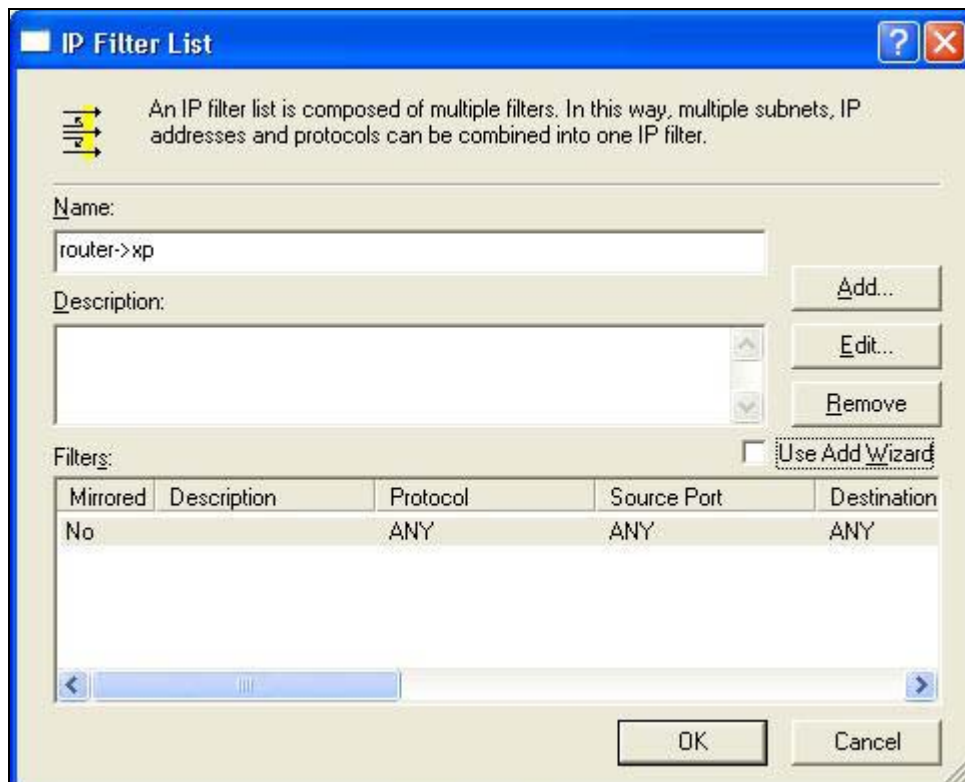
select **[All network connections]**

#### **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.

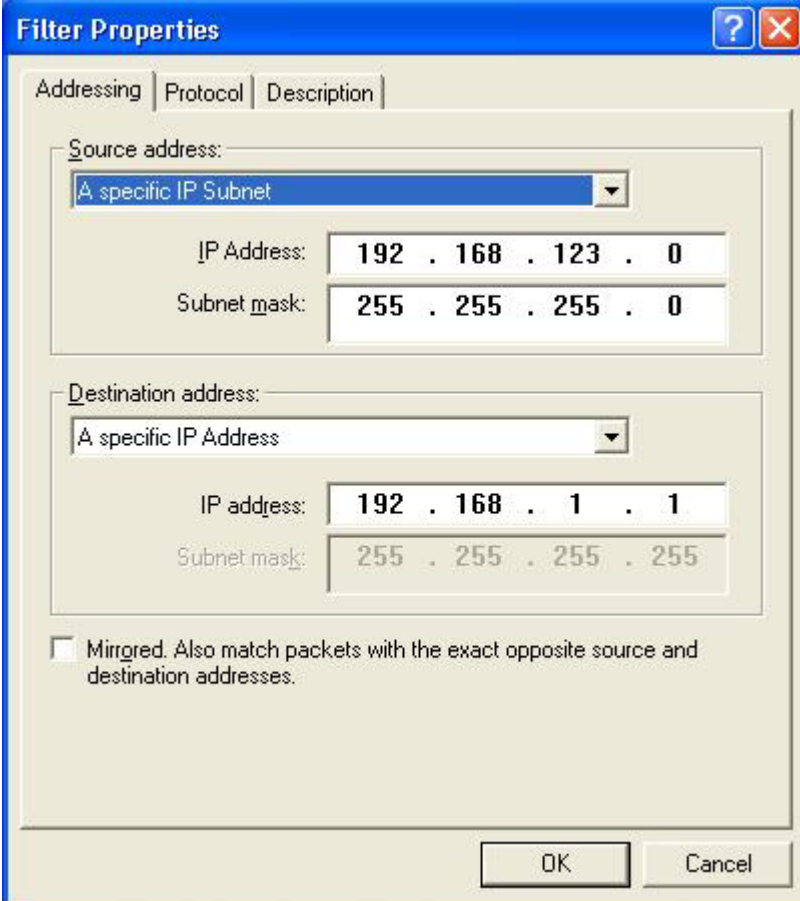


click [Add] button





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

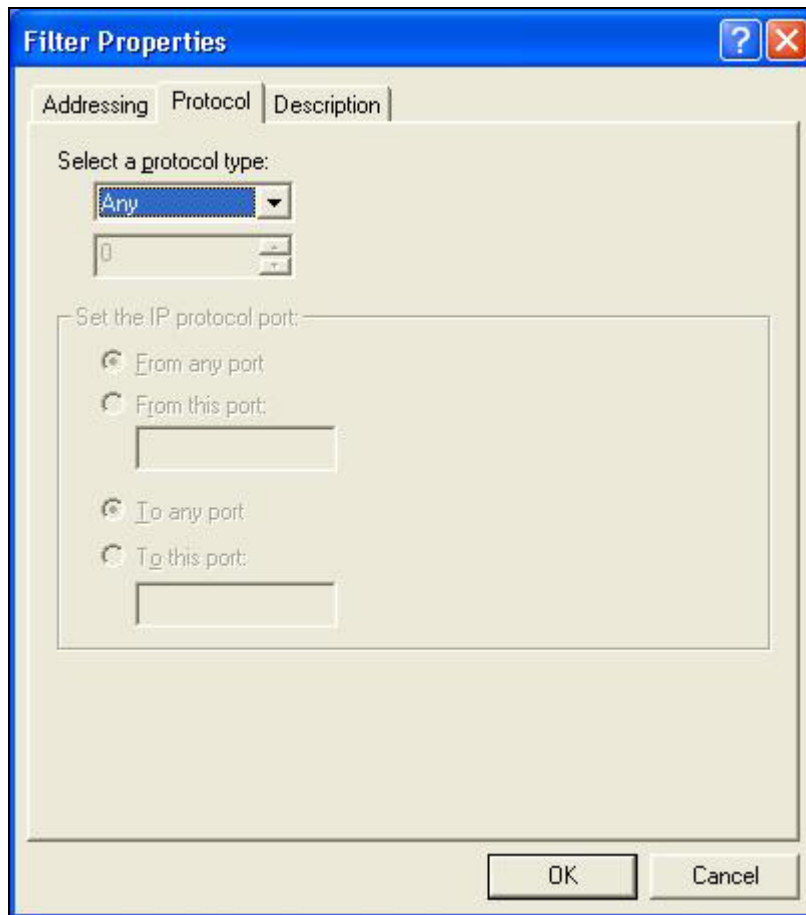


The image shows a 'Filter Properties' dialog box with three tabs: 'Addressing', 'Protocol', and 'Description'. The 'Addressing' tab is selected. It contains two main sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu is set to 'A specific IP Subnet'. Below it, the 'IP Address' field contains '192 . 168 . 123 . 0' and the 'Subnet mask' field contains '255 . 255 . 255 . 0'. In the 'Destination address' section, a dropdown menu is set to 'A specific IP Address'. Below it, the 'IP address' field contains '192 . 168 . 1 . 1' and the 'Subnet mask' field contains '255 . 255 . 255 . 255'. At the bottom of the dialog, there is an unchecked checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' and two buttons: 'OK' and 'Cancel'.

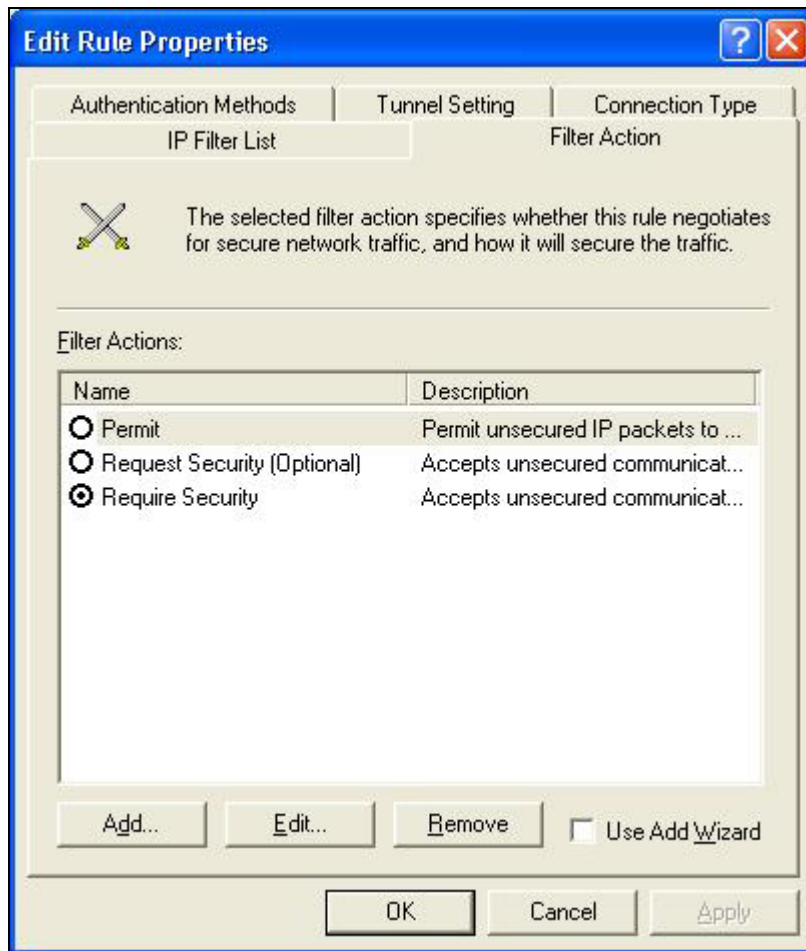
In the Source address field, select **[A specific IP Subnet]**. fill in  
IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

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

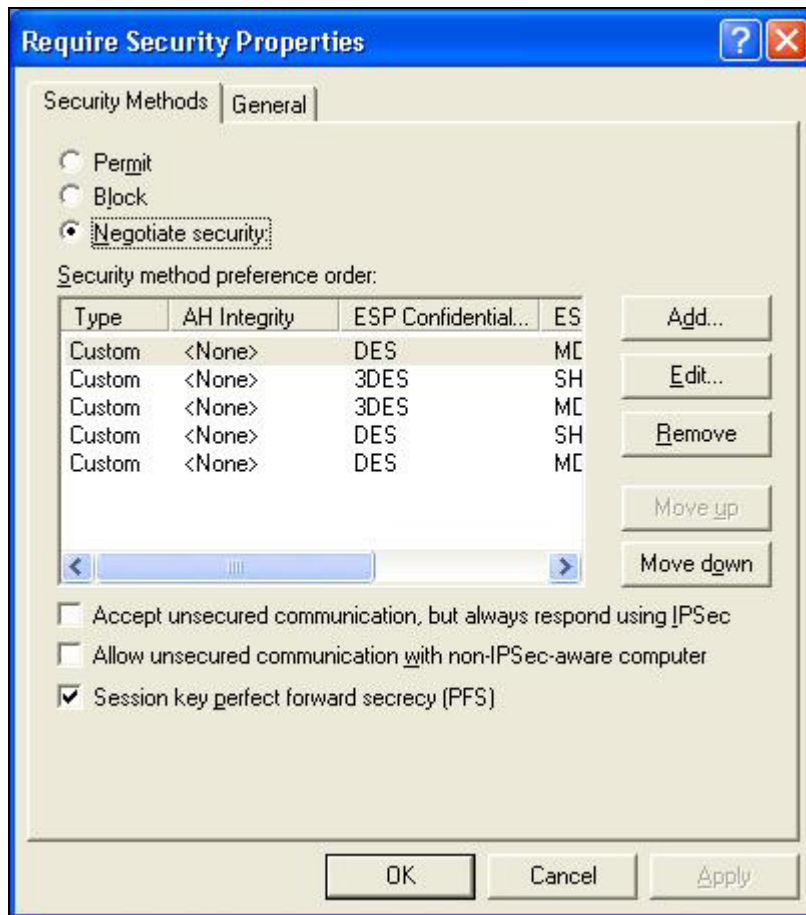
If you want to select a protocol for your filter, click **[Protocol]** page.



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

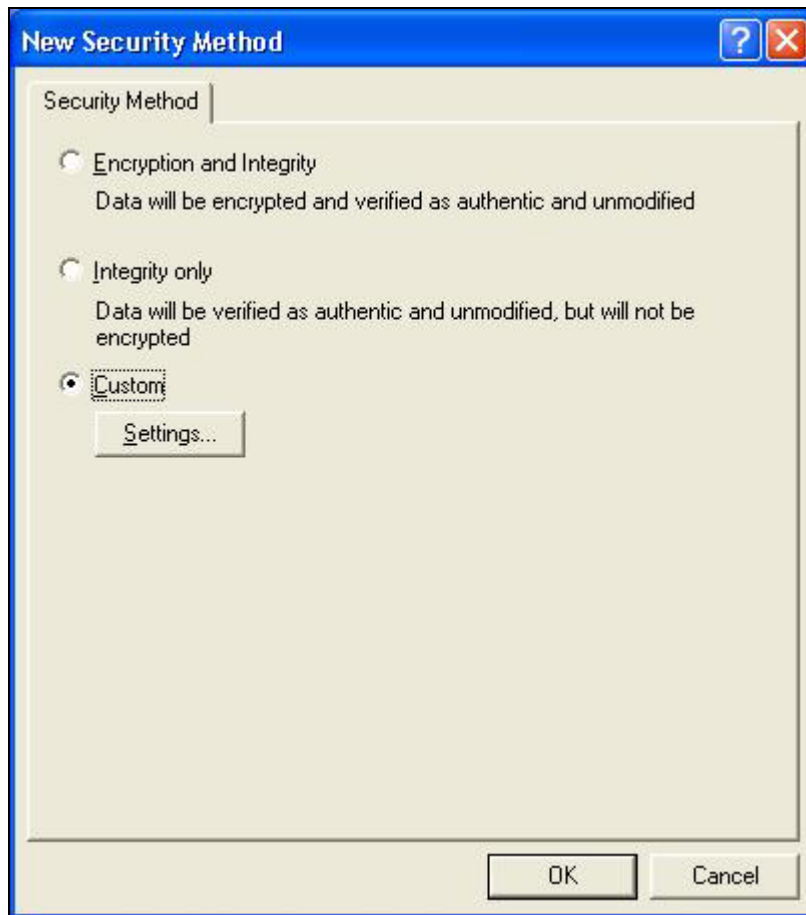


select [**Filter Action tab**], select [**Require Security**], then click [**Edit**] button.

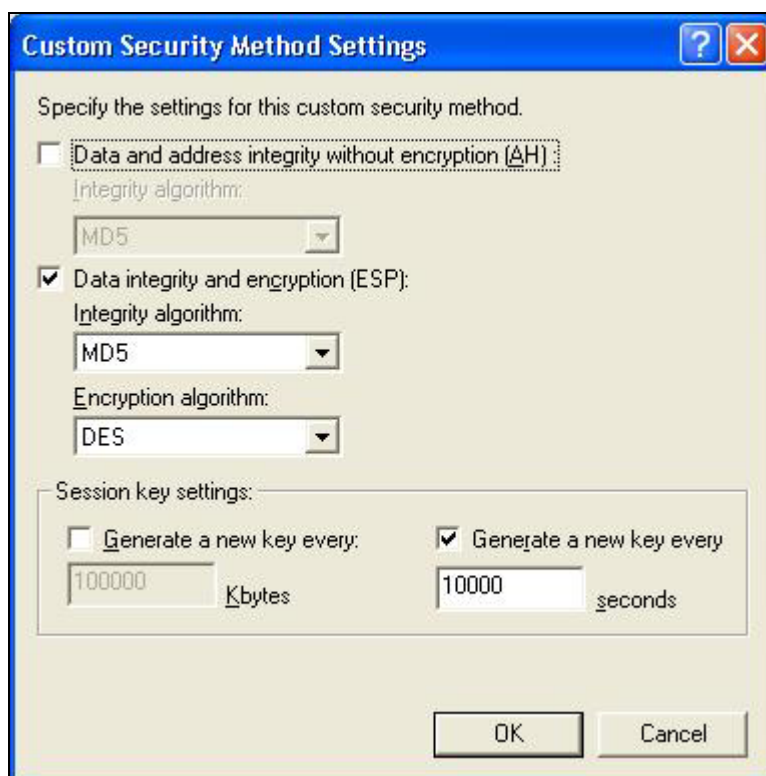


select **[Negotiate security]**, Select **[Session key Perfect Forward Secrecy (PFS)]**

click **[Edit]** button.



select [Custom] button



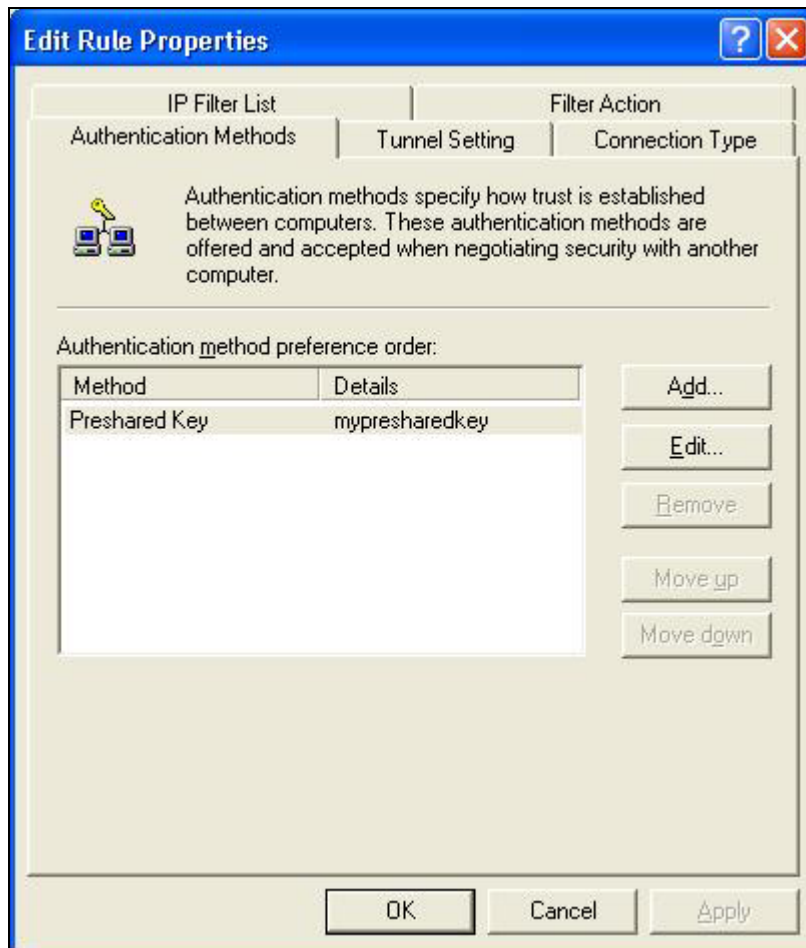
Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

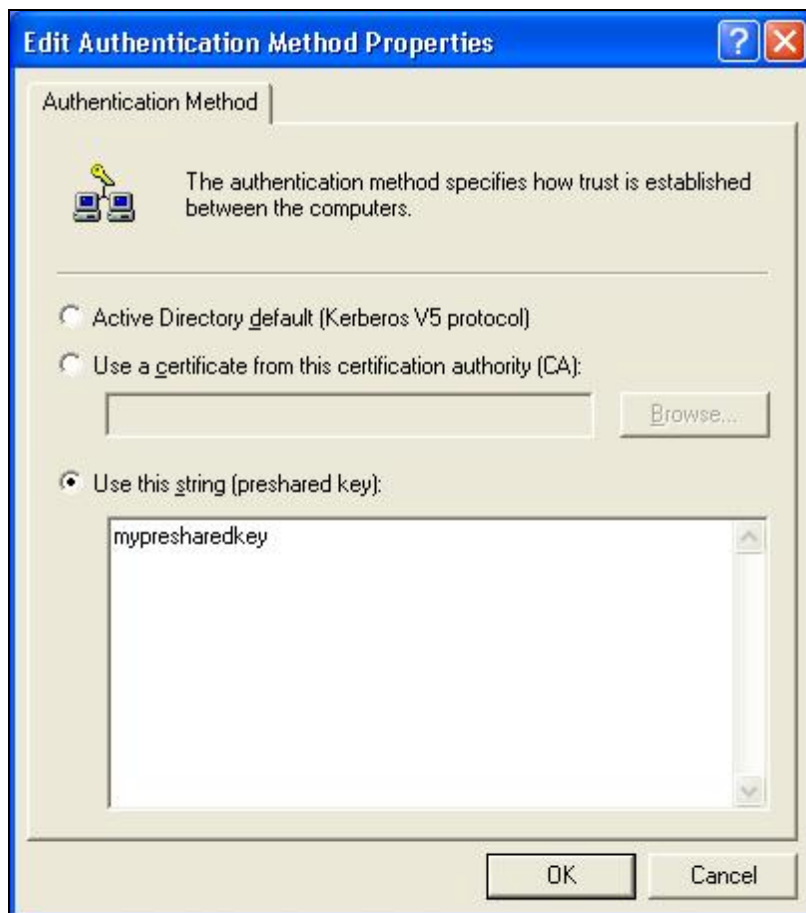
Configure “**Encryption algorithm**”: **[DES]**

Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button

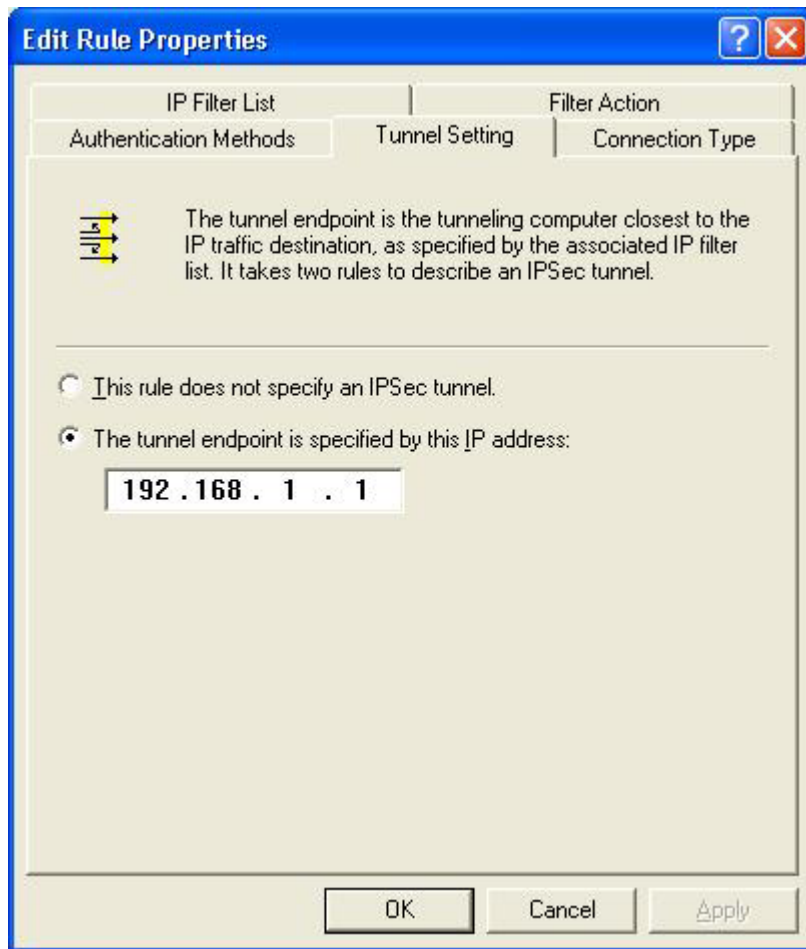


select **[Authentication Methods]** page, click **[Add]** button.



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.

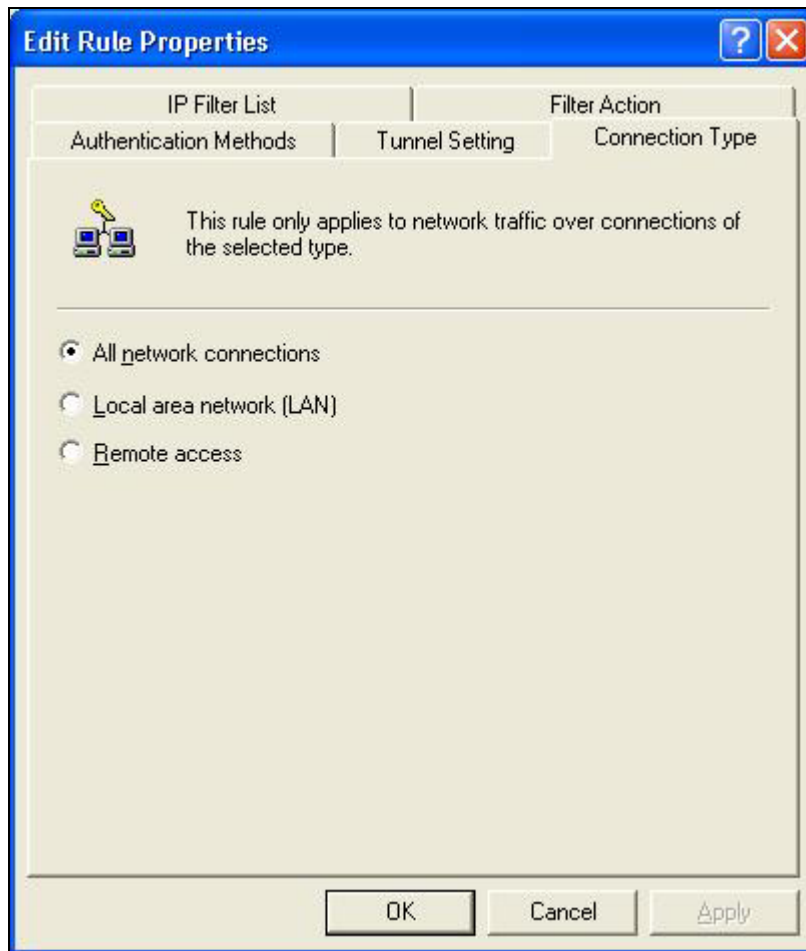
Select **[Tunnel Setting]**



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

Select [Connection Type]





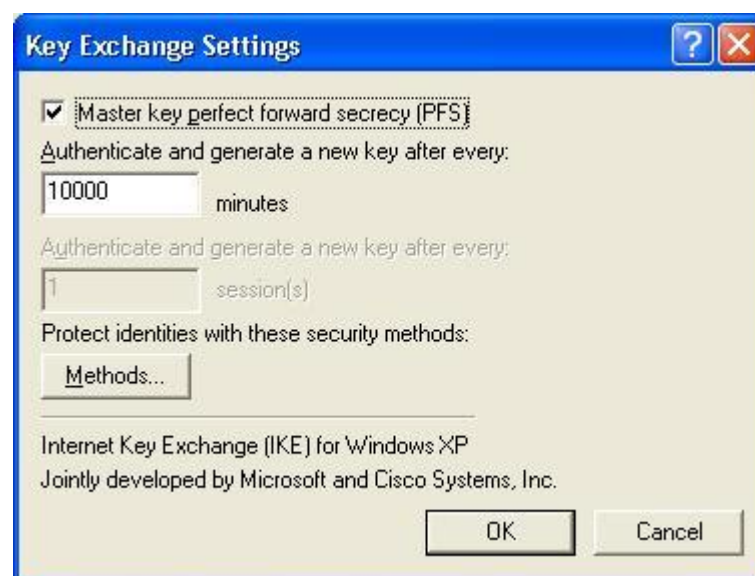
select **[All network connections]**

Configure IKE properties

Select [General]



Click [Advanced...]



enable “**Master key perfect forward security (PFS)**”

configure “**Authenticate and generate a new key after every [10000] seconds**”

click [**Methods...**]



click [**Add**] button



Configure “**Integrity algorithm**”: [**SHA1**]

Configure “**Encryption algorithm**”: [**3DES**]

Configure “**Diffie-Hellman 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

Multi-Functional Broadband NAT Router

**Administrator's Main Menu**

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- [Security Setting](#)
  - [Packet Filters](#)
  - [Domain Filters](#)
  - [MAC Control](#)
  - [VPN](#)
  - [Miscellaneous](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

### VPN Settings

| Item                     | Setting                                    |
|--------------------------|--|
| ▶ VPN                    | <input checked="" type="checkbox"/> Enable |
| ▶ Max. number of tunnels | <input type="text" value="2"/>             |

| ID | Tunnel Name                    | Method                                  |
|----|--------------------------------|---|
| 1  | <input type="text" value="1"/> | IKE <input type="button" value="More"/> |
| 2  | <input type="text"/>           | IKE <input type="button" value="More"/> |
| 3  | <input type="text"/>           | IKE <input type="button" value="More"/> |
| 4  | <input type="text"/>           | IKE <input type="button" value="More"/> |
| 5  | <input type="text"/>           | IKE <input type="button" value="More"/> |

### VPN Settings:

VPN: Enable

Max. number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Press "**More**" →

Multi-Functional Broadband NAT Router

### 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... |

No change!

Log out

### 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

Multi-Functional Broadband NAT Router

### VPN Settings - Tunnel 1 - Set IKE Proposal

**Administrator's Main Menu**

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- [Security Setting](#)
  - [Packet Filters](#)
  - [Domain Filters](#)
  - [MAC Control](#)
  - [VPN](#)
  - [Miscellaneous](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

| Item                 | Setting  |
|----------------------|--|
| ▶ IKE Proposal index | <input type="text" value="1"/> <input type="button" value="Remove"/> |

| ID | Proposal Name                  | DH Group  | Encrypt algorithm | Auth algorithm | Life Time | Life Time Unit |
|----|--------------------------------|-----------|-------------------|----------------|-----------|----------------|
| 1  | <input type="text" value="1"/> | Group 2 ▼ | 3DES ▼            | SHA1 ▼         | 10000     | Sec ▼          |
| 2  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 3  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 4  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 5  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 6  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 7  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 8  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 9  | <input type="text"/>           | Group 1 ▼ | 3DES ▼            | SHA1 ▼         | 0         | Sec ▼          |
| 10 | <input type="text"/>           | 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.



Multi-Functional Broadband NAT Router

### VPN Settings - Tunnel 1 - Set IPSec Proposal

**Administrator's Main Menu**

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- [Security Setting](#)
  - [Packet Filters](#)
  - [Domain Filters](#)
  - [MAC Control](#)
  - [VPN](#)
  - [Miscellaneous](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

Item:  [Remove](#)

| 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.

The screenshot shows a web-based interface for a "Multi-Functional Broadband NAT Router". The interface is divided into two main sections: a blue sidebar on the left for navigation and a white main area on the right for content.

**Administrator's Main Menu (Left Sidebar):**

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- [Toolbox](#)
  - [View Log](#)
  - [Firmware Upgrade](#)
  - [Backup Setting](#)
  - [Reset to Default](#)
  - [Reboot](#)
  - [Miscellaneous](#)

At the bottom of the sidebar is a "Log out" button.

**System Log (Right Main Area):**

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 (QRRESP) [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_NNT_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
```