

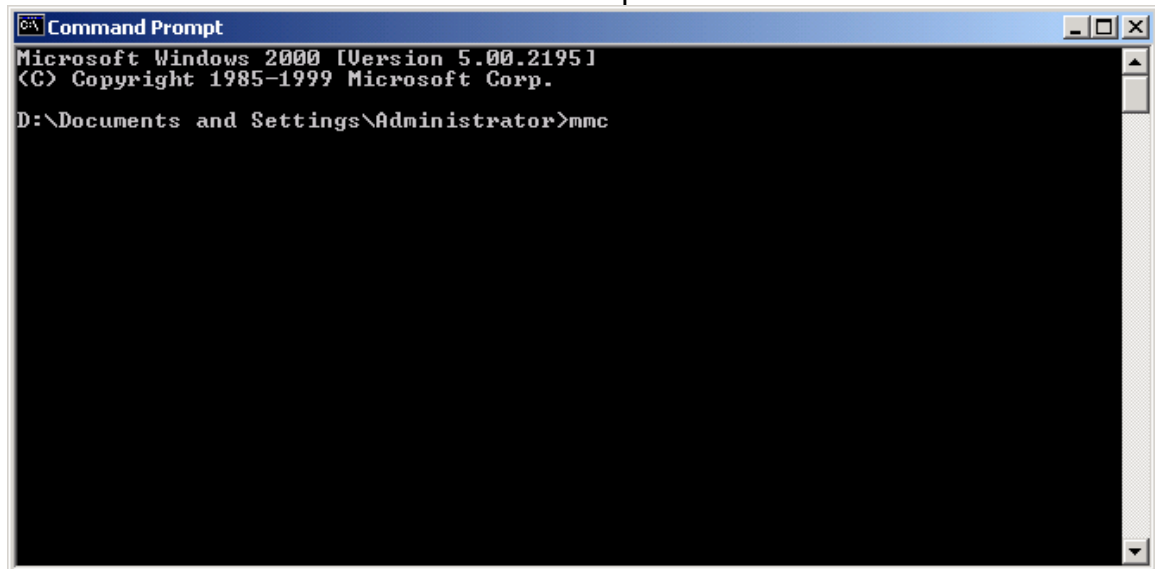
DI-804V With Windows 2000 Advanced Server IPSec VPN Configuration Procedures

Document version: 1.0

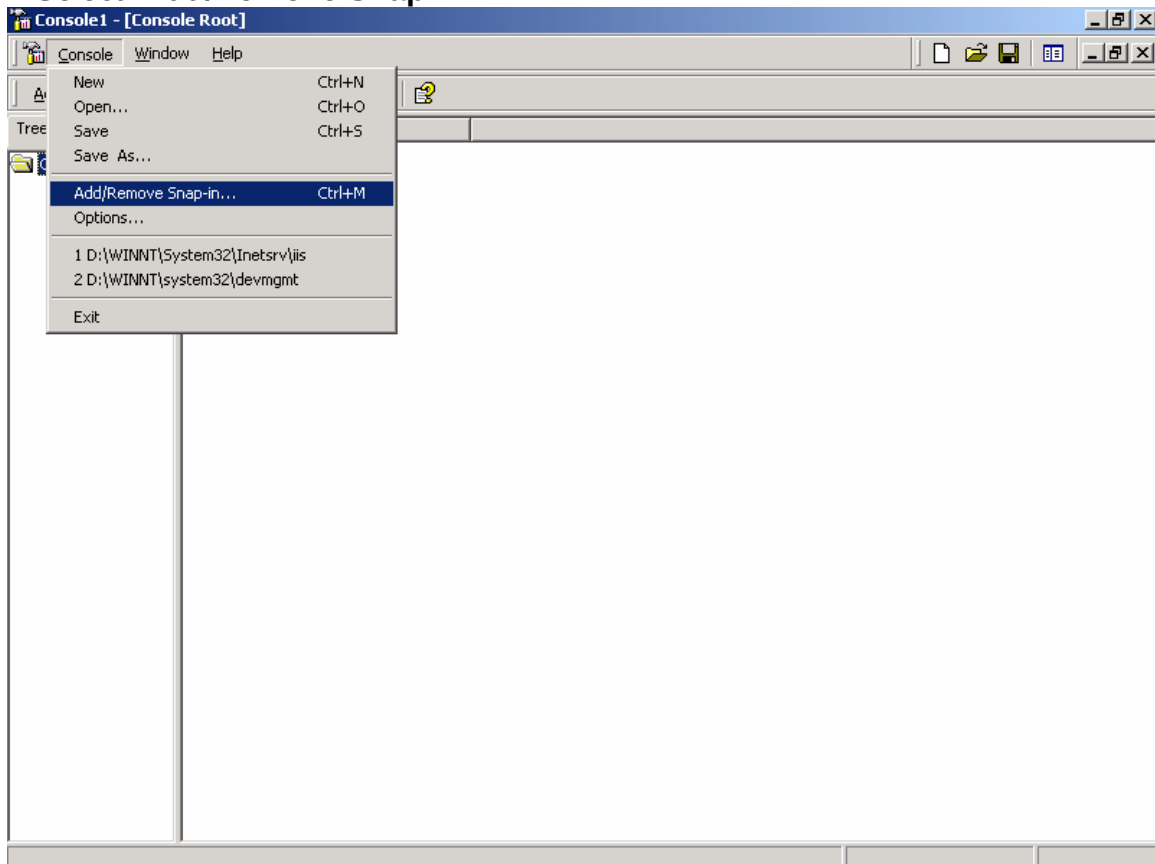
Date: 10 Sept 2002

Technical Requirement: Customer is required to understand their network and the Win2000 server machine well for this configuration. Please consult Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences arise from it.

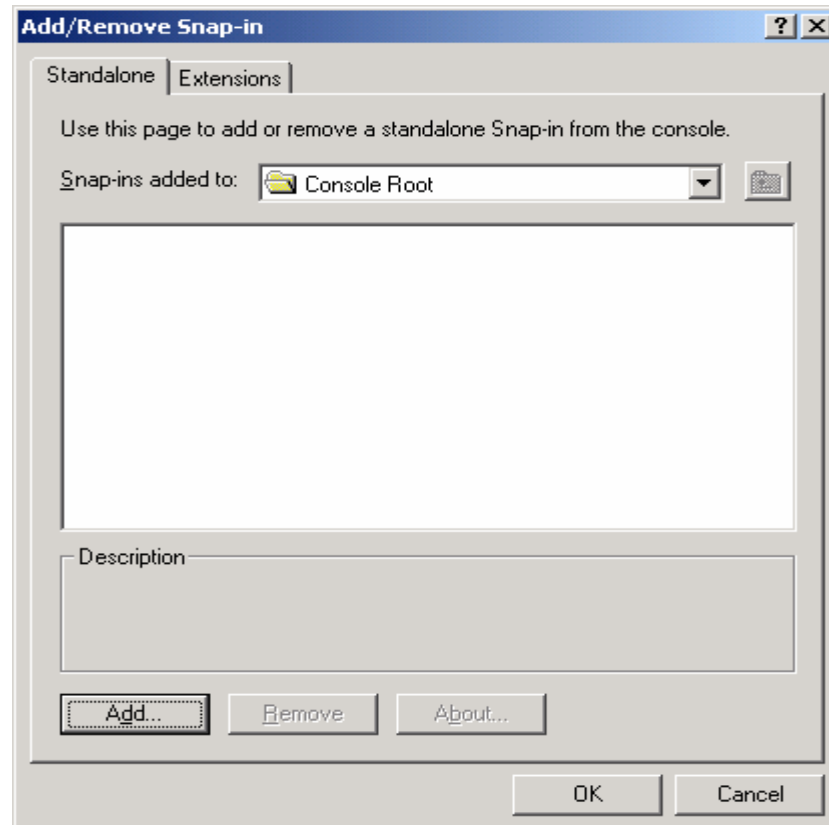
1. Enter “mmc” on the Dos Command Prompt



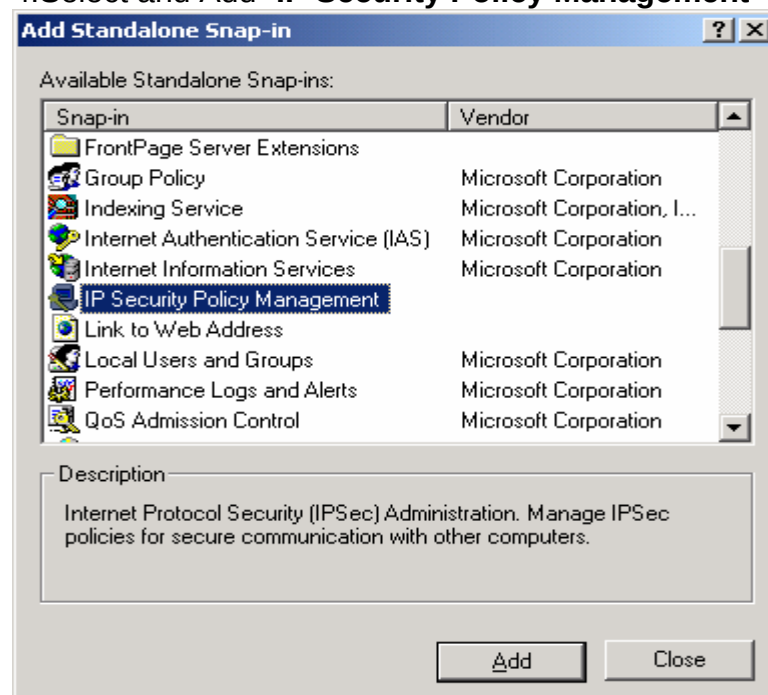
2. Select “Add/Remove Snap-in”



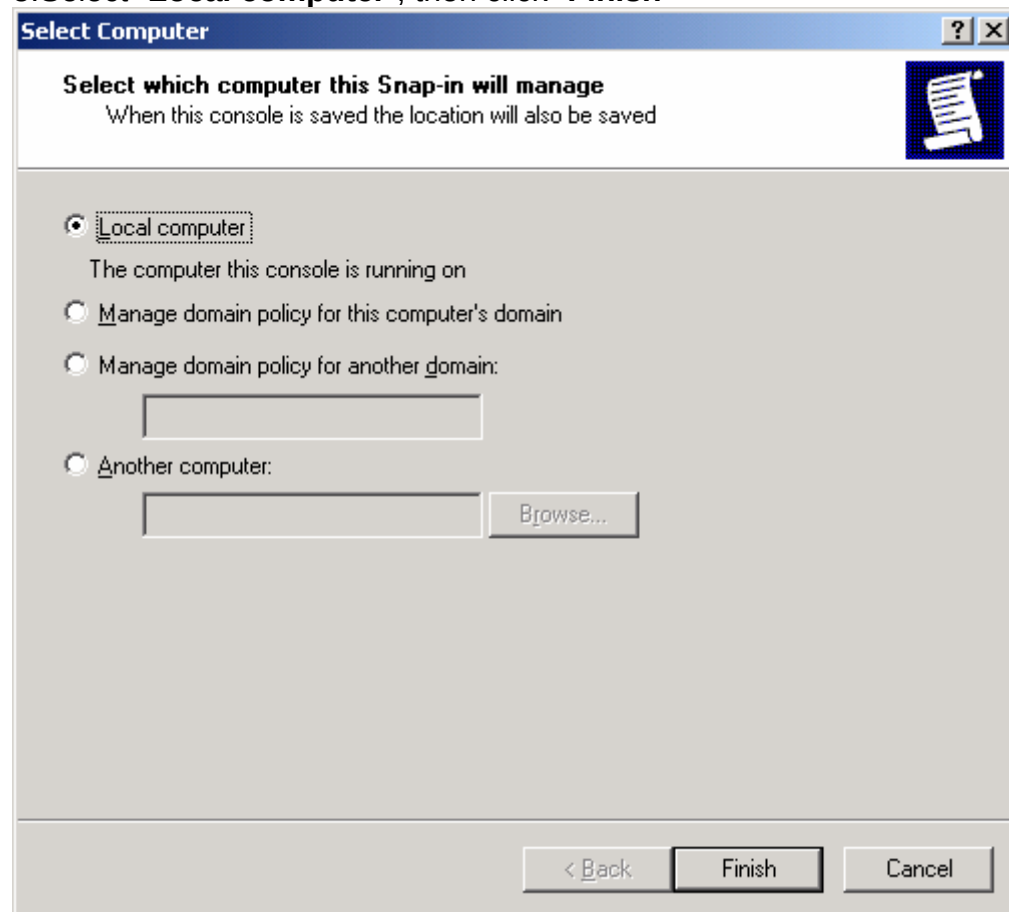
3. Click “Add”



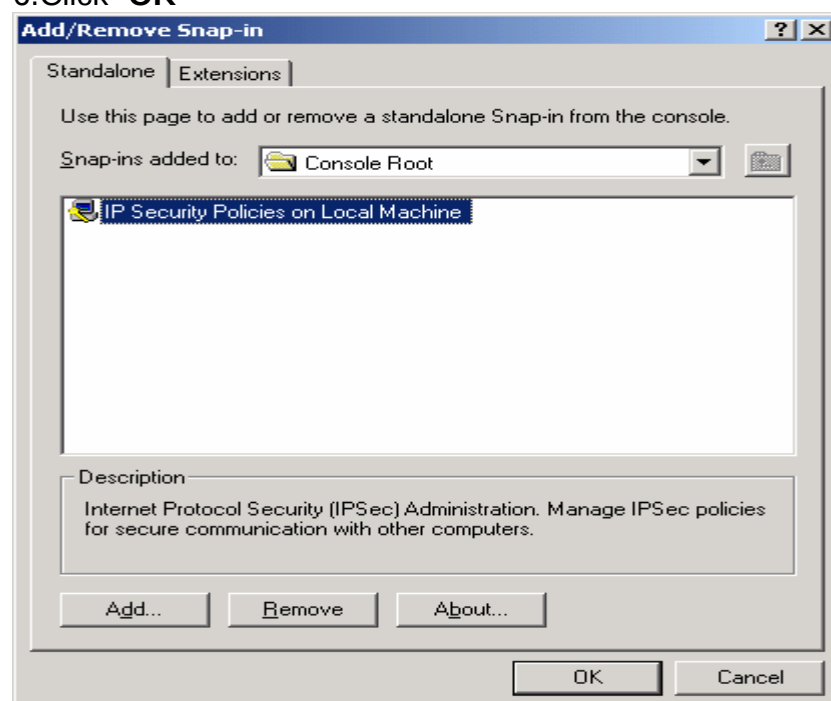
4. Select and Add “IP Security Policy Management”



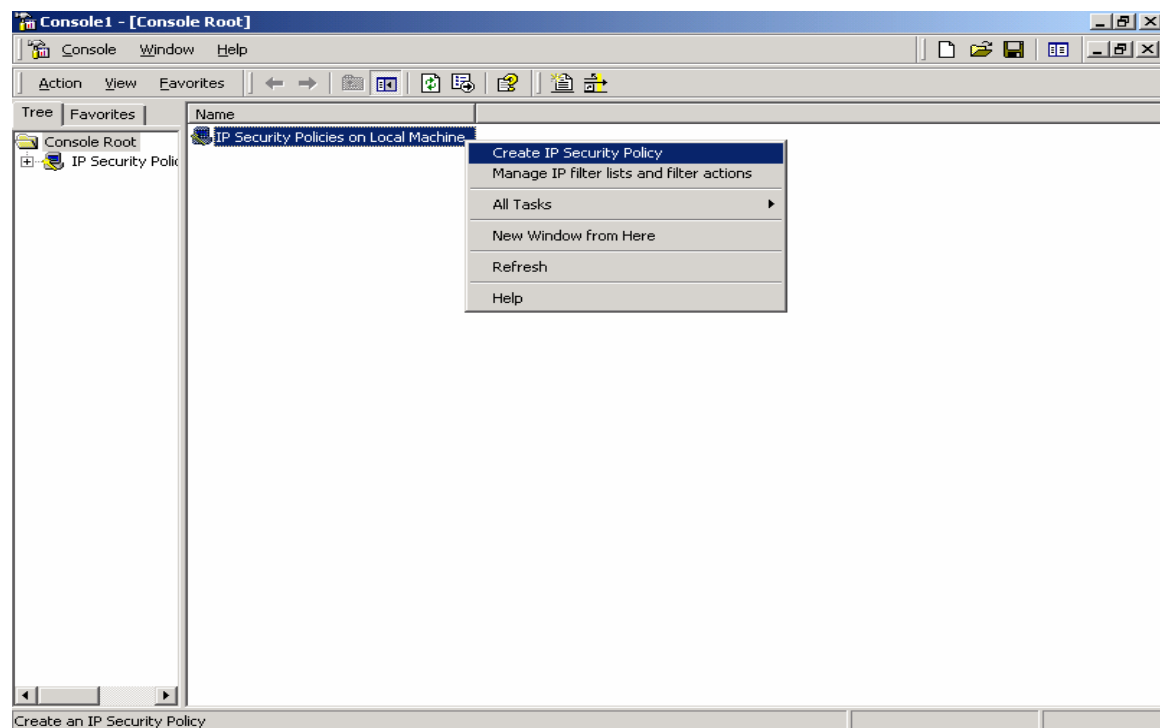
5. Select **“Local computer”**, then click **“Finish”**



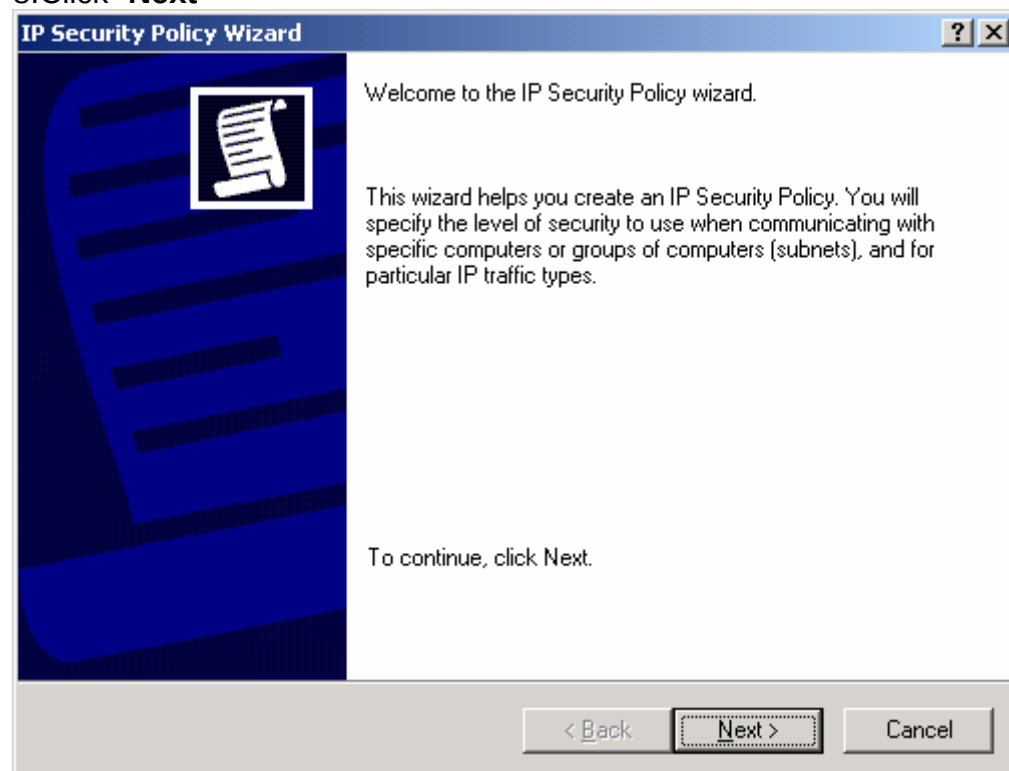
6. Click **“OK”**



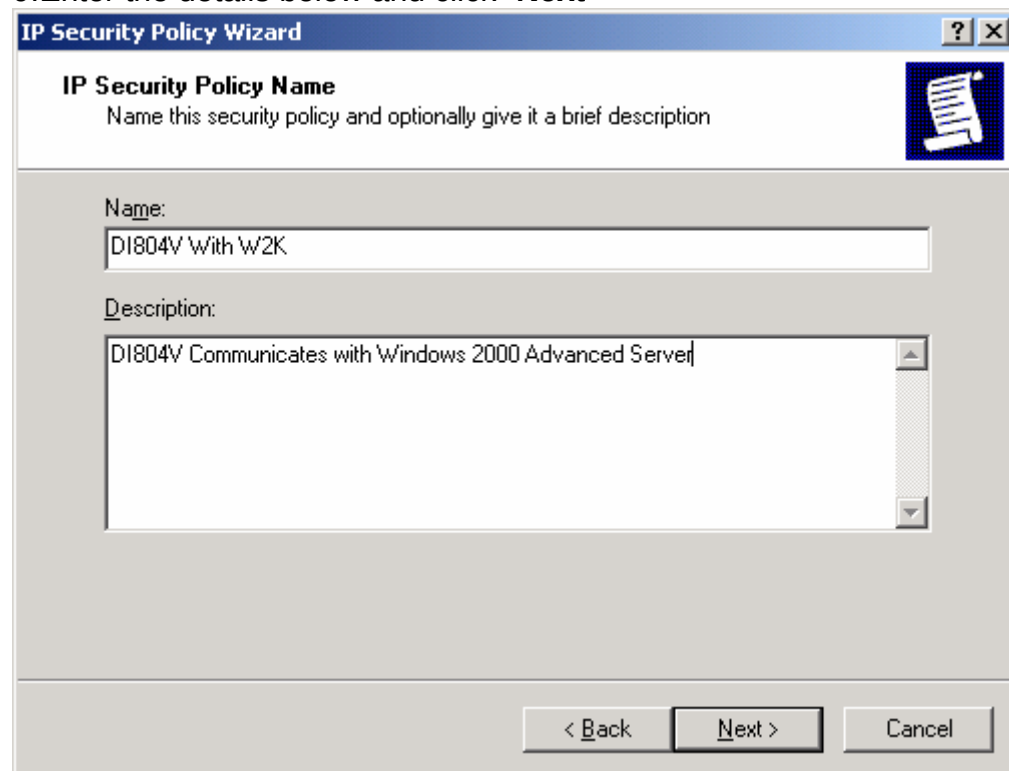
7. Right-click on **“IP Security Policies on Local Machine”** and select **“Create IP Security Policy”**



8. Click **“Next”**



9. Enter the details below and click “Next”



The screenshot shows the 'IP Security Policy Wizard' window. The title bar is blue with the text 'IP Security Policy Wizard' and standard window controls. The main area has a header 'IP Security Policy Name' with a subtitle 'Name this security policy and optionally give it a brief description'. Below this, there is a 'Name:' label and a text box containing 'DI804V With W2K'. Underneath is a 'Description:' label and a larger text box containing 'DI804V Communicates with Windows 2000 Advanced Server'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

IP Security Policy Wizard

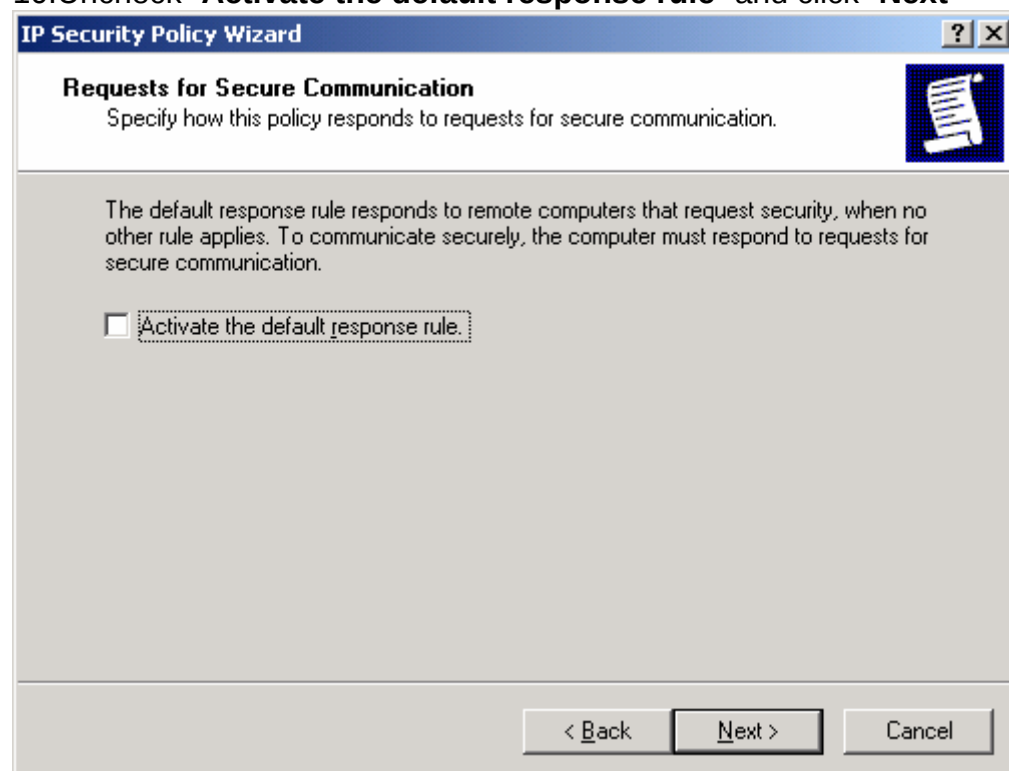
IP Security Policy Name
Name this security policy and optionally give it a brief description

Name:
DI804V With W2K

Description:
DI804V Communicates with Windows 2000 Advanced Server

< Back Next > Cancel

10. Uncheck “Activate the default response rule” and click “Next”



The screenshot shows the 'IP Security Policy Wizard' window at the 'Requests for Secure Communication' step. The title bar is blue with the text 'IP Security Policy Wizard' and standard window controls. The main area has a header 'Requests for Secure Communication' with a subtitle 'Specify how this policy responds to requests for secure communication.' Below this, there is a paragraph of text explaining the default response rule. Underneath, there is a checkbox labeled 'Activate the default response rule.' which is currently unchecked. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

IP Security Policy Wizard

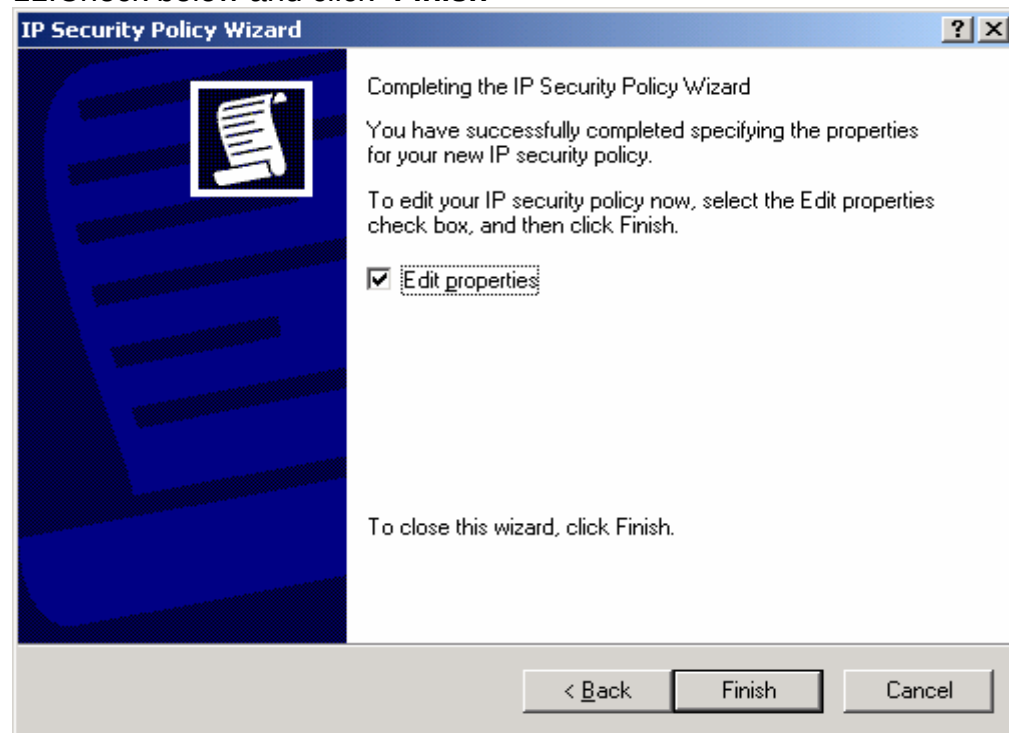
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.

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.

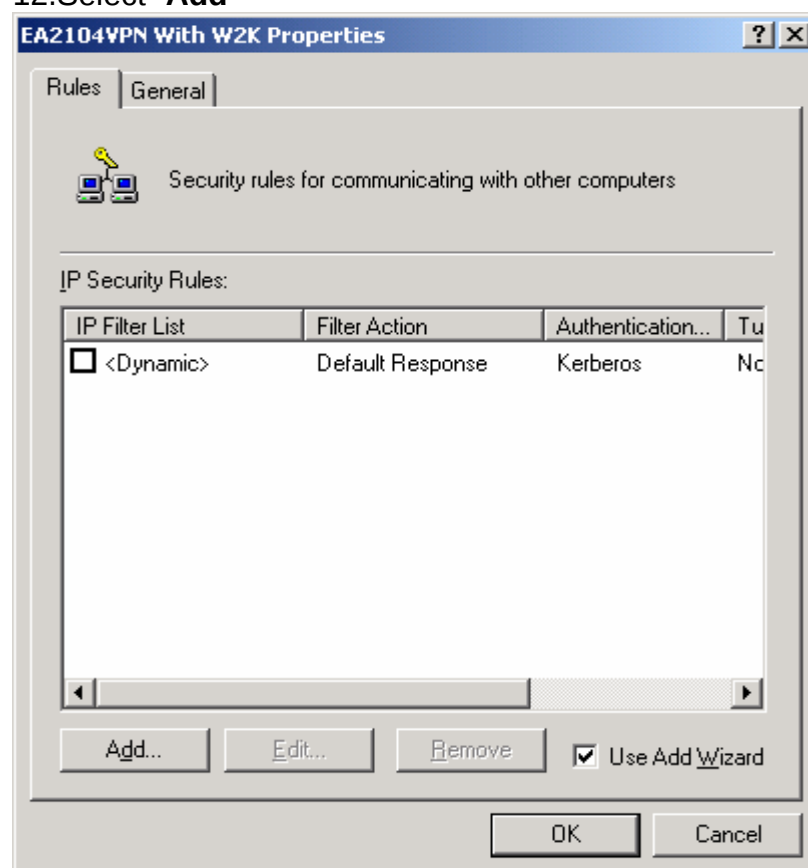
☐ Activate the default response rule.

< Back Next > Cancel

11. Check below and click **"Finish"**



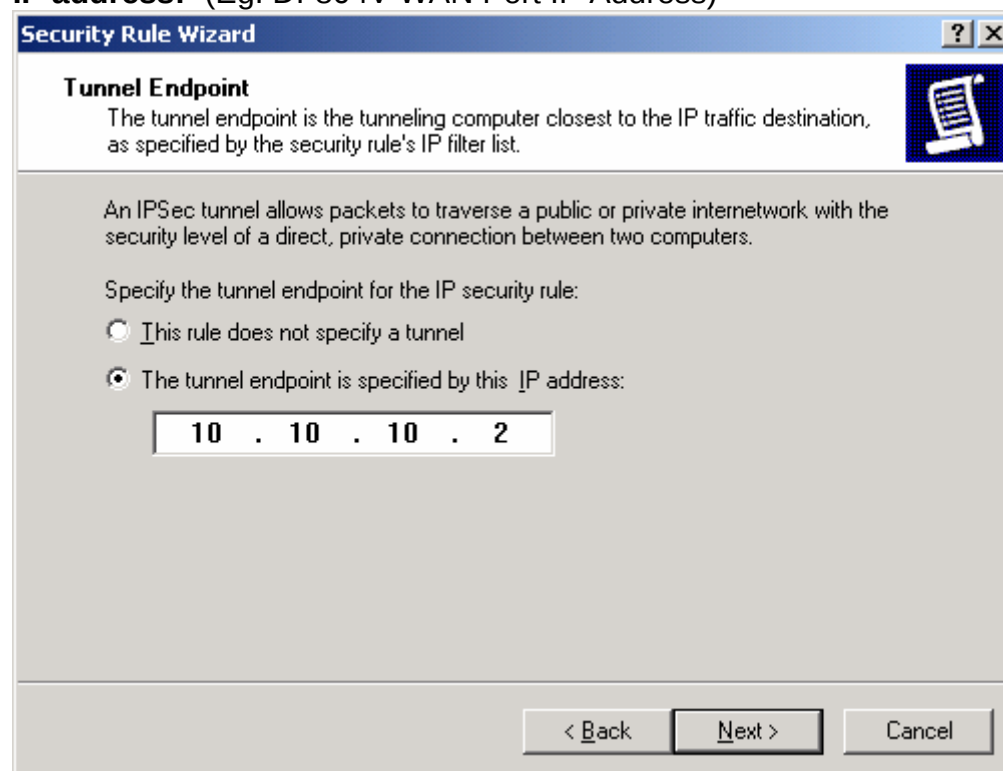
12. Select **"Add"**



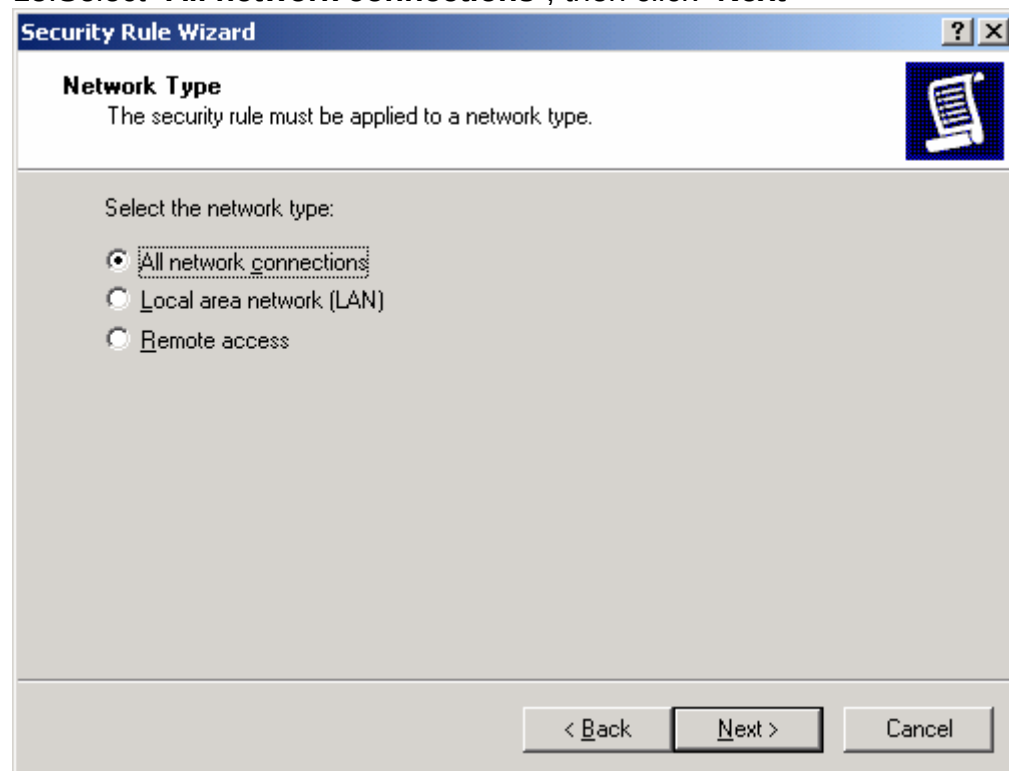
13. Click "Next"



14. Enter the IP Address detail into "**The tunnel endpoint specified by this IP address:**" (Eg. DI-804V WAN Port IP Address)

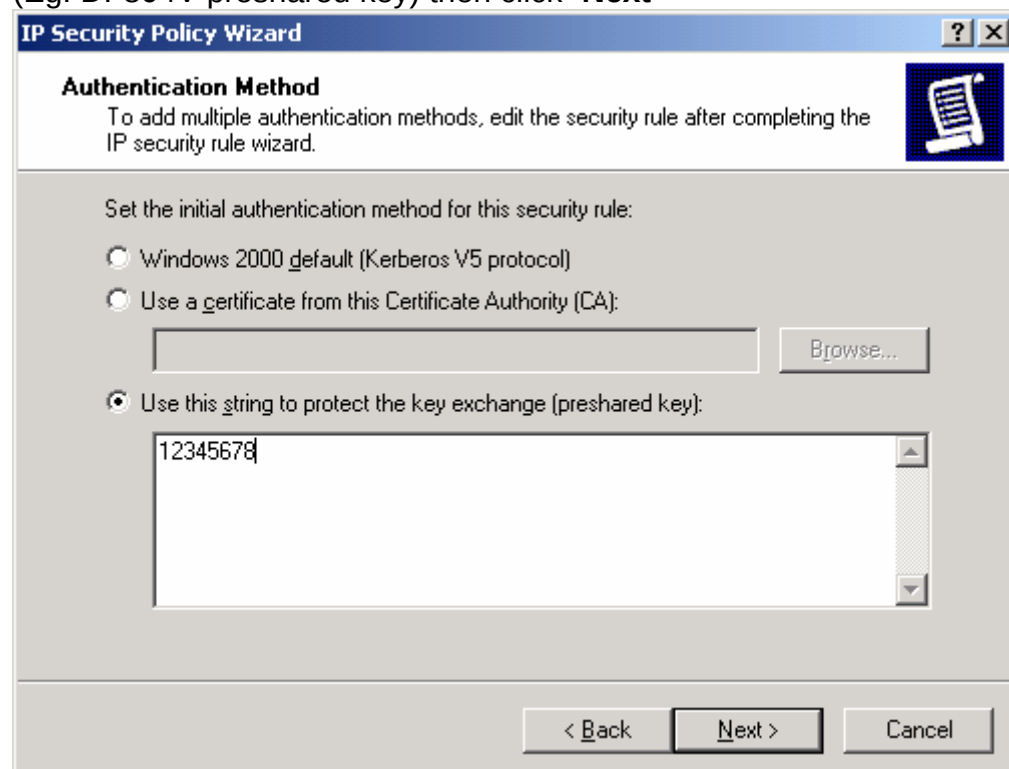


15. Select **"All network connections"**, then click **"Next"**



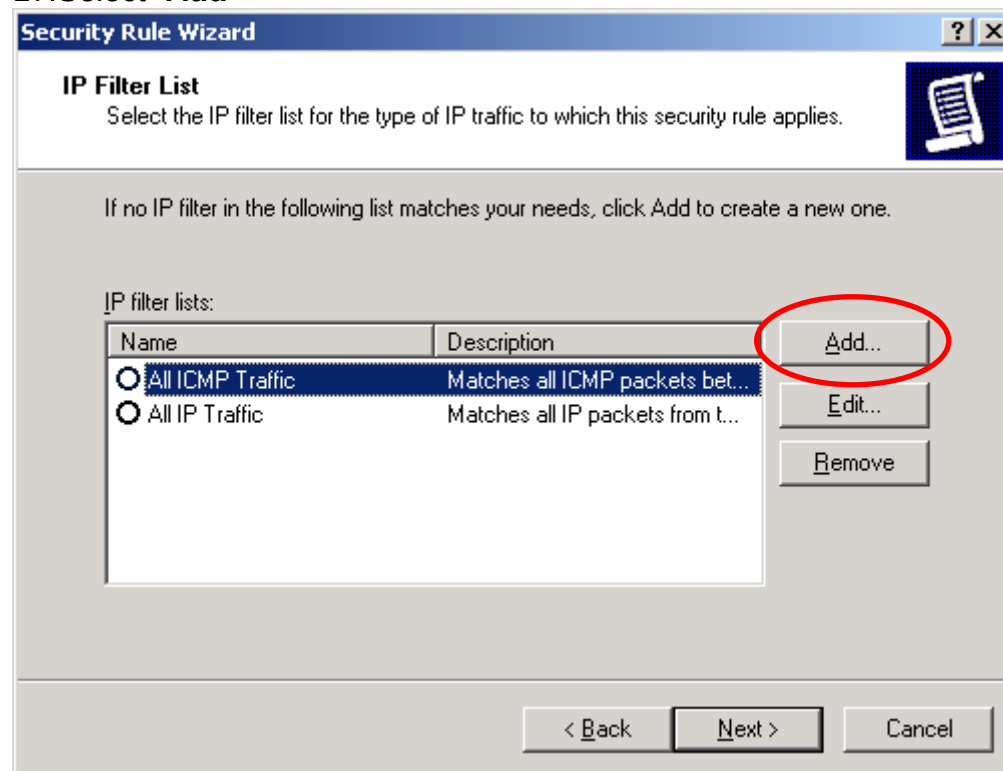
The screenshot shows the "Security Rule Wizard" window. The title bar is blue with a question mark and a close button. The main area has a header "Network Type" with a sub-header "The security rule must be applied to a network type." and a document icon. Below this, it says "Select the network type:" followed by three radio button options: "All network connections" (which is selected), "Local area network (LAN)", and "Remote access". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

16. Select **"Use this string to protect the key exchange (preshared key)"** (Eg. DI-804V preshared key) then click **"Next"**

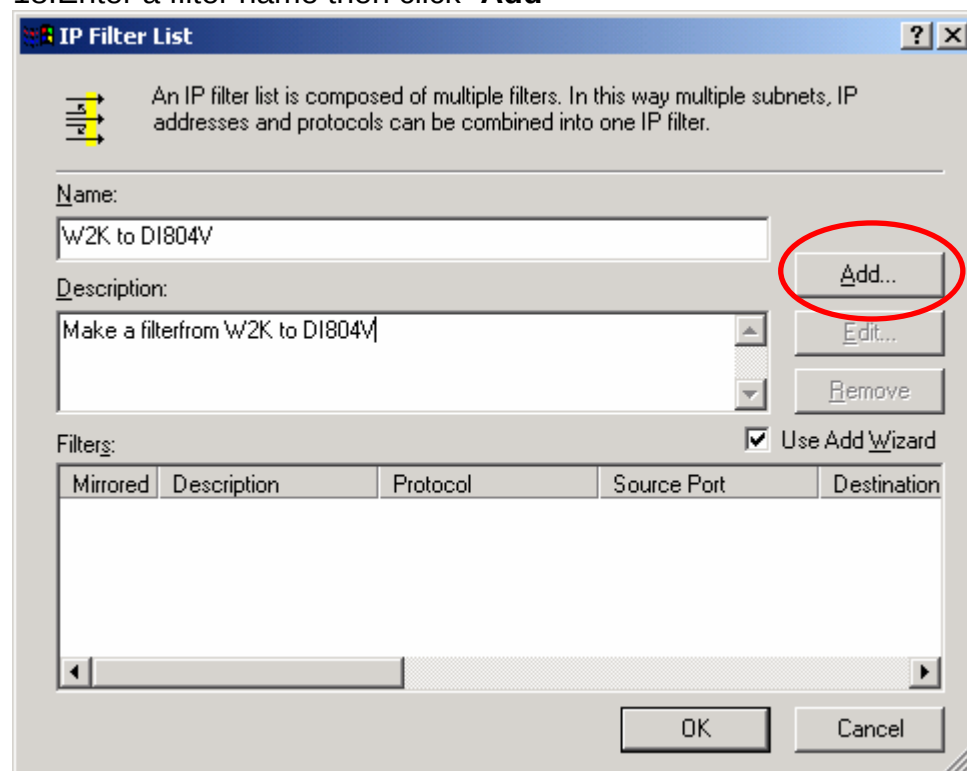


The screenshot shows the "IP Security Policy Wizard" window. The title bar is blue with a question mark and a close button. The main area has a header "Authentication Method" with a sub-header "To add multiple authentication methods, edit the security rule after completing the IP security rule wizard." and a document icon. Below this, it says "Set the initial authentication method for this security rule:" followed by two radio button options: "Windows 2000 default (Kerberos V5 protocol)" and "Use a certificate from this Certificate Authority (CA):". The second option has a text box and a "Browse..." button. The first option is selected, and it has a sub-header "Use this string to protect the key exchange (preshared key):" followed by a large text box containing the string "12345678". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

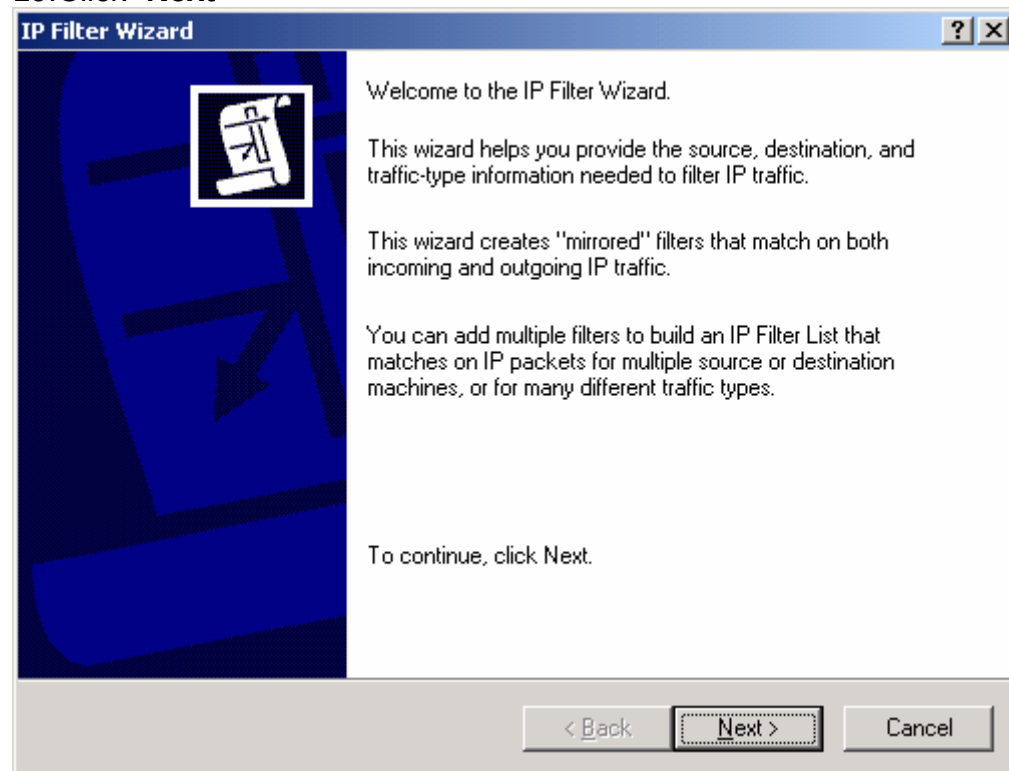
17. Select "Add"



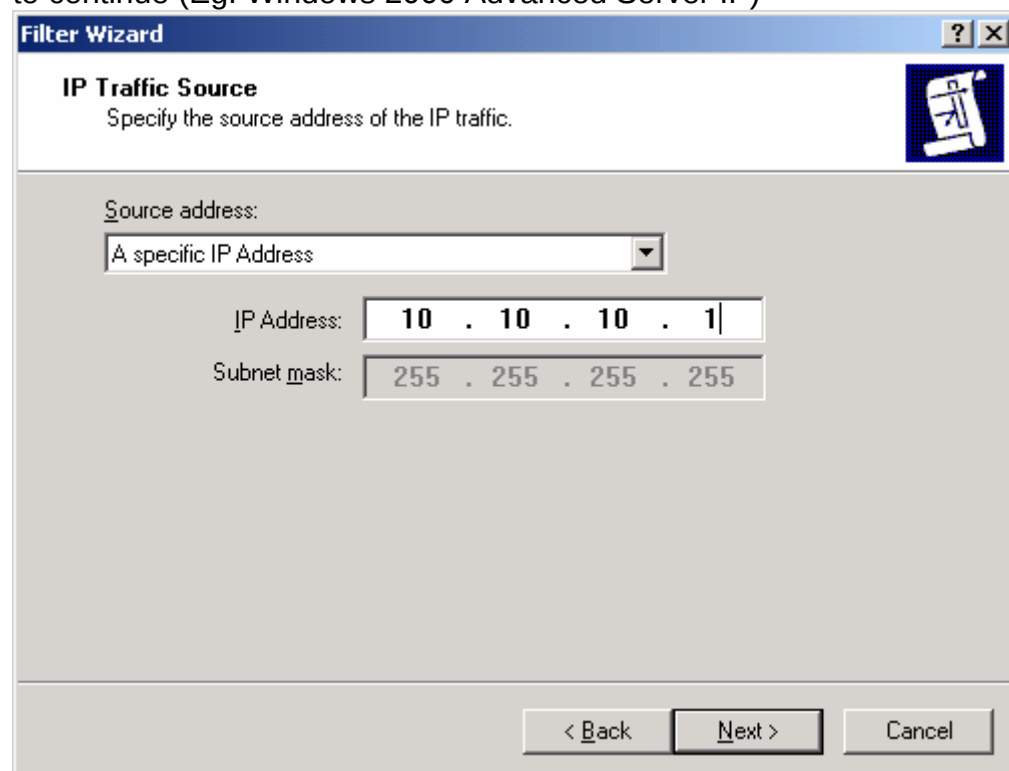
18. Enter a filter name then click "Add"



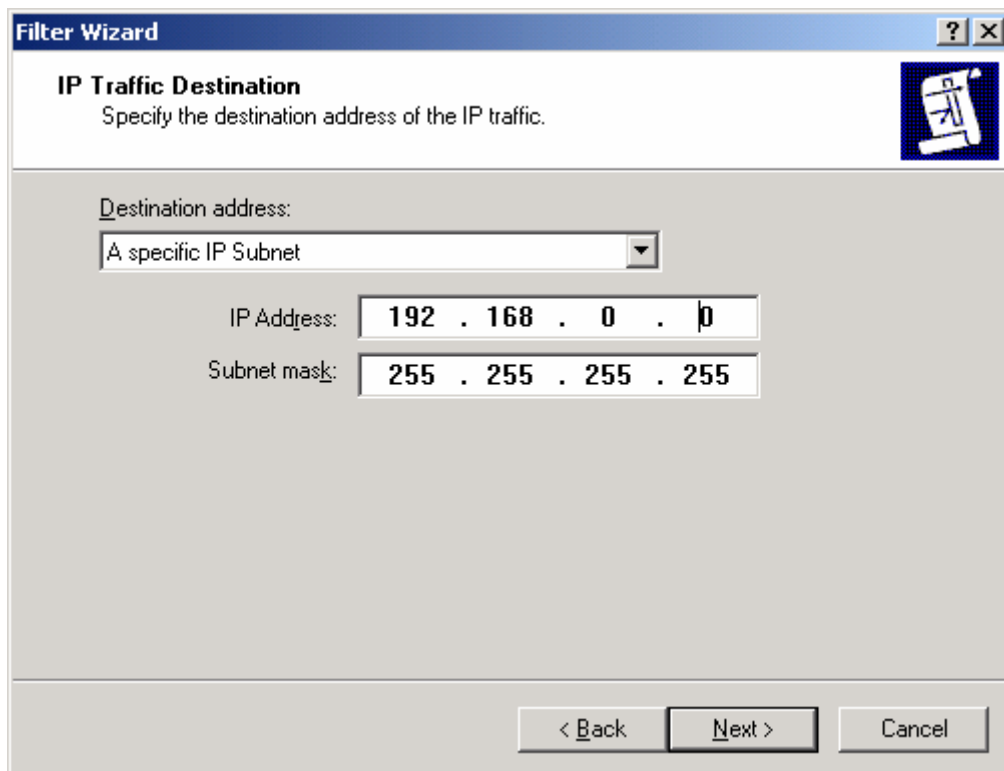
19. Click **"Next"**



20. Select **"A specific IP Address"** and input the Source address, then **"Next"** to continue (Eg. Windows 2000 Advanced Server IP)



21. Select “**A specific IP Subnet**” and input the Destination subnet address, then “**Next**” to continue (Eg. DI-804V Private network)



The screenshot shows the 'Filter Wizard' window at the 'IP Traffic Destination' step. The title bar reads 'Filter Wizard'. Below the title bar, the step is labeled 'IP Traffic Destination' with the instruction 'Specify the destination address of the IP traffic.' and a small icon of a document with a checkmark. The main area contains a 'Destination address:' label followed by a dropdown menu currently showing 'A specific IP Subnet'. Below this, there are two input fields: 'IP Address:' with the value '192 . 168 . 0 . 0' and 'Subnet mask:' with the value '255 . 255 . 255 . 255'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Filter Wizard

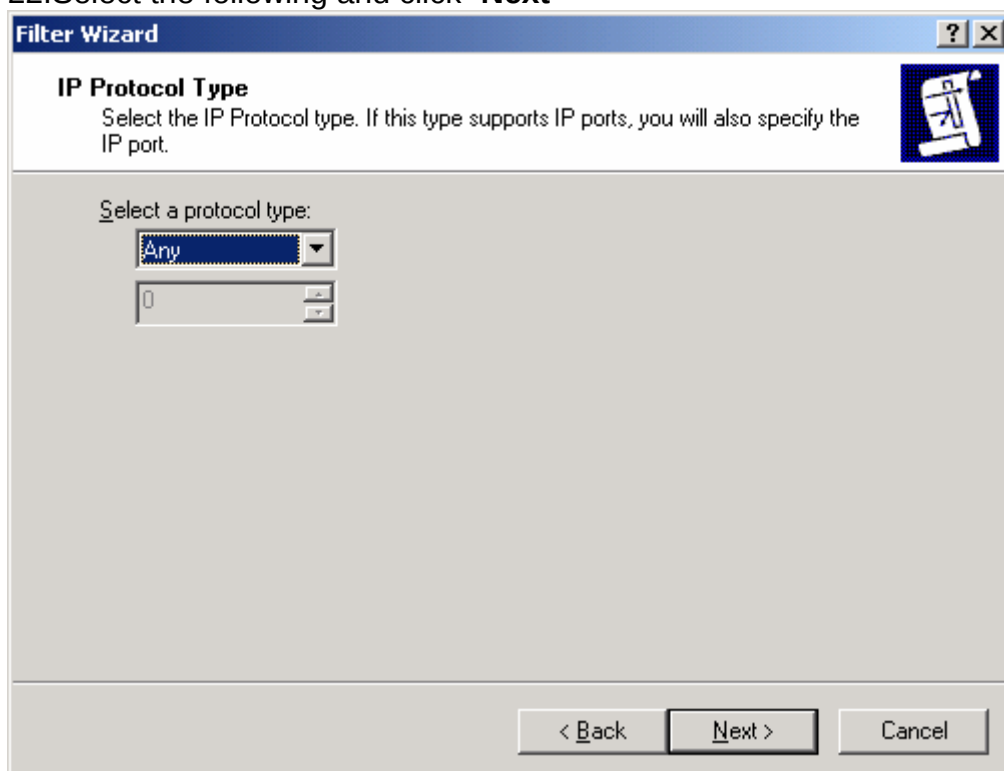
IP Traffic Destination
Specify the destination address of the IP traffic.

Destination address:
A specific IP Subnet

IP Address: 192 . 168 . 0 . 0
Subnet mask: 255 . 255 . 255 . 255

< Back Next > Cancel

22. Select the following and click “**Next**”



The screenshot shows the 'Filter Wizard' window at the 'IP Protocol Type' step. The title bar reads 'Filter Wizard'. Below the title bar, the step is labeled 'IP Protocol Type' with the instruction 'Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.' and a small icon of a document with a checkmark. The main area contains a 'Select a protocol type:' label followed by a dropdown menu currently showing 'Any'. Below this, there is an empty input field for the IP port. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Filter Wizard

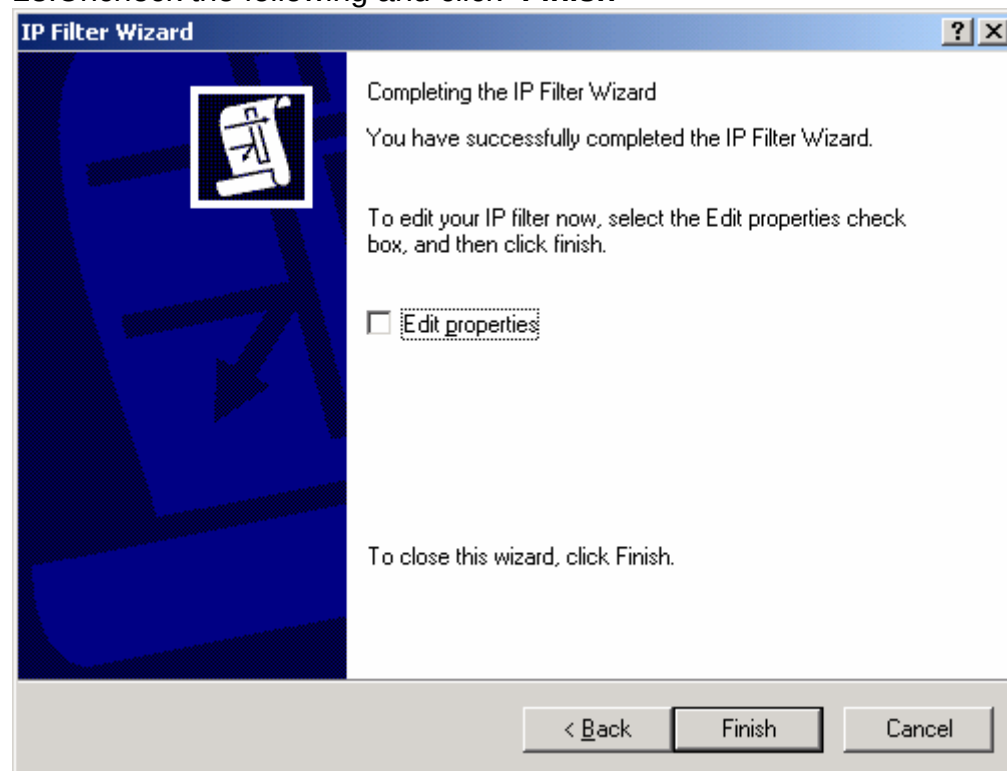
IP Protocol Type
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.

Select a protocol type:
Any

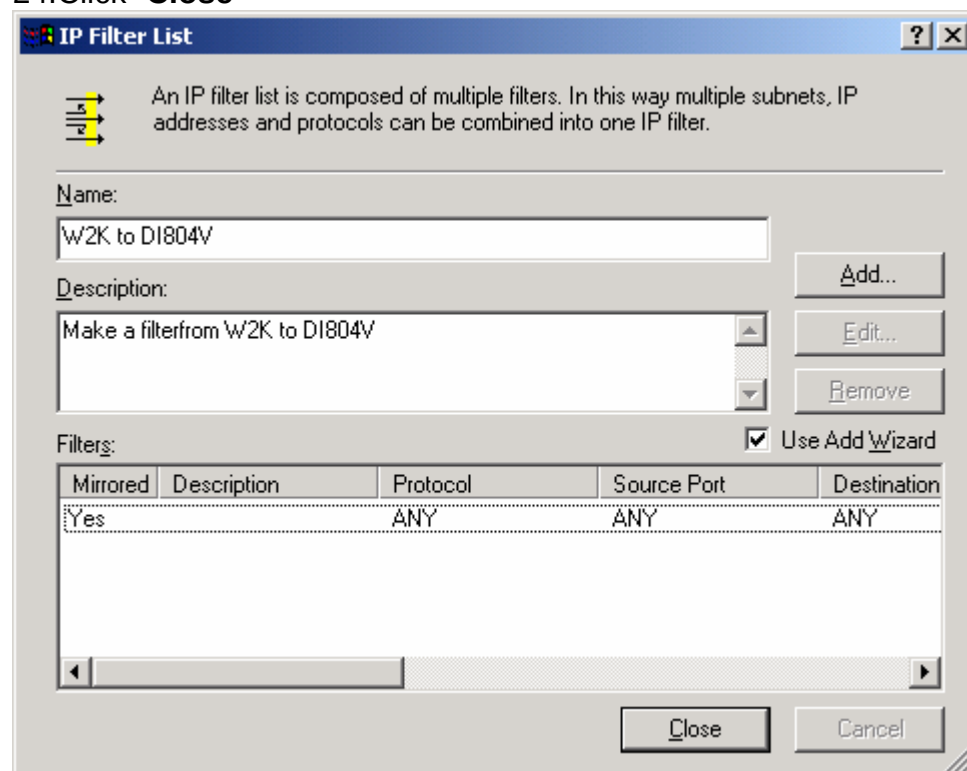
0

< Back Next > Cancel

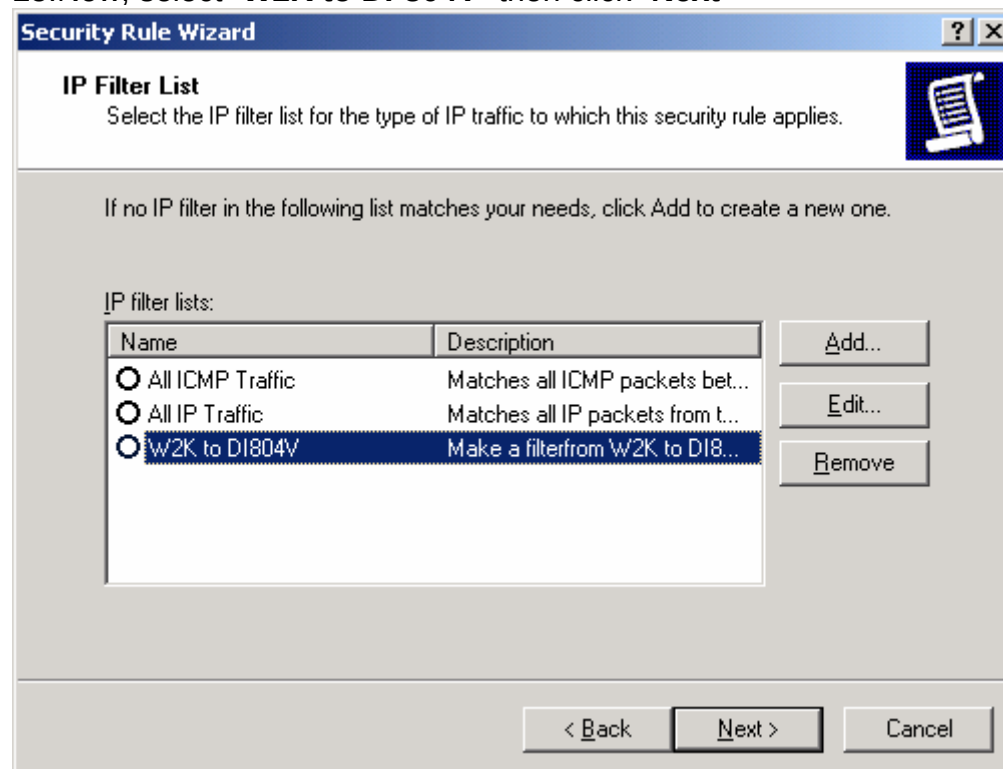
23. Uncheck the following and click **“Finish”**



24. Click **“Close”**



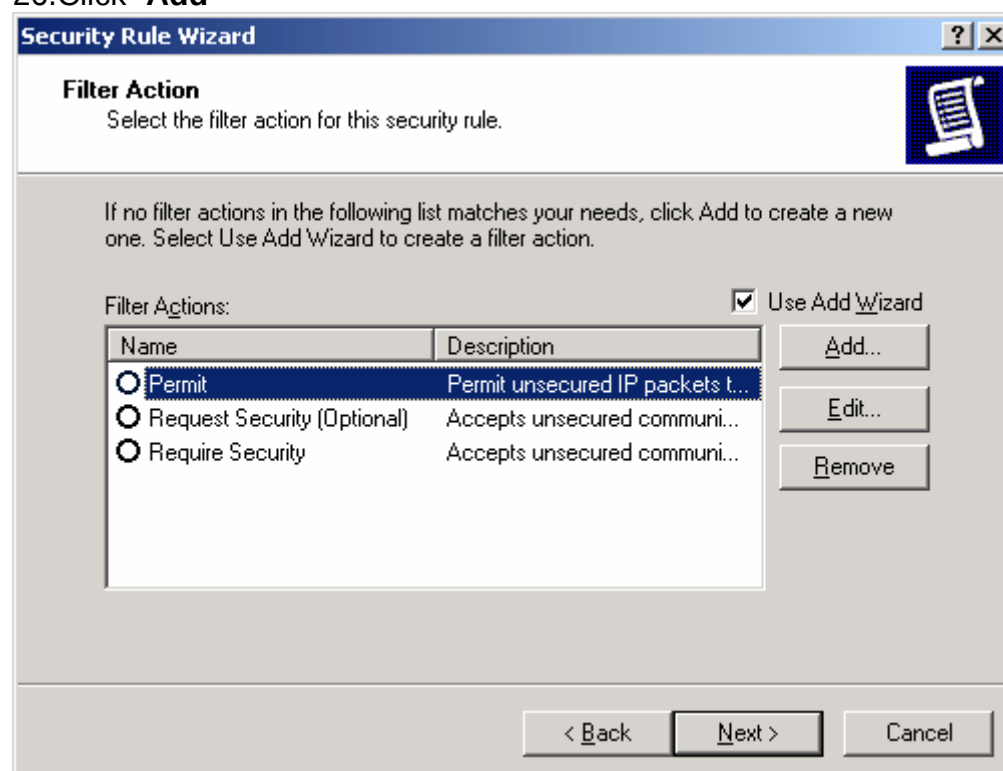
25. Now, select “W2K to DI-804V” then click “Next”



The screenshot shows the 'Security Rule Wizard' window at the 'IP Filter List' step. 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.' and a document icon. A message states: 'If no IP filter in the following list matches your needs, click Add to create a new one.' Below this, the 'IP filter lists:' section contains a table with two columns: 'Name' and 'Description'. The table lists three options: 'All ICMP Traffic' (Matches all ICMP packets bet...), 'All IP Traffic' (Matches all IP packets from t...), and 'W2K to DI804V' (Make a filter from W2K to DI8...). The 'W2K to DI804V' option is selected. To the right of the table are three buttons: 'Add...', 'Edit...', and 'Remove'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Name	Description
☐ All ICMP Traffic	Matches all ICMP packets bet...
☐ All IP Traffic	Matches all IP packets from t...
☒ W2K to DI804V	Make a filter from W2K to DI8...

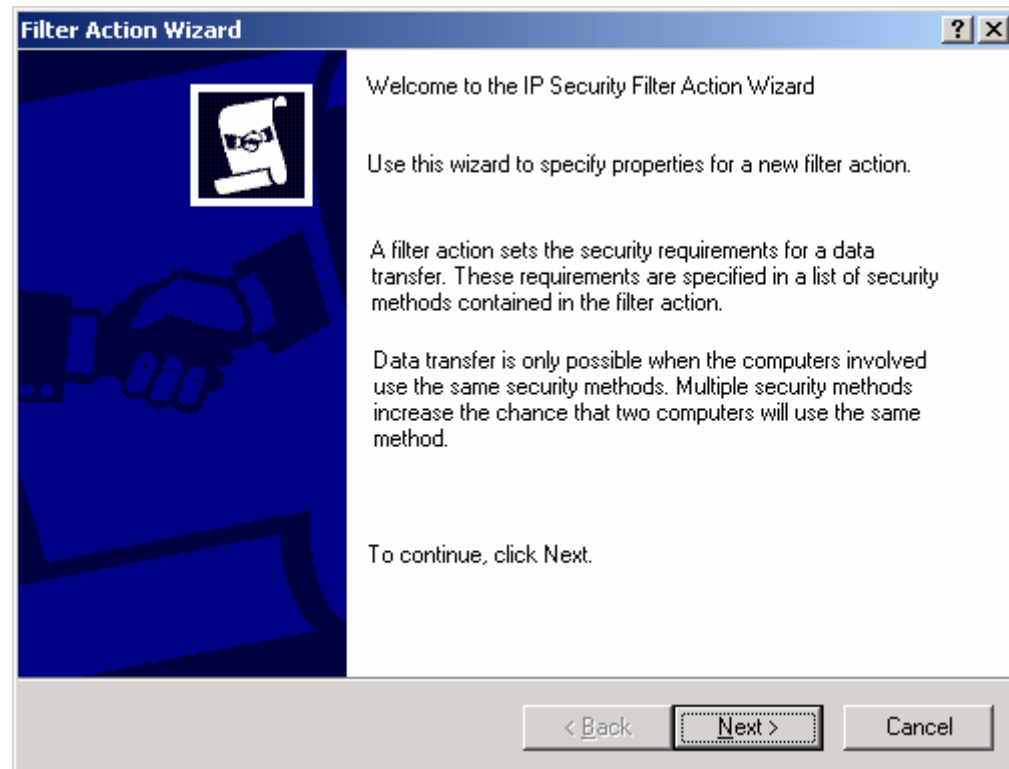
26. Click “Add”



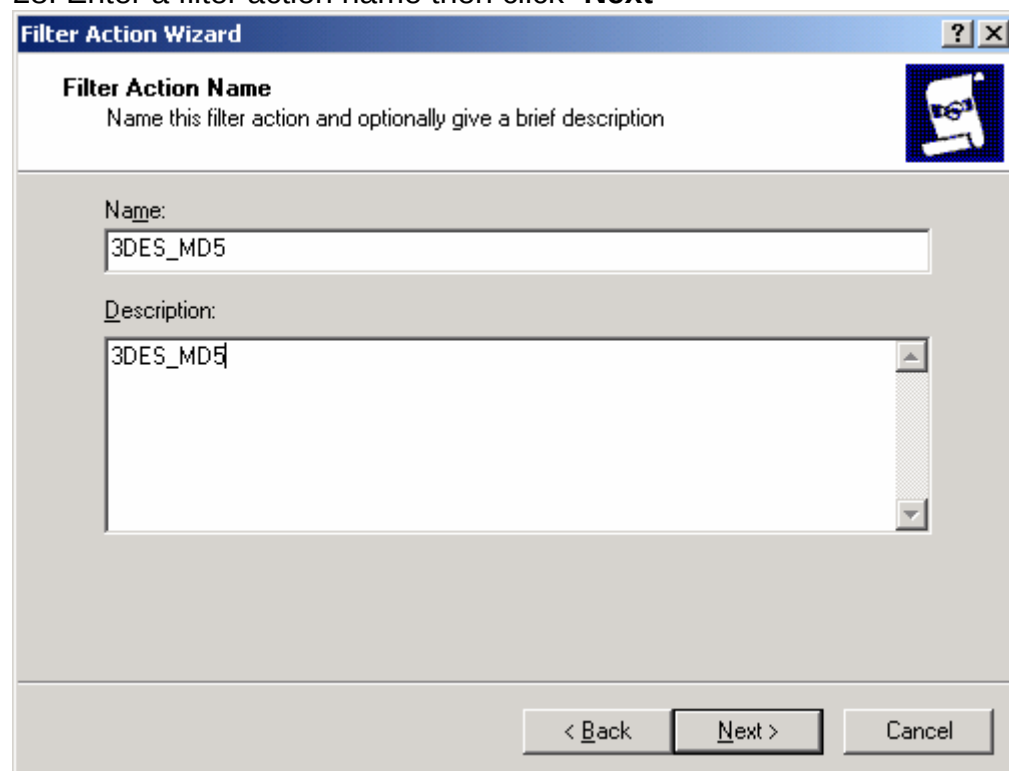
The screenshot shows the 'Security Rule Wizard' window at the 'Filter Action' step. The title bar reads 'Security Rule Wizard'. Below the title bar, the section is titled 'Filter Action' with a subtitle 'Select the filter action for this security rule.' and a document icon. A message states: 'If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.' Below this, the 'Filter Actions:' section contains a table with two columns: 'Name' and 'Description'. The table lists three options: 'Permit' (Permit unsecured IP packets t...), 'Request Security (Optional)' (Accepts unsecured communi...), and 'Require Security' (Accepts unsecured communi...). The 'Permit' option is selected. To the right of the table are three buttons: 'Add...', 'Edit...', and 'Remove'. Above the table, there is a checkbox labeled 'Use Add Wizard' which is checked. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Name	Description
☒ Permit	Permit unsecured IP packets t...
☐ Request Security (Optional)	Accepts unsecured communi...
☐ Require Security	Accepts unsecured communi...

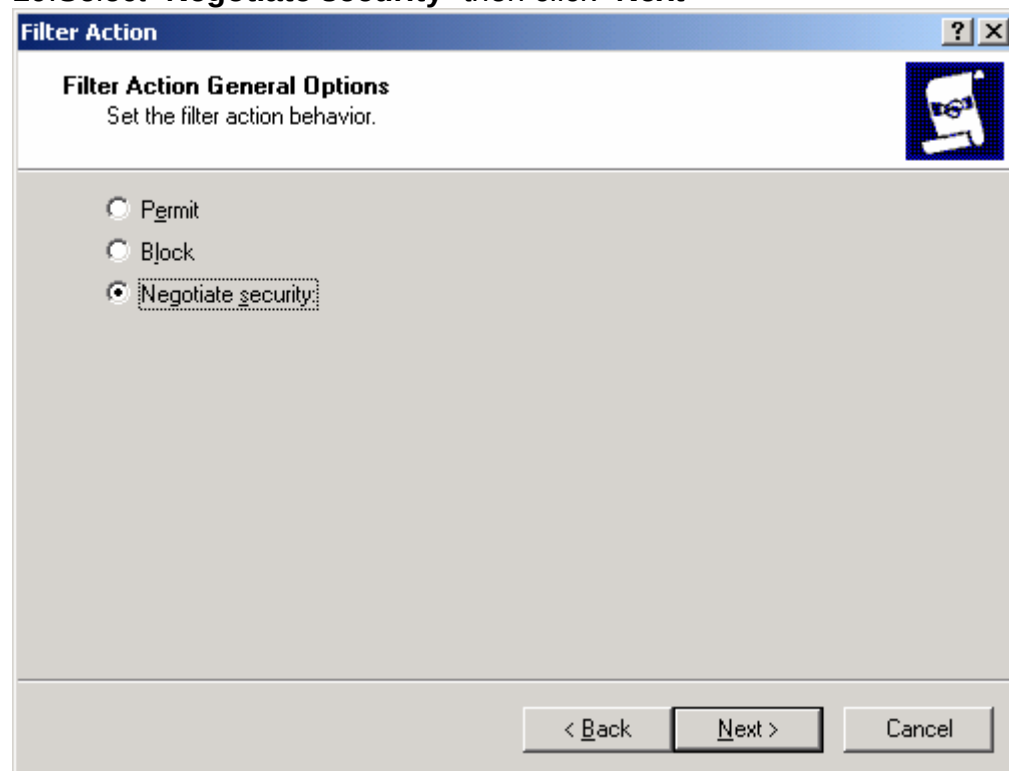
27. Click **"Next"**



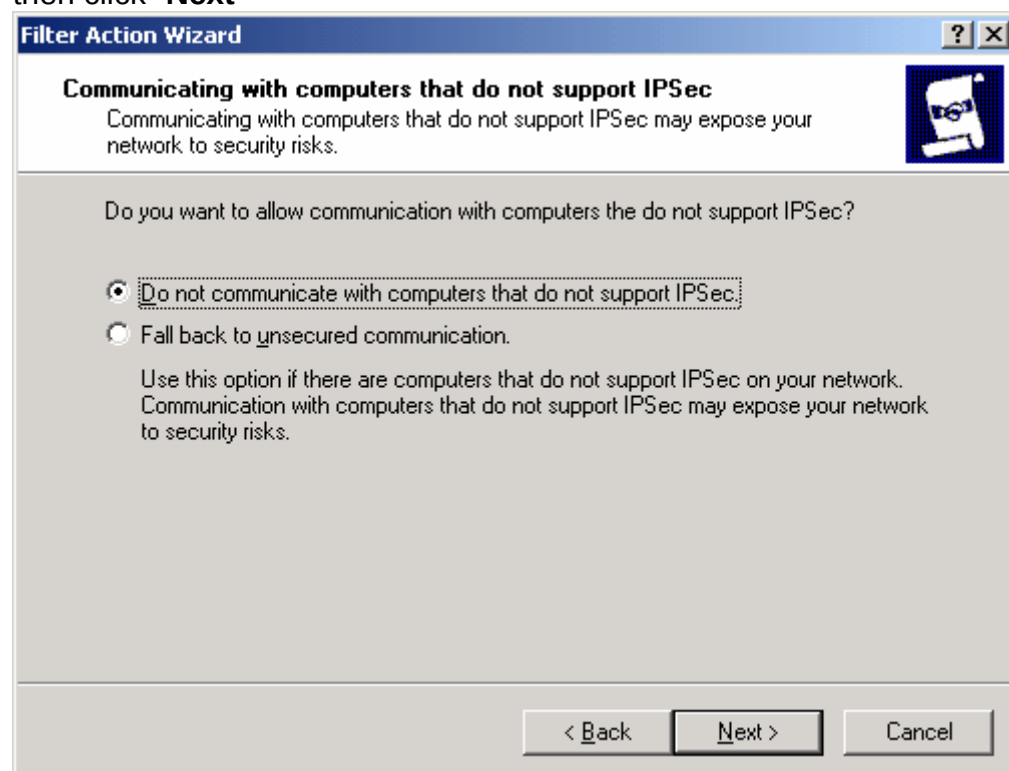
28. Enter a filter action name then click **"Next"**



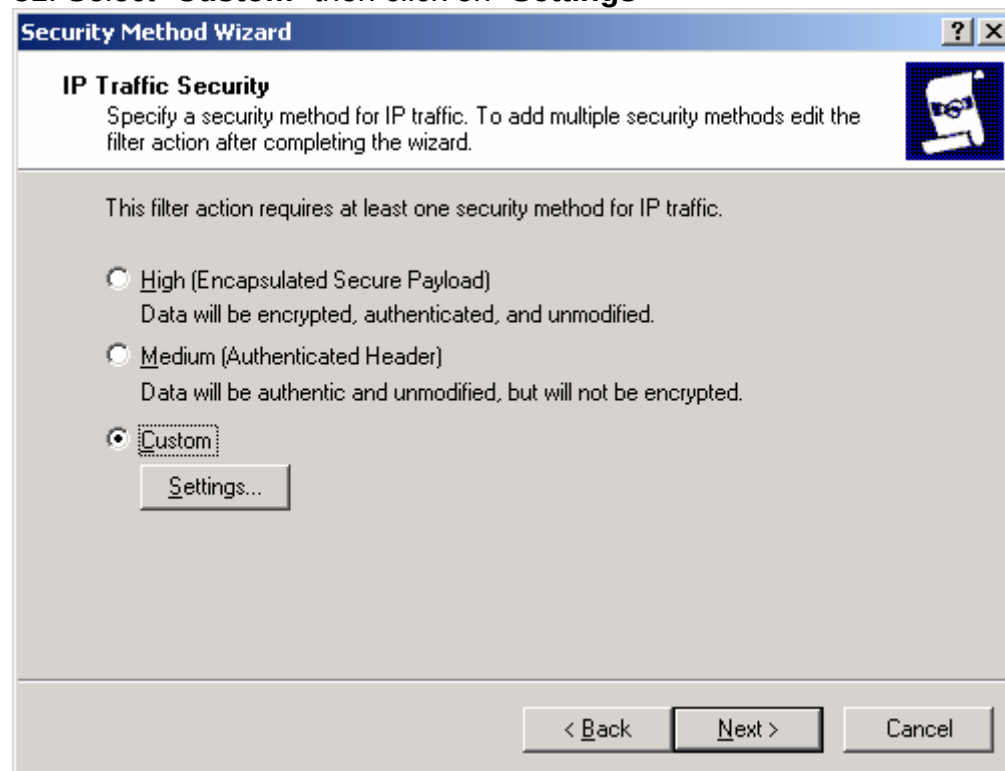
29. Select **"Negotiate security"** then click **"Next"**



30. Select **"Do not communicate with computer that do not support IPSec"** then click **"Next"**

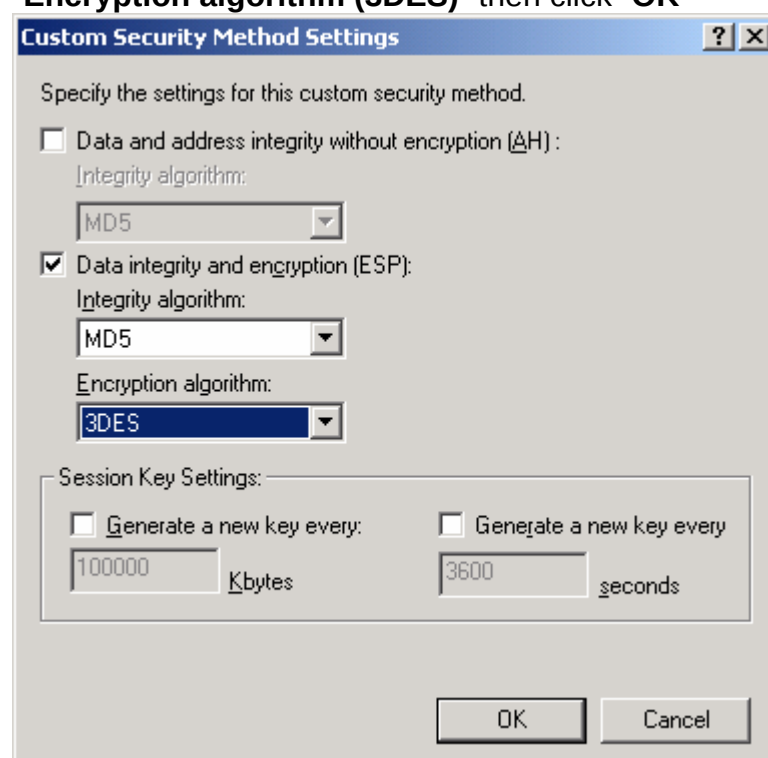


31. Select **“Custom”** then click on **“Settings”**



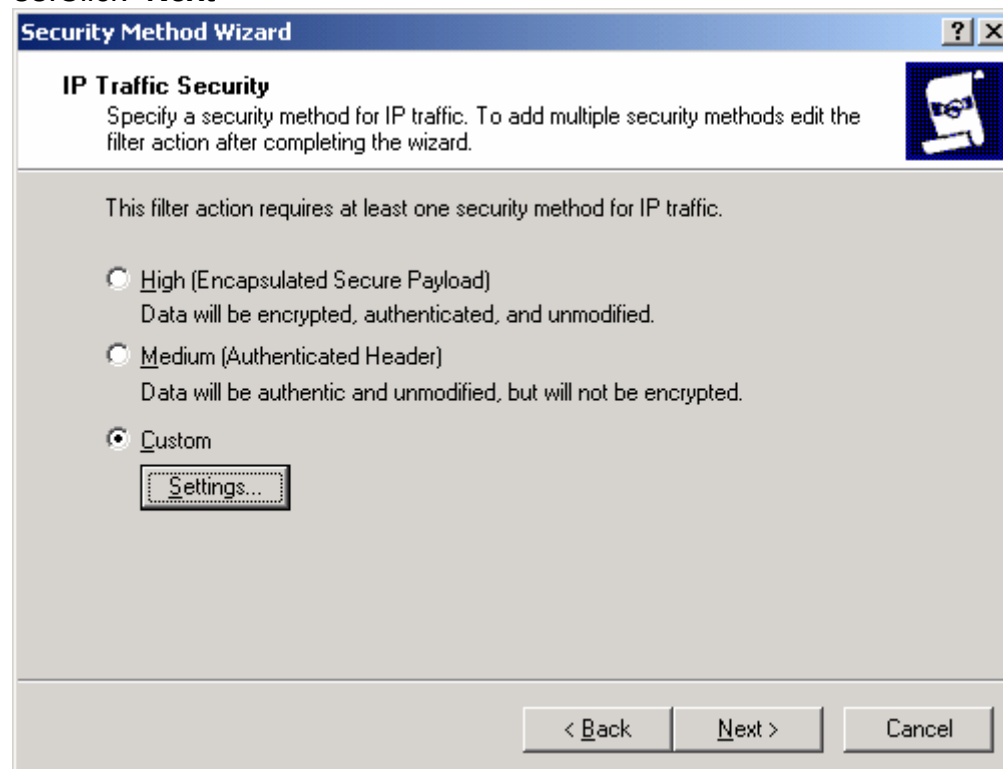
The screenshot shows the "Security Method Wizard" dialog box. The title bar is blue with a question mark and a close button. The main area has a light gray background. At the top, it says "IP Traffic Security" and "Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard." Below this, it states "This filter action requires at least one security method for IP traffic." There are three radio button options: "High (Encapsulated Secure Payload)" with the description "Data will be encrypted, authenticated, and unmodified.", "Medium (Authenticated Header)" with the description "Data will be authentic and unmodified, but will not be encrypted.", and "Custom" which is selected. Below the "Custom" option is a "Settings..." button. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

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



The screenshot shows the "Custom Security Method Settings" dialog box. The title bar is blue with a question mark and a close button. The main area has a light gray background. It says "Specify the settings for this custom security method." There are two checkboxes: "Data and address integrity without encryption (AH) :" which is unchecked, and "Data integrity and encryption (ESP) :" which is checked. Below the "Data integrity and encryption (ESP) :" checkbox, there are two dropdown menus: "Integrity algorithm:" set to "MD5" and "Encryption algorithm:" set to "3DES". At the bottom, there is a "Session Key Settings:" section with two checkboxes: "Generate a new key every:" with a text box containing "100000" and the unit "Kbytes", and "Generate a new key every" with a text box containing "3600" and the unit "seconds". At the bottom right, there are "OK" and "Cancel" buttons.

33. Click "Next"



The "Security Method Wizard" dialog box has a title bar with a question mark and a close button. The main area is titled "IP Traffic Security" and contains a sub-header "Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard." Below this, a note states "This filter action requires at least one security method for IP traffic." There are three radio button options: "High (Encapsulated Secure Payload)" with a description "Data will be encrypted, authenticated, and unmodified.", "Medium (Authenticated Header)" with a description "Data will be authentic and unmodified, but will not be encrypted.", and "Custom" which is selected. A "Settings..." button is located below the "Custom" option. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Security Method Wizard

IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.

This filter action requires at least one security method for IP traffic.

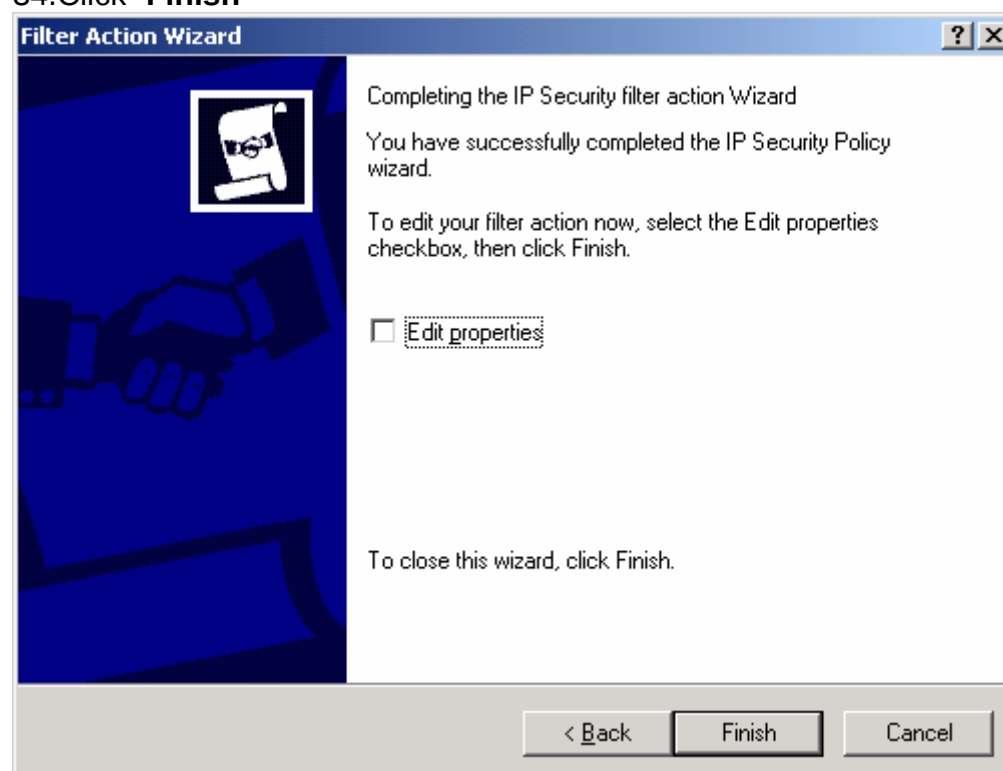
☐ High (Encapsulated Secure Payload)
Data will be encrypted, authenticated, and unmodified.

☐ Medium (Authenticated Header)
Data will be authentic and unmodified, but will not be encrypted.

☒ Custom
[Settings...](#)

< Back Next > Cancel

34. Click "Finish"



The "Filter Action Wizard" dialog box has a title bar with a question mark and a close button. The main area is titled "Completing the IP Security filter action Wizard" and contains a sub-header "You have successfully completed the IP Security Policy wizard." Below this, a note states "To edit your filter action now, select the Edit properties checkbox, then click Finish." There is an unchecked checkbox labeled "Edit properties". At the bottom, a note states "To close this wizard, click Finish." There are three buttons: "< Back", "Finish", and "Cancel".

Filter Action Wizard

Completing the IP Security filter action Wizard
You have successfully completed the IP Security Policy wizard.

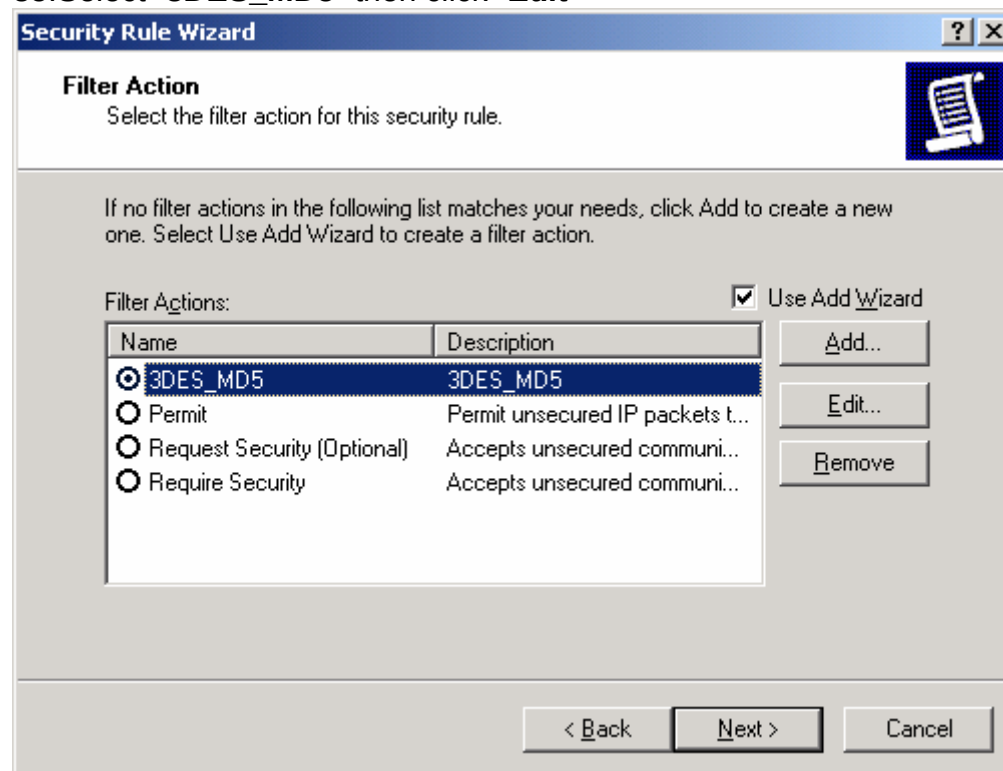
To edit your filter action now, select the Edit properties checkbox, then click Finish.

☐ Edit properties

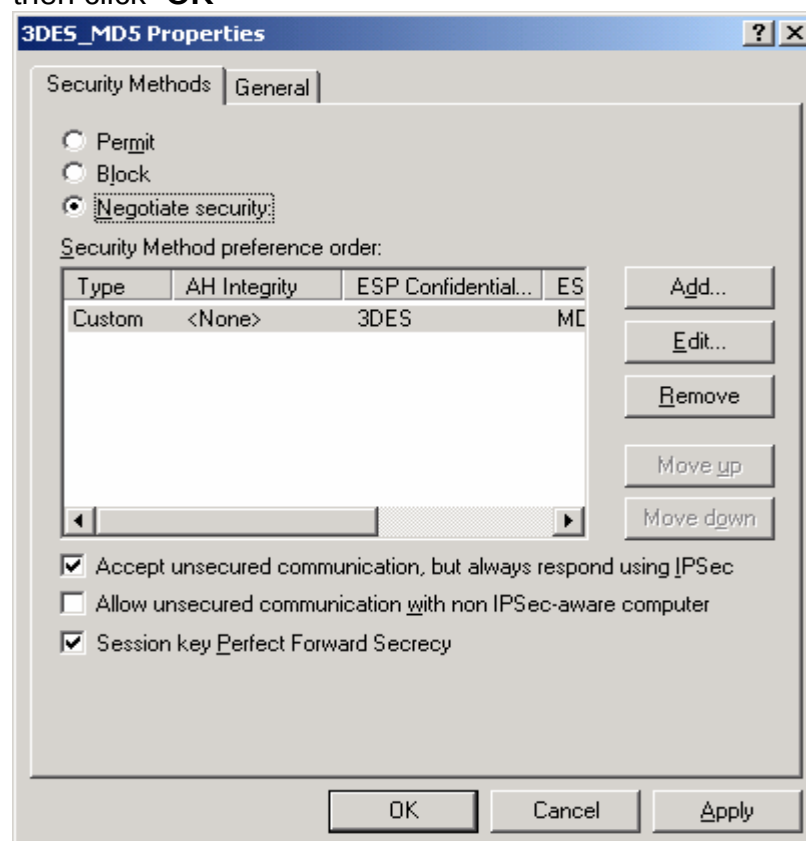
To close this wizard, click Finish.

< Back Finish Cancel

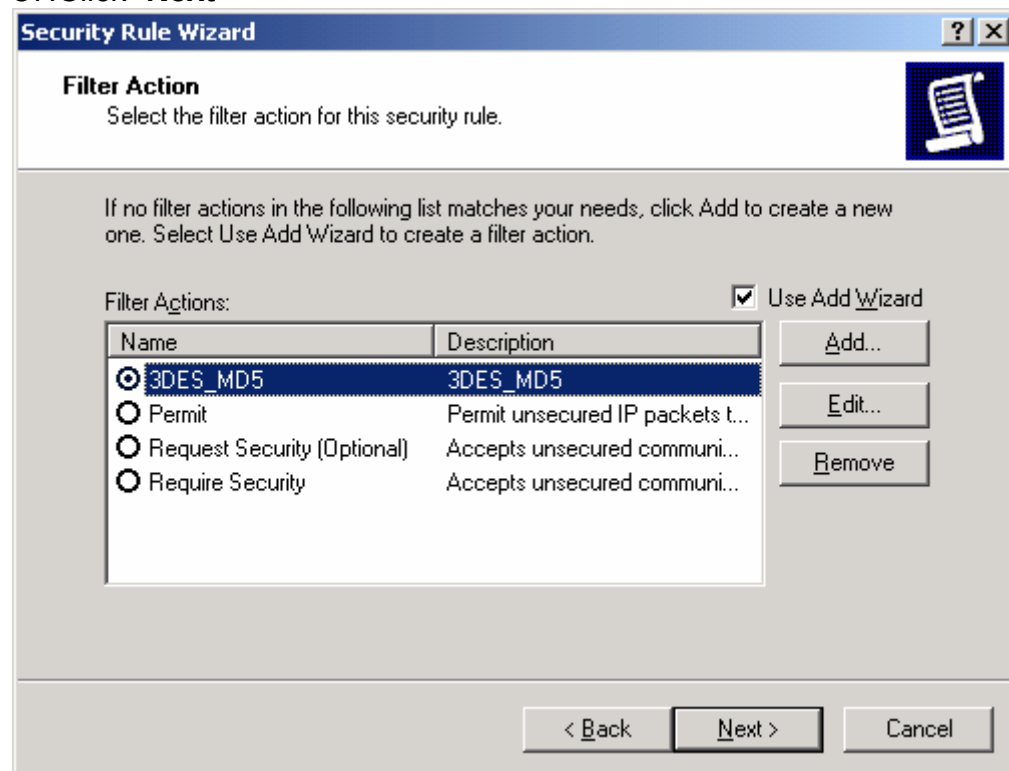
35. Select **"3DES_MD5"** then click **"Edit"**



36. Select the following and check **"Session key Perfect Forward Secrecy"** then click **"OK"**



37. Click "Next"



Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

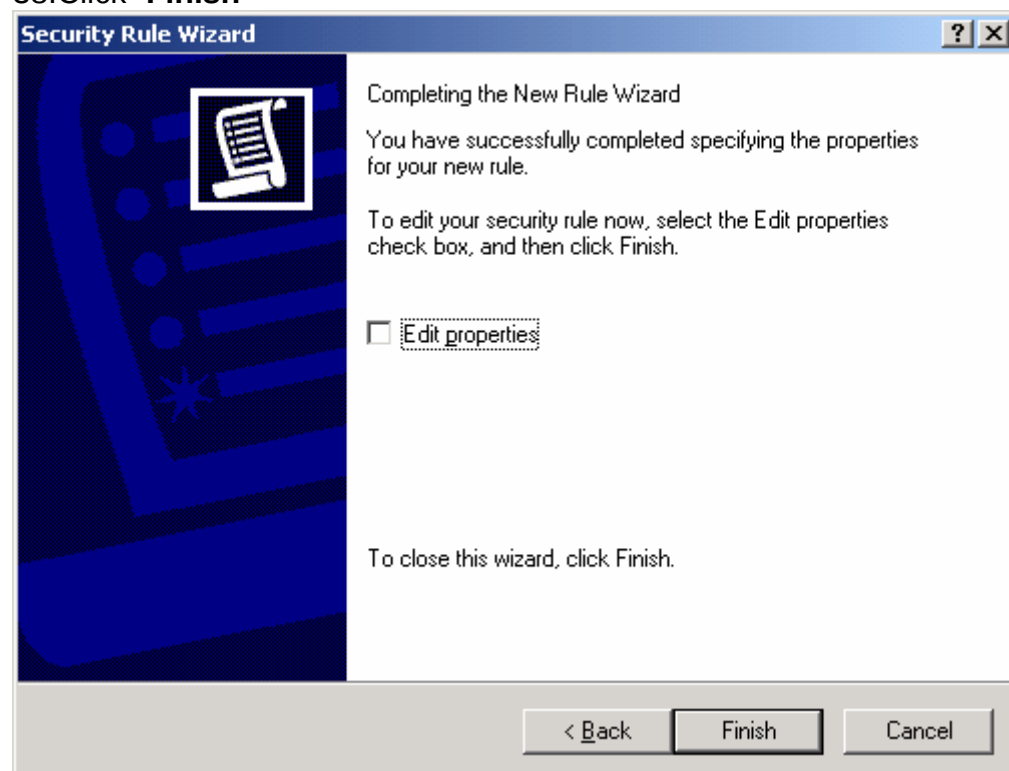
Filter Actions: ☒ Use Add Wizard

Name	Description
☒ 3DES_MD5	3DES_MD5
☐ Permit	Permit unsecured IP packets t...
☐ Request Security (Optional)	Accepts unsecured communi...
☐ Require Security	Accepts unsecured communi...

Buttons: Add... Edit... Remove

Navigation: < Back Next > Cancel

38. Click "Finish"



Security Rule Wizard

Completing the New Rule Wizard

You have successfully completed specifying the properties for your new rule.

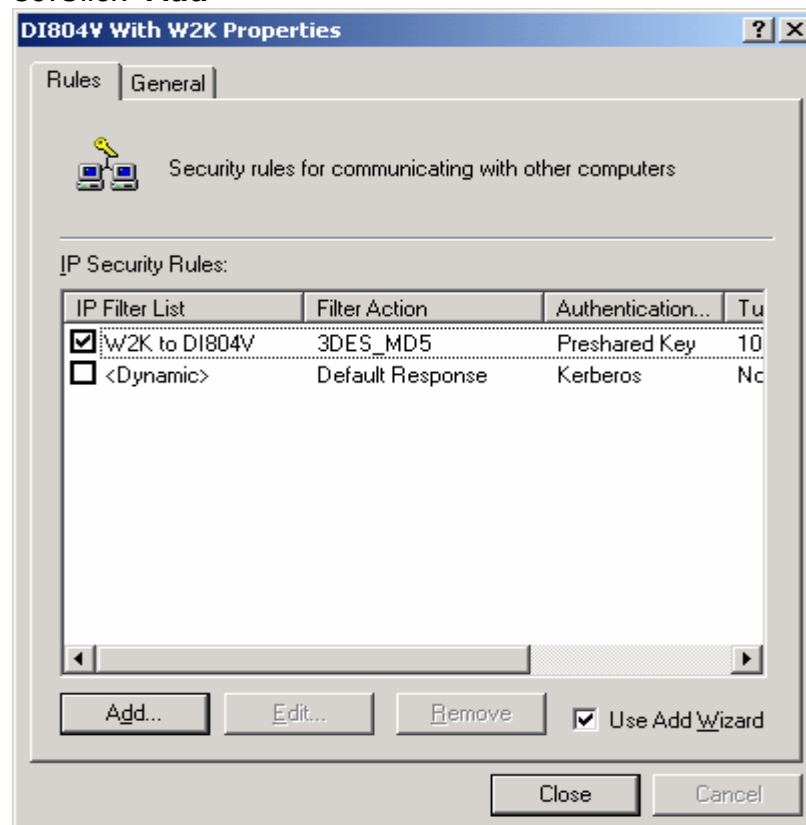
To edit your security rule now, select the Edit properties check box, and then click Finish.

☐ Edit properties

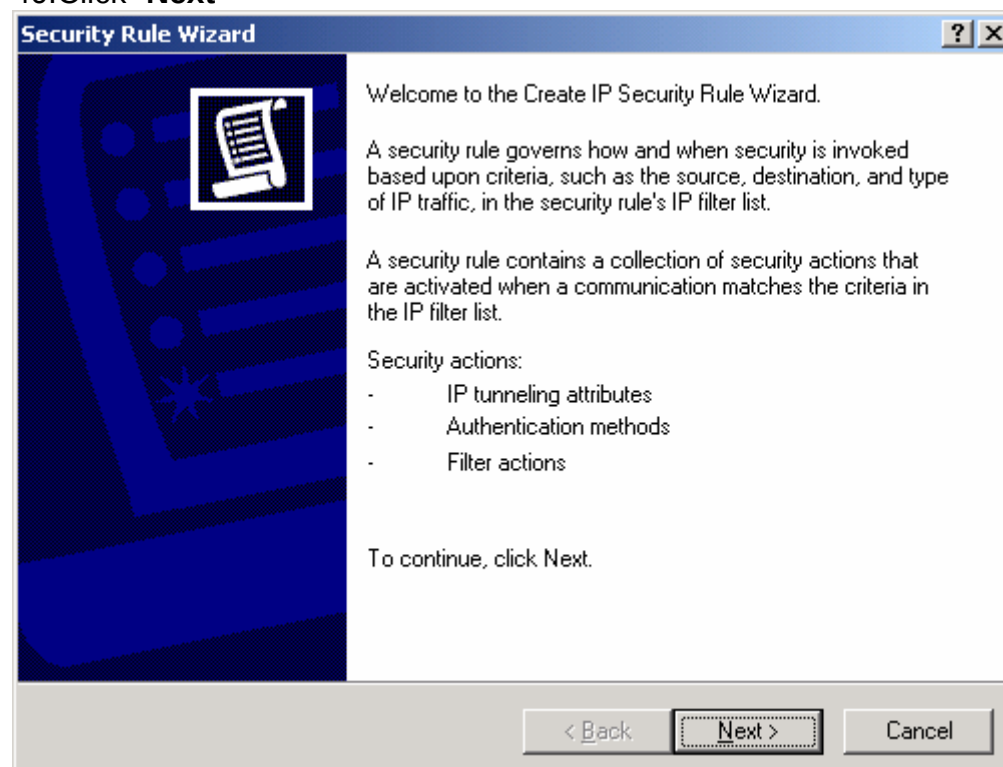
To close this wizard, click Finish.

Navigation: < Back Finish Cancel

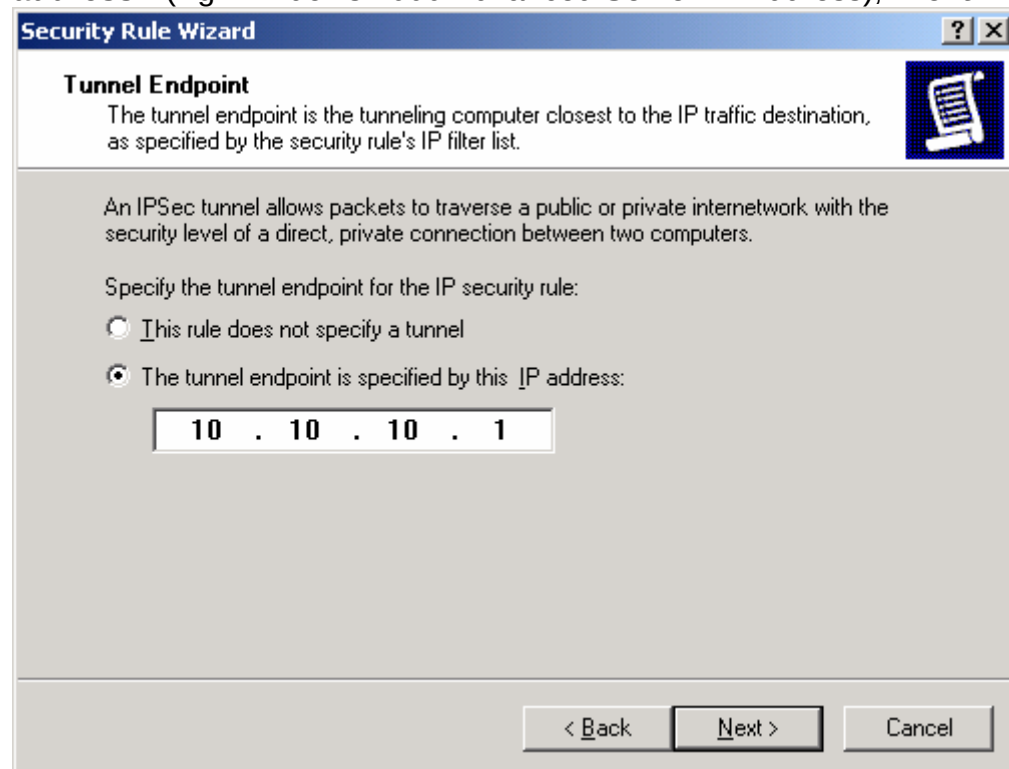
39. Click **"Add"**



40. Click **"Next"**



41. Input the IP Address into “**The tunnel endpoint specified by this IP address:**” (Eg. Windows 2000 Advanced Server IP Address), “**Next**”



The screenshot shows the 'Security Rule Wizard' window, specifically the 'Tunnel Endpoint' step. The window has a title bar with a question mark and a close button. The main area contains a description of a tunnel endpoint, a paragraph about IPsec tunnels, and two radio button options. The second option, 'The tunnel endpoint is specified by this IP address:', is selected. Below it is a text box containing the IP address '10 . 10 . 10 . 1'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

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:

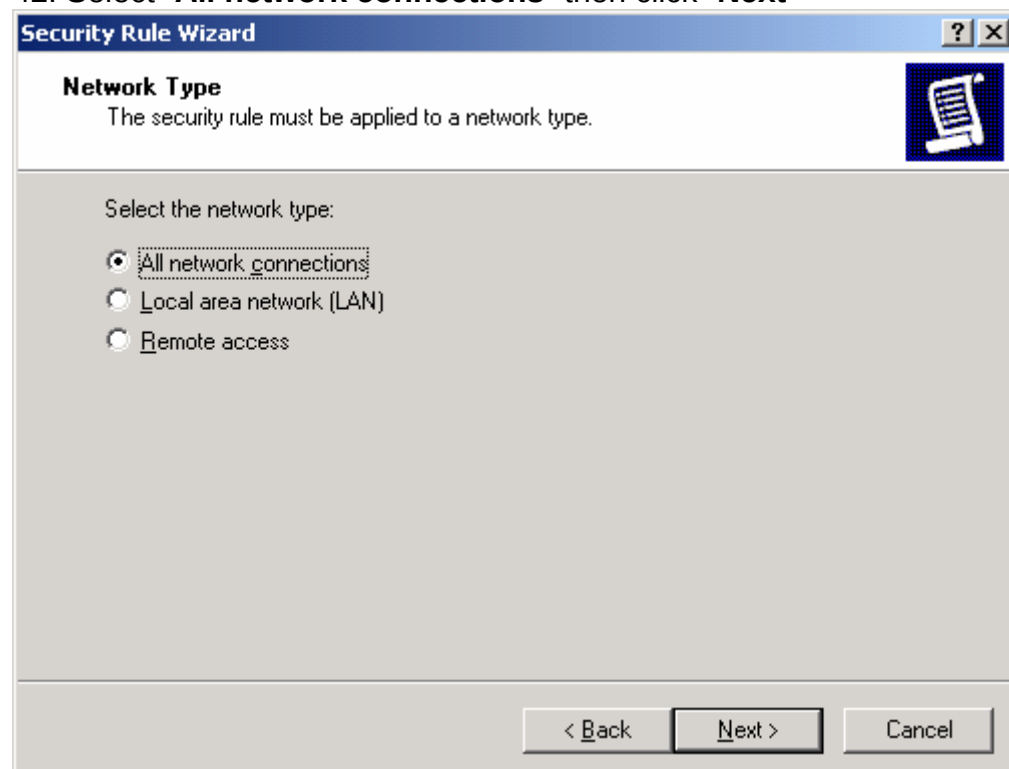
☐ This rule does not specify a tunnel

☒ The tunnel endpoint is specified by this IP address:

10 . 10 . 10 . 1

< Back Next > Cancel

42. Select “**All network connections**” then click “**Next**”



The screenshot shows the 'Security Rule Wizard' window, specifically the 'Network Type' step. The window has a title bar with a question mark and a close button. The main area contains a description of network types and three radio button options. The first option, 'All network connections', is selected. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Security Rule Wizard

Network Type
The security rule must be applied to a network type.

Select the network type:

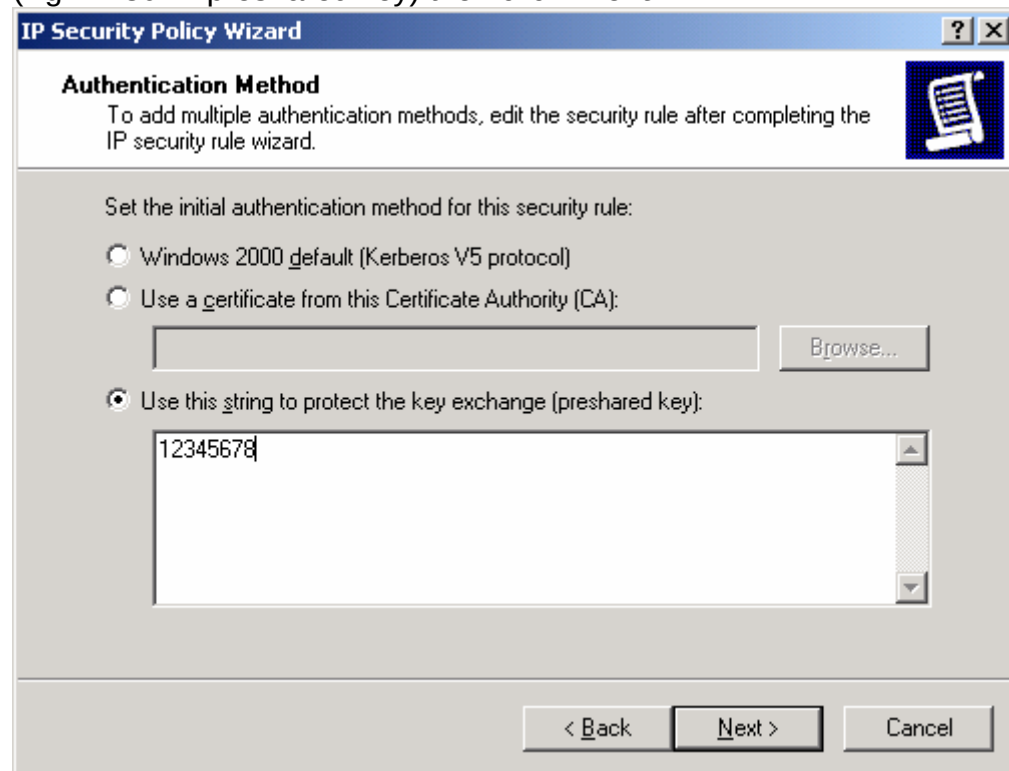
☒ All network connections

☐ Local area network (LAN)

☐ Remote access

< Back Next > Cancel

43. Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DI-804V preshared key) then click “**Next**”



The screenshot shows the 'Authentication Method' step of the IP Security Policy Wizard. The title bar reads 'IP Security Policy Wizard'. Below the title bar, 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.' There are three radio button options: 'Windows 2000 default (Kerberos V5 protocol)', 'Use a certificate from this Certificate Authority (CA):' (with an empty text box and a 'Browse...' button), and 'Use this string to protect the key exchange (preshared key):' (which is selected). Below the selected option is a large text box containing the string '12345678'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

IP Security Policy Wizard

Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.

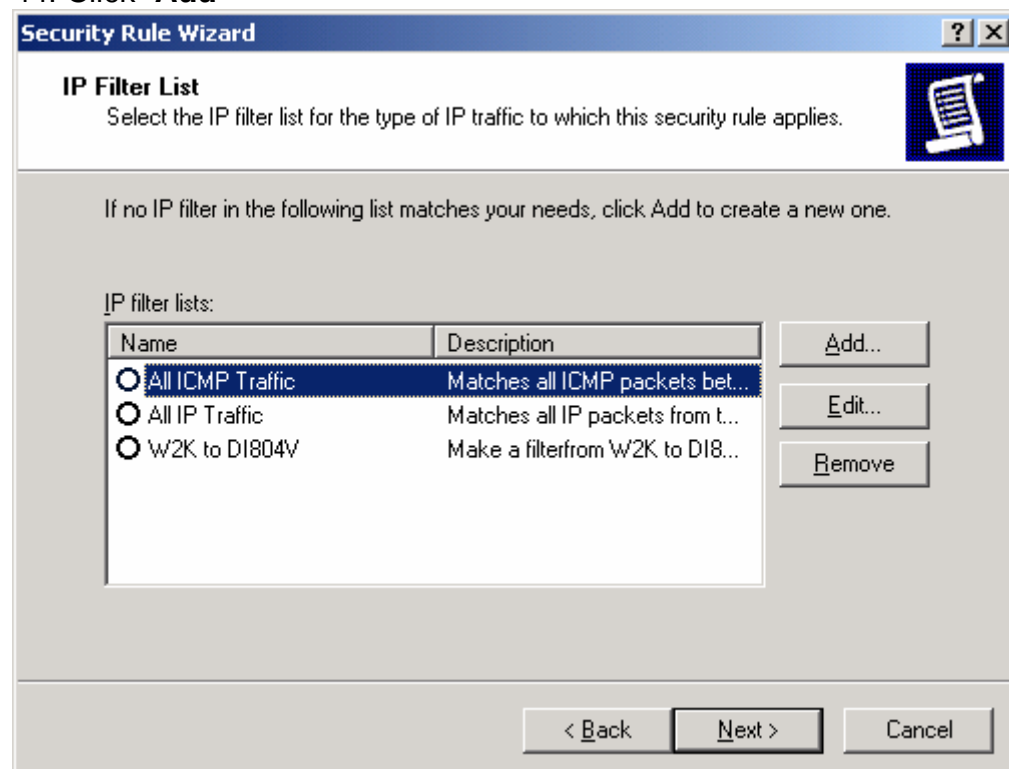
Set the initial authentication method for this security rule:

☐ Windows 2000 default (Kerberos V5 protocol)

☐ Use a certificate from this Certificate Authority (CA):

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

44. 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 sub-instruction: 'Select the IP filter list for the type of IP traffic to which this security rule applies.' A note states: 'If no IP filter in the following list matches your needs, click Add to create a new one.' Below this is a table of IP filter lists. The first column is 'Name' and the second is 'Description'. The first row is 'All ICMP Traffic' (selected with a radio button) with description 'Matches all ICMP packets bet...'. The second row is 'All IP Traffic' with description 'Matches all IP packets from t...'. The third row is 'W2K to DI804V' with description 'Make a filterfrom W2K to DI8...'. To the right of the table are buttons for 'Add...', 'Edit...', and 'Remove'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

Security Rule Wizard

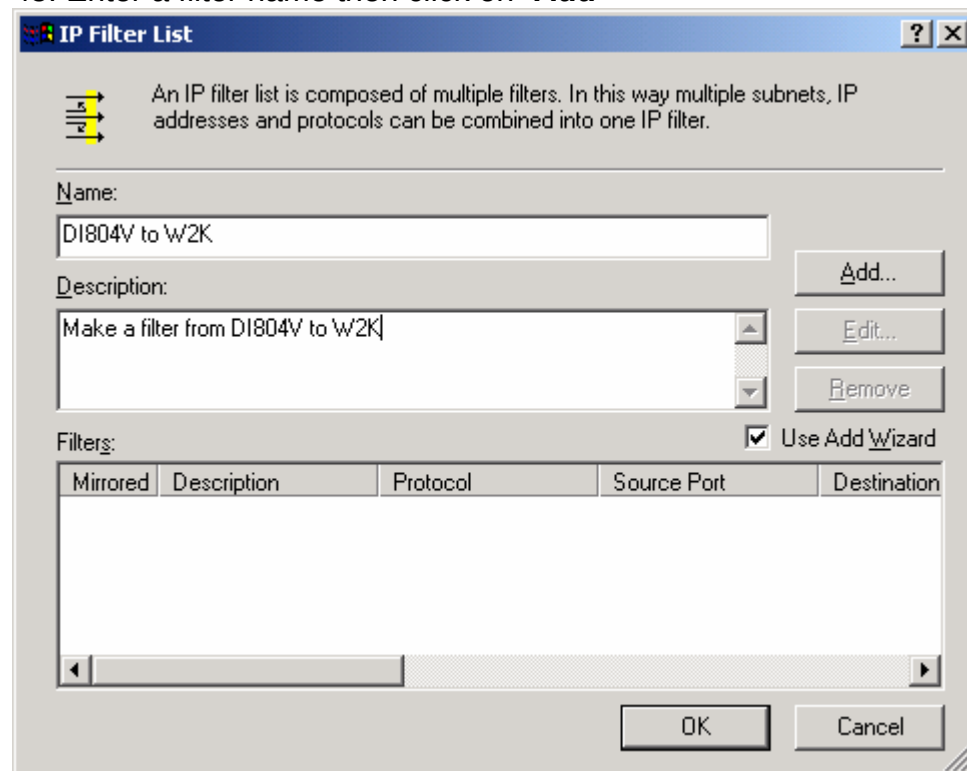
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
☒ All ICMP Traffic	Matches all ICMP packets bet...
☐ All IP Traffic	Matches all IP packets from t...
☐ W2K to DI804V	Make a filterfrom W2K to DI8...

45. Enter a filter name then click on “Add”



The IP Filter List dialog box has a title bar with a question mark and a close button. Below the title bar is a help icon and a text box explaining that an IP filter list is composed of multiple filters. The main area contains a 'Name' field with the text 'D1804V to W2K', a 'Description' field with the text 'Make a filter from D1804V to W2K', and a 'Filters' section with a table. The table has columns for 'Mirrored', 'Description', 'Protocol', 'Source Port', and 'Destination'. To the right of the 'Description' field are three buttons: 'Add...', 'Edit...', and 'Remove'. To the right of the 'Filters' section is a checkbox labeled 'Use Add Wizard'. At the bottom are 'OK' and 'Cancel' buttons.

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: D1804V to W2K

Description: Make a filter from D1804V to W2K

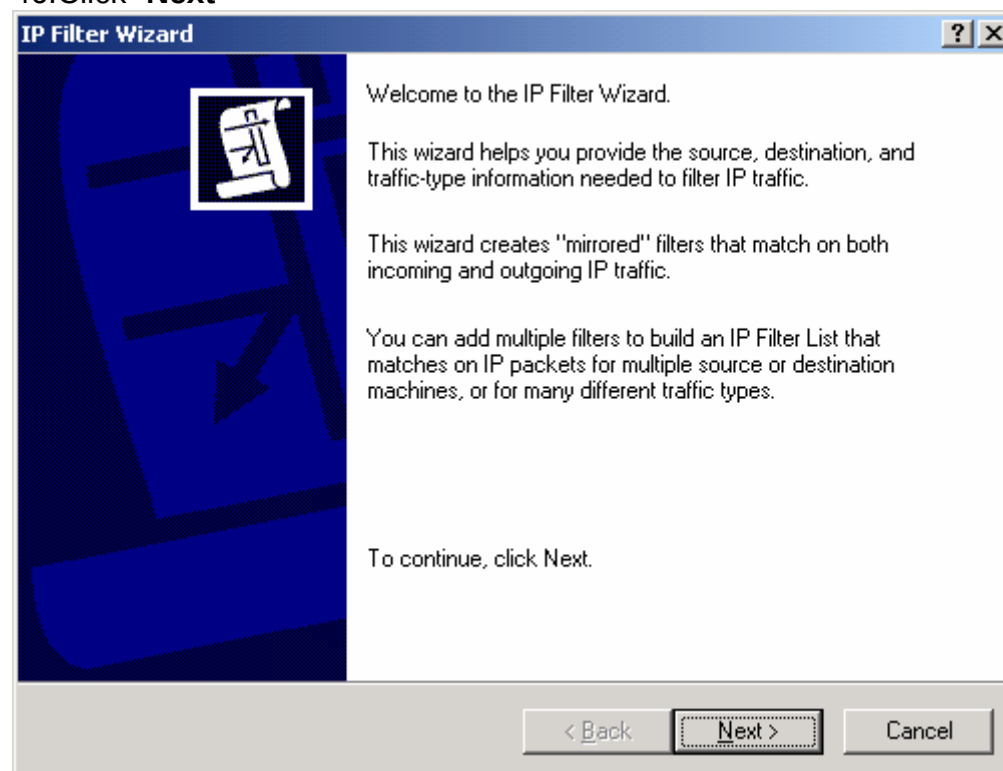
Filters:

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

Use Add Wizard ☒

OK Cancel

46. Click “Next”



The IP Filter Wizard dialog box has a title bar with a question mark and a close button. The main area contains a large blue graphic on the left and text on the right. The text includes a welcome message, an explanation of the wizard's purpose, a description of 'mirrored' filters, and instructions on how to use the wizard. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

IP Filter Wizard

Welcome to the IP Filter Wizard.

This wizard helps you provide the source, destination, and traffic-type information needed to filter IP traffic.

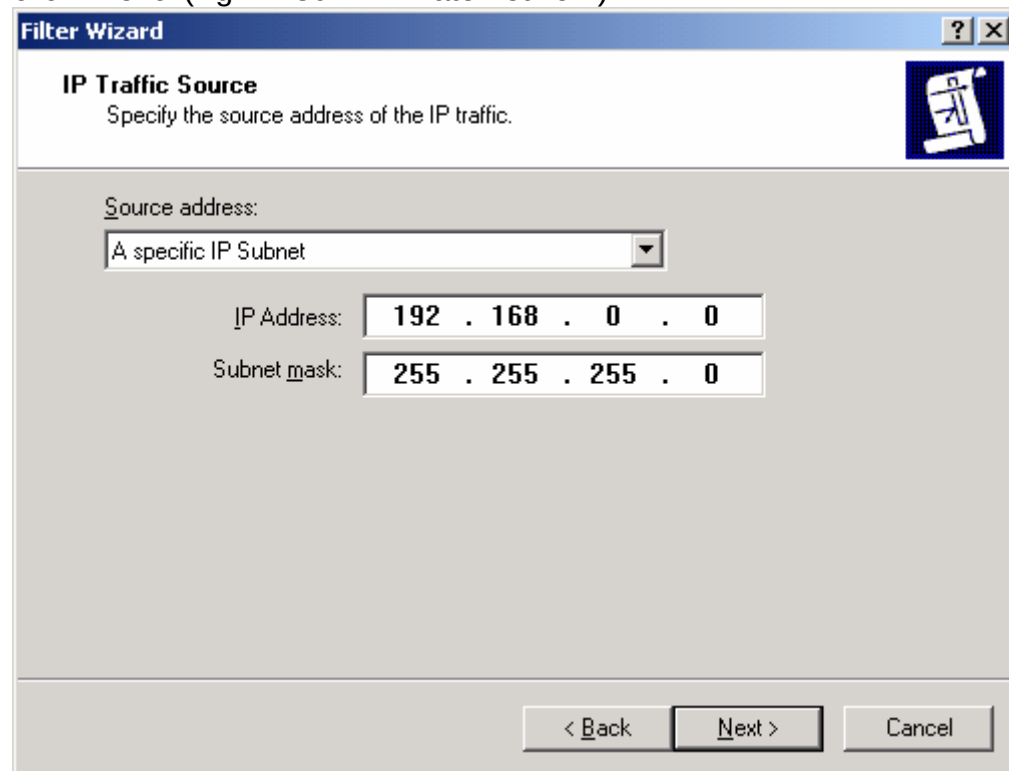
This wizard creates "mirrored" filters that match on both incoming and outgoing IP traffic.

You can add multiple filters to build an IP Filter List that matches on IP packets for multiple source or destination machines, or for many different traffic types.

To continue, click Next.

< Back Next > Cancel

47. Select “**A specific IP Subnet**” and input the Source subnet address then click “**Next**” (Eg. DI-804V Private network)



The image shows a Windows-style dialog box titled "Filter Wizard" with a blue header bar containing a question mark icon and a close button. The main title is "IP Traffic Source" in bold, followed by the instruction "Specify the source address of the IP traffic." in a smaller font. On the right side of the title bar is a small icon of a document with a pencil. Below the title bar, there is a section for "Source address:" which includes a dropdown menu currently set to "A specific IP Subnet". Below this, there are two input fields: "IP Address:" with the value "192 . 168 . 0 . 0" and "Subnet mask:" with the value "255 . 255 . 255 . 0". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Filter Wizard

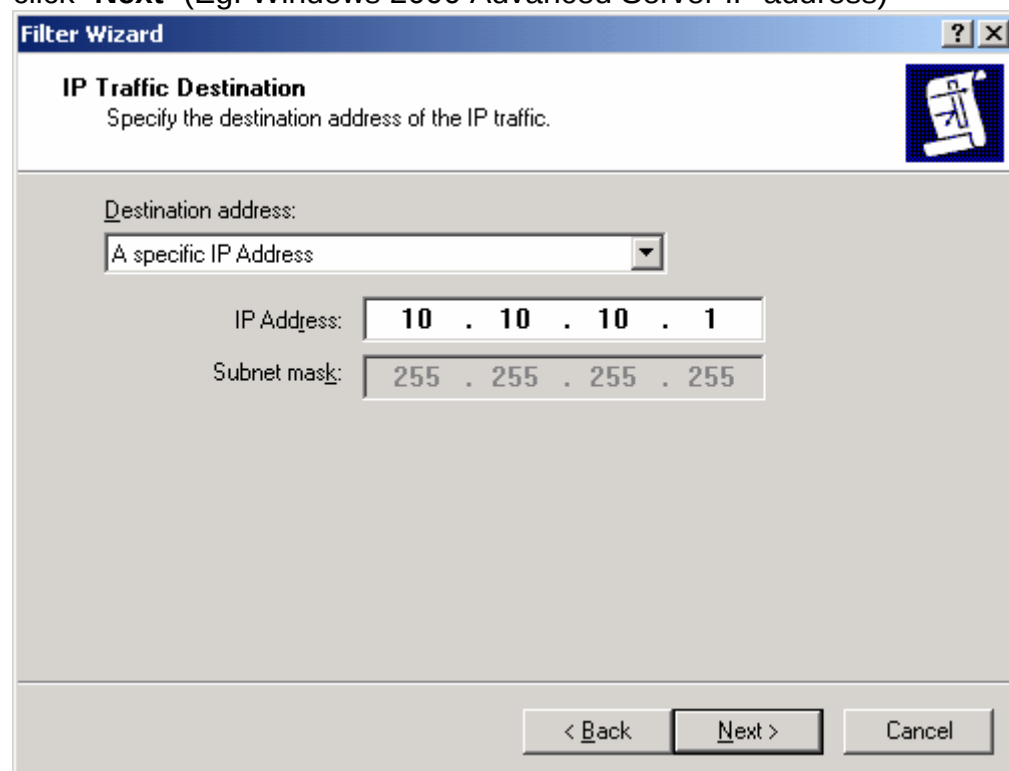
IP Traffic Source
Specify the source address of the IP traffic.

Source address:
A specific IP Subnet

IP Address: 192 . 168 . 0 . 0
Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

48. Select “**A specific IP Address**” and input the Destination address then click “**Next**” (Eg. Windows 2000 Advanced Server IP address)



The image shows a Windows-style dialog box titled "Filter Wizard" with a blue header bar containing a question mark icon and a close button. The main title is "IP Traffic Destination" in bold, followed by the instruction "Specify the destination address of the IP traffic." in a smaller font. On the right side of the title bar is a small icon of a document with a pencil. Below the title bar, there is a section for "Destination address:" which includes a dropdown menu currently set to "A specific IP Address". Below this, there are two input fields: "IP Address:" with the value "10 . 10 . 10 . 1" and "Subnet mask:" with the value "255 . 255 . 255 . 255". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Filter Wizard

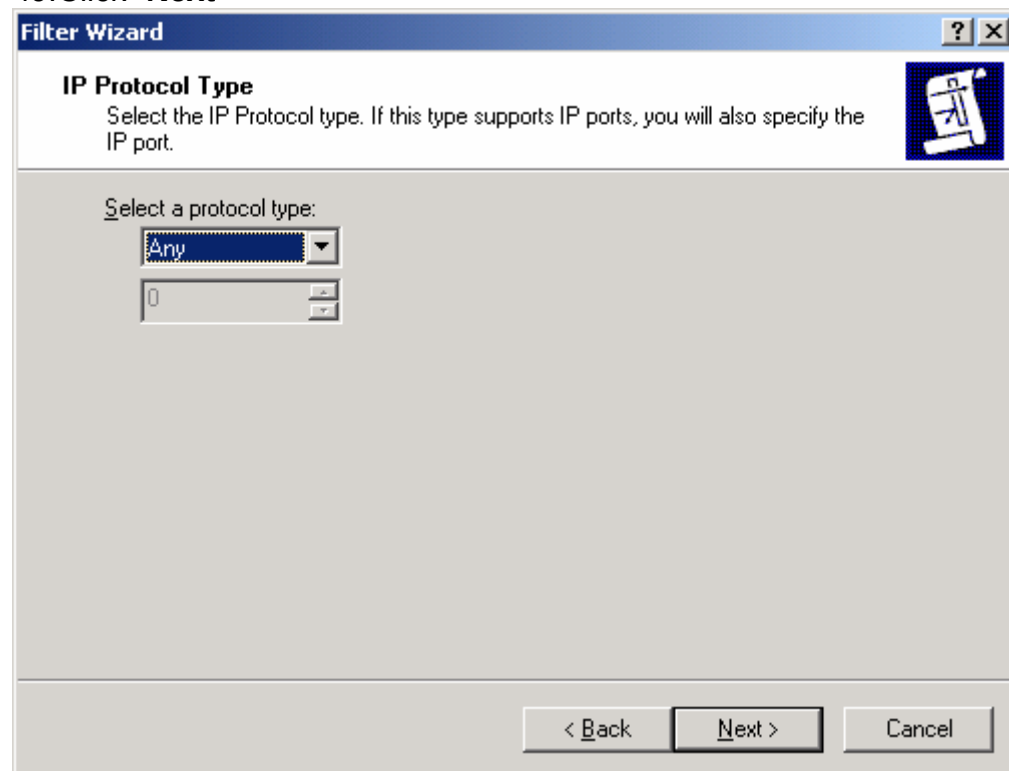
IP Traffic Destination
Specify the destination address of the IP traffic.

Destination address:
A specific IP Address

IP Address: 10 . 10 . 10 . 1
Subnet mask: 255 . 255 . 255 . 255

< Back Next > Cancel

49. Click **Next**



The **Filter Wizard** dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled **IP Protocol Type** and contains the instruction: "Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port." Below this, there is a label "Select a protocol type:" followed by a dropdown menu showing "Any" and a text box containing "0". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Filter Wizard

IP Protocol Type
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.

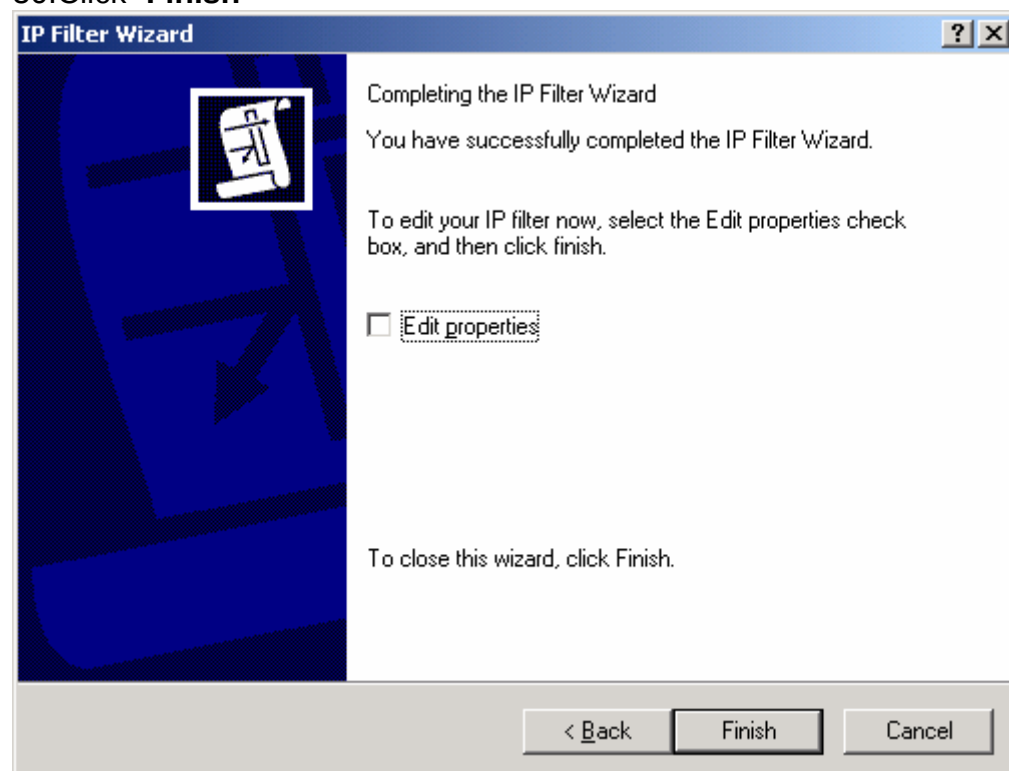
Select a protocol type:

Any

0

< Back Next > Cancel

50. Click **Finish**



The **IP Filter Wizard** dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled **Completing the IP Filter Wizard** and contains the text: "You have successfully completed the IP Filter Wizard." Below this, there is a checkbox labeled "Edit properties" which is currently unchecked. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel".

IP Filter Wizard

Completing the IP Filter Wizard
You have successfully completed the IP Filter Wizard.

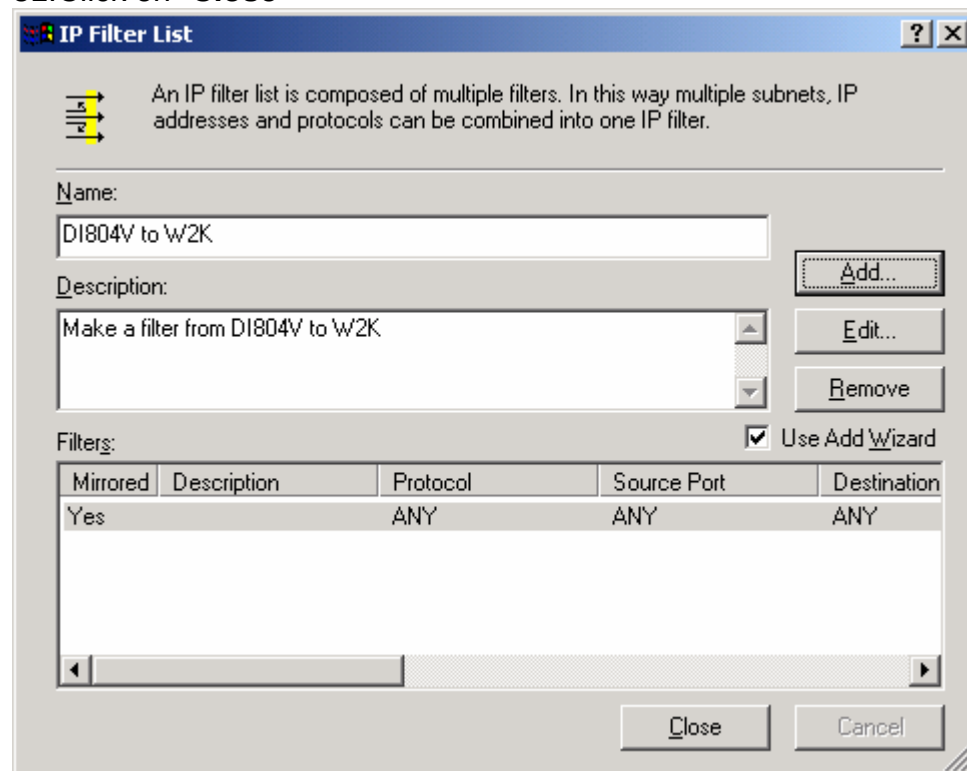
To edit your IP filter now, select the Edit properties check box, and then click finish.

☐ Edit properties

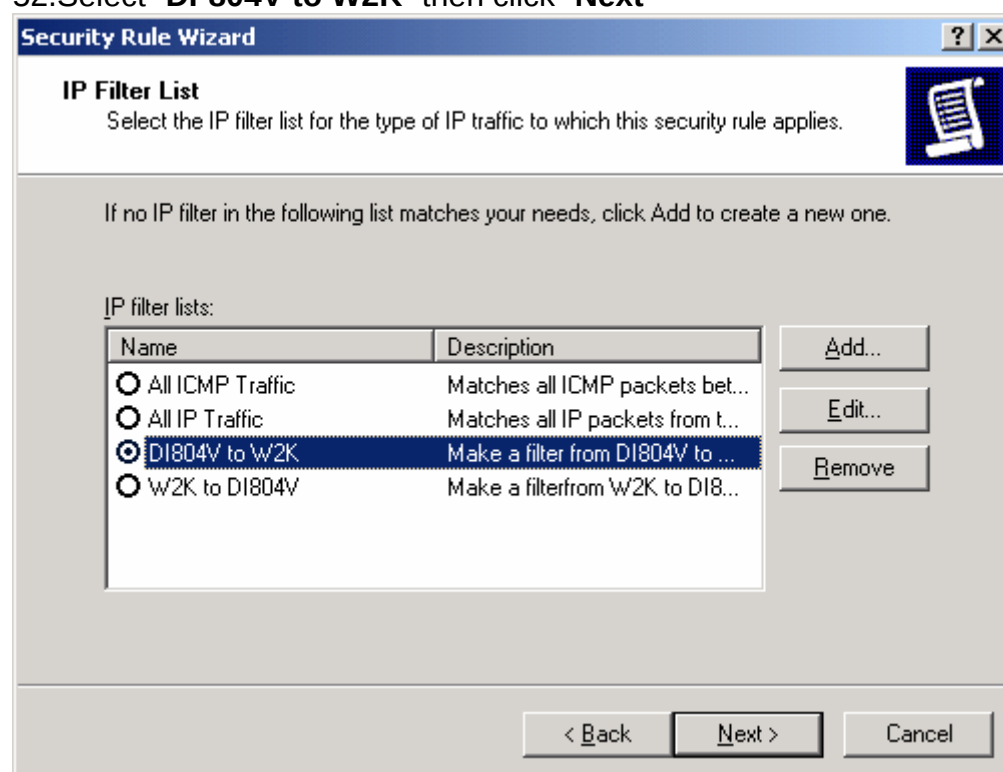
To close this wizard, click Finish.

< Back Finish Cancel

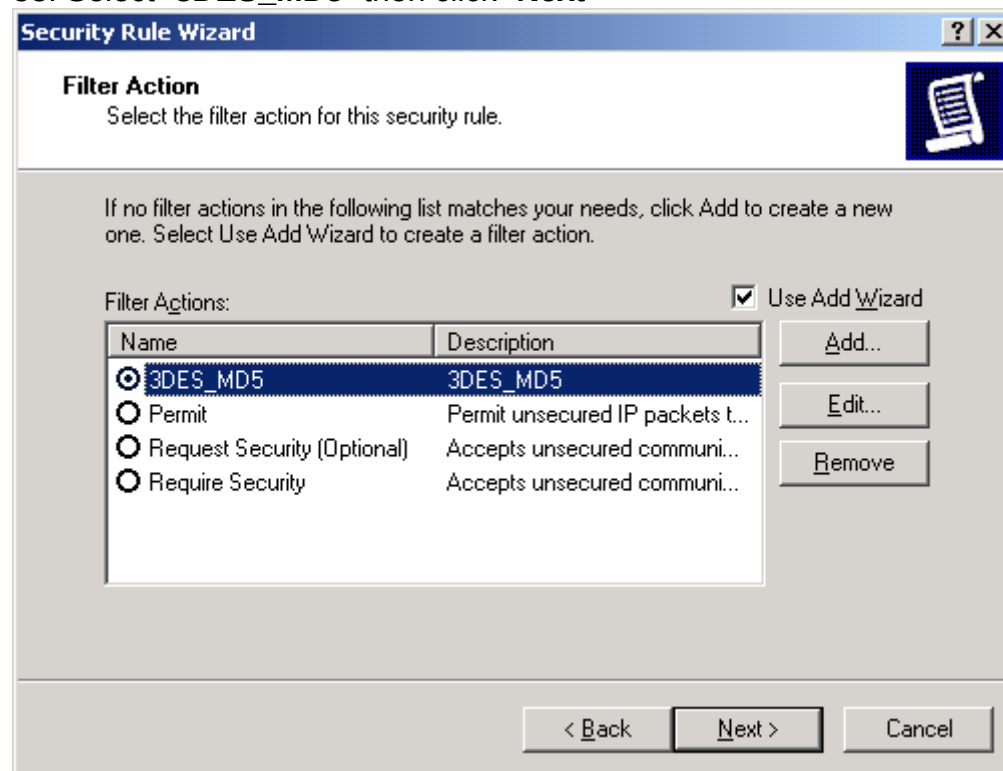
51. Click on “Close”



52. Select “DI-804V to W2K” then click “Next”



53. Select “3DES_MD5” then click “Next”



The screenshot shows the 'Security Rule Wizard' window at the 'Filter Action' step. The title bar reads 'Security Rule Wizard'. Below the title bar, the text 'Filter Action' is followed by the instruction 'Select the filter action for this security rule.' To the right is a document icon. A paragraph states: 'If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.' Below this is a section titled 'Filter Actions:' with a checked box for 'Use Add Wizard'. A table lists filter actions with columns 'Name' and 'Description'. The first row, '3DES_MD5', is selected. To the right of the table are buttons for 'Add...', 'Edit...', and 'Remove'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

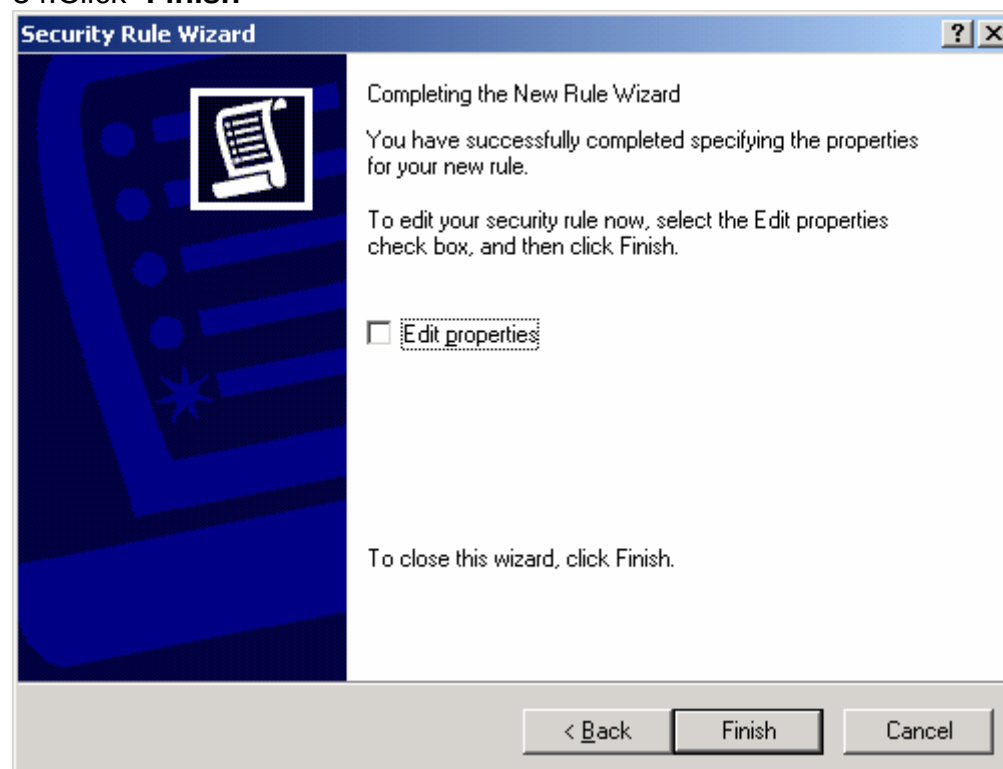
Filter Actions: ☒ Use Add Wizard

Name	Description
☒ 3DES_MD5	3DES_MD5
☐ Permit	Permit unsecured IP packets t...
☐ Request Security (Optional)	Accepts unsecured communi...
☐ Require Security	Accepts unsecured communi...

Add... Edit... Remove

< Back Next > Cancel

54. Click “Finish”



The screenshot shows the 'Security Rule Wizard' window at the 'Completing the New Rule Wizard' step. The title bar reads 'Security Rule Wizard'. On the left is a large graphic of a document with a star. The main text says 'Completing the New Rule Wizard' followed by 'You have successfully completed specifying the properties for your new rule.' Below this is the instruction 'To edit your security rule now, select the Edit properties check box, and then click Finish.' and a checkbox for 'Edit properties'. At the bottom is the instruction 'To close this wizard, click Finish.' and buttons for '< Back', 'Finish', and 'Cancel'.

Security Rule Wizard

Completing the New Rule Wizard

You have successfully completed specifying the properties for your new rule.

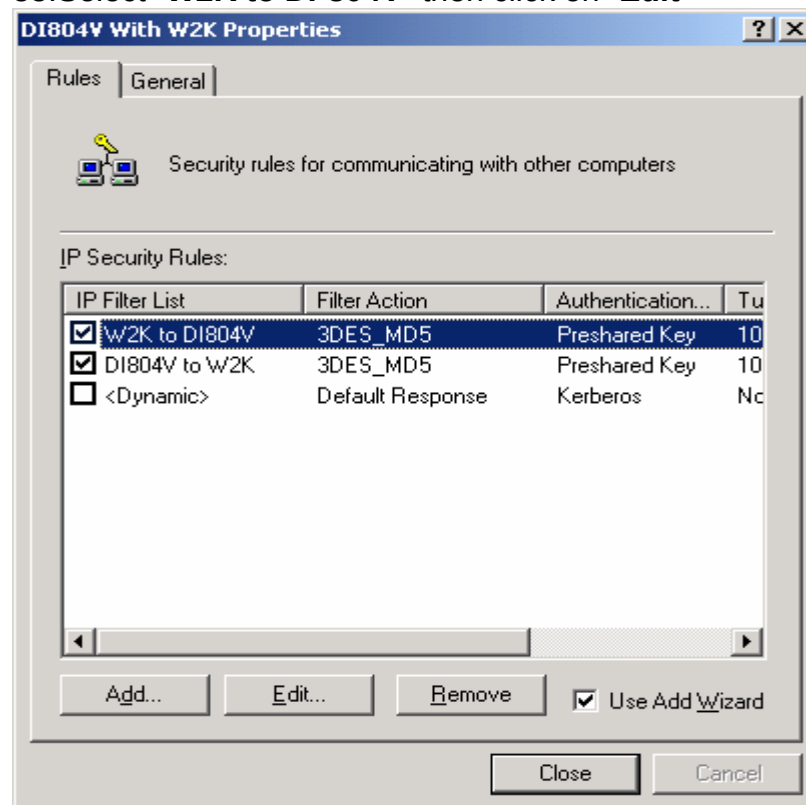
To edit your security rule now, select the Edit properties check box, and then click Finish.

☐ Edit properties

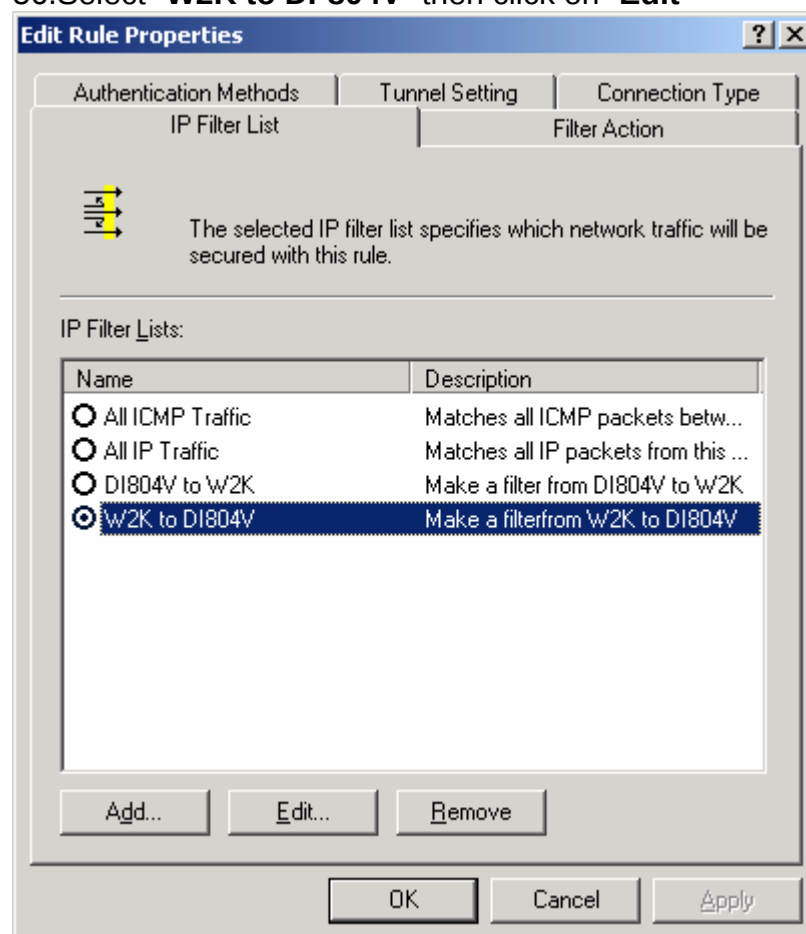
To close this wizard, click Finish.

< Back Finish Cancel

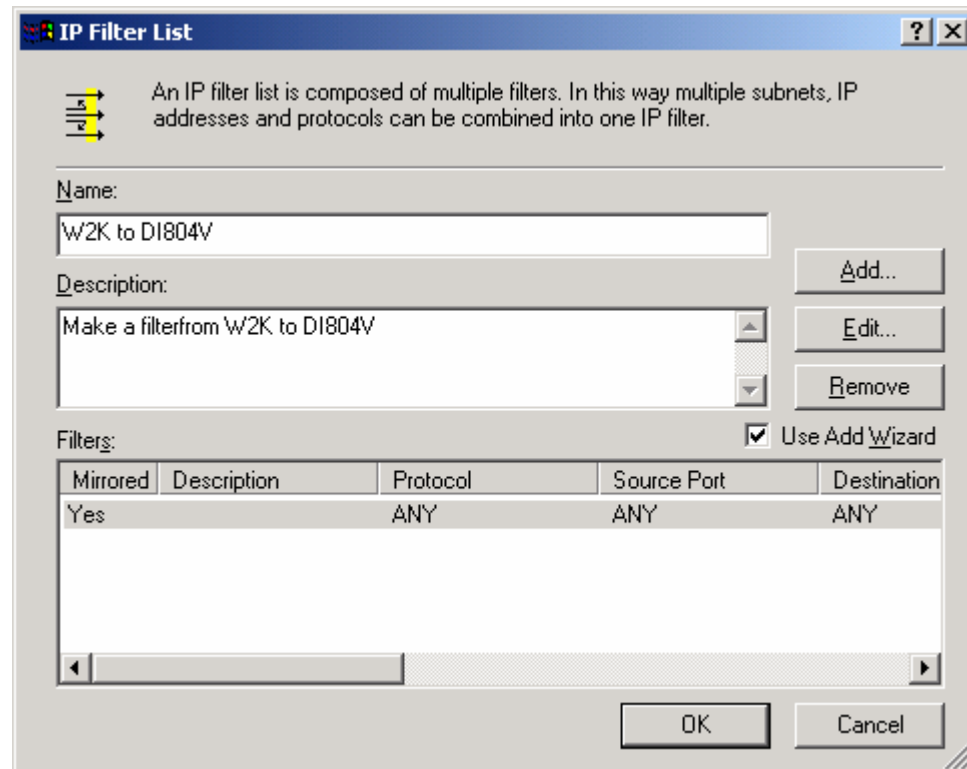
55. Select **"W2K to DI-804V"** then click on **"Edit"**



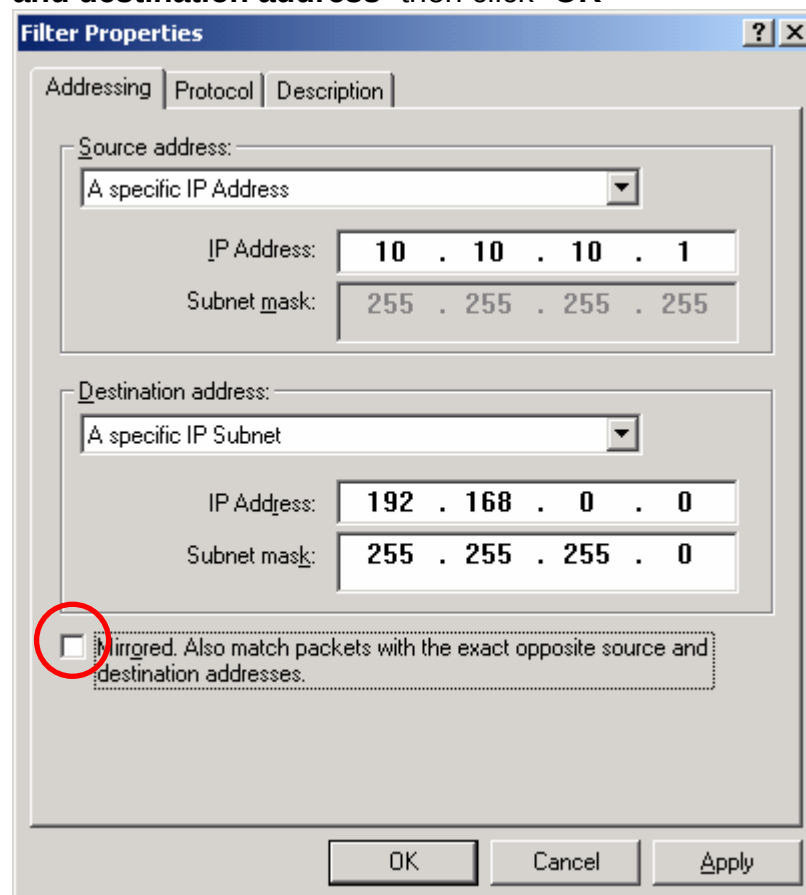
56. Select **"W2K to DI-804V"** then click on **"Edit"**



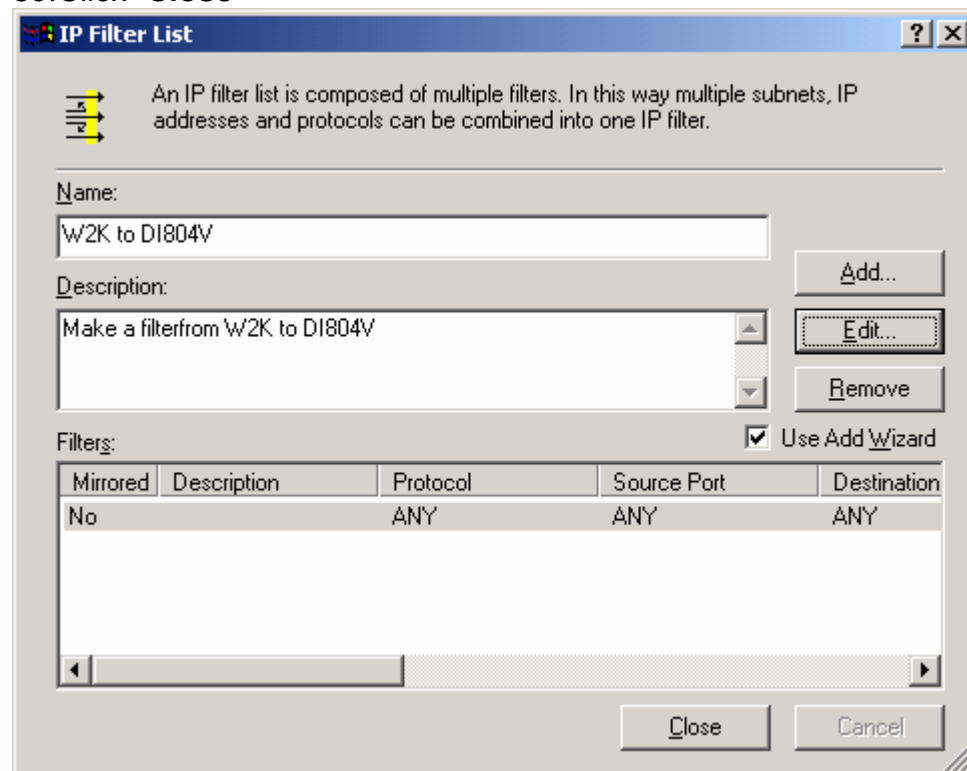
57. Click **"Edit"**



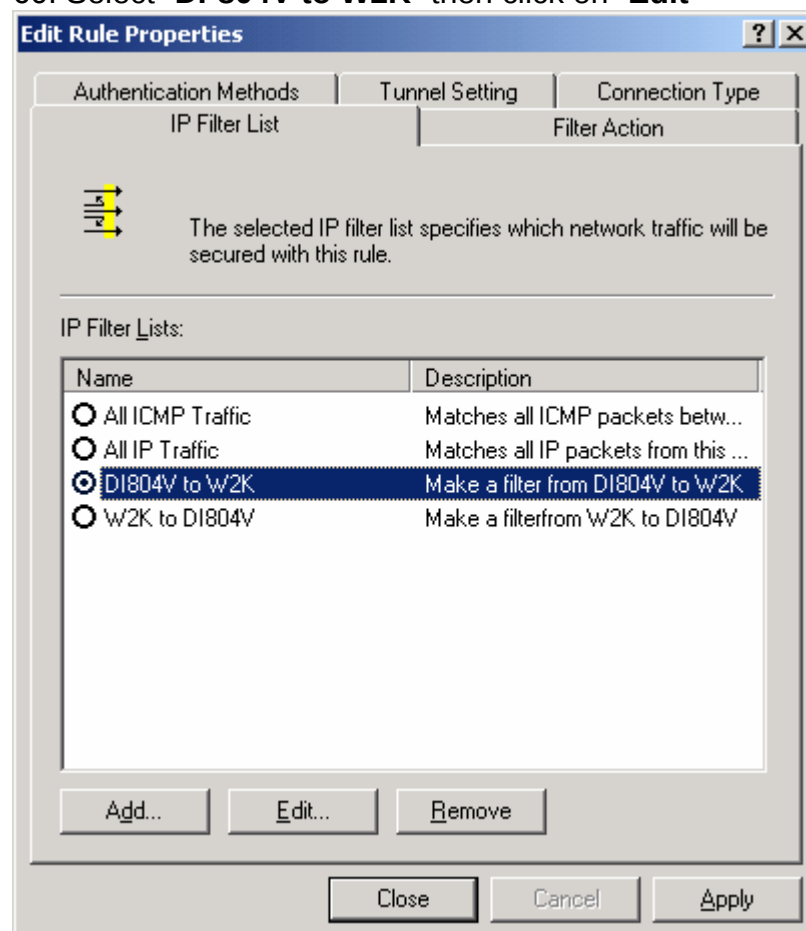
58. Uncheck **"Mirrored. Also match packets with exact opposite source and destination address"** then click **"OK"**



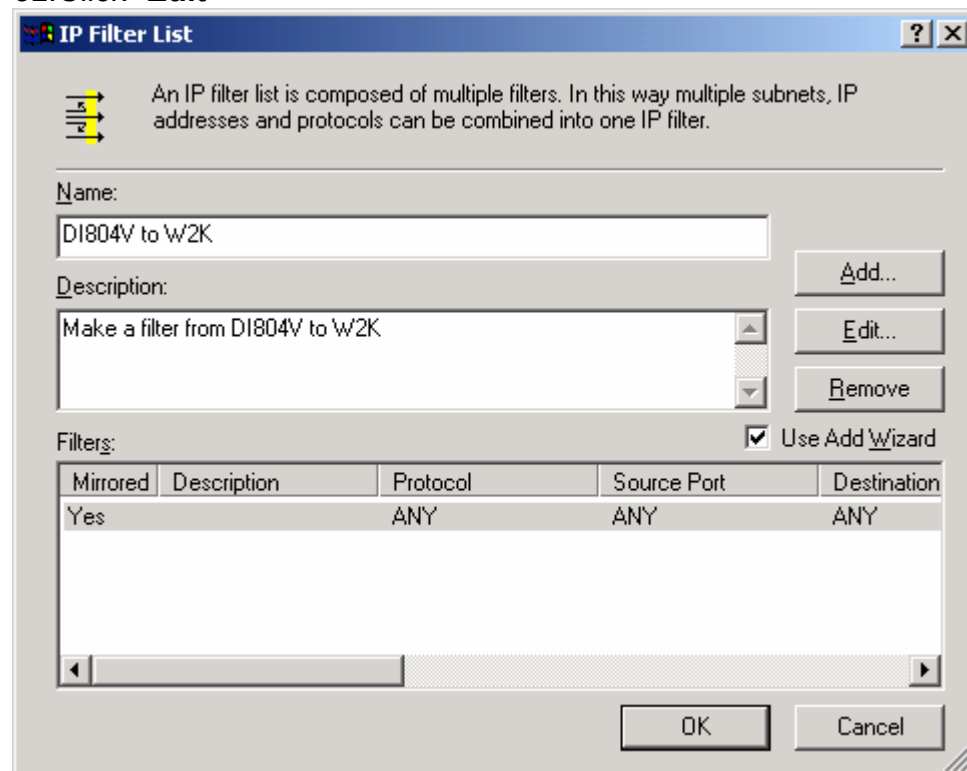
59. Click **“Close”**



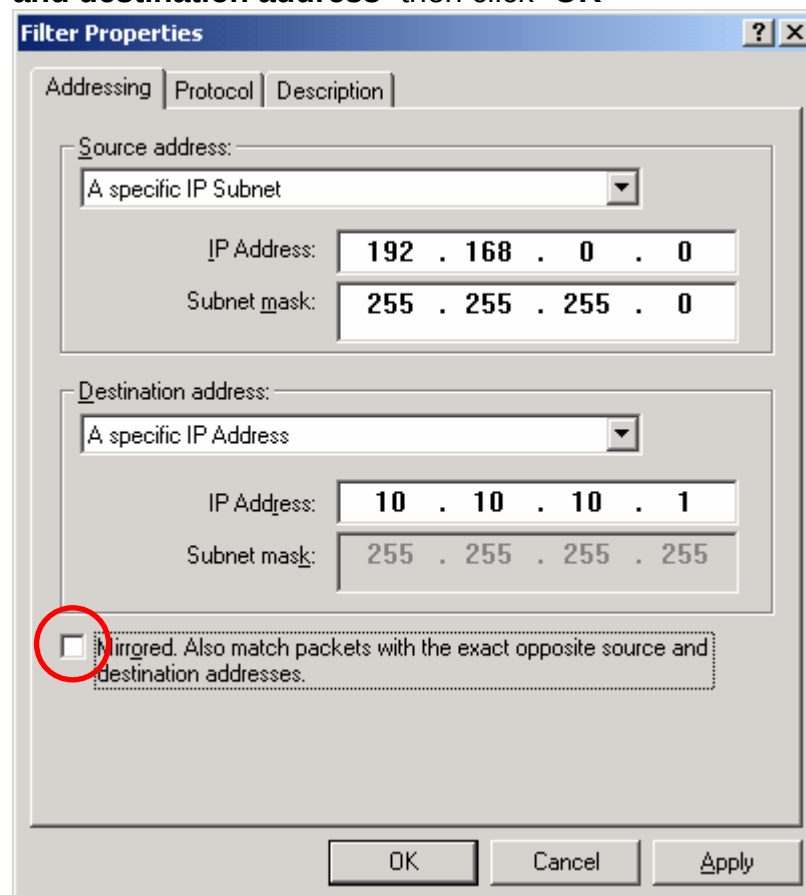
60. Select **“DI-804V to W2K”** then click on **“Edit”**



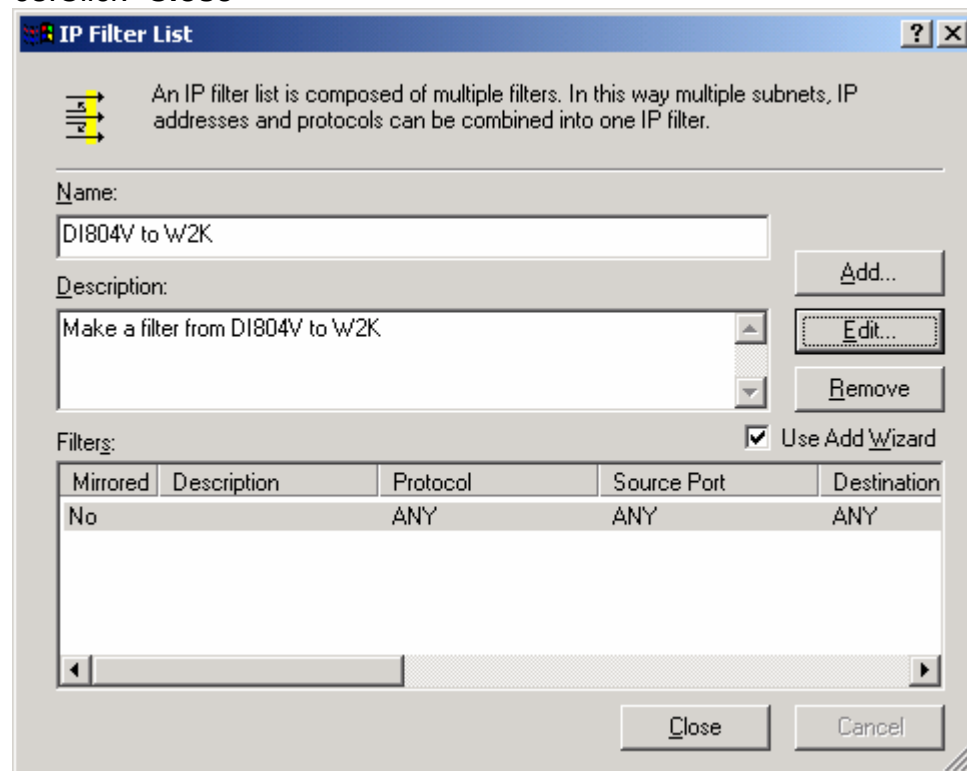
61. Click **Edit**



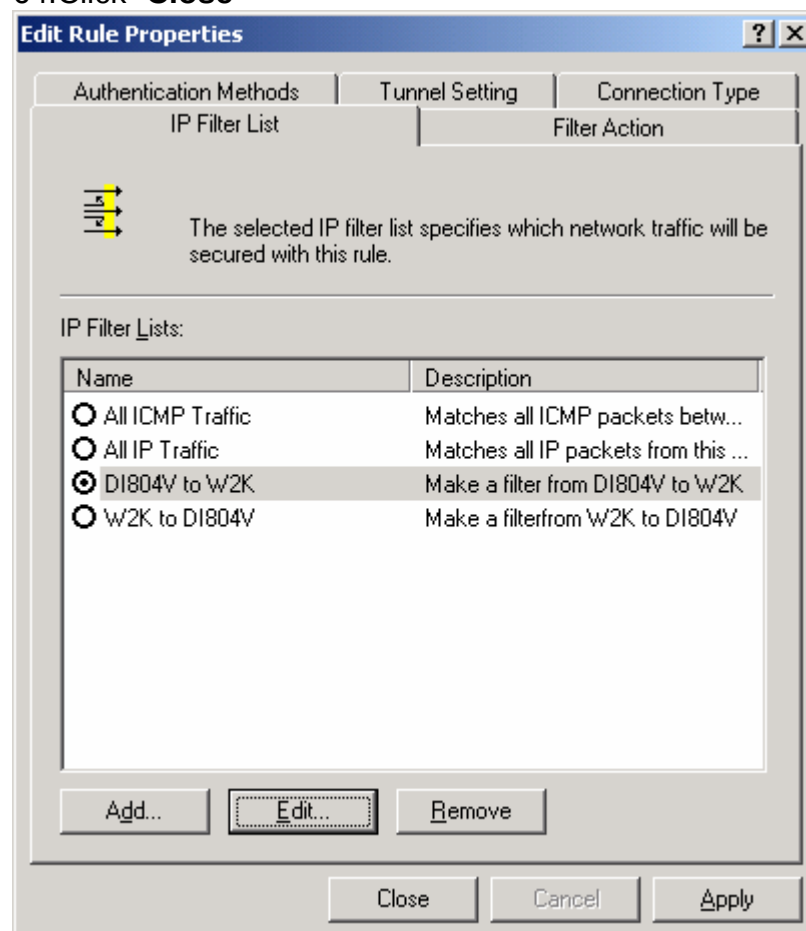
62. Uncheck **Mirrored. Also match packets with exact opposite source and destination address** then click **OK**



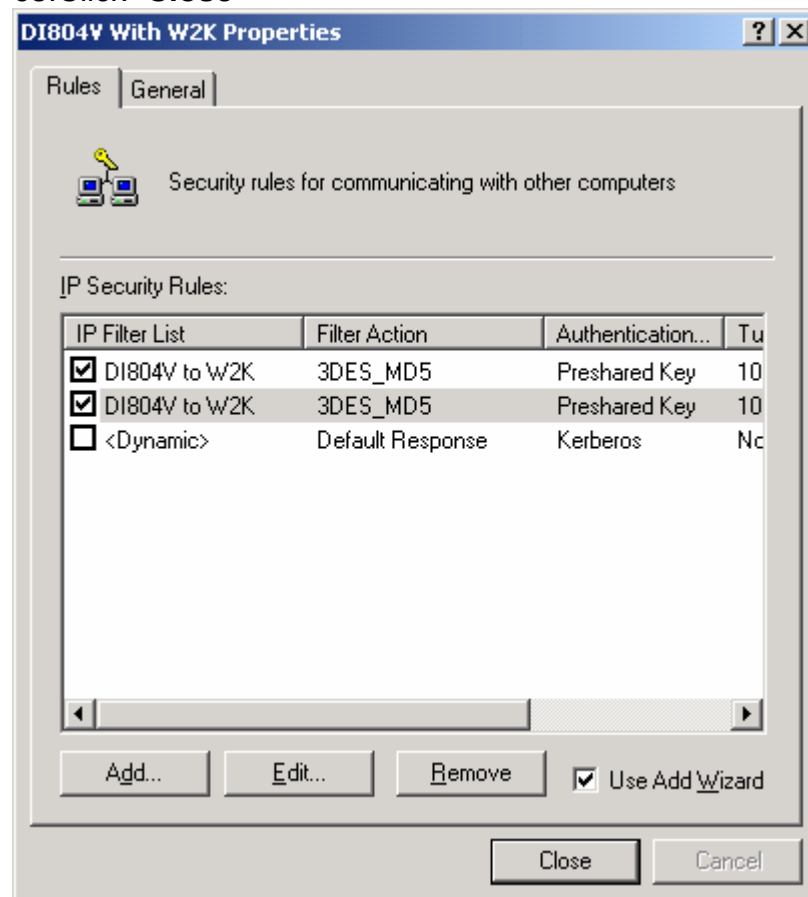
63. Click **“Close”**



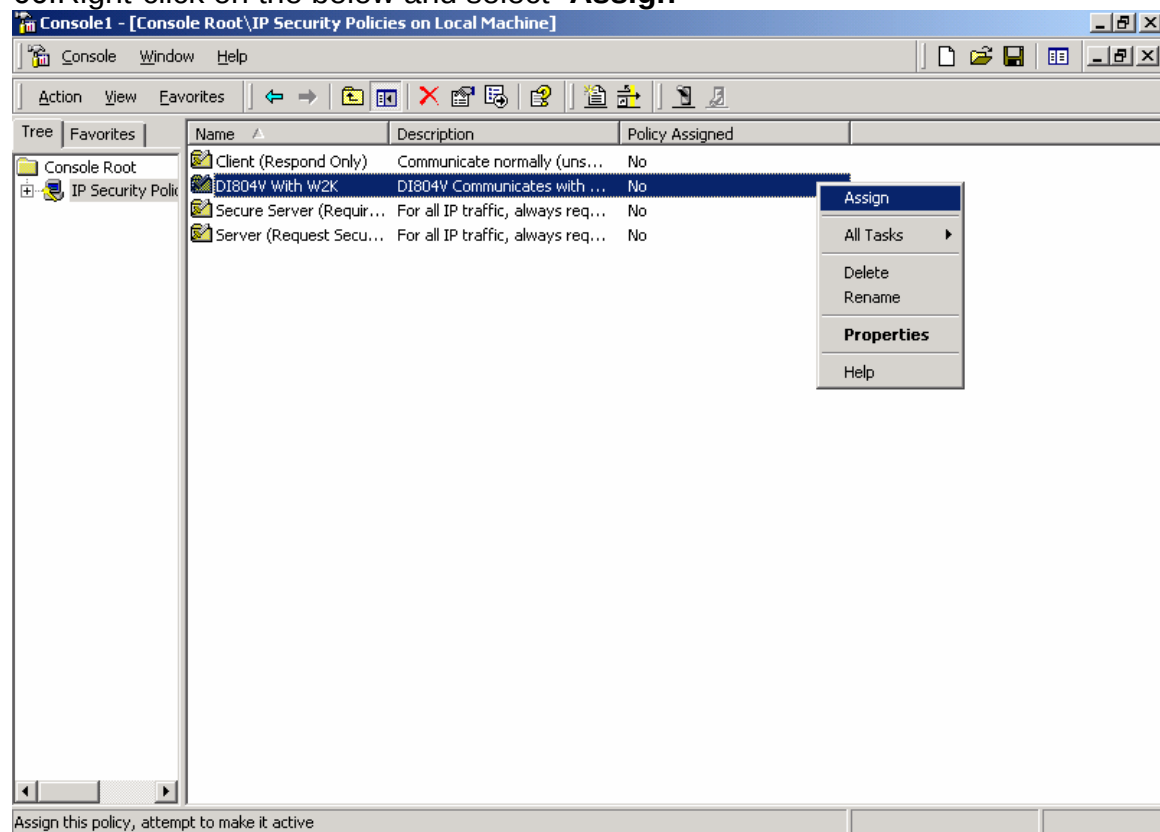
64. Click **“Close”**



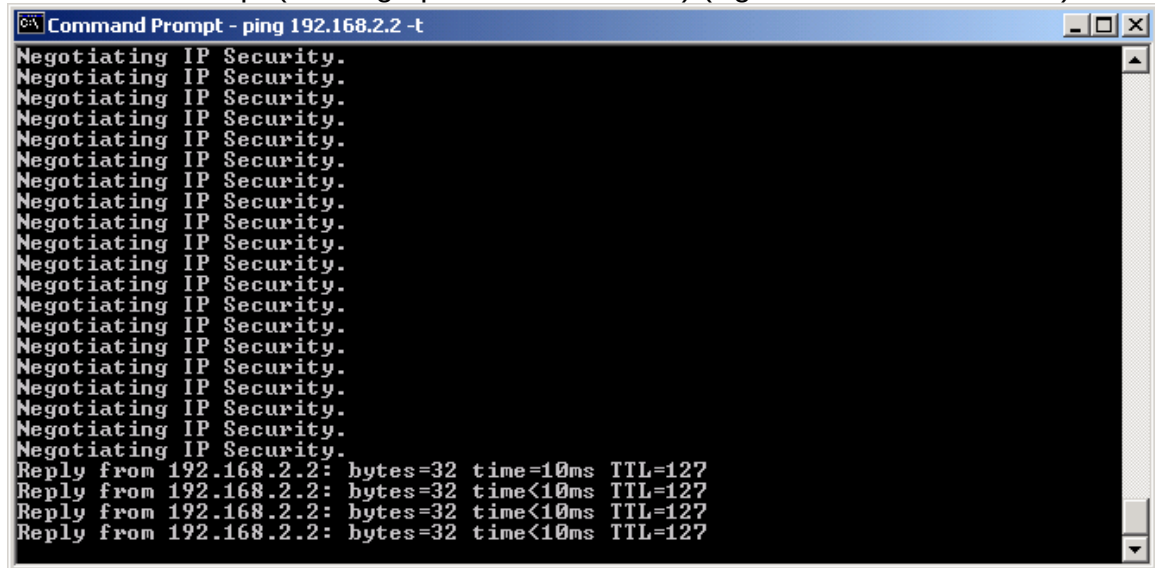
65. Click **“Close”**



66. Right-click on the below and select **“Assign”**

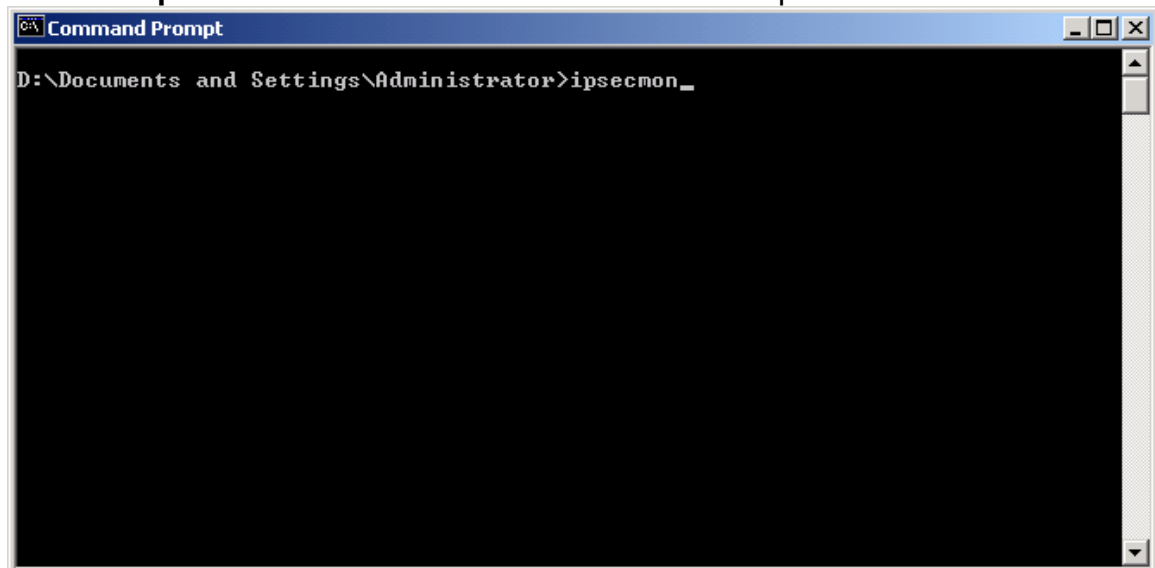


67. Do a **PING** to a valid machine on the Remote private network on the Dos Command Prompt (to bring up the IPSec tunnel) (Eg. PING 192.168.0.2 -t)



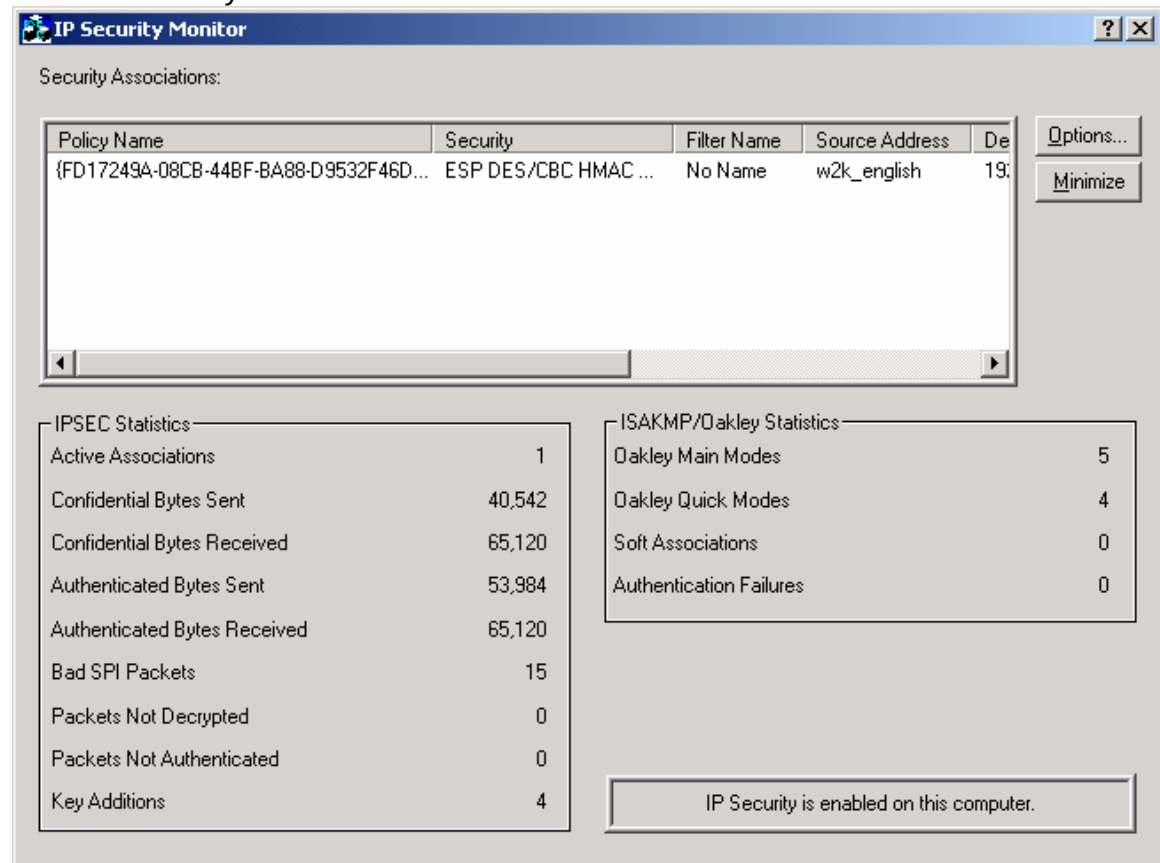
```
Command Prompt - ping 192.168.2.2 -t
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Reply from 192.168.2.2: bytes=32 time=10ms TTL=127
Reply from 192.168.2.2: bytes=32 time<10ms TTL=127
Reply from 192.168.2.2: bytes=32 time<10ms TTL=127
Reply from 192.168.2.2: bytes=32 time<10ms TTL=127
```

68. Enter “**ipsecmon**” on another Dos Command Prompt



```
Command Prompt
D:\Documents and Settings\Administrator>ipsecmon_
```

69. This allows you to check if the IPsec tunnel is built



~ End of Document. Thank you for reading ~