



RF550VPN/RF560VPN

IPSec Tunneling

Reference Guide



How To: Configuring IPSec Tunneling in Windows XP or 2000 and Connecting to an RF550VPN/RF560VPN

Copyright © 2003

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved. Multi-Tech Systems, Inc. makes no representations or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

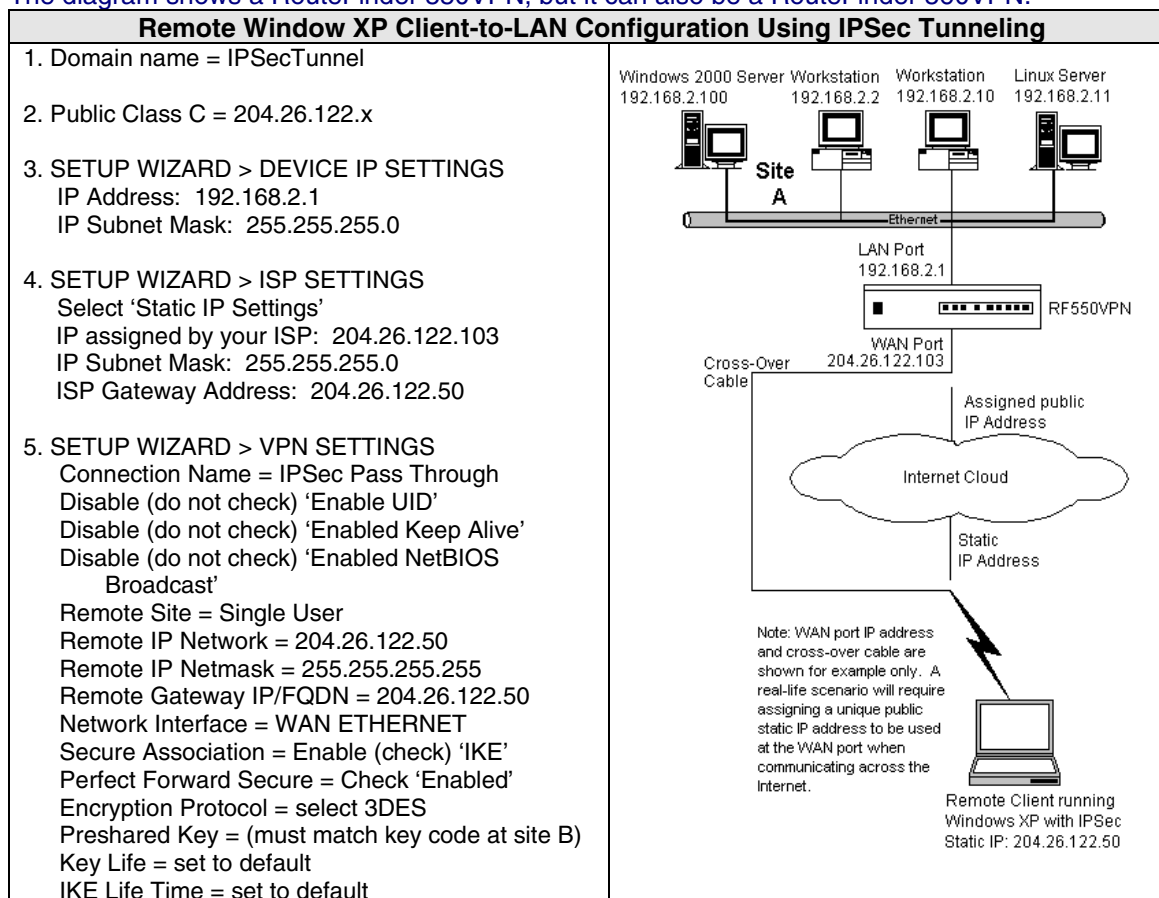
Manual Number S000261D

| Revision | Date | Description |
|----------|----------|---|
| A | 05/30/02 | Initial release |
| A1 | 05/31/02 | Added Win2K/XP screen differences |
| B | 08/12/02 | Added RF550VPN settings and static IP note. |
| C | 04/16/03 | Updated for RF550VPN software version 4.64. |
| D | 07/07/03 | Add RF560VPN. |

The following configuration procedure shows how to configure IPSec tunneling on a Windows XP Professional client so that this client can access a LAN through the Internet. The LAN is located on the protected side of a RF550VPN/RF560VPN. It is assumed that the RF550VPN/RF560VPN is already configured. This configuration procedure will also work on Windows 2000 with service pack 2 installed. Comments are included for screens that differ between Win XP and 2K.

Note: The remote client must use a static IP address for IPSec tunneling. This configuration will not work using a dynamic IP address at the remote client.

The diagram shows a RouteFinder 550VPN, but it can also be a RouteFinder 560VPN.



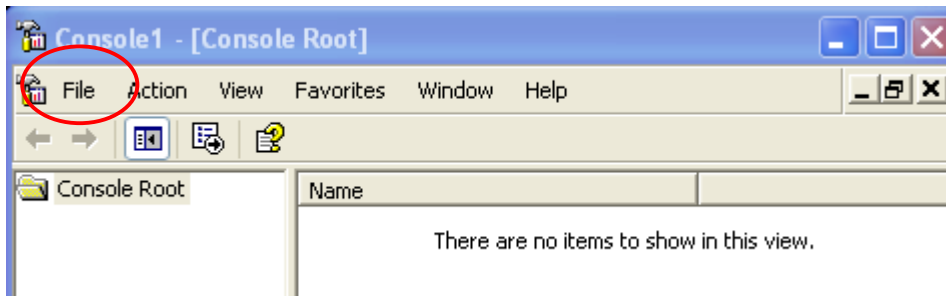
1. At the Windows XP Professional workstation, type **mmc** in DOS command mode.

```

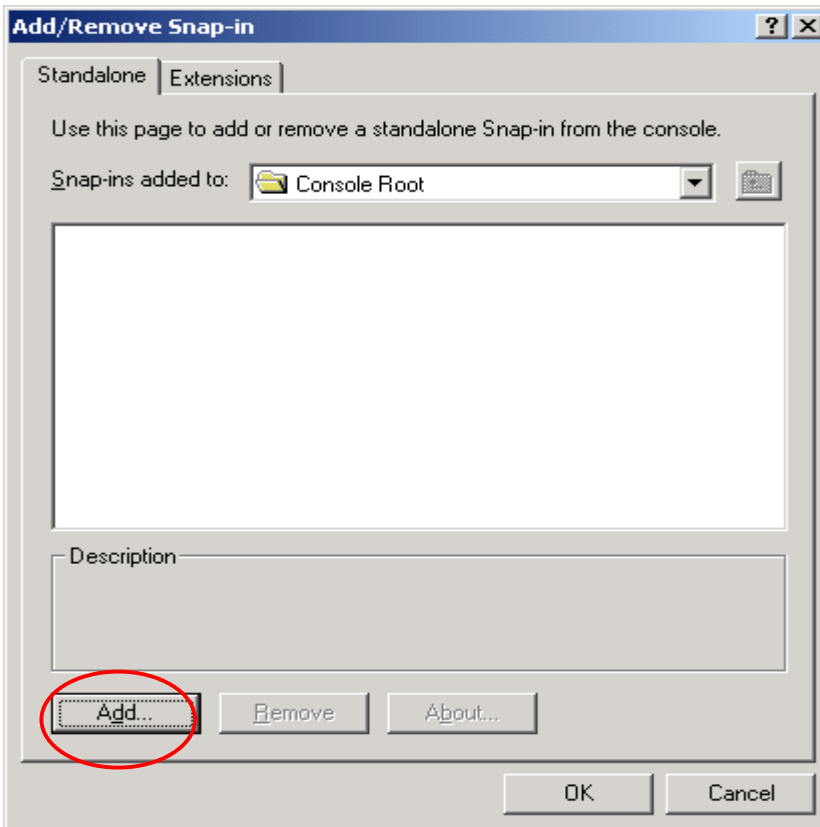
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jerome Meyer>mmc
  
```

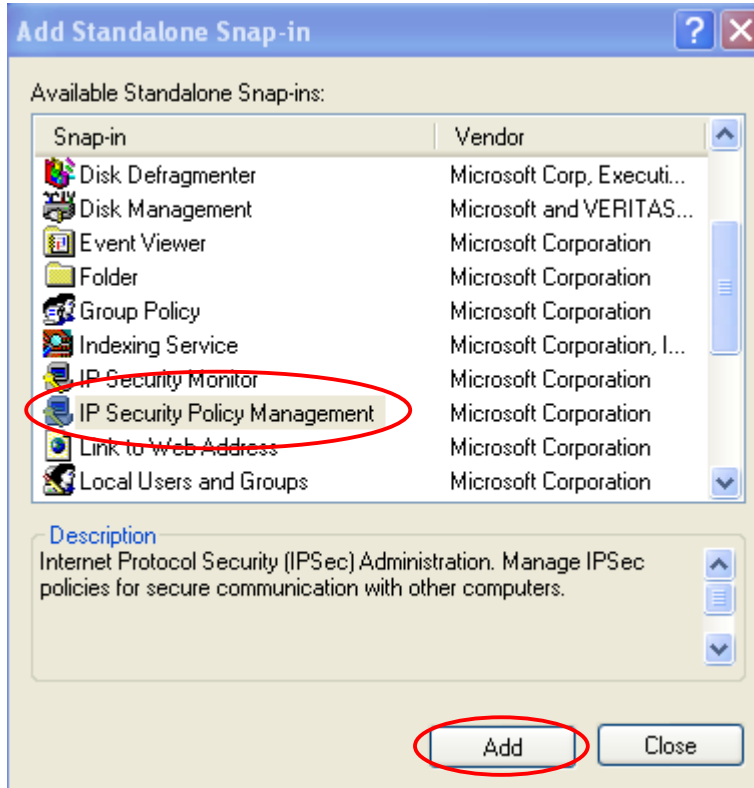
2. Left click on **File** and select **Add/Remove Snap-in**. For Win 2K, left click on **Console** and select **Add/Remove Snap-in**.



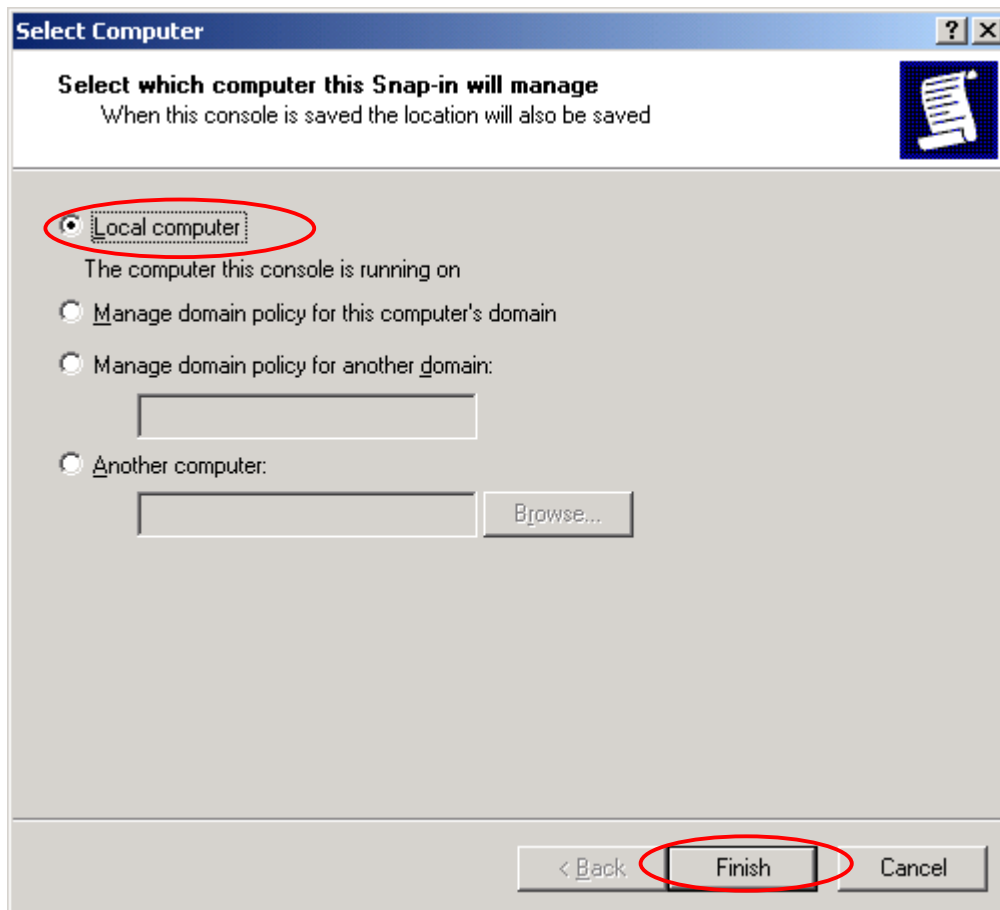
3. Click **Add**.



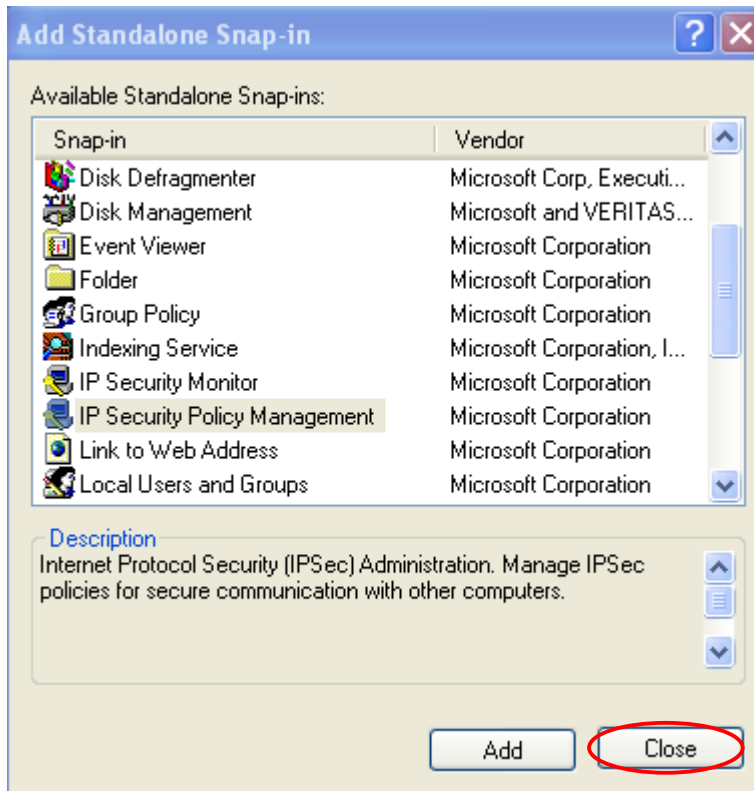
4. Scroll down and highlight **IP Security Policy Management** and click **Add**.



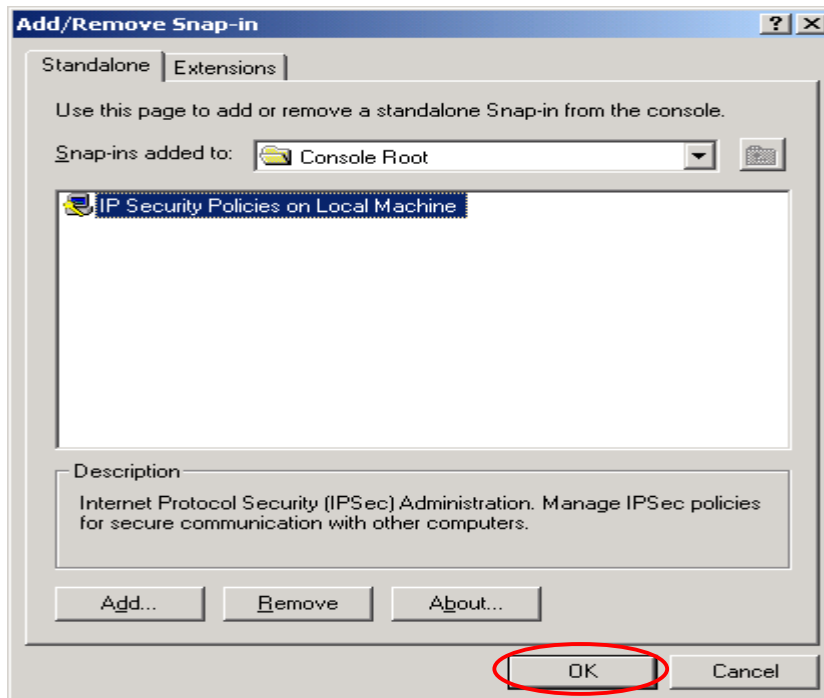
5. Choose **Local computer** and click **Finish**.



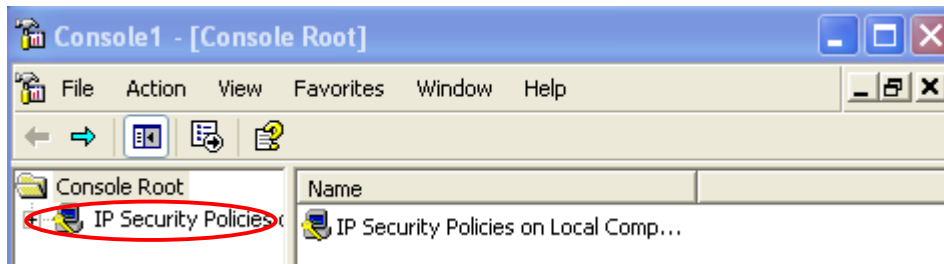
6. Click **Close**.



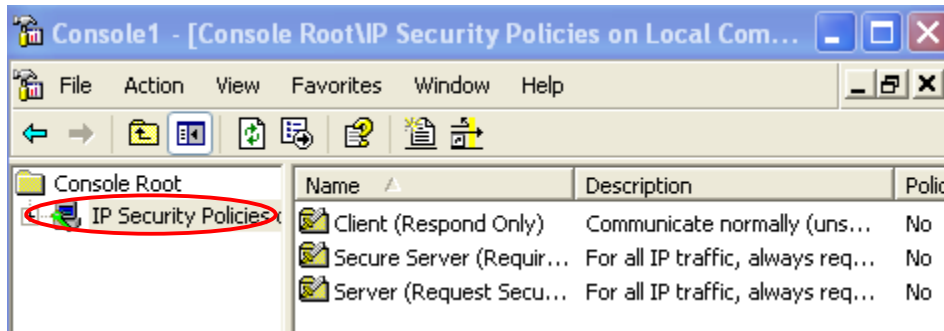
7. Click **OK**.



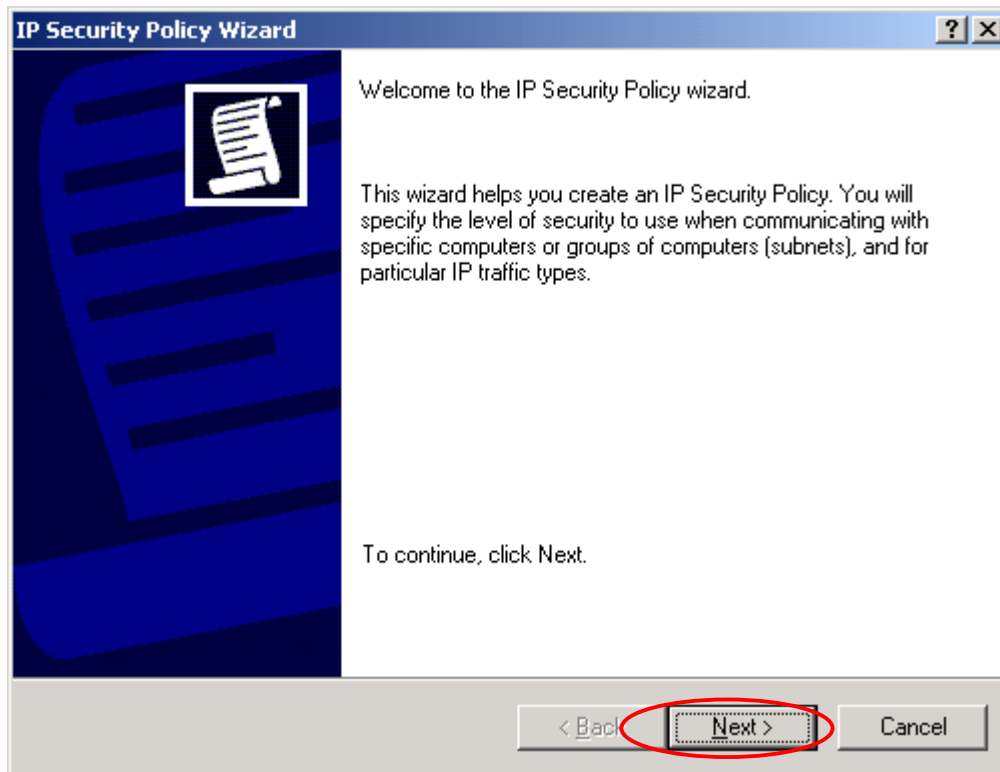
8. Click left button on **IP Security Policies on Local Computer** under **Console Root** to display the local computer security policies under **Name**.



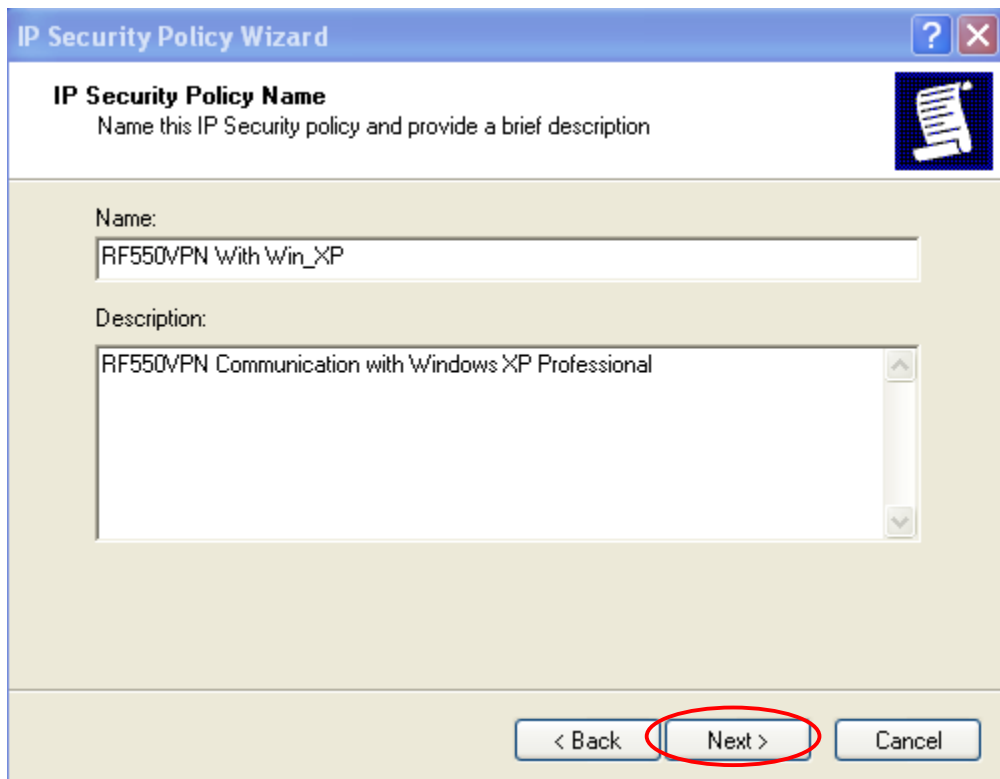
9. Right click on **IP Security Policies on Local Computer** and select **Create IP Security Policy**.



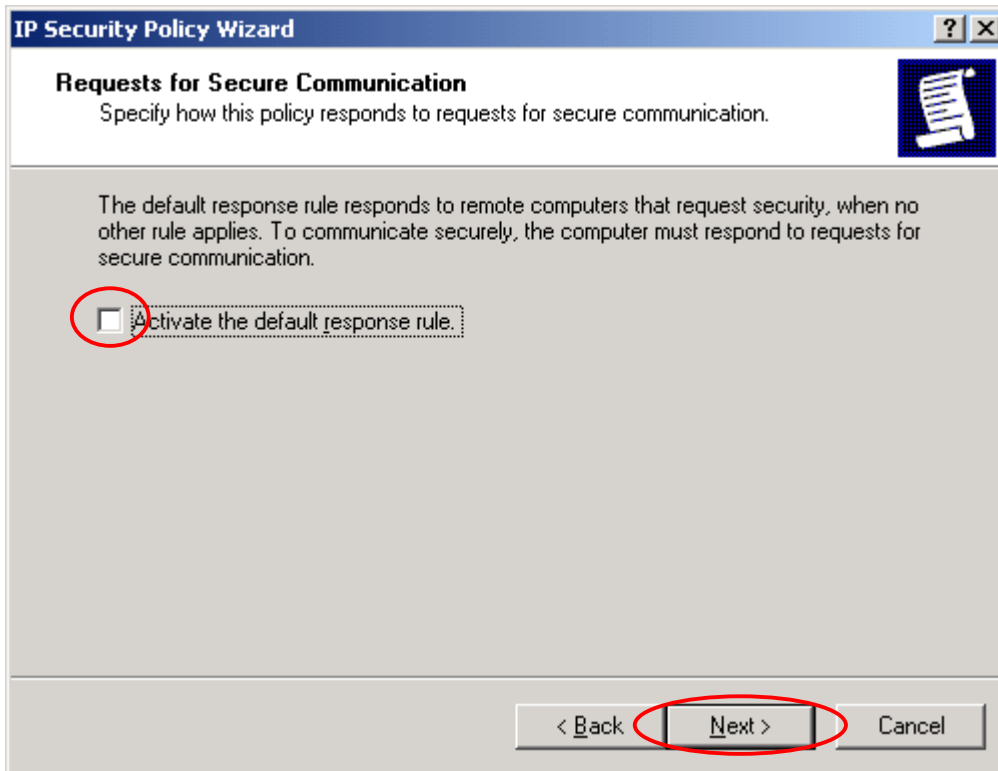
10. Click **Next**.



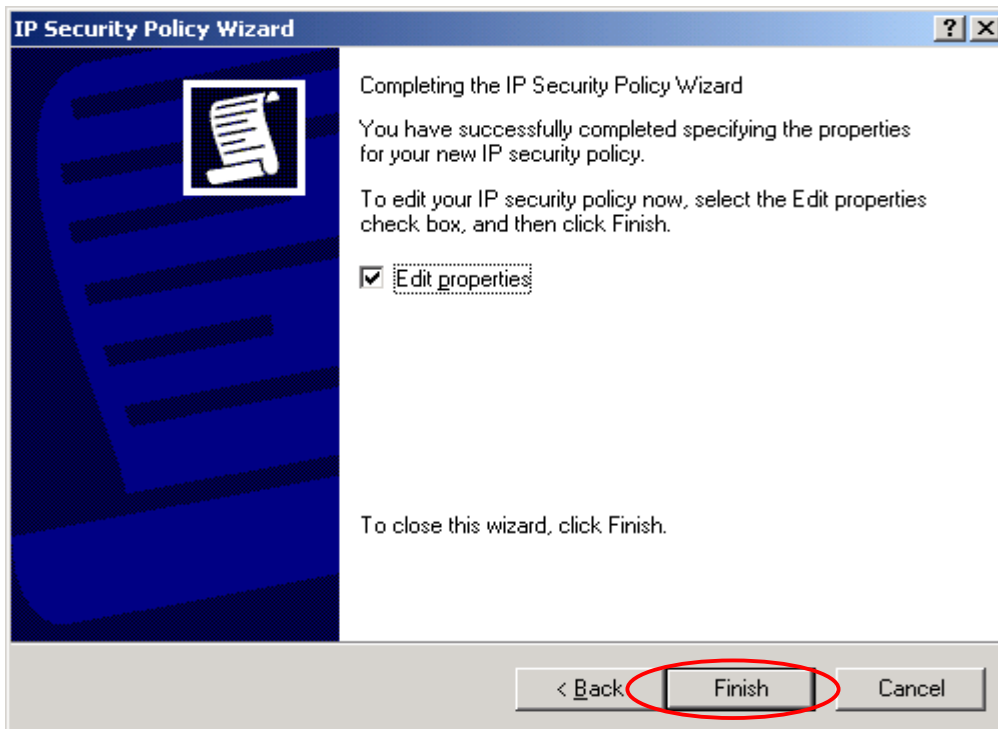
11. Type Name and Description for security policy, and then click **Next**.



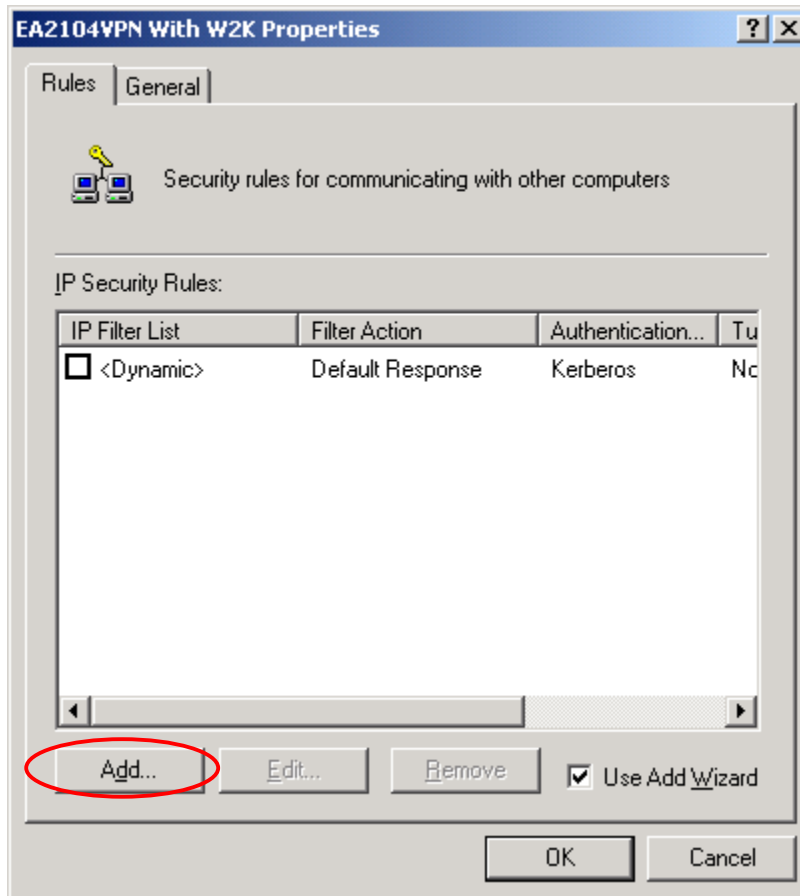
12. Uncheck **Activate the default response rule**, then click **Next**.



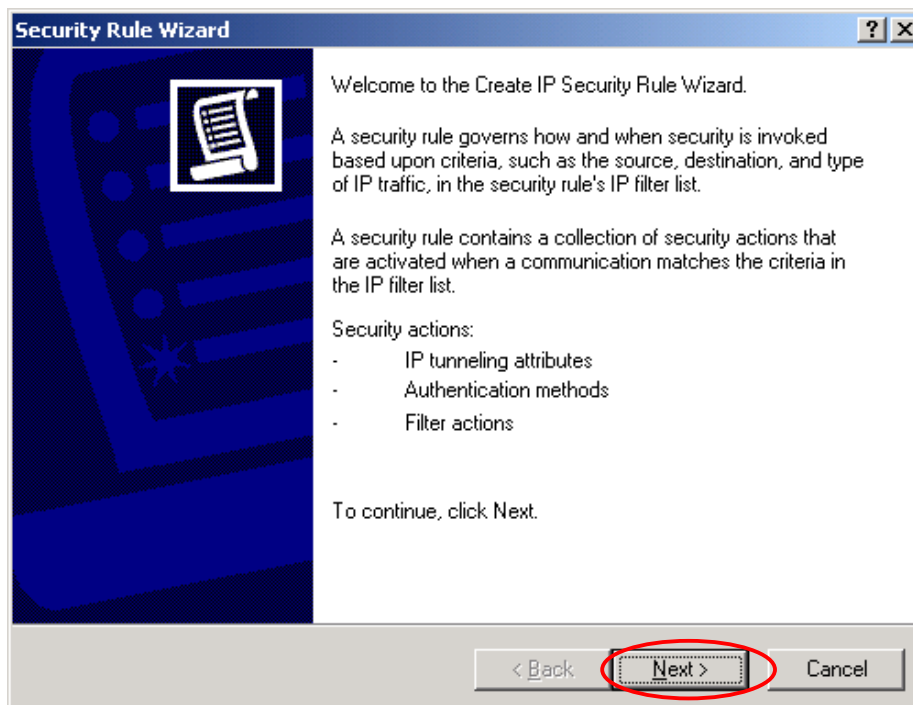
13. Click **Finish**.



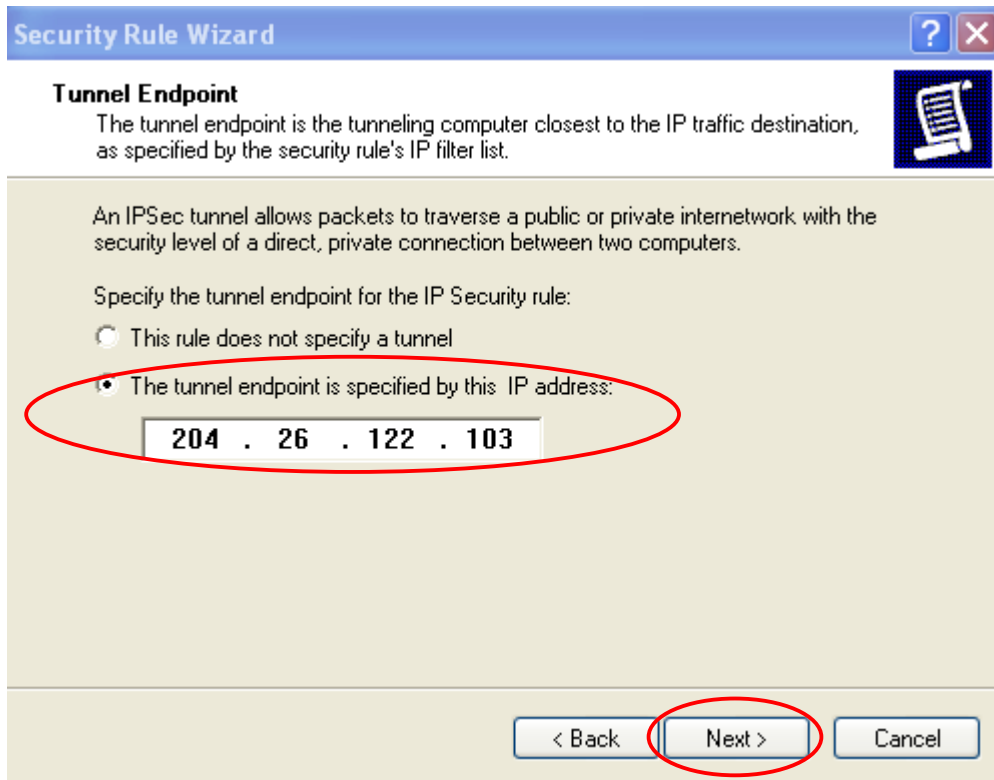
14. Click **Add**.



15. Click **Next**.

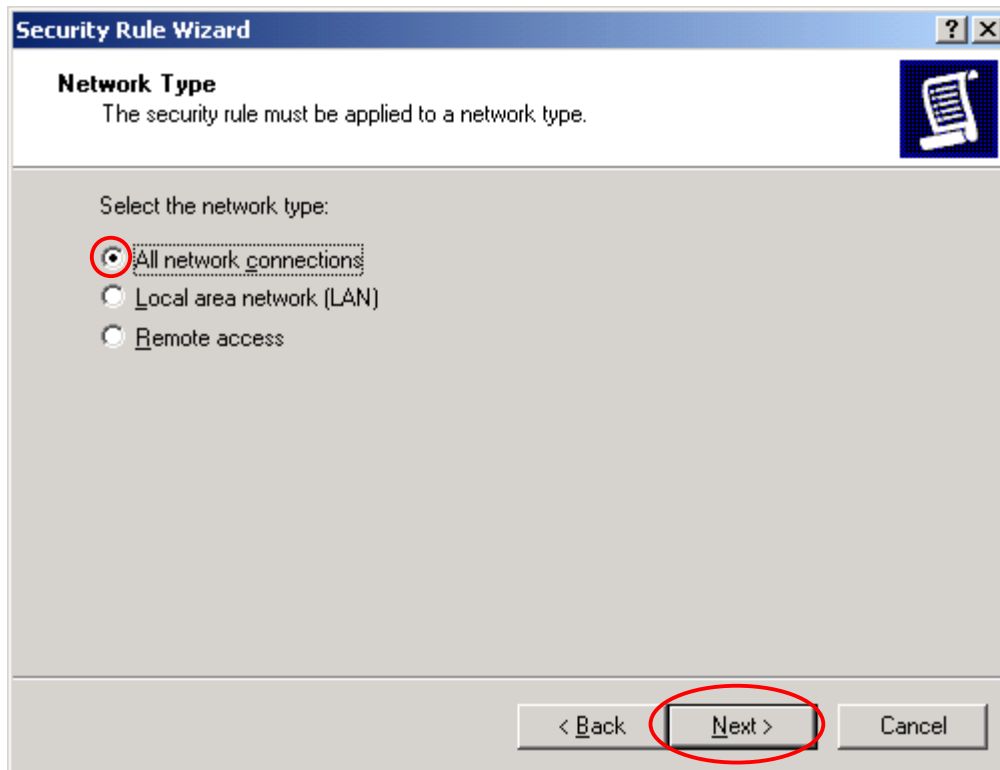


16. Input IP Address into **The tunnel endpoint specified by this IP address:** and then click **Next**. (Ex: RF550VPN/RF560VPN WAN Port IP Address 204.26.122.103)



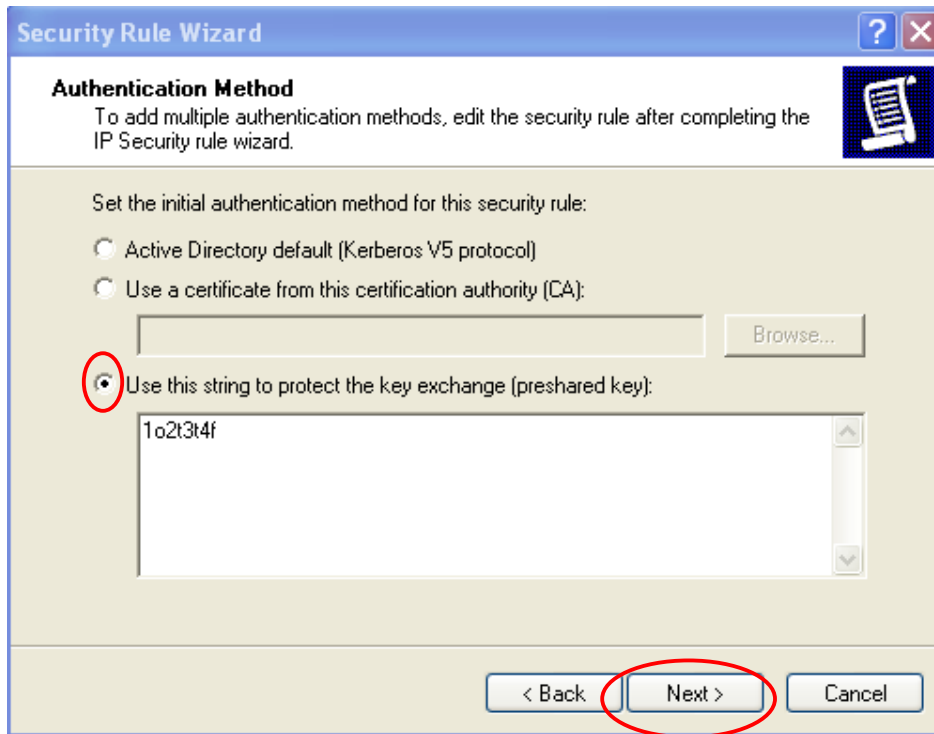
The screenshot shows the 'Security Rule Wizard' window at the 'Tunnel Endpoint' step. The title bar reads 'Security Rule Wizard'. Below the title bar, the section is titled 'Tunnel Endpoint' with a subtext: 'The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.' A paragraph explains: 'An IPsec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.' Below this, it says 'Specify the tunnel endpoint for the IP Security rule:'. There are two radio button options. The first is 'This rule does not specify a tunnel'. The second is 'The tunnel endpoint is specified by this IP address:', which is selected and circled in red. Below the selected option is a text box containing the IP address '204 . 26 . 122 . 103'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

17. Choose **All network connections**, and then click **Next**.



The screenshot shows the 'Security Rule Wizard' window at the 'Network Type' step. The title bar reads 'Security Rule Wizard'. Below the title bar, the section is titled 'Network Type' with a subtext: 'The security rule must be applied to a network type.' A paragraph says 'Select the network type:'. There are three radio button options. The first is 'All network connections', which is selected and circled in red. The second is 'Local area network (LAN)'. The third is 'Remote access'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

18. Choose **Use this string to protect the key exchange (preshared key)**. Enter the key code and then click **Next**. (Ex: RF550VPN/RF560VPN preshared key 1o2t3t4f)



The screenshot shows the 'Authentication Method' step of the Security Rule Wizard. The title bar reads 'Security Rule Wizard'. Below the title bar, the section is titled 'Authentication Method' with a subtitle: 'To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.' There are three radio button options: 'Active Directory default (Kerberos V5 protocol)', 'Use a certificate from this certification authority (CA):' (with an empty text box and a 'Browse...' button), and 'Use this string to protect the key exchange (preshared key):'. The third option is selected and circled in red. Below it is a text box containing the preshared key '1o2t3t4f'. At the bottom, there are three buttons: '< Back', 'Next >' (circled in red), 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)

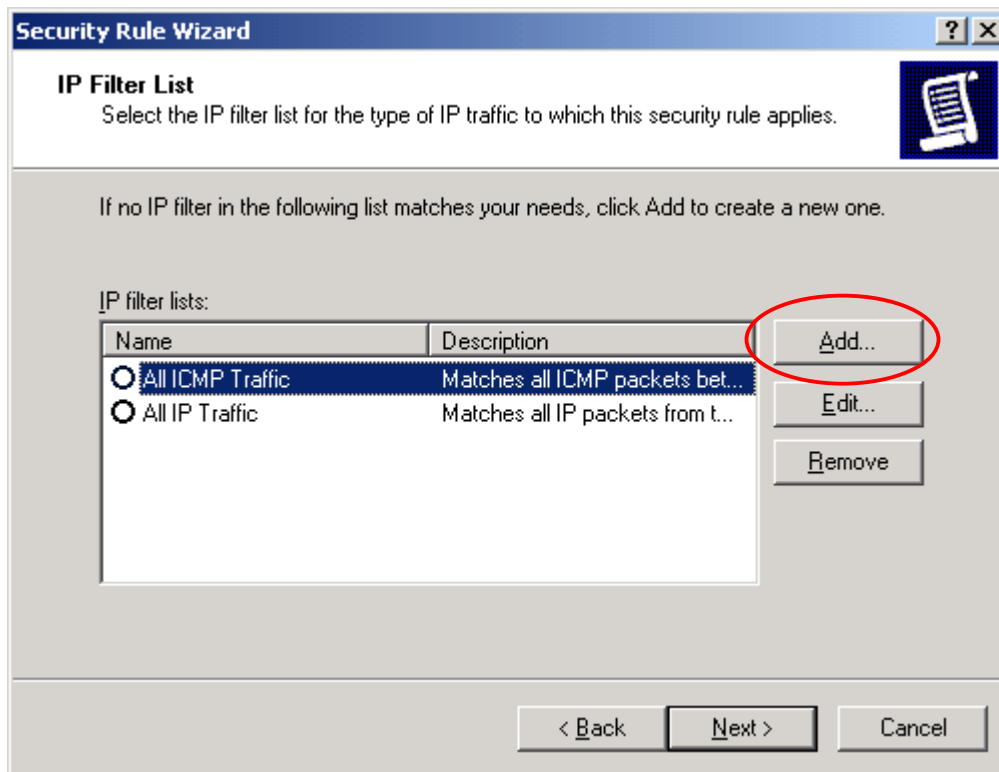
☐ Use a certificate from this certification authority (CA):

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

1o2t3t4f

< Back **Next >** Cancel

19. Click **Add**.



The screenshot shows the 'IP Filter List' step of the Security Rule Wizard. The title bar reads 'Security Rule Wizard'. Below the title bar, the section is titled 'IP Filter List' with a subtitle: 'Select the IP filter list for the type of IP traffic to which this security rule applies.' There is a text box with the instruction: 'If no IP filter in the following list matches your needs, click Add to create a new one.' Below this is a table with two columns: 'Name' and 'Description'. The table contains two entries: 'All ICMP Traffic' and 'All IP Traffic'. To the right of the table are three buttons: 'Add...' (circled in red), 'Edit...', and 'Remove'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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.

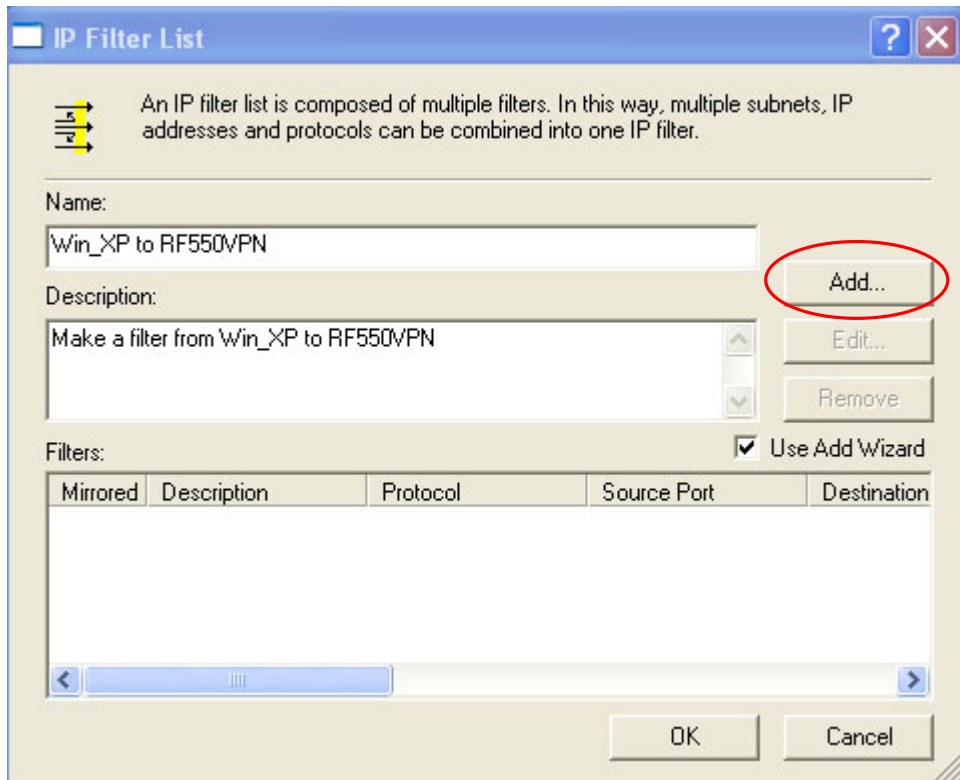
IP filter lists:

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

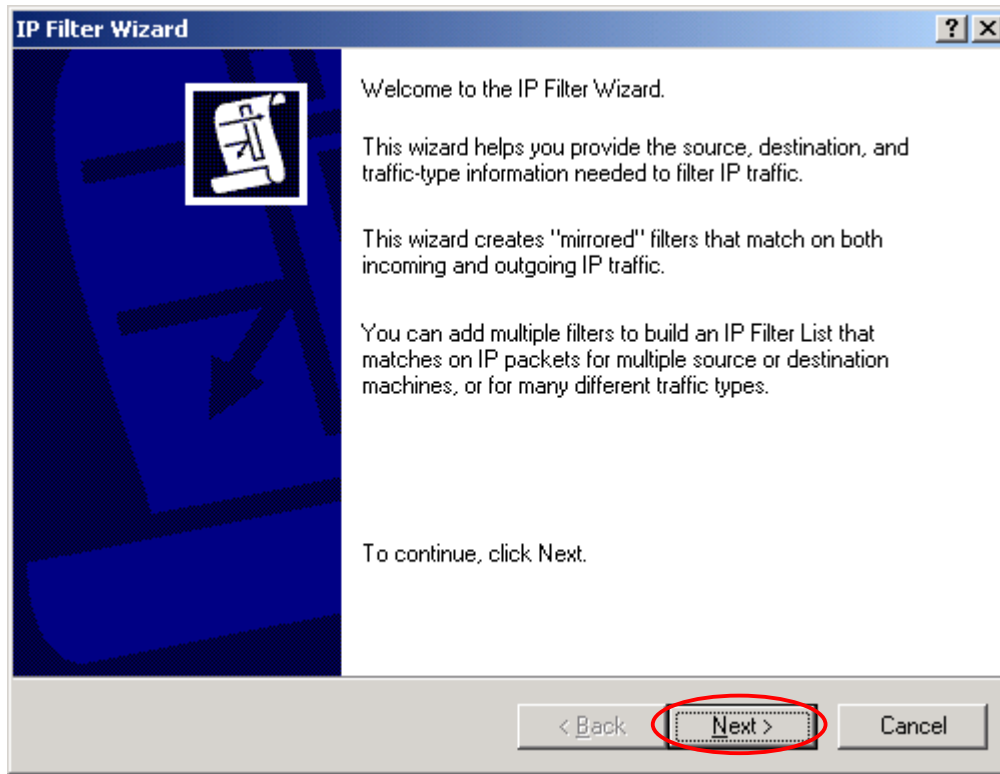
Add... Edit... Remove

< Back Next > Cancel

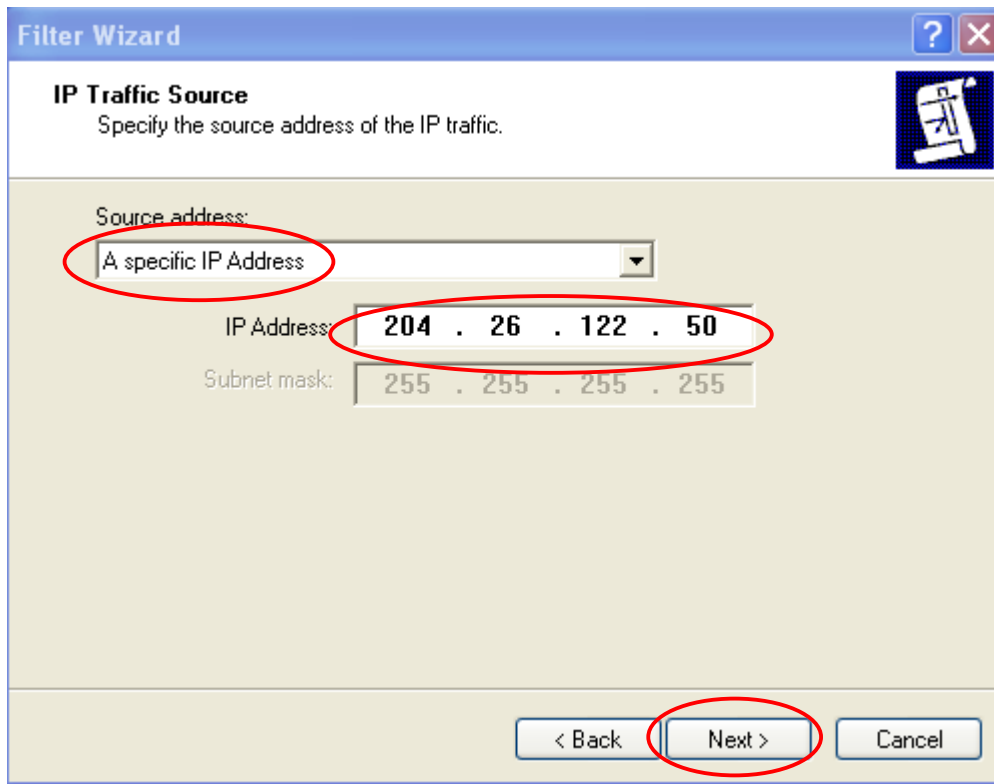
20. Type a filter name and description then click **Add**.



21. Click **Next**.

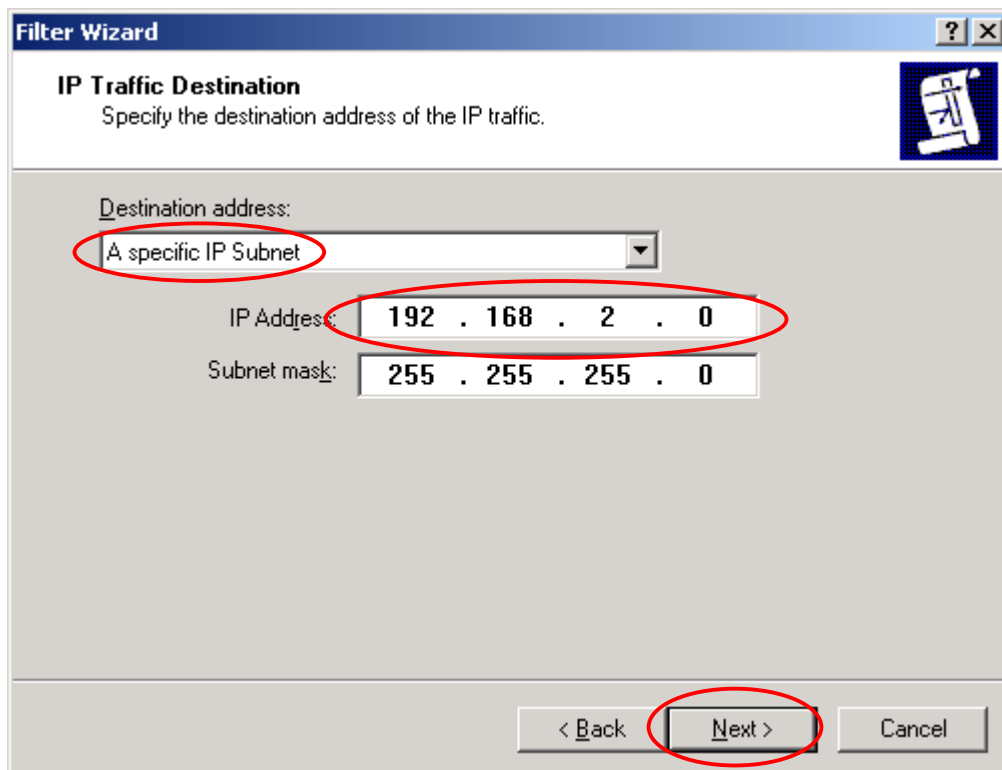


22. Select **A specific IP Address** and input Source IP address, and then click **Next**.
(Ex: Windows XP Professional IP address 204.26.122.50)



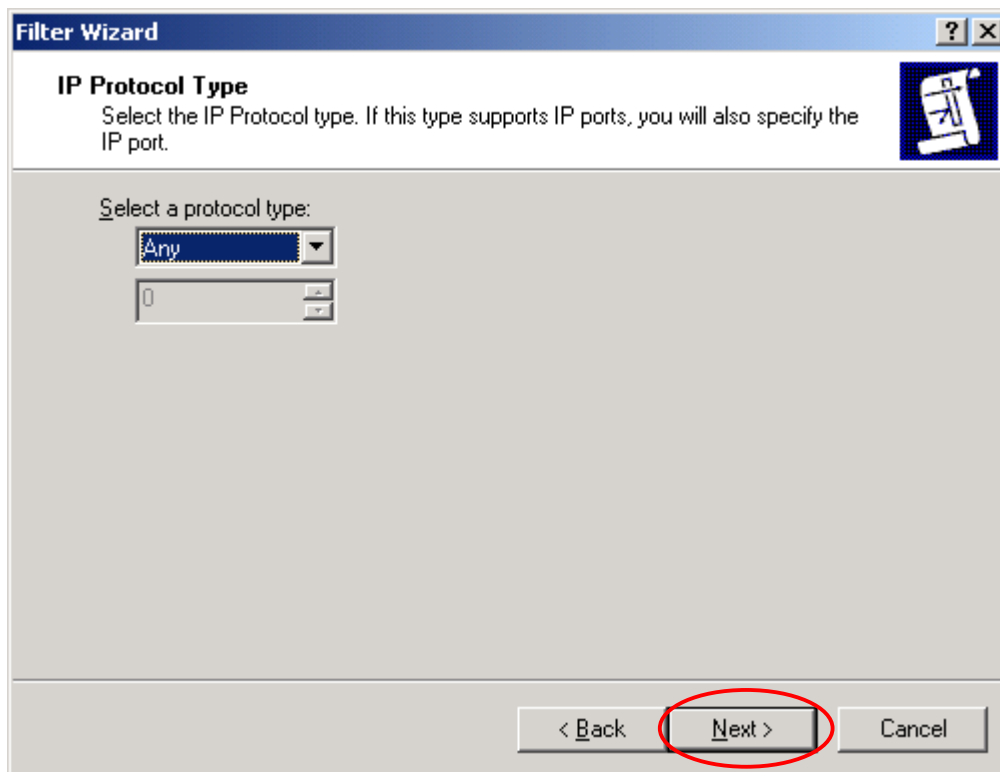
The screenshot shows the 'Filter Wizard' dialog box, specifically the 'IP Traffic Source' step. The title bar reads 'Filter Wizard'. Below the title, it says 'IP Traffic Source' and 'Specify the source address of the IP traffic.' There is a dropdown menu for 'Source address:' with 'A specific IP Address' selected. Below this, the 'IP Address:' field contains '204 . 26 . 122 . 50' and the 'Subnet mask:' field contains '255 . 255 . 255 . 255'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

23. Select **A specific IP Subnet** and input destination IP address, and then click **Next**.
(Ex: RF550VPN/RF560VPN Private network (LAN) 192.168.2.0)

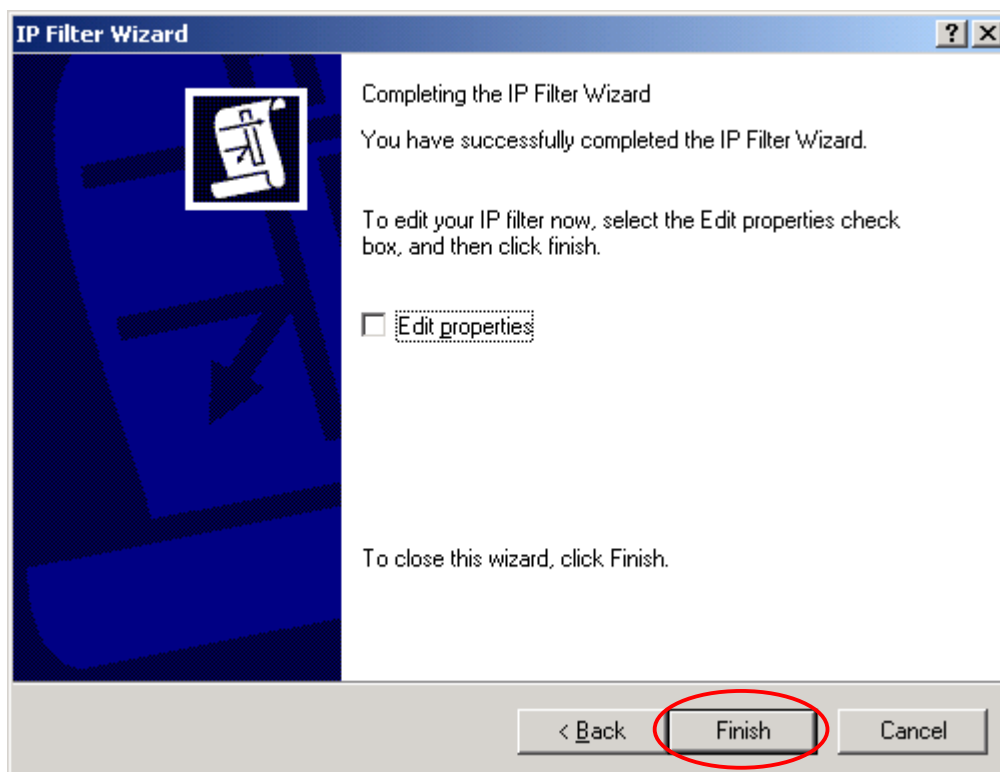


The screenshot shows the 'Filter Wizard' dialog box, specifically the 'IP Traffic Destination' step. The title bar reads 'Filter Wizard'. Below the title, it says 'IP Traffic Destination' and 'Specify the destination address of the IP traffic.' There is a dropdown menu for 'Destination address:' with 'A specific IP Subnet' selected. Below this, the 'IP Address:' field contains '192 . 168 . 2 . 0' and the 'Subnet mask:' field contains '255 . 255 . 255 . 0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is circled in red.

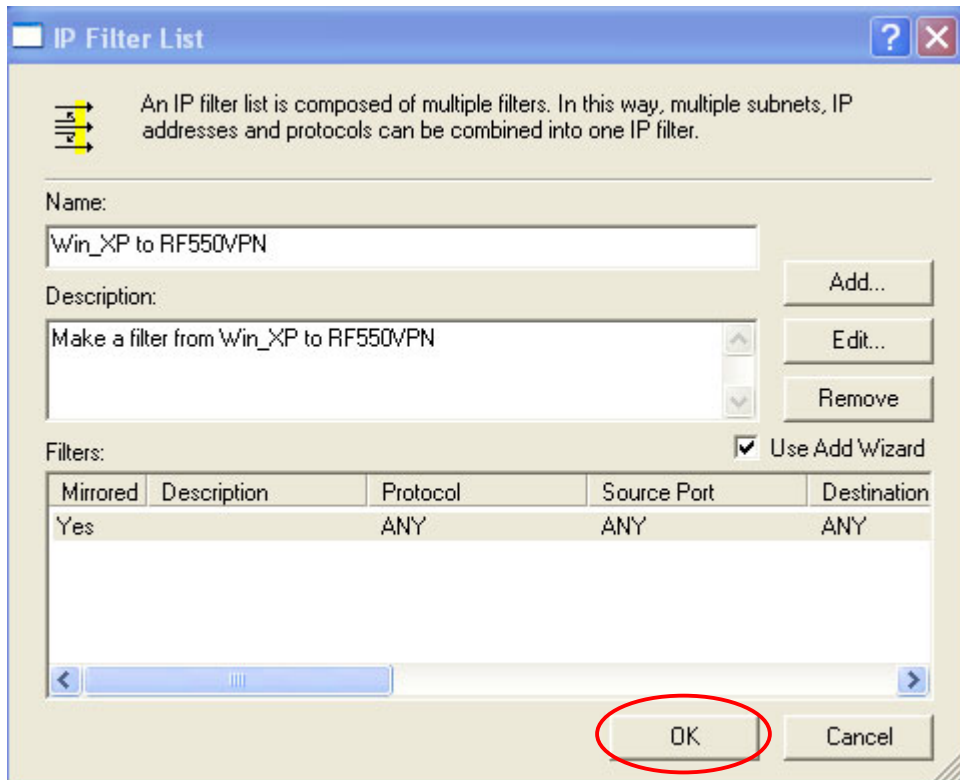
24. Click **Next**.



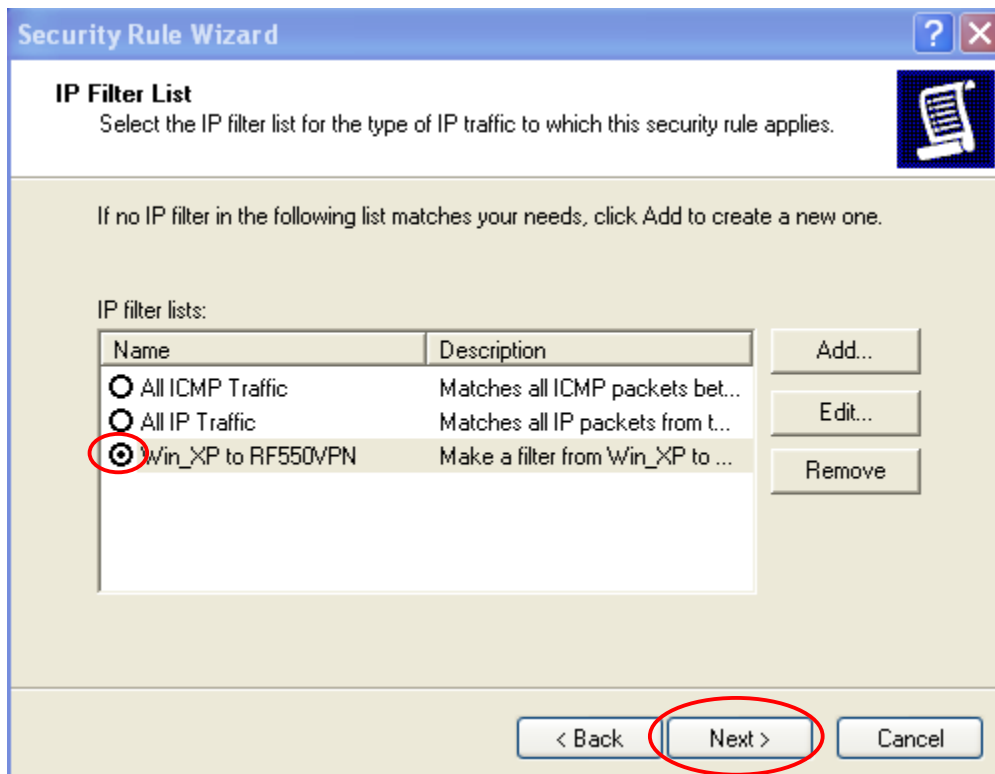
25. Click **Finish**.



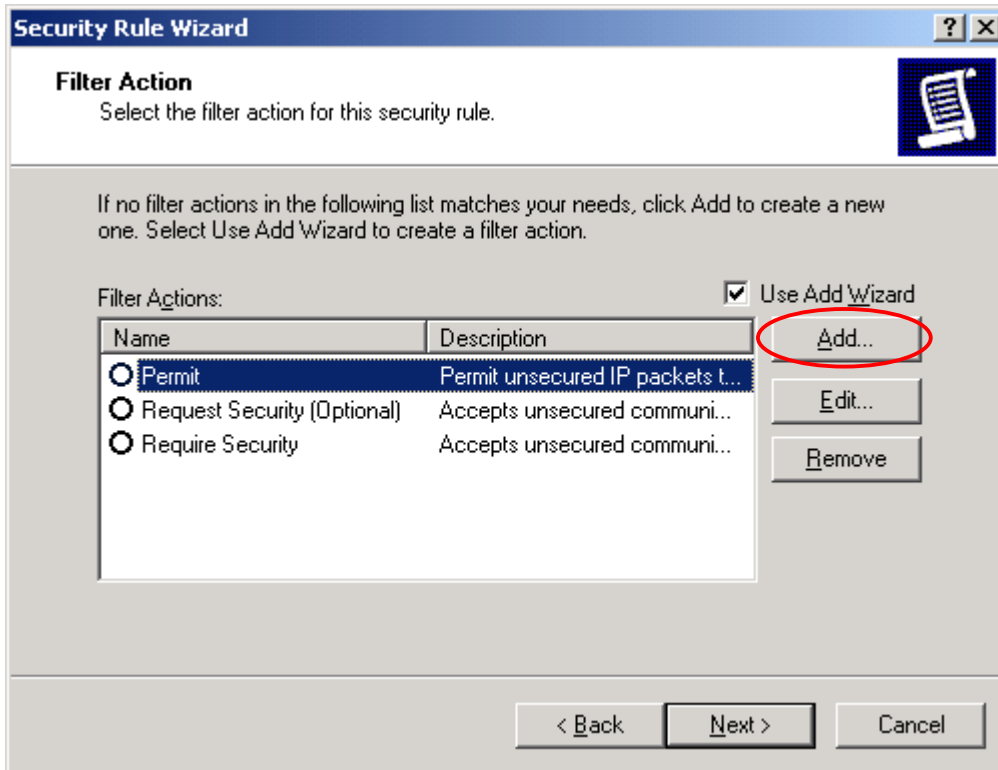
26. Click **OK**. For Win 2K click on **Close**.



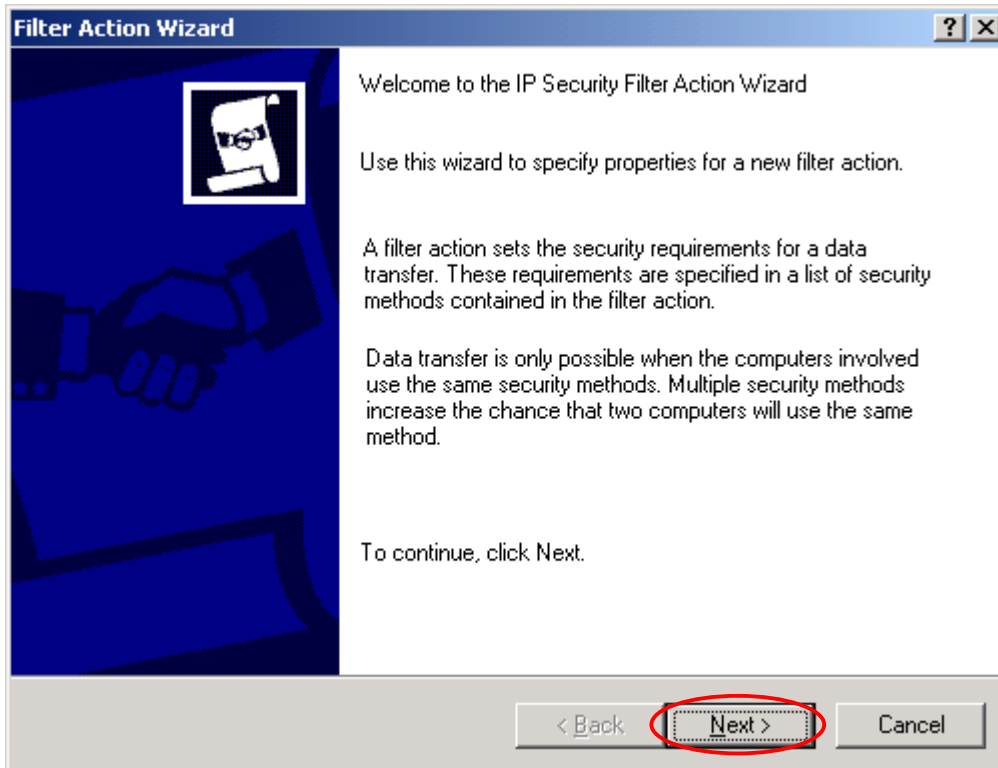
27. Choose **Win_XP to RF550VPN/RF560VPN** and then click **Next**.



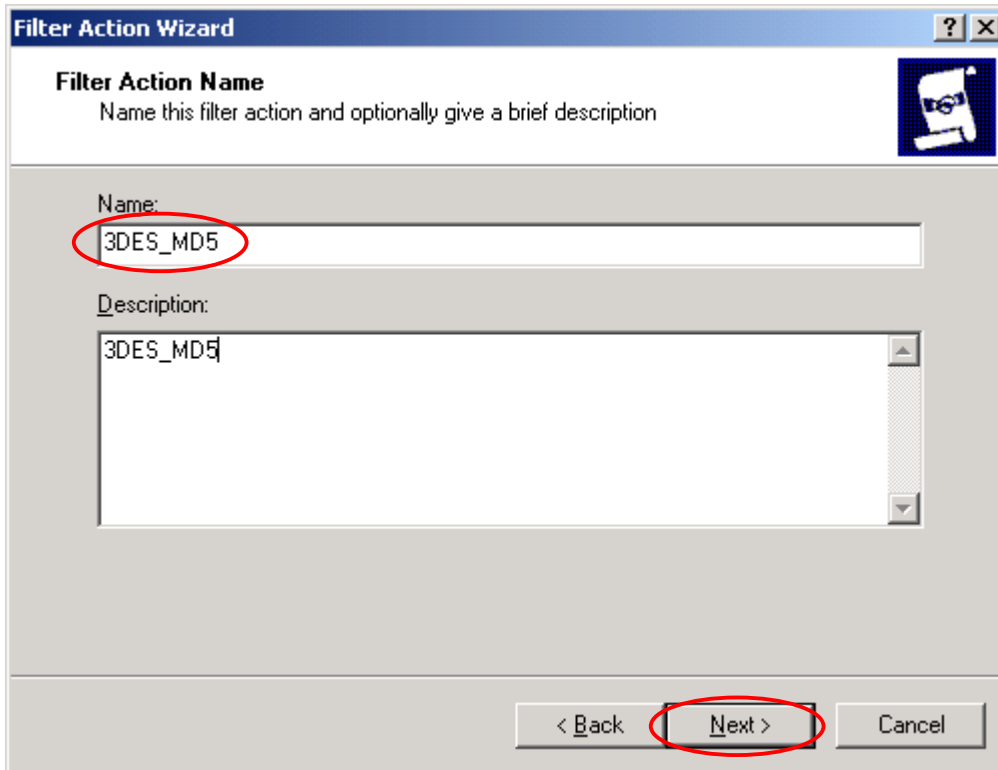
28. Click **Add**.



29. Click **Next**.

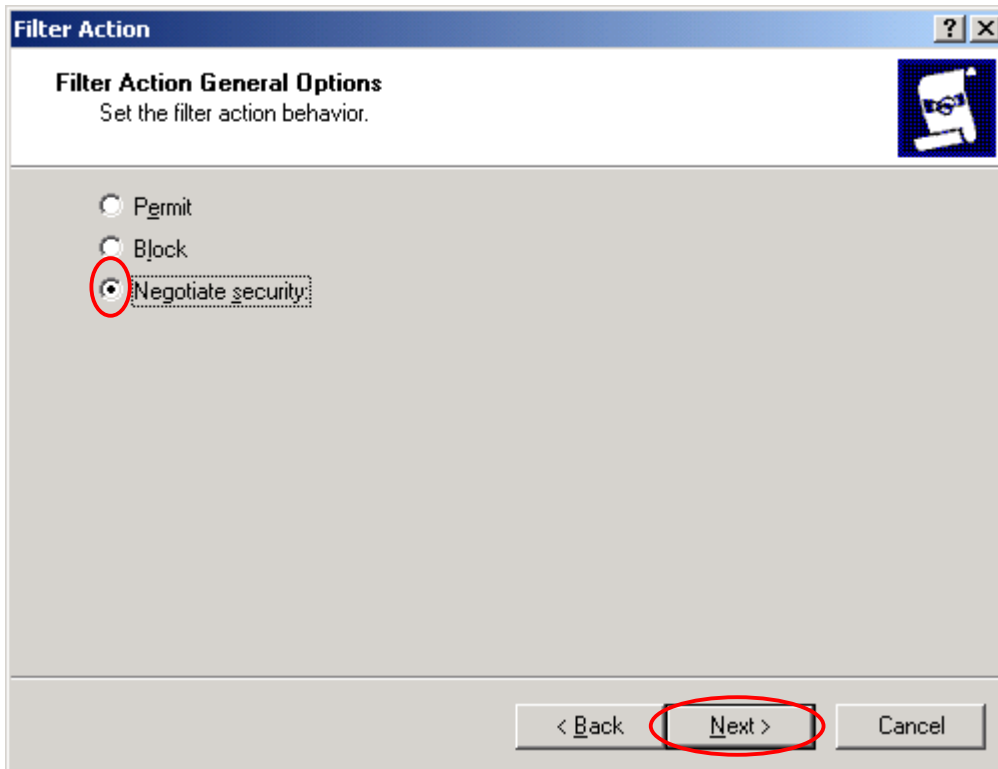


30. Type a filter action name and then click **Next**. (Ex: 3DES_MD5)



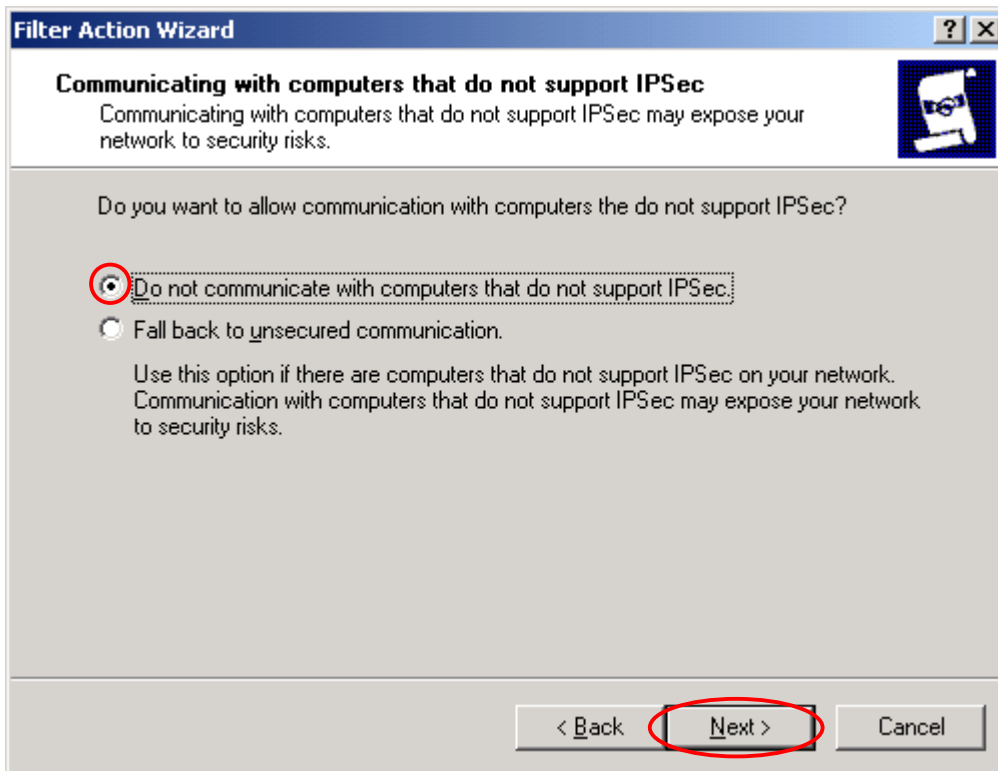
The **Filter Action Wizard** dialog box is shown. The title bar includes a question mark icon and a close button. The main area is titled **Filter Action Name** with the instruction "Name this filter action and optionally give a brief description". Below this, there is a "Name:" label followed by a text box containing "3DES_MD5". Underneath is a "Description:" label followed by a larger text box also containing "3DES_MD5". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is circled in red.

31. Choose **Negotiate security** and then click **Next**.

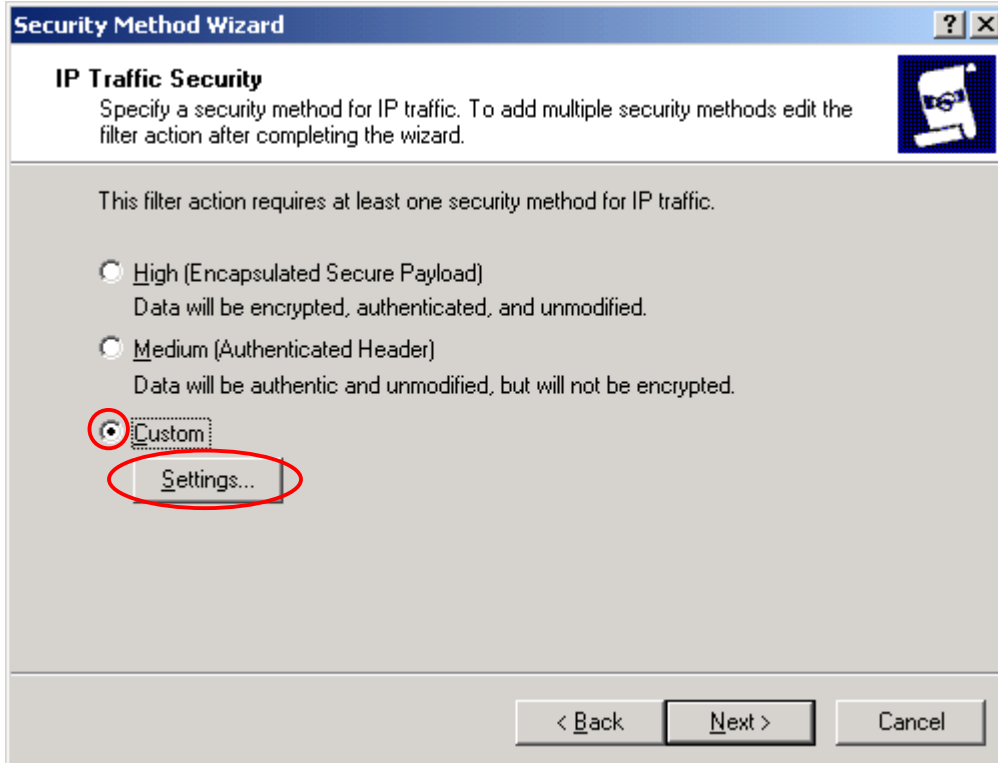


The **Filter Action** dialog box is shown. The title bar includes a question mark icon and a close button. The main area is titled **Filter Action General Options** with the instruction "Set the filter action behavior.". Below this, there are three radio button options: "Permit", "Block", and "Negotiate security:". The "Negotiate security:" option is selected and circled in red. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is circled in red.

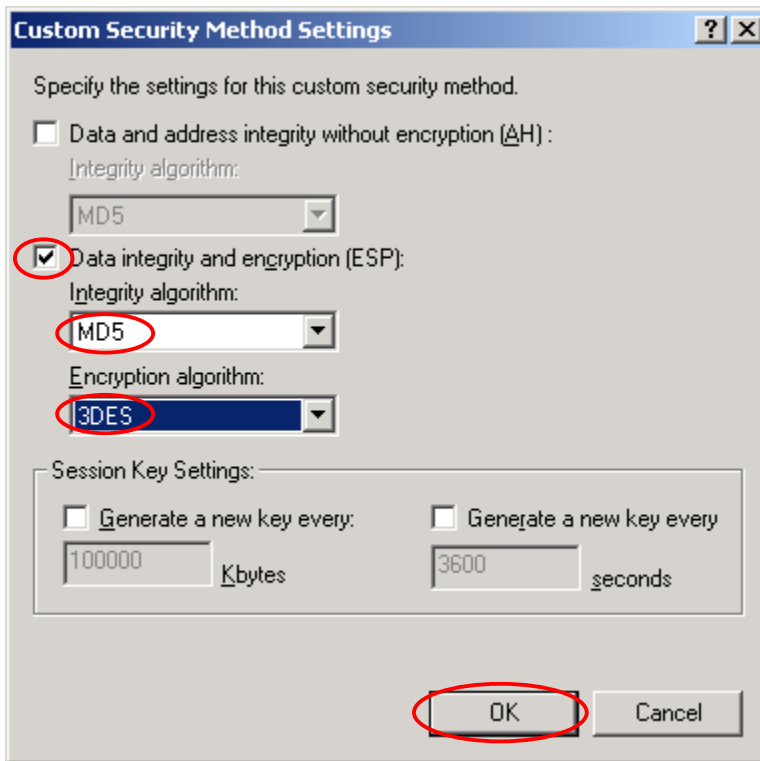
32. Choose **Do not communicate with computer that do not support IPSec**, and then click **Next**.



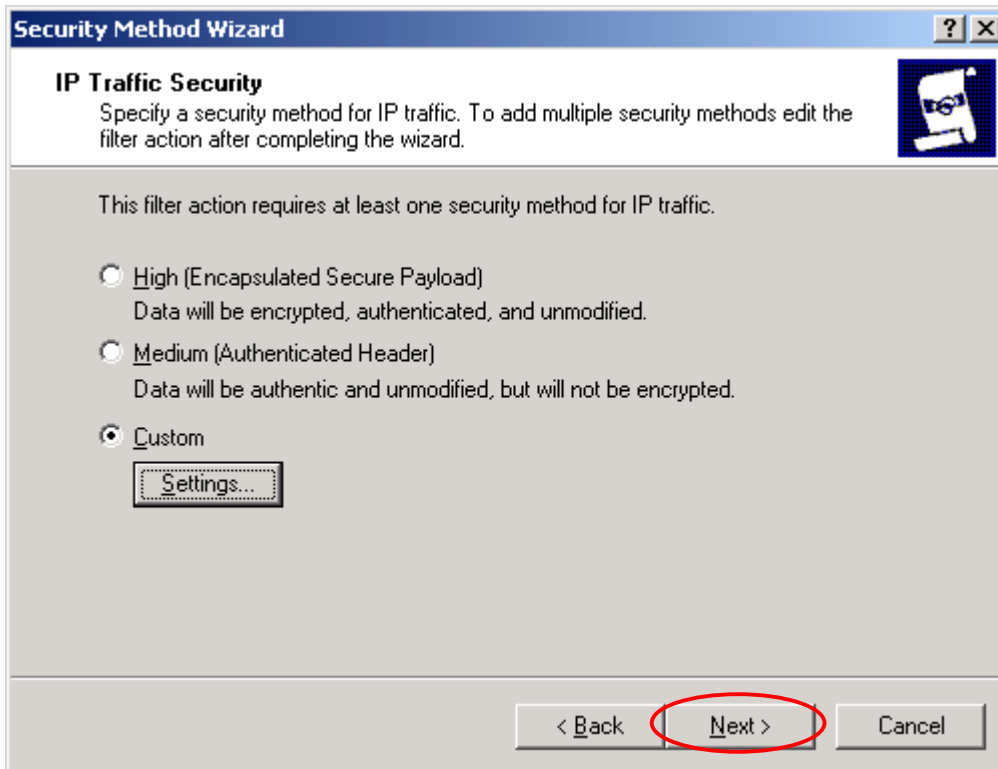
33. Choose **Custom** and then click **Settings**.



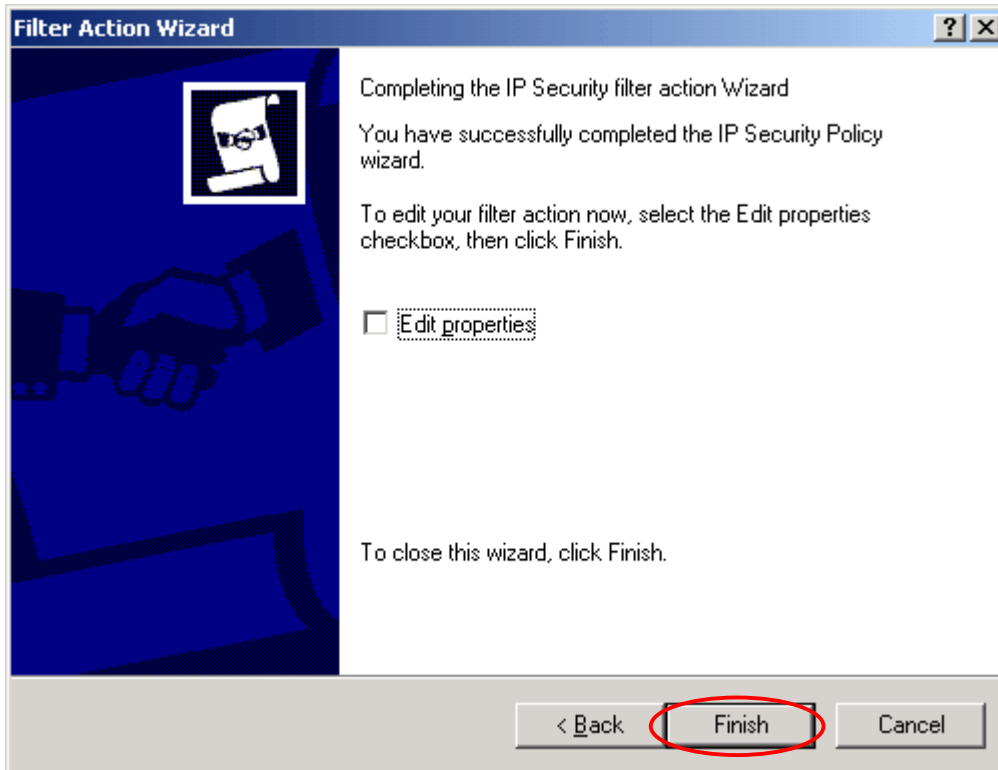
34. Check **Data integrity and encryption (ESP)**, select **Integrity algorithm (MD5)** and **Encryption algorithm (3DES)**, and then click **OK**.



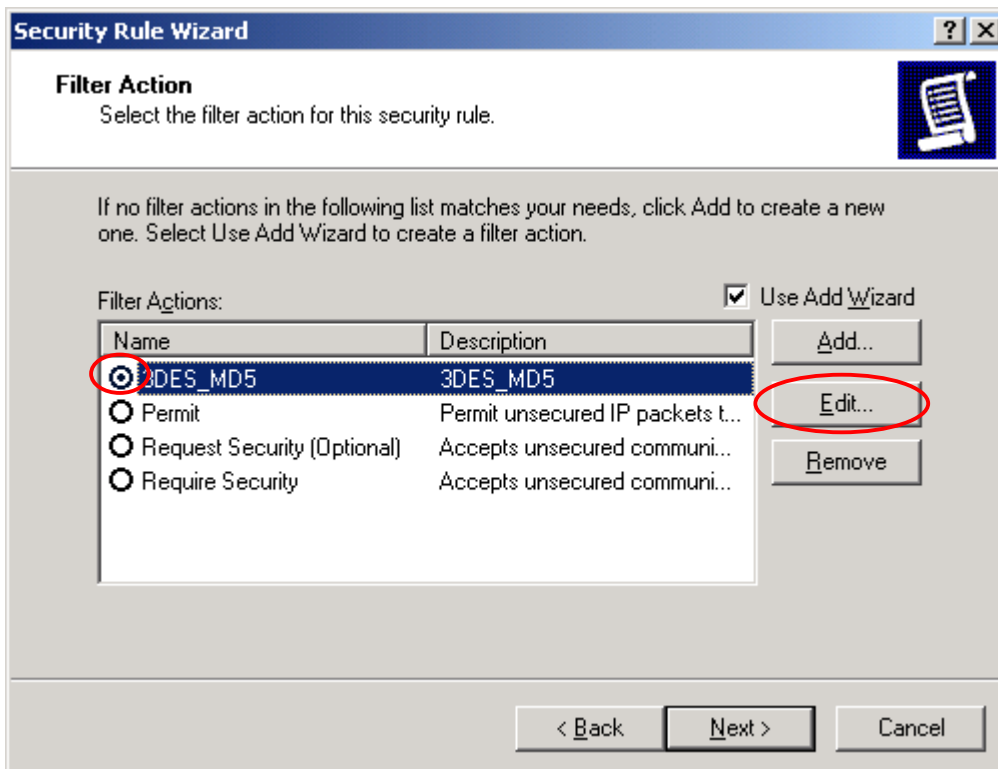
35. Click **Next**.



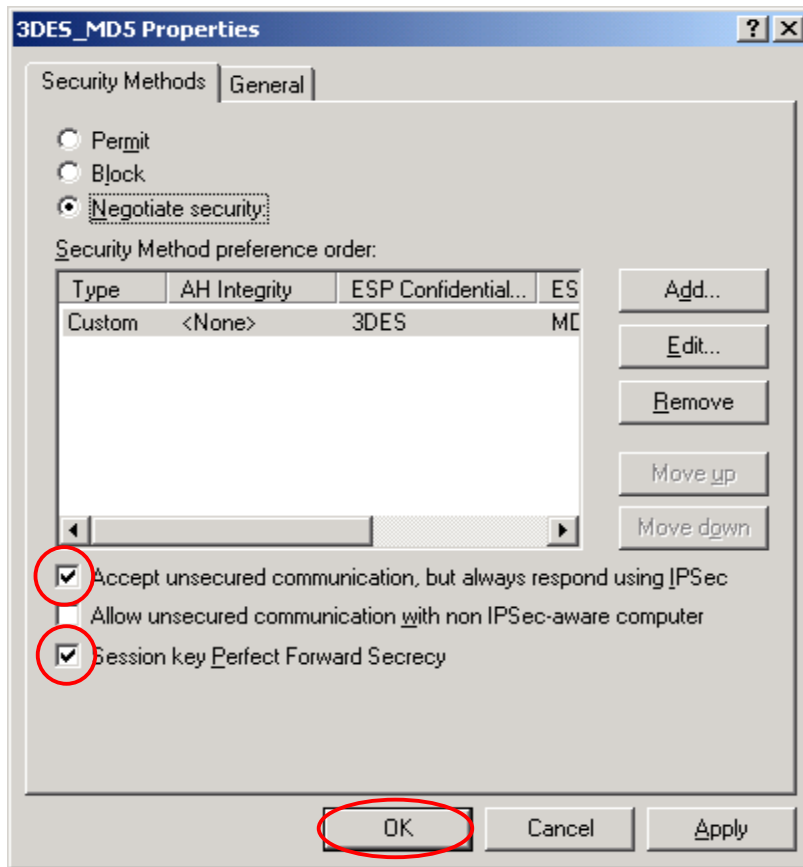
36. Click **Finish**.



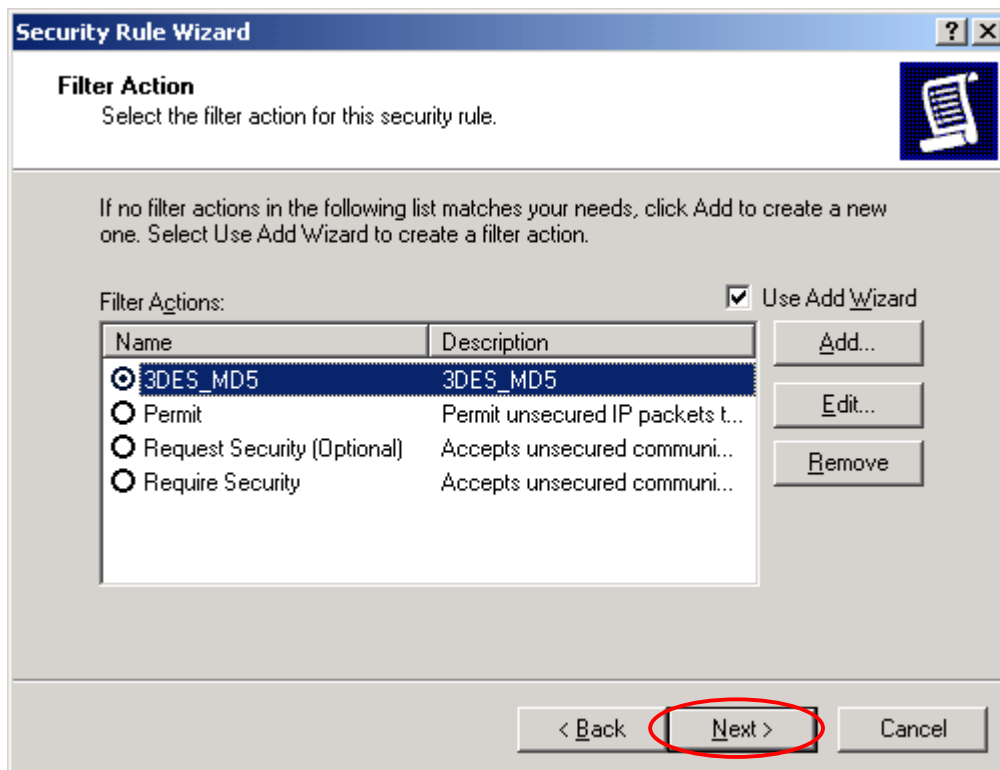
37. Select **3DES_MD5** and then click **Edit**.



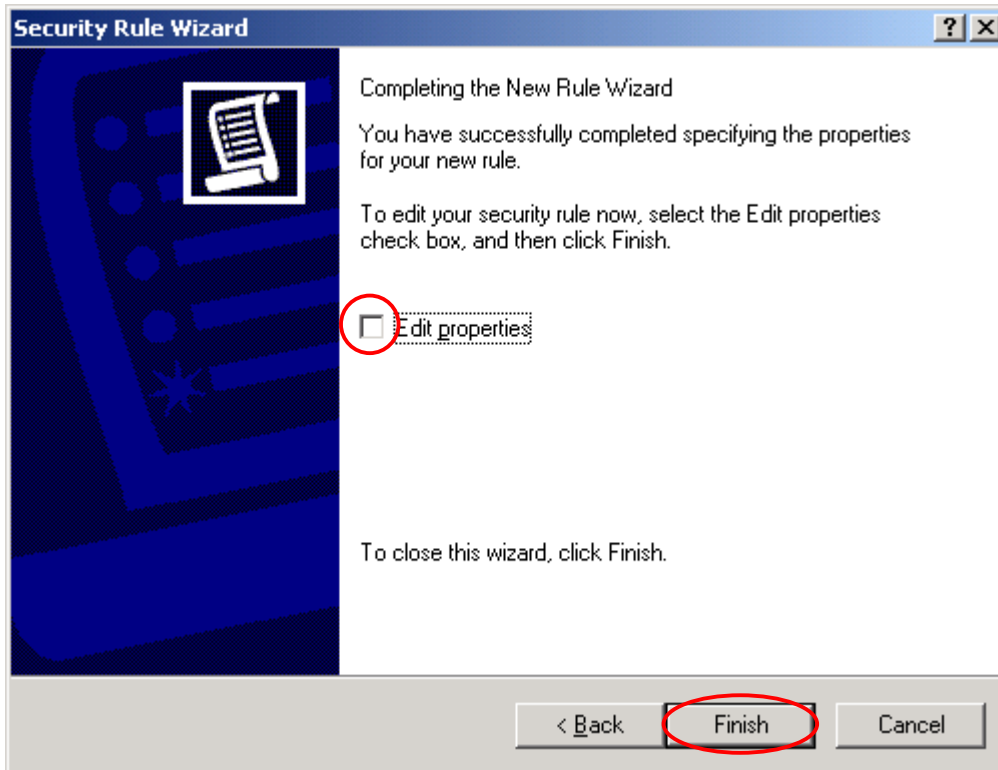
38. Check **Accept unsecured communications** and **Session key Perfect Forward Secrecy**, and then click **OK**.



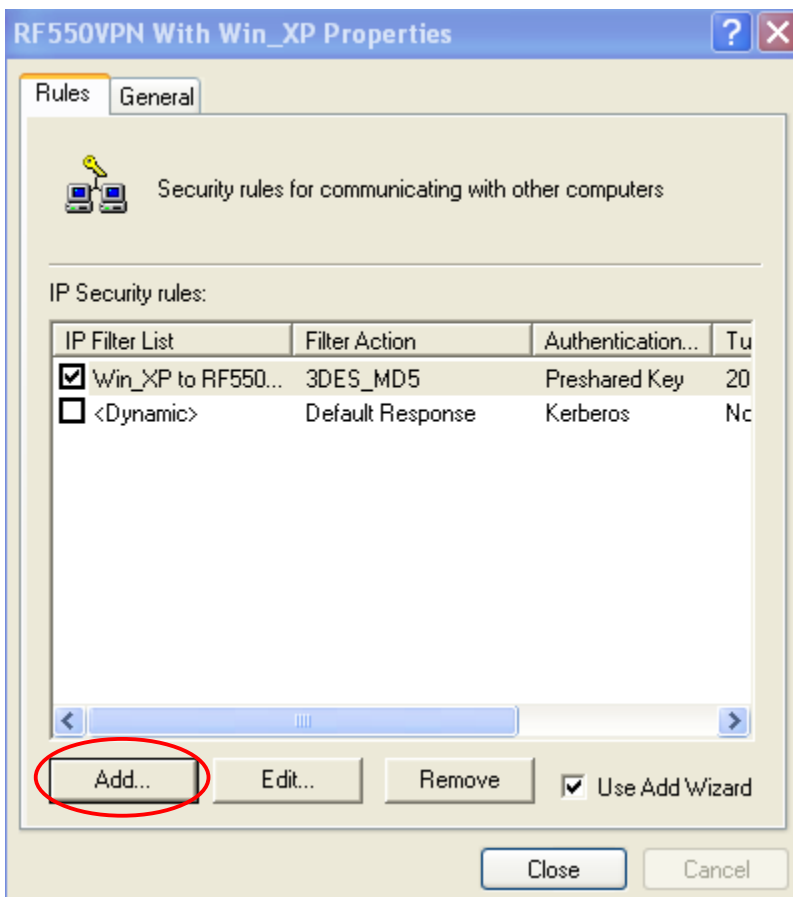
39. Click **Next**.



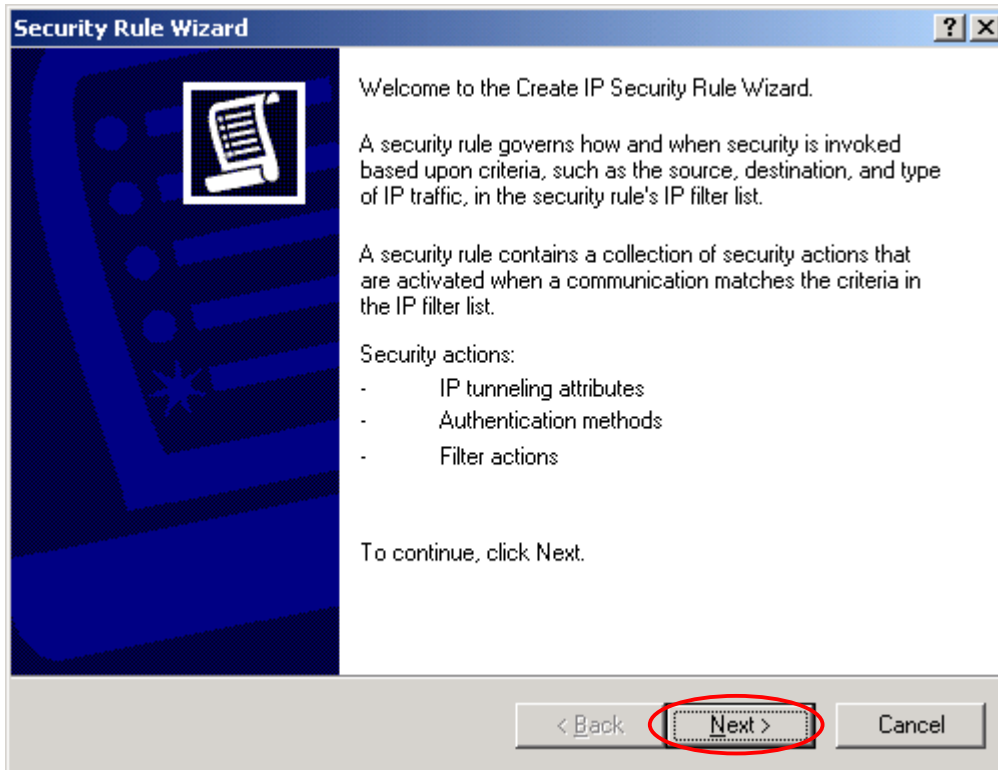
40. Uncheck **Edit properties** and click **Finish**.



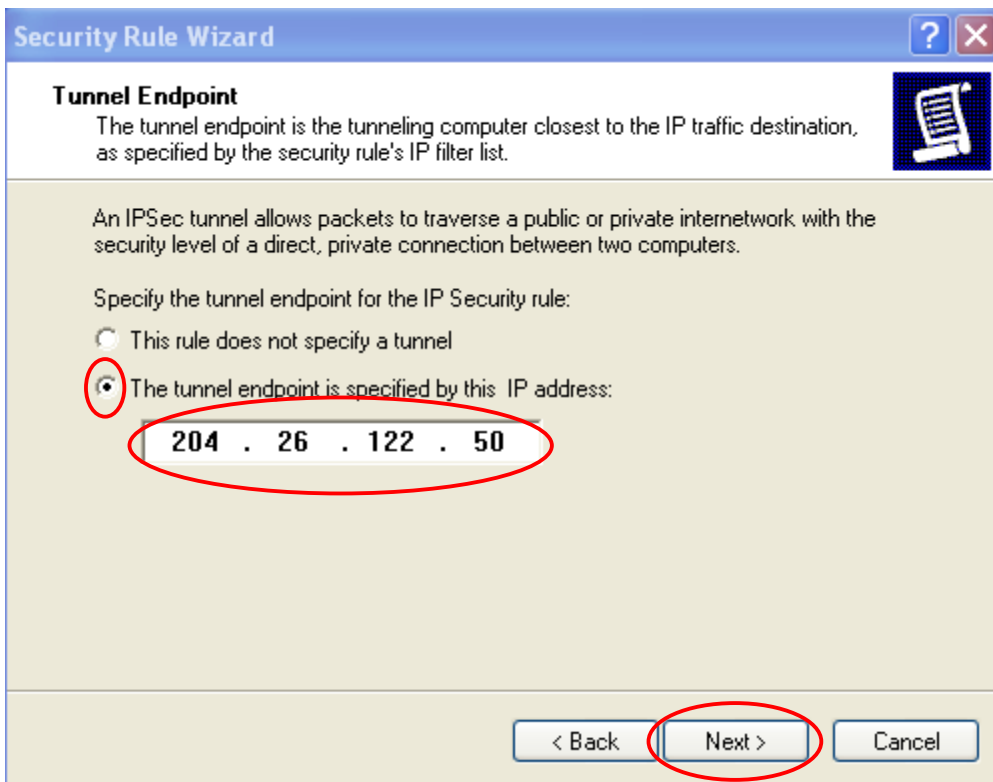
41. Click **Add**.



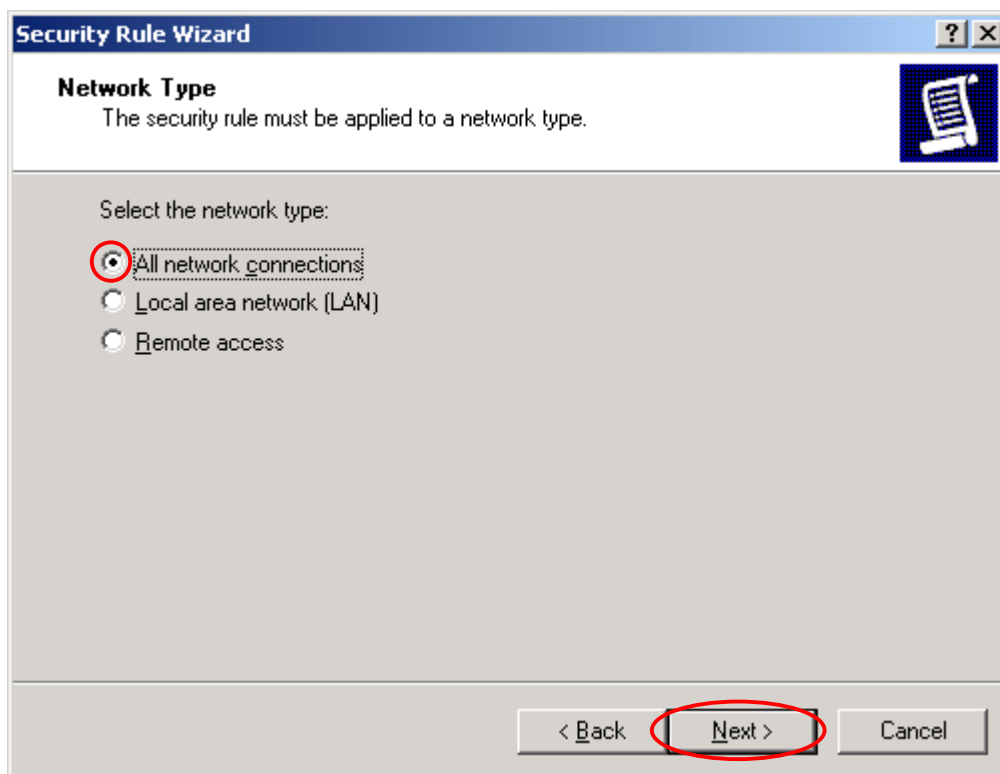
42. Click **Next**.



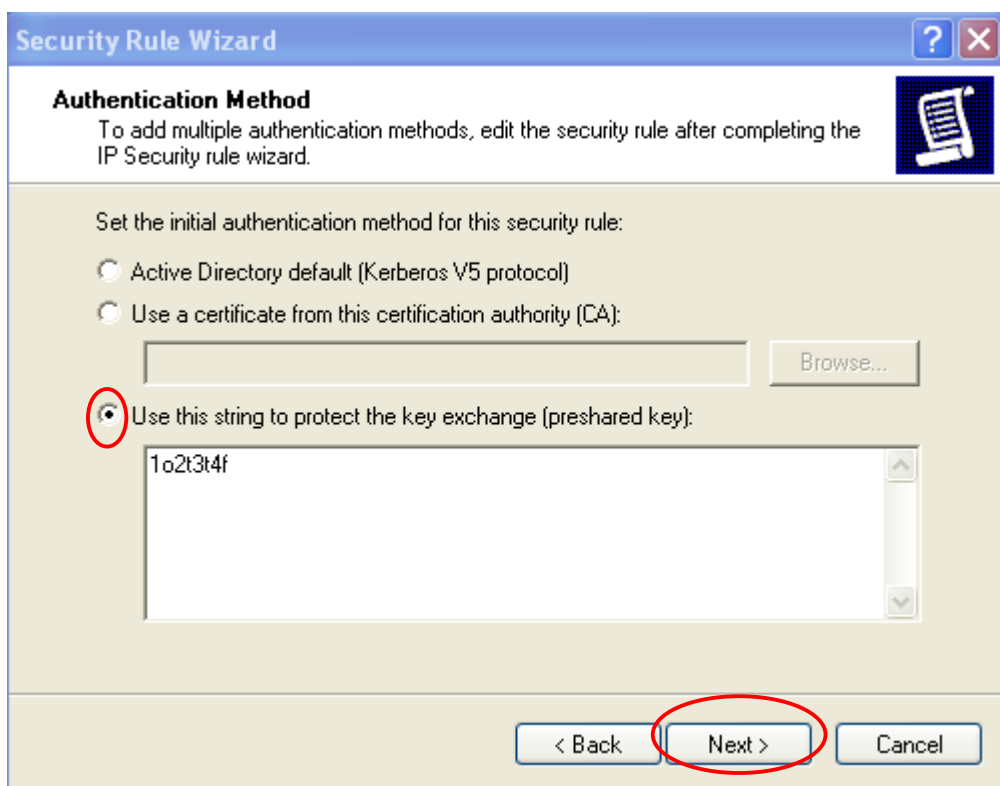
43. Input IP Address into **The tunnel endpoint specified by this IP address:** and then click **Next**. (Ex: Windows XP Professional IP Address 204.26.122.50)



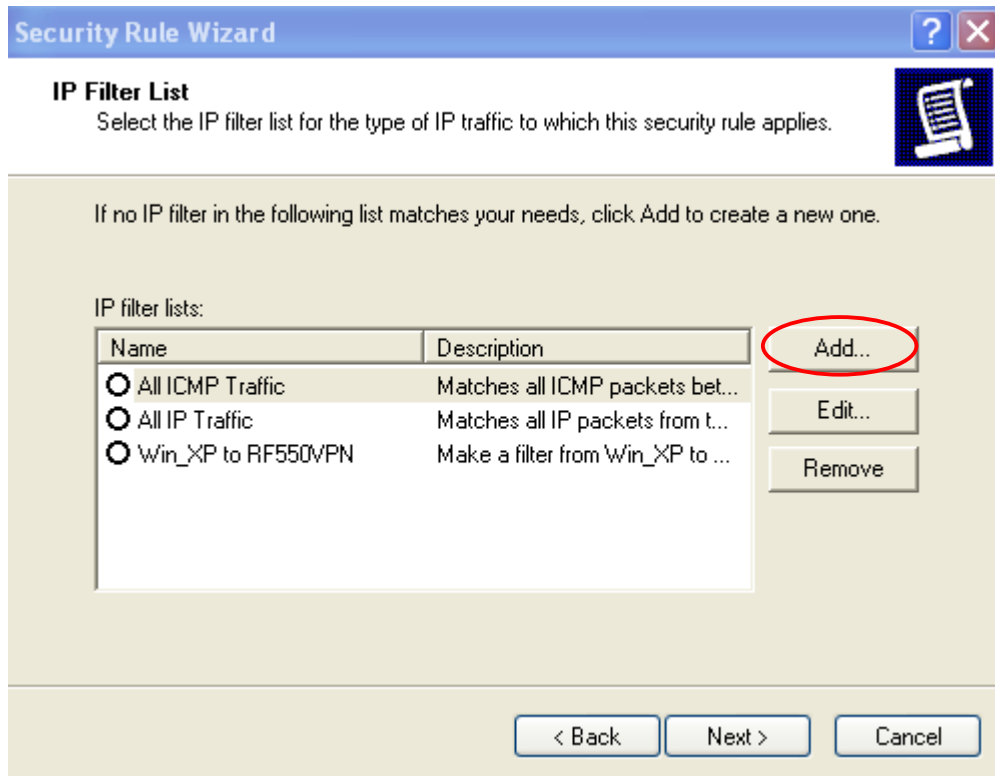
44. Choose **All network connections**, and then click **Next**.



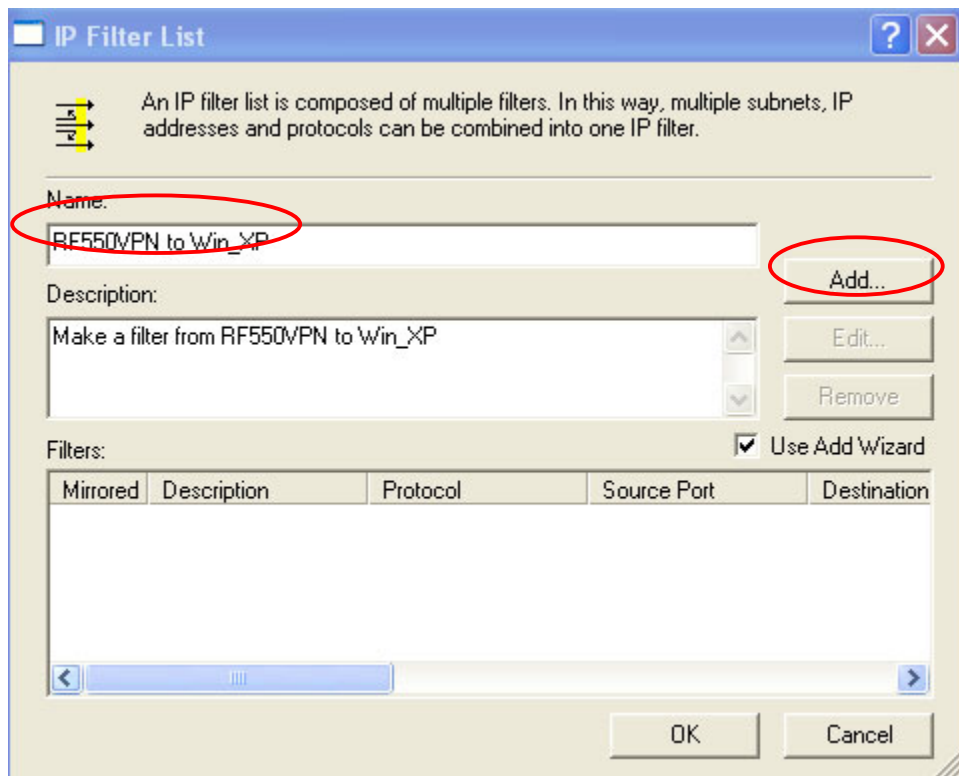
45. Choose **Use this string to protect the key exchange (preshared key)**. Enter the key code, and then click **Next**. (Ex: RF550VPN/RF560VPN preshared key 1o2t3t4f)



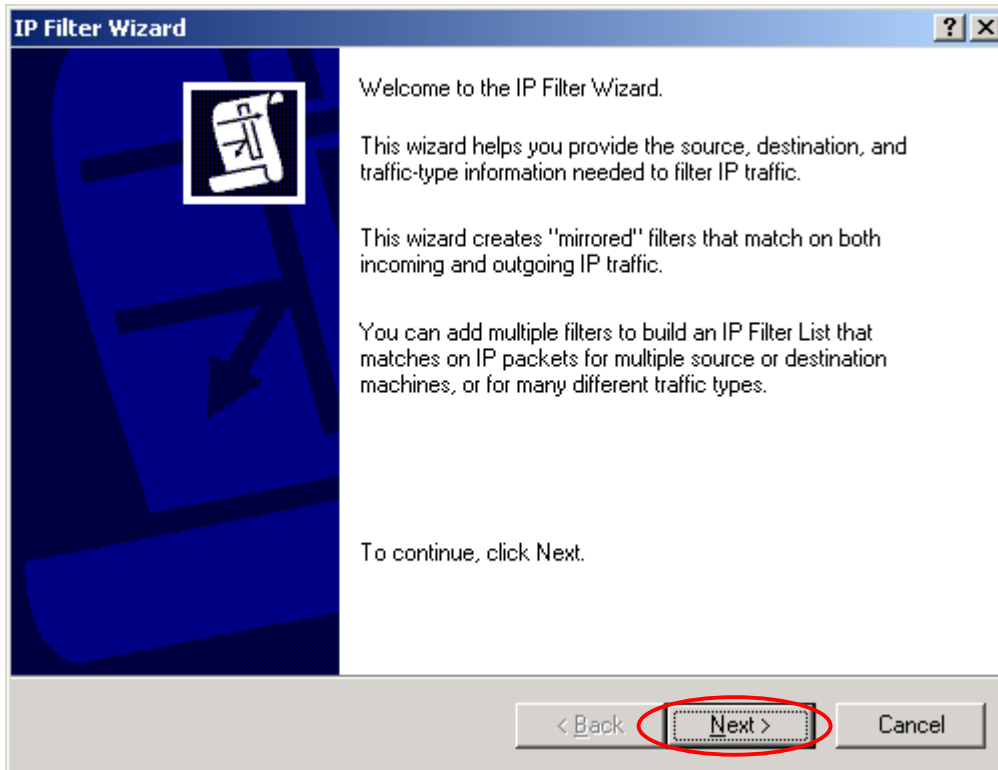
46. Click **Add**.



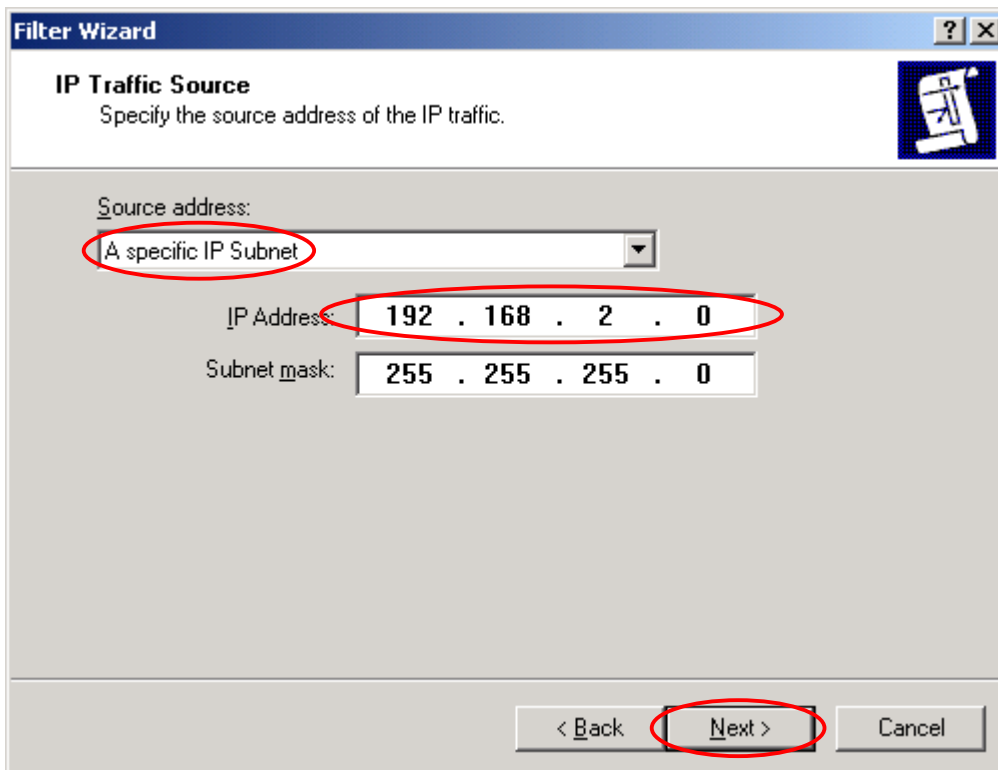
47. Type a filter name and description and then click **Add**.



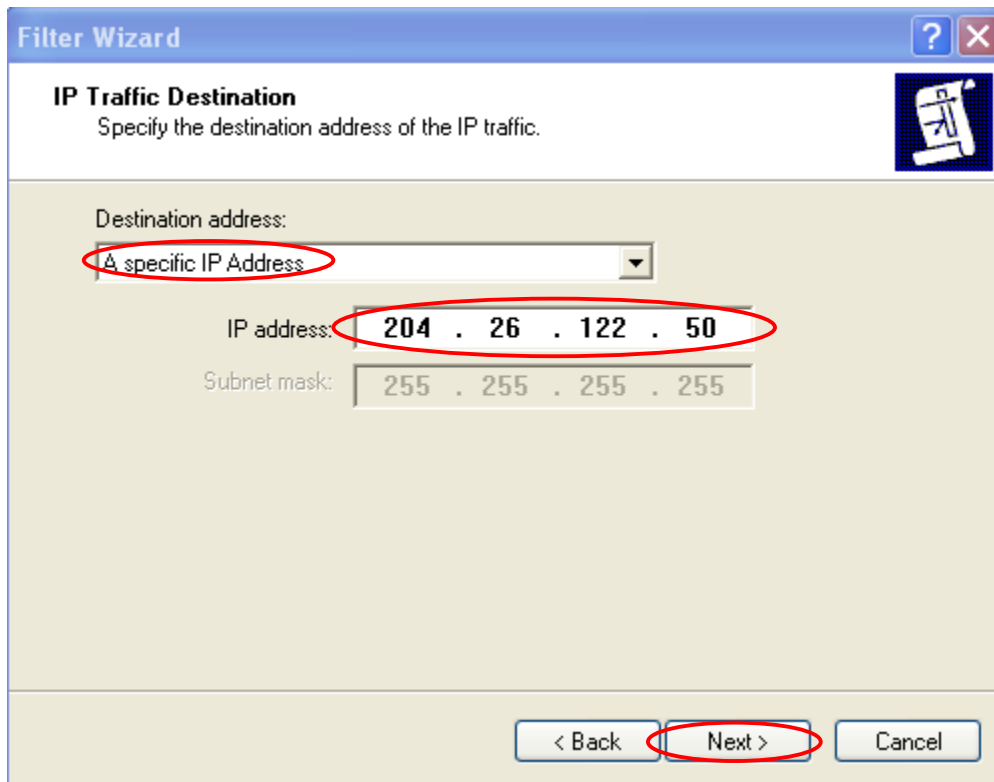
48. Click **Next**.



49. Select **"A specific IP Subnet"** and input Source address and then click **"Next."**
(Ex: RF550VPN/RF560VPN Private network(LAN) 192.168.2.0)

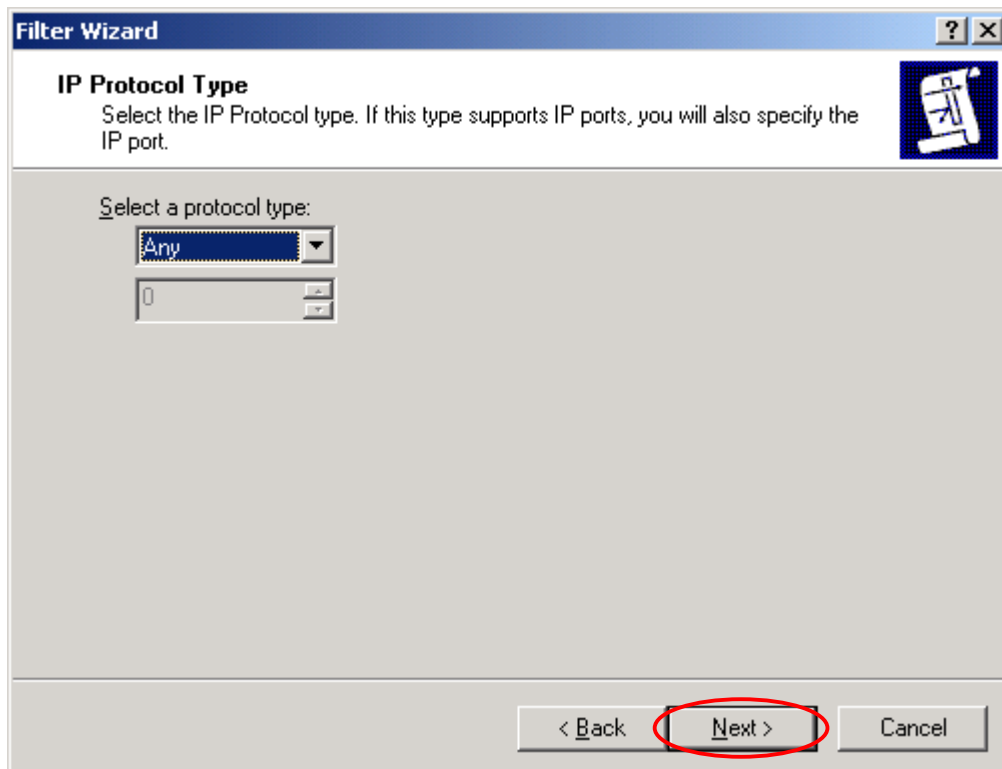


50. Select **A specific IP Address** and input destination IP address and then click **Next**.
(Ex: Windows XP Professional IP address 204.26.122.50)



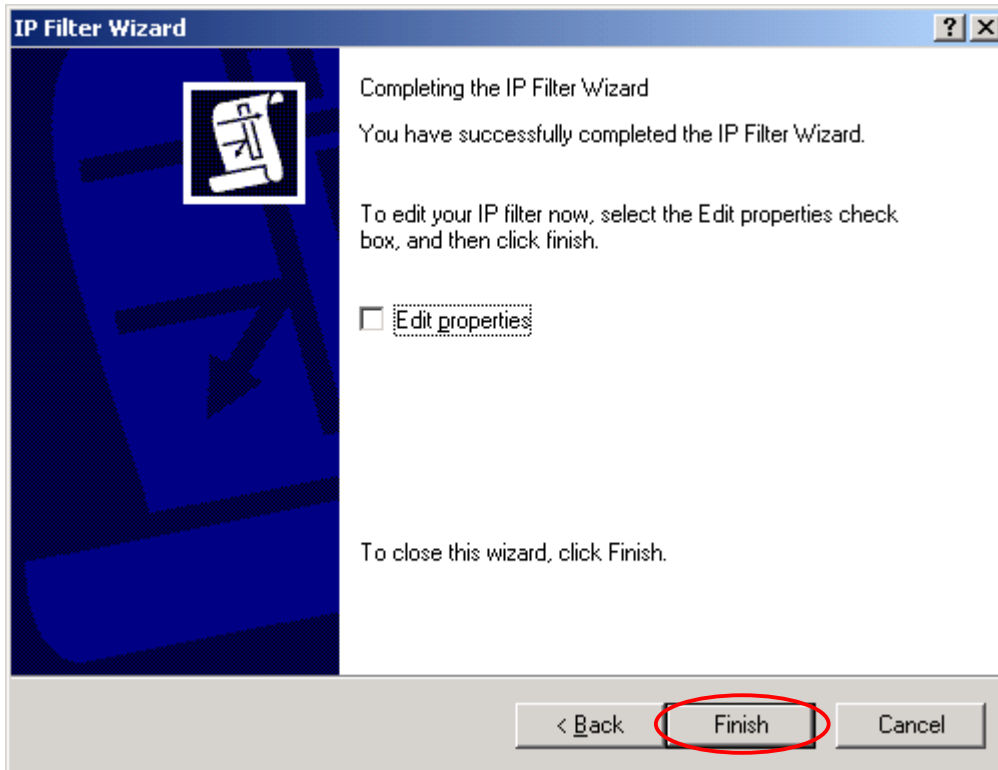
The screenshot shows the 'Filter Wizard' window with the 'IP Traffic Destination' tab selected. The instruction 'Specify the destination address of the IP traffic.' is displayed. The 'Destination address:' dropdown menu is set to 'A specific IP Address'. Below it, the 'IP address:' field contains '204 . 26 . 122 . 50' and the 'Subnet mask:' field contains '255 . 255 . 255 . 255'. At the bottom, the 'Next >' button is highlighted with a red circle.

51. Click **Next**.

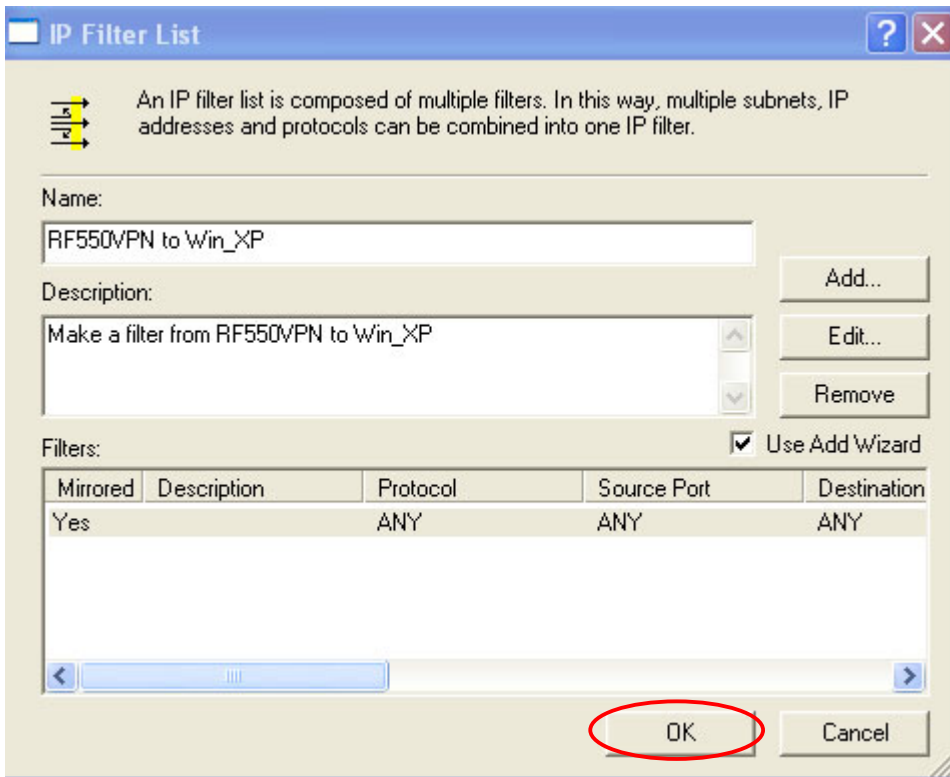


The screenshot shows the 'Filter Wizard' window with the 'IP Protocol Type' tab selected. The instruction 'Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.' is displayed. The 'Select a protocol type:' dropdown menu is set to 'Any'. Below it, there is an empty field for specifying a port. At the bottom, the 'Next >' button is highlighted with a red circle.

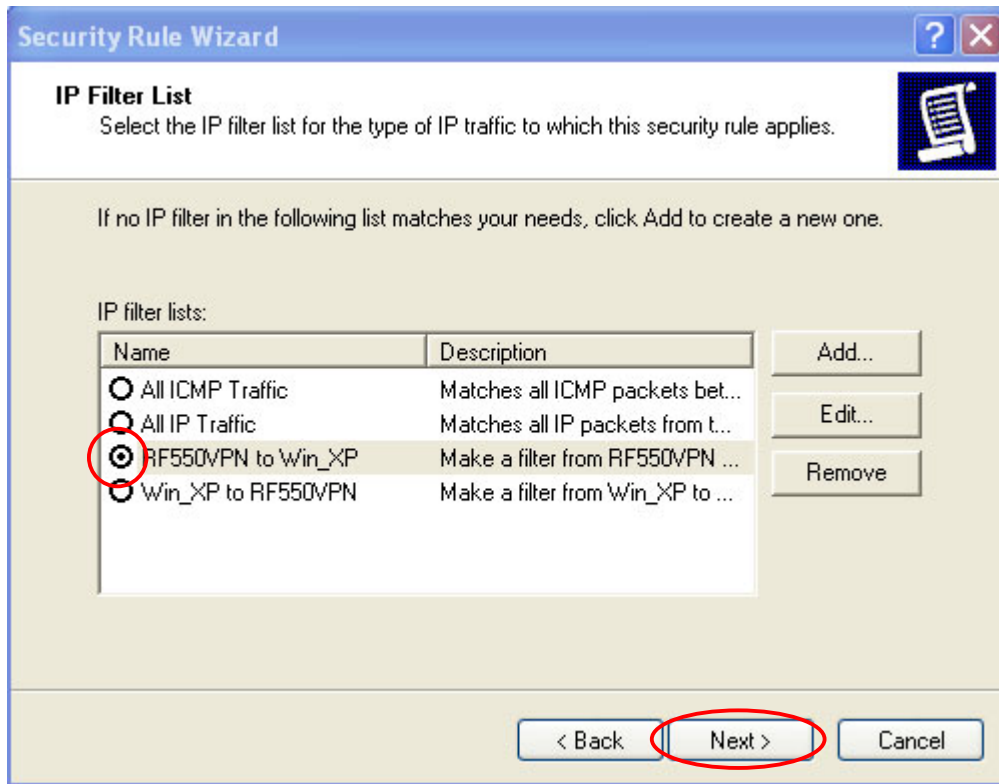
52. Click **Finish**.



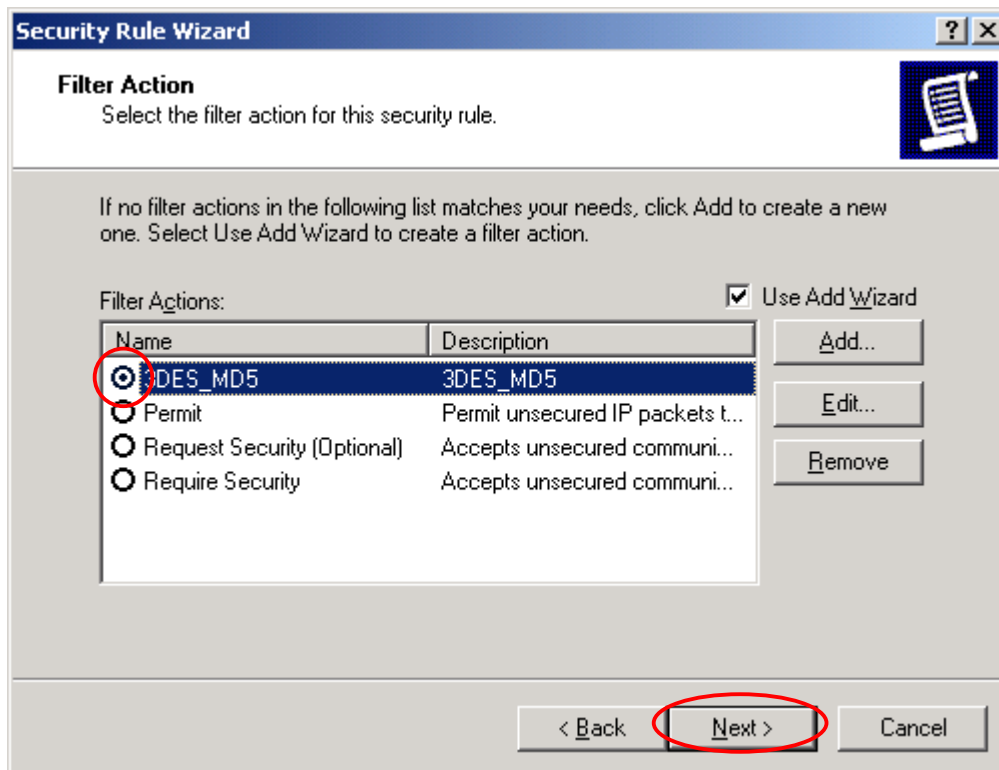
53. Click **OK**. For Win 2K click on **Close**.



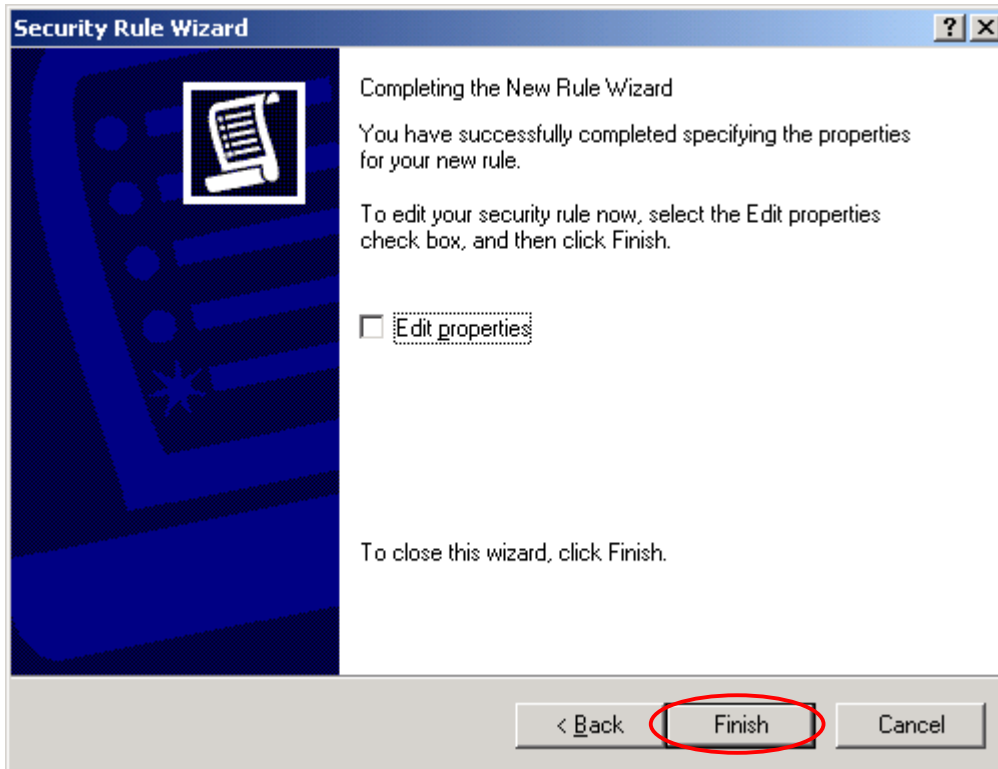
54. Select **RF550VPN/RF560VPN to Win_XP**, and then click **Next**.



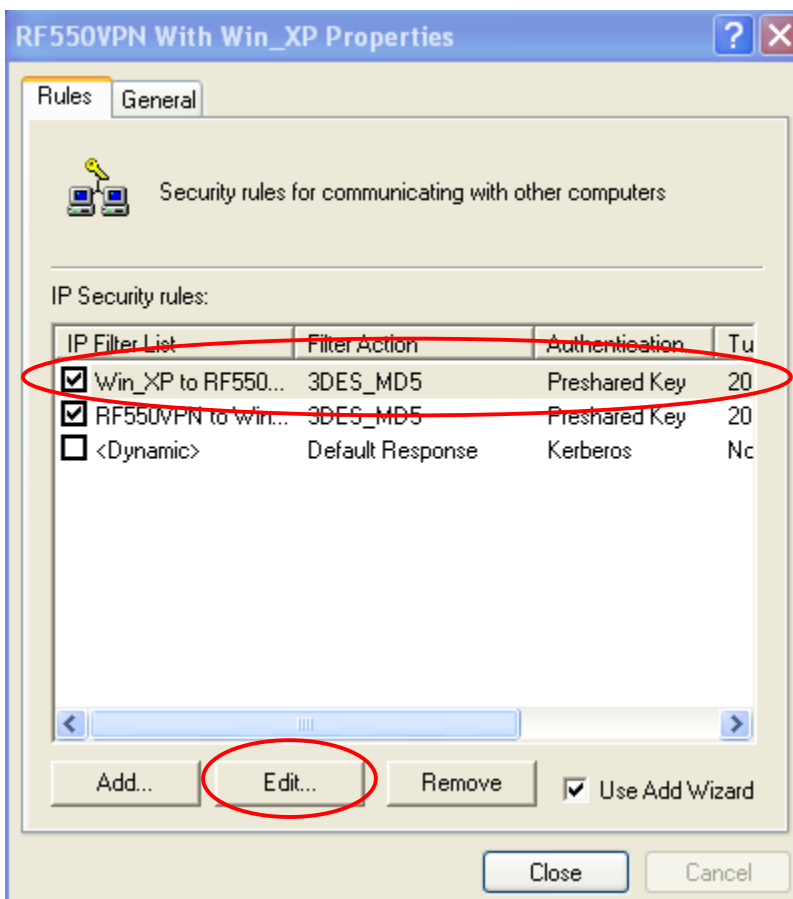
55. Choose **3DES_MD5** and then click **Next**.



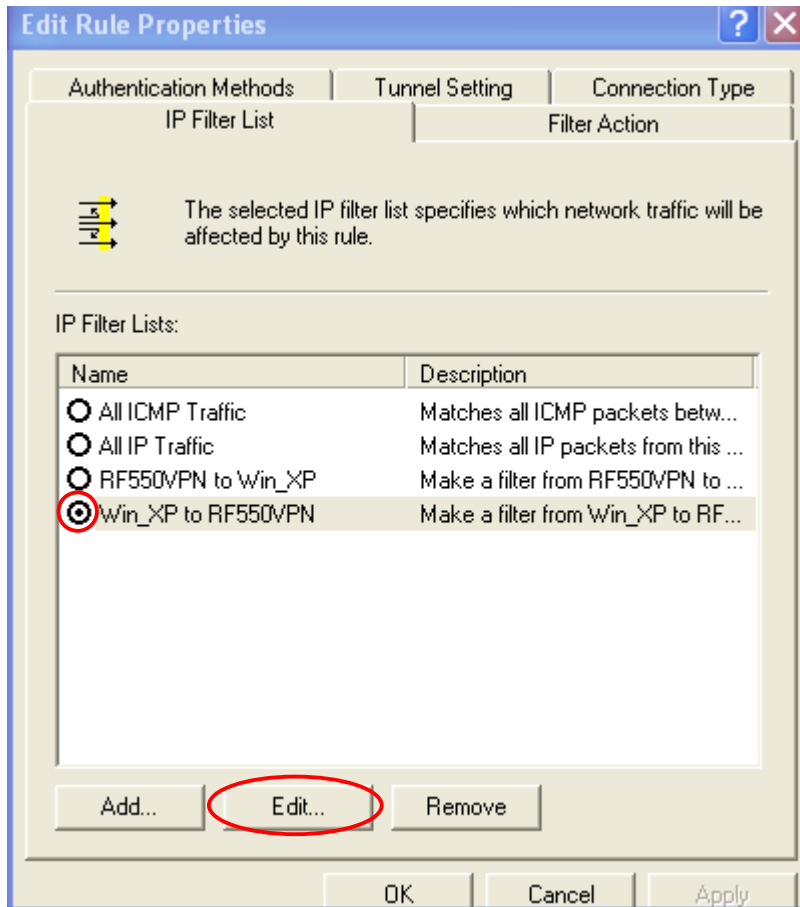
56. Click **Finish**.



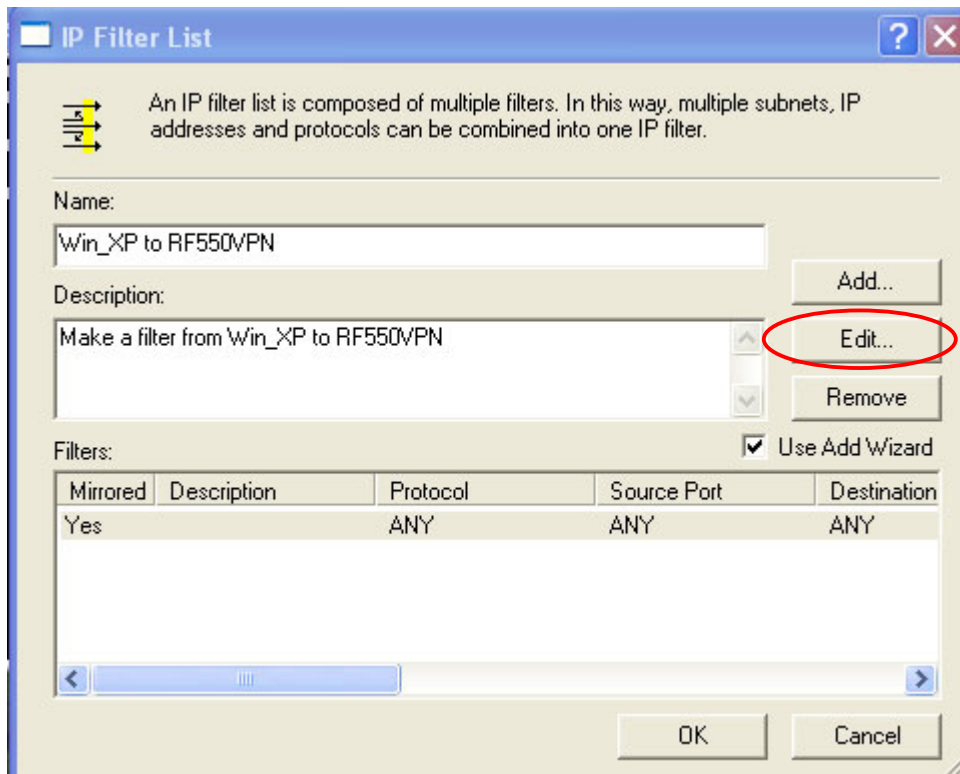
57. Highlight **Win_XP to RF550VPN/RF560VPN** and then click **Edit**.



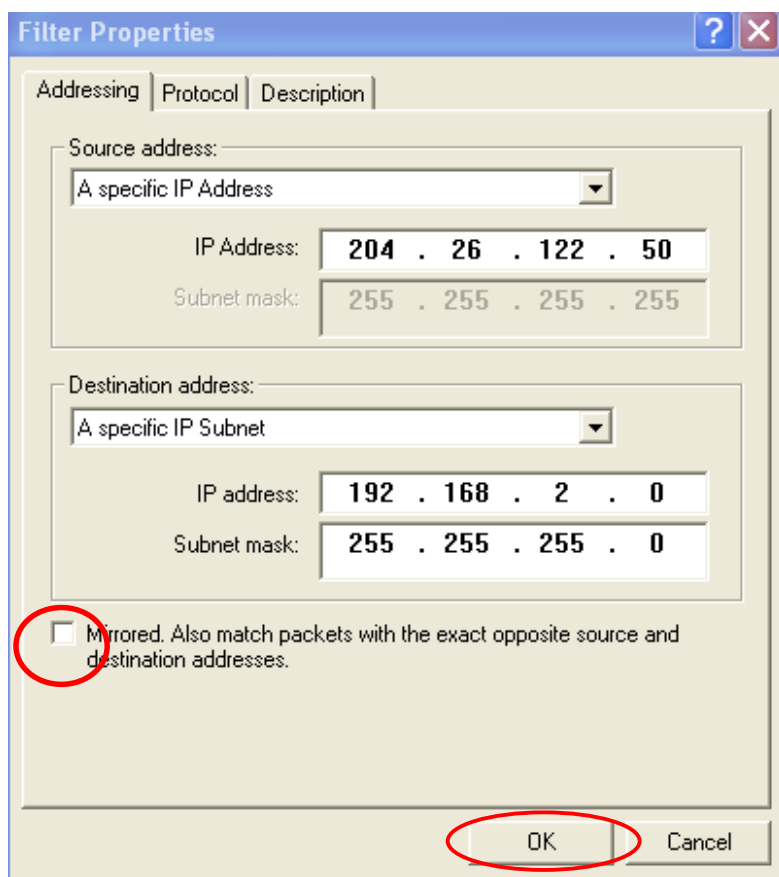
58. Select **Win_XP to RF550VPN/RF560VPN** and then click **Edit**.



59. Click **Edit**.



60. Uncheck **Mirrored**. Also match packets with exact opposite source and destination address and then click **OK**.



The **Filter Properties** dialog box has three tabs: **Addressing**, **Protocol**, and **Description**. The **Addressing** tab is active.

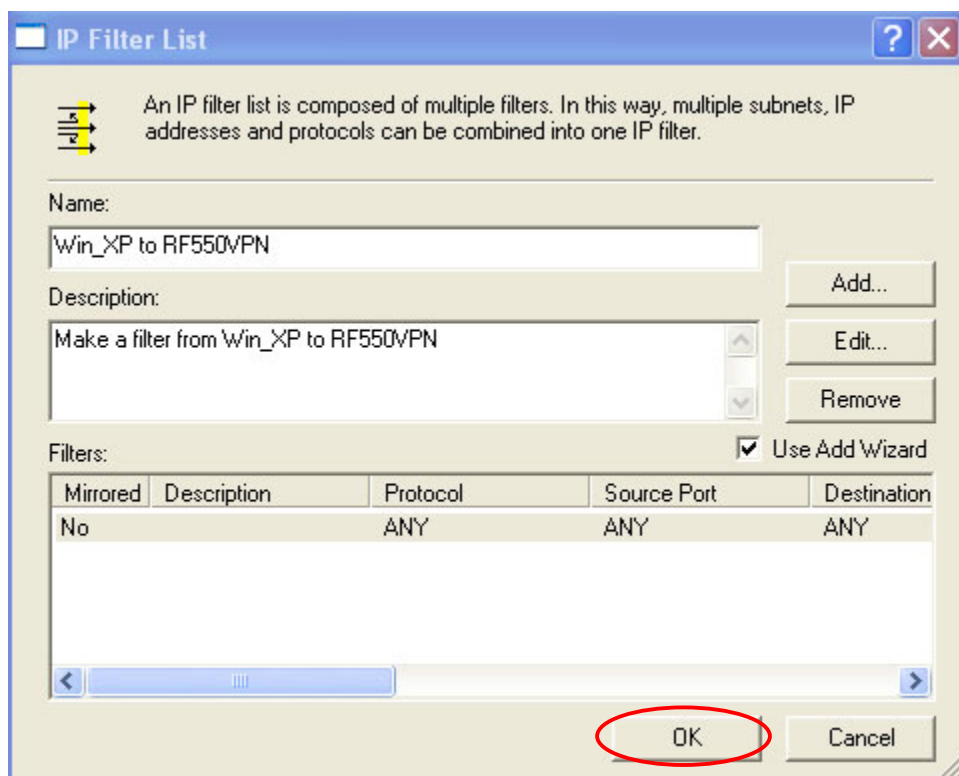
Source address:
 A specific IP Address
 IP Address: 204 . 26 . 122 . 50
 Subnet mask: 255 . 255 . 255 . 255

Destination address:
 A specific IP Subnet
 IP address: 192 . 168 . 2 . 0
 Subnet mask: 255 . 255 . 255 . 0

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

OK **Cancel**

61. Click **OK**. For Win 2K click on **Close**.



The **IP Filter List** dialog box contains the following information:

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:
Win_XP to RF550VPN

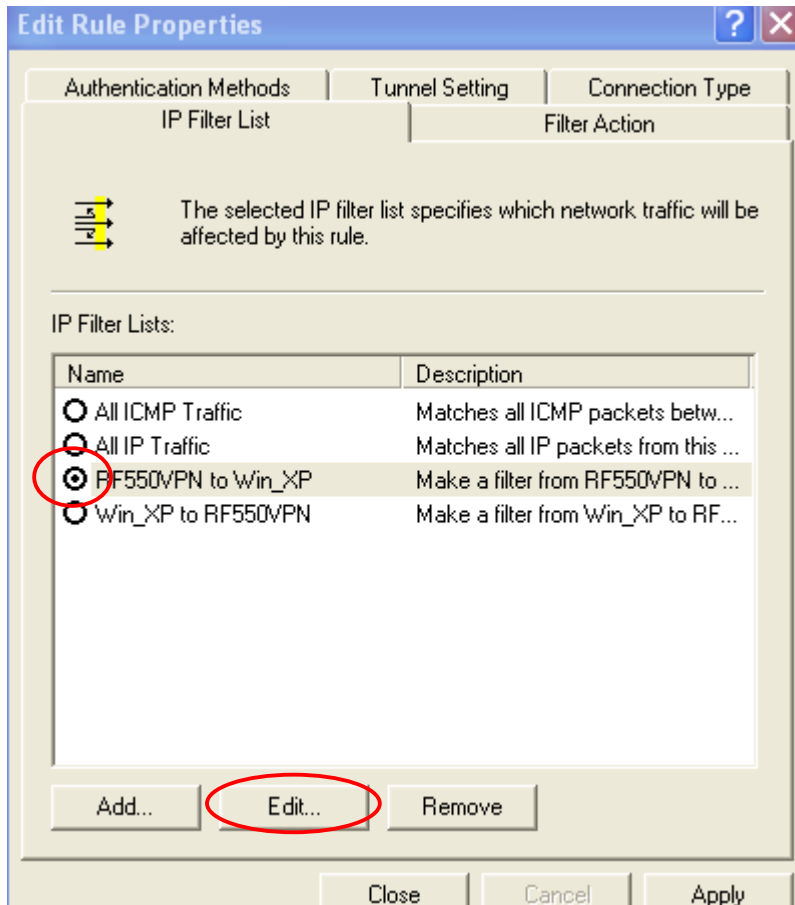
Description:
Make a filter from Win_XP to RF550VPN

Filters: ☒ Use Add Wizard

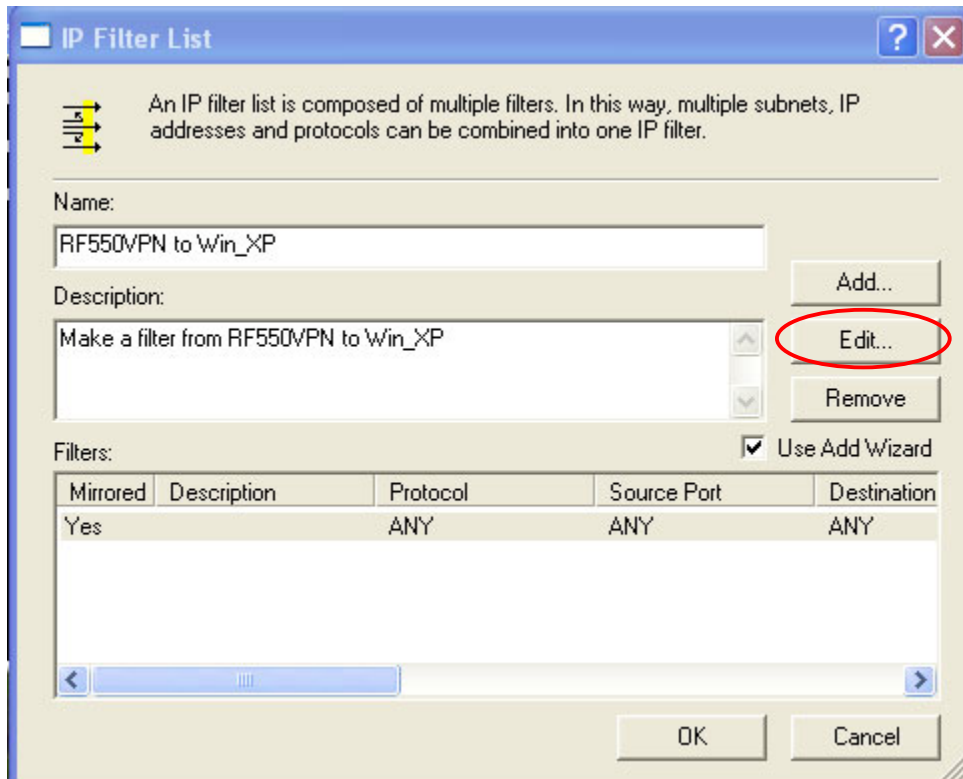
| Mirrored | Description | Protocol | Source Port | Destination |
|----------|-------------|----------|-------------|-------------|
| No | | ANY | ANY | ANY |

OK **Cancel**

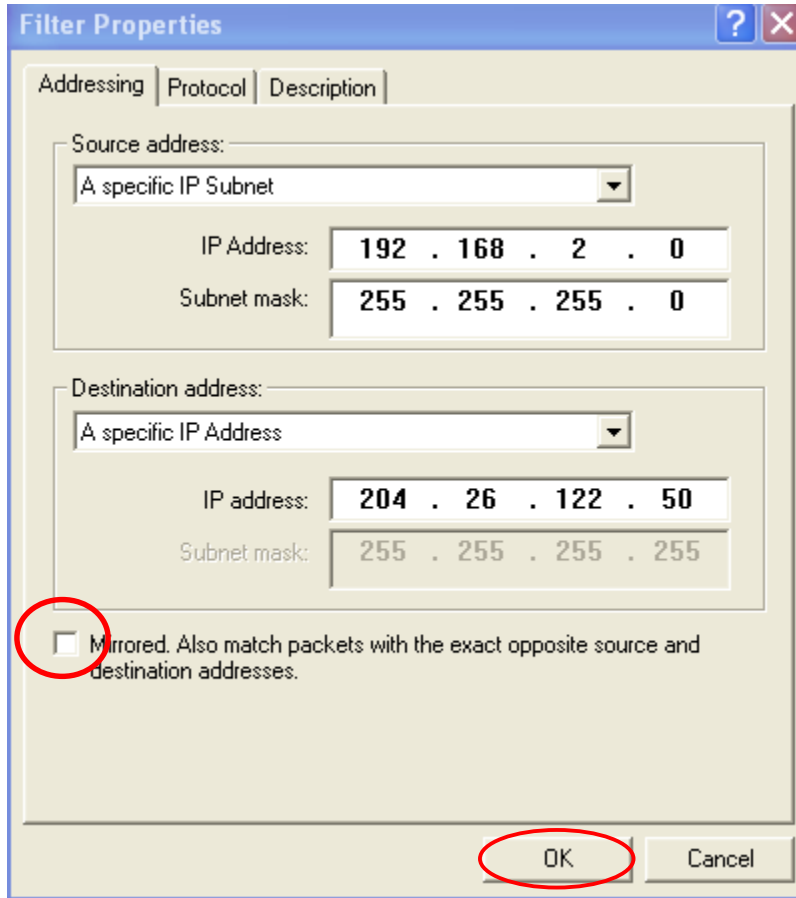
62. Choose **RF550VPN/RF560VPN to Win_XP** and then click **Edit**.



63. Click **Edit**.



64. Uncheck **Mirrored**. Also match packets with exact opposite source and destination address and then click **OK**.



The **Filter Properties** dialog box has three tabs: **Addressing**, **Protocol**, and **Description**. The **Addressing** tab is active.

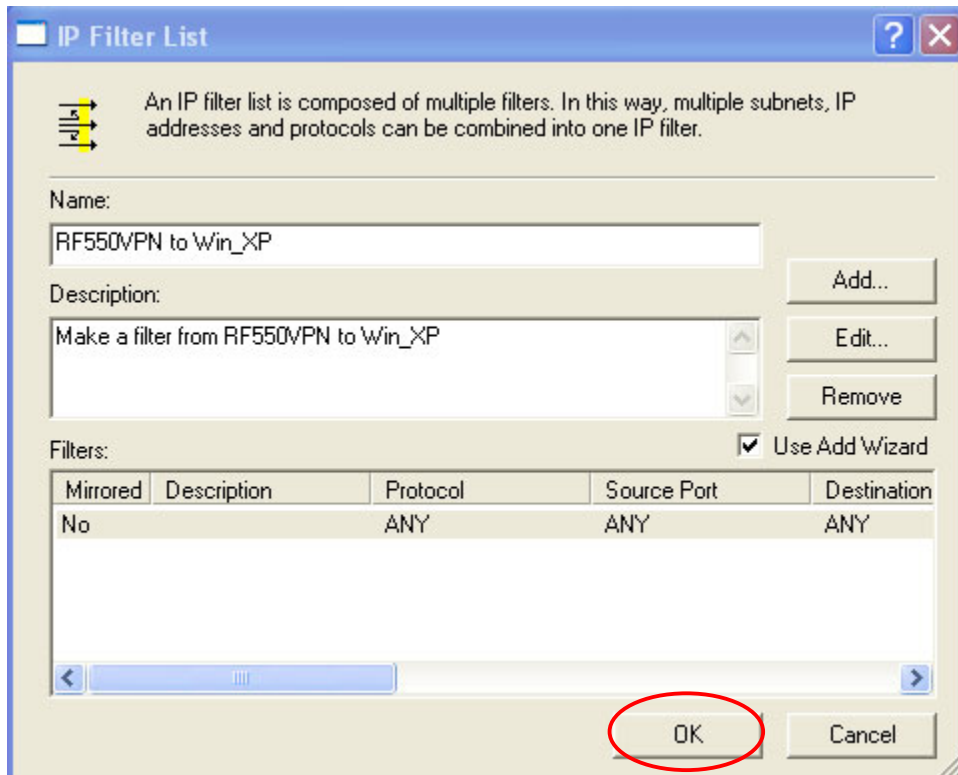
Source address:
 A specific IP Subnet (dropdown)
 IP Address: 192 . 168 . 2 . 0
 Subnet mask: 255 . 255 . 255 . 0

Destination address:
 A specific IP Address (dropdown)
 IP address: 204 . 26 . 122 . 50
 Subnet mask: 255 . 255 . 255 . 255

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

OK (circled) **Cancel**

65. Click **OK**. For Win 2K click on **Close**.



The **IP Filter List** dialog box has a title bar with a minus sign, maximize, and close button. Below the title bar is a help icon and a text box: "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:
 RF550VPN to Win_XP

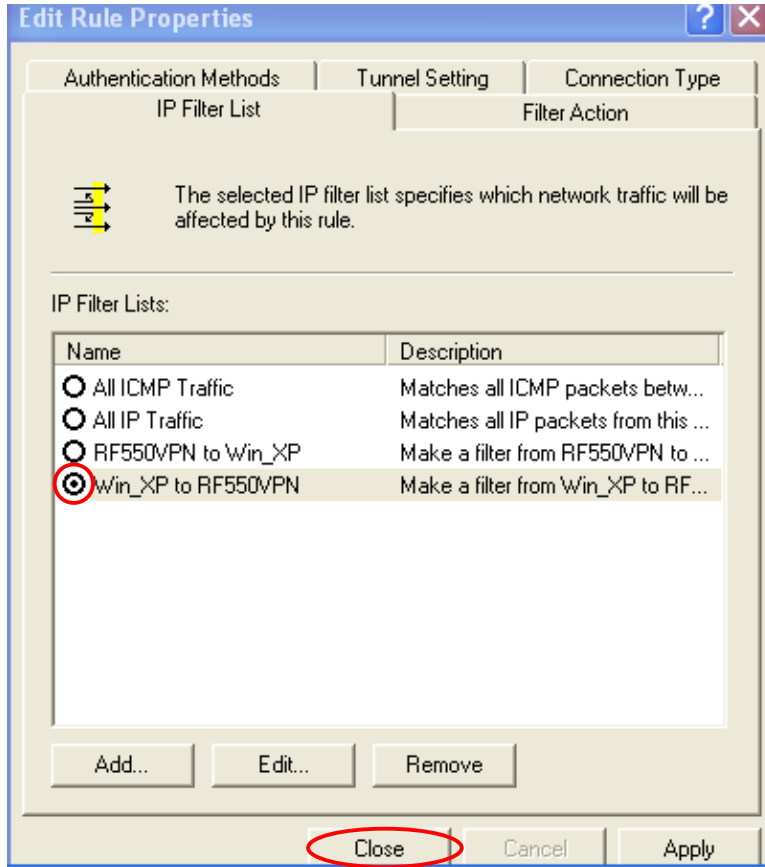
Description:
 Make a filter from RF550VPN to Win_XP

Filters: ☒ Use Add Wizard

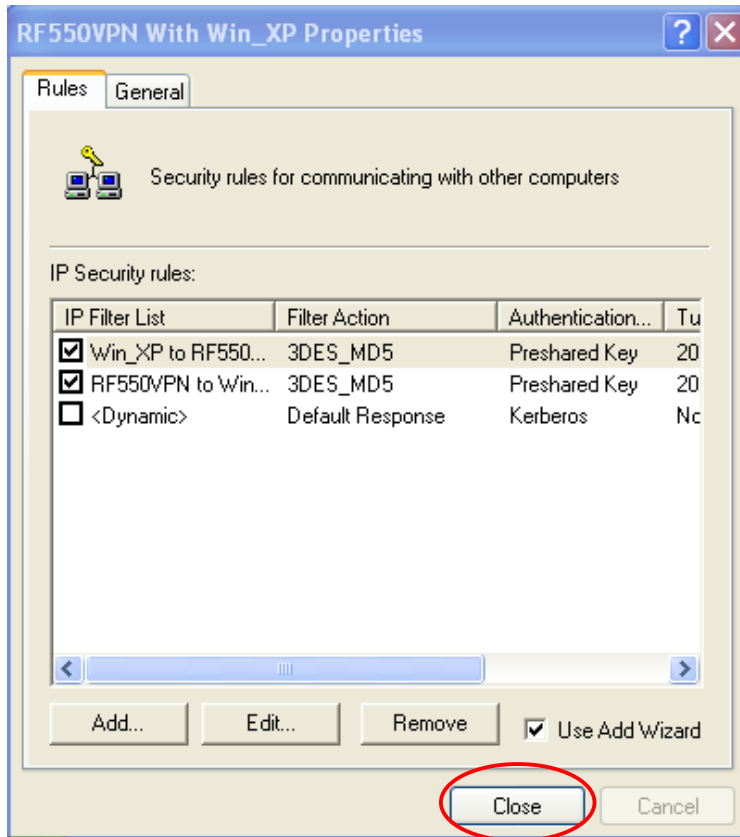
| Mirrored | Description | Protocol | Source Port | Destination |
|----------|-------------|----------|-------------|-------------|
| No | | ANY | ANY | ANY |

OK (circled) **Cancel**

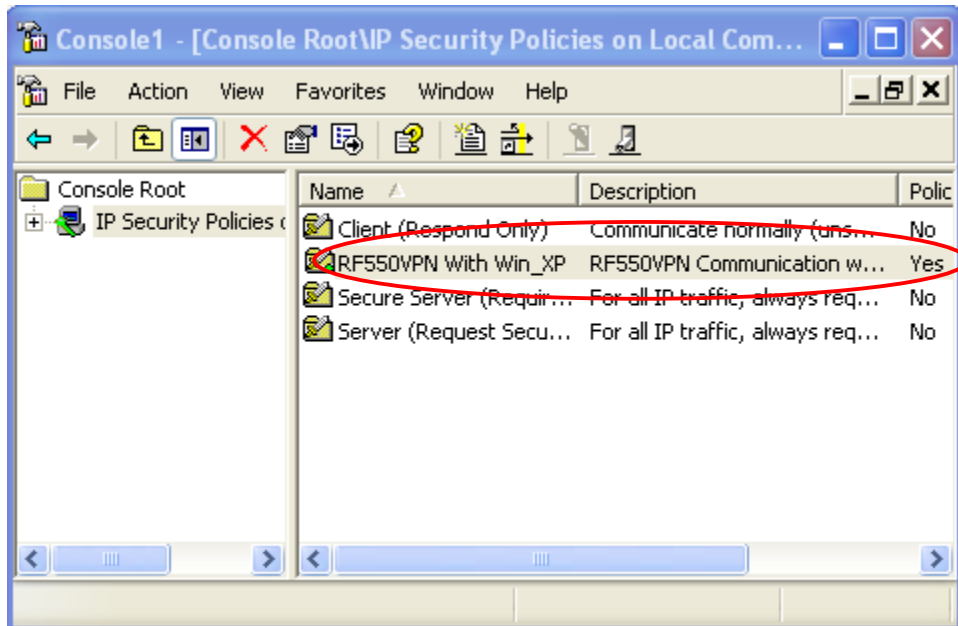
66. Highlight **Win_XP to RF550VPN/RF560VPN** and make sure a dot is in the circle for this selection, and then click **Close**.



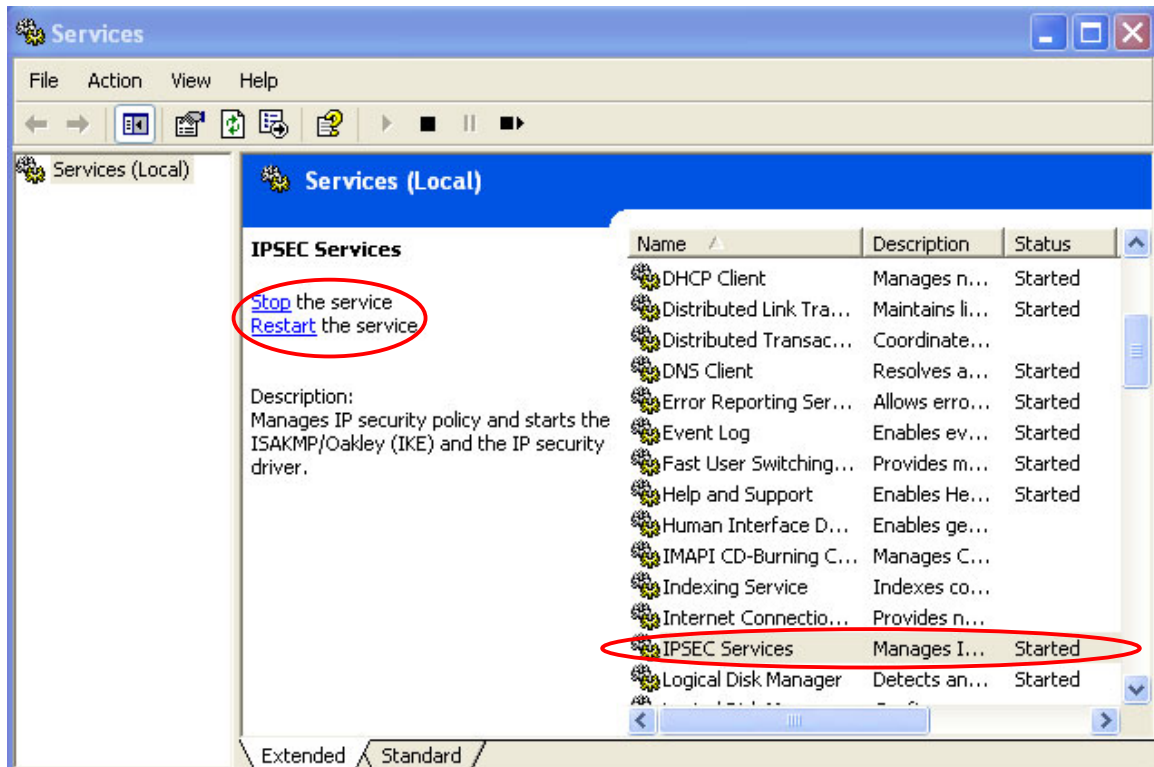
67. Click **Close**.



68. Click right button on **RF550VPN/RF560VPN with Win_XP** and click **Assign**. The **Policy Assigned** column will change from **No** to **Yes** for this item.



69. Now you want to verify that IPsec Services have been started. To do this, left click **Start** in the lower left corner of the screen; then click **Administrative Tools**; then **Services**, and then **IPSEC Services**. Start **IPSEC Services**.



70. Ping Remote private network (192.168.2.100) on Dos Command Mode. After several failures, you should see successful replies. If this fails, check your cabling, RF550VPN/RF560VPN configuration and Win XP IPsec configuration.

```

C:\> Command Prompt - ping 192.168.2.100 -t

Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127
Reply from 192.168.2.100: bytes=32 time=3ms TTL=127

```