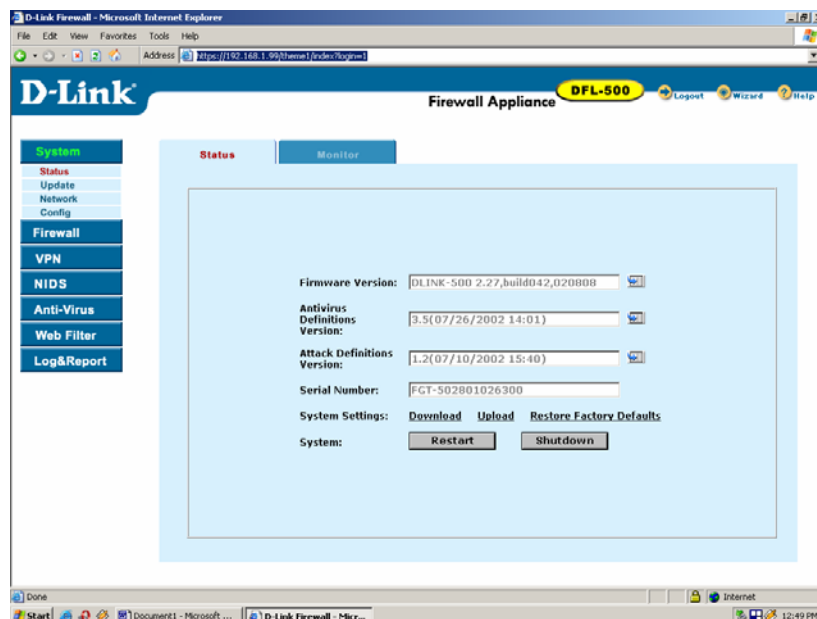


DFL-500 With Windows XP/2000 IPSec VPN Client Configuration Guide

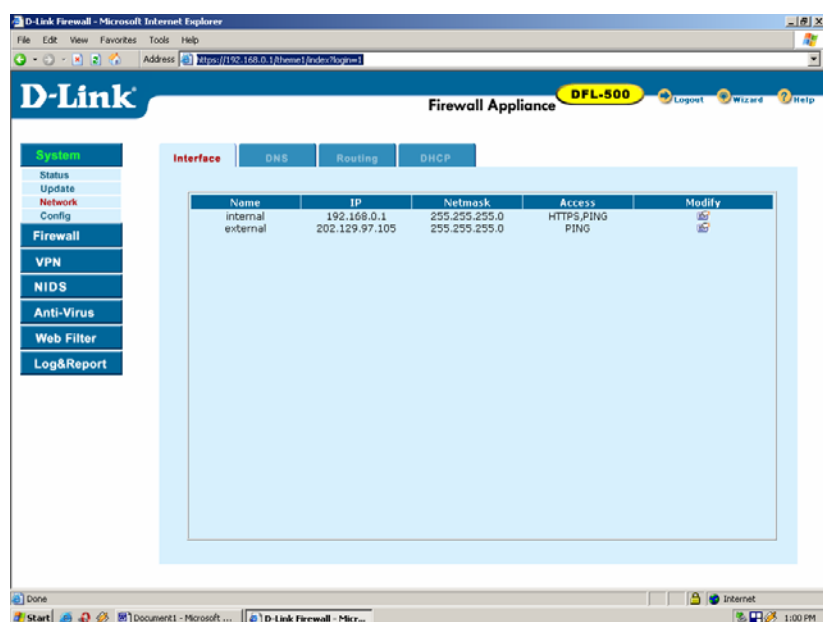
I. Configuring D-Link DFL-500 Firewall

1. Connect your computer to the internal port of the DFL-500 Firewall
2. Change the computer IP address to 192.168.1.100 255.255.255.0
3. In Internet Explorer address type: https://192.168.1.99
4. You will see the message with a Security Alert
5. Click **"yes"**, you are in the Web Base Interface (WBI)
6. Type **"admin"** in the Name field and click **"Login"**



7. Click on **"Network"** under **"System"** menu
8. You will see **"internal"** and **"external"** interfaces
9. Click on **Modify** picture for **"internal"** interface
10. Put the ip address for the internal interface, for example 192.168.0.1 following the subnet mask 255.255.255.0 and press **"OK"**. You will loose the connection to the firewall after you press **"OK"**
11. Now you can connect your firewall to switch or hub and connect your computer to that switch or hub
12. Make sure all the stations in the network (including your own computer) have the default address of your internal firewall interface, for example 192.168.0.1
13. Change the ip address of your computer to 192.168.0.100 255.255.255.0
14. Change the ip address in your Internet Explorer to https://192.168.0.1
15. Go to **Systems/Network** again and choose **External** interface
16. Put the static IP address supplied by your internet provider, for example 202.129.97.105 255.255.255.0
17. Go to the **Routing** bookmark under **System/Network** and press **"New"**
18. Add the default route with the ip address supplied by your Internet prover. You create a default router by typing 0.0.0.0 for the destination network and destination network mask.
19. Go back to **System/Network** menu

20. You will get the following configuration:

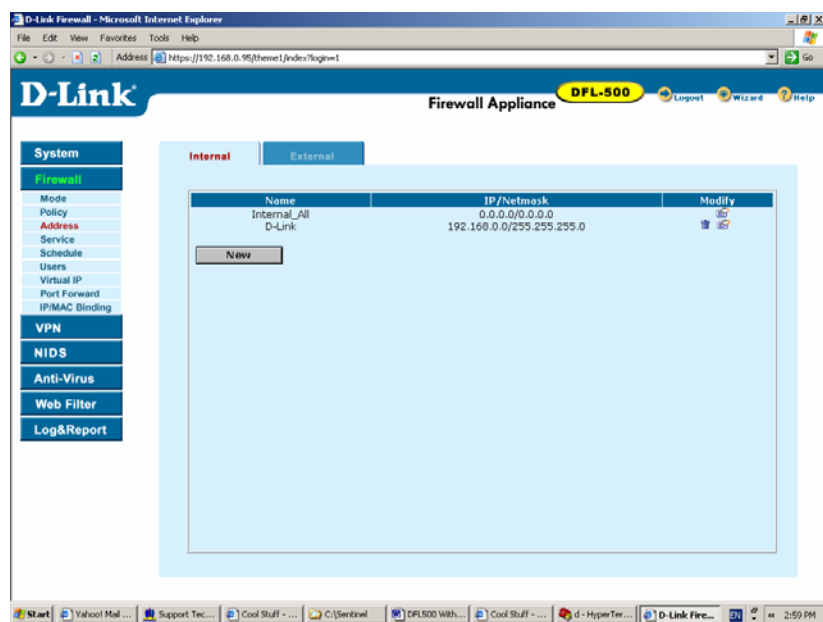


21. Go to **Firewall** menu and choose **Addresses**

22. If your XP/2000 IPsec client has a dynamically assigned IP address, you need to skip steps 23 – 26!

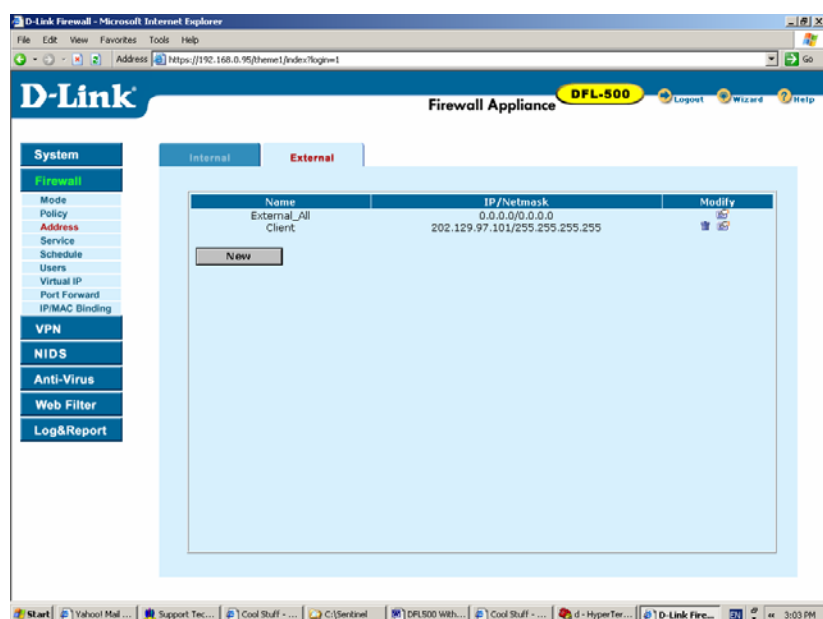
23. In the **Internal** submenu press **"New"**

24. Type the name of your internal network, for example **"D-Link"** and put the ip address of the internal network, for example 192.168.0.0 255.255.255.0. You will see the following screen:



25. Go to **External** submenu and press “**New**”

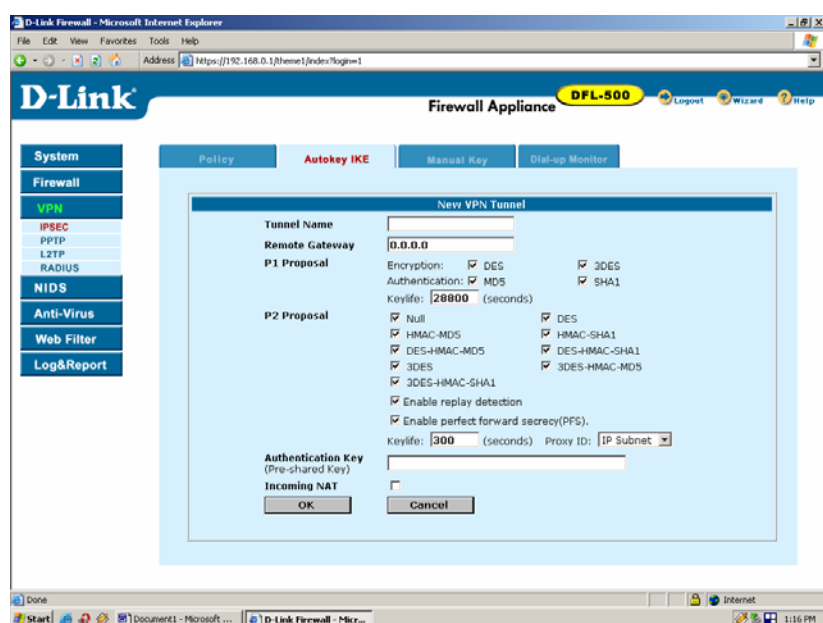
26. Type the name of the VPN client, for example “**Client**” and put the ip address of the client, for example 202.129.97.101 255.255.255.255. You will see the following screen:



27. Go to **VPN** menu and choose **IPSec** submenu

28. Choose **Autokey IKE** bookmark and click “**New**”

29. You will see the following screen:



29. Put in the **Tunnel Name**, for example “**VPN_Client**”

In “**Remote Gateway**” field type the ip address of the client, for example 202.129.97.101.

Type 0.0.0.0, if your XP/2000 IPSec client has a dynamically assigned IP address!

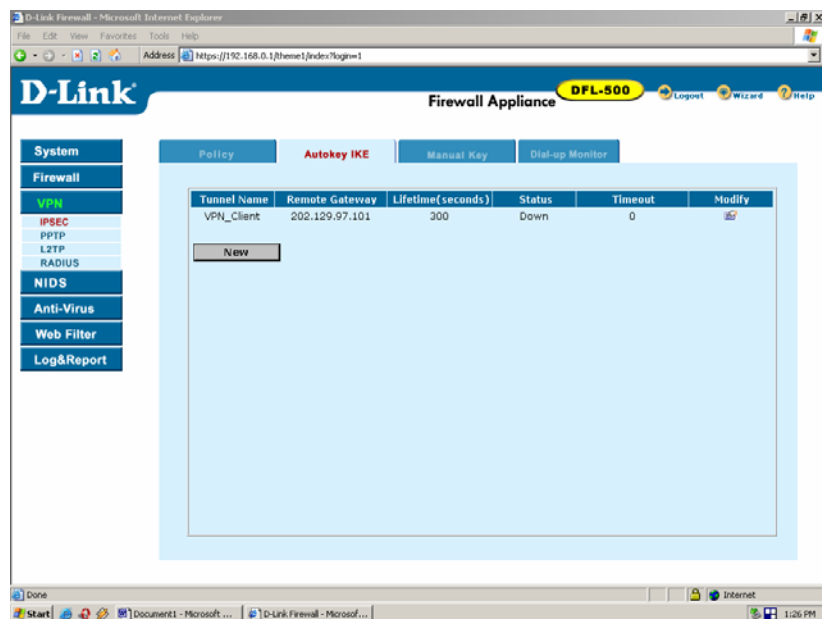
30. Choose the encryption and authentication algorithms you would like to you or leave it as default

31. Put the “**Authentication Key**”, it can be any key, but it is better to use meaningless combination of digits and characters. Don’t forget the key, you will use it later.

32. Check “**Incoming NAT**” and press **OK**

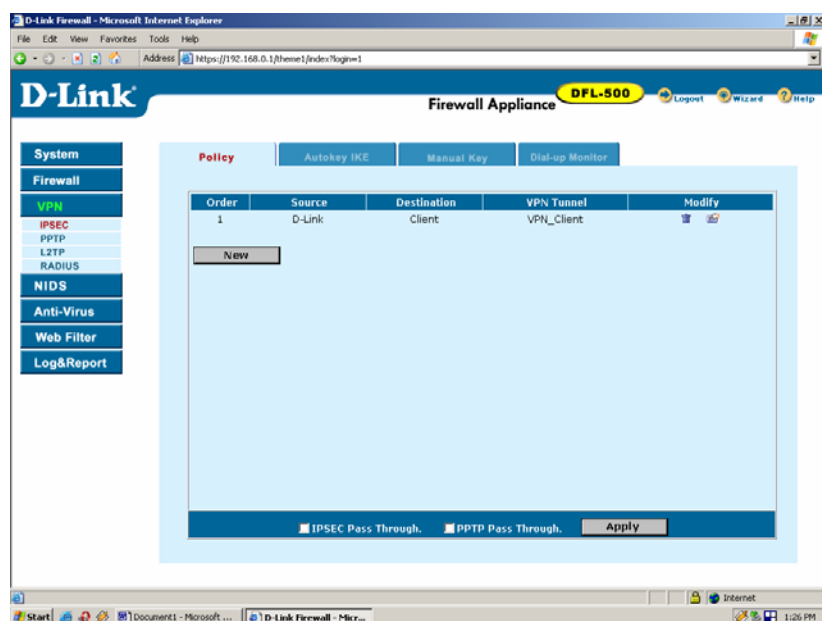
33. If your XP/2000 IPSec client has a dynamically assigned IP address, you need to skip steps 34 – 37!

34. You will get the following screen:



35. Choose “Policy” submenu in VPN/IPSec menu

36. Press “New” and choose “D-Link” for source, “Client” for destination and “VPN_Client” for VPN Tunnel name and press “OK”:



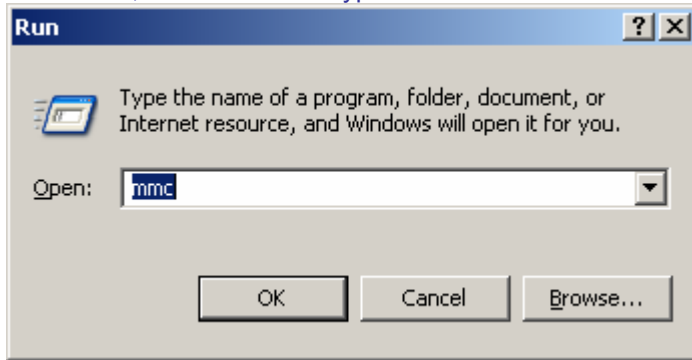
37. The DFL-500 Firewall configuration is finally ready.

II. Configuring Windows XP IPsec Client

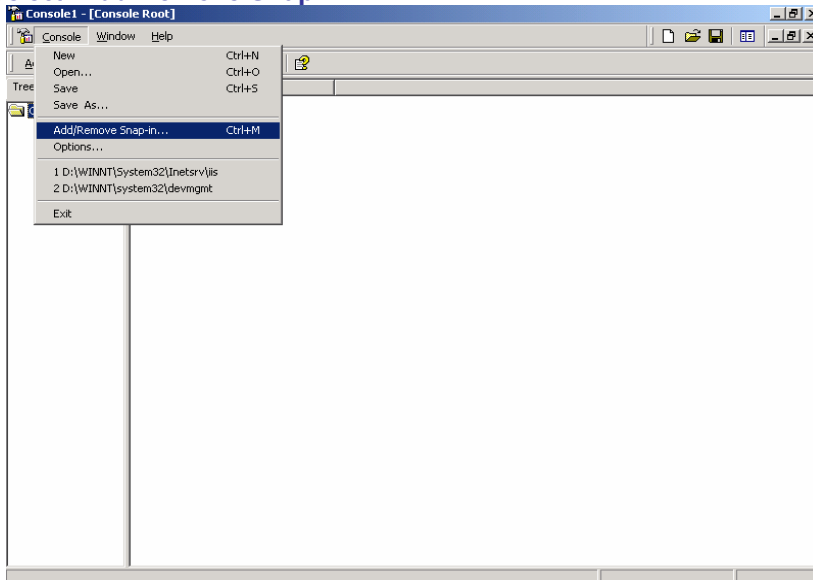
Technical Requirement: Customer is required to understand their network and the Windows XP well for this configuration. Please consult Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences arise from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

The configuration is very similar to the one with DI-804V, that's why you will see DI-804V in screenshot examples. You will have DFL-500 in your setup though.

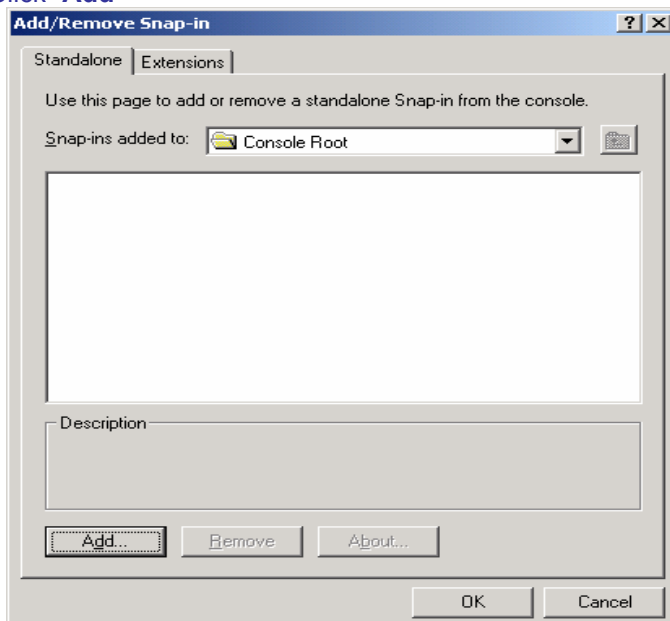
1. Click **"Start"**, then **"Run"** and type **"mmc"**. Click **"OK"**



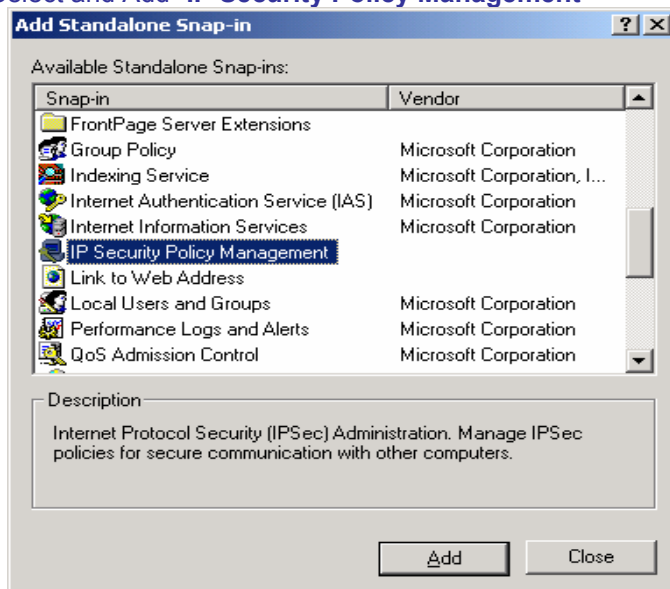
2. Select **"Add/Remove Snap-in"**



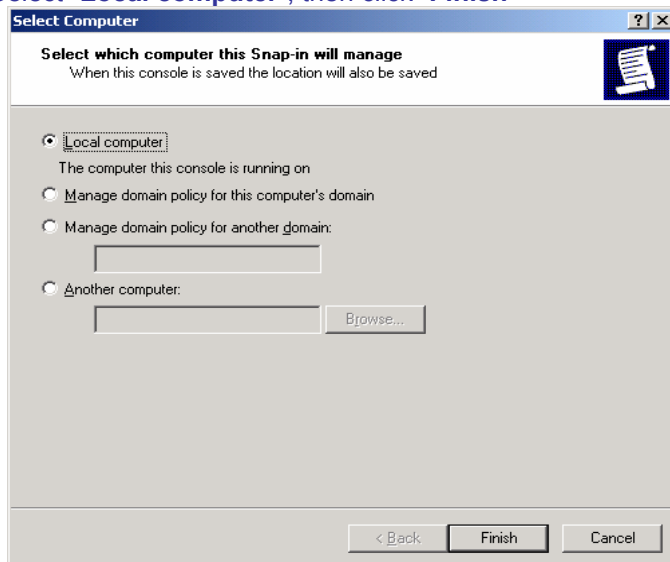
3. Click **"Add"**



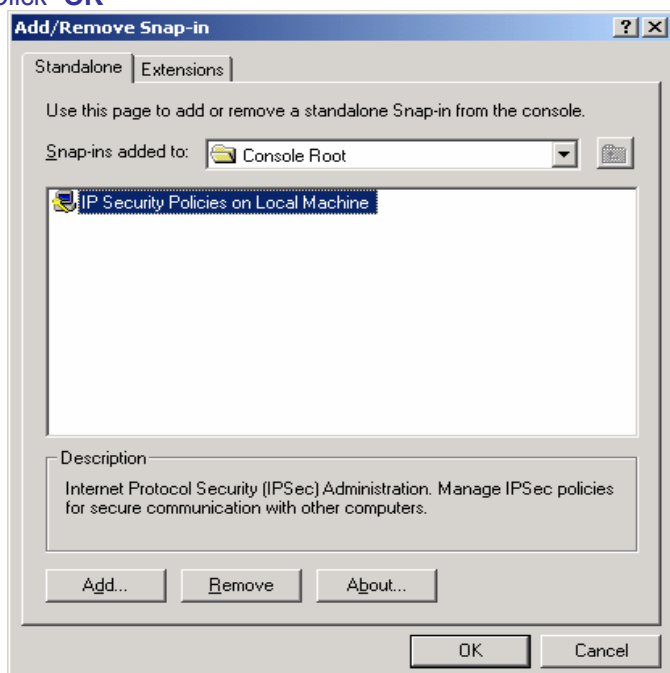
4. Select and Add “IP Security Policy Management”



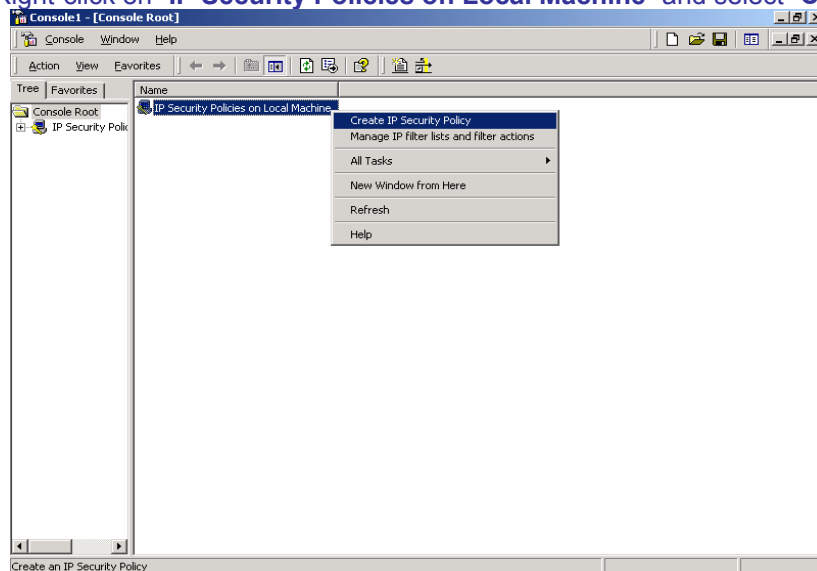
5. Select “Local computer”, then click “Finish”



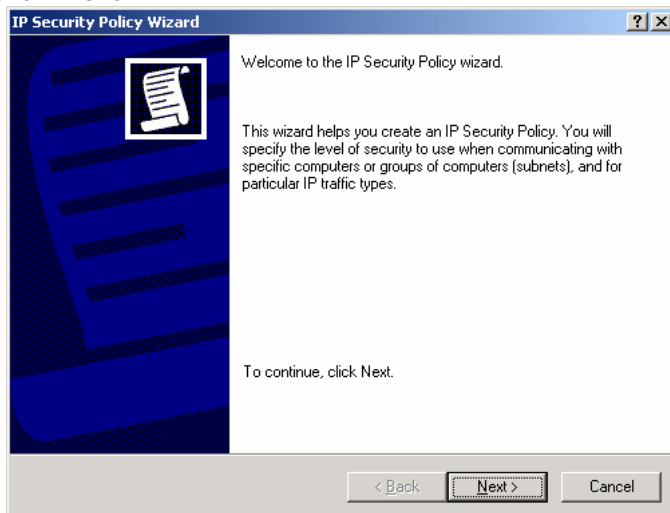
6. Click “OK”



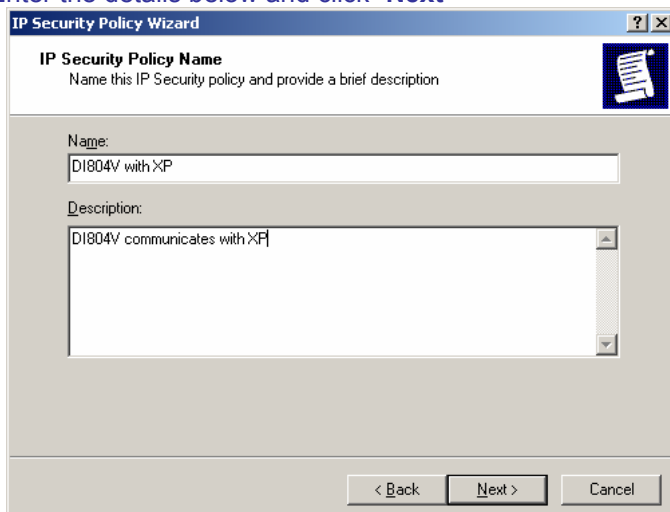
7. Right-click on “IP Security Policies on Local Machine” and select “Create IP Security Policy”



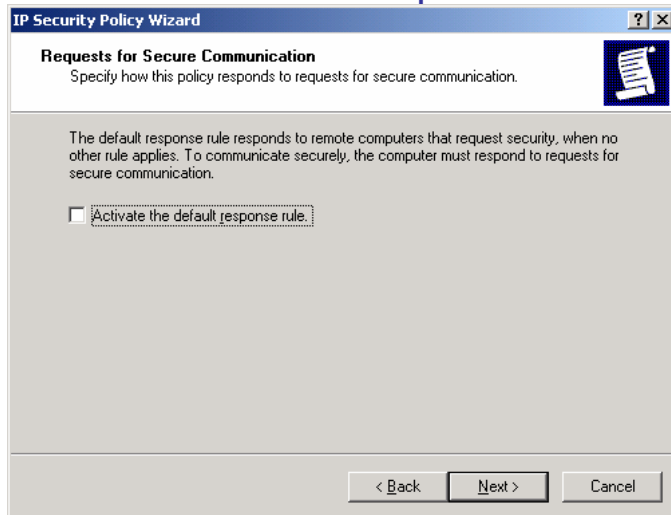
8. Click “Next”



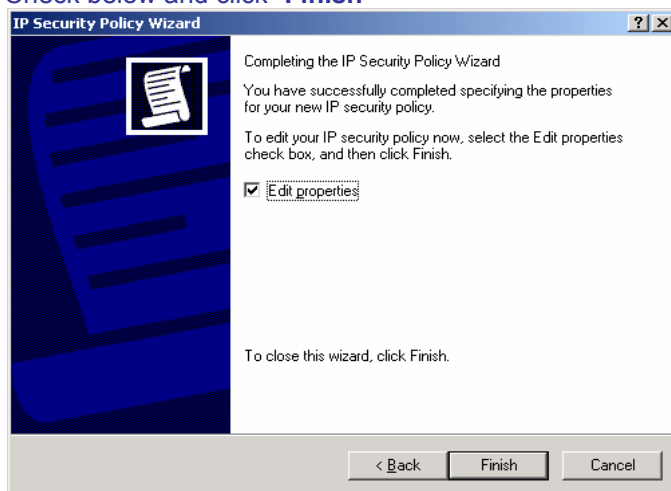
9. Enter the details below and click “Next”



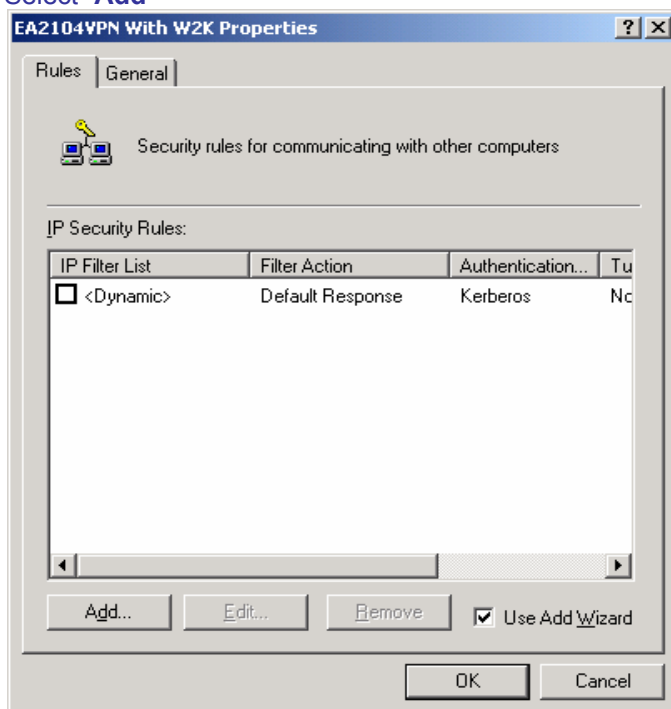
10. Uncheck “**Activate the default response rule**” and click “**Next**”



11. Check below and click “**Finish**”



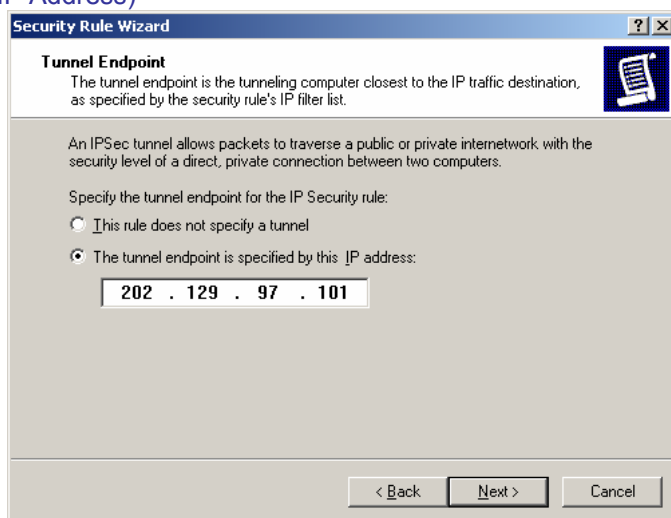
12. Select “**Add**”



13. Click "Next"

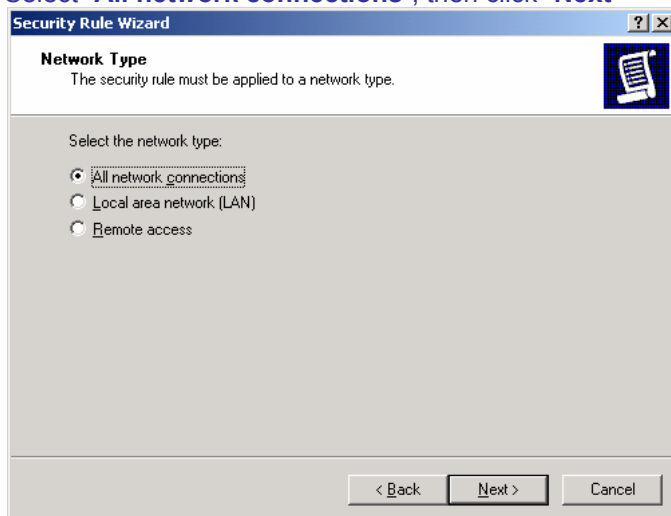


14. Enter the IP Address detail into "The tunnel endpoint specified by this IP address:" (Eg. Windows XP IP Address)*

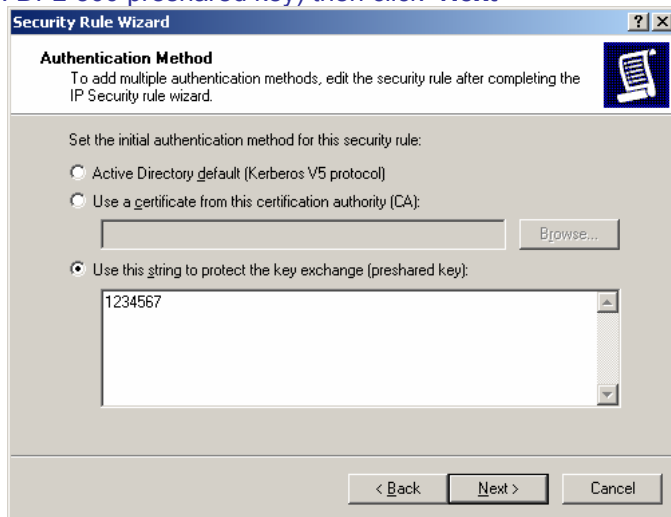


* If your client gets IP address dynamically, put the dynamic IP address here! You will have to change this setting every time you connect to the Internet. Unfortunately, this is the limitation of XP/2000 IPSec client. If your XP/2000 IPSec client is connected to the Internet through the router, use the private IP of your computer, NOT the public IP address of the router!

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



16. Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DFL-500 preshared key) then click “**Next**”



The screenshot shows the 'Authentication Method' step of the Security Rule Wizard. It instructs the user to set the initial authentication method. Three options are available: '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 below it contains the preshared key '1234567'. Navigation buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

Security Rule Wizard

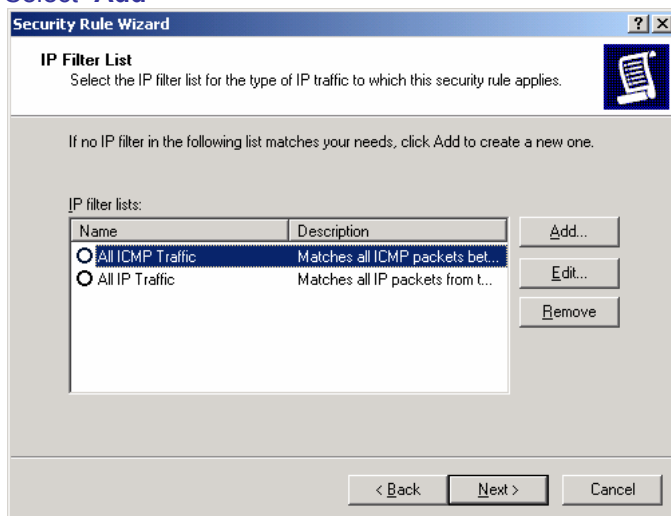
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

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. Select “**Add**”



The screenshot shows the 'IP Filter List' step of the Security Rule Wizard. It asks the user to select an IP filter list for the type of IP traffic to which the security rule applies. A list of IP filter lists is shown with columns 'Name' and 'Description'. Two filters are listed: 'All ICMP Traffic' and 'All IP Traffic'. The 'Add...' button is highlighted. Navigation buttons at the bottom include '< 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.

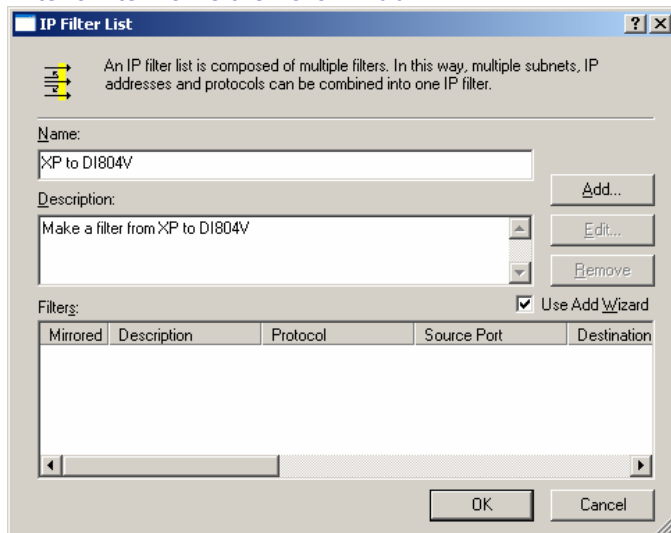
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
☒ All ICMP Traffic	Matches all ICMP packets bet...
☐ All IP Traffic	Matches all IP packets from t...

< Back Next > Cancel

18. Enter a filter name then click “**Add**”



The screenshot shows the 'IP Filter List' dialog box. It explains that an IP filter list is composed of multiple filters. It has fields for 'Name' and 'Description'. The 'Name' field contains 'XP to D1804V' and the 'Description' field contains 'Make a filter from XP to D1804V'. There are 'Add...', 'Edit...', and 'Remove' buttons. Below these is a 'Filters' section with a table that has columns 'Mirrored', 'Description', 'Protocol', 'Source Port', and 'Destination'. The 'Use Add Wizard' checkbox is checked. Navigation buttons at the bottom are 'OK' and 'Cancel'.

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:

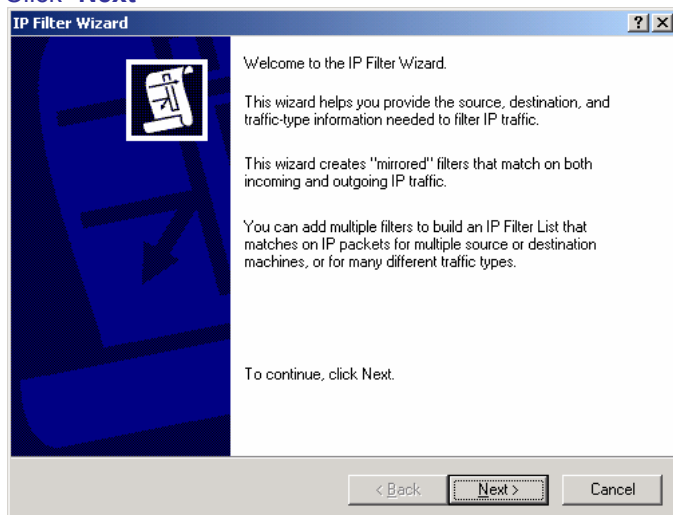
Description:

Filters: ☒ Use Add Wizard

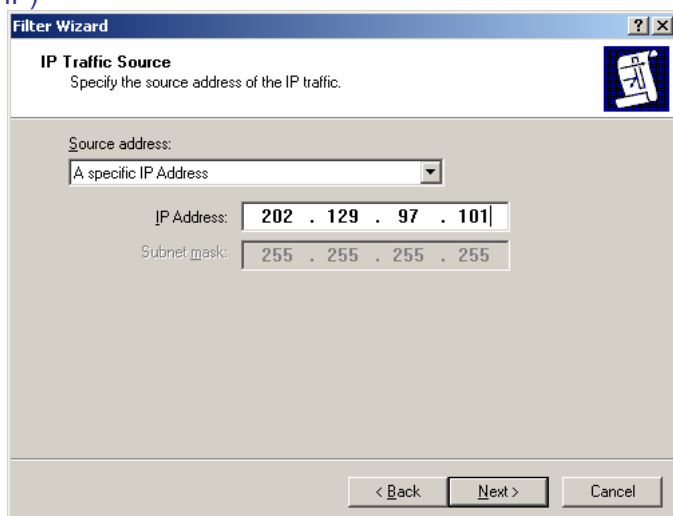
Mirrored	Description	Protocol	Source Port	Destination
----------	-------------	----------	-------------	-------------

OK Cancel

19. Click **“Next”**

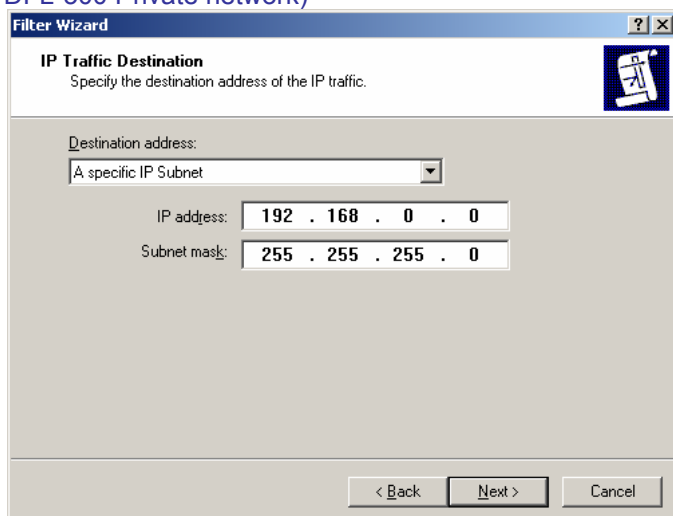


20. Select **“A specific IP Address”** and input the Source address, then **“Next”** to continue (Eg. Windows XP IP) *

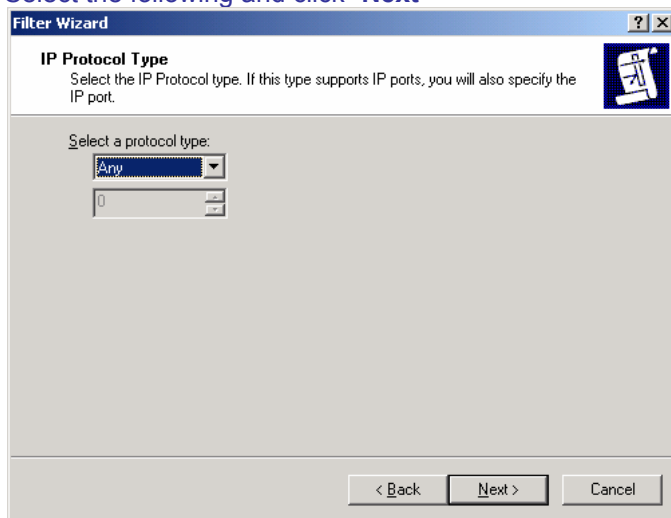


* If your client gets IP address dynamically choose **“My IP address”**.

21. Select **“A specific IP Subnet”** and input the Destination subnet address, then **“Next”** to continue (Eg. DFL-500 Private network)



22. Select the following and click “Next”



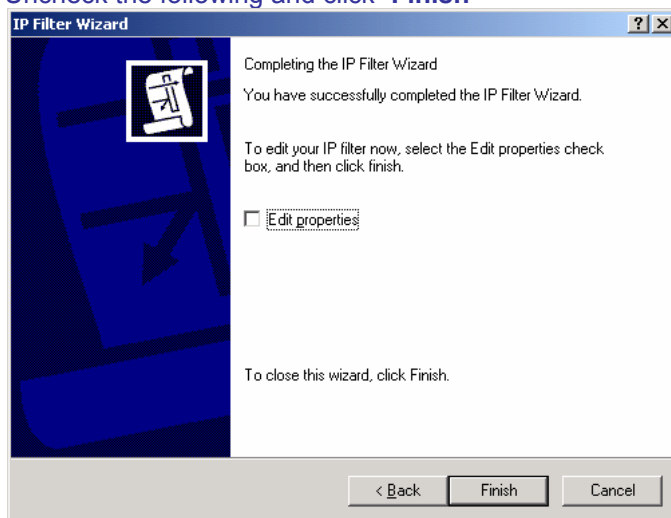
Filter Wizard

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”



IP Filter Wizard

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

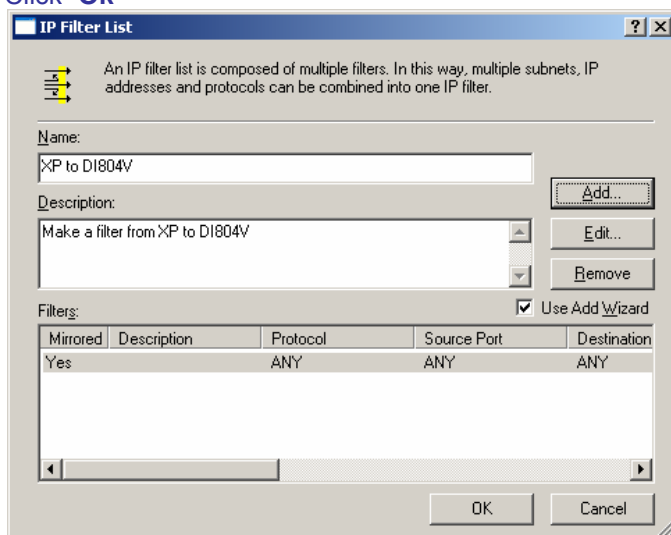
To edit your IP filter now, select the Edit properties check box, and then click finish.

☐ Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

24. Click “OK”



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:
XP to D1804V

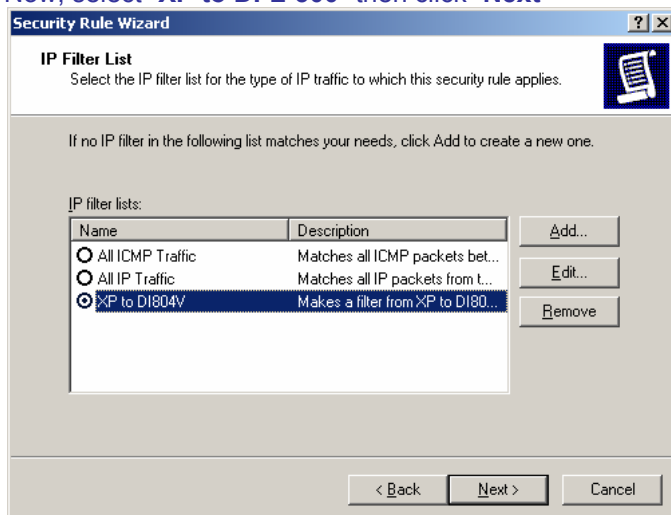
Description:
Make a filter from XP to D1804V

Filters:
☒ Use Add Wizard

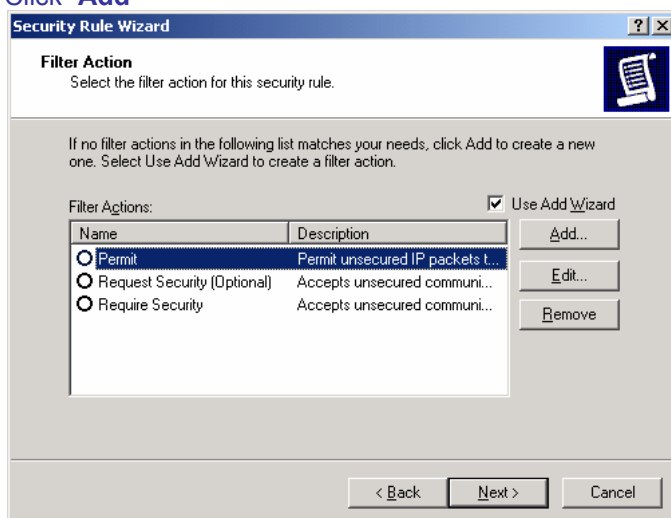
Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

OK Cancel

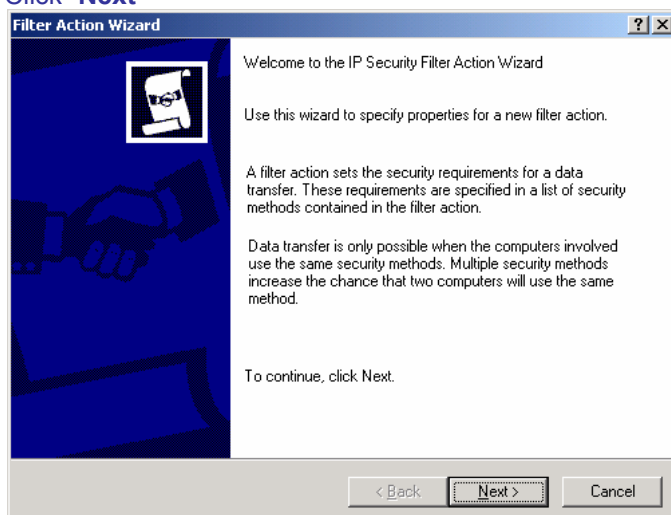
25. Now, select “XP to DFL-500” then click “Next”



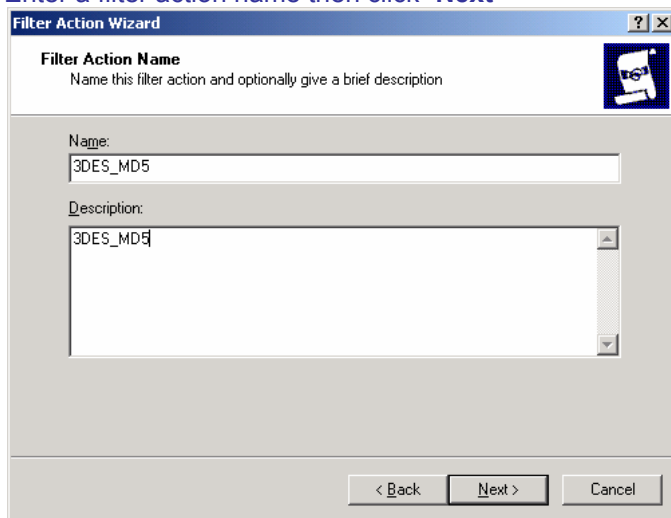
26. Click “Add”



27. Click “Next”

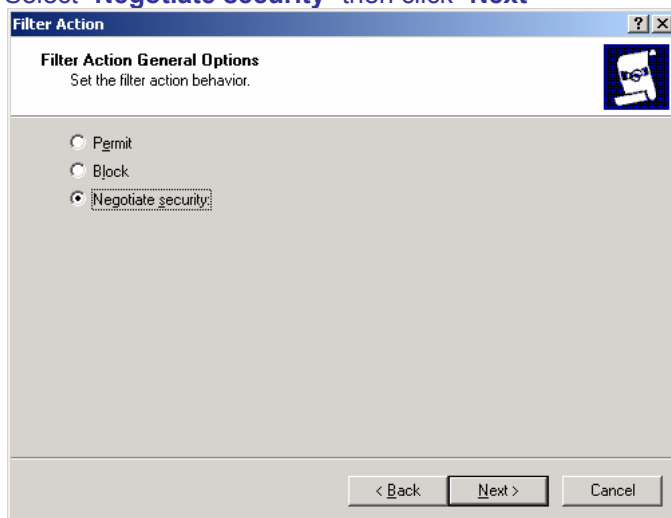


28. Enter a filter action name then click “Next”



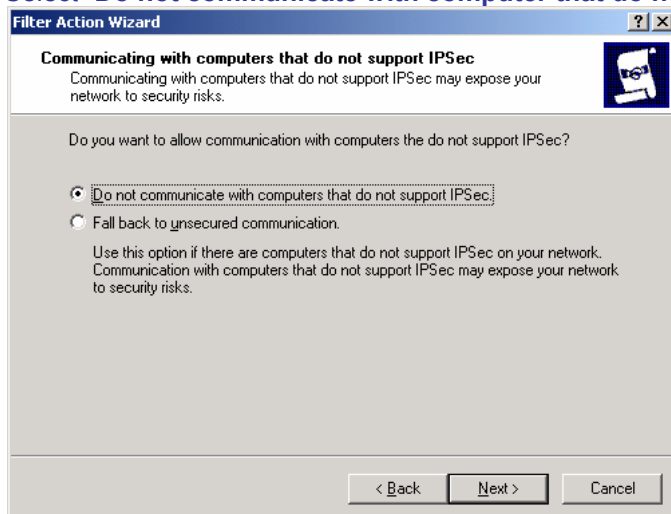
The 'Filter Action Wizard' dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled 'Filter Action Name' with the instruction 'Name this filter action and optionally give a brief description'. There are two text input fields: 'Name:' containing '3DES_MD5' and 'Description:' containing '3DES_MD5'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

29. Select “Negotiate security” then click “Next”



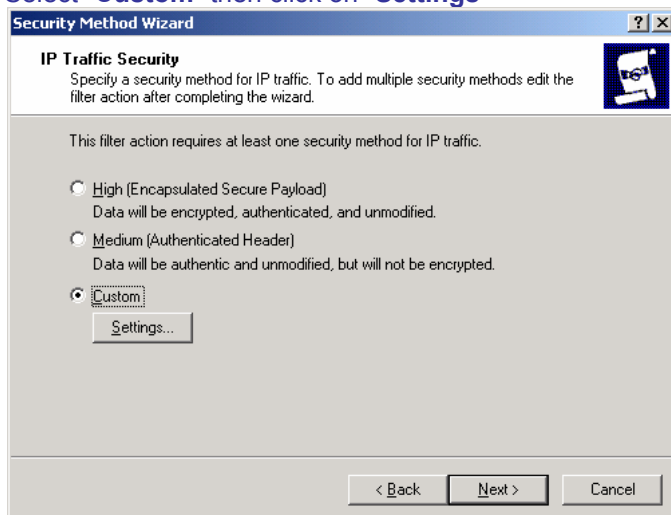
The 'Filter Action General Options' dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled 'Filter Action General Options' with the instruction 'Set the filter action behavior.'. There are three radio buttons: 'Permit', 'Block', and 'Negotiate security'. The 'Negotiate security' option is selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

30. Select “Do not communicate with computer that do not support IPSec” then click “Next”

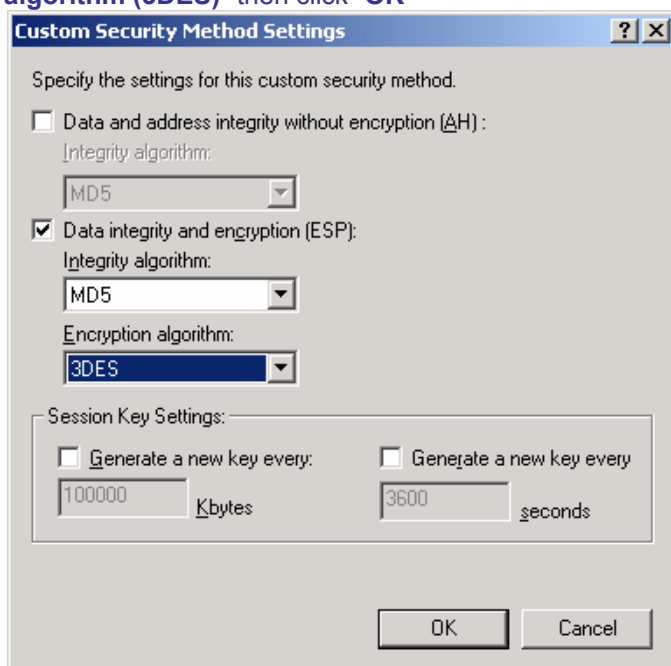


The 'Filter Action Wizard' dialog box is shown. It has a title bar with a question mark and a close button. The main area is titled 'Communicating with computers that do not support IPSec' with the instruction 'Communicating with computers that do not support IPSec may expose your network to security risks.'. Below this, it asks 'Do you want to allow communication with computers the do not support IPSec?'. There are two radio buttons: 'Do not communicate with computers that do not support IPSec.' (selected) and 'Fall back to unsecured communication.'. Below the second option, it says 'Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

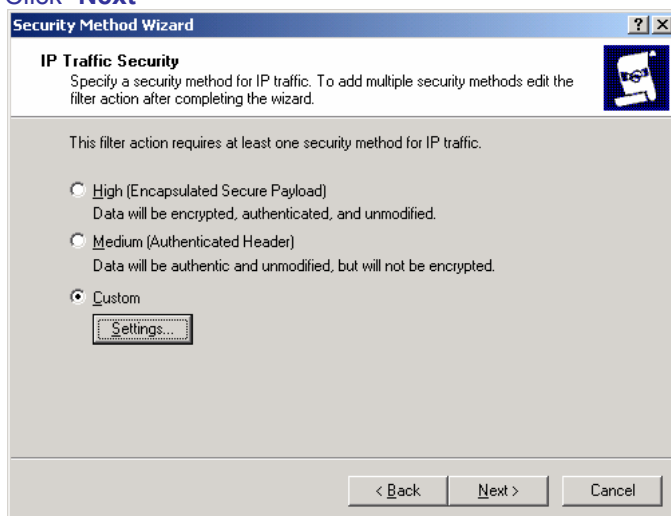
31. Select **Custom** then click on **Settings**



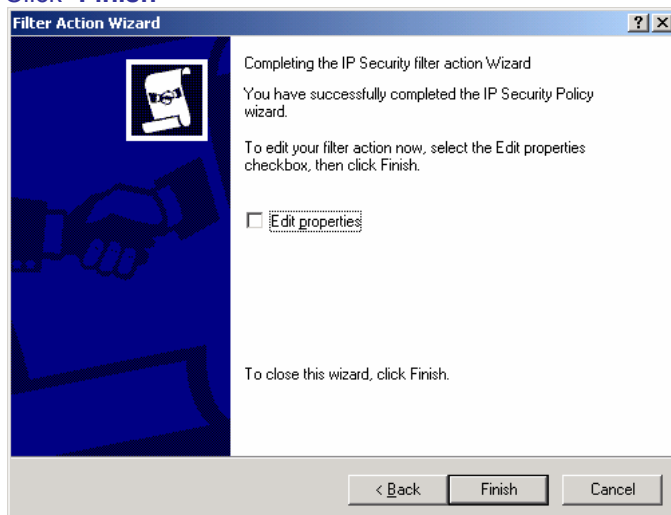
32. Check **Data integrity and encryption (ESP)**, select the **Integrity algorithm (MD5)** and **Encryption algorithm (3DES)** then click **OK**



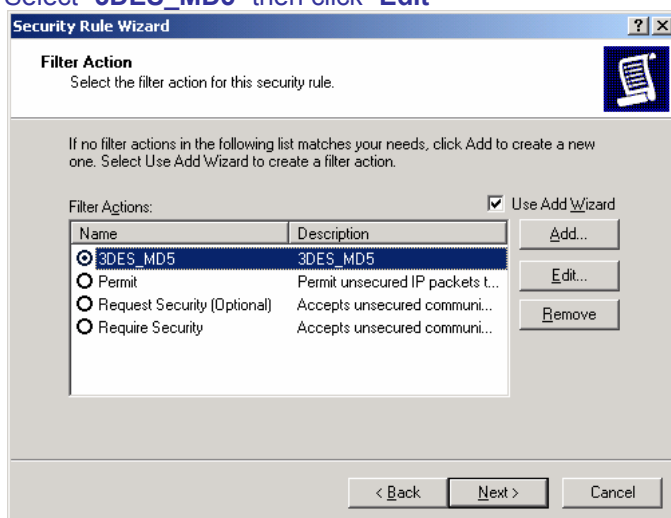
33. Click **Next**



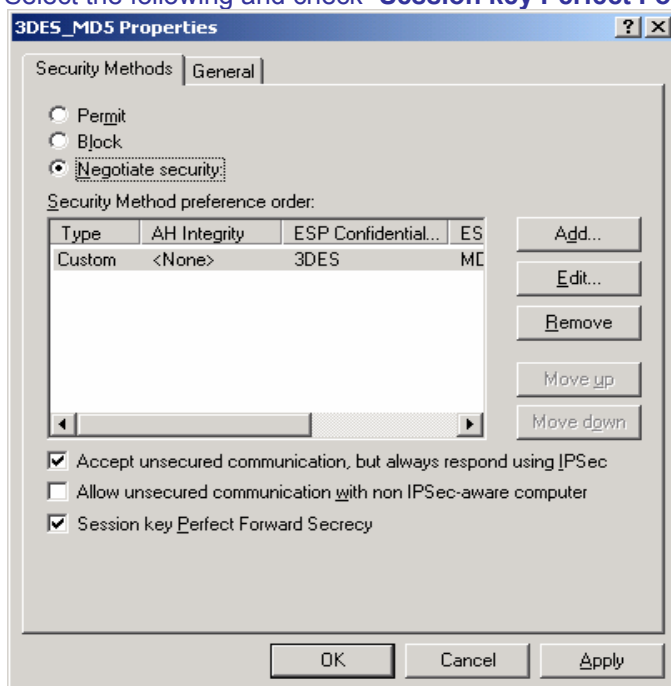
34. Click **“Finish”**



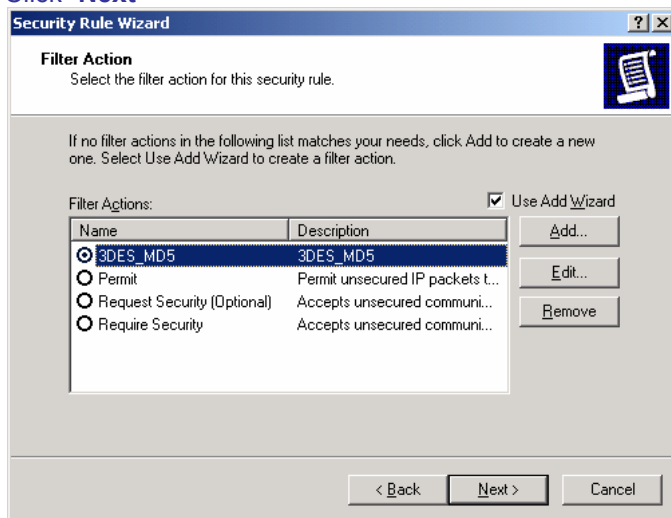
35. Select **“3DES_MD5”** then click **“Edit”**



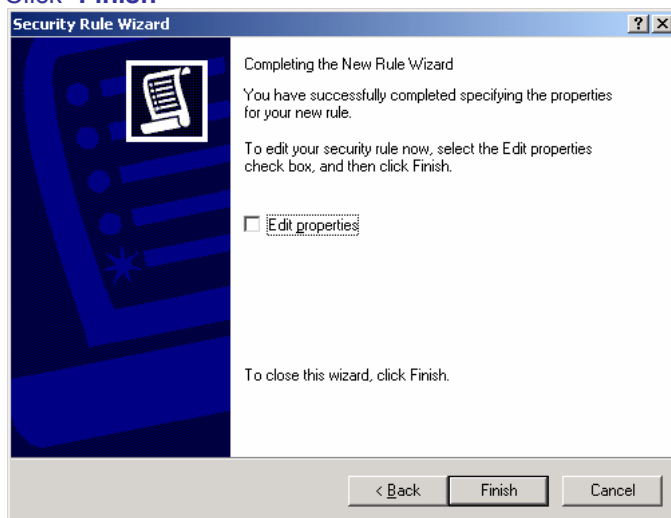
36. Select the following and check **“Session key Perfect Forward Secrecy”** then click **“OK”**



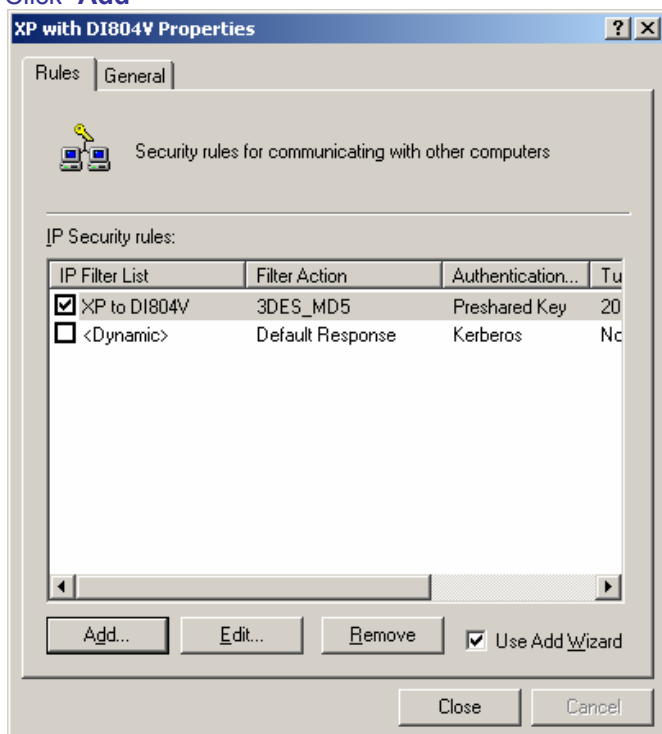
37. Click “Next”



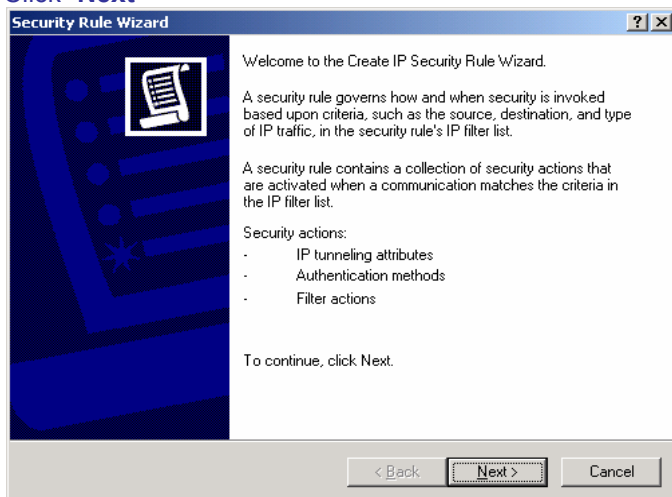
38. Click “Finish”



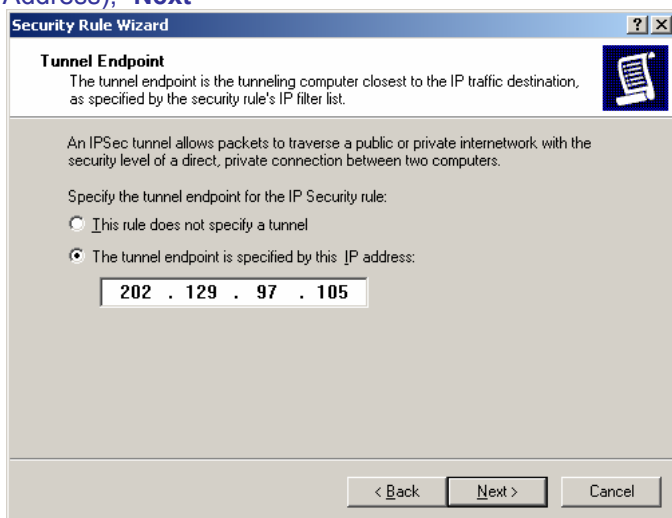
39. Click “Add”



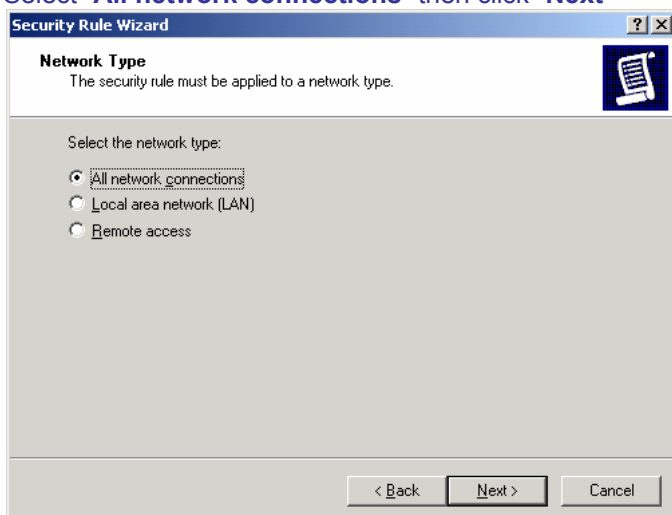
40. Click **“Next”**



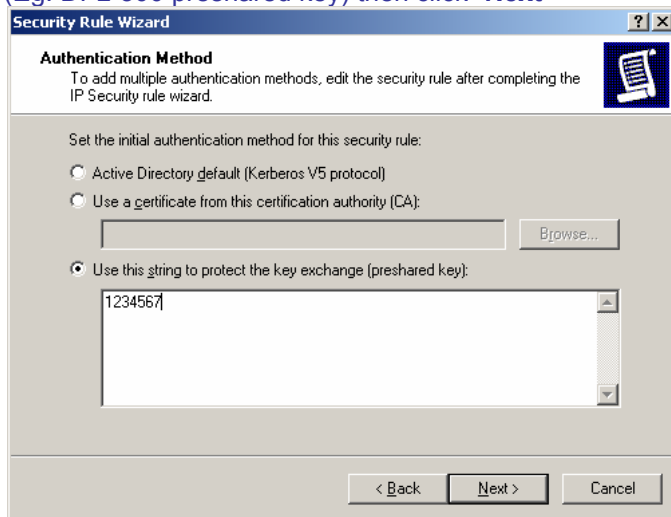
41. Input the IP Address into **“The tunnel endpoint specified by this IP address:”** (Eg. DFL-500 WAN IP Address), **“Next”**



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



43. Select “Use this string to protect the key exchange (preshared key)” (Eg. DFL-500 preshared key) then click “Next”



The screenshot shows the 'Authentication Method' step of the Security Rule Wizard. It instructs the user to set the initial authentication method. Three options are available: 'Active Directory default (Kerberos V5 protocol)', 'Use a certificate from this certification authority (CA):' (with a 'Browse...' button), and 'Use this string to protect the key exchange (preshared key):'. The third option is selected, and a text box contains the string '1234567'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Security Rule Wizard

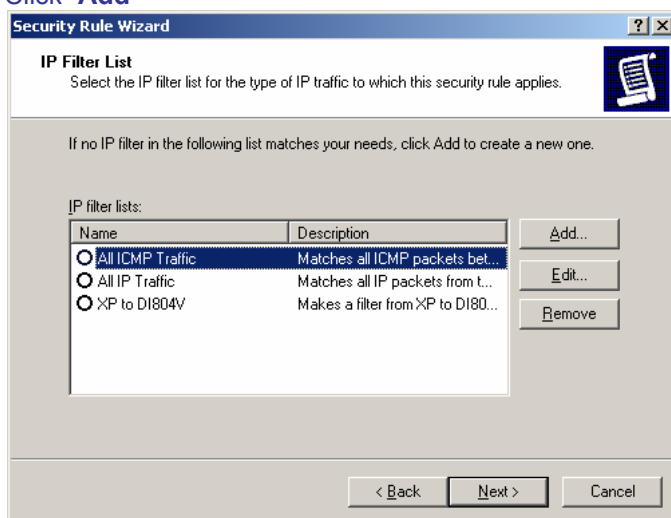
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

- ☐ Active Directory default (Kerberos V5 protocol)
- ☐ Use a certificate from this certification authority (CA):
Browse...
- ☒ Use this string to protect the key exchange (preshared key):
1234567

< Back Next > Cancel

44. Click “Add”



The screenshot shows the 'IP Filter List' step of the Security Rule Wizard. It asks the user to select an IP filter list for the type of IP traffic to which the security rule applies. A list of IP filter lists is shown with columns 'Name' and 'Description'. The first item, 'All ICMP Traffic', is selected. To the right of the list are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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.

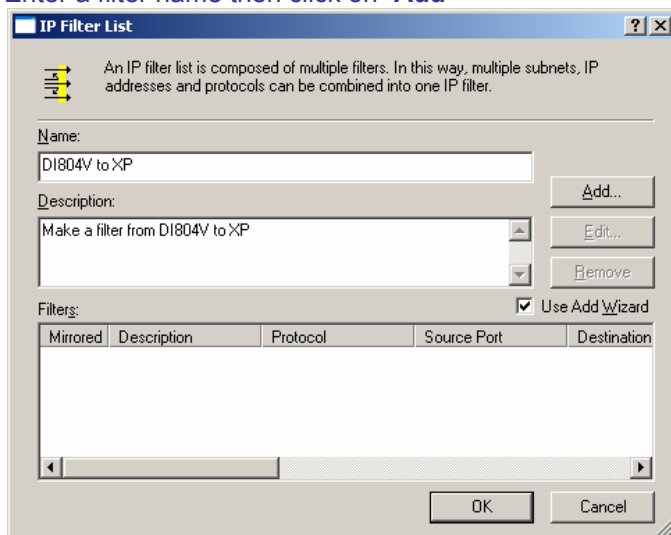
IP filter lists:

Name	Description
☒ All ICMP Traffic	Matches all ICMP packets bet...
☐ All IP Traffic	Matches all IP packets from t...
☐ XP to D1804V	Makes a filter from XP to D180...

Add... Edit... Remove

< Back Next > Cancel

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



The screenshot shows the 'IP Filter List' dialog box. It explains that an IP filter list is composed of multiple filters. It has fields for 'Name' (containing 'D1804V to XP') and 'Description' (containing 'Make a filter from D1804V to XP'). To the right are 'Add...', 'Edit...', and 'Remove' buttons. Below these is a 'Filters:' section with a checked 'Use Add Wizard' checkbox and a table with columns 'Mirrored', 'Description', 'Protocol', 'Source Port', and 'Destination'. 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 XP

Description:
Make a filter from D1804V to XP

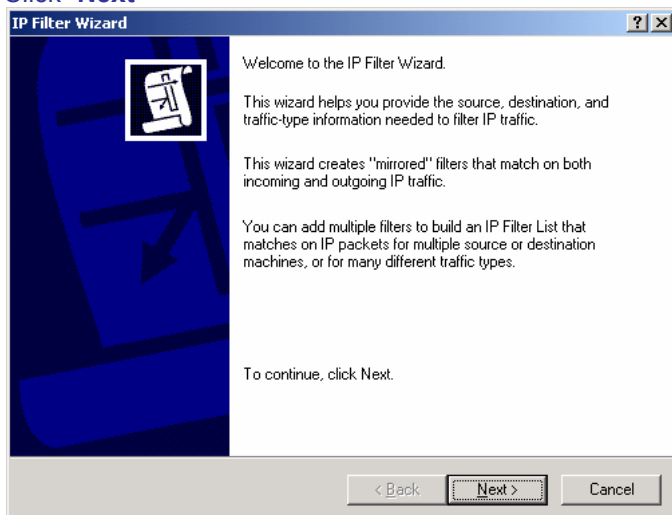
Add... Edit... Remove

Filters: ☒ Use Add Wizard

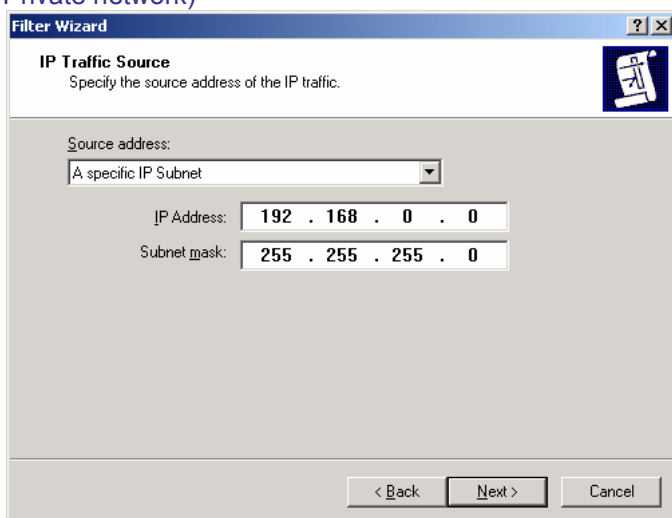
Mirrored	Description	Protocol	Source Port	Destination
----------	-------------	----------	-------------	-------------

OK Cancel

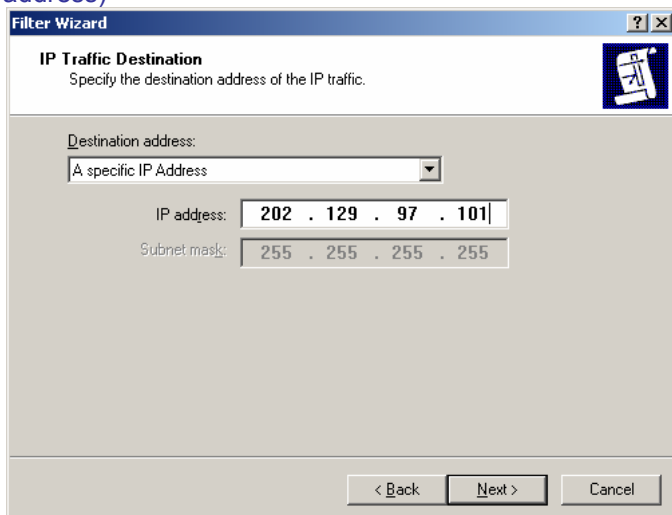
46. Click “Next”



47. Select “A specific IP Subnet” and input the Source subnet address then click “Next” (Eg. DFL-500 Private network)

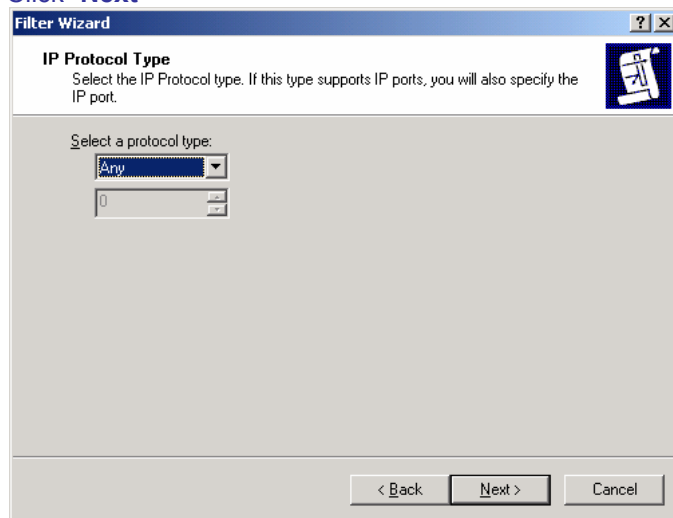


48. Select “A specific IP Address” and input the Destination address then click “Next” (Eg. Windows XP IP address)*



* If your client gets IP address dynamically choose “My IP Address”.

49. Click “Next”



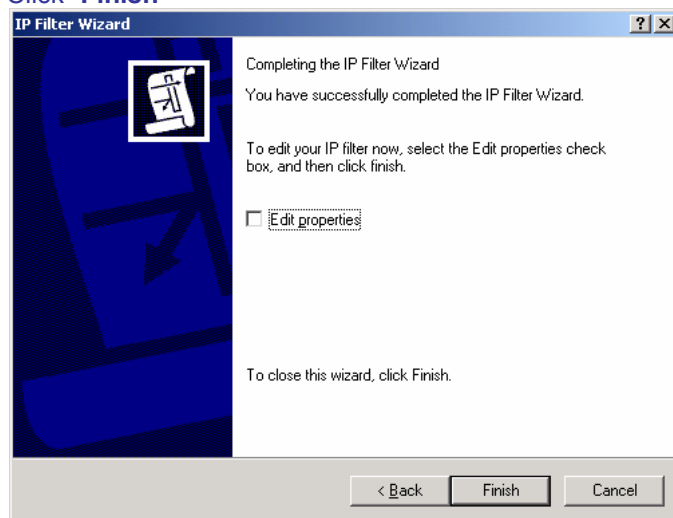
Filter Wizard

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”



IP Filter Wizard

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

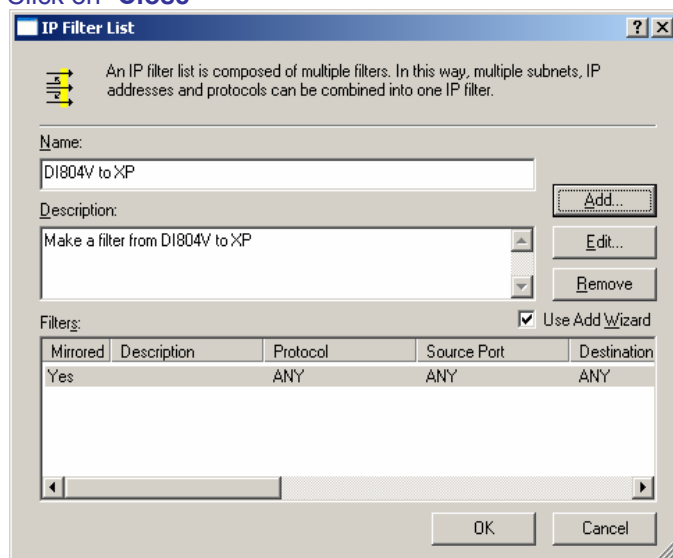
To edit your IP filter now, select the Edit properties check box, and then click finish.

☐ Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

51. Click on “Close”



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:
DI804V to XP

Description:
Make a filter from DI804V to XP

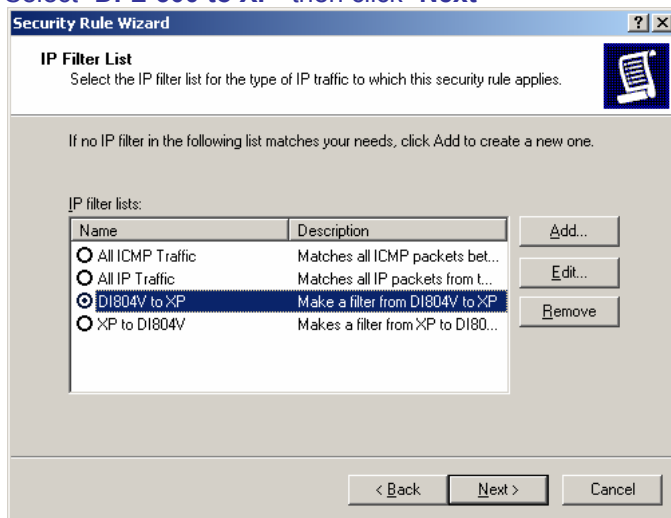
Add... Edit... Remove

Filters: ☒ Use Add Wizard

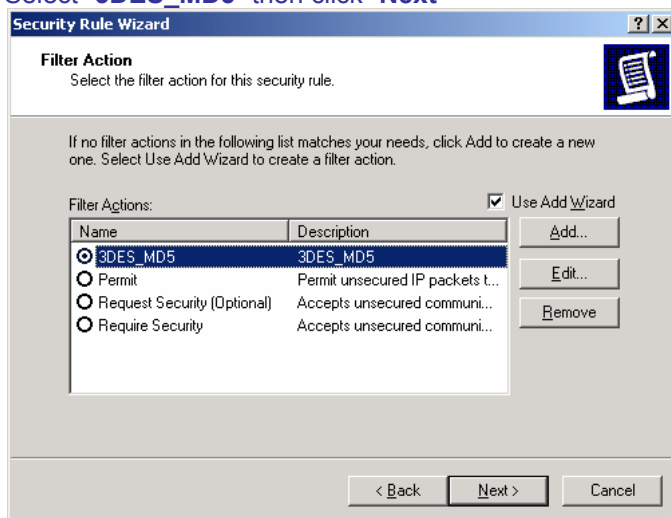
Mirrored	Description	Protocol	Source Port	Destination
Yes		ANY	ANY	ANY

OK Cancel

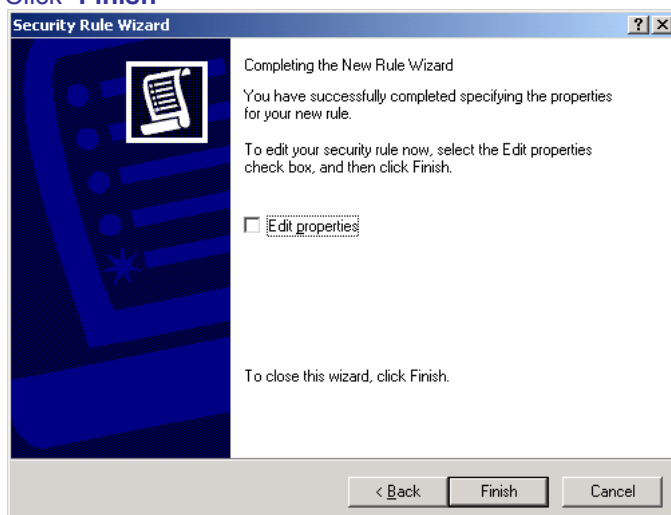
52. Select “DFL-500 to XP” then click “Next”



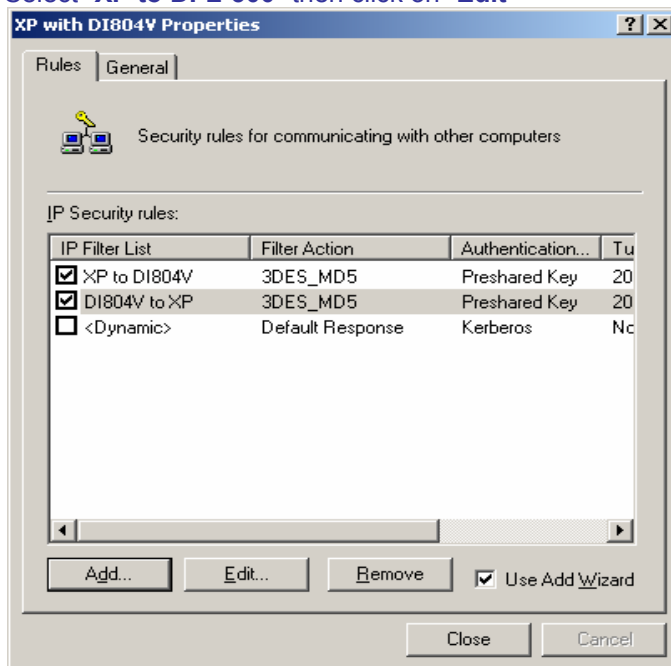
53. Select “3DES_MD5” then click “Next”



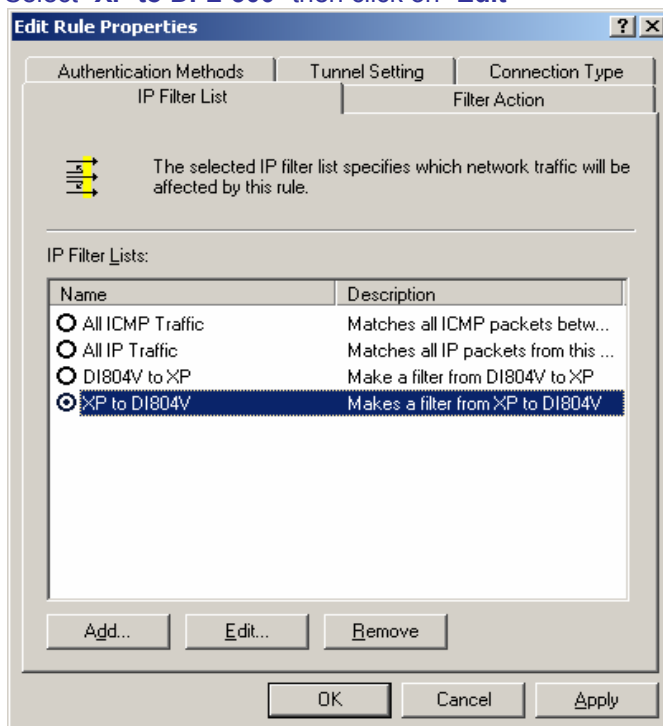
54. Click “Finish”



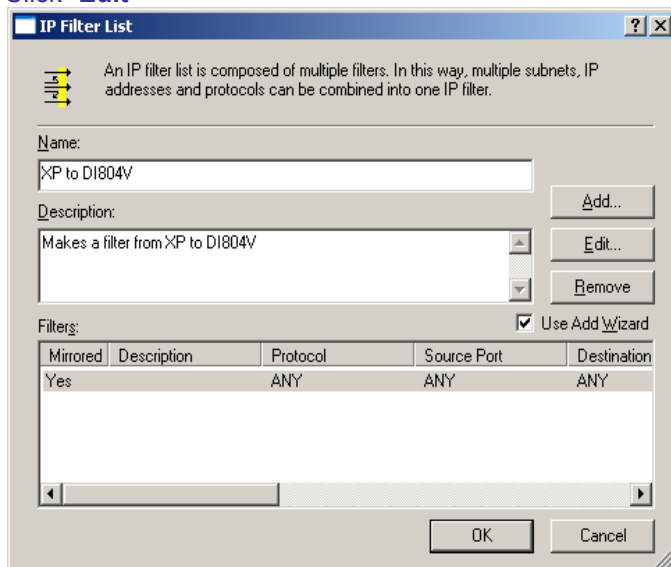
55. Select **"XP to DFL-500"** then click on **"Edit"**



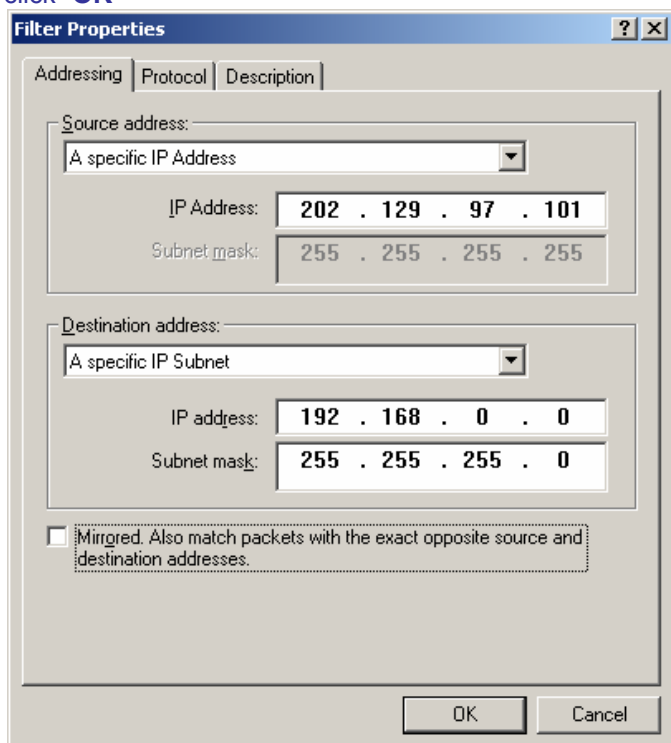
56. Select **"XP to DFL-500"** then click on **"Edit"**



57. Click **Edit**

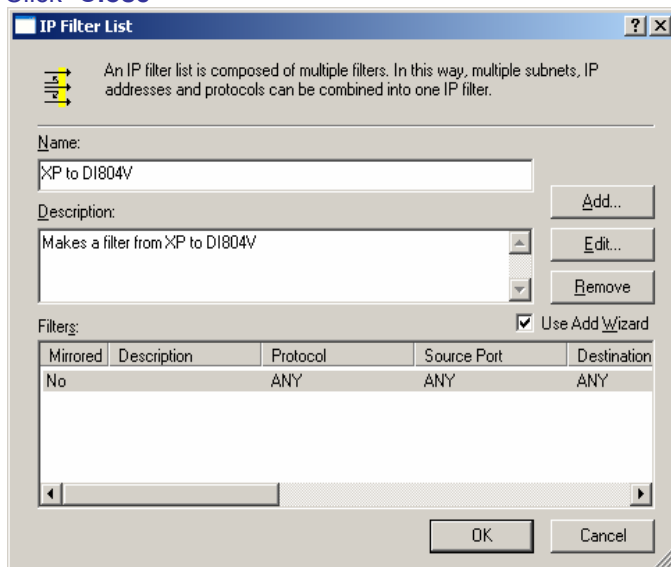


58. Uncheck **Mirrored. Also match packets with exact opposite source and destination address** then click **OK** *

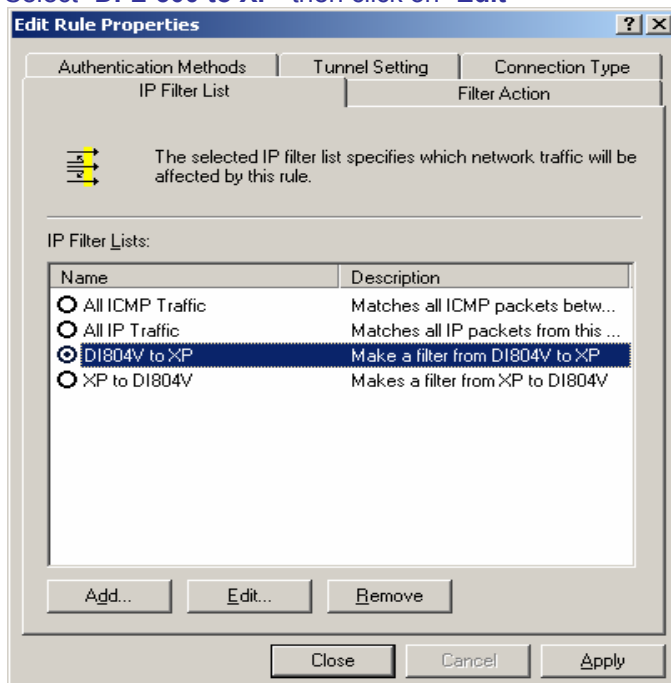


* If your client gets IP address dynamically you will see "My IP Address" in Source address field.

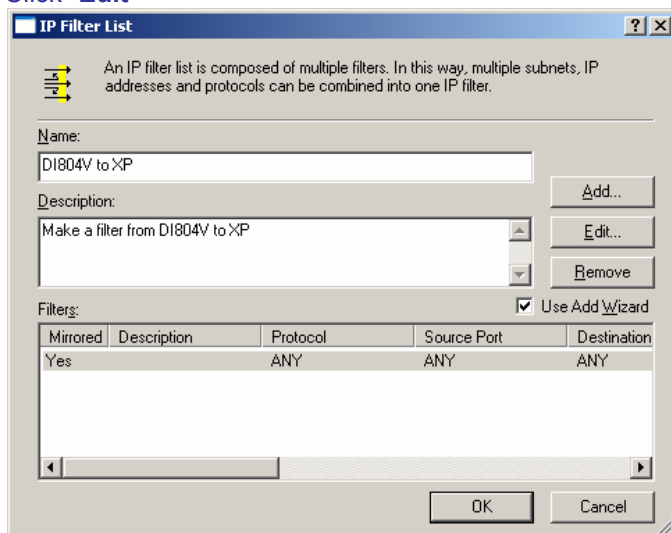
59. Click **“Close”**



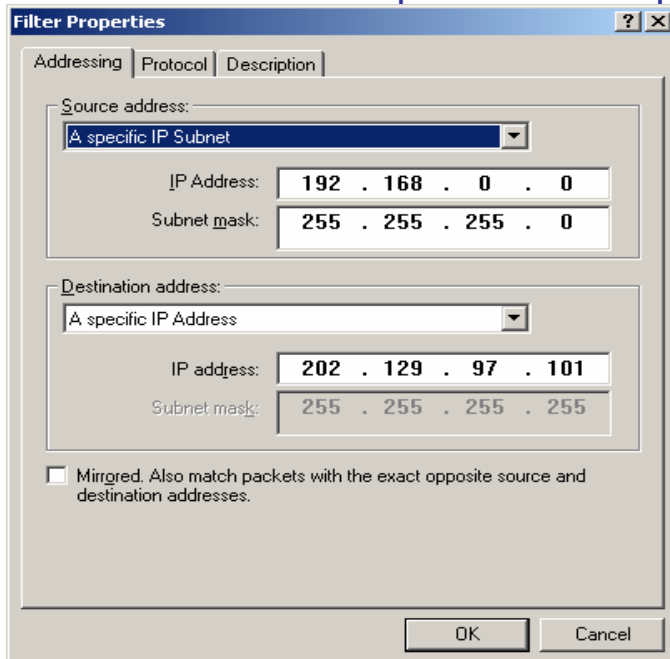
60. Select **“DFL-500 to XP”** then click on **“Edit”**



61. Click **“Edit”**



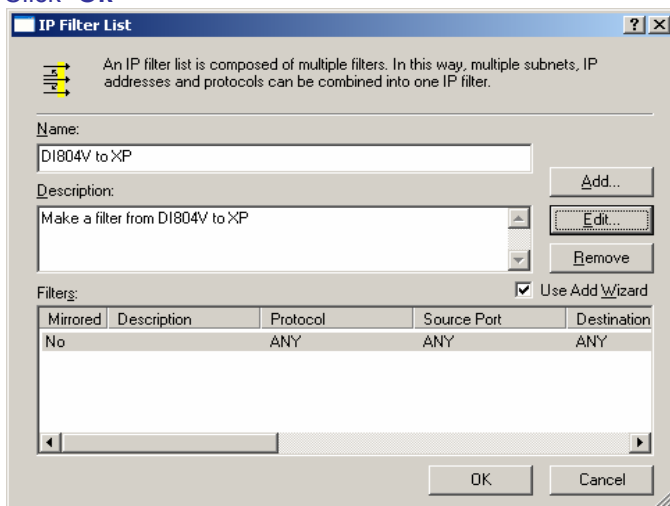
62. Uncheck “Mirrored. Also match packets with exact opposite source...” then click “OK” *



The **Filter Properties** dialog box has three tabs: **Addressing**, **Protocol**, and **Description**. The **Addressing** tab is active. It contains two sections: **Source address:** and **Destination address:**. Each section has a dropdown menu (currently showing "A specific IP Subnet" and "A specific IP Address" respectively) and two input fields for **IP Address** and **Subnet mask**. The source IP is 192.168.0.0 and the source mask is 255.255.255.0. The destination IP is 202.129.97.101 and the destination mask is 255.255.255.255. At the bottom, there is an unchecked checkbox labeled "Mirrored. Also match packets with the exact opposite source and destination addresses." and **OK** and **Cancel** buttons.

* If your client gets IP address dynamically you will see “My IP Address” in Destination address field.

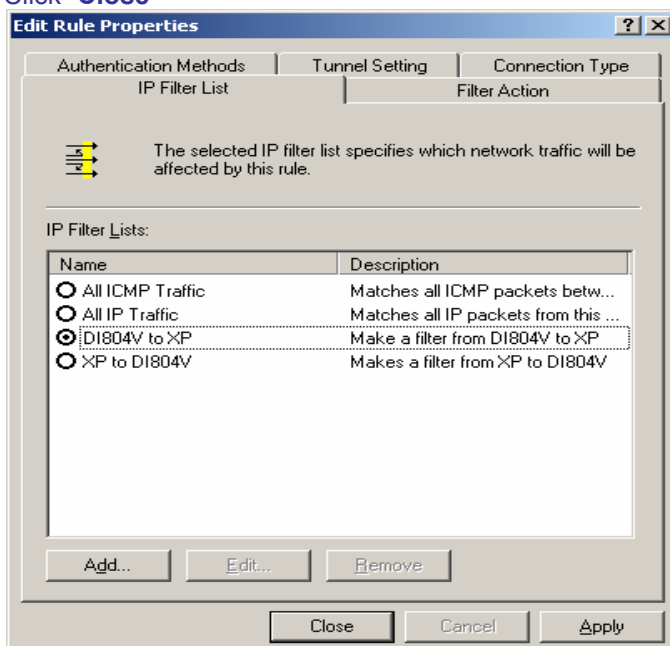
63. Click “OK”



The **IP Filter List** dialog box contains a text area for **Name** (DI804V to XP) and a text area for **Description** (Make a filter from DI804V to XP). There are **Add...**, **Edit...**, and **Remove** buttons. Below is a **Filters:** table with columns: **Mirrored**, **Description**, **Protocol**, **Source Port**, and **Destination**. The table has one row with values: No, ANY, ANY, ANY. A **Use Add Wizard** checkbox is checked. **OK** and **Cancel** buttons are at the bottom.

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

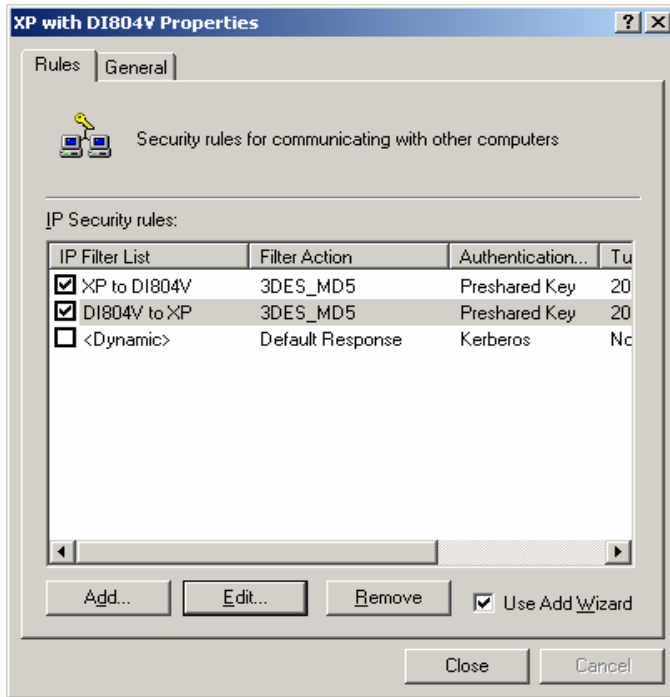
64. Click “Close”



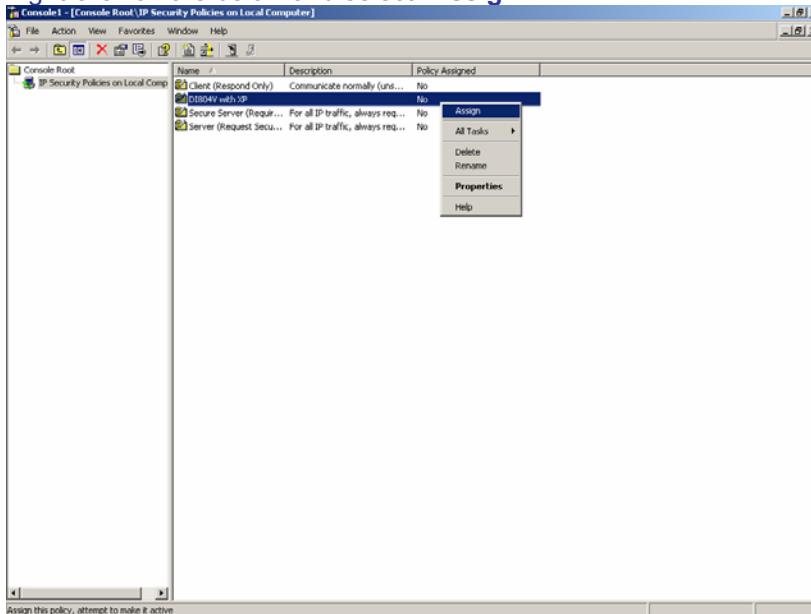
The **Edit Rule Properties** dialog box has tabs for **Authentication Methods**, **Tunnel Setting**, and **Connection Type**. The **Connection Type** tab is active, showing **IP Filter List** and **Filter Action**. It contains a list of **IP Filter Lists** with columns **Name** and **Description**. The list includes: **All ICMP Traffic** (Matches all ICMP packets between...), **All IP Traffic** (Matches all IP packets from this ...), **DI804V to XP** (Make a filter from DI804V to XP), and **XP to DI804V** (Makes a filter from XP to DI804V). The **DI804V to XP** filter is selected. There are **Add...**, **Edit...**, and **Remove** buttons. At the bottom are **Close**, **Cancel**, and **Apply** buttons.

Name	Description
All ICMP Traffic	Matches all ICMP packets between...
All IP Traffic	Matches all IP packets from this ...
DI804V to XP	Make a filter from DI804V to XP
XP to DI804V	Makes a filter from XP to DI804V

65. Click “Close”



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



67. On XP/2000 IPsec client machine do a **PING** to a valid machine (which HAS the default gateway pointing to DFL-500 internal IP address and NO anti-virus or ANY other blocking software installed) on the Remote private network in the Dos Command Prompt: “ping 192.168.0.101 -t”

