

# Level1 router IPSec VPN vs. WinXP IPSec

**Level1 router is applicable to FBR-1407, FBR-1409TX, FBR-1417TX, WBR-2401, WBR-3403TX, WBR-3404TX and WBR-3402**

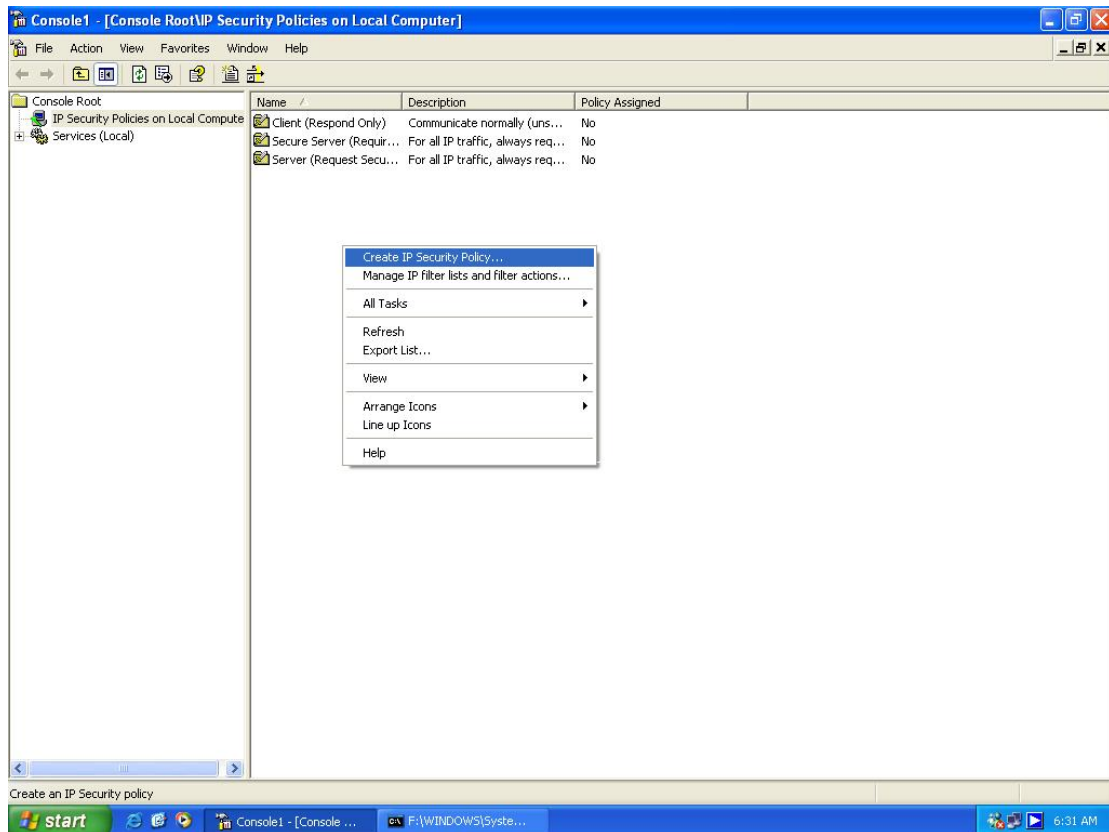
192.168.0.x---LevelOne VPN router---172.16.6.97---172.16.6.10 ---WinXP.

LevelOne Router LAN IP :192.168.0.1      WAN IP :172.16.6.97

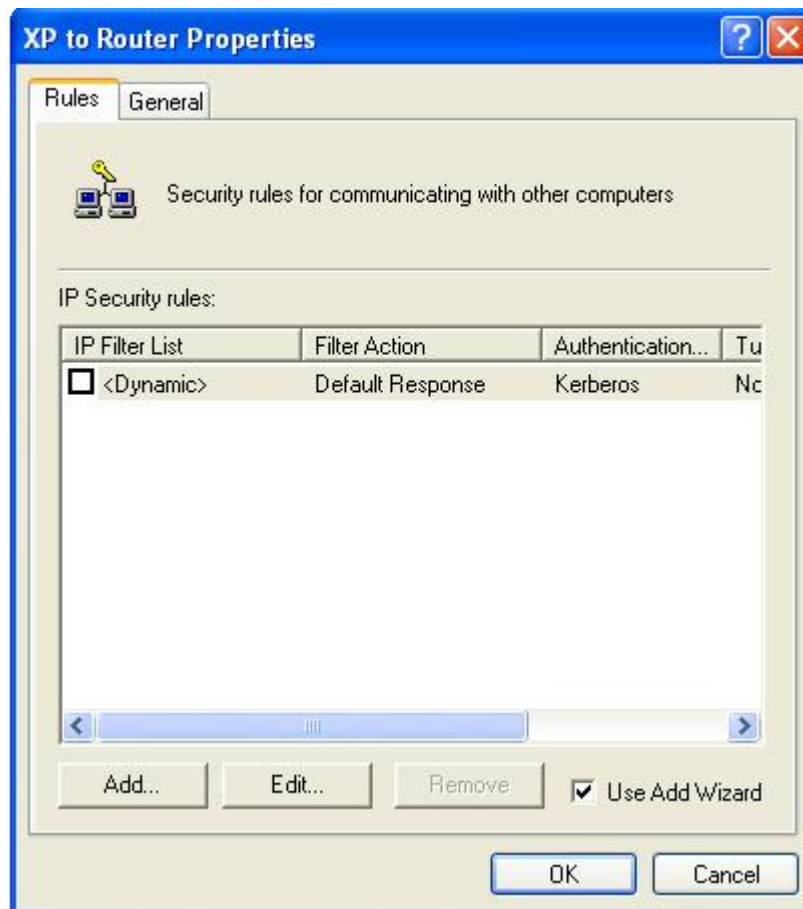
WinXP IP 172.16.6.10

## WinXP configuration



1. Select  $\diamond$  run  $\diamond$ secpol.msc
2. right click "IP Security Policy on Local Machine" Create IP Security Policy




3. click Next ◊ type policy name , for example XP to Router , click Next
4. Deselect “Active to default response rules”. Click Next , click finish .
5. click Add ◊ Next



## 6. Type Router WAN IP >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.

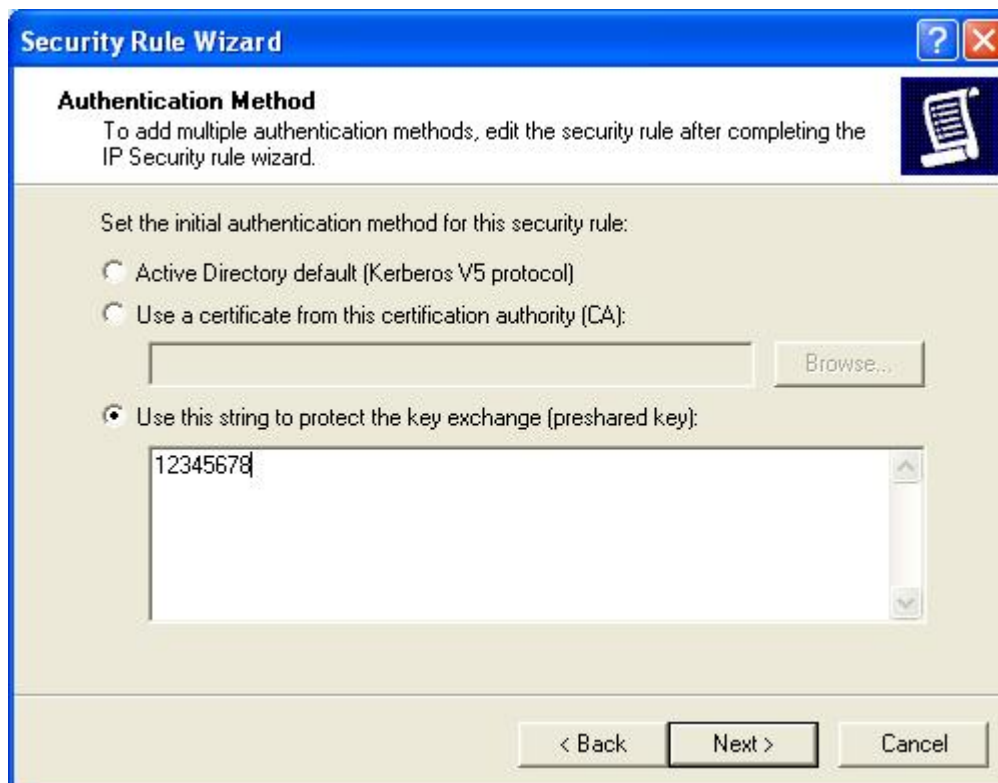
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

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:

< Back    Next >    Cancel

6. Network Type click Next , Authentication select Preshared Key , key 12345678  
◇Next



The screenshot shows the 'Security Rule Wizard' dialog box, specifically the 'Authentication Method' step. The title bar reads 'Security Rule Wizard' and includes help and close buttons. The main heading is 'Authentication Method' with a sub-instruction: 'To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.' Below this, the user is prompted to 'Set the initial authentication method for this security rule:'. Three radio button options are listed: 'Active Directory default (Kerberos V5 protocol)', 'Use a certificate from this certification authority (CA):', and 'Use this string to protect the key exchange (preshared key)'. The third option is selected. A text box next to the second option contains a 'Browse...' button. The selected option has a text box containing the string '12345678'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**Security Rule 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:

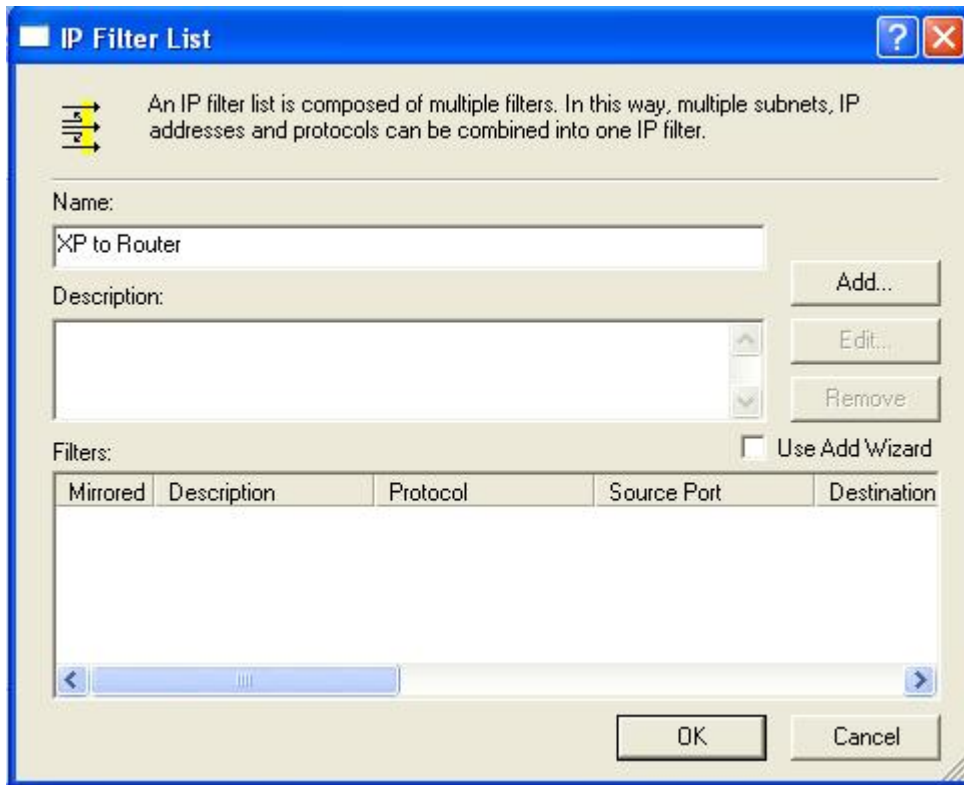
- Active Directory default (Kerberos V5 protocol)
- Use a certificate from this certification authority (CA):  
 - Use this string to protect the key exchange (preshared key):

< Back   Next >   Cancel

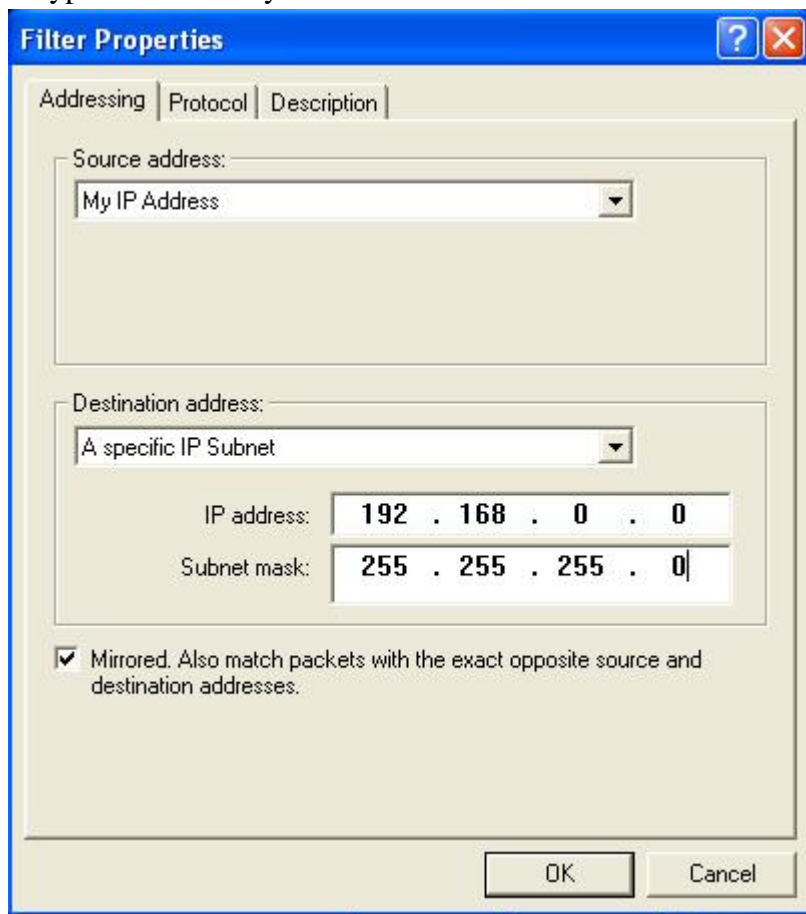
7. Click Add .



8.Type Name XP to Router , de-select Use Add Wizard ◊ Add



9.Type Source IP My IP Address and Destination IP Subnet. Click OK ◊Close .



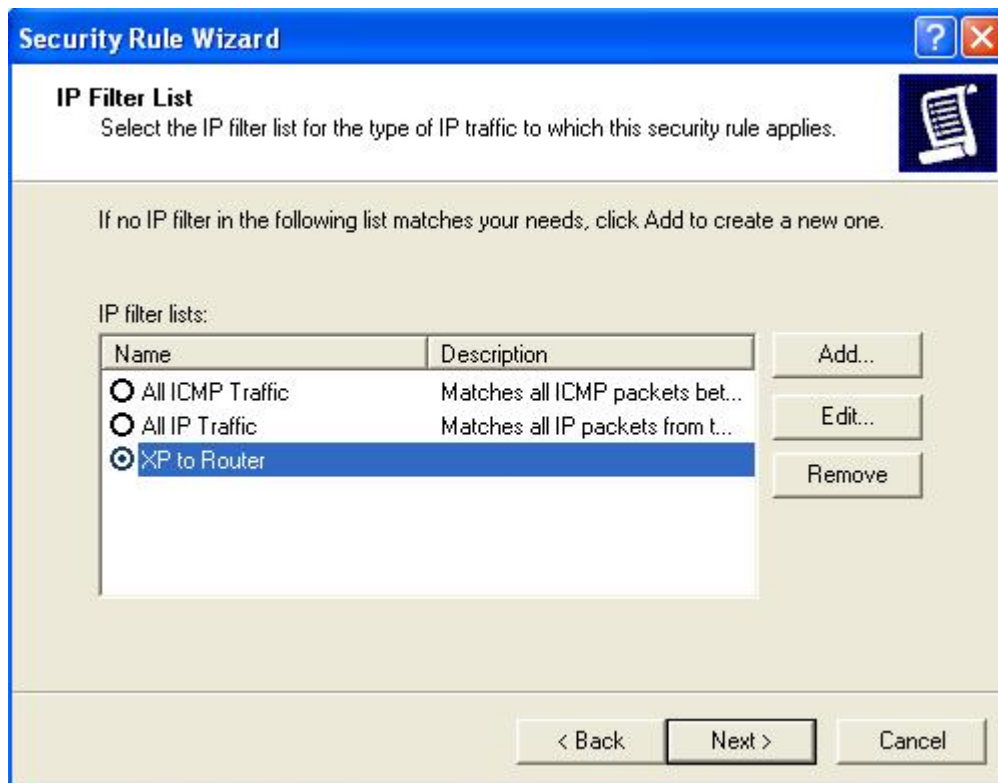
The image shows a 'Filter Properties' dialog box with a blue title bar containing a help icon and a close icon. The dialog has three tabs: 'Addressing', 'Protocol', and 'Description', with 'Addressing' selected. It contains two dropdown menus for 'Source address' (set to 'My IP Address') and 'Destination address' (set to 'A specific IP Subnet'). Below these are two rows of IP address fields: 'IP address' with the value '192 . 168 . 0 . 0' and 'Subnet mask' with the value '255 . 255 . 255 . 0'. A checked checkbox at the bottom is labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Source address:	My IP Address
Destination address:	A specific IP Subnet
IP address:	192 . 168 . 0 . 0
Subnet mask:	255 . 255 . 255 . 0

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

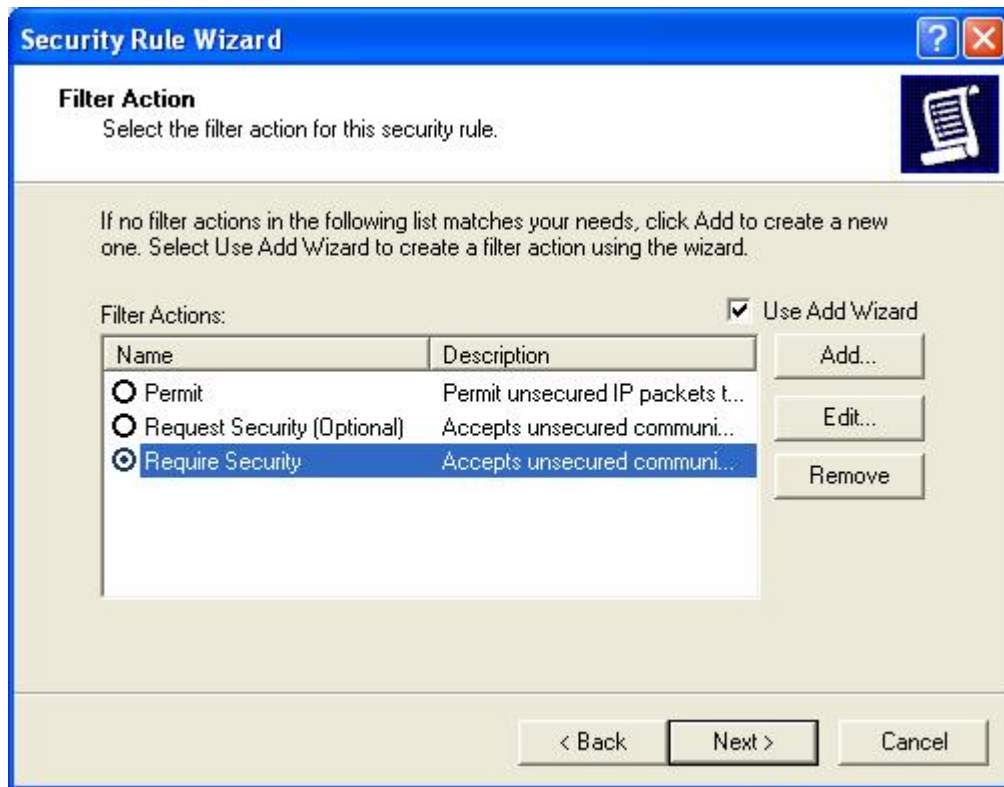
OK Cancel

10. Click XP to Router >Next

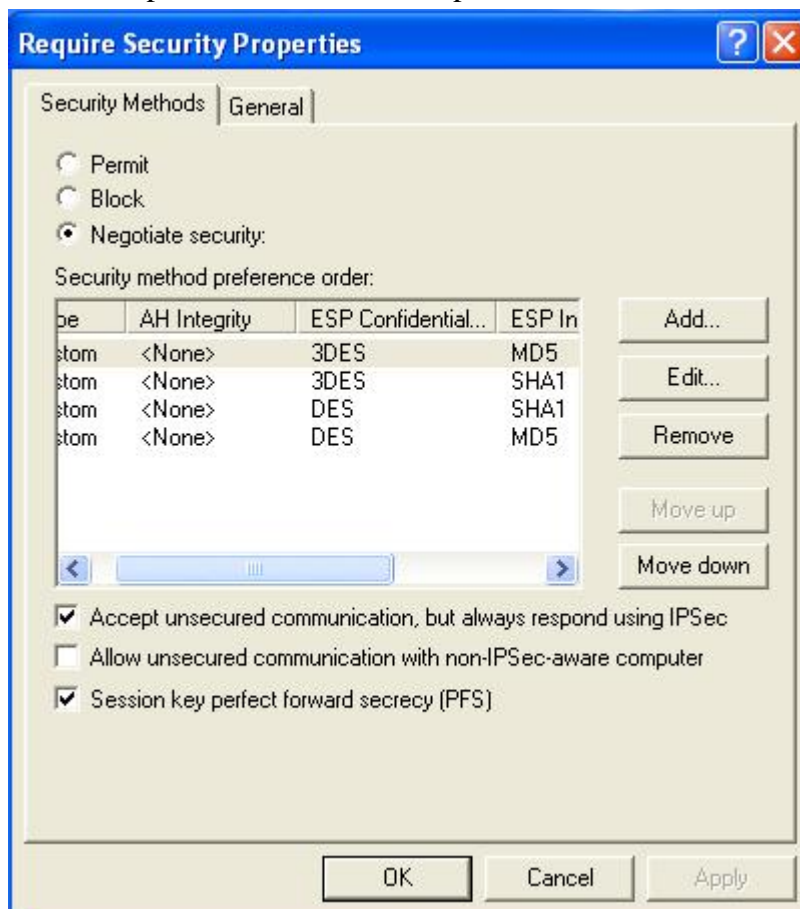




11. Click Require Security –edit .



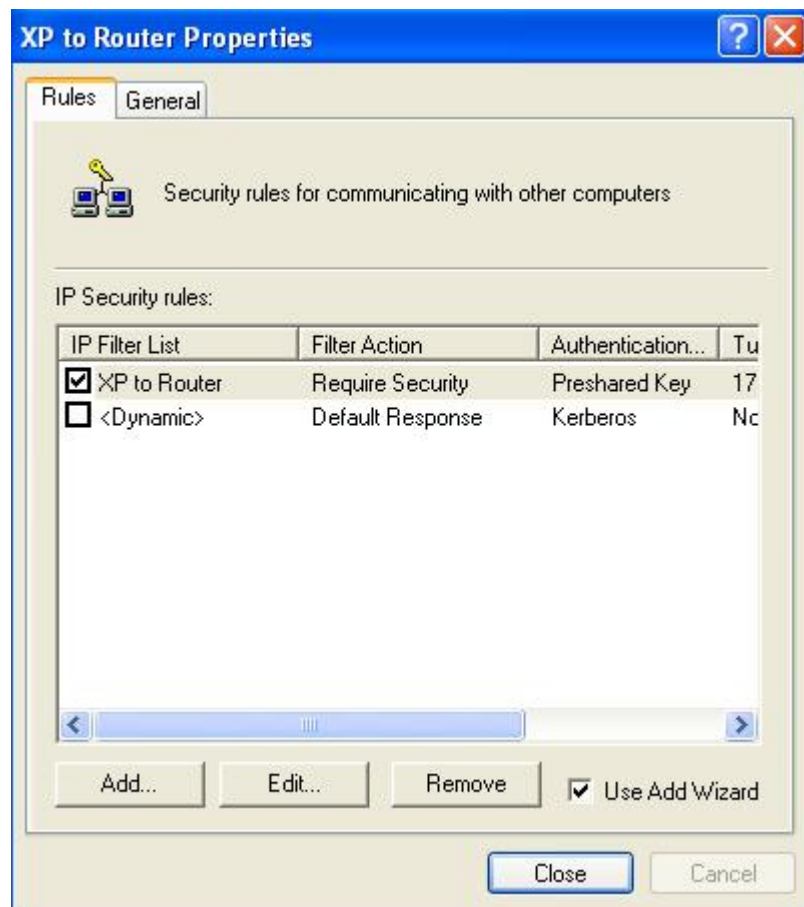
12. Move up 3DES with MD5 to top then back to 11 click next.



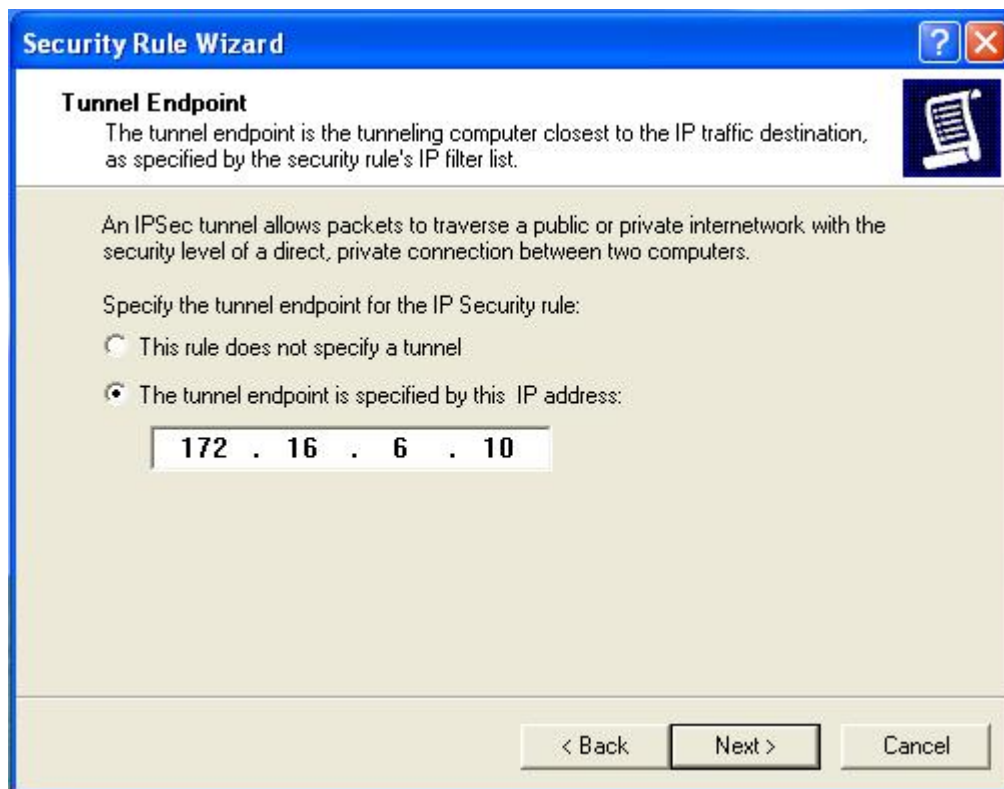
### 13. Click Finish



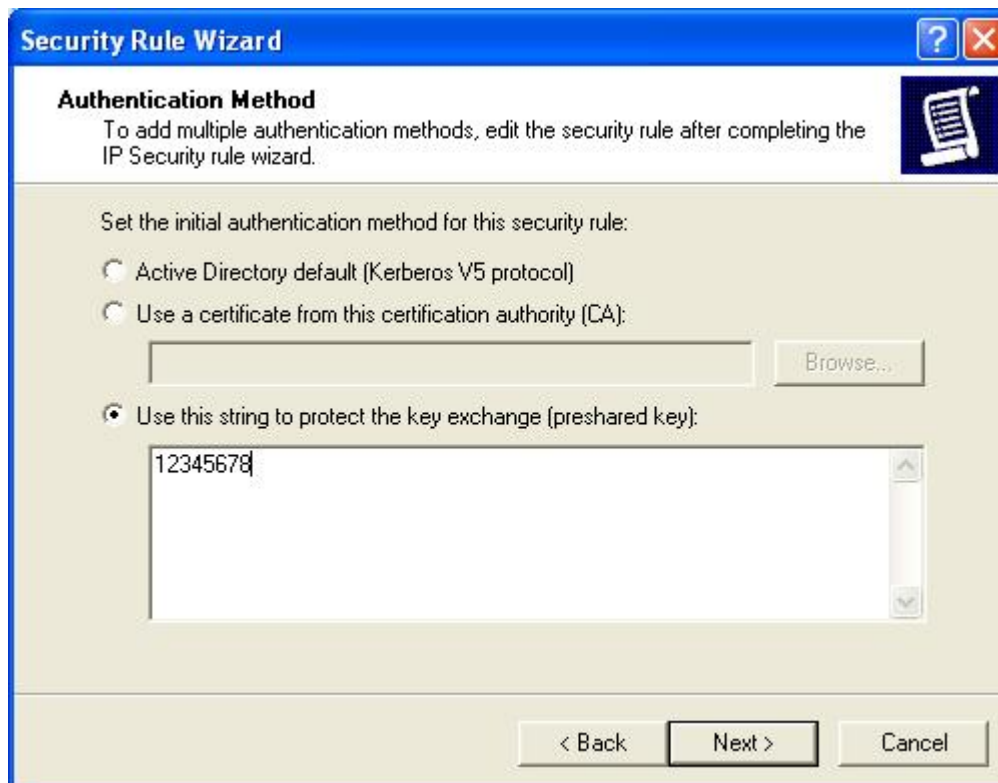
#### 14. Click Add



## 15.Type WinXP self IP Address



16. Click Next ◊ Authentication select Preshared Key , key 12345678 ◊ Next



The image shows a screenshot of the "Security Rule Wizard" dialog box. The title bar is blue and contains the text "Security Rule Wizard" along with help and close buttons. The main area has a light beige background. At the top left, the section is titled "Authentication Method" with a sub-instruction: "To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard." To the right of this text is a small icon of a document with a pencil. Below the instruction, the text reads "Set the initial authentication method for this security rule:". There are three radio button options: "Active Directory default (Kerberos V5 protocol)", "Use a certificate from this certification authority (CA):", and "Use this string to protect the key exchange (preshared key)". The third option is selected. Below the second option is an empty text box and a "Browse..." button. Below the selected option is a text box containing the string "12345678". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

**Security Rule 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:

- Active Directory default (Kerberos V5 protocol)
- Use a certificate from this certification authority (CA):  
 - Use this string to protect the key exchange (preshared key):

< Back    Next >    Cancel

## 17.IP Filter List click Add



18.Type name Router to XP , de-select Use Add Wizard . Add .

**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: Router to XP

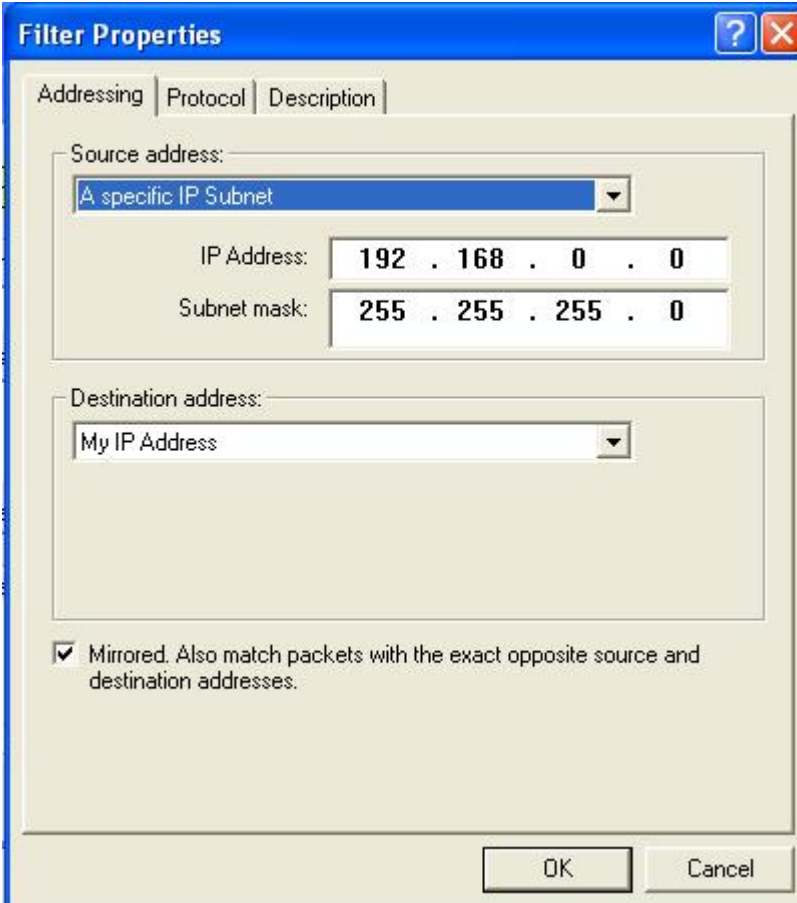
Description:

Filters:  Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
----------	-------------	----------	-------------	-------------

OK Cancel

## 19.Type Source and Destination IP.



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. The dialog is divided into three tabs: "Addressing", "Protocol", and "Description". The "Addressing" tab is selected. Under "Source address:", there is a dropdown menu with "A specific IP Subnet" selected. Below this are two input fields: "IP Address:" with the value "192 . 168 . 0 . 0" and "Subnet mask:" with the value "255 . 255 . 255 . 0". Under "Destination address:", there is a dropdown menu with "My IP Address" selected. At the bottom, there is a checked checkbox labeled "Mirrored. Also match packets with the exact opposite source and destination addresses." and two buttons: "OK" and "Cancel".

Filter Properties

Addressing | Protocol | Description

Source address:

A specific IP Subnet

IP Address: 192 . 168 . 0 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address:

My IP Address

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

OK Cancel



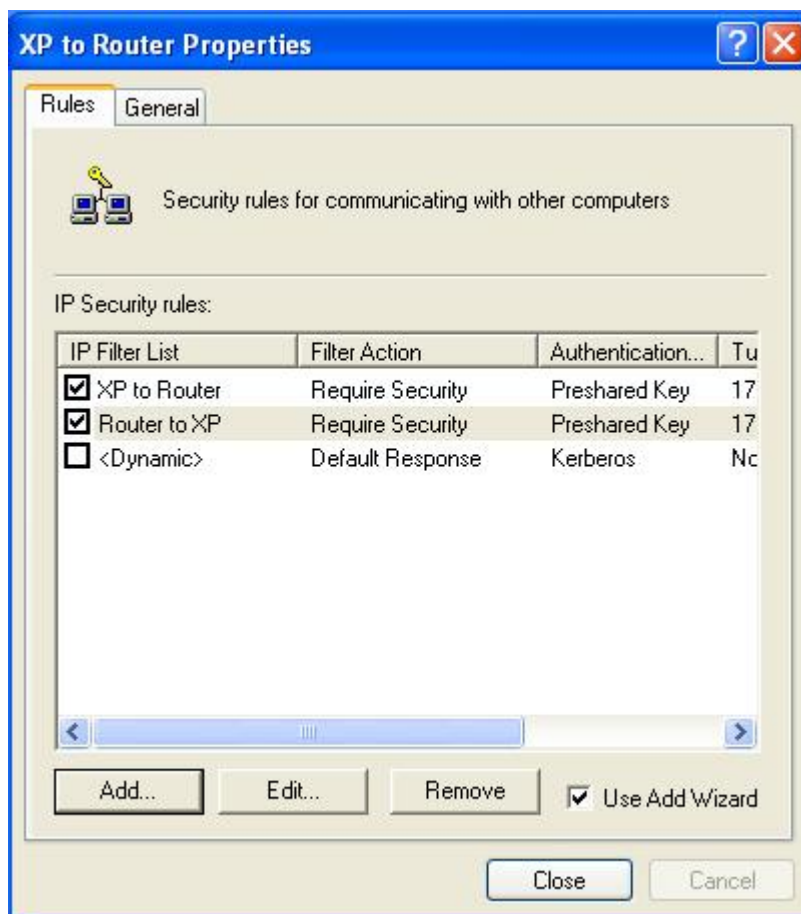
20.OK ◊Close , Click Router to XP ◊Next .



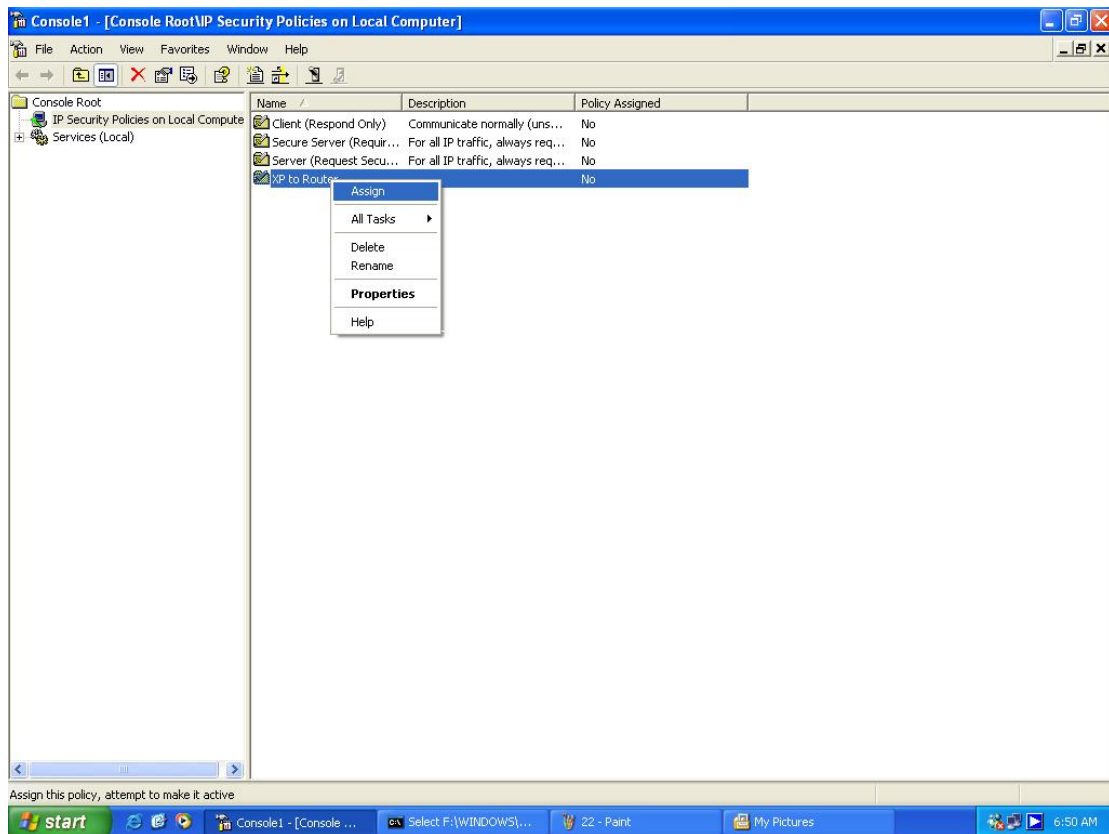
21. Click Require Security .



22. Click Finish ◊ Close .



### 23.Right click XP to Router Policy ◇Assign.

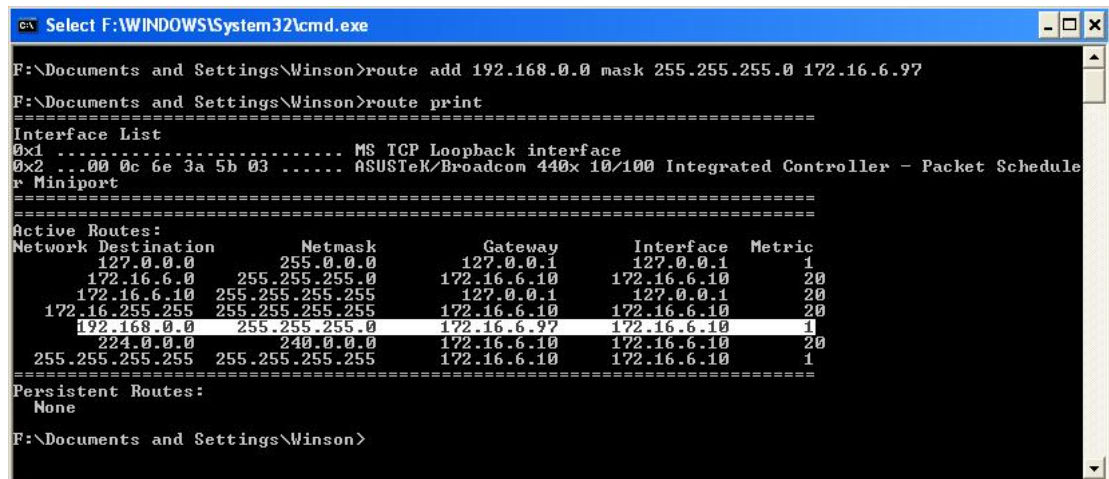


### 24.Type command as below

route add 192.168.0.0 mask 255.255.255.0 172.16.6.97

(Route add Router\_Lan\_subnet mask Router\_Lan\_mask Router\_WAN\_IP)

This step just only for testing when WinXP and WAN IP are both private IP.



## 25.Configure LevelOne VPN router

### System Status

Item	WAN Status	Sidenote
IP Address	172.16.6.97	Static IP
Subnet Mask	255.255.255.0	
Gateway	172.16.6.1	
Domain Name Server	168.95.1.1	

### VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	<input type="text" value="5"/>

ID	Tunnel Name	Method
1	<input type="text" value="WinXP"/>	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 - Tunnel 1 - IKE

Item	Setting
Tunnel Name	<input type="text" value="WinXP"/>
Local Subnet	<input type="text" value="192.168.0.0"/>
Local Netmask	<input type="text" value="255.255.255.0"/>
Remote Subnet	<input type="text" value="172.16.6.10"/>
Remote Netmask	<input type="text" value="255.255.255.255"/>
Remote Gateway	<input type="text" value="172.16.6.10"/>
Preshare Key	<input type="text" value="12345678"/>
IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>

**Item** **Setting**

↳ IKE Proposal index

test

Remove

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	test	Group 2	3DES	MD5	28800	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.

Proposal ID -- select one -- Add to Proposal index

**Item** **Setting**

↳ IPSec Proposal index

test

Remove

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	test	Group 2	ESP	3DES	MD5	28800	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.

Proposal ID -- select one -- Add to Proposal index



