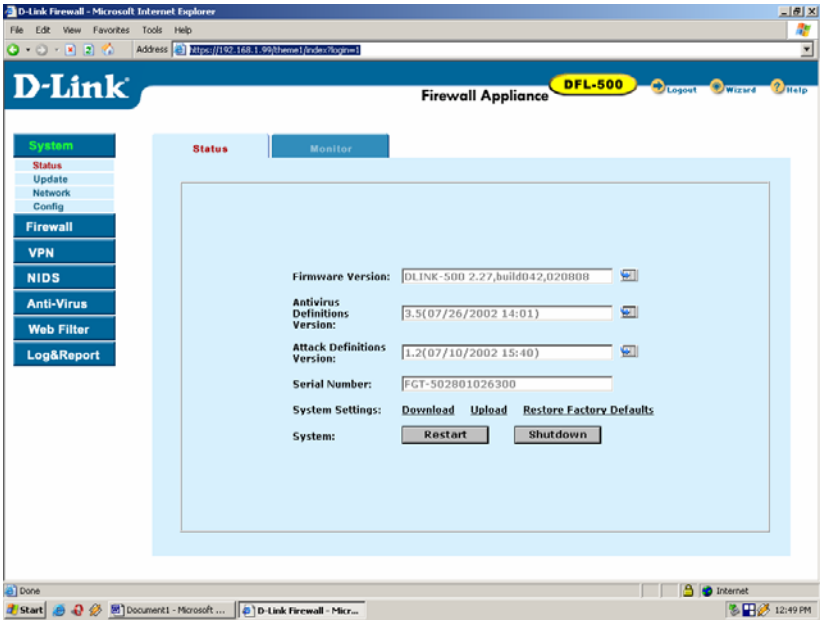
DFL-500 With Windows XP/2000 IPSec VPN Client Configuration Guide

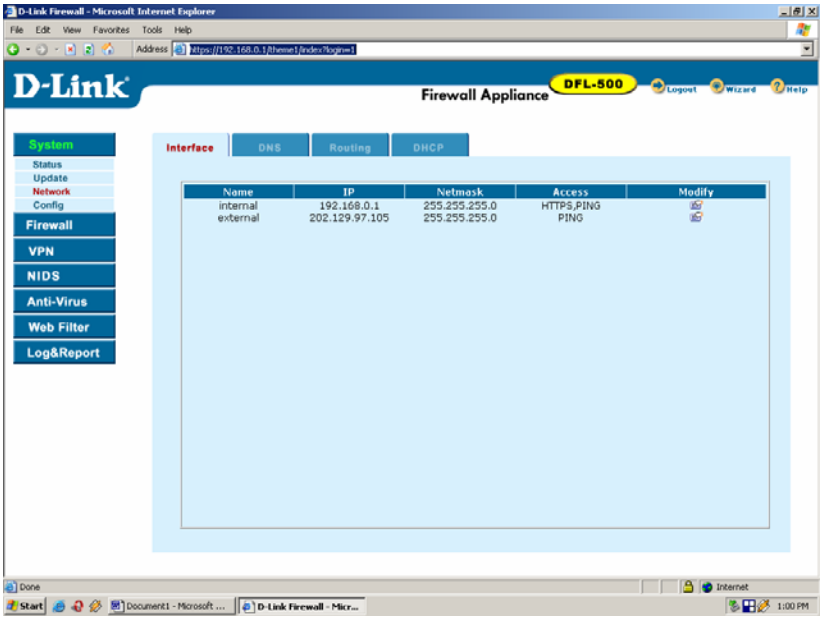
I. Configuring D-Link DFL-500 Firewall

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**"

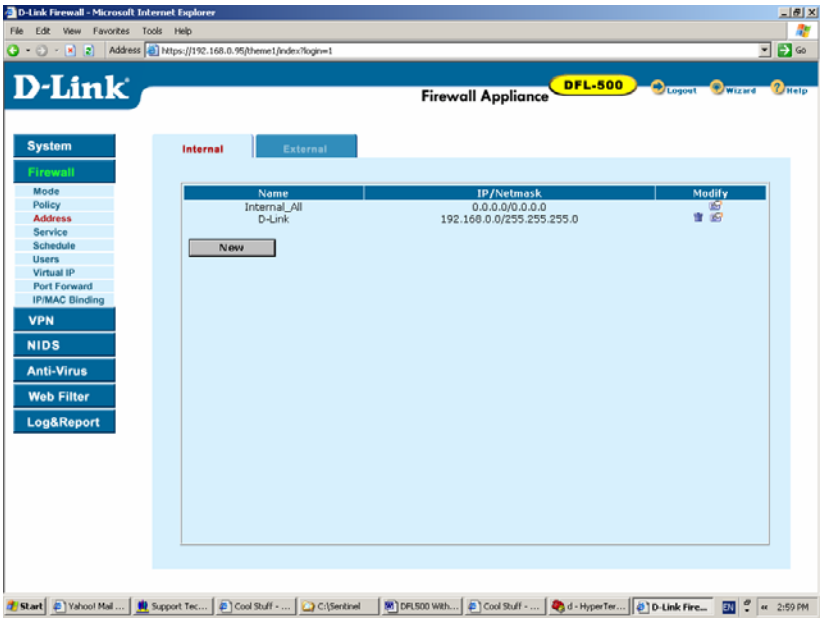


7. Click on "**Network**" under "**System**" menu
8. You will see "**internal**" and "**external**" interfaces
9. Click on **Modify** picture for "**internal**" interface
10. Put the ip address for the internal interface, for example 192.168.0.1 following the subnet mask 255.255.255.0 and press "**OK**". 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

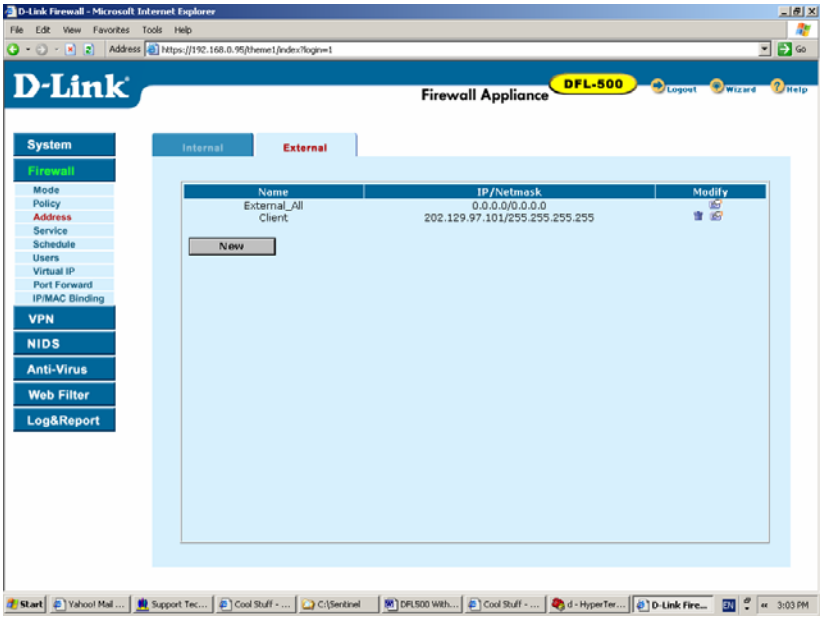
20. You will get the following configuration:



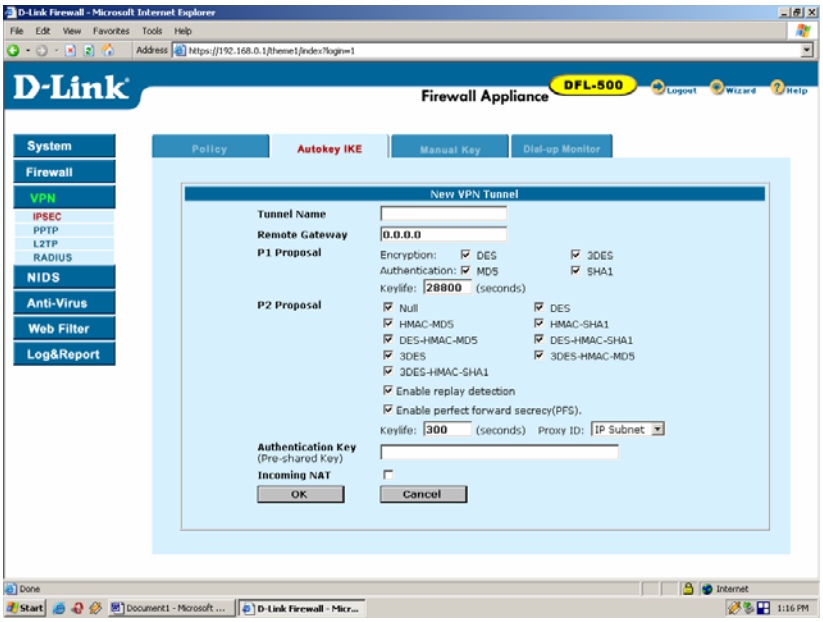
21. Go to **Firewall** menu and choose **Addresses**
22. If your XP/2000 IPSec client has a dynamically assigned IP address, you need to skip steps 23 – 26!
23. In the **Internal** submenu press "**New**"
24. Type the name of your internal network, for example "**D-Link**" and put the ip address of the 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:

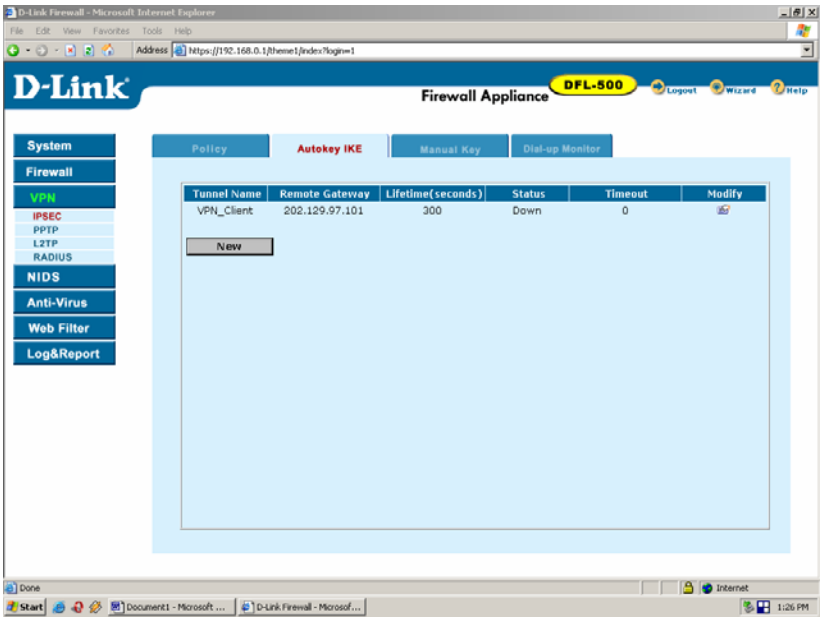


27. Go to **VPN** menu and choose **IPSec** submenu
28. Choose **Autokey IKE** bookmark and click “**New**”
29. You will see the following screen:

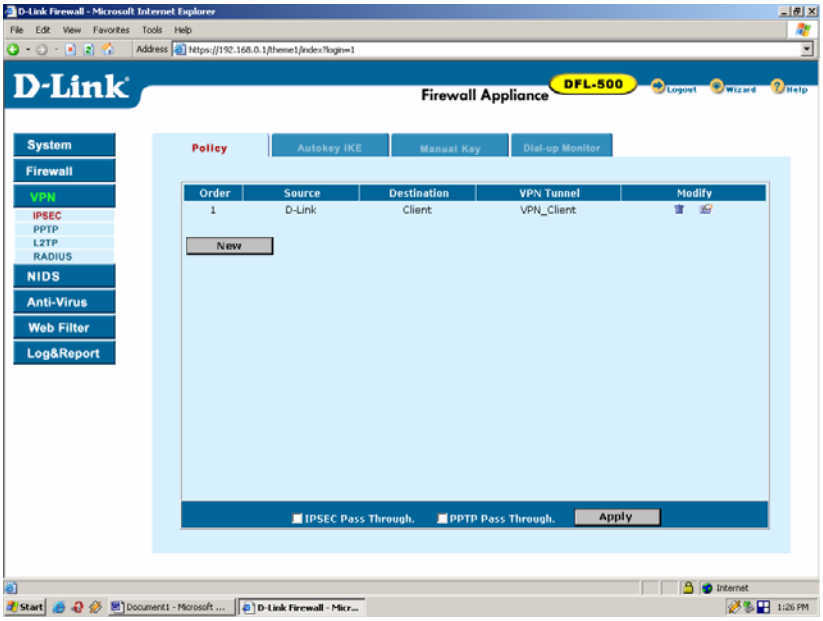


29. Put in the **Tunnel Name**, for example “**VPN_Client**”
    In “**Remote Gateway**” field type the ip address of the client, for example 202.129.97.101.
    Type 0.0.0.0, if your XP/2000 IPSec client has a dynamically assigned IP address!
30. Choose the encryption and authentication algorithms you 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**":



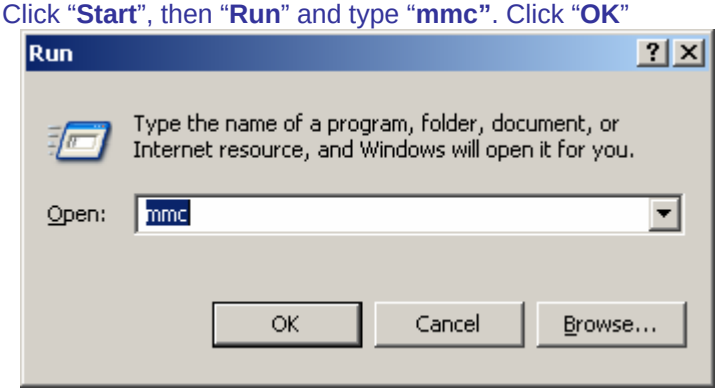
37. The DFL-500 Firewall configuration is finally ready.

II. Configuring Windows XP IPSec Client

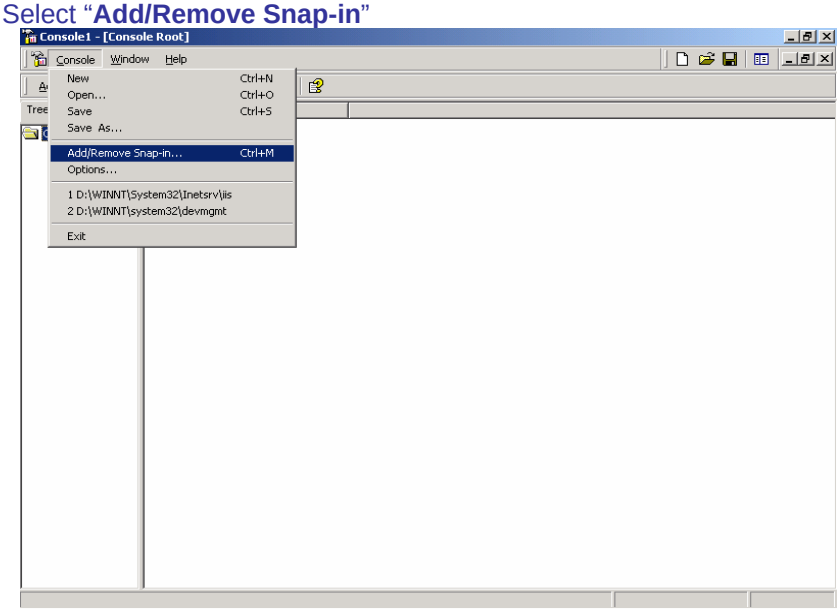
Technical Requirement: Customer is required to understand their network and the Windows XP well for this configuration. Please consult Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences arise from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

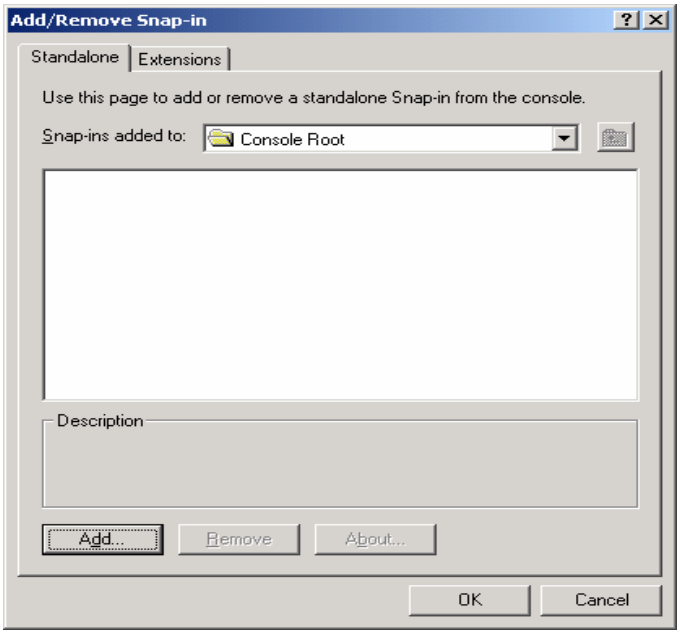
1. Click "**Start**", then "**Run**" and type "**mmc"**. Click "**OK**"



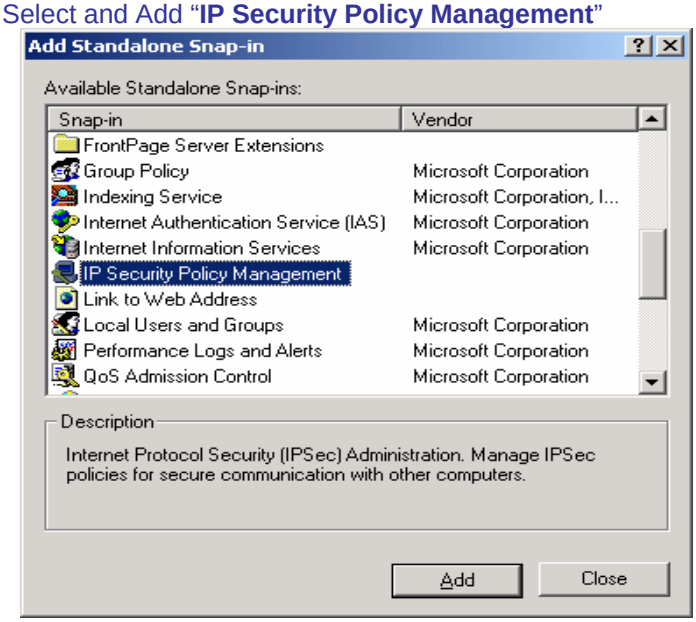
2. Select "**Add/Remove Snap-in**"



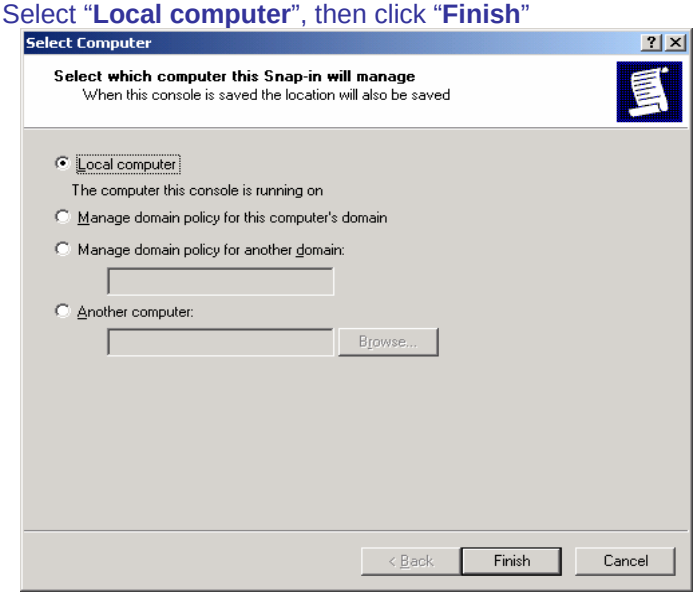
3. Click "**Add**"



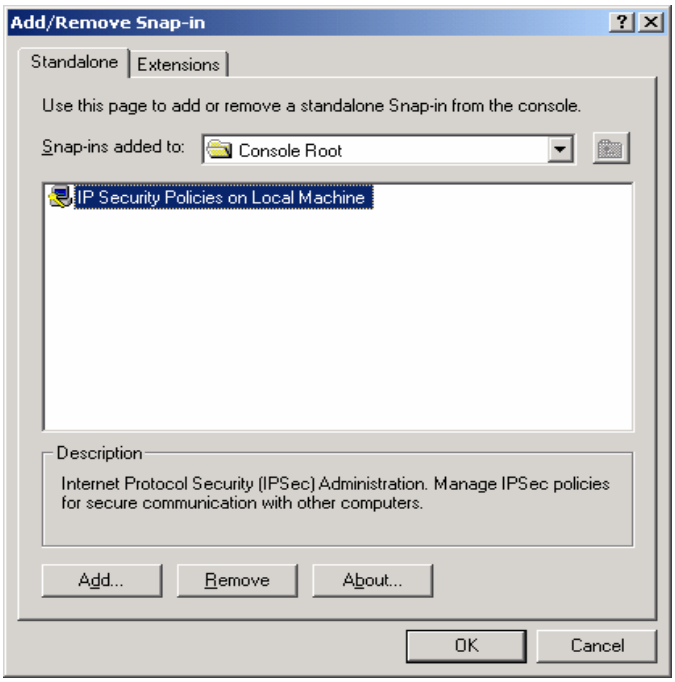
4. Select and Add "**IP Security Policy Management**"



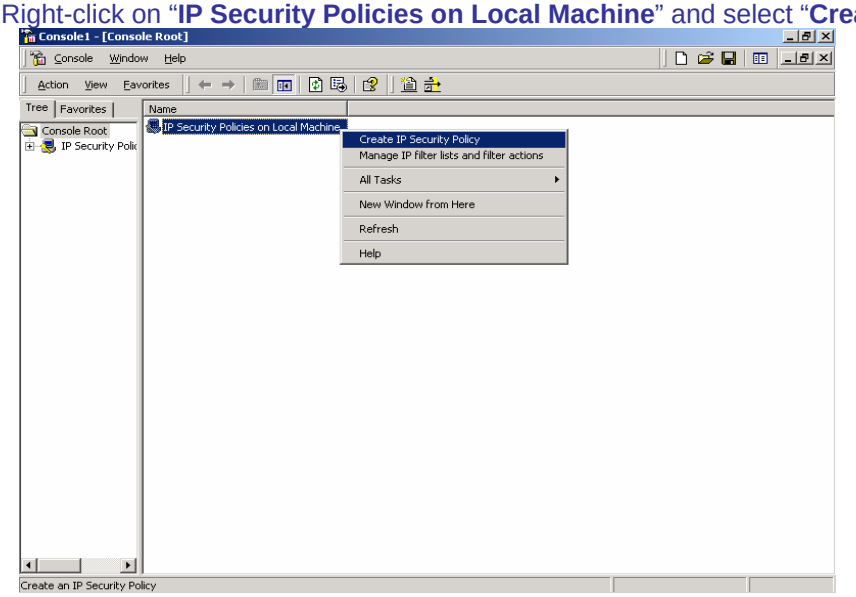
5. Select "**Local computer**", then click "**Finish**"



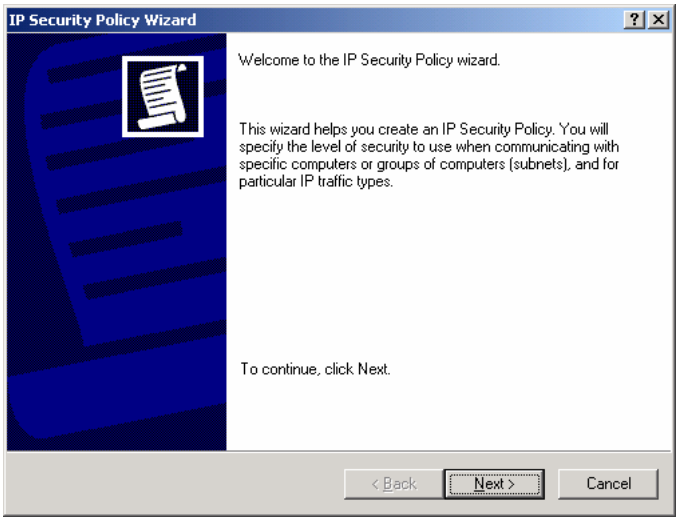
6. Click "**OK**"



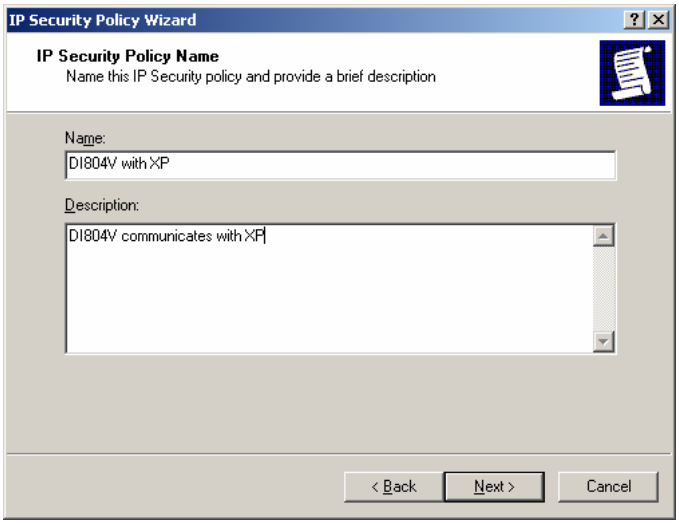
7. Right-click on “**IP Security Policies on Local Machine**” and select “**Create IP Security Policy**”



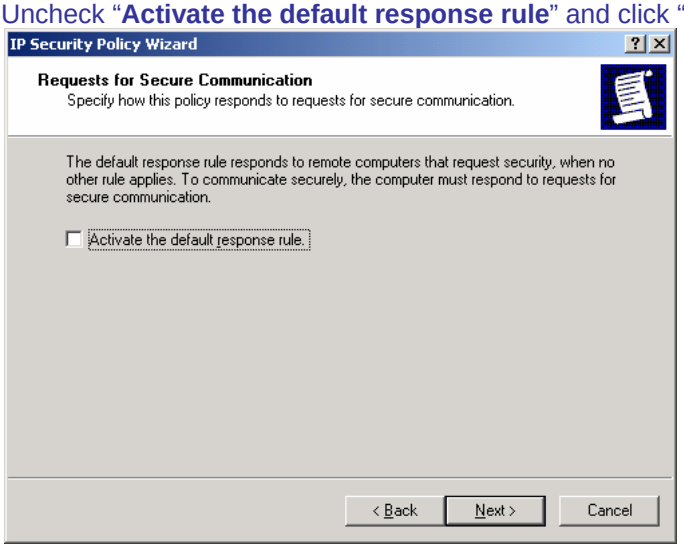
8. Click “**Next**”



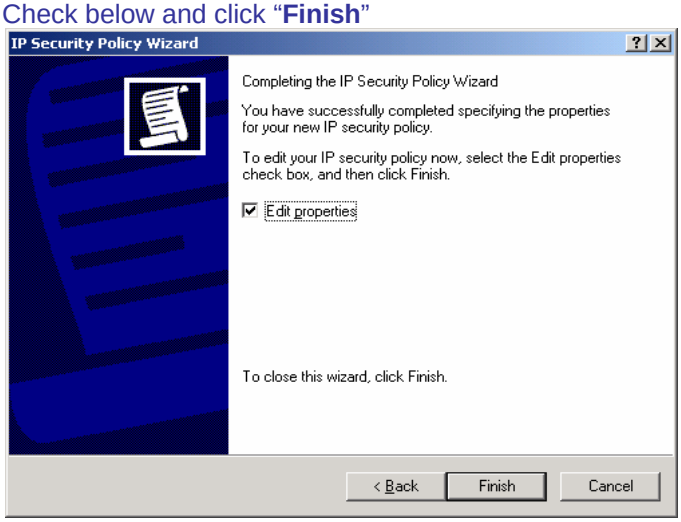
9. Enter the details below and click “**Next**”



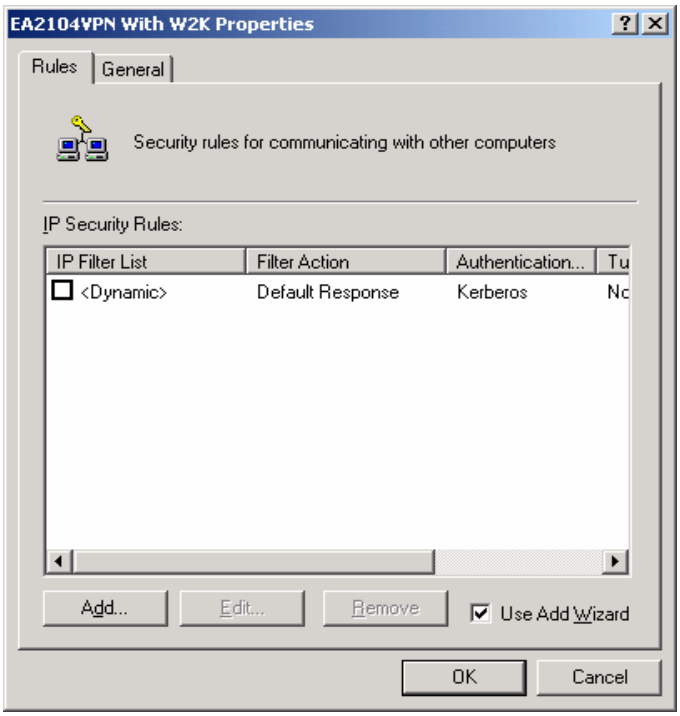
10. Uncheck “**Activate the default response rule**” and click “**Next**”



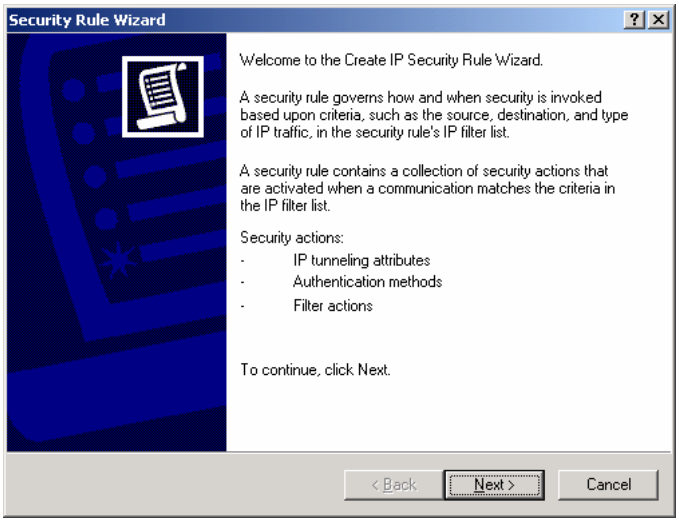
11. Check below and click “**Finish**”



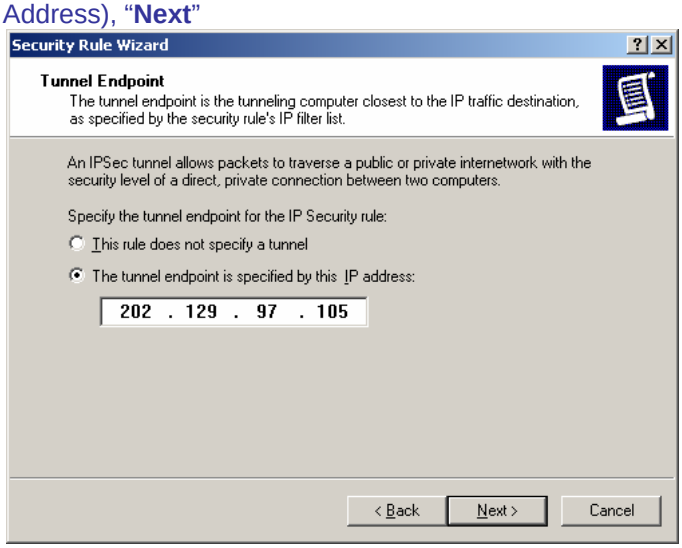
12. Select “**Add**”



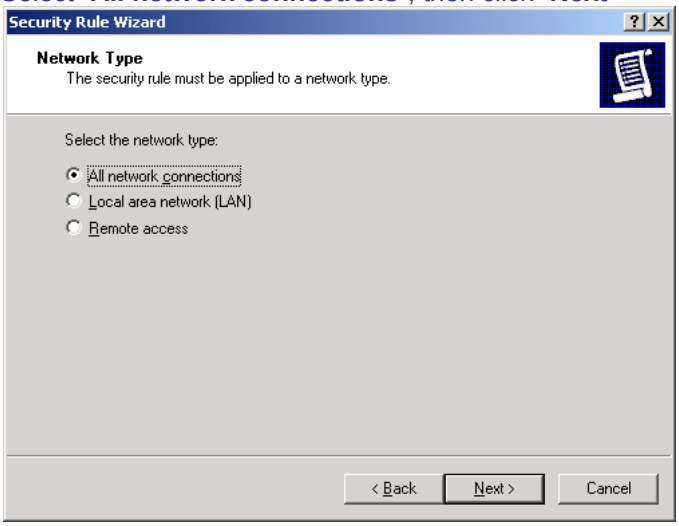
13. Click “Next”



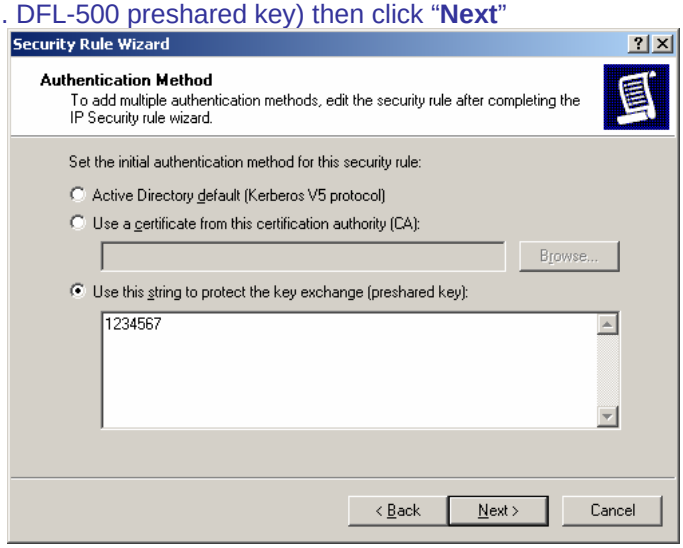
14. Input the IP Address into “**The tunnel endpoint specified by this IP address:**” (Eg. DFL-500 WAN IP Address), “**Next**”



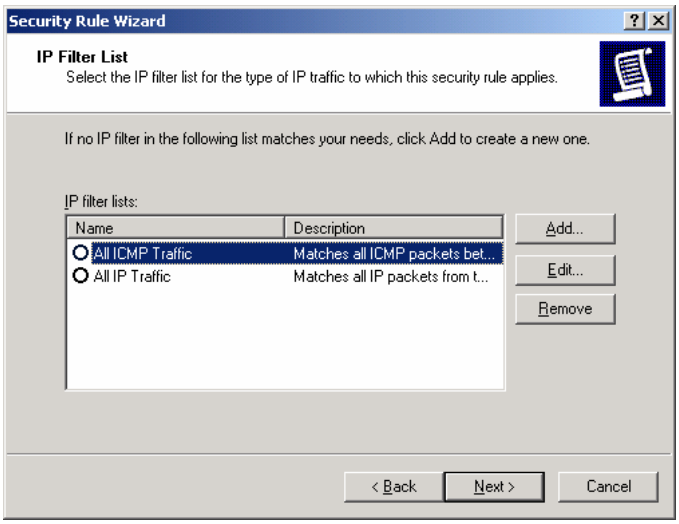
15. Select “**All network connections**”, then click “**Next**”



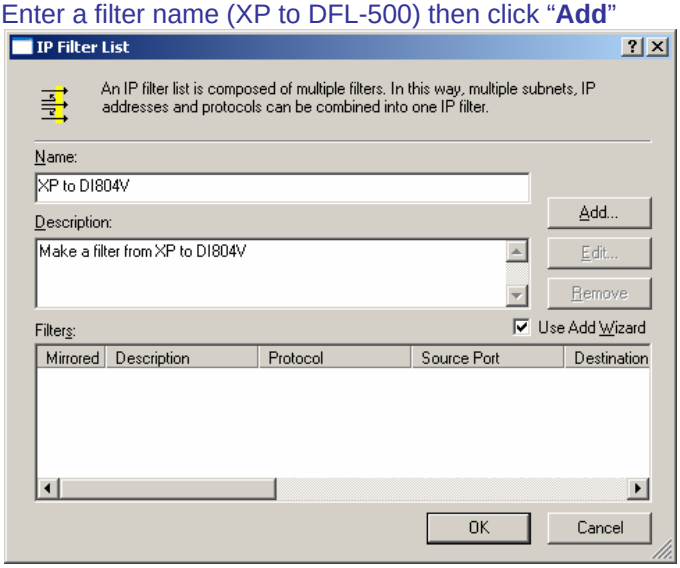
16. Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DFL-500 preshared key) then click “**Next**”



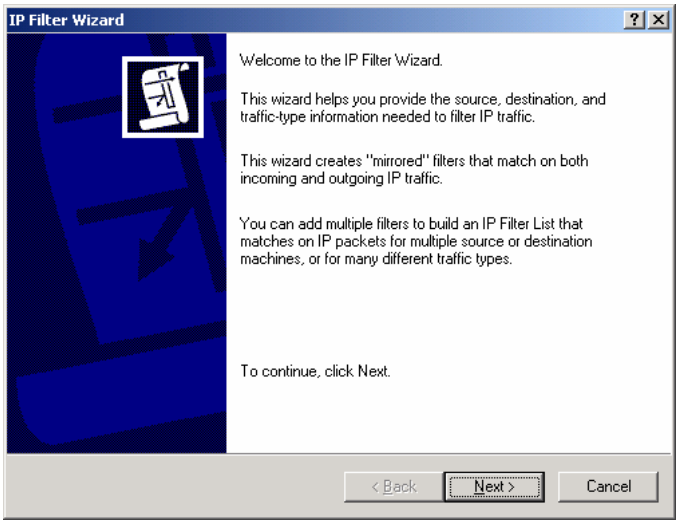
17. Select “**Add**”



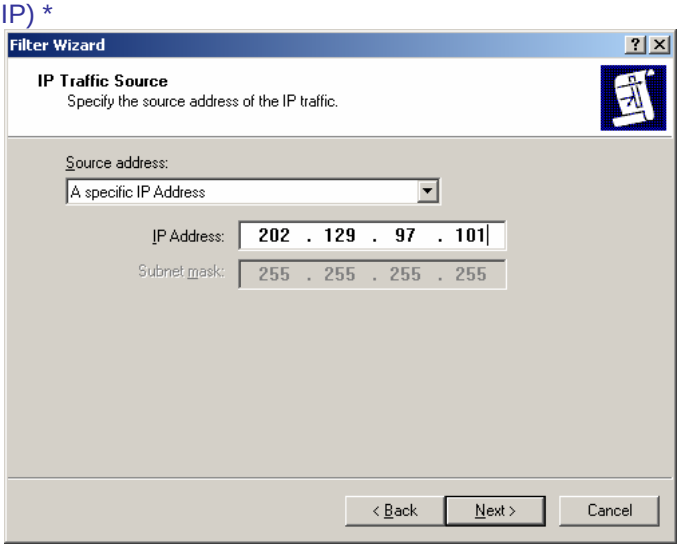
18. Enter a filter name (XP to DFL-500) then click “**Add**”



19. Click “**Next**”

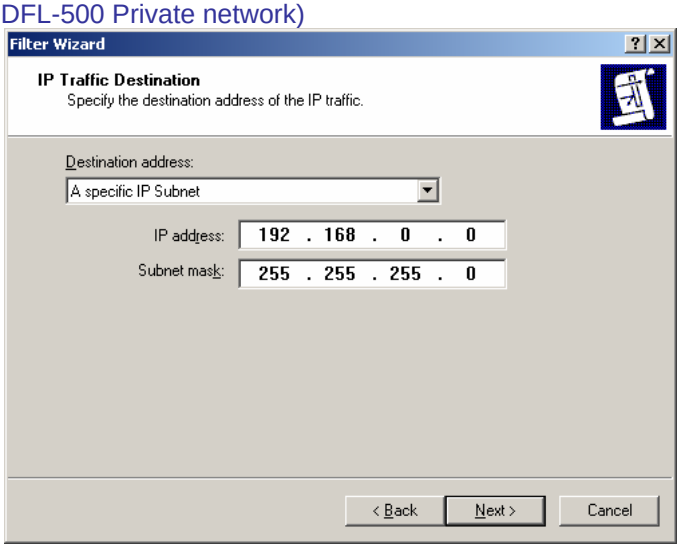


20. Select “**A specific IP Address**” and input the Source address, then “**Next**” to continue (Eg. Windows XP IP) *

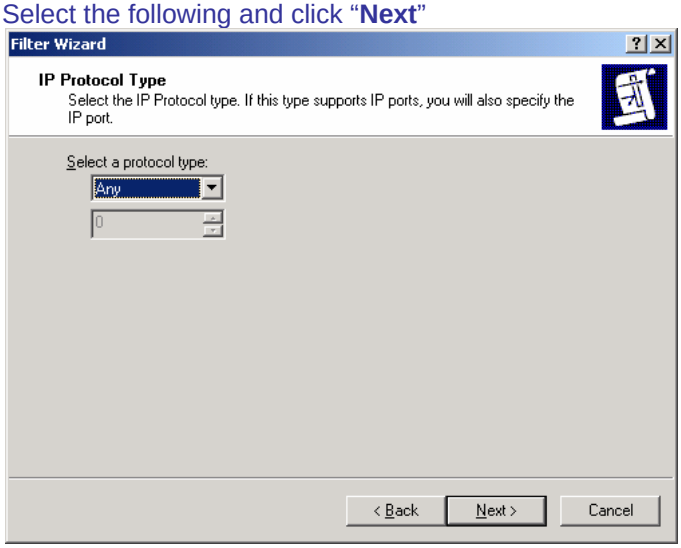


* If your client gets IP address dynamically choose “My IP address”.

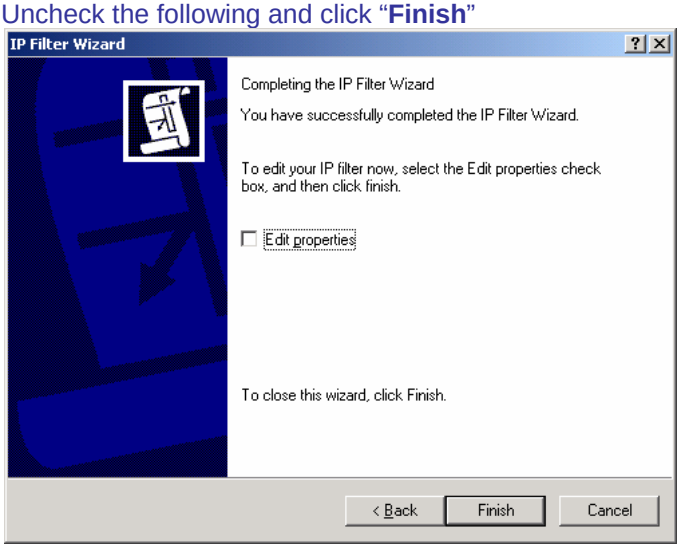
21. Select “**A specific IP Subnet**” and input the Destination subnet address, then “**Next**” to continue (Eg. DFL-500 Private network)



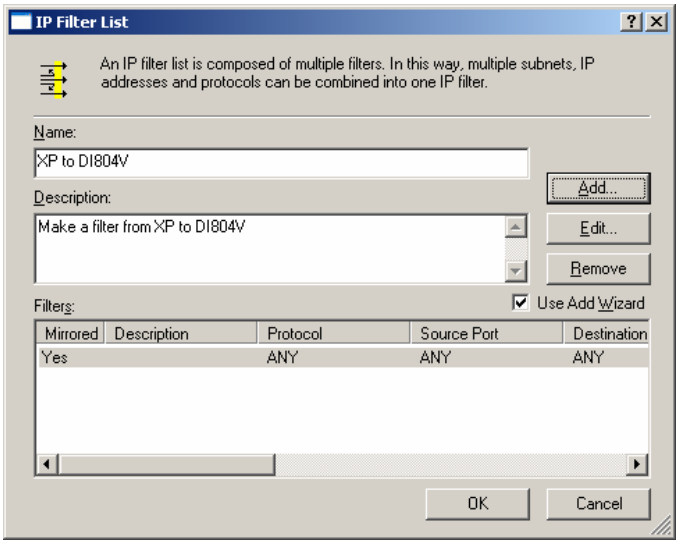
22. Select the following and click “**Next**”



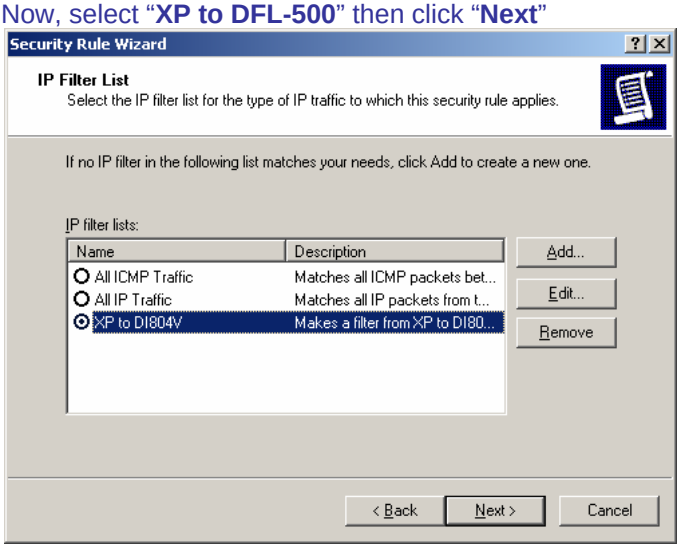
23. Uncheck the following and click “**Finish**”



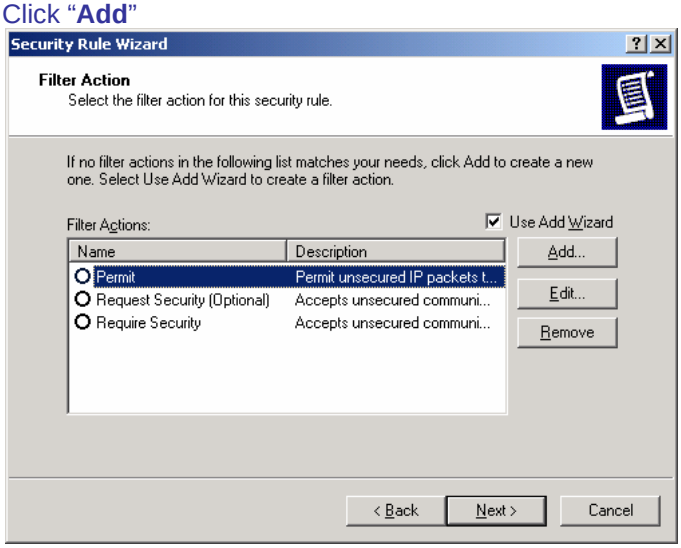
24. Click “**Ok**”



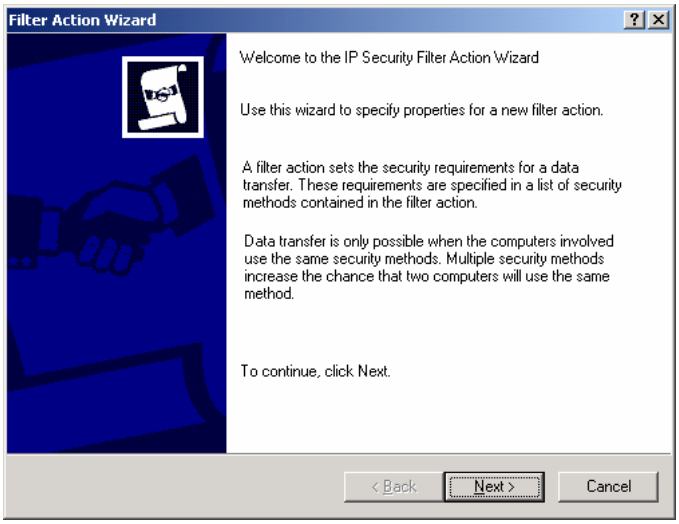
25. Now, select “**XP to DFL-500**” then click “**Next**”



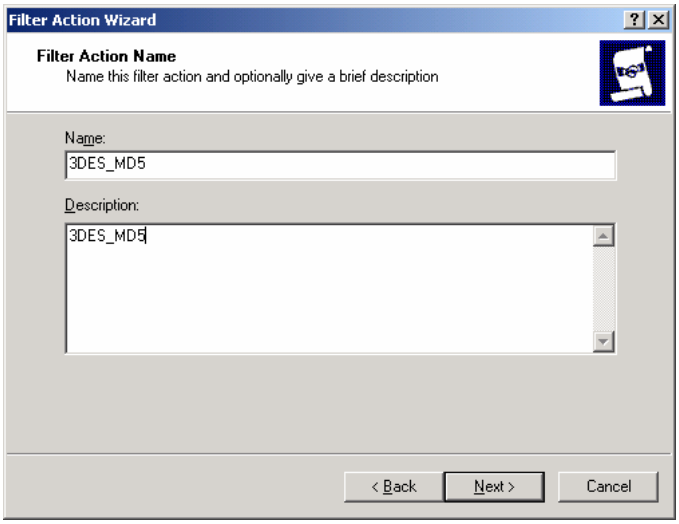
26. Click “**Add**”



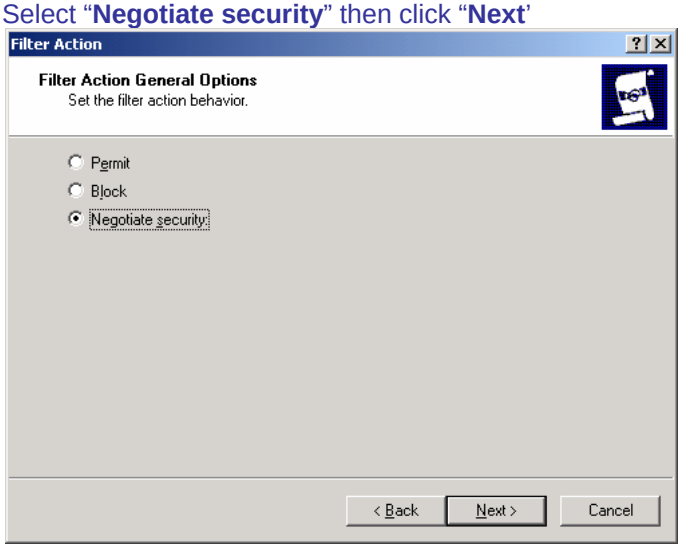
27. Click “**Next**”



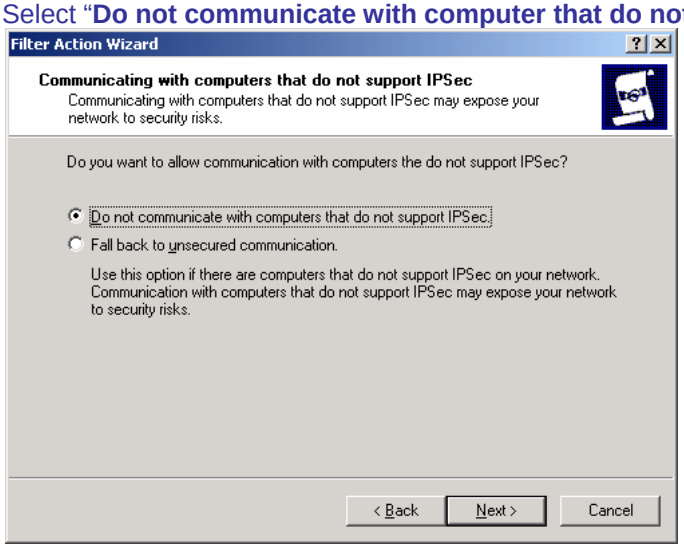
28. Enter a filter action name then click “**Next**”



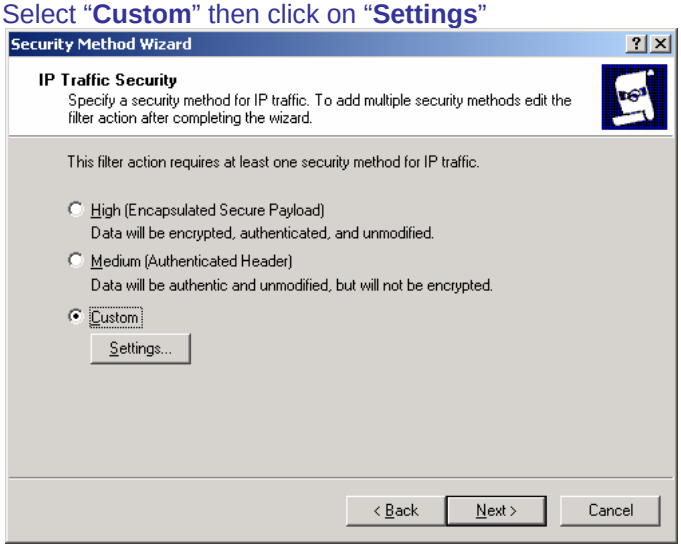
29. Select “**Negotiate security**” then click “**Next**’



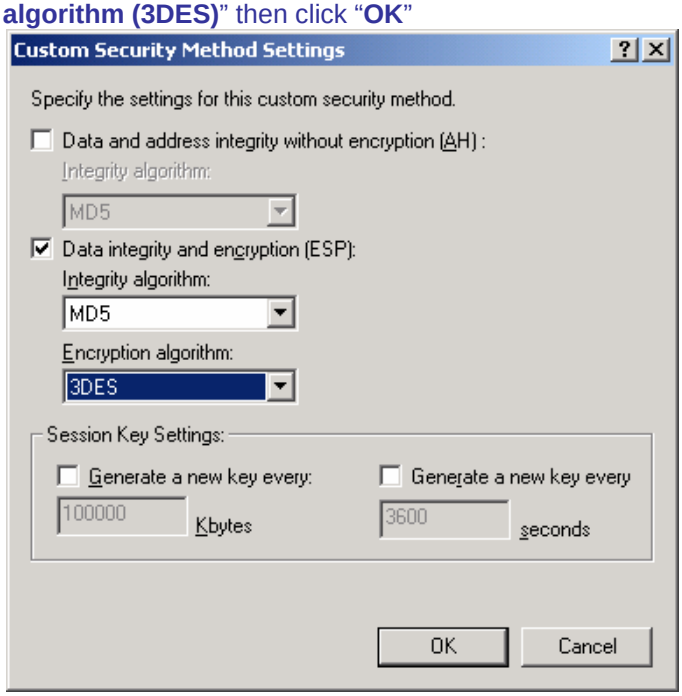
30. Select “**Do not communicate with computer that do not support IPSec**” then click “**Next**”



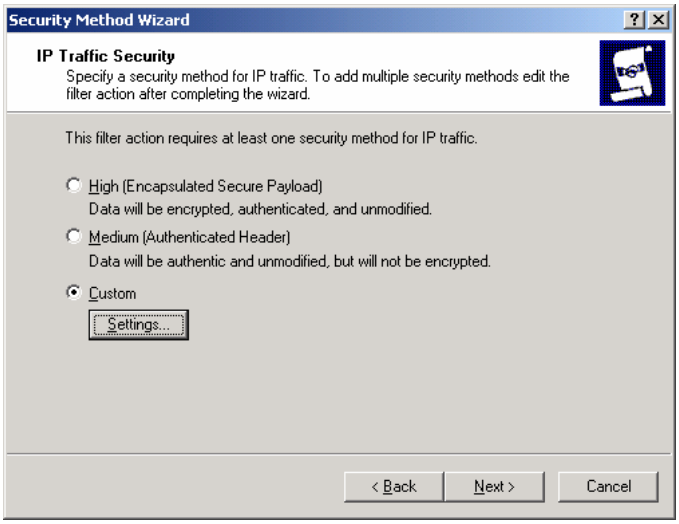
31. Select “**Custom**” then click on “**Settings**”



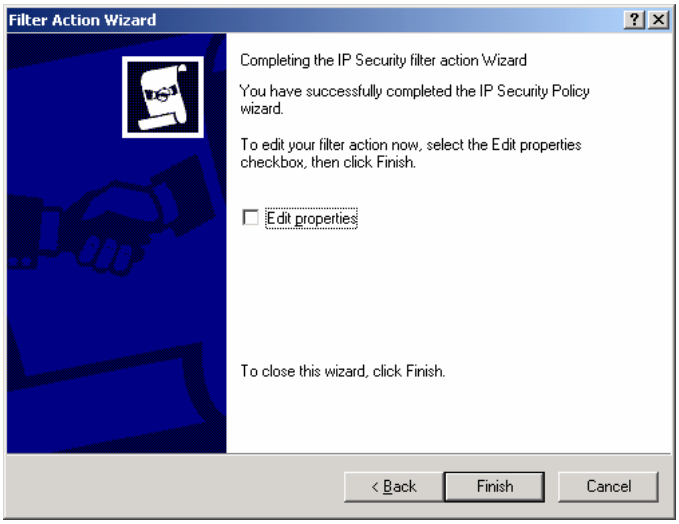
32. Check “**Data integrity and encryption (ESP)**”, select the “**Integrity algorithm (MD5)**” and “**Encryption algorithm (3DES)**” then click “**OK**”



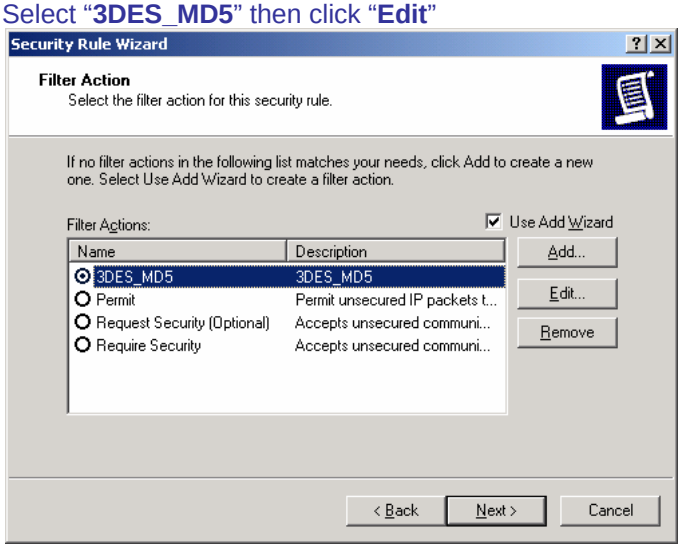
33. Click “**Next**”



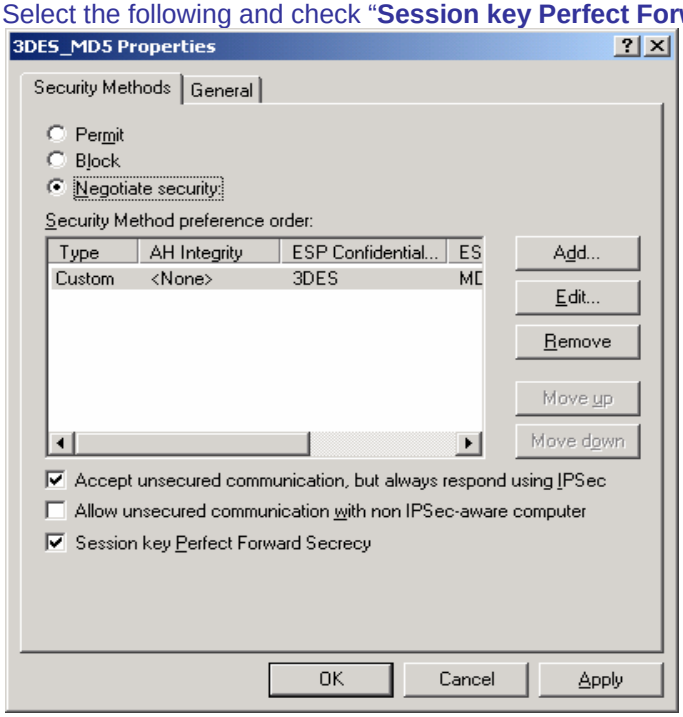
34. Click “**Finish**”



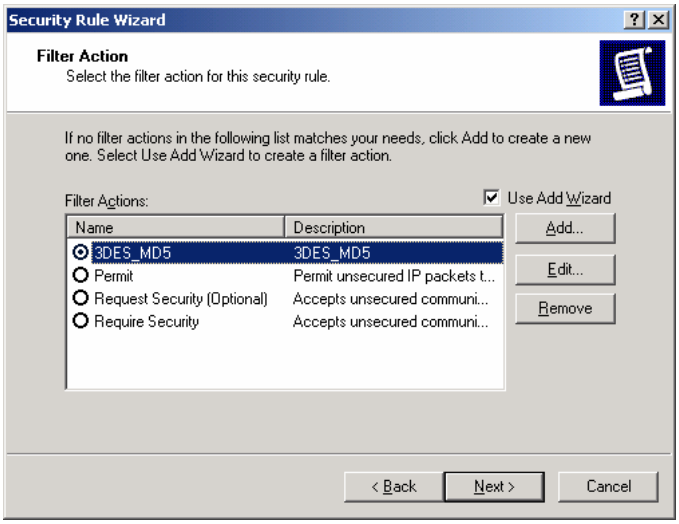
35. Select “**3DES_MD5**” then click “**Edit**”



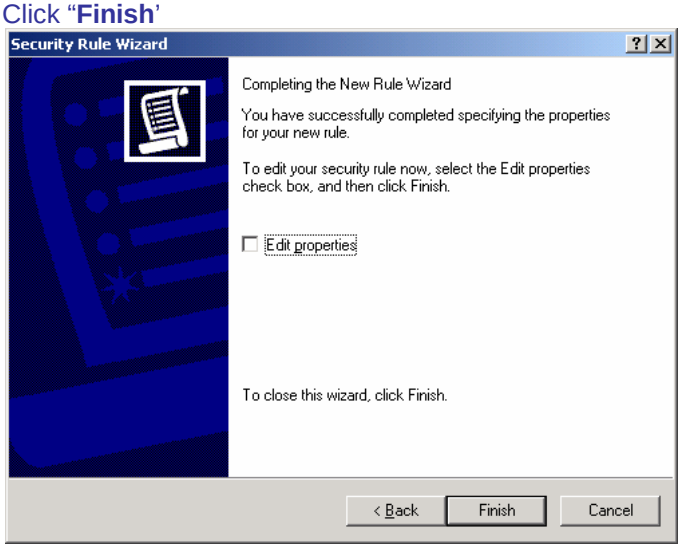
36. Select the following and check “**Session key Perfect Forward Secrecy**” then click “**OK**”



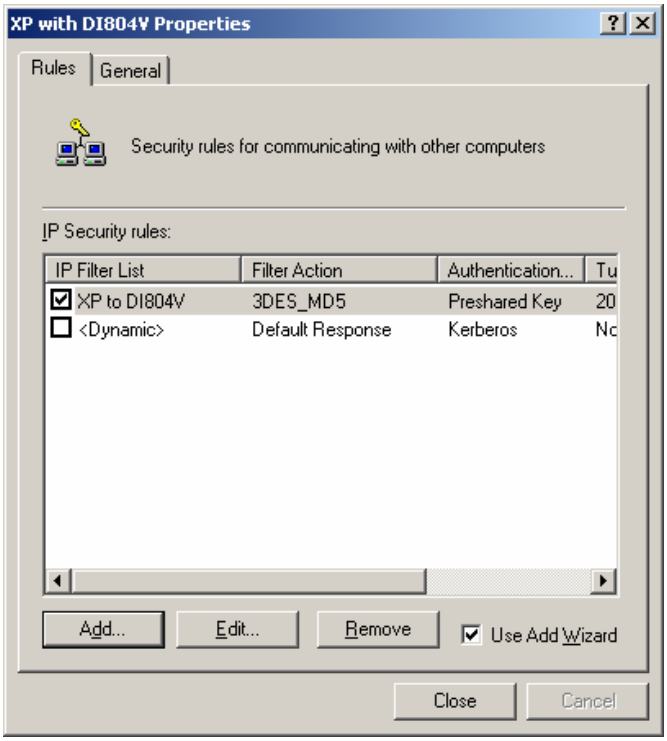
37. Click “**Next**”



38. Click “**Finish**’

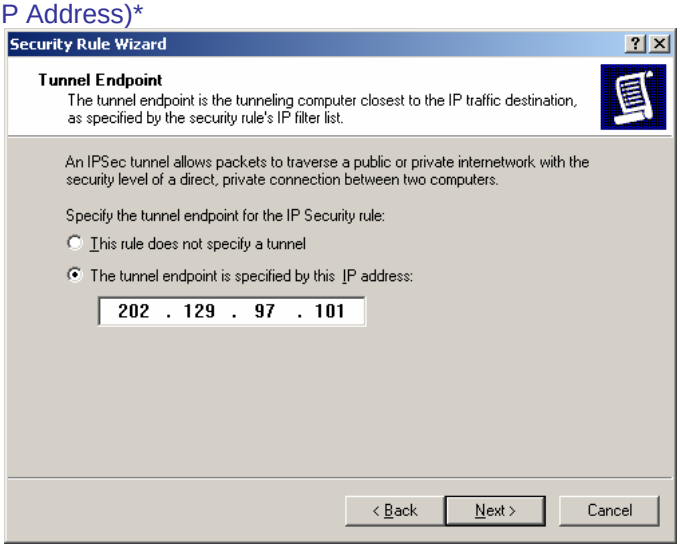


39. Click “**Add**”



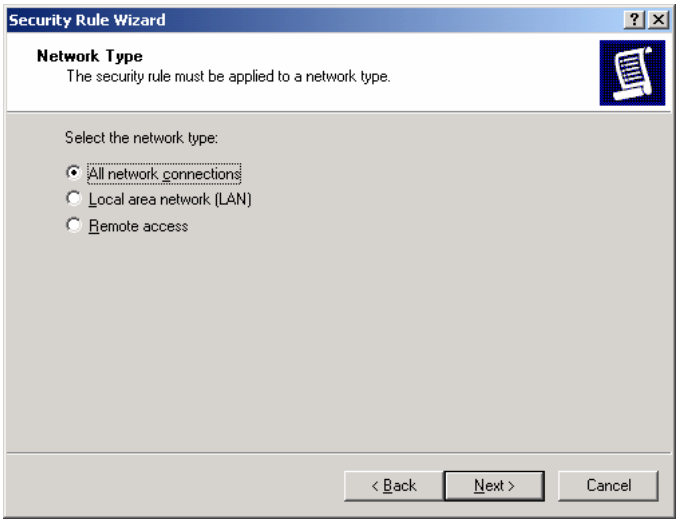
40. Click “**Next**”

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

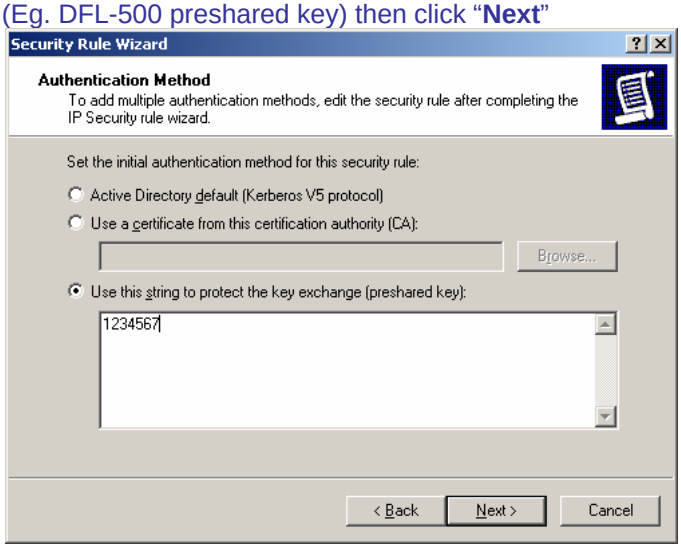


* If your client gets IP address dynamically, put the dynamic IP address here! You will have to change this setting every time you connect to the Internet. Unfortunately, this is the limitation of XP/2000 IPSec client. If your XP/2000 IPSec client is connected to the Internet through the router, use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

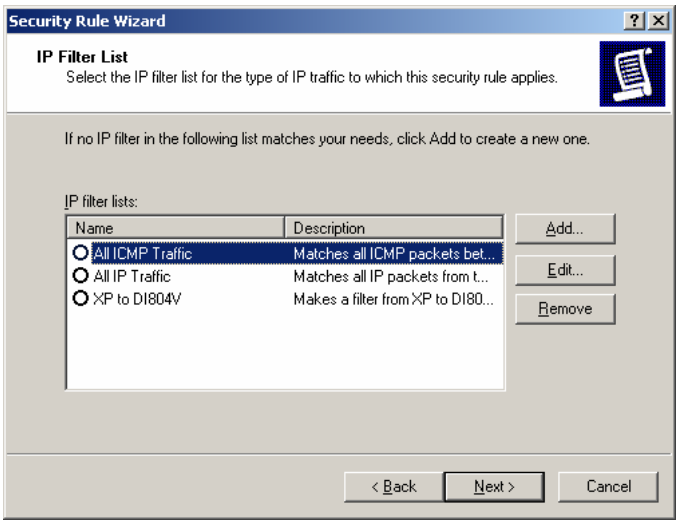
42. Select “**All network connections**” then click “**Next**”



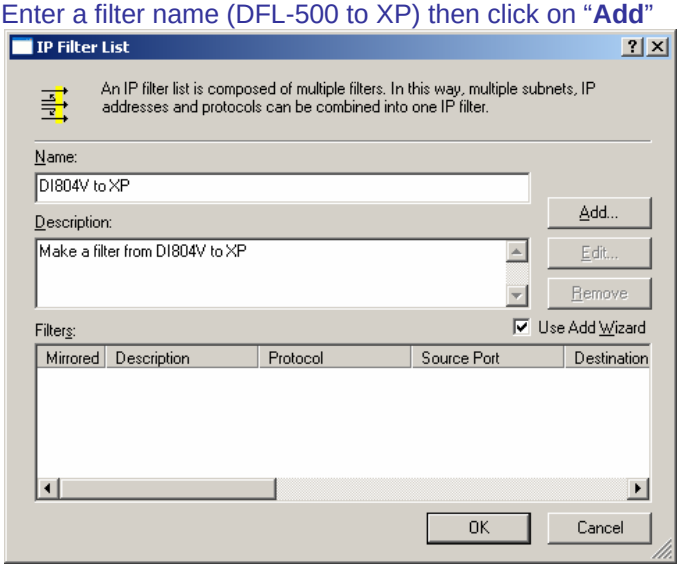
43. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DFL-500 preshared key) then click "**Next**"



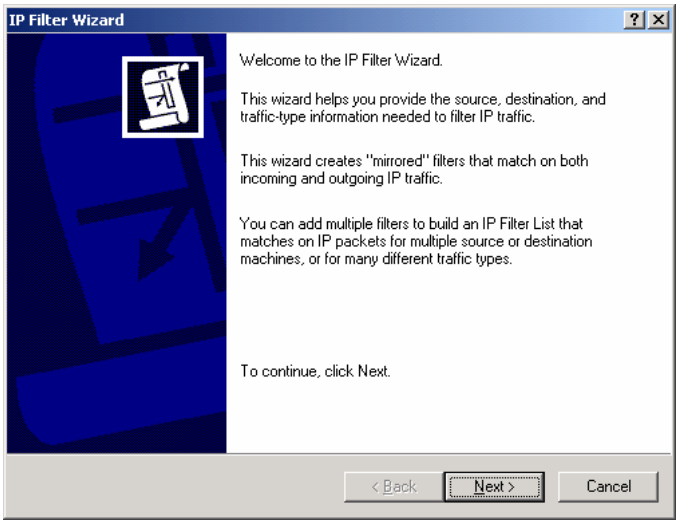
44. Click "**Add**"



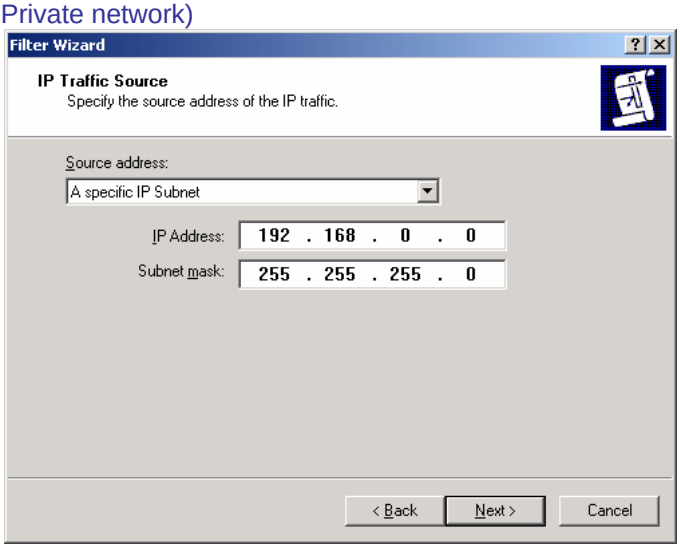
45. Enter a filter name (DFL-500 to XP) then click on "**Add**"



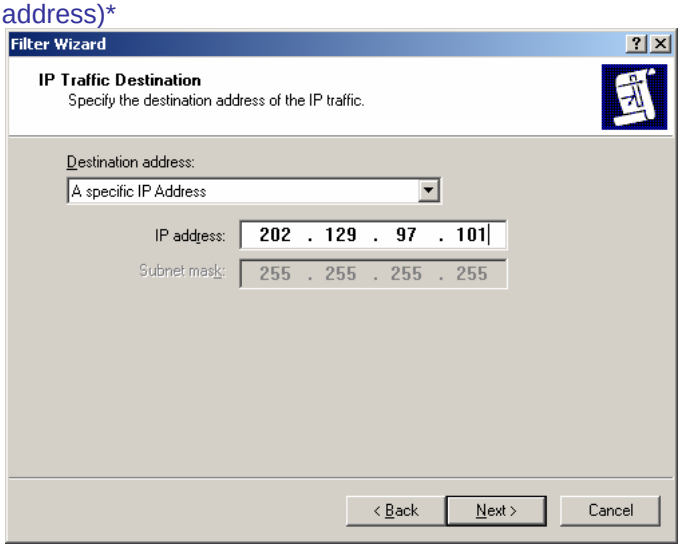
46. Click “**Next**”



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

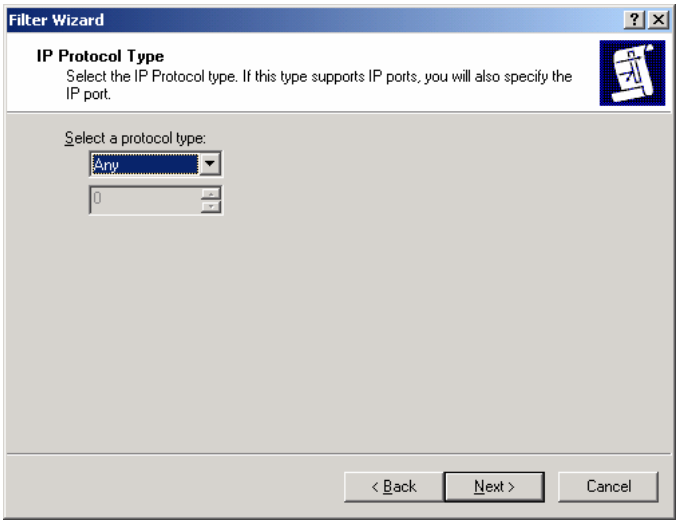


48. Select “**A specific IP Address**” and input the Destination address then click “**Next**” (Eg. Windows XP IP address)*

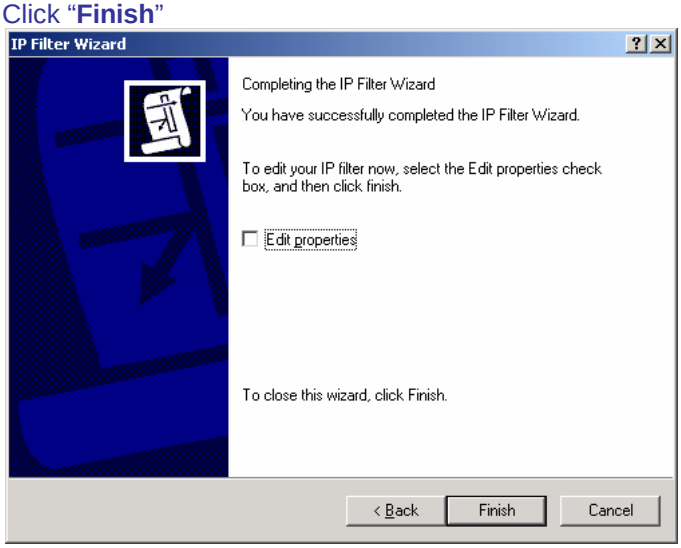


* If your client gets IP address dynamically choose “My IP Address”.

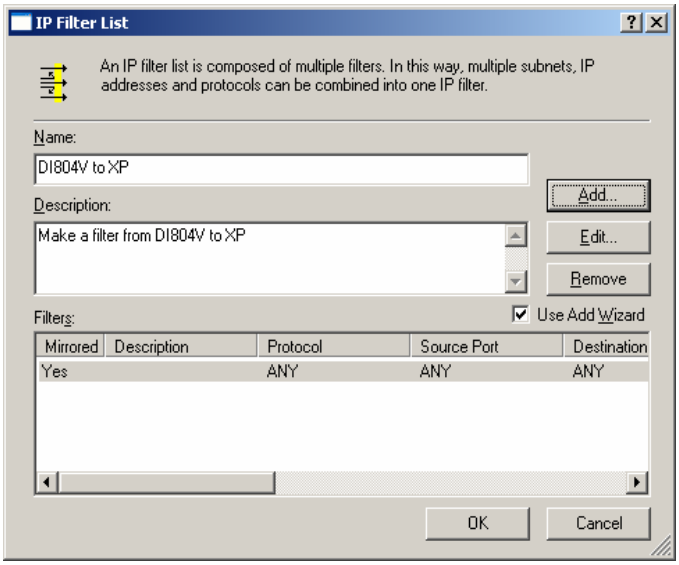
49. Click “**Next**”



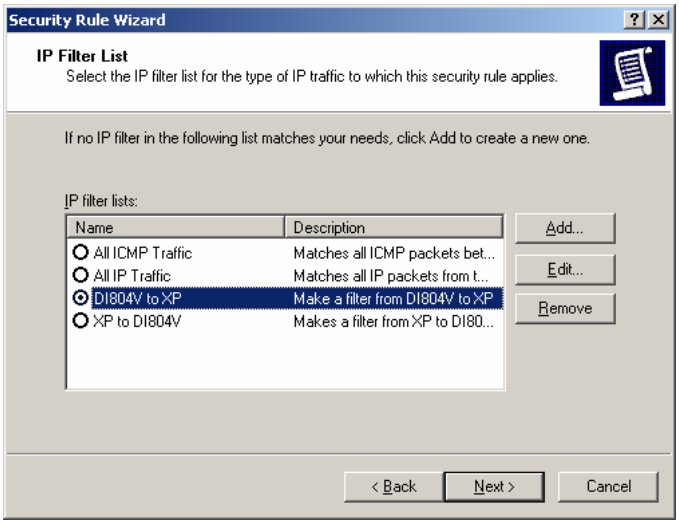
50. Click “**Finish**”



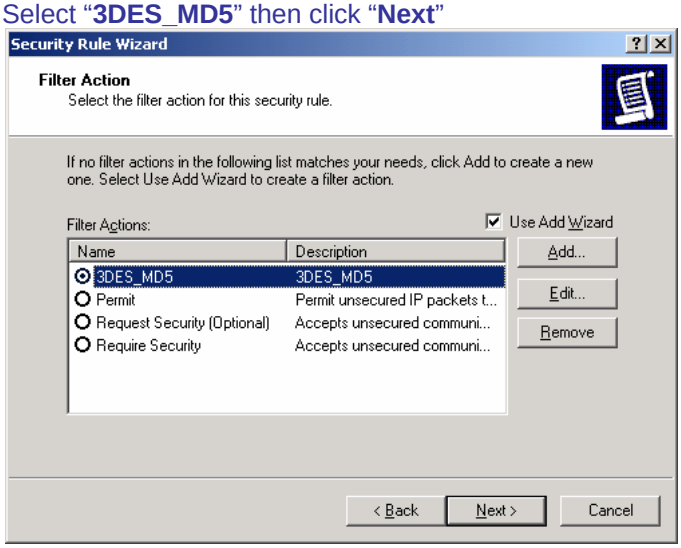
51. Click on “**Close**”



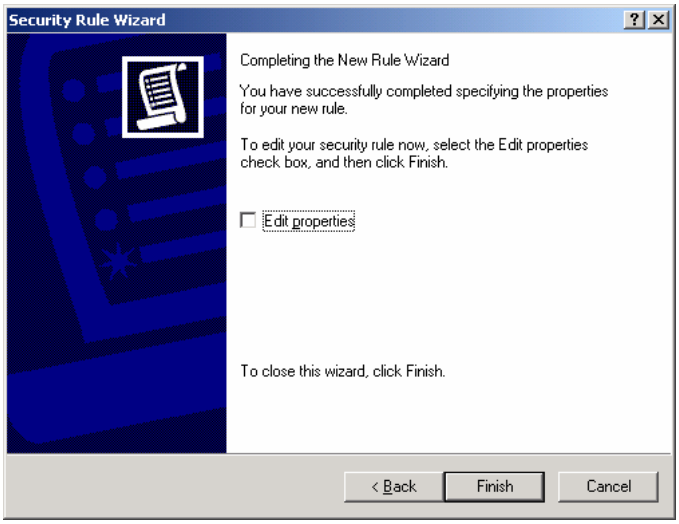
52. Select “**DFL-500 to XP**” then click “**Next**”



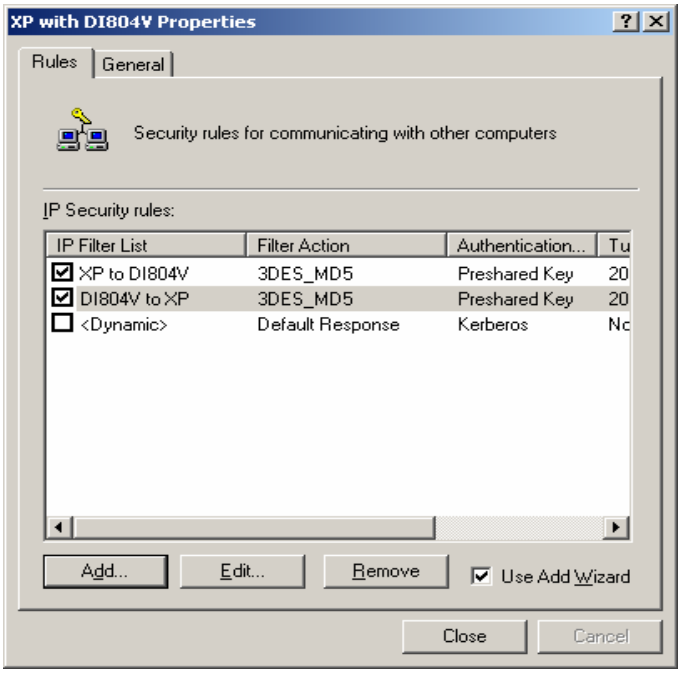
53. Select “**3DES_MD5**” then click “**Next**”



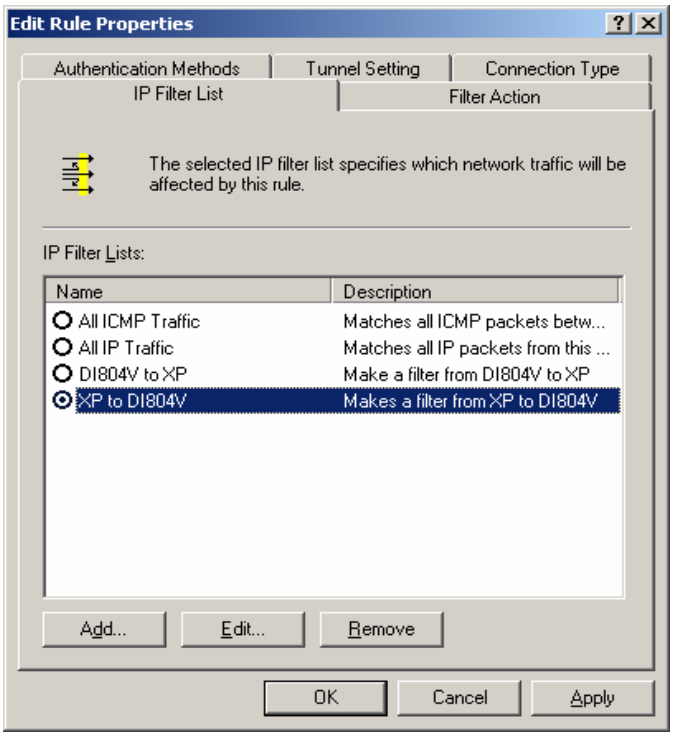
54. Click “**Finish**”



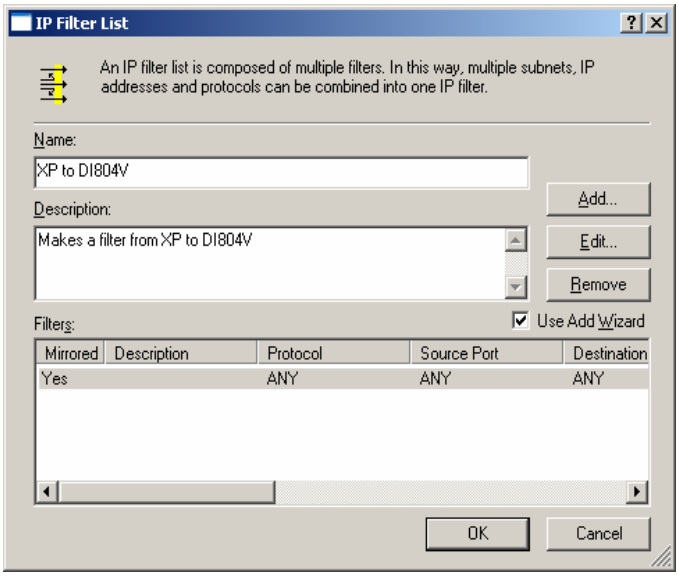
55. Select “**XP to DFL-500**” then click on “**Edit**”



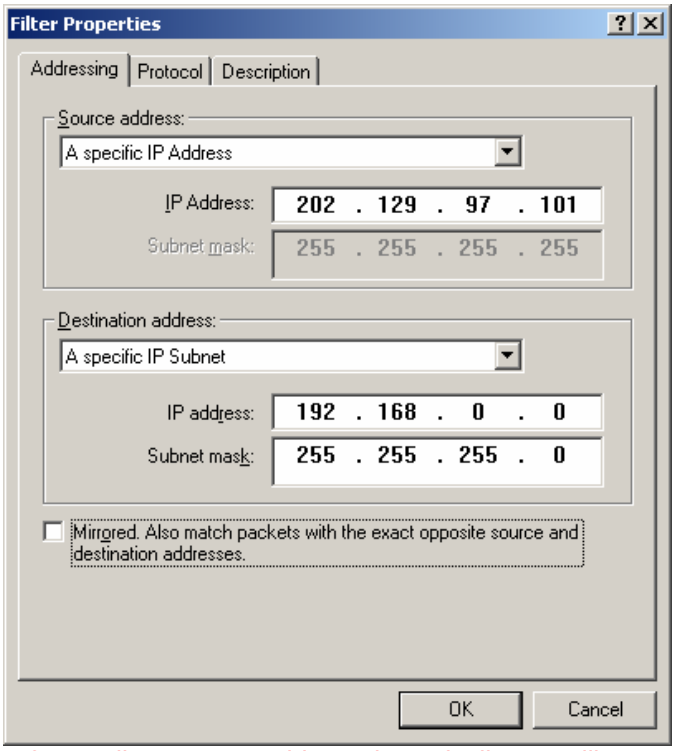
56. Select “**XP to DFL-500**” then click on “**Edit**”



57. Click “**Edit**”

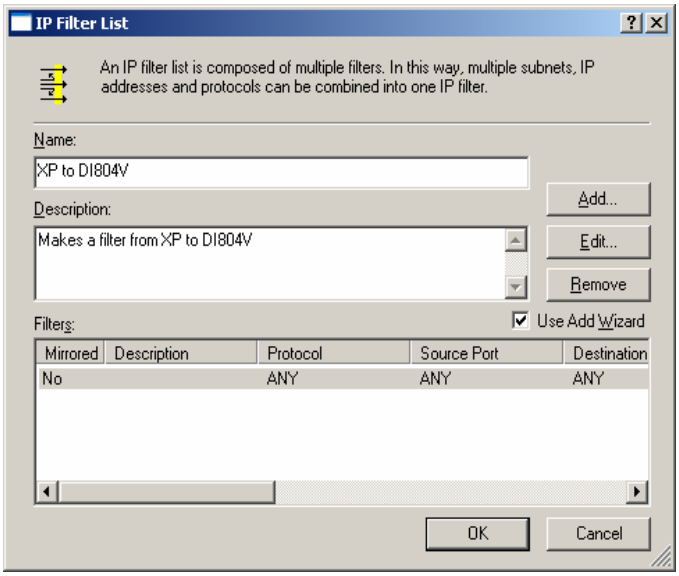


58. Uncheck “**Mirrored. Also match packets with exact opposite source and destination address**” then click “**OK**” *

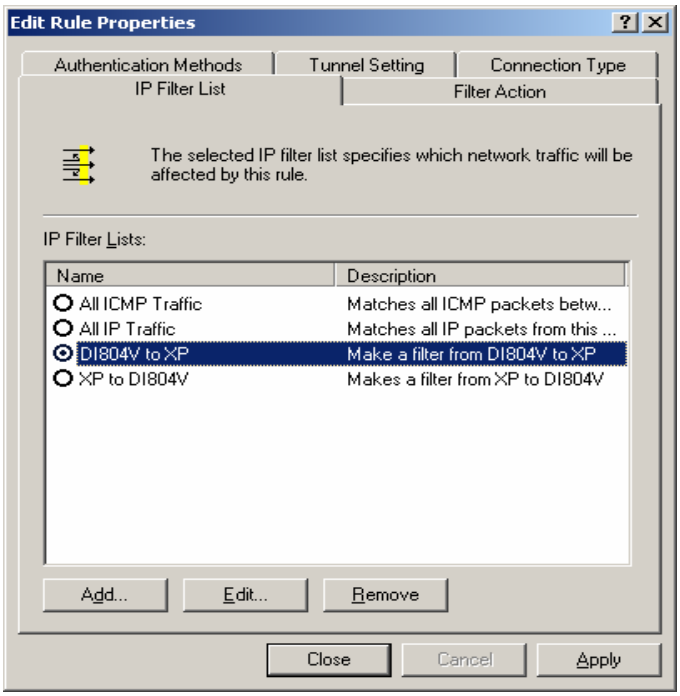


* If your client gets IP address dynamically you will see “My IP Address” in Source address field.

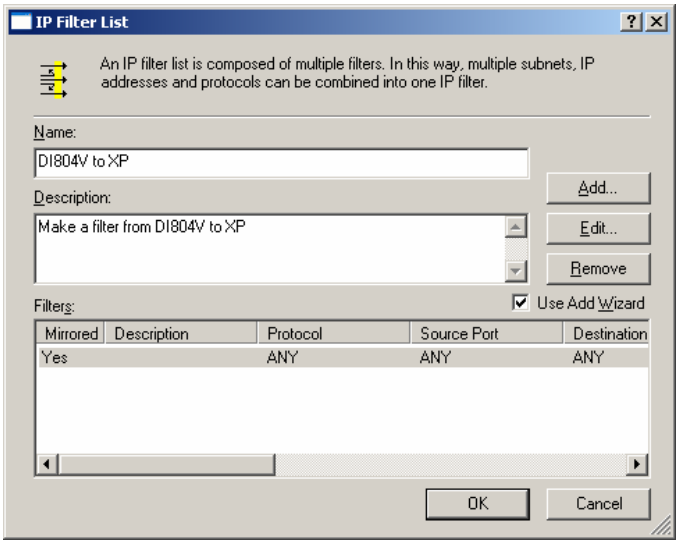
59. Click “**Close**”



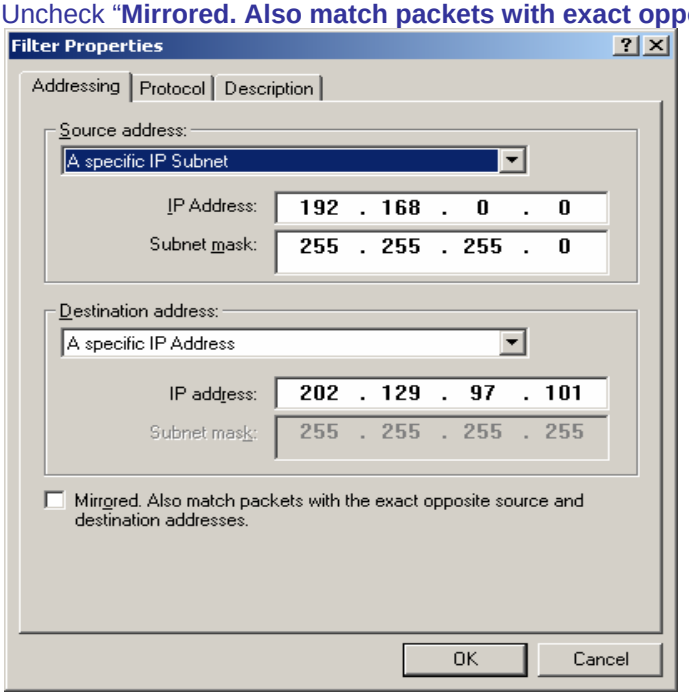
60. Select “**DFL-500 to XP**” then click on “**Edit**”



61. Click “**Edit**”

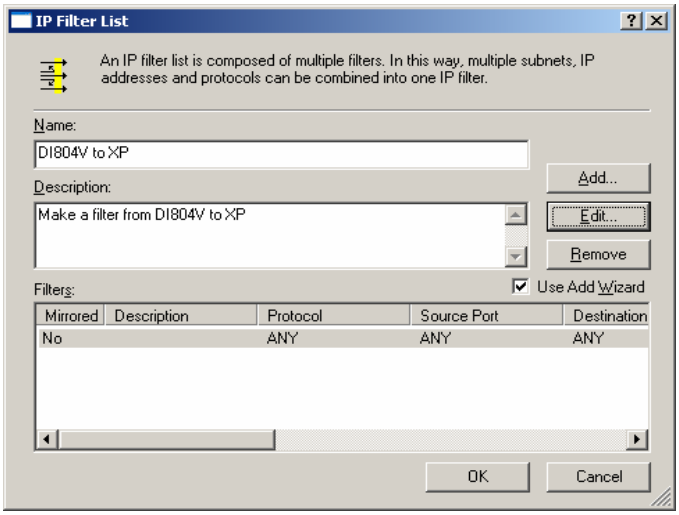


62. Uncheck “**Mirrored. Also match packets with exact opposite source…**” then click “**OK**” *

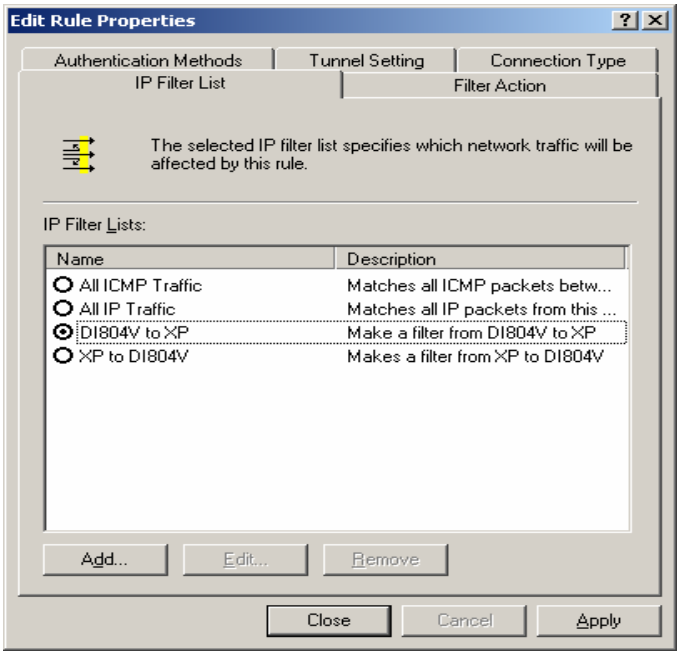


* If your client gets IP address dynamically you will see “My IP Address” in Destination address field.

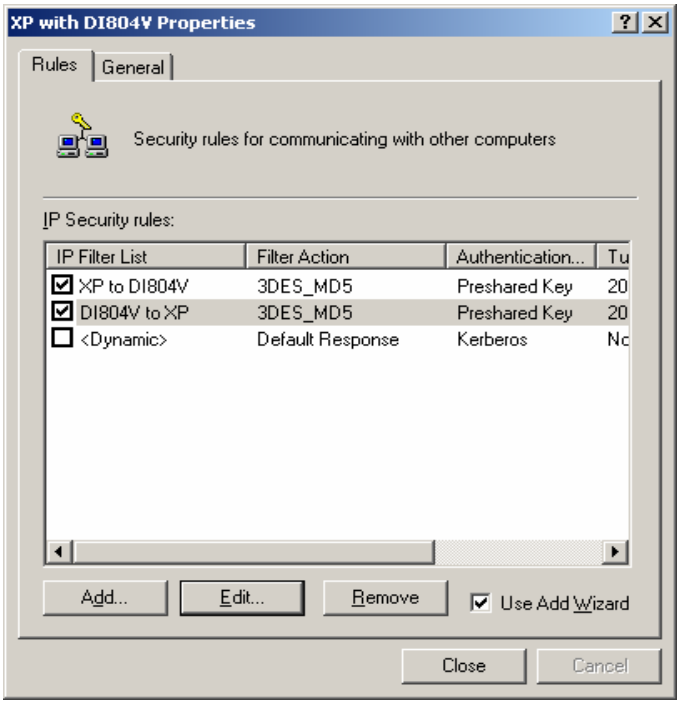
63. Click “**Ok**”



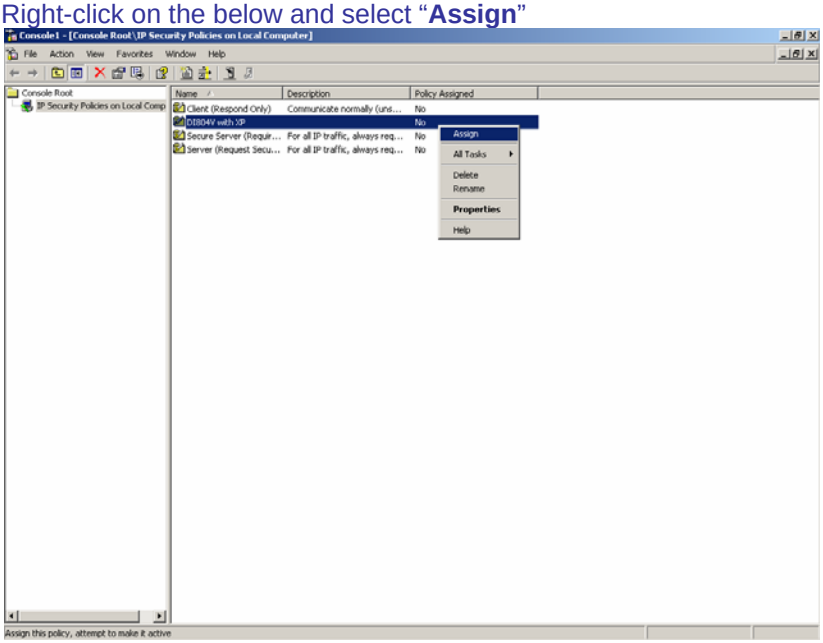
64. Click “**Close**”



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”