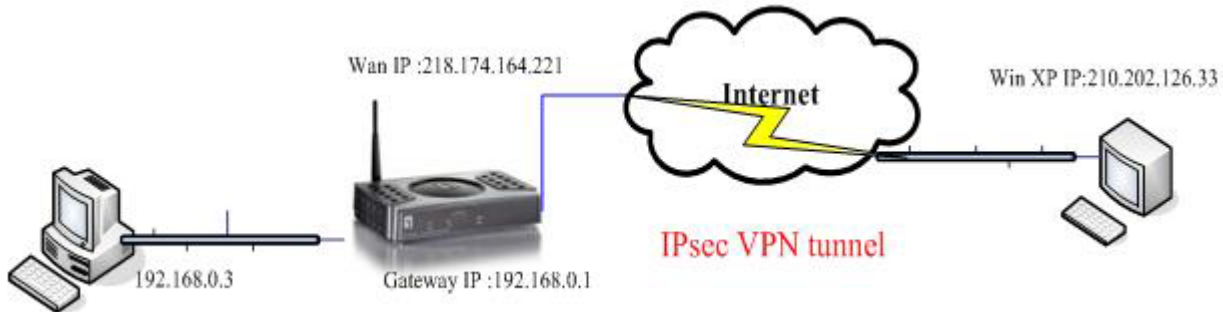




## WBR-3407TX IPsec VPN vs. WinXP IPsec VPN

### WBR-3407TX IPsec VPN policy settings

1. Basic structure:



2. WBR-3407A VPN Policy Reference settings :

## VPN - Auto Policy

**General** Policy Name: ADSLmodem  
Remote VPN Endpoint  
Address Type: Fixed IP Address  
Address Data: 210.202.126.33  
 NetBIOS Enable

**Local LAN** IP Address Subnet address  
IP address: 192 168 0 0  
Subnet Mask: 255 255 255 0

**Remote LAN** IP Address Single address  
IP address: 210 202 126 33  
Subnet Mask:

**IKE** Direction: Initiator and Responder  
Exchange Mode: Main Mode  
Diffie-Hellman (DH) Group: Group 2 (1024 Bit)  
Local Identity Type: WAN IP Address  
Data: n/a  
Remote Identity Type: IP Address  
Data: n/a

**SA Parameters** Encryption: 3DES  
Authentication: MD5  
Pre-shared Key: 12345678  
SA Life Time: 28800 (Seconds)  
 Enable PFS (Perfect Forward Security)

Back Save Cancel Help



LEVEL one  
one world one brand one level



3. VPN policy status :

## VPN Status

### Current VPN Tunnels (SAs)

Policy Name	Remote Endpoint	SPI (In)	SPI (Out)	Action
ADSLmodem	210.202.126.33	dd11a9d7	d4c53d49	<input type="button" value="Drop"/>

4. Ping to WBR-3407A LAN IP address.

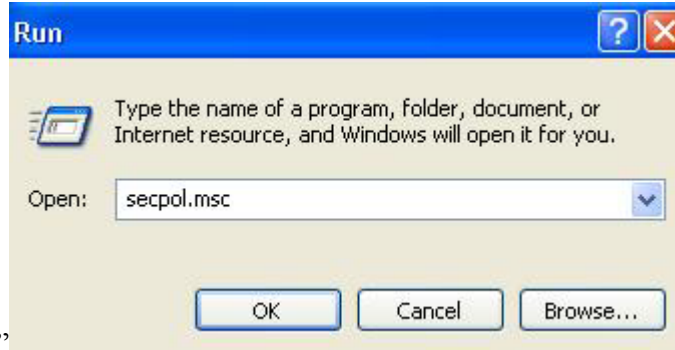
```
C:\Documents and Settings\alanh>ping 192.168.0.3 -t
Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time=96ms TTL=127
Reply from 192.168.0.3: bytes=32 time=97ms TTL=127
Reply from 192.168.0.3: bytes=32 time=129ms TTL=127
Reply from 192.168.0.3: bytes=32 time=99ms TTL=127
Reply from 192.168.0.3: bytes=32 time=96ms TTL=127
Reply from 192.168.0.3: bytes=32 time=109ms TTL=127
Reply from 192.168.0.3: bytes=32 time=96ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 96ms, Maximum = 129ms, Average = 103ms
Control-C
^C
C:\Documents and Settings\alanh>
```



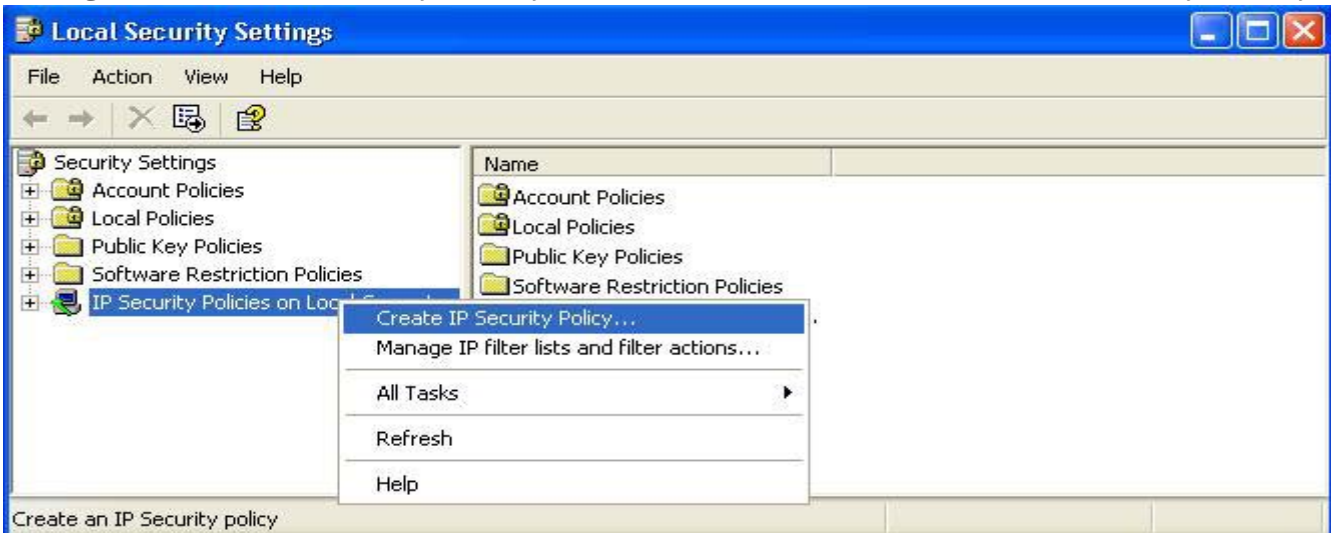
## WinXP IPsec settings

1. WinXP configuration:



Starts:\Run\ "Secpol.msc"

2. Right click "IP security Policy On local machine" and Create IP security Policy



3. Click Next button.





4. Create one policy name, and then click next.

**IP Security Policy Wizard**

**IP Security Policy Name**  
Name this IP Security policy and provide a brief description

Name:  
Winxp to VPNrouter

Description:

< Back   Next >   Cancel

5. Please Deselect “Active to default response rules”, then click “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.

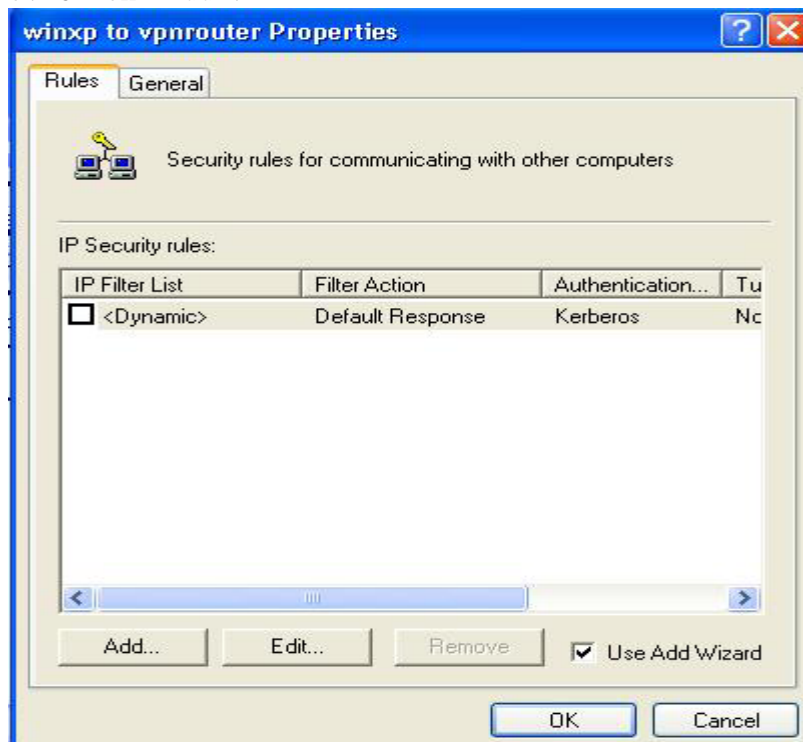
Activate the default response rule.

< Back   Next >   Cancel

6. Then Click “Finish”.



7. Click “Add”.

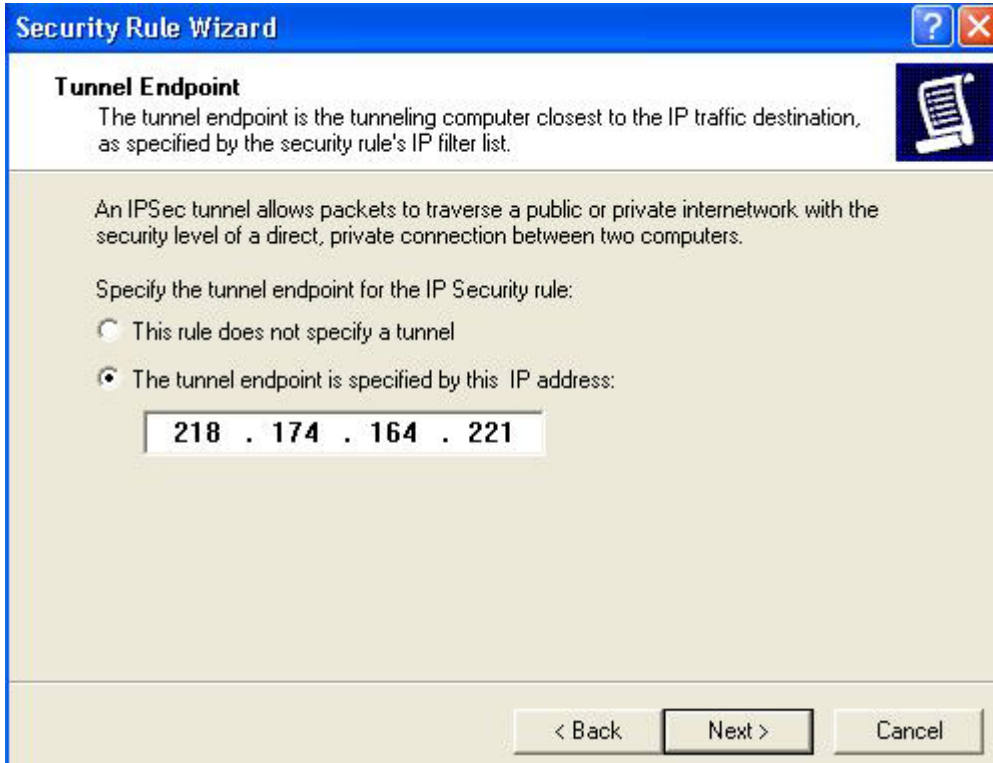




8. Click "Next".



9. Type WBR-3407A Wan IP address

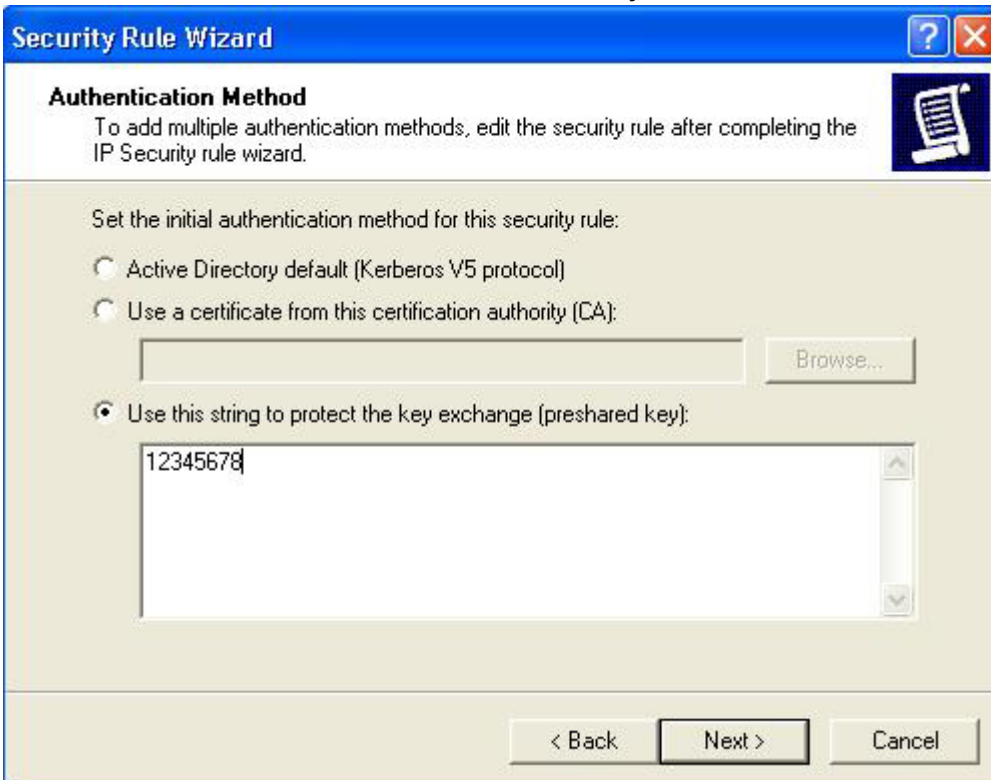




10. Choice Network Type.



11. Use the Authentication Preshared Key.

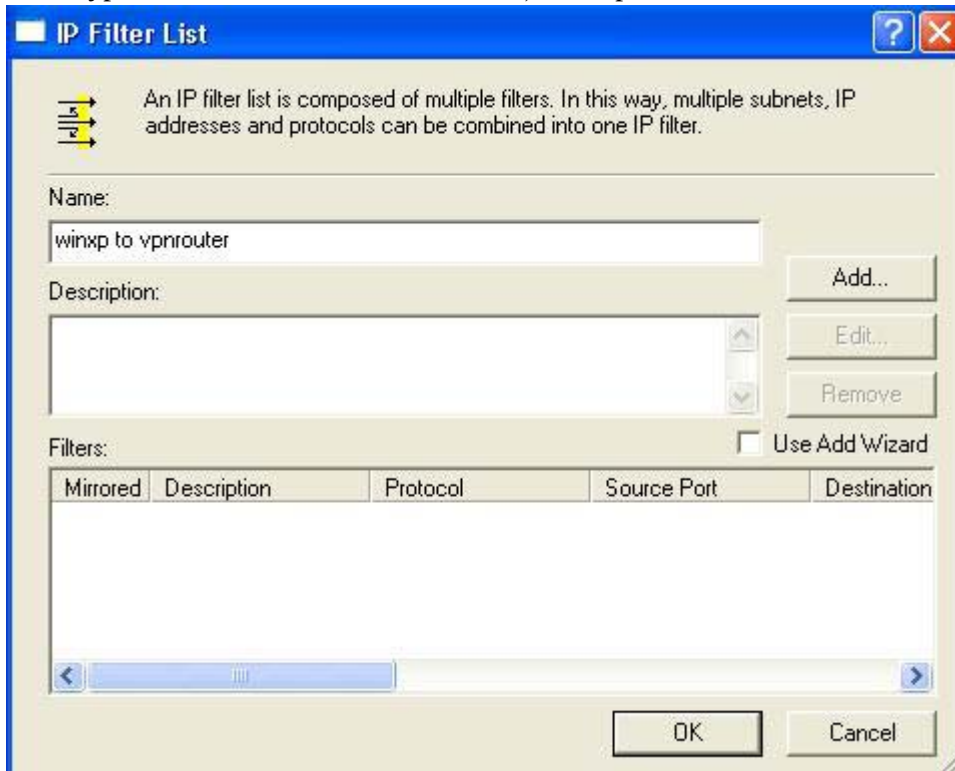




12. Click “Add” to set “IP Filter List”.



13. Type the IP Filter list Name, and please disable “Use Add Wizard”.







14. Type Source address->"My IP address", Destination address->"A specific IP Subnet".

**Filter Properties** [?] [X]

Addressing | Protocol | Description

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

15. Choice Winxp to vpnrouter, then click "Next".

**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:

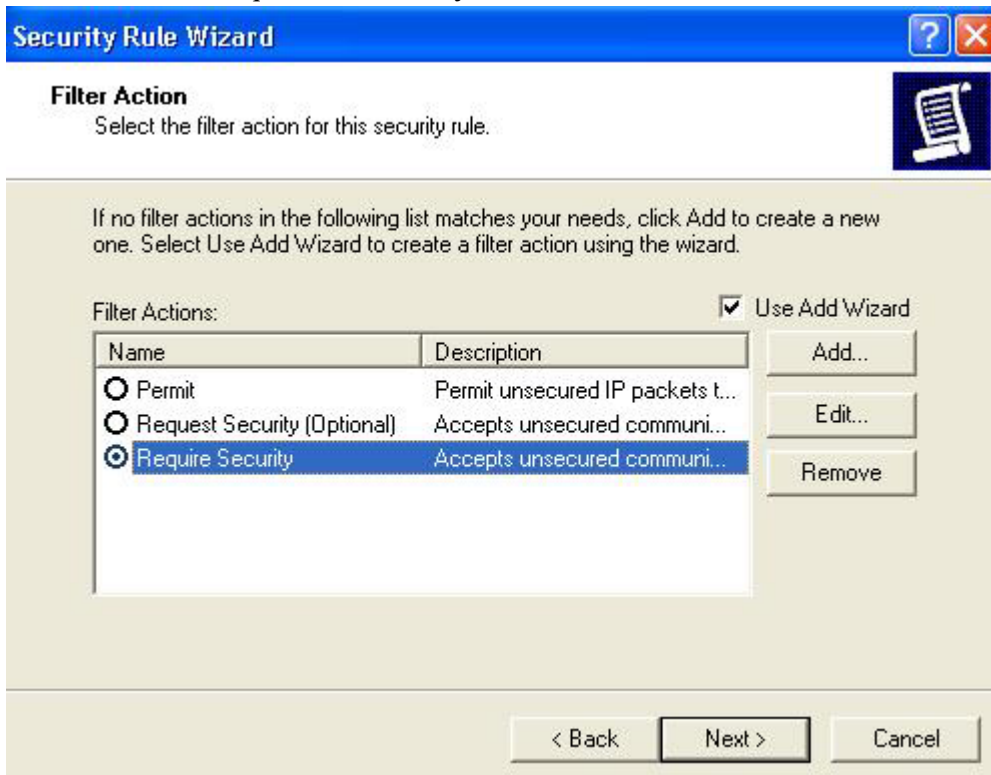
Name	Description
<input type="radio"/> All ICMP Traffic	Matches all ICMP packets bet...
<input type="radio"/> All IP Traffic	Matches all IP packets from t...
<input checked="" type="radio"/> winxp to vpnrouter	

Add... Edit... Remove

< Back Next > Cancel



16. To Edit “Require Security”.

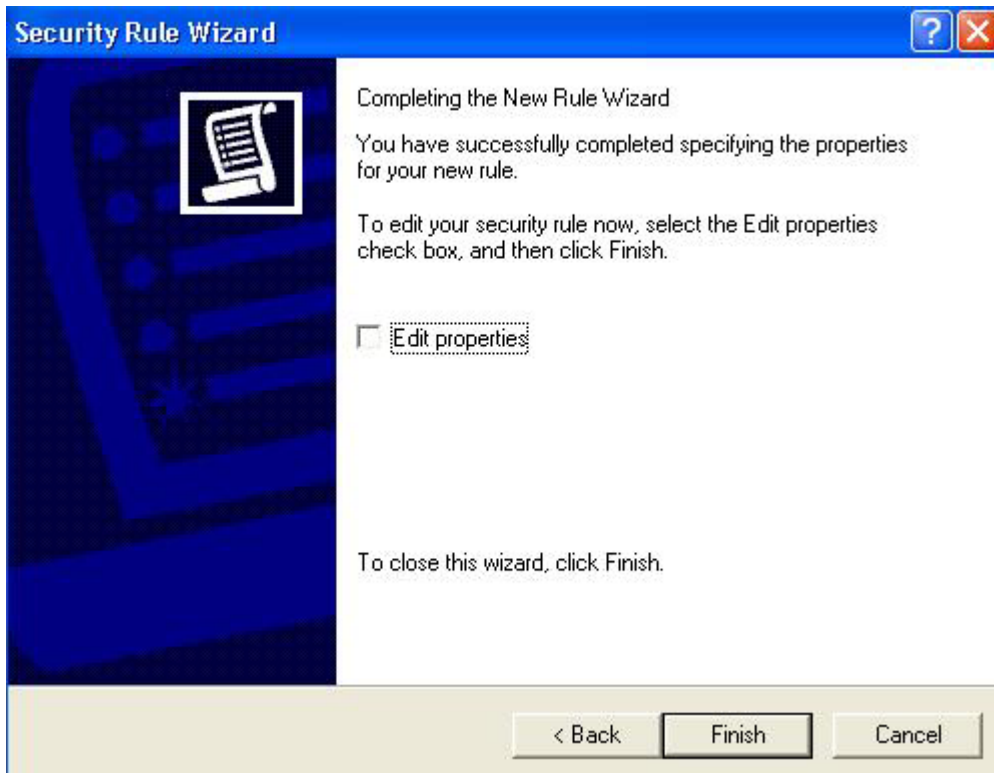


17. You can choice Security “3DES & MD5” to Move Up, and Enable “PFS”security.

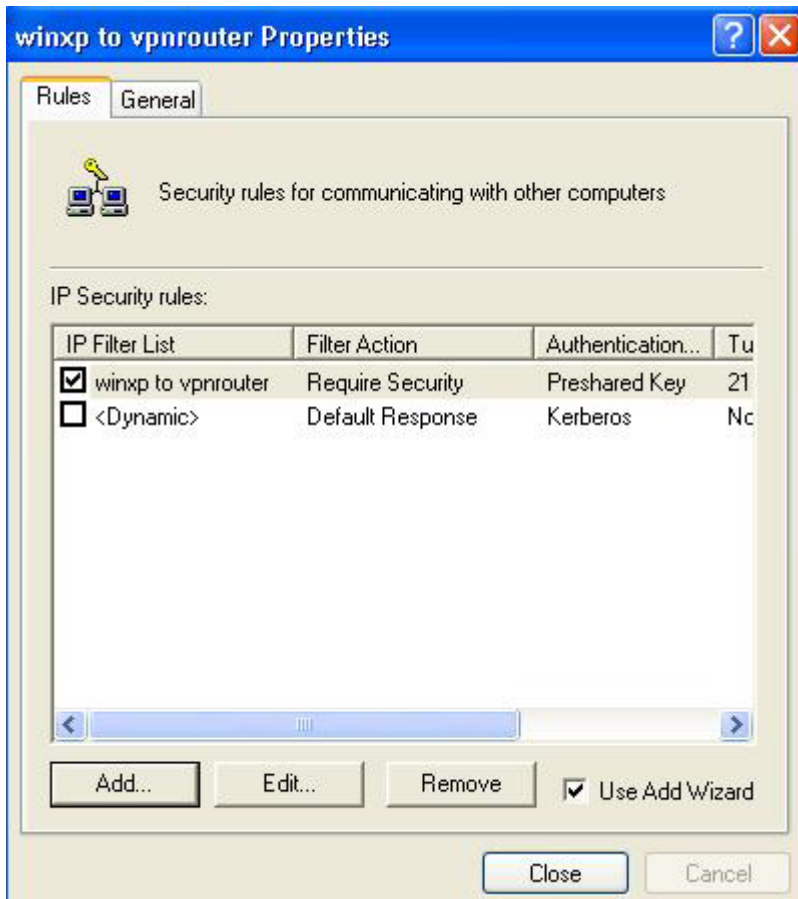




18. Click Finish.



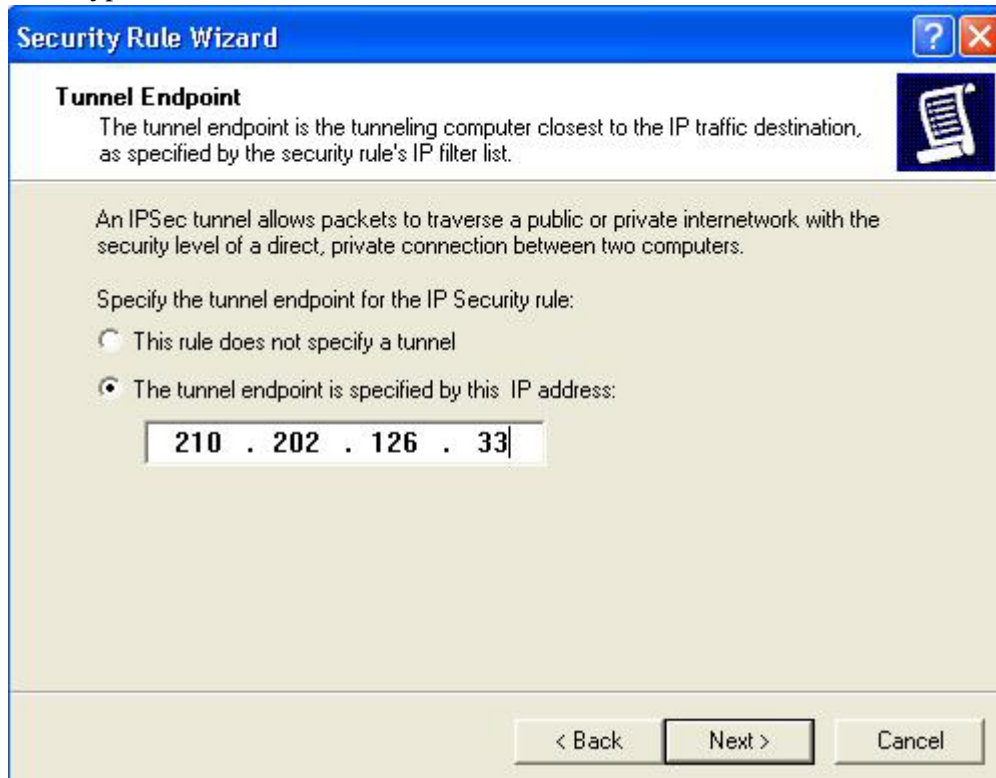
19. Click ADD.



20. Click "Next".



21. Type WinXP IP address.

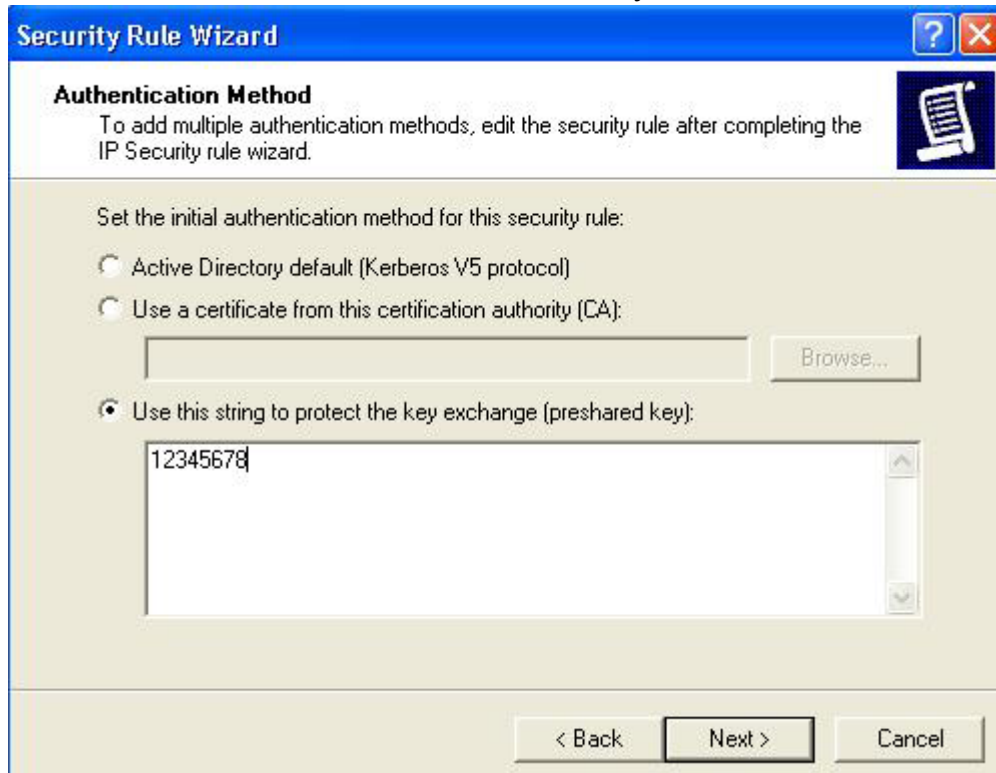




22. Choice the Network Type.



23. Use the Authentication Preshared Key.

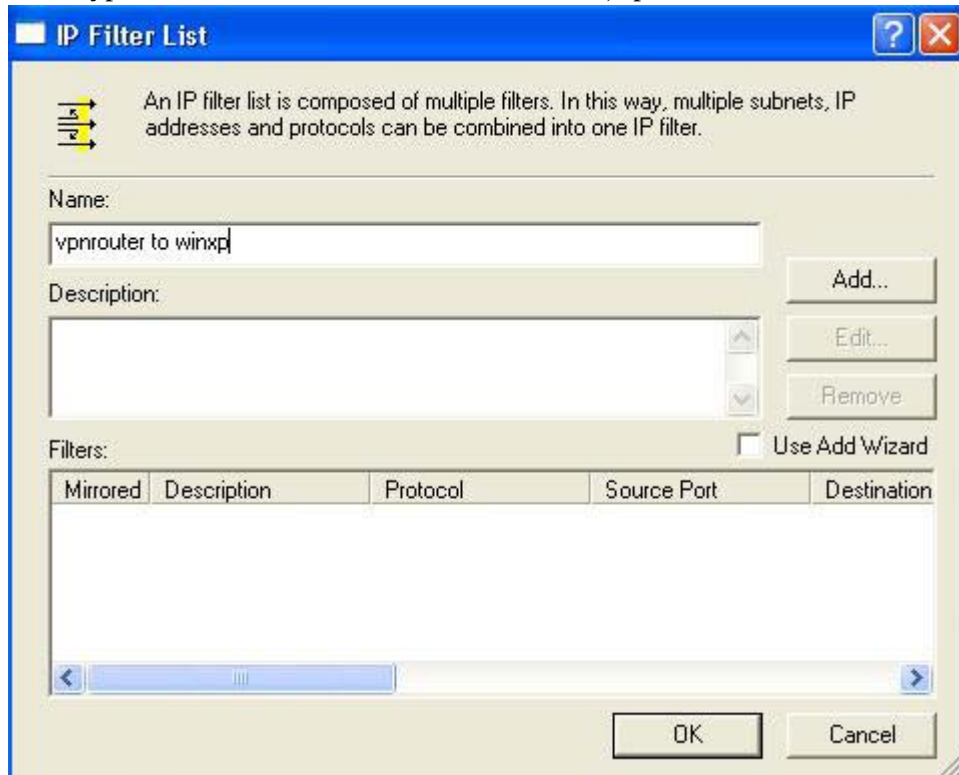




24. IP Filter List to click "Add".

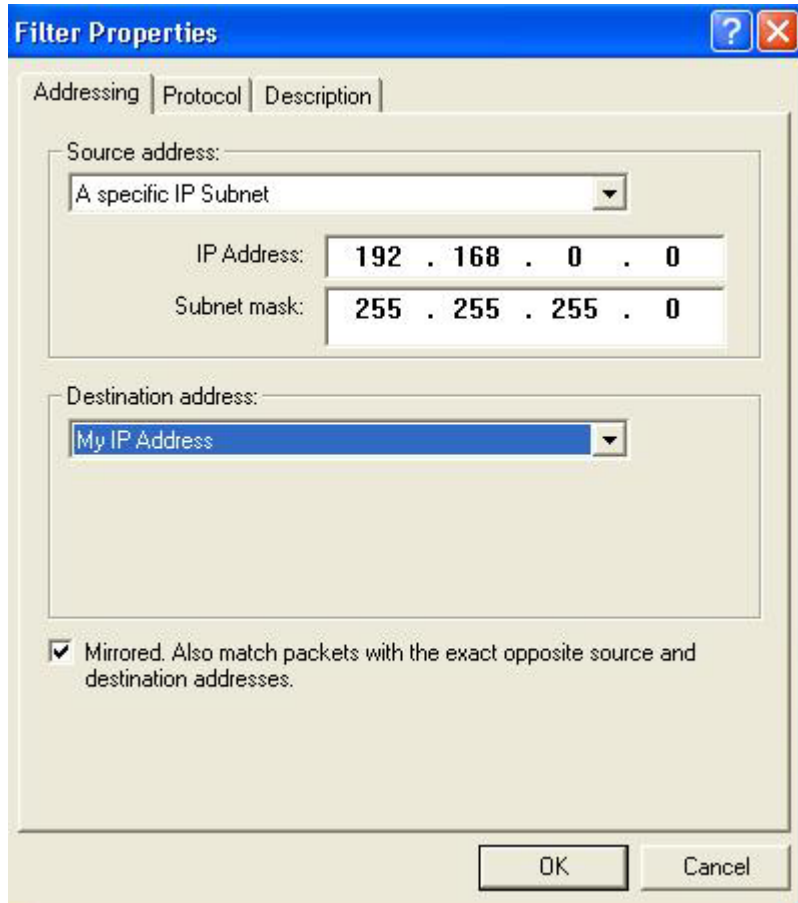


25. Type the IP Filter List name. And, please disable "Use Add Wizard".





26. Type Source address -> "A specific IP subnet" and Destination address->"My IP address".



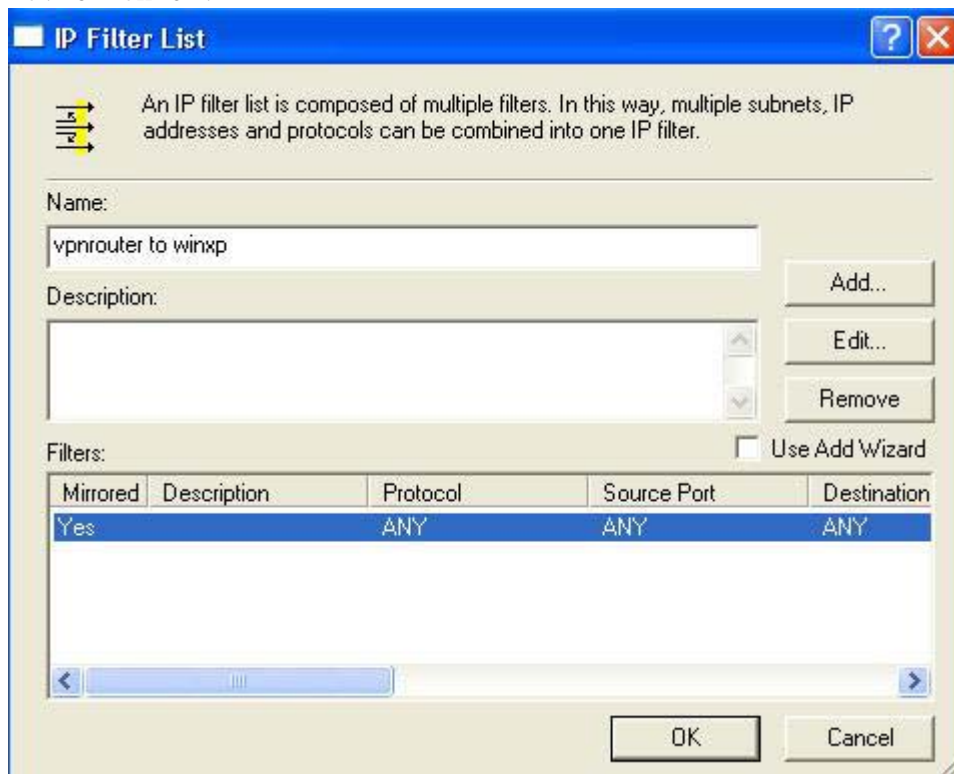
The "Filter Properties" dialog box has three tabs: "Addressing", "Protocol", and "Description". The "Addressing" tab is active. It contains two main sections: "Source address:" and "Destination address:".

**Source address:** A dropdown menu is set to "A specific IP Subnet". Below it are two input fields: "IP Address:" with the value "192 . 168 . 0 . 0" and "Subnet mask:" with the value "255 . 255 . 255 . 0".

**Destination address:** A dropdown menu is set to "My IP Address".

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".

27. Click OK.



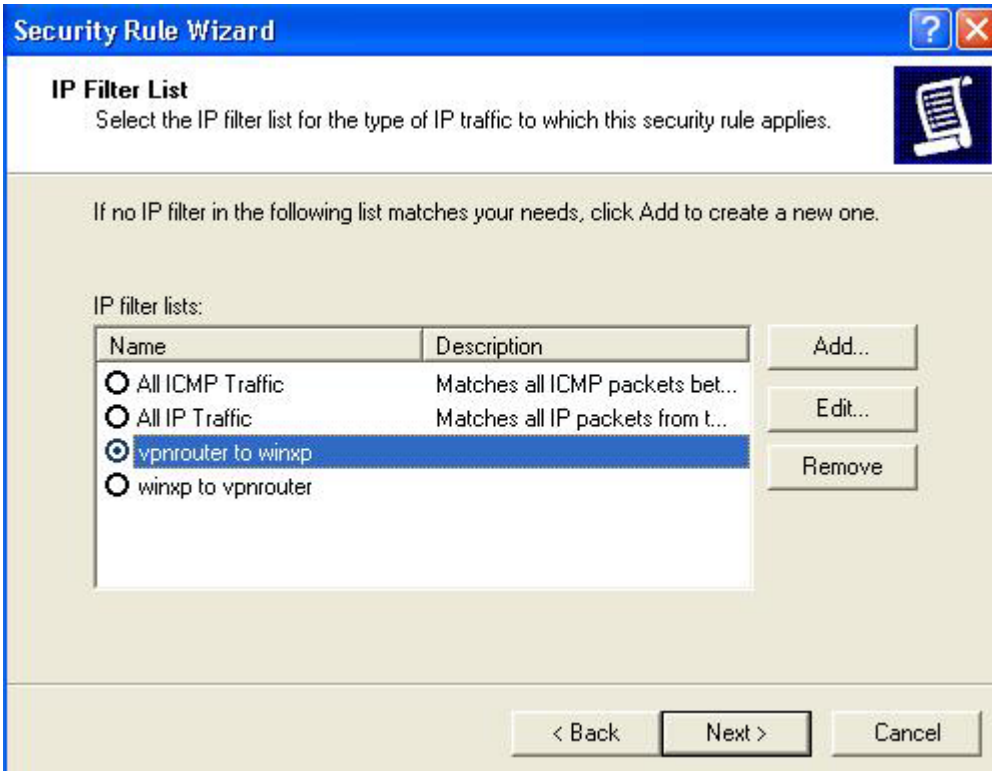
The "IP Filter List" dialog box shows a list of filters. It includes a "Name:" field with "vpnroutel to winxp" and a "Description:" field. To the right of the description field are "Add...", "Edit...", and "Remove" buttons. Below the description field is a "Filters:" section with a "Use Add Wizard" checkbox. A table lists the filters:

Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

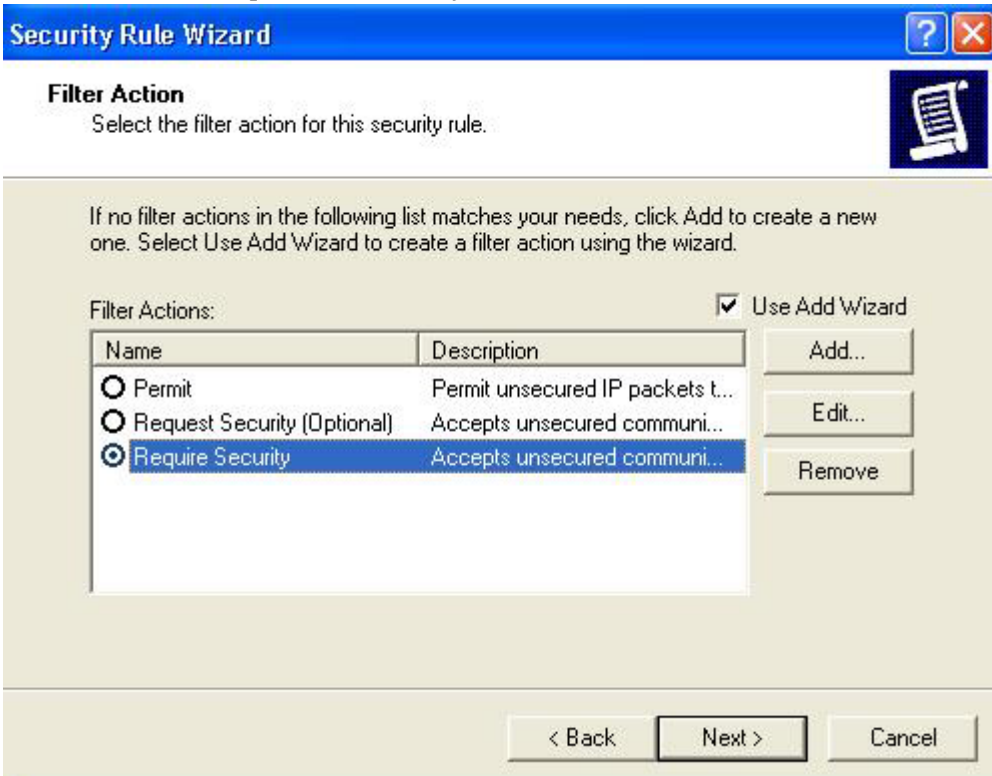
At the bottom are "OK" and "Cancel" buttons.



28. Click "Next".



29. To Edit "Require Security".







30. Click "Finish".



31. Click "Assign".

