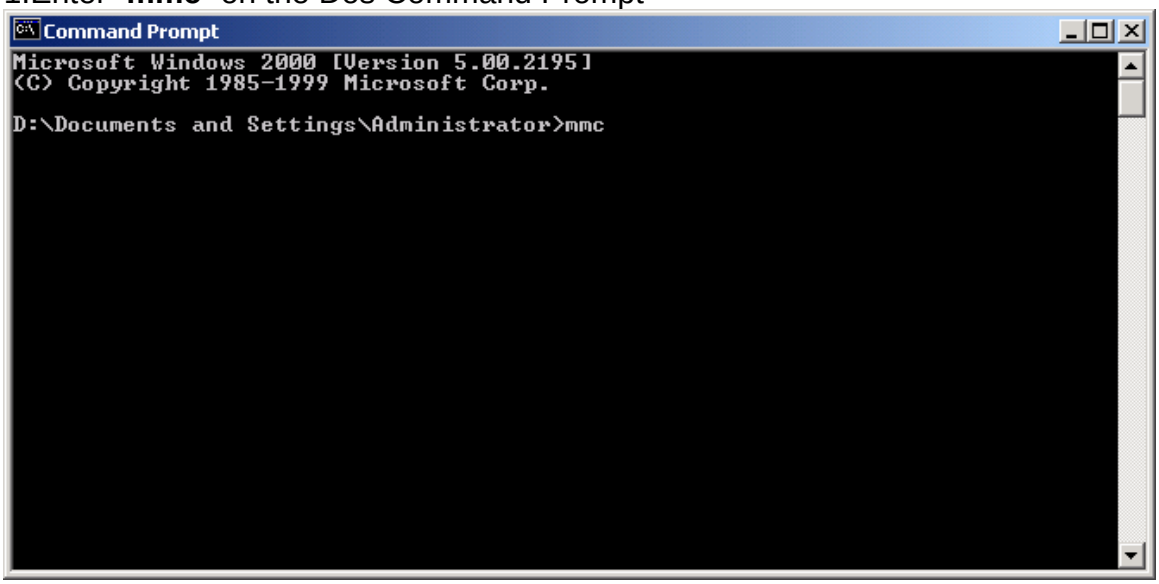
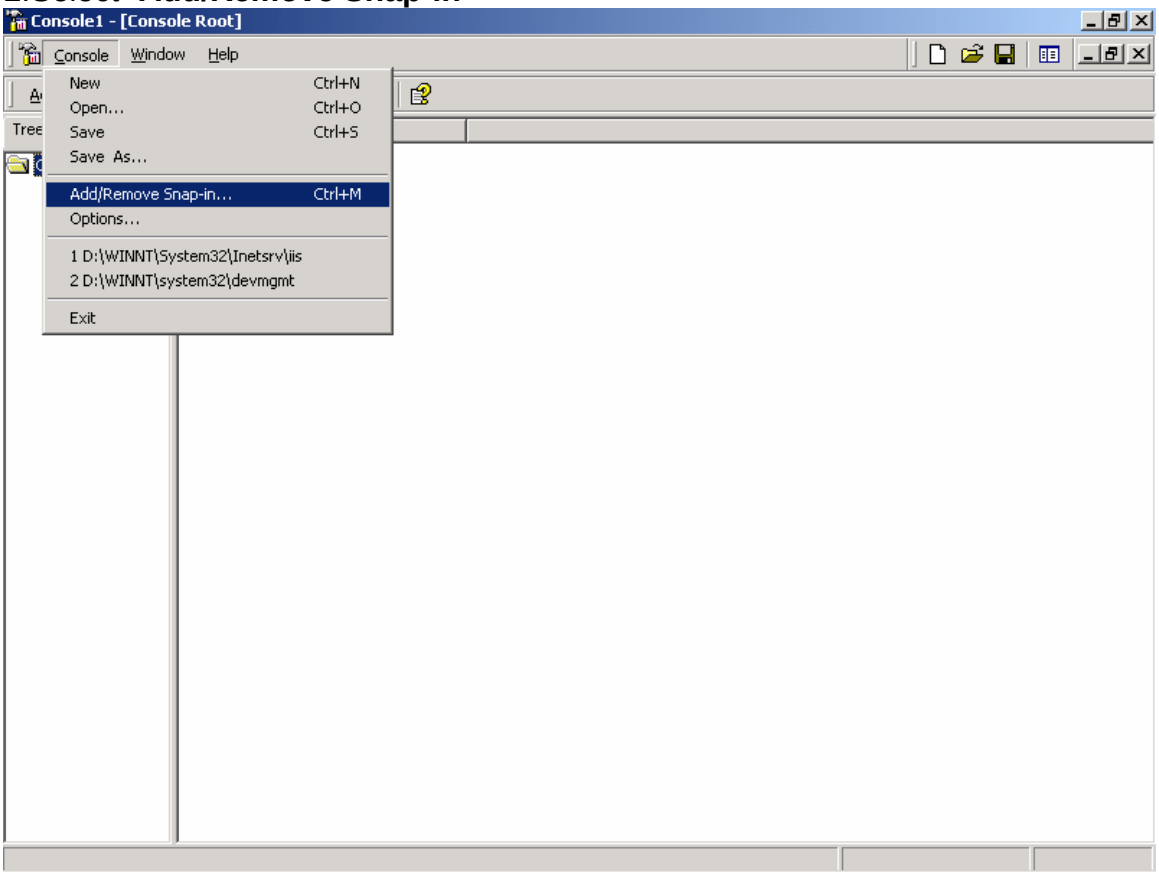
DI-804V With Windows 2000 Advanced Server IPSec VPN Configuration Procedures

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.

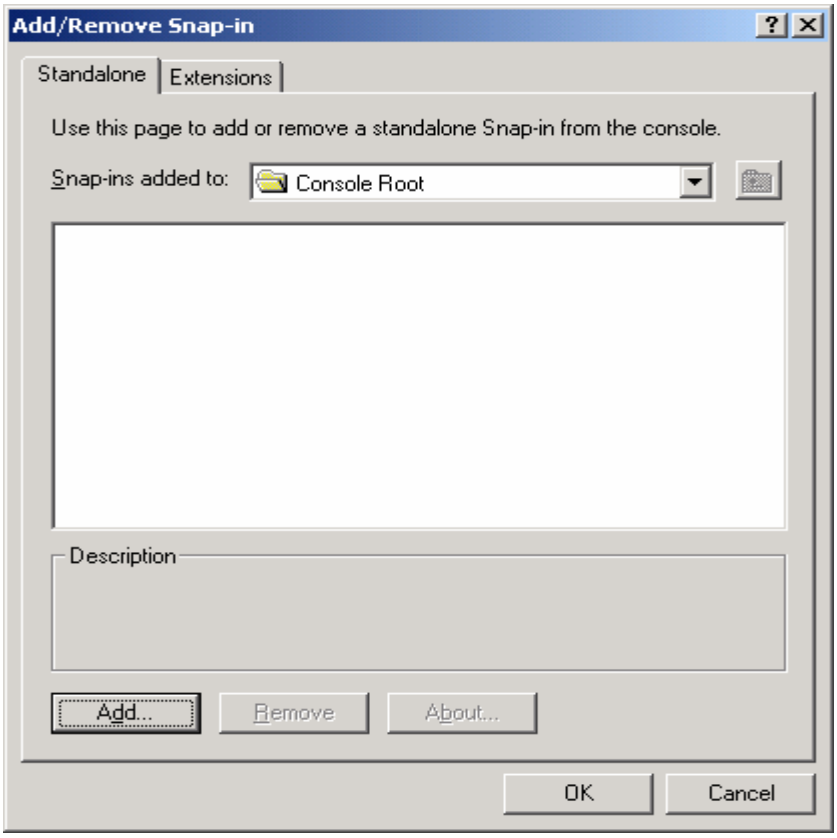
1.Enter "**mmc**" on the Dos Command Prompt



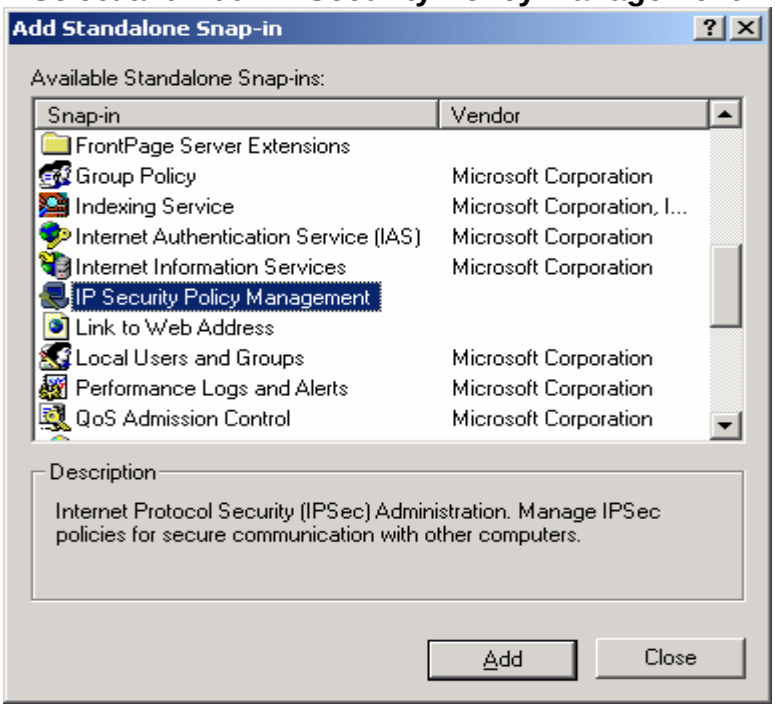
2.Select "**Add/Remove Snap-in**"



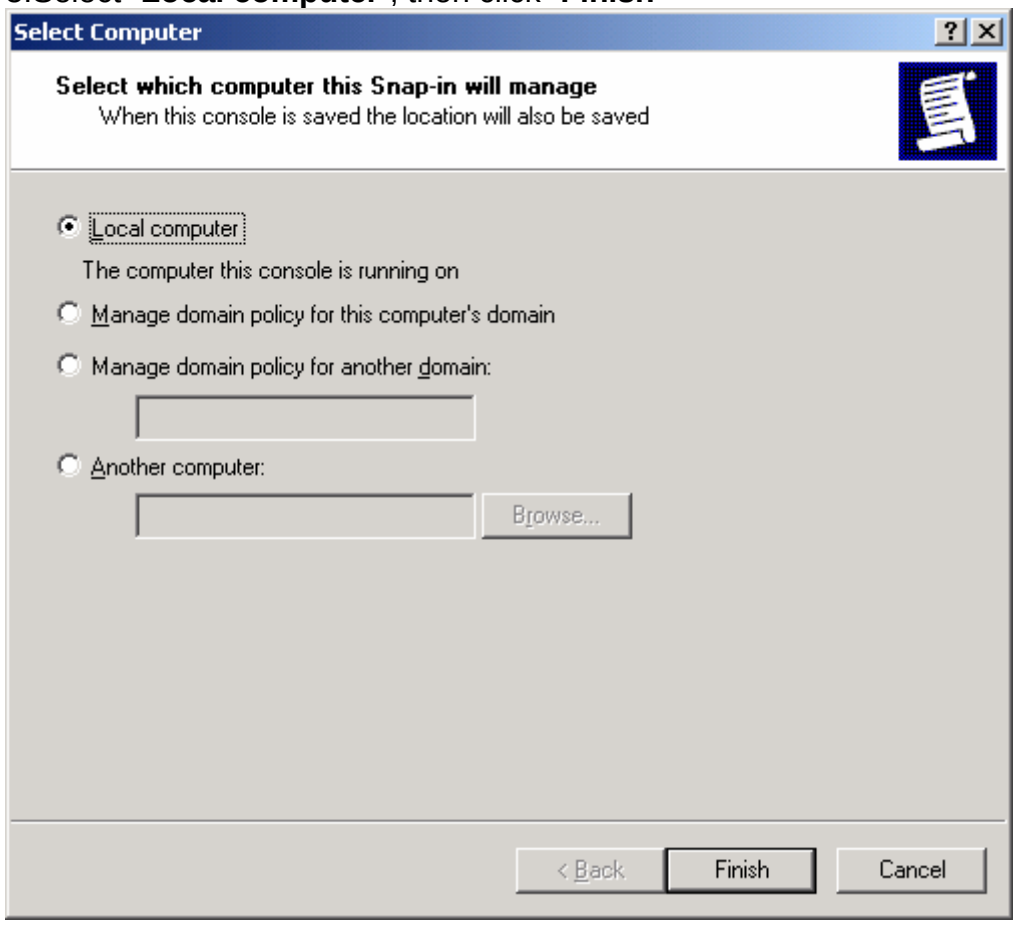
3.Click “**Add**”



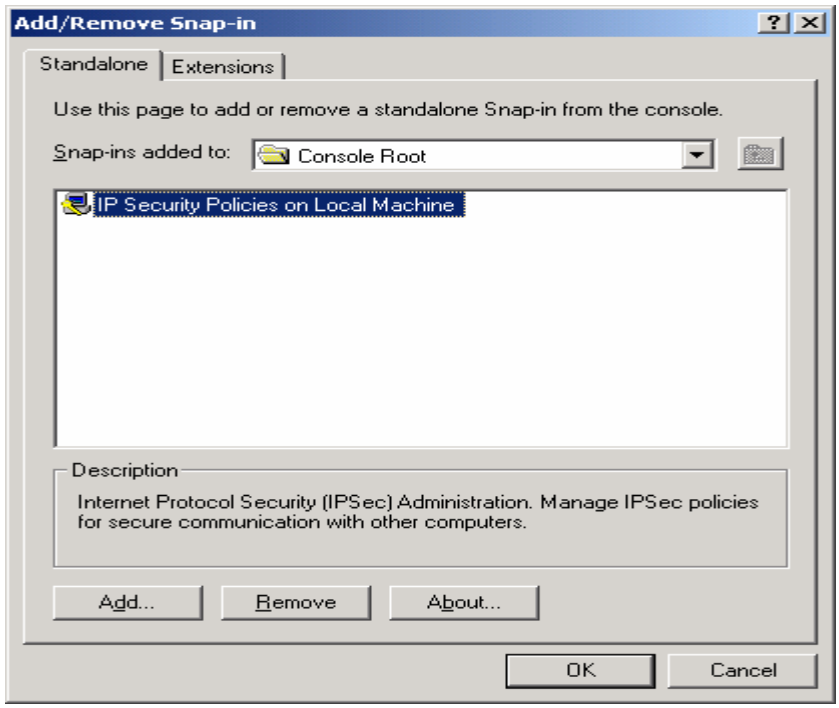
4.Select and Add “**IP Security Policy Management**”



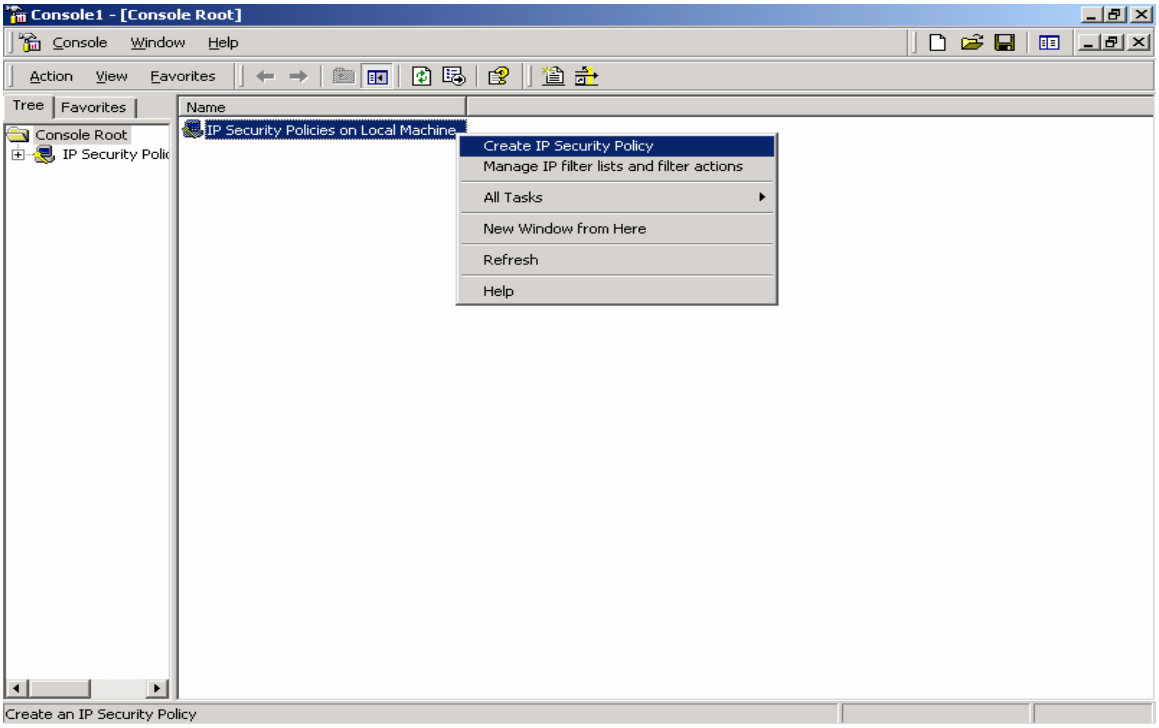
5.Select “**Local computer**”, then click “**Finish**”



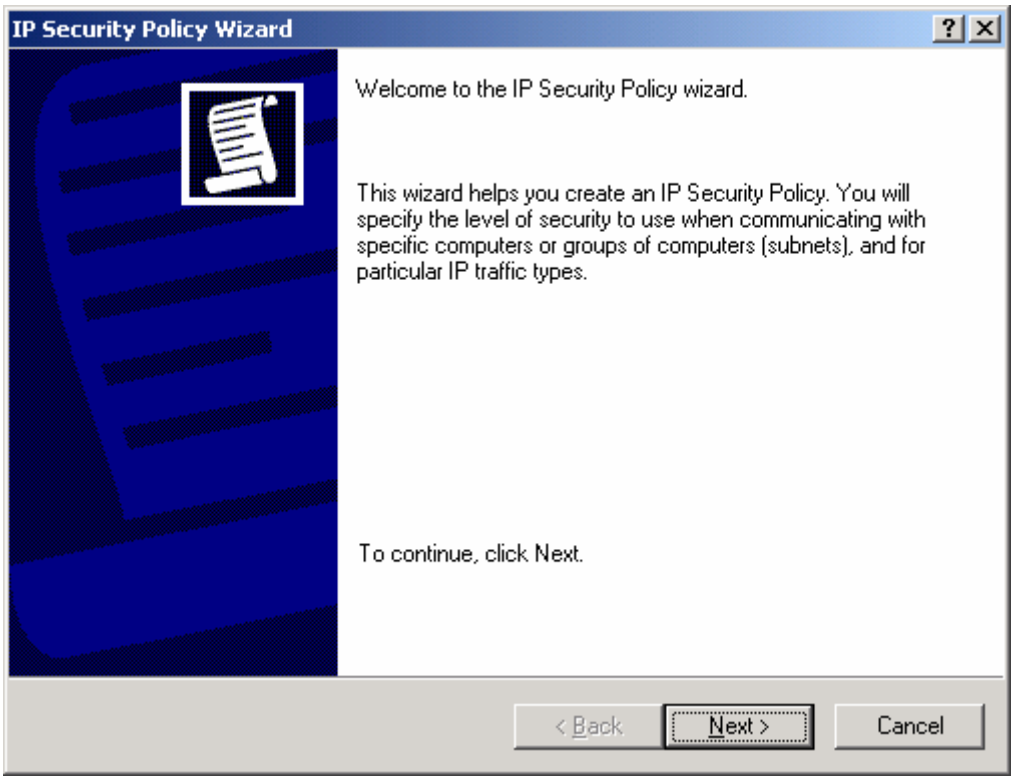
6.Click “**OK**”



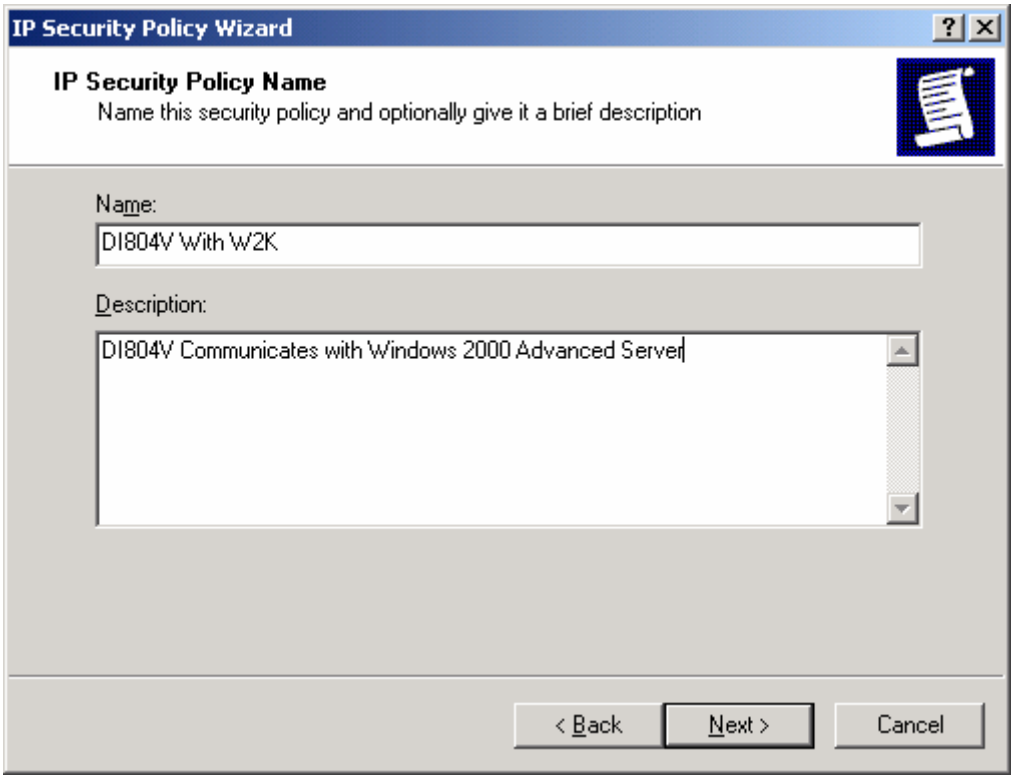
7.Right-click on “**IP Security Policies on Local Machine**” and select “**Create IP Security Policy**”


Console1 - [Console Root]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
IP Security Polic
Name
IP Security Policies on Local Machine
Create IP Security Policy
Manage IP filter lists and filter actions
All Tasks
New Window from Here
Refresh
Help
Create an IP Security Policy

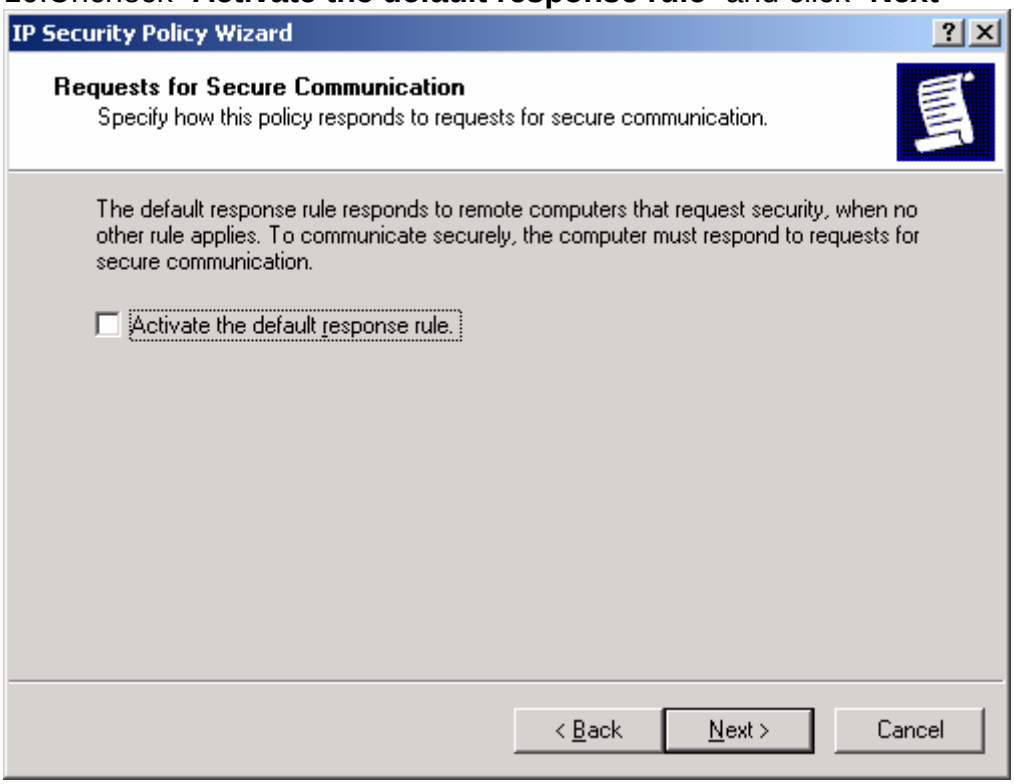
8.Click "**Next**"


IP Security Policy Wizard
Welcome to the IP Security Policy wizard.
This wizard helps you create an IP Security Policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
To continue, click Next.
< Back
Next >
Cancel

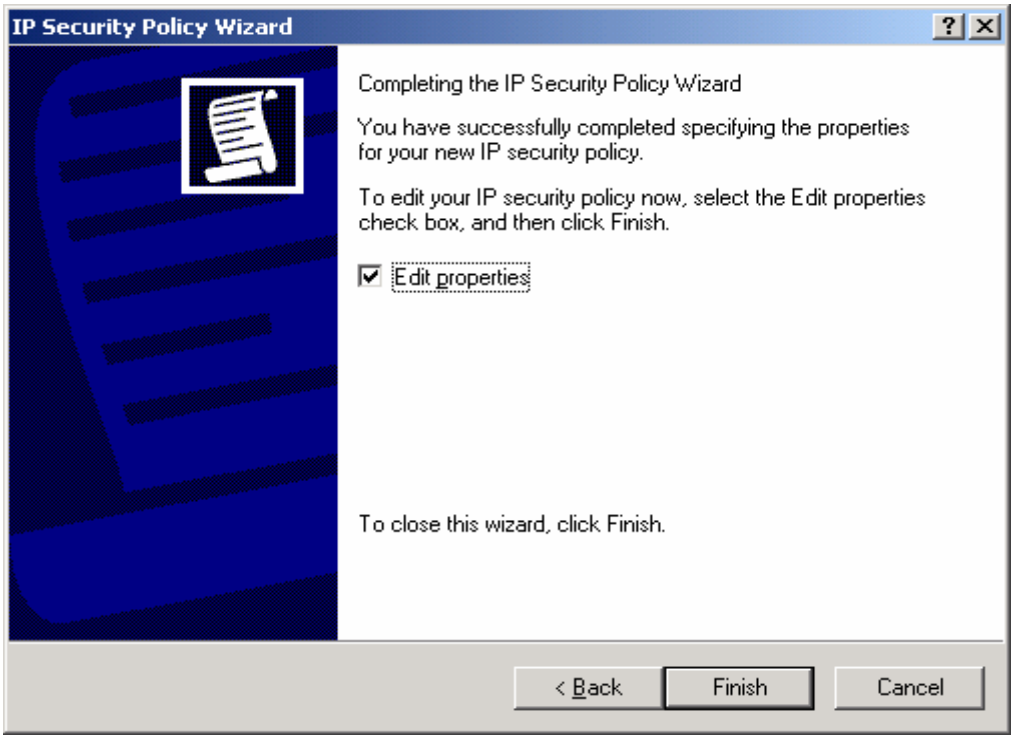
9.Enter the details below and click “**Next**”



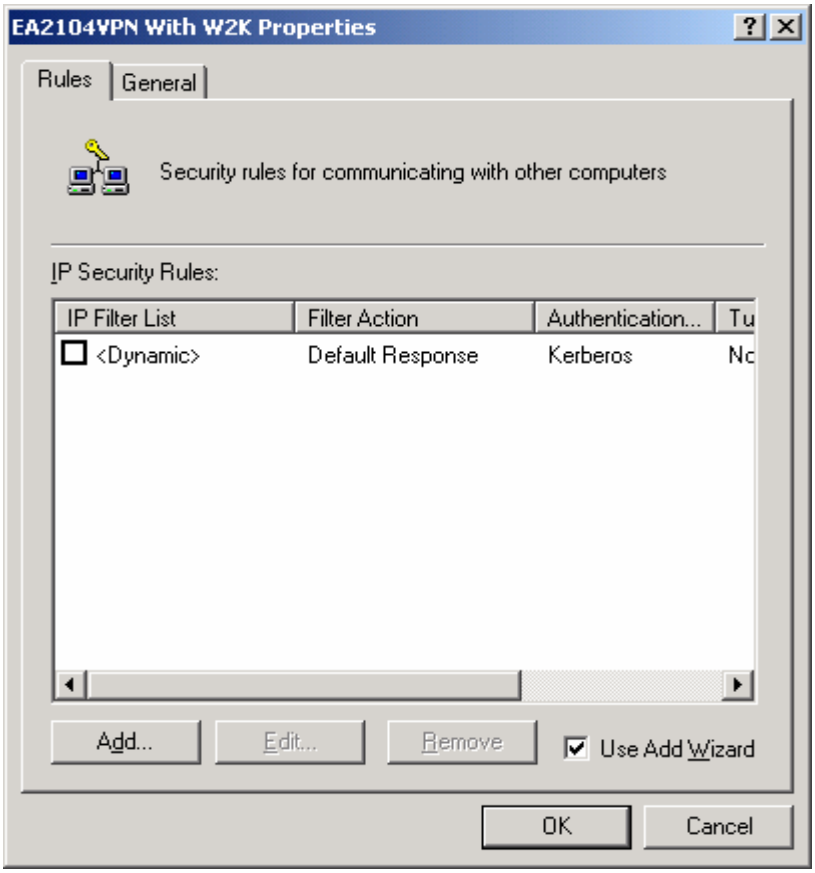
10.Uncheck “**Activate the default response rule**” and click “**Next**”



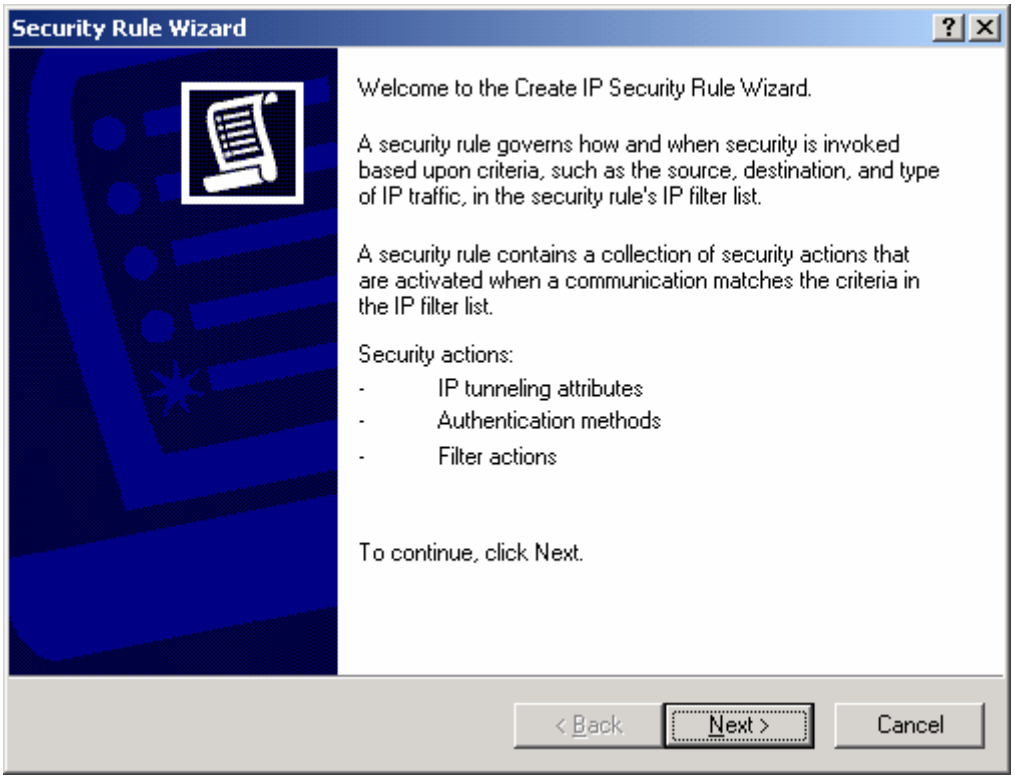
11.Check below and click “**Finish**”



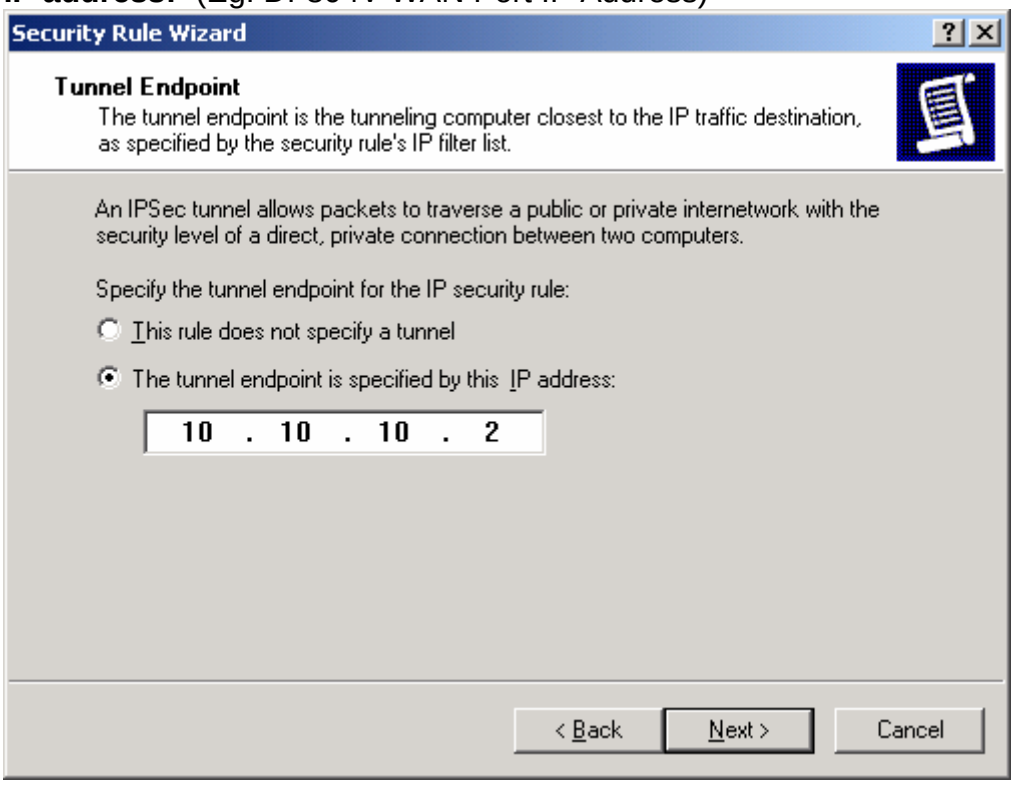
12.Select “**Add**”



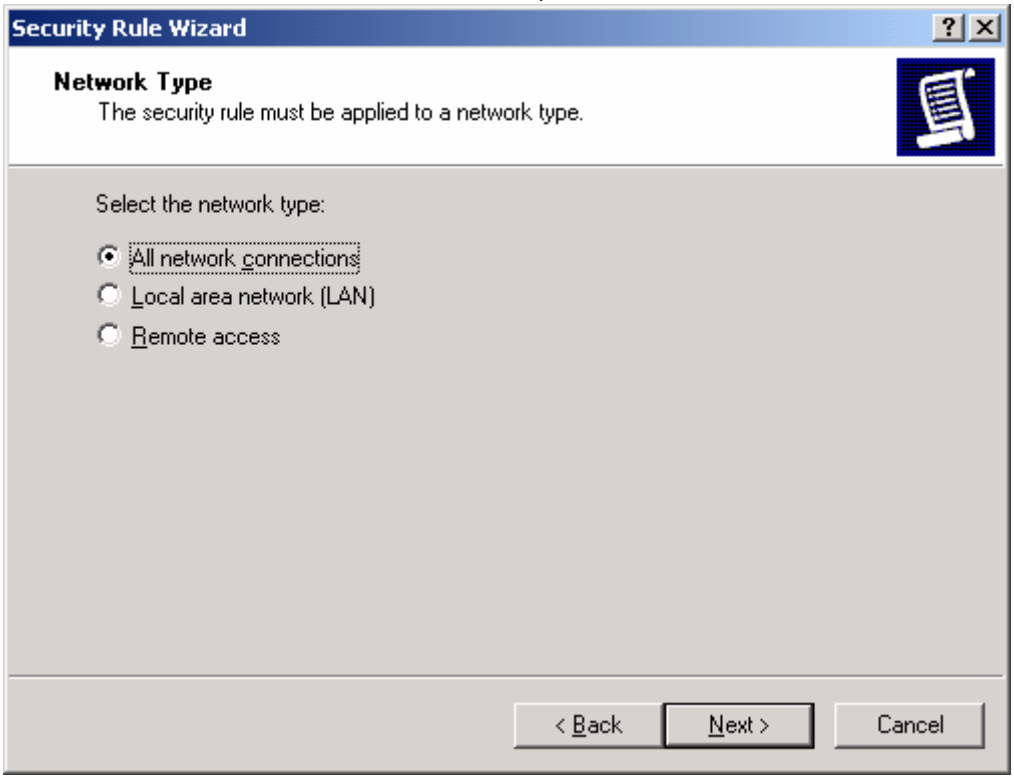
13.Click “Next”



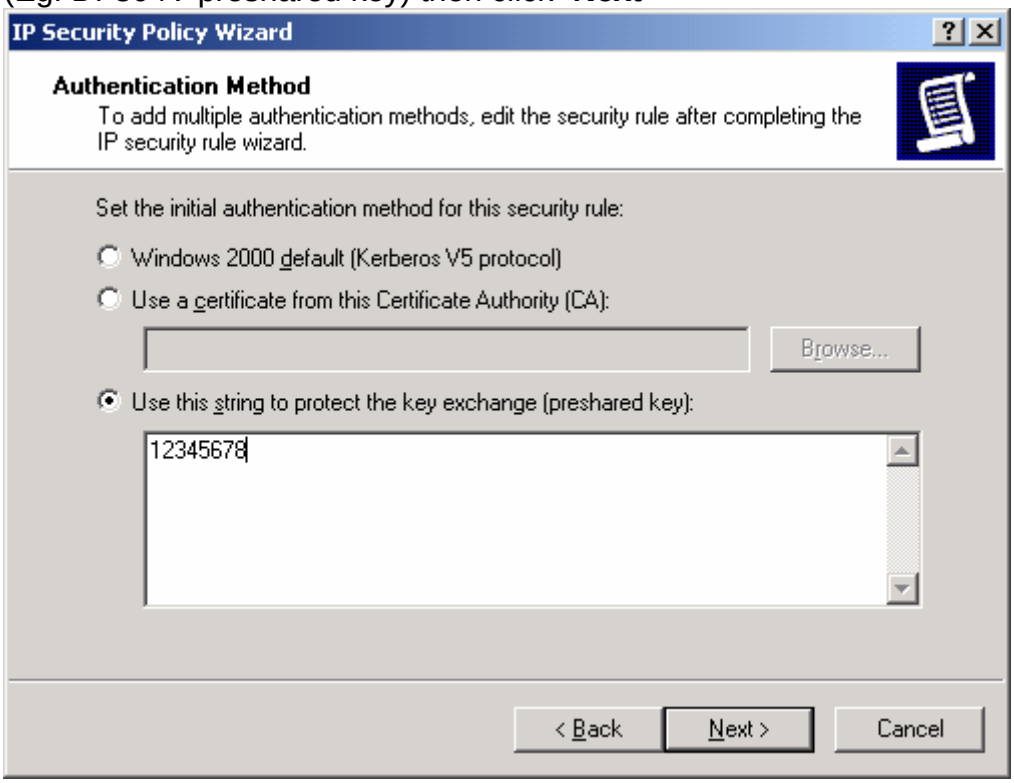
14.Enter the IP Address detail into “**The tunnel endpoint specified by this IP address:**” (Eg. DI-804V WAN Port IP Address)



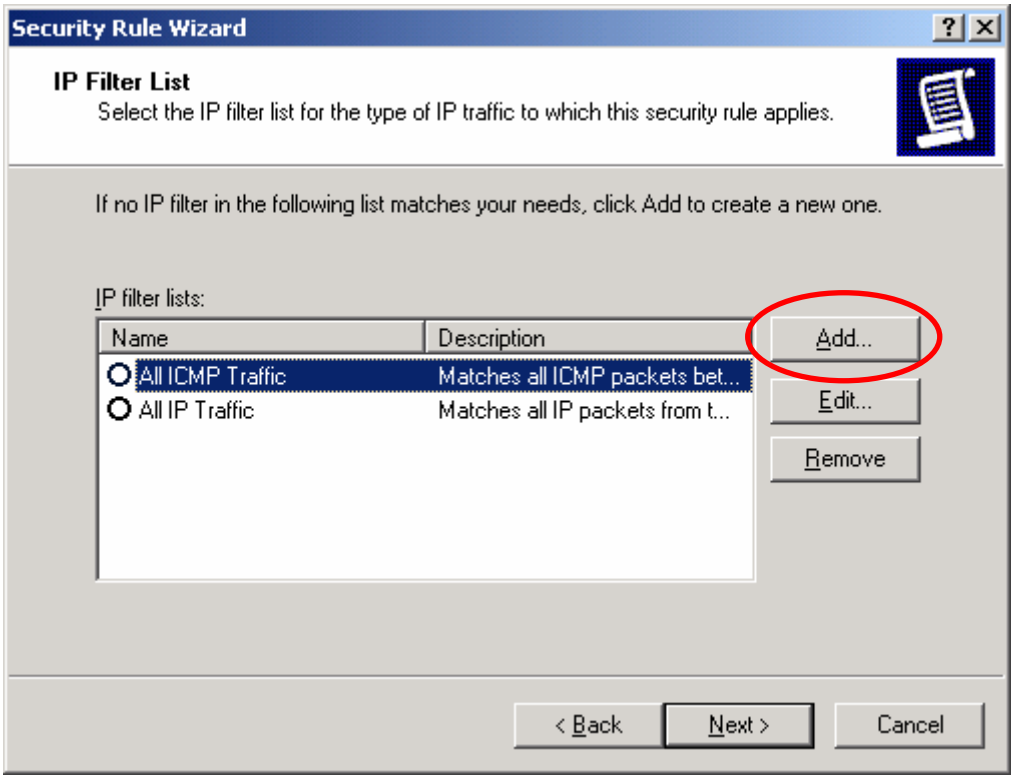
15.Select “**All network connections**”, then click “**Next**”



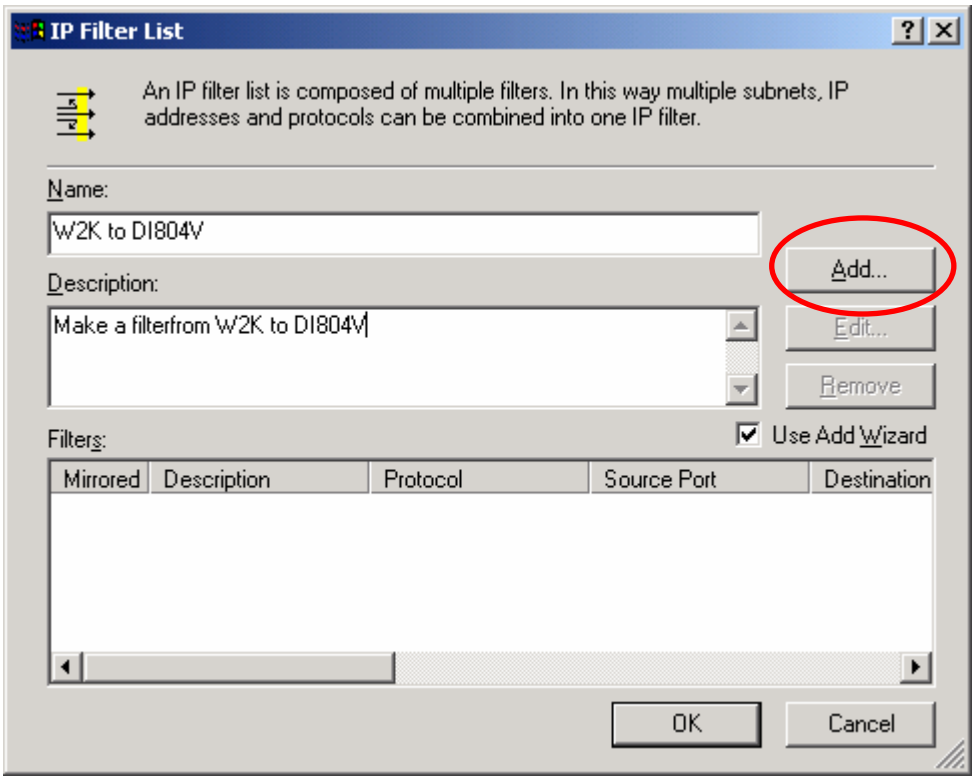
16.Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DI-804V preshared key) then click “**Next**”



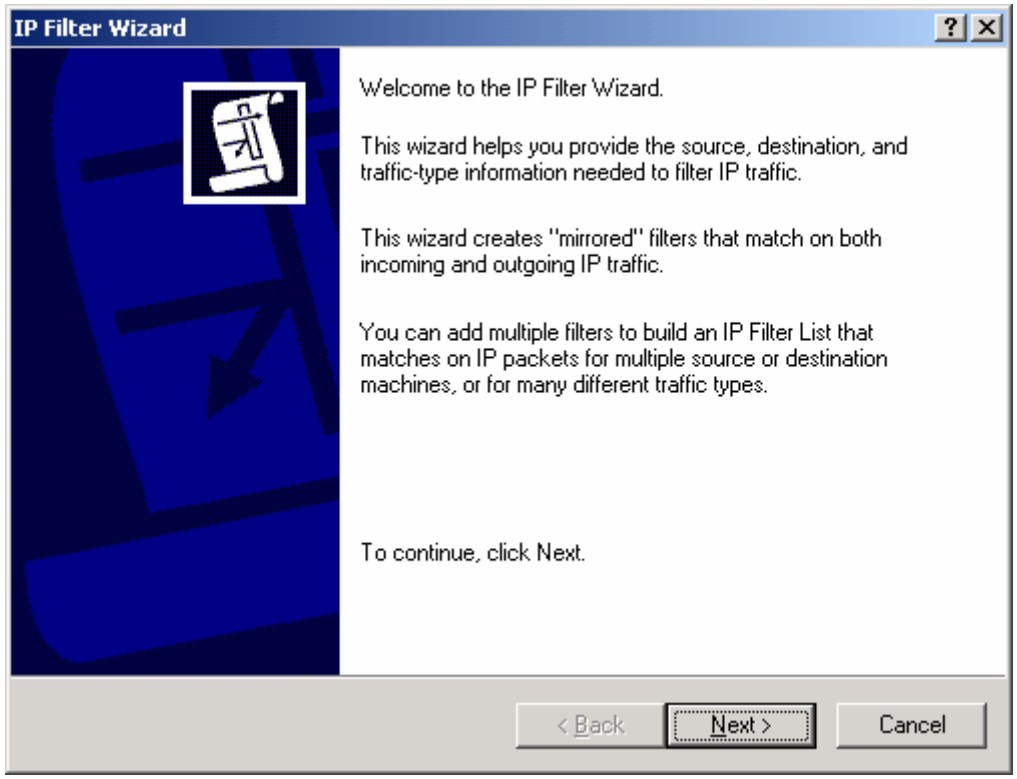
17.Select “**Add**”



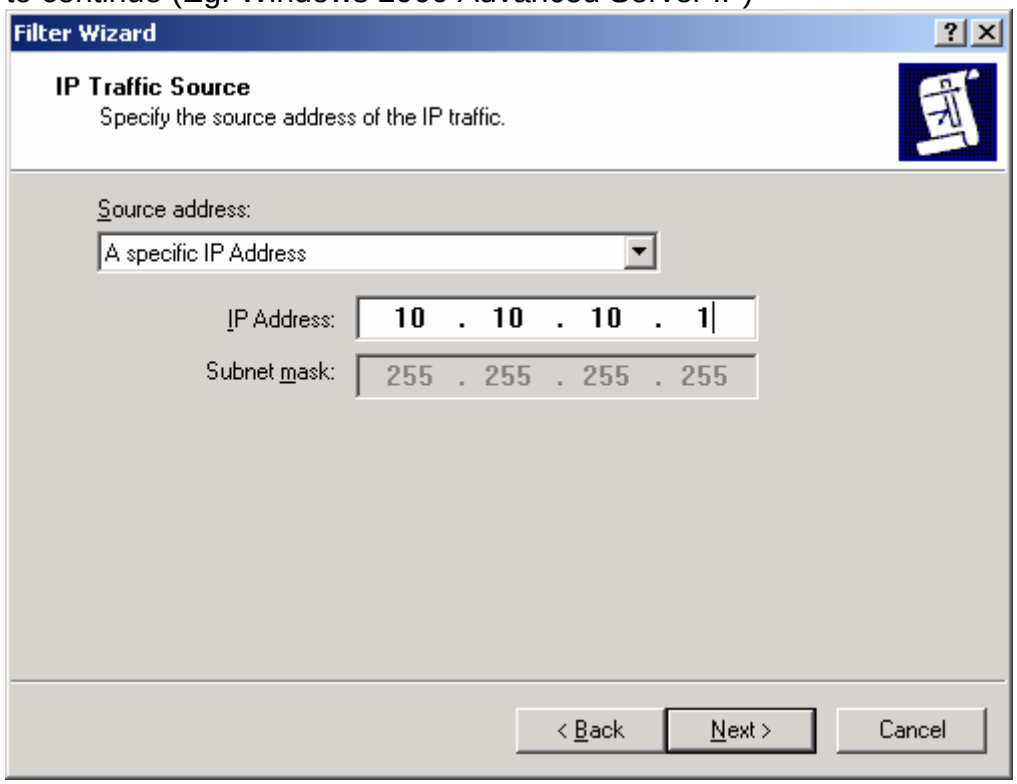
18.Enter a filter name then click “**Add**”



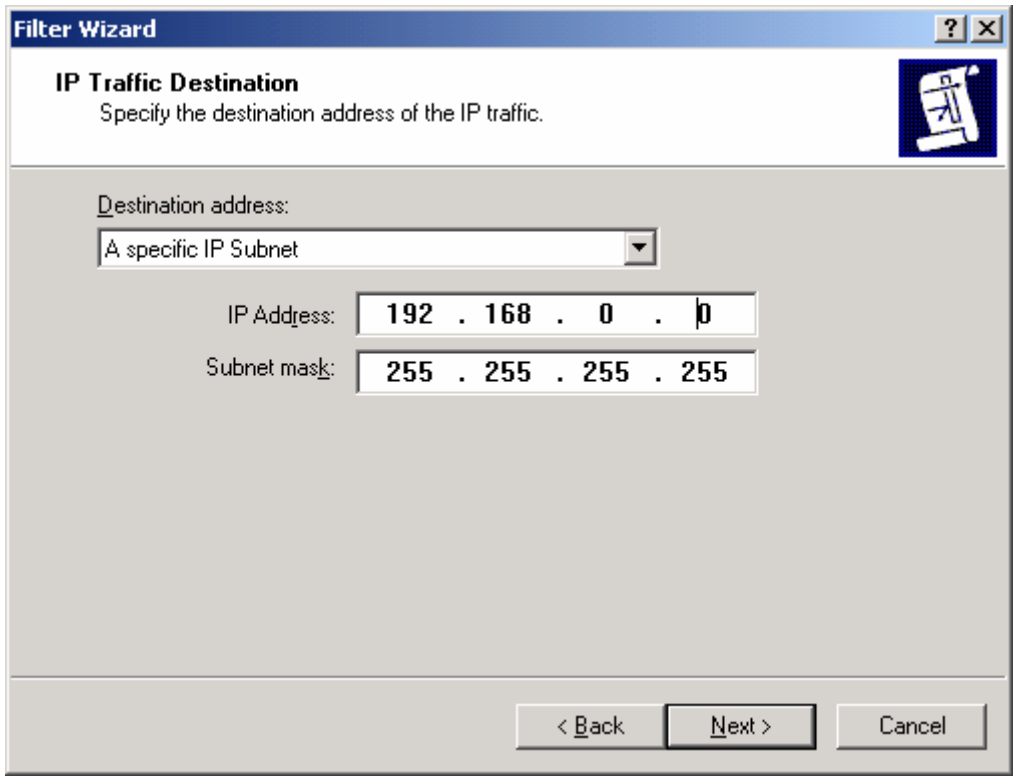
19.Click “**Next**”



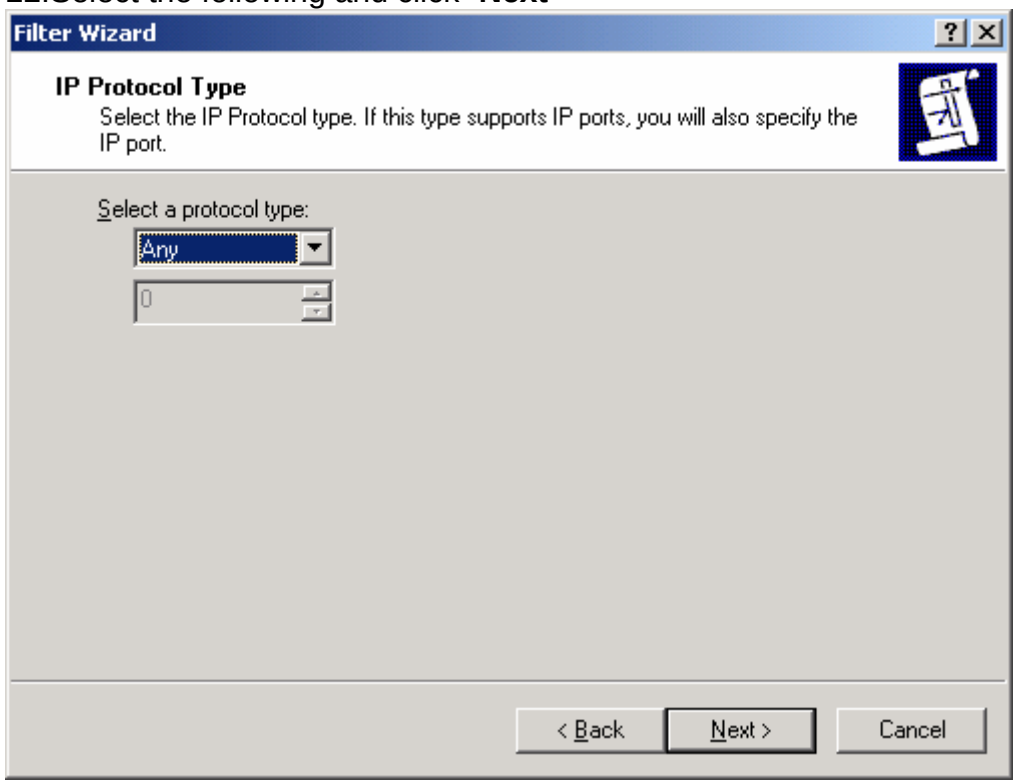
20.Select “**A specific IP Address**” and input the Source address, then “**Next**” to continue (Eg. Windows 2000 Advanced Server IP)



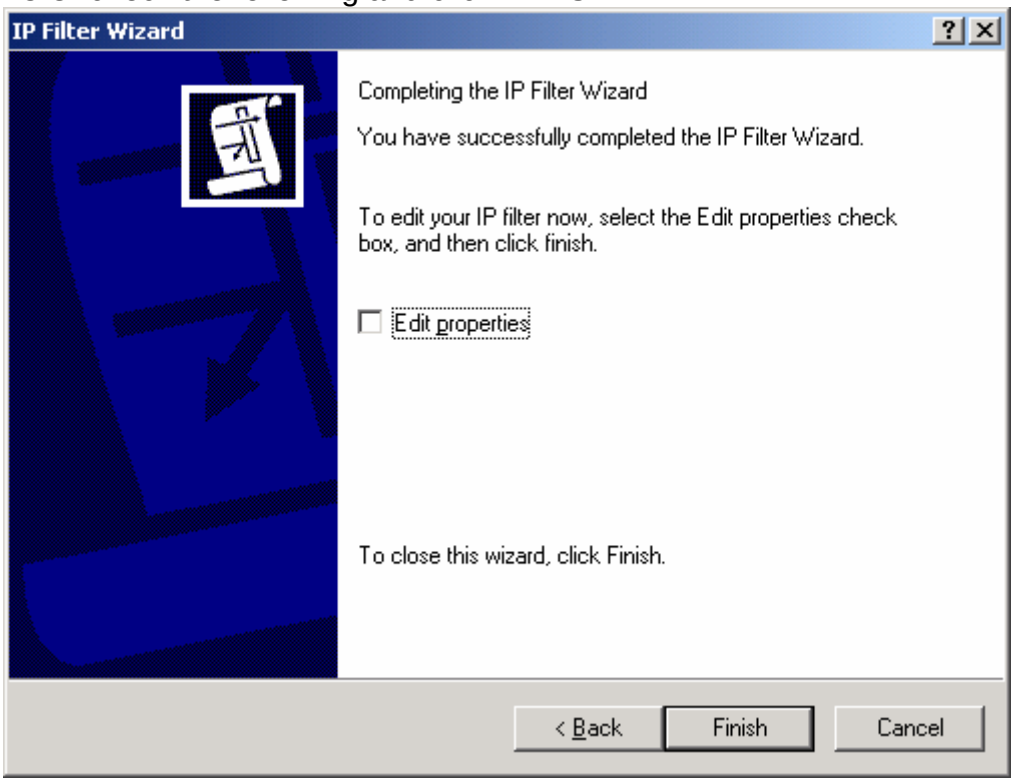
21. Select “**A specific IP Subnet**” and input the Destination subnet address, then “**Next**” to continue (Eg. DI-804V Private network)



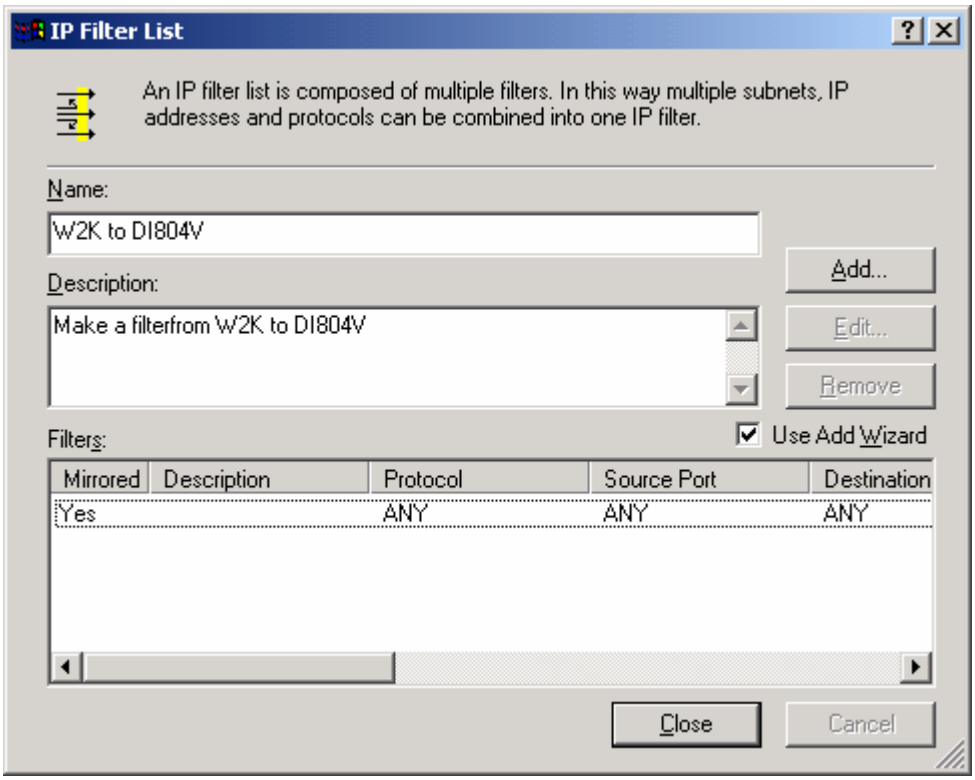
22.Select the following and click “**Next**”



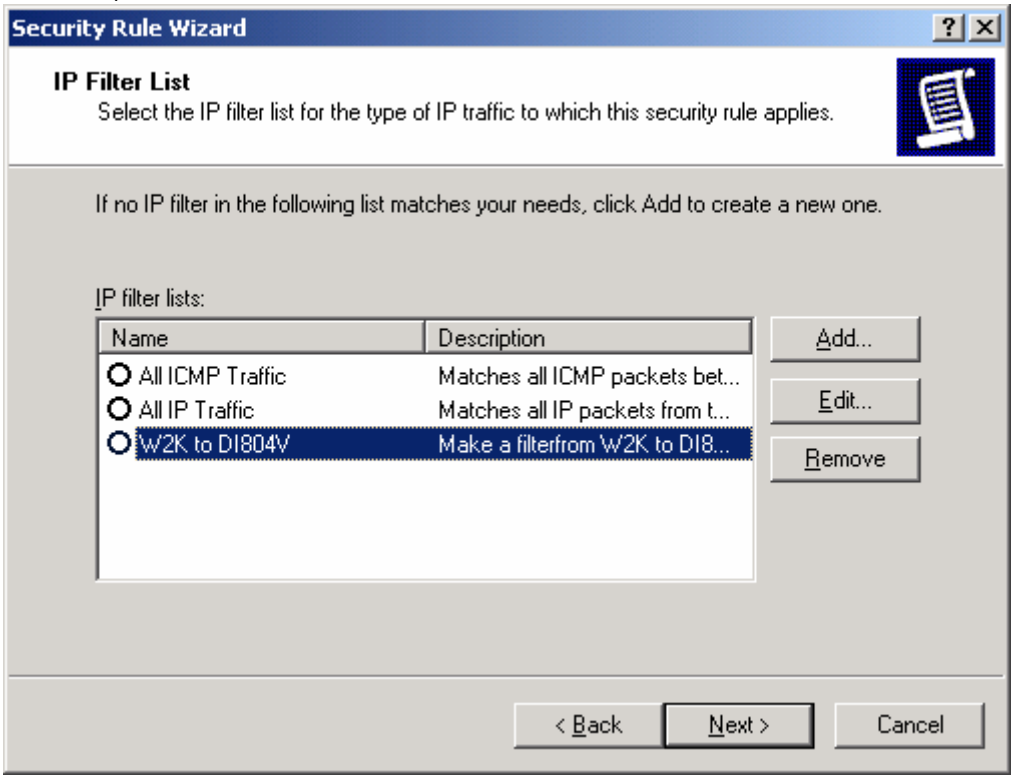
23.Uncheck the following and click “**Finish**”



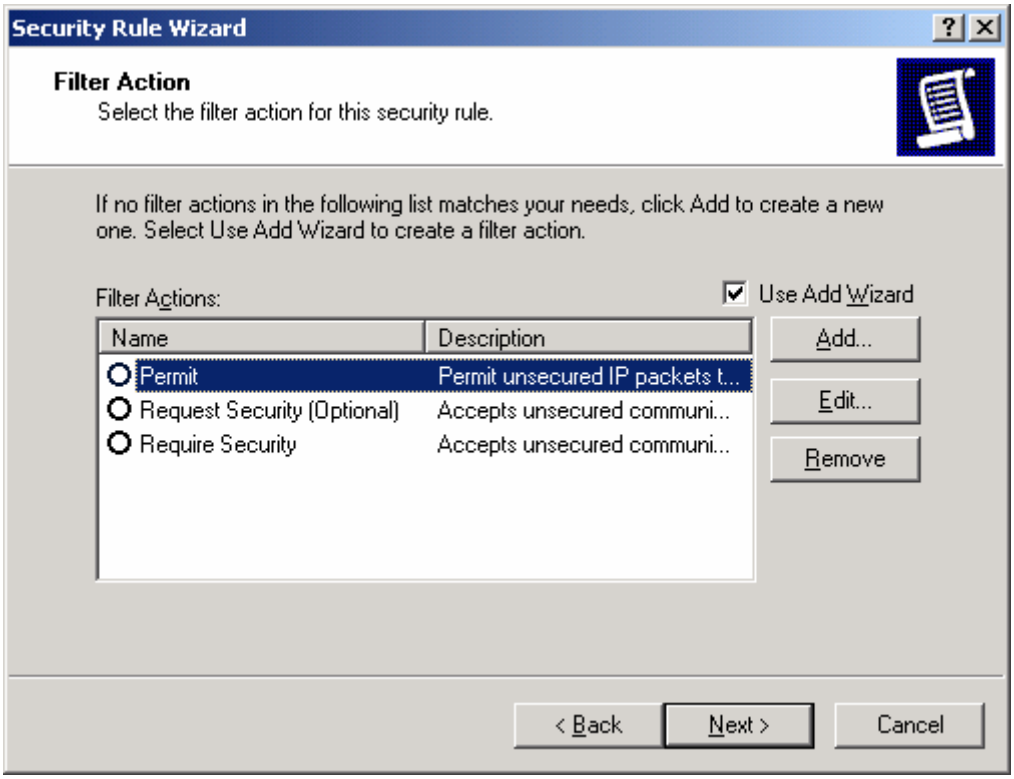
24.Click “**Close**”



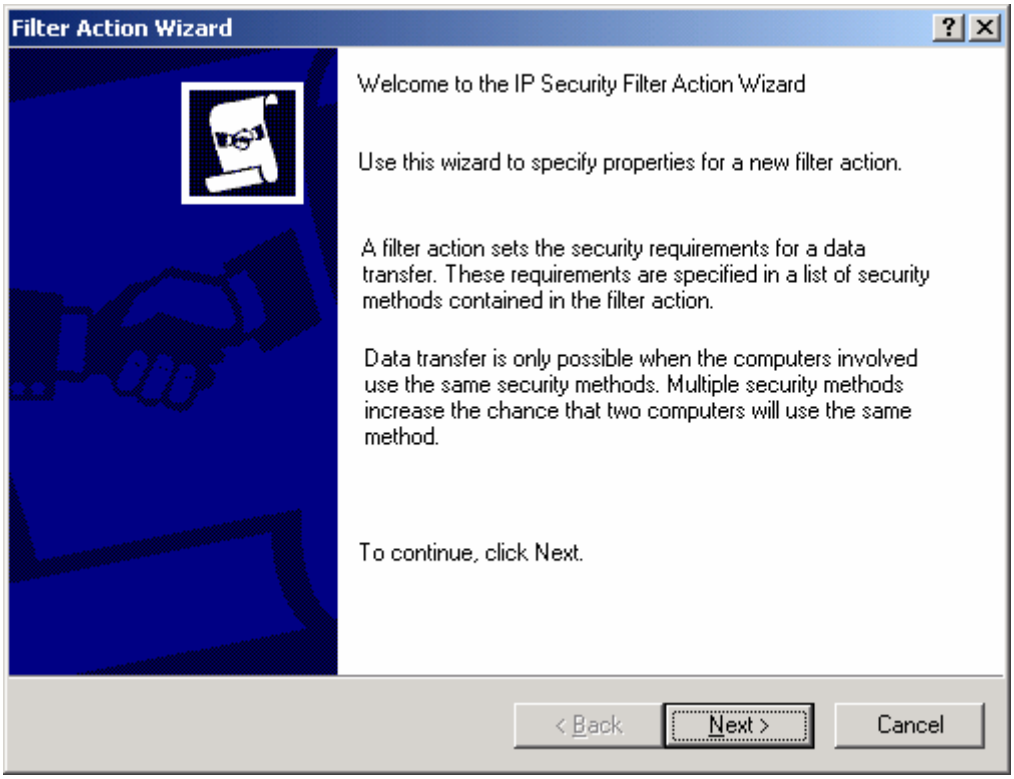
25.Now, select “**W2K to DI-804V**” then click “**Next**”



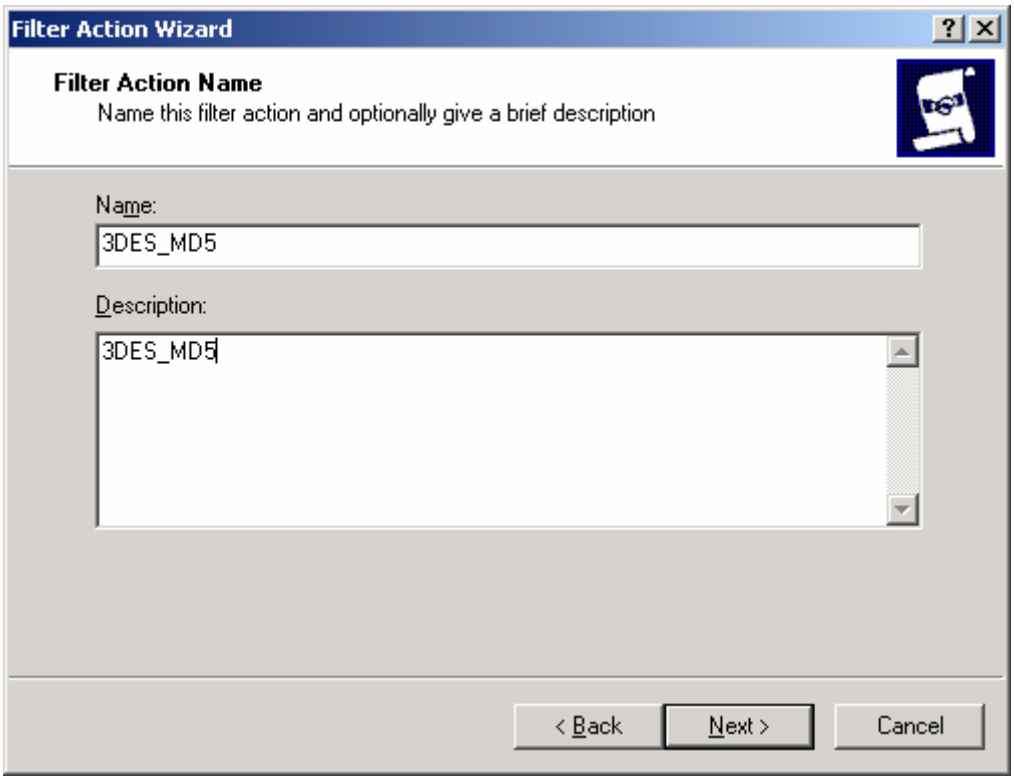
26.Click “**Add**”



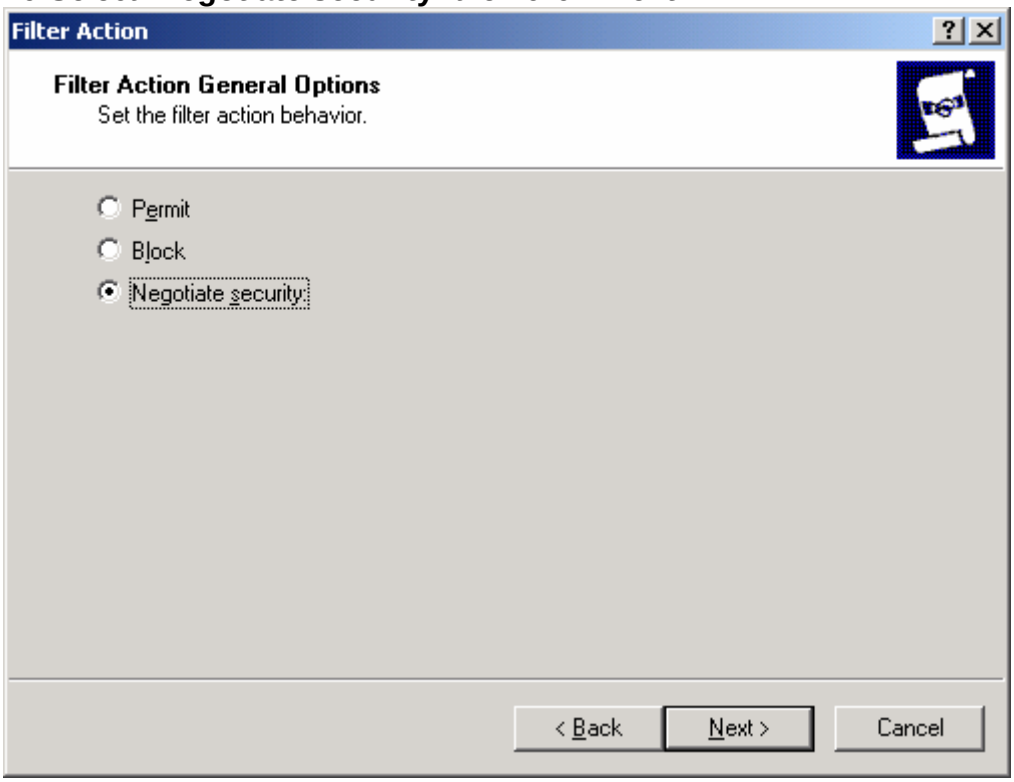
27.Click “**Next**”



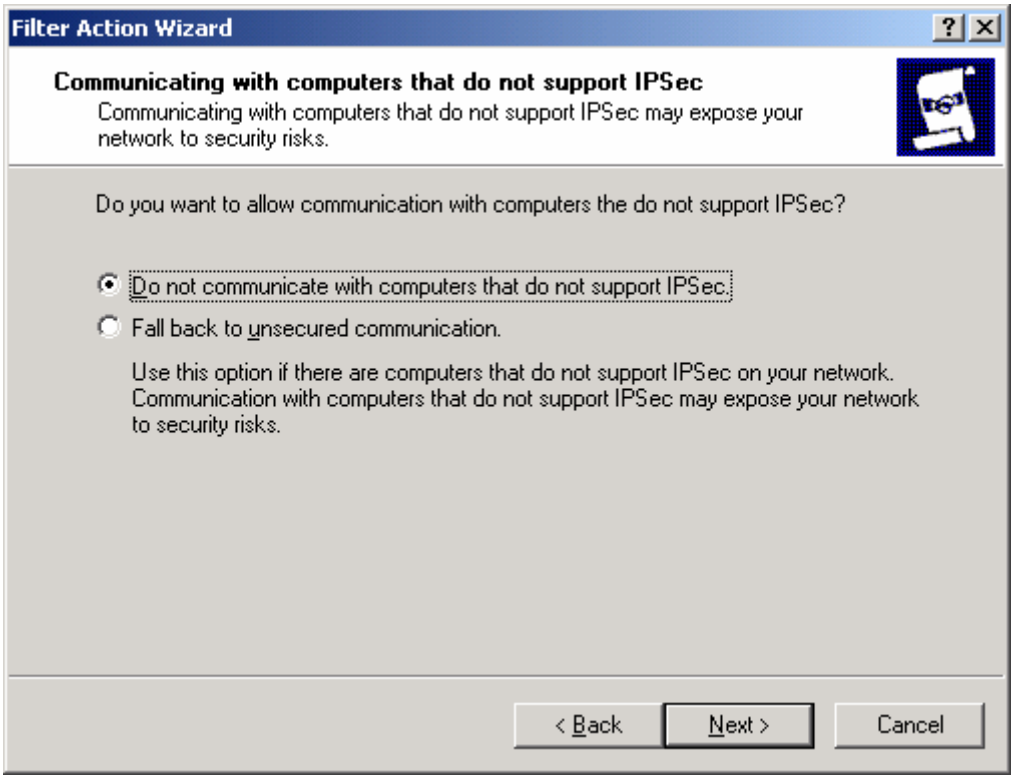
28. Enter a filter action name then click “**Next**”



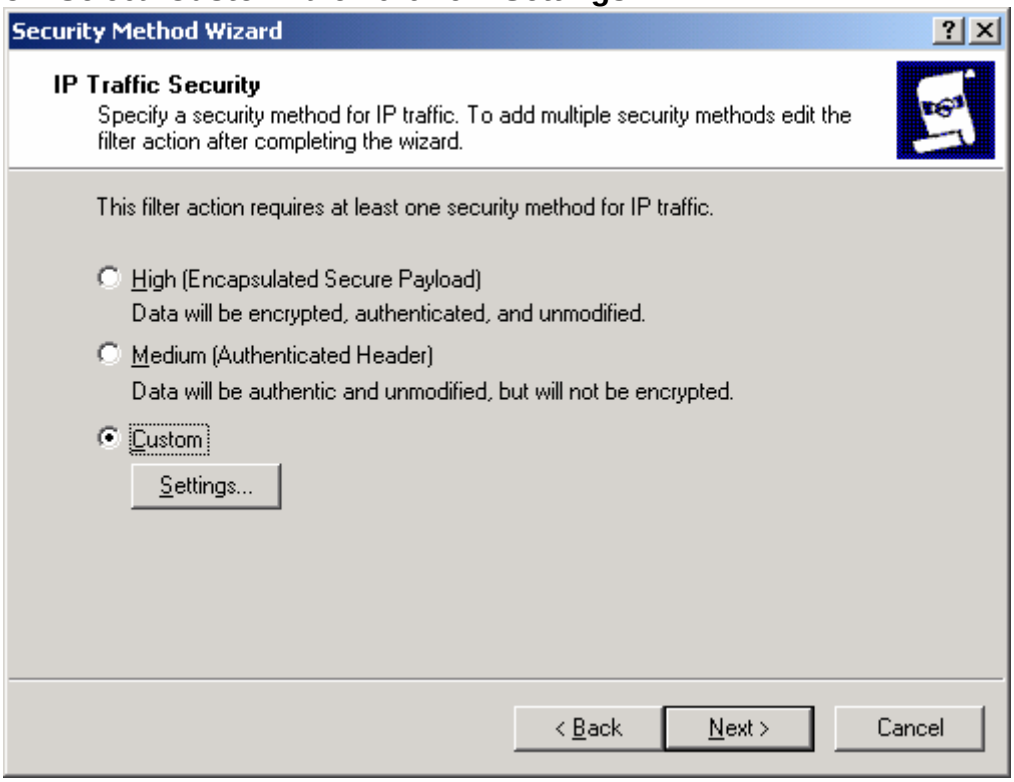
29.Select “**Negotiate security**” then click “**Next**’



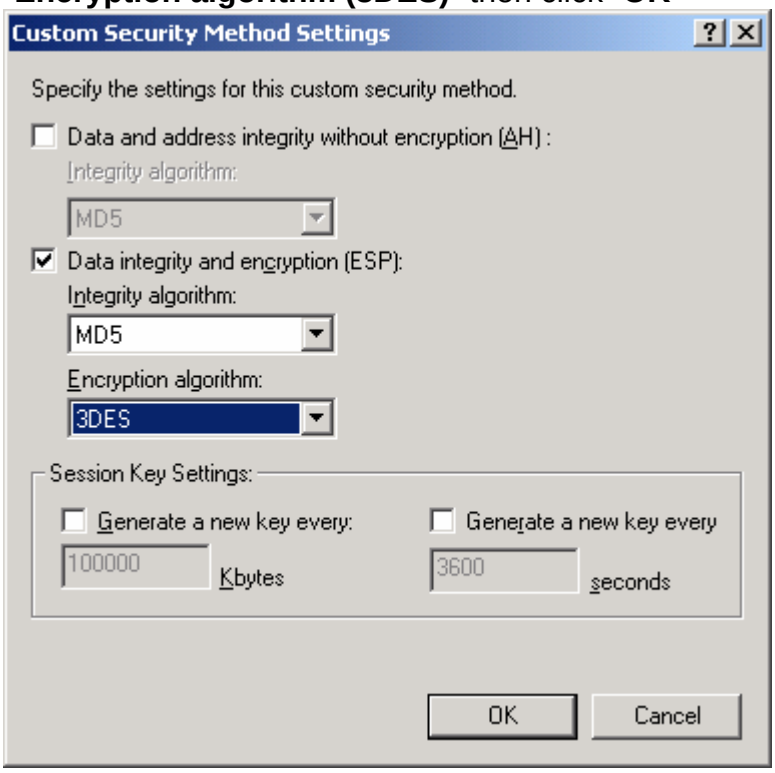
30.Select “**Do not communicate with computer that do not support IPSec**” then click “**Next**”



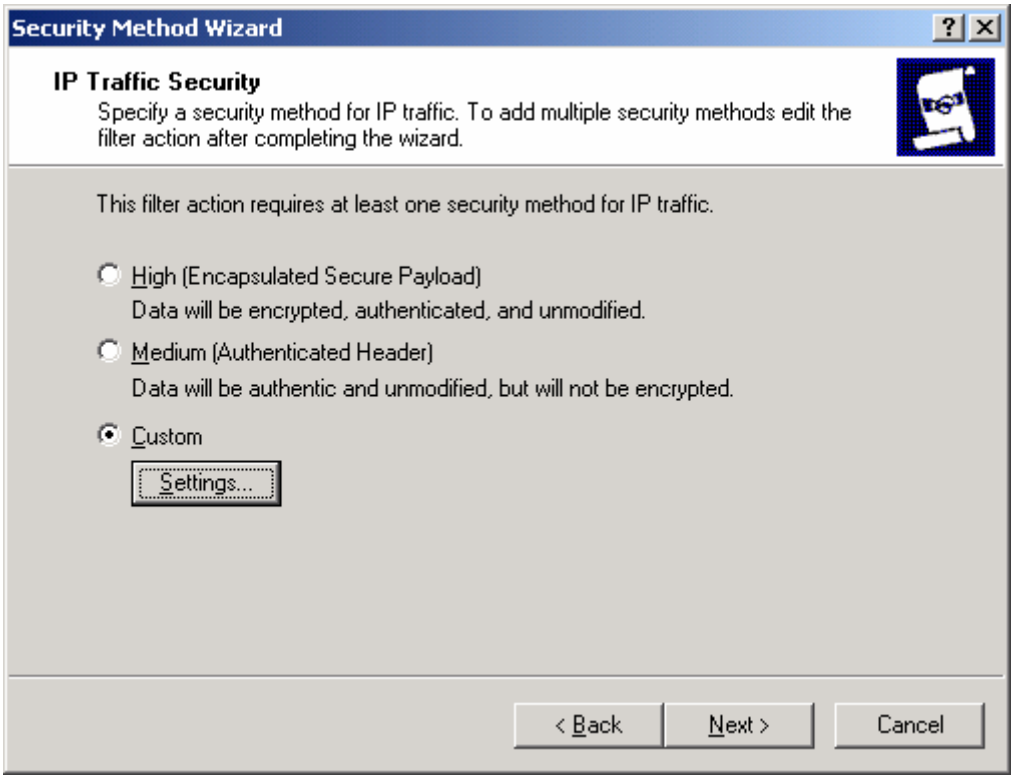
31. Select “**Custom**” then click on “**Settings**”



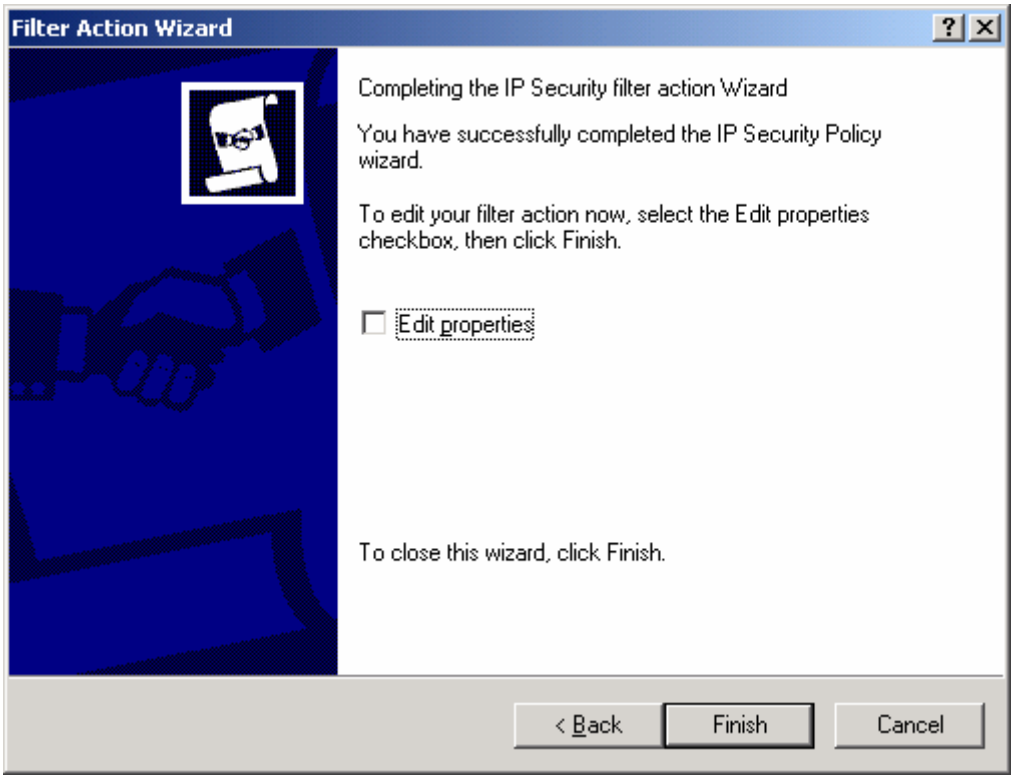
32.Check “**Data integrity and encryption (ESP)**”, select the “**Integrity algorithm (MD5)**” and
“**Encryption algorithm (3DES)**” then click “**OK**”



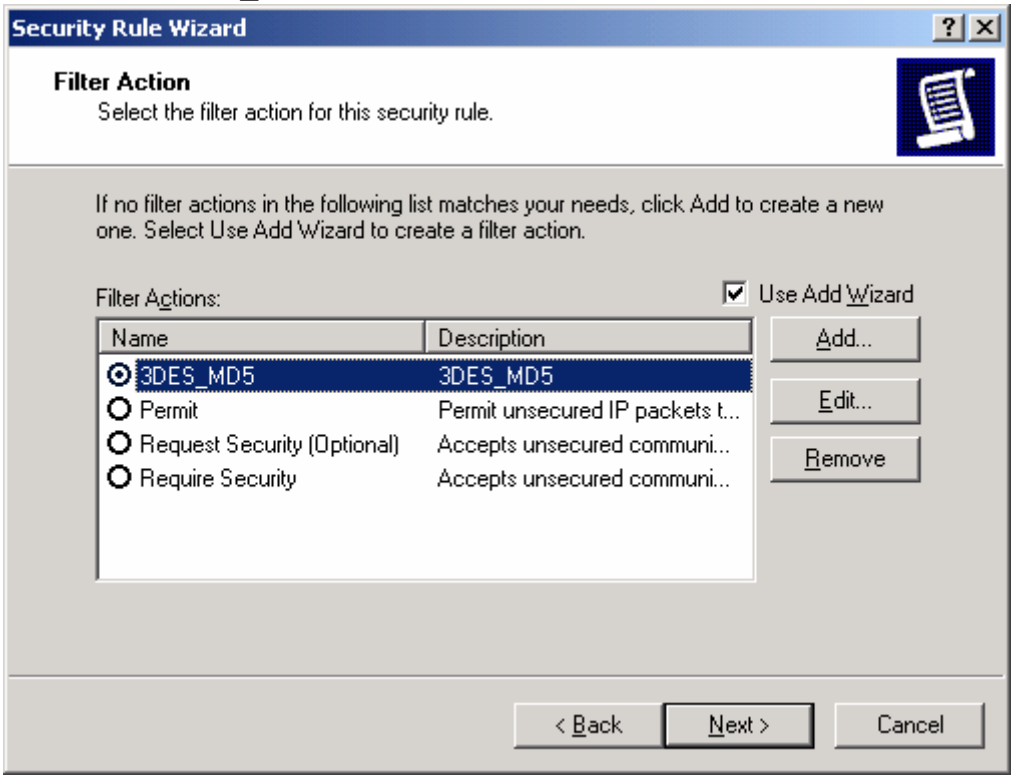
33.Click “**Next**”



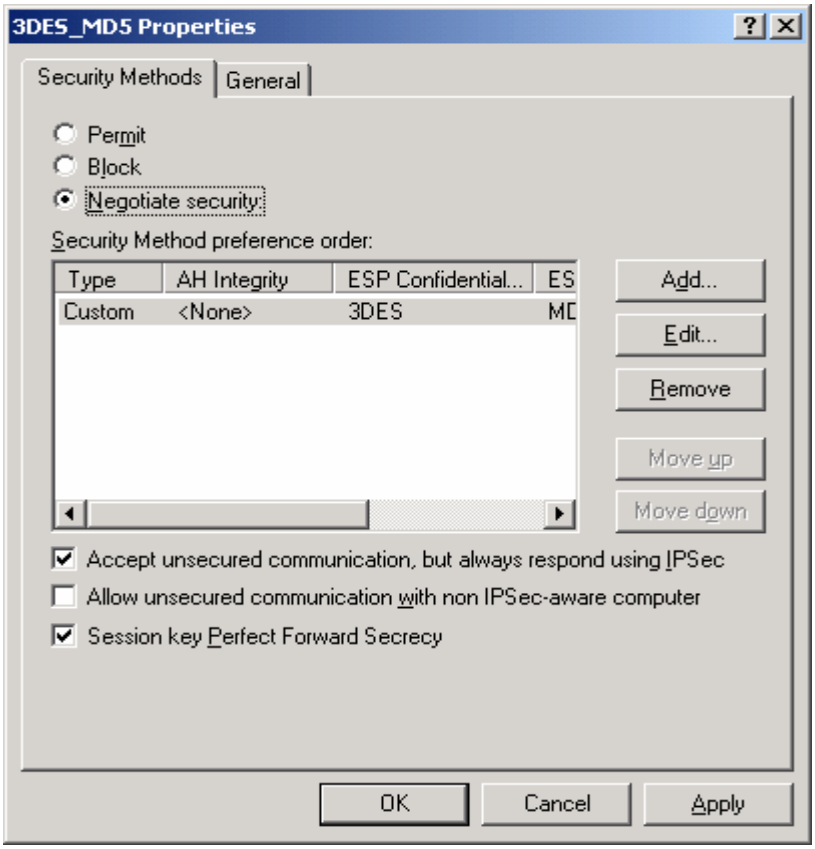
34.Click “**Finish**”



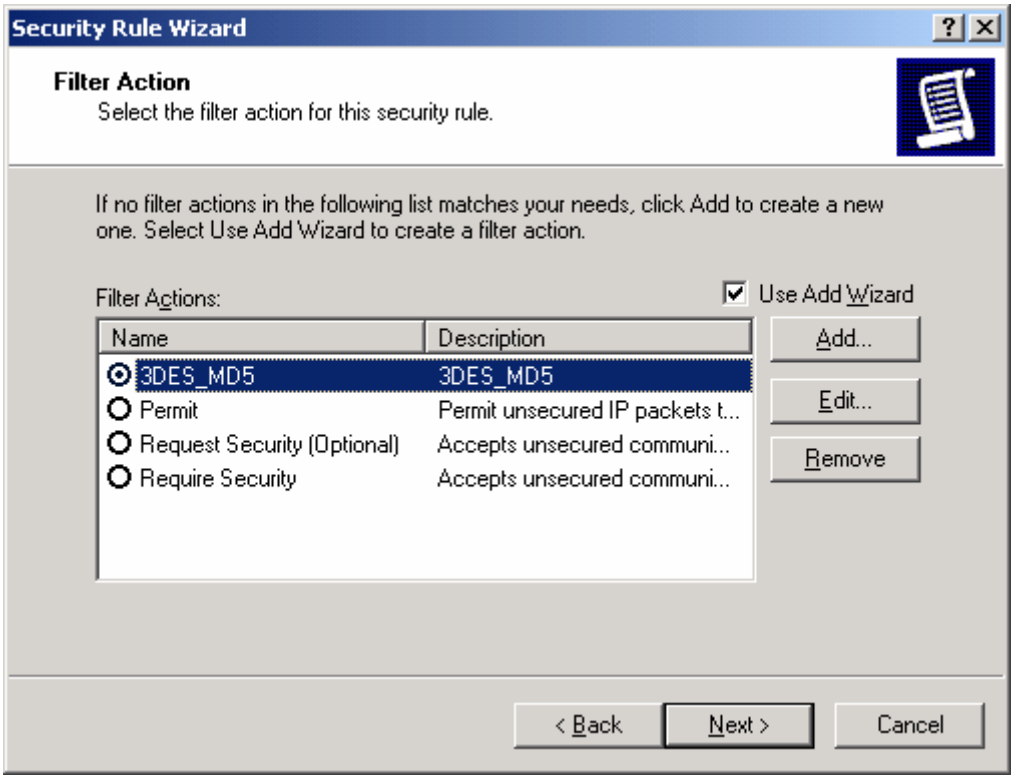
35.Select “**3DES_MD5**” then click “**Edit**”



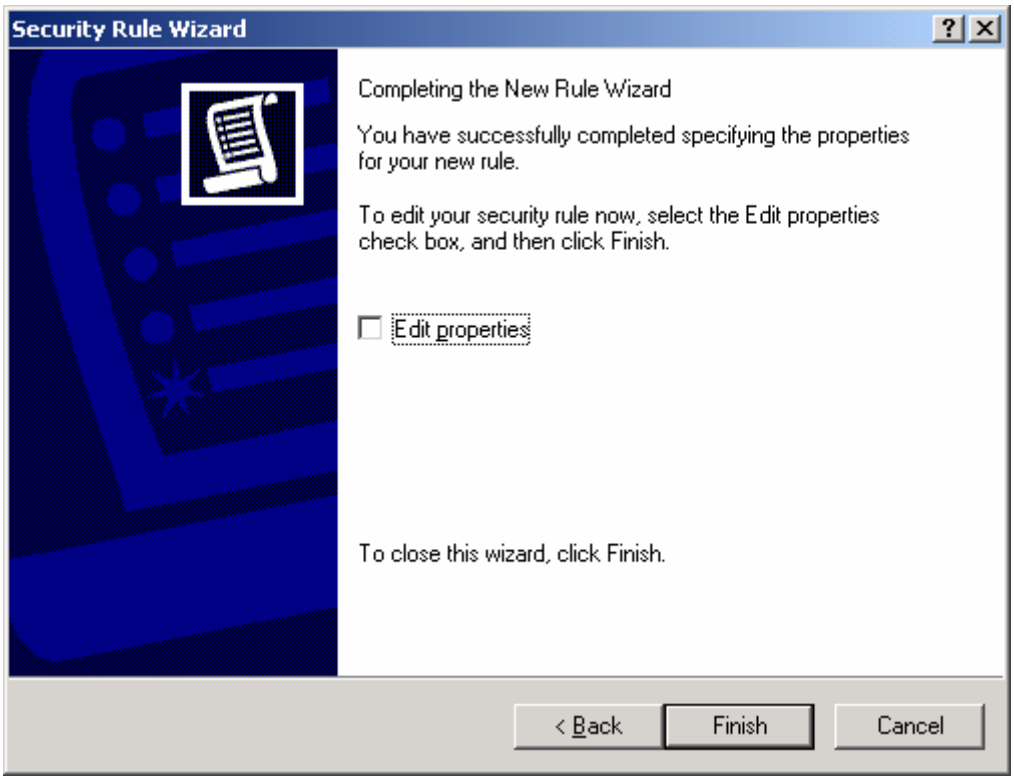
36.Select the following and check “**Session key Perfect Forward Secrecy**” then click “**OK**”



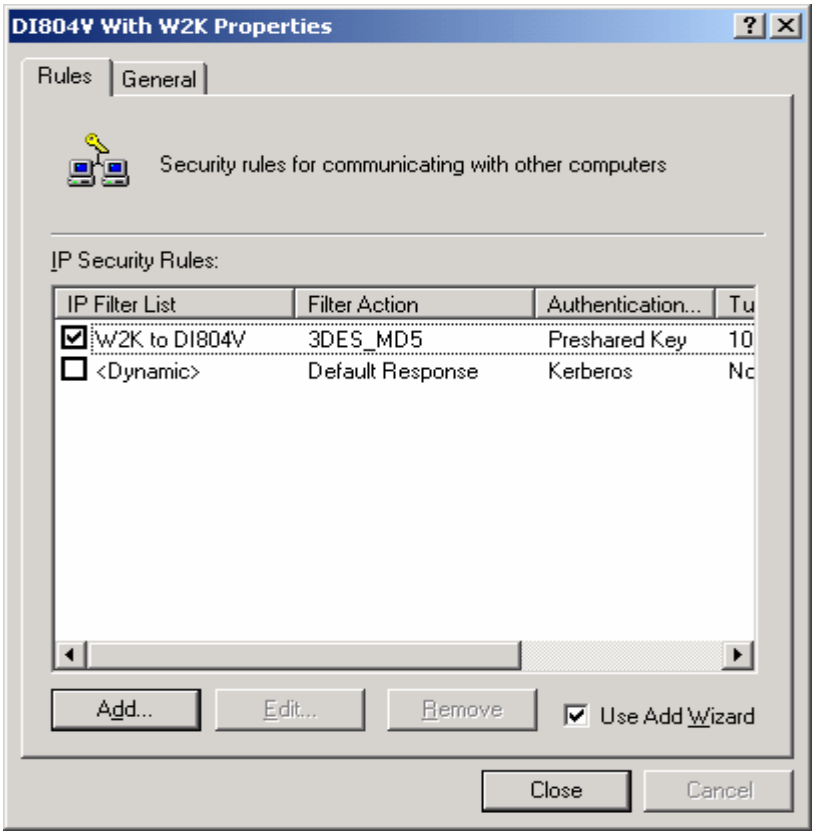
37.Click “**Next**”



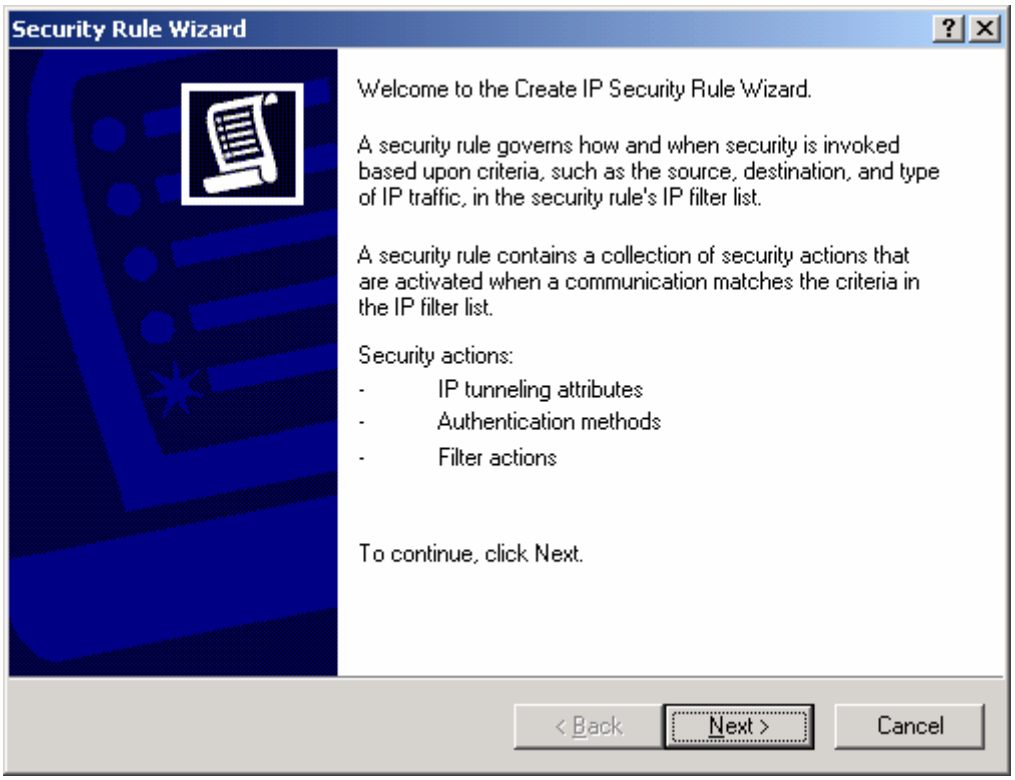
38.Click “**Finish**’



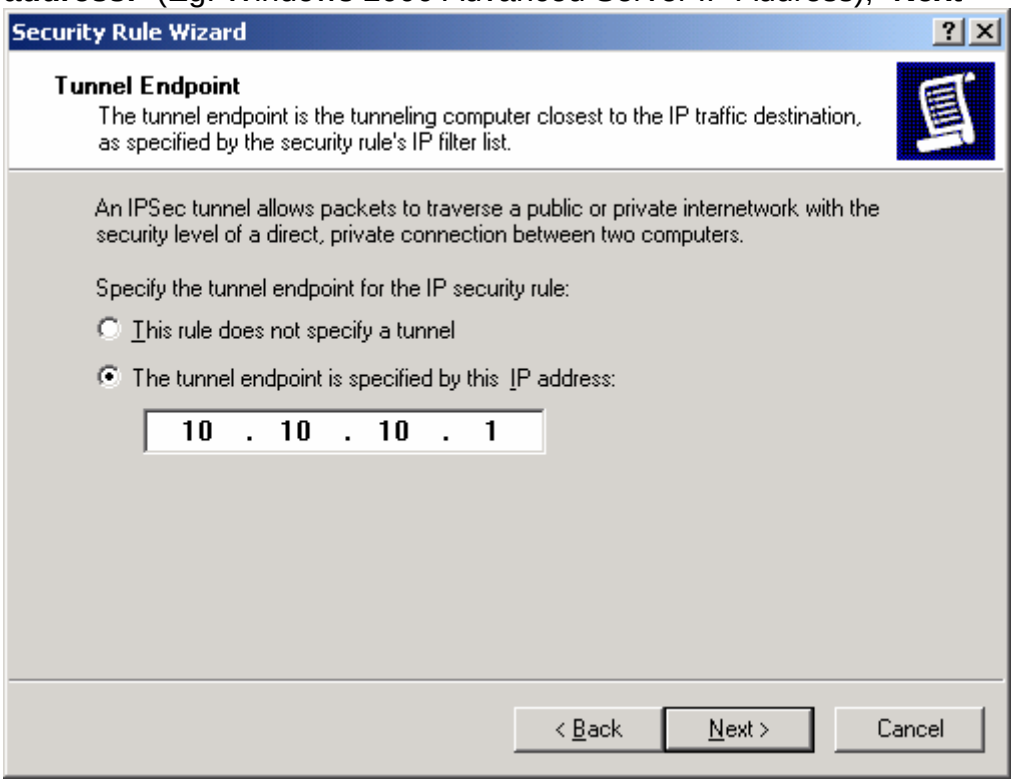
39.Click “**Add**”



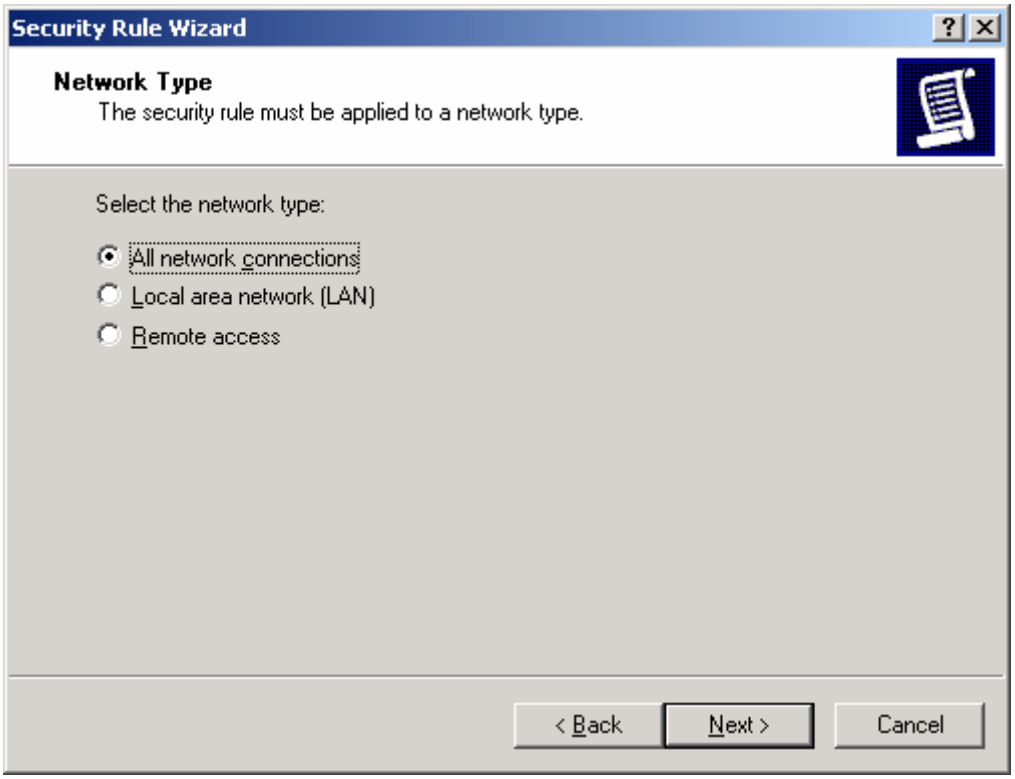
40.Click “**Next**”



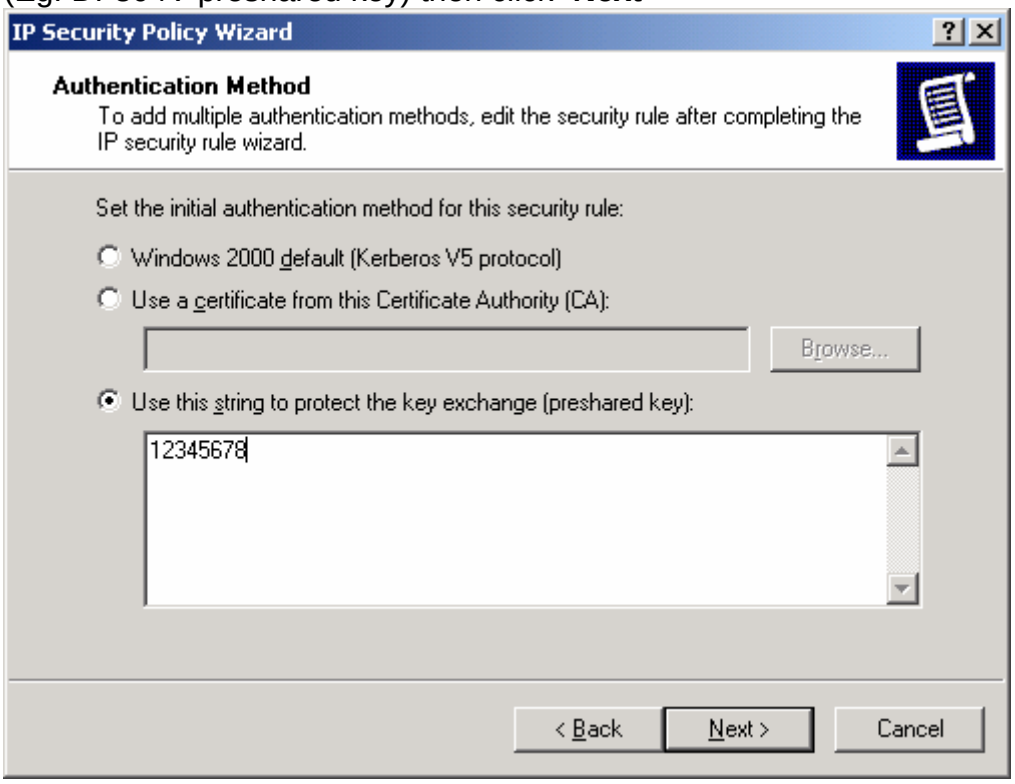
41. Input the IP Address into “**The tunnel endpoint specified by this IP address:**” (Eg. Windows 2000 Advanced Server IP Address), “**Next**”



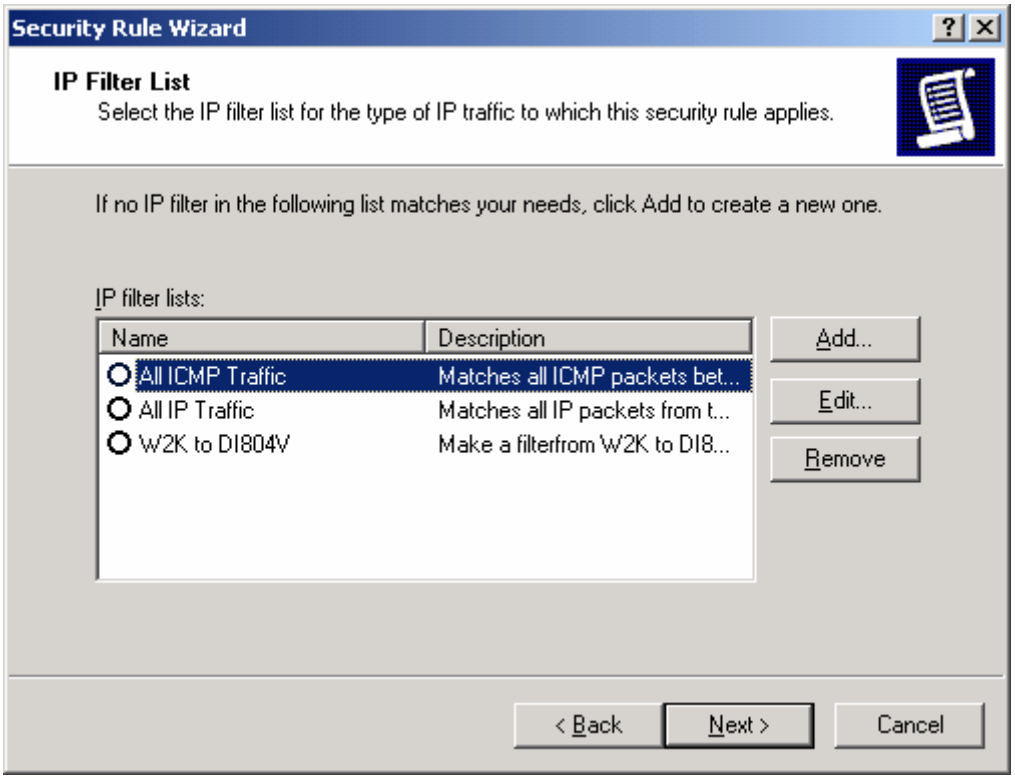
42. Select “**All network connections**” then click “**Next**”



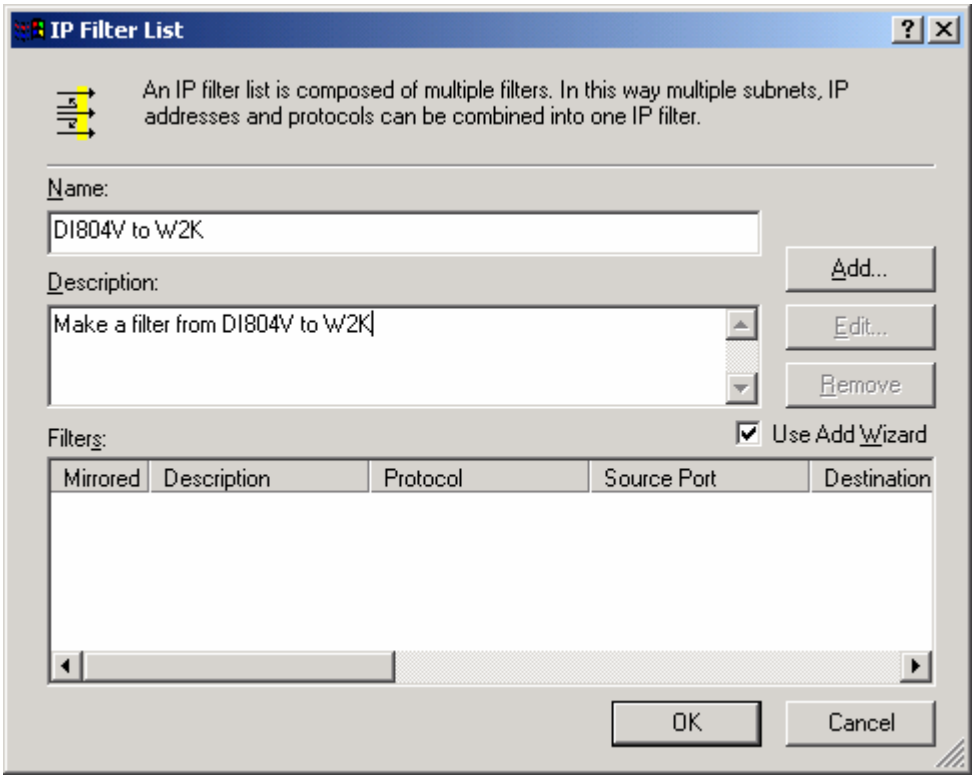
43. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DI-804V preshared key) then click "**Next**"



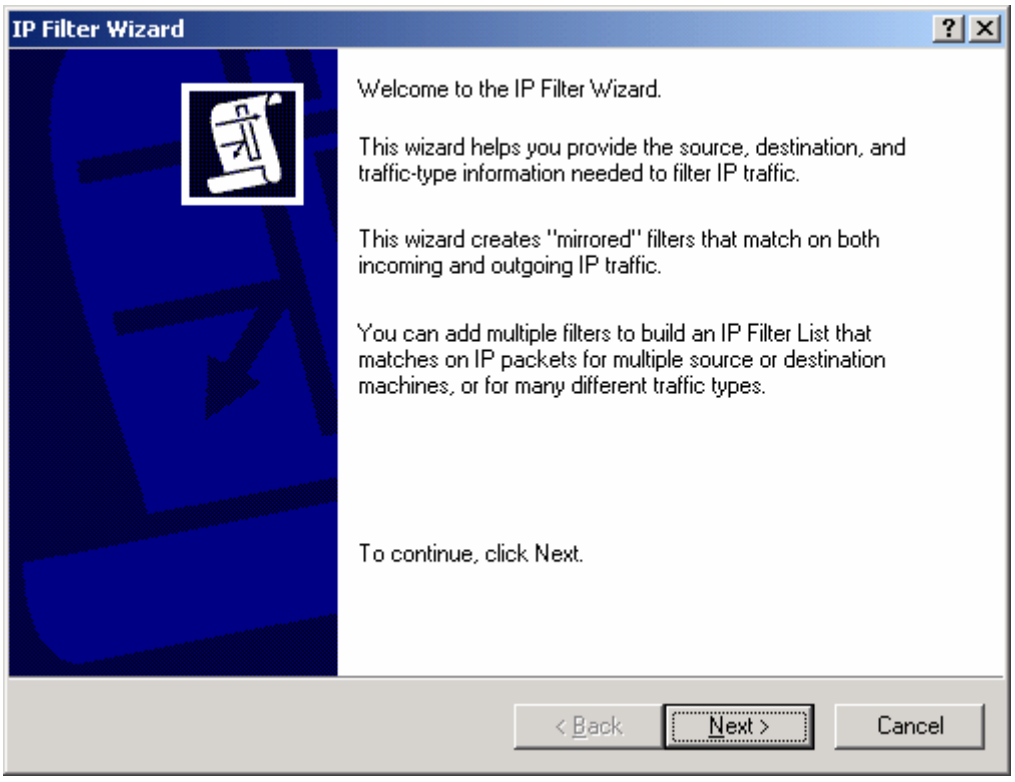
44. Click "**Add**"



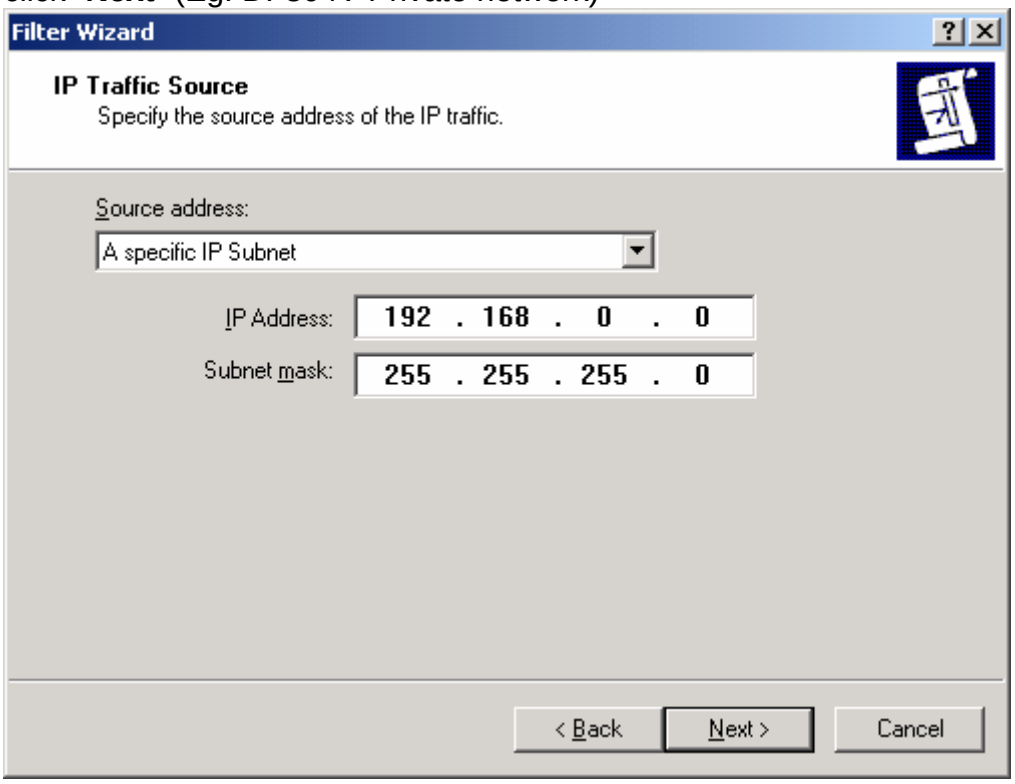
45. Enter a filter name then click on “**Add**”



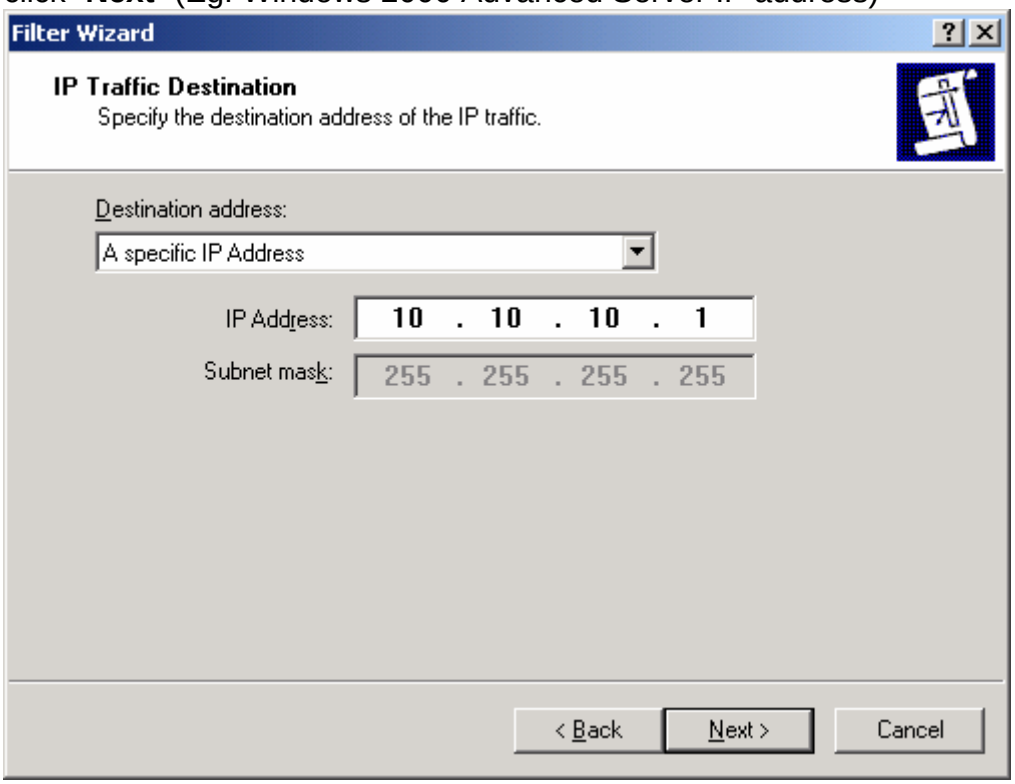
46.Click “**Next**”



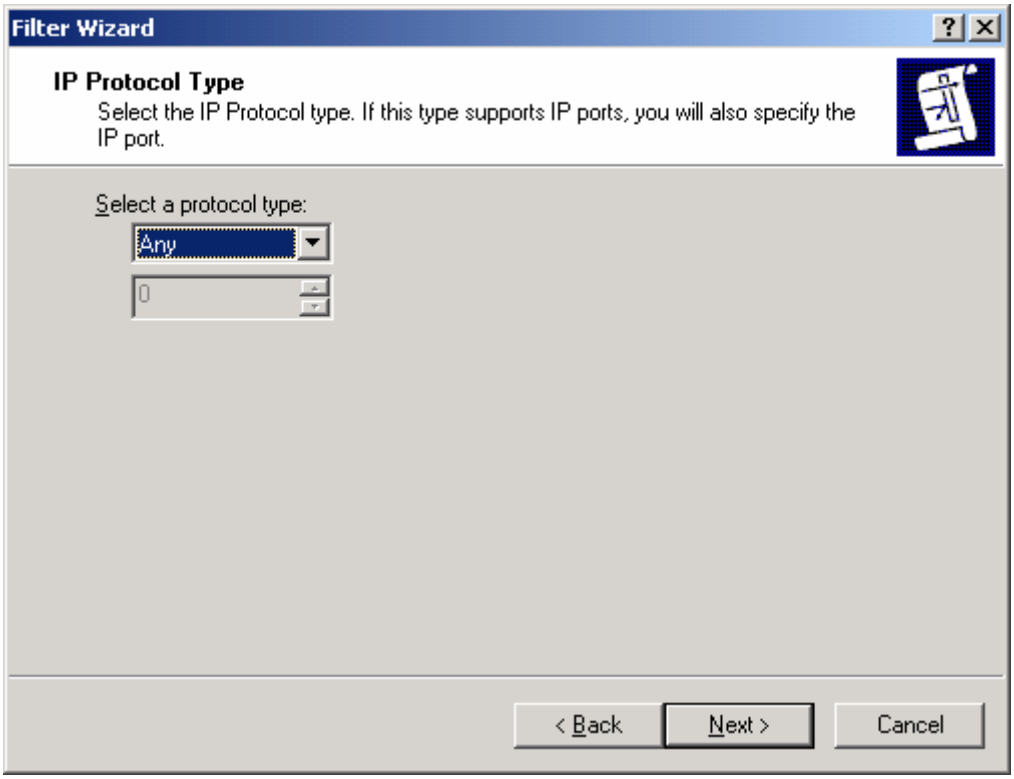
47. Select “**A specific IP Subnet**” and input the Source subnet address then click “**Next**” (Eg. DI-804V Private network)



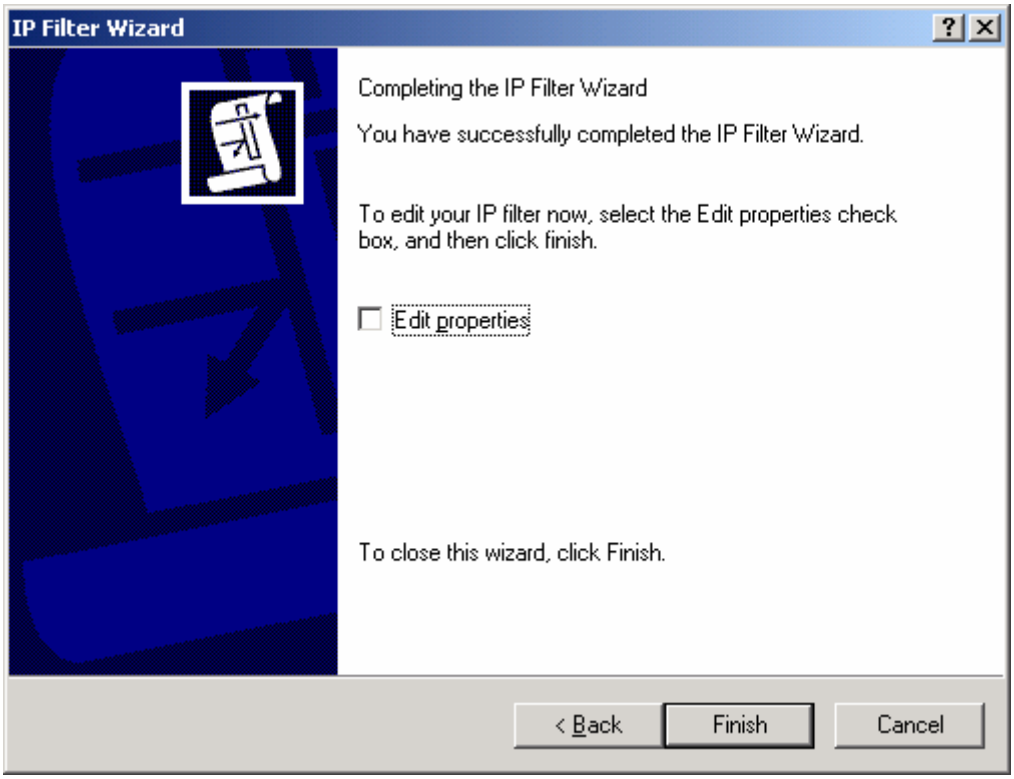
48. Select “**A specific IP Address**” and input the Destination address then click “**Next**” (Eg. Windows 2000 Advanced Server IP address)



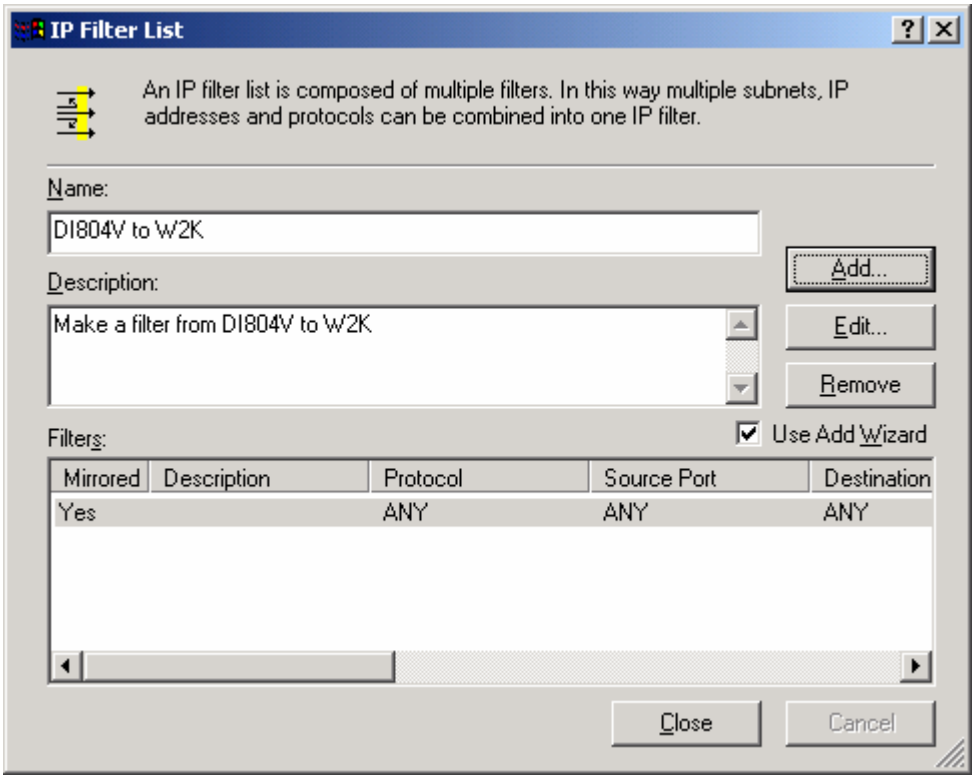
49.Click “**Next**”



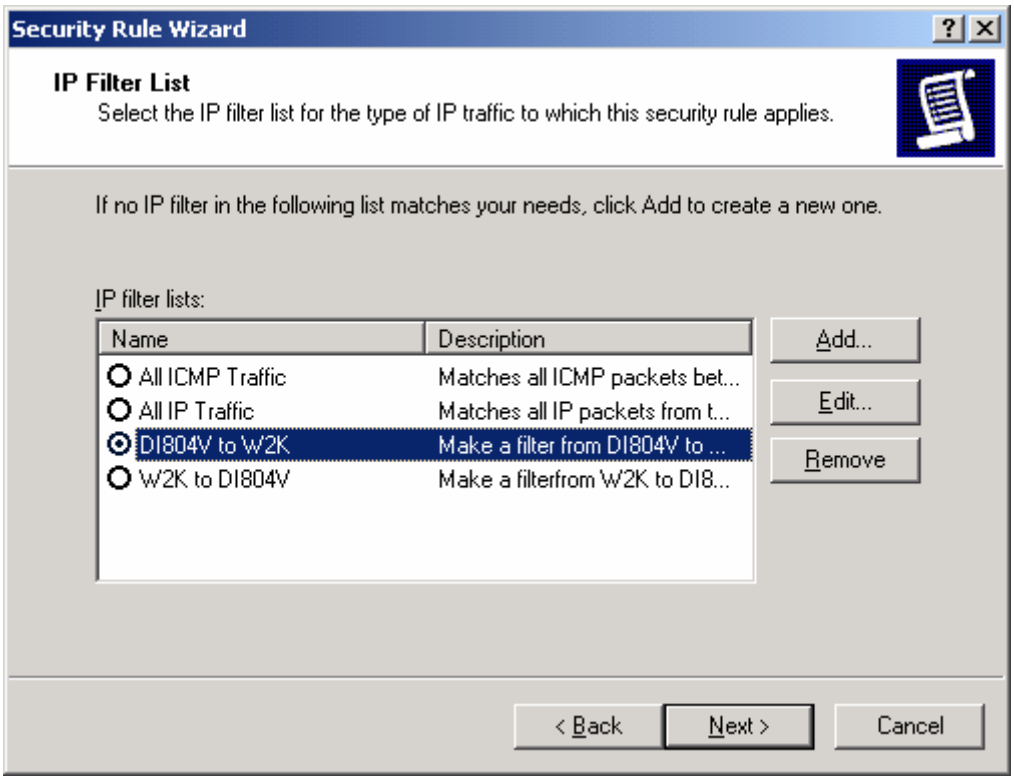
50.Click “**Finish**”



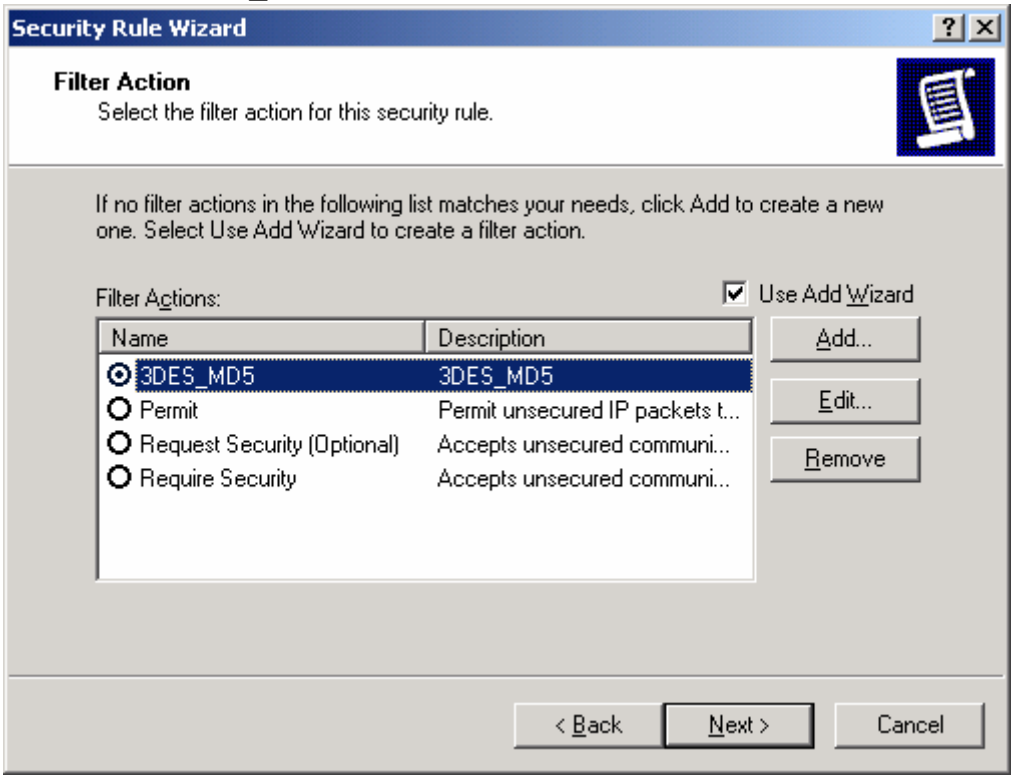
51.Click on “**Close**”



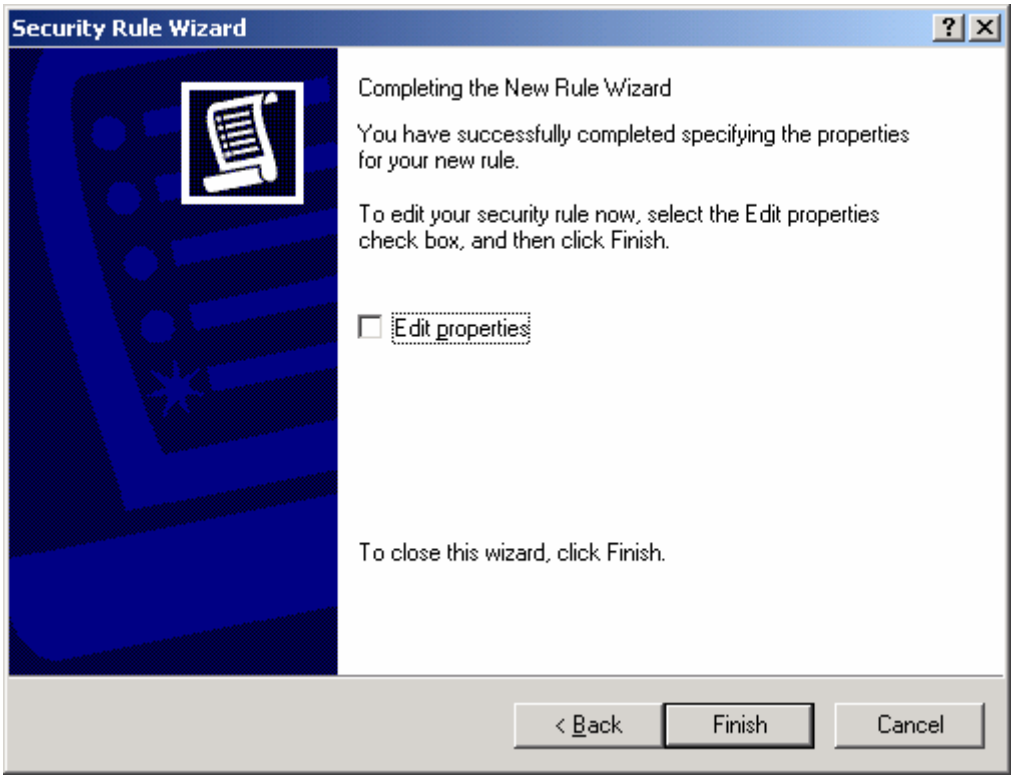
52.Select “**DI-804V to W2K**” then click “**Next**”



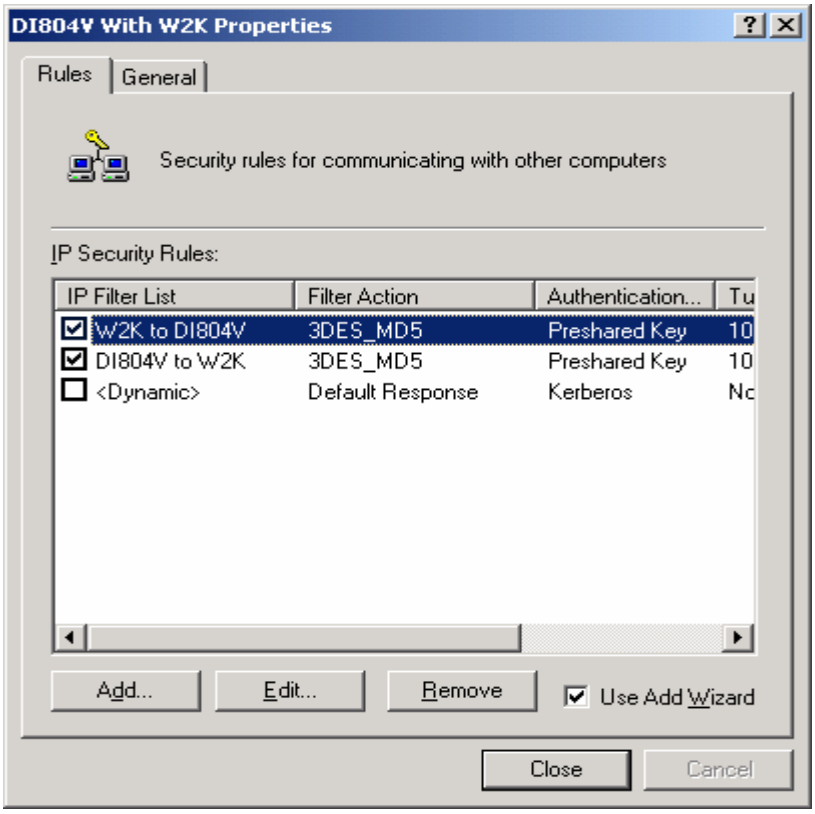
53. Select “**3DES_MD5**” then click “**Next**”



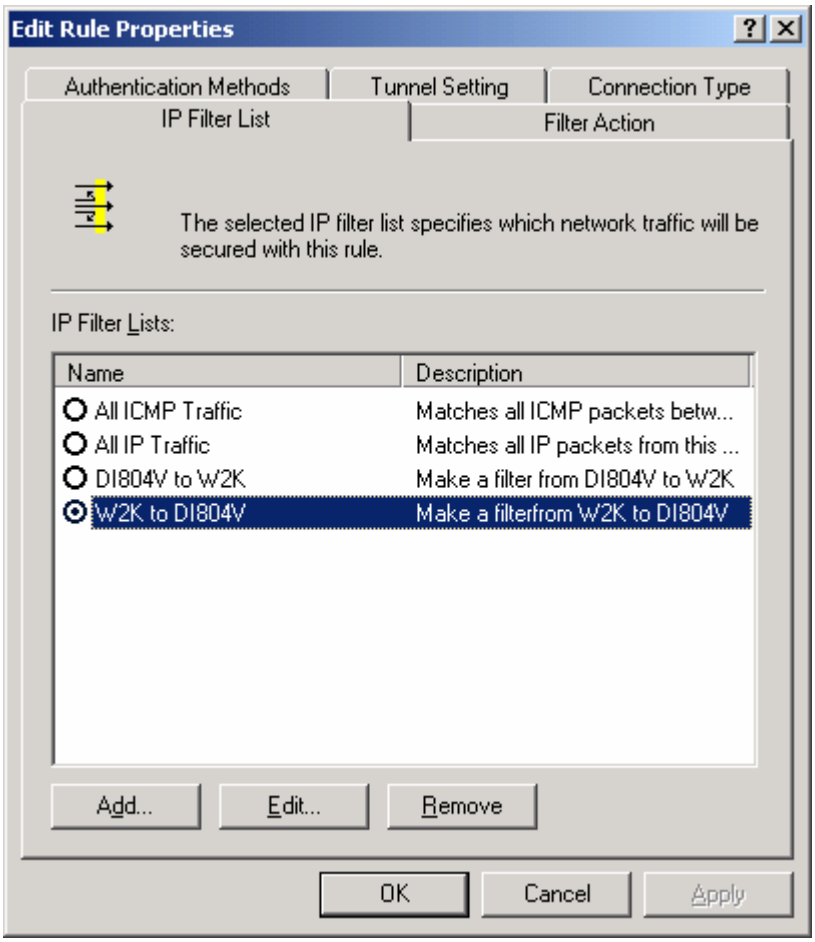
54.Click “**Finish**”



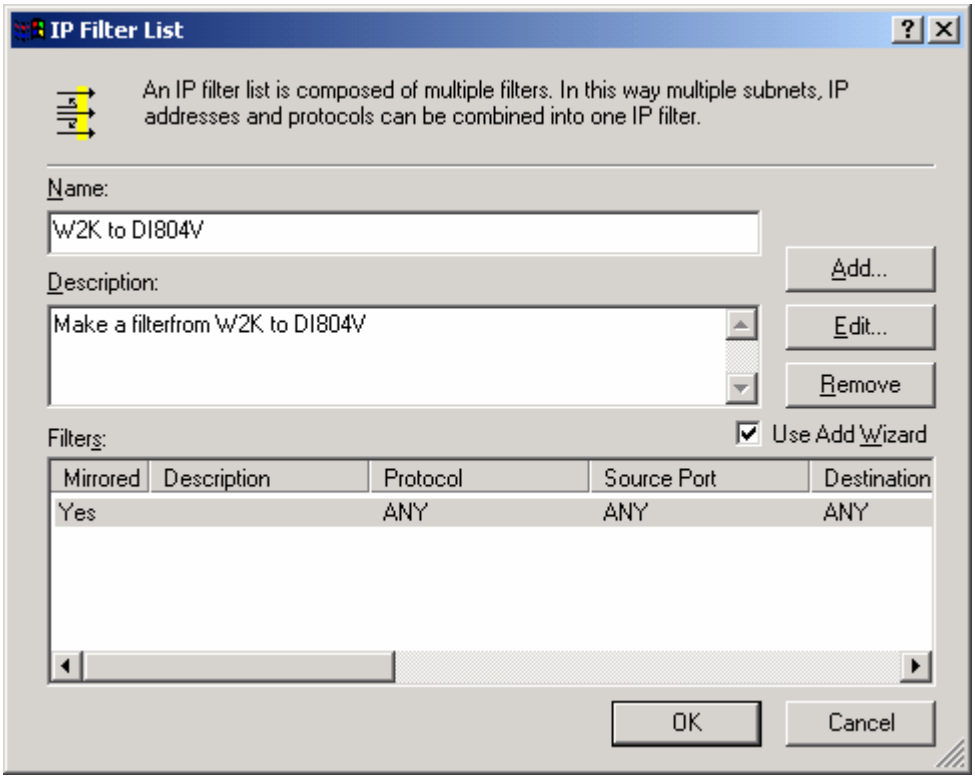
55.Select “**W2K to DI-804V**” then click on “**Edit**”



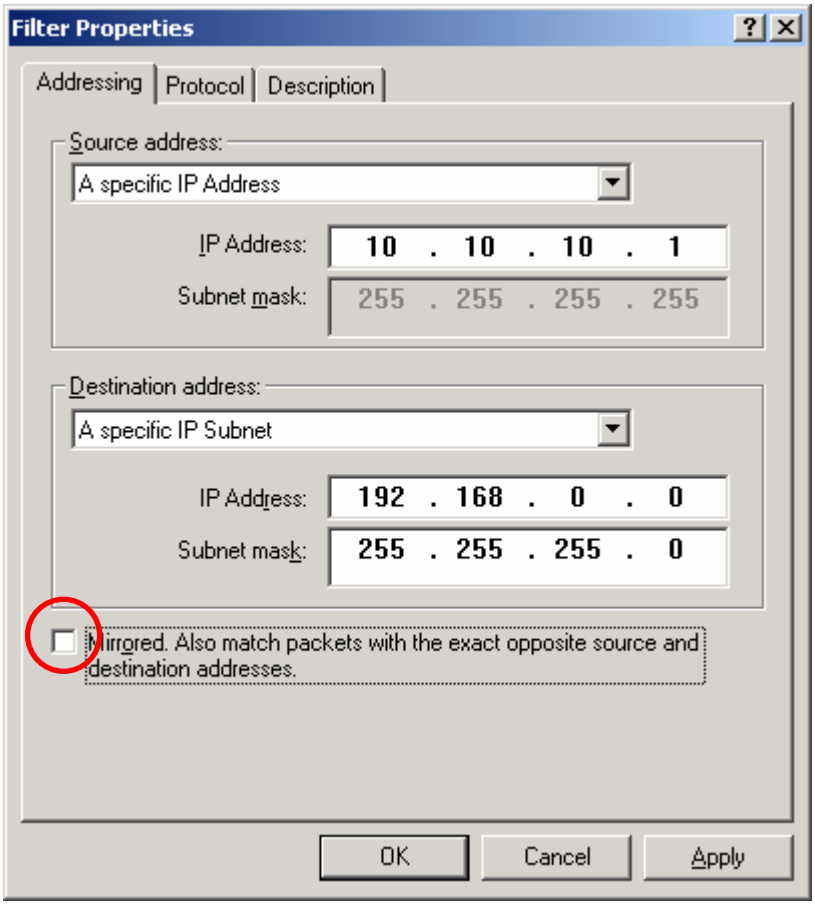
56.Select “**W2K to DI-804V**” then click on “**Edit**”



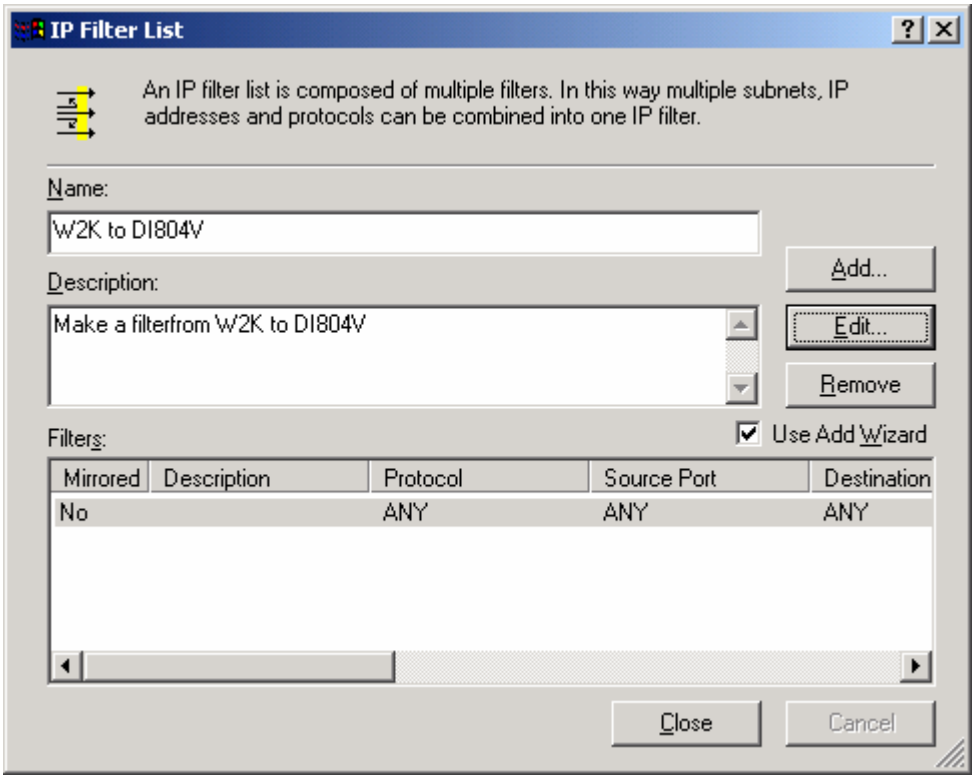
57.Click “**Edit**”



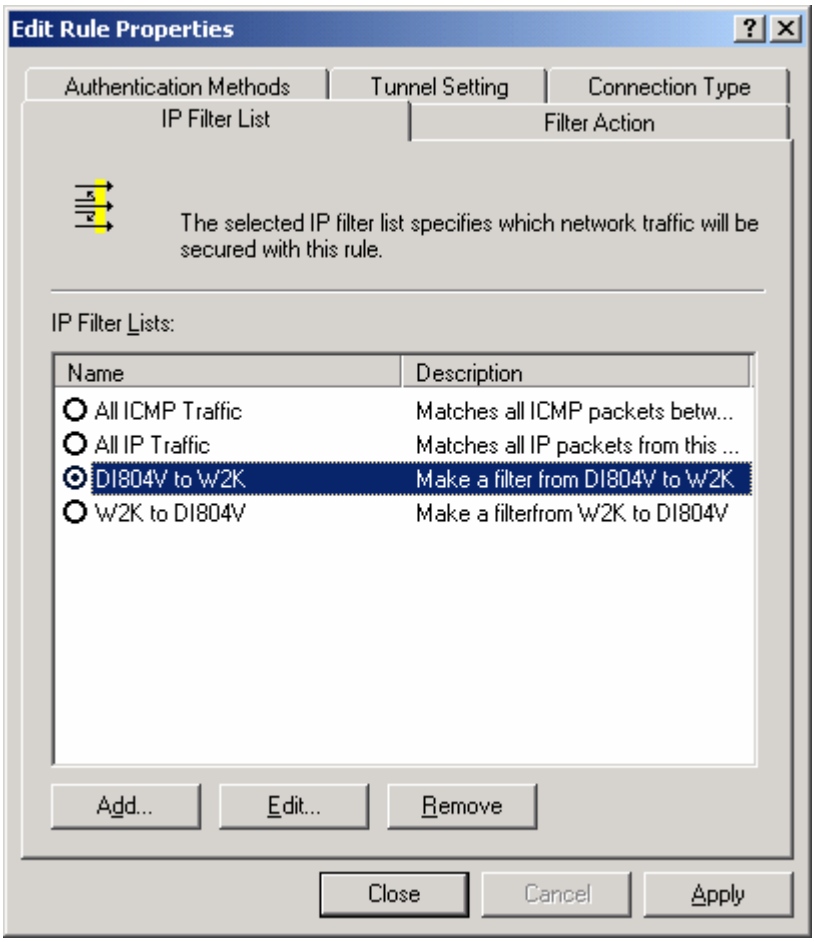
58.Uncheck “**Mirrored. Also match packets with exact opposite source and destination address**” then click “**OK**”



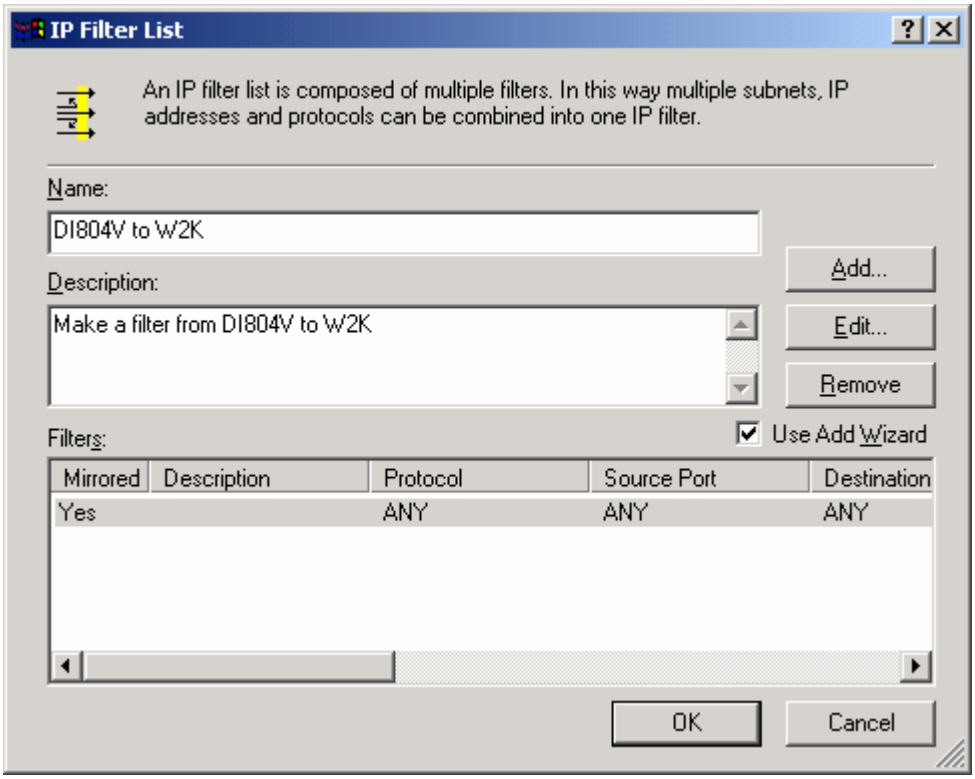
59.Click “**Close**”



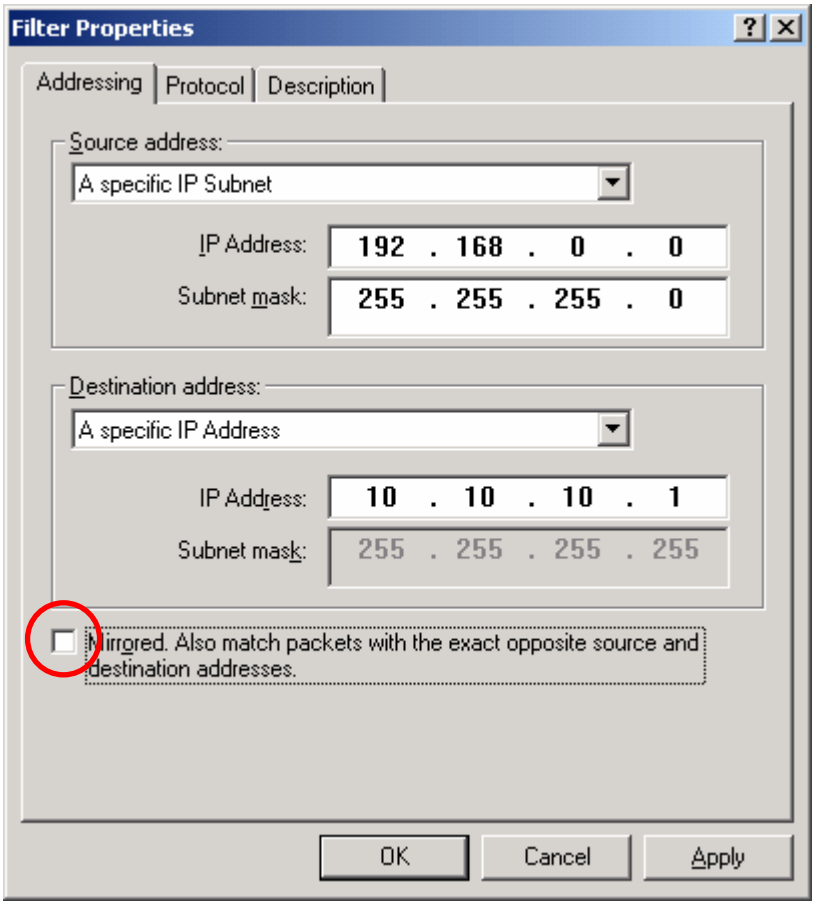
60. Select “**DI-804V to W2K**” then click on “**Edit**”



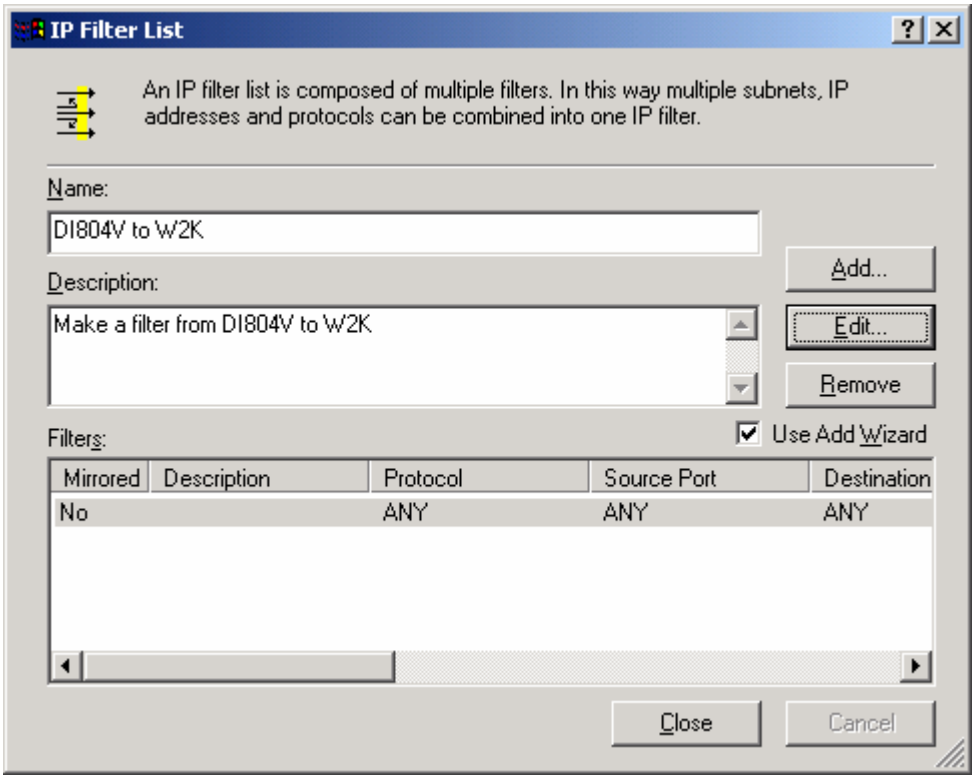
61.Click “**Edit**”



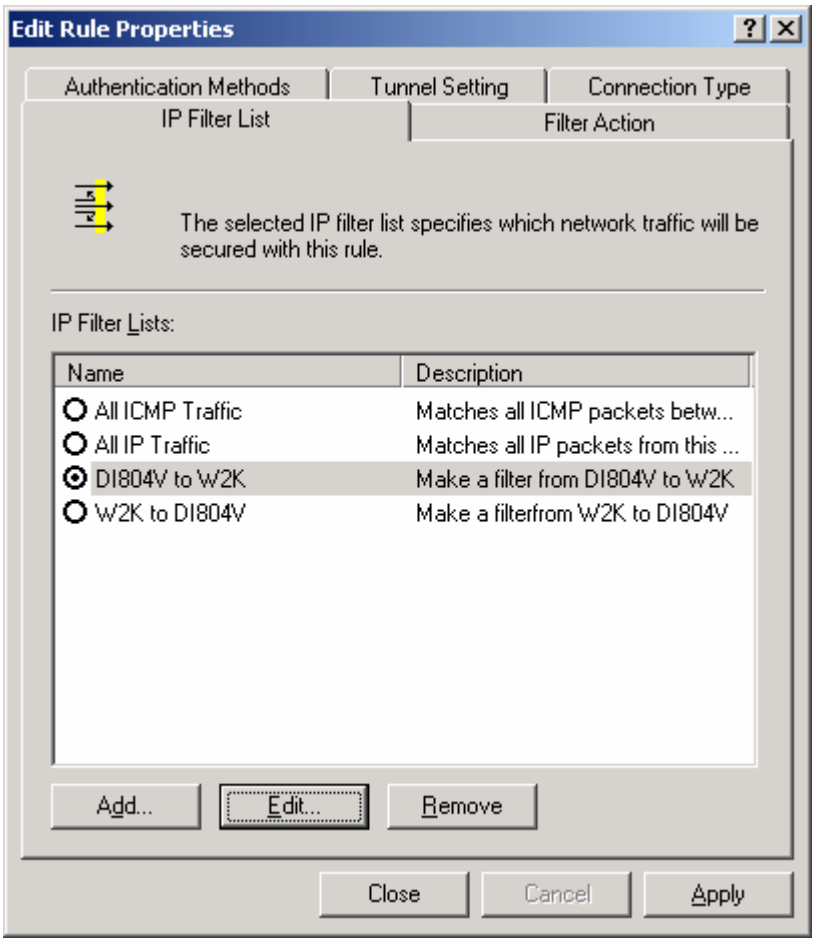
62. Uncheck “**Mirrored. Also match packets with exact opposite source and destination address**” then click “**OK**”



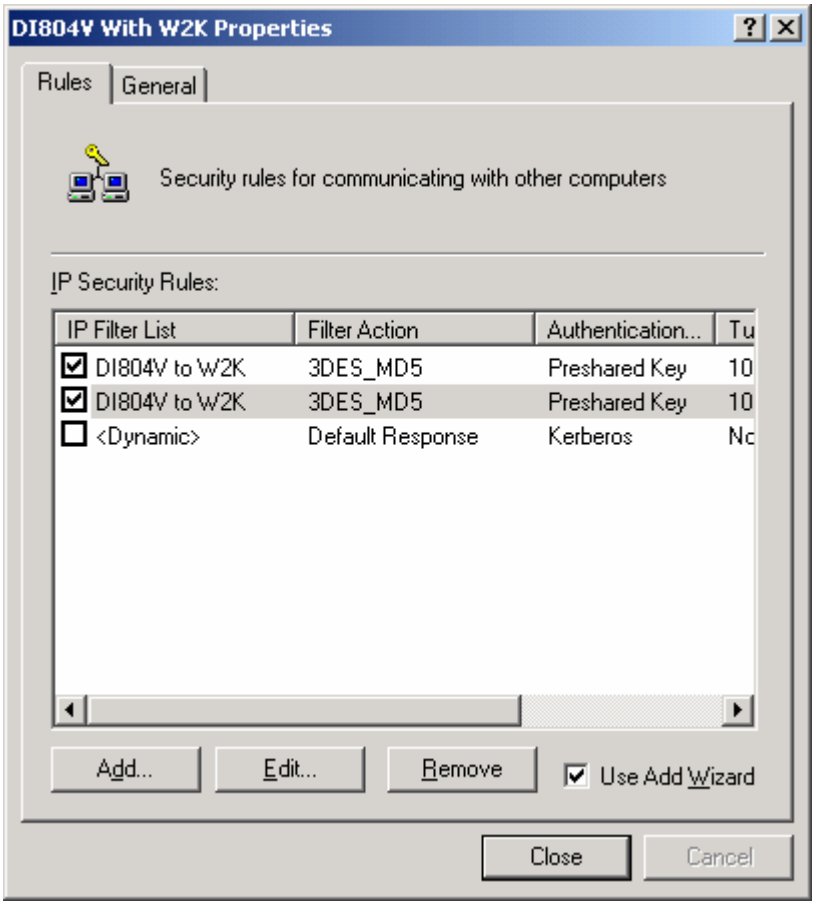
63.Click “**Close**”



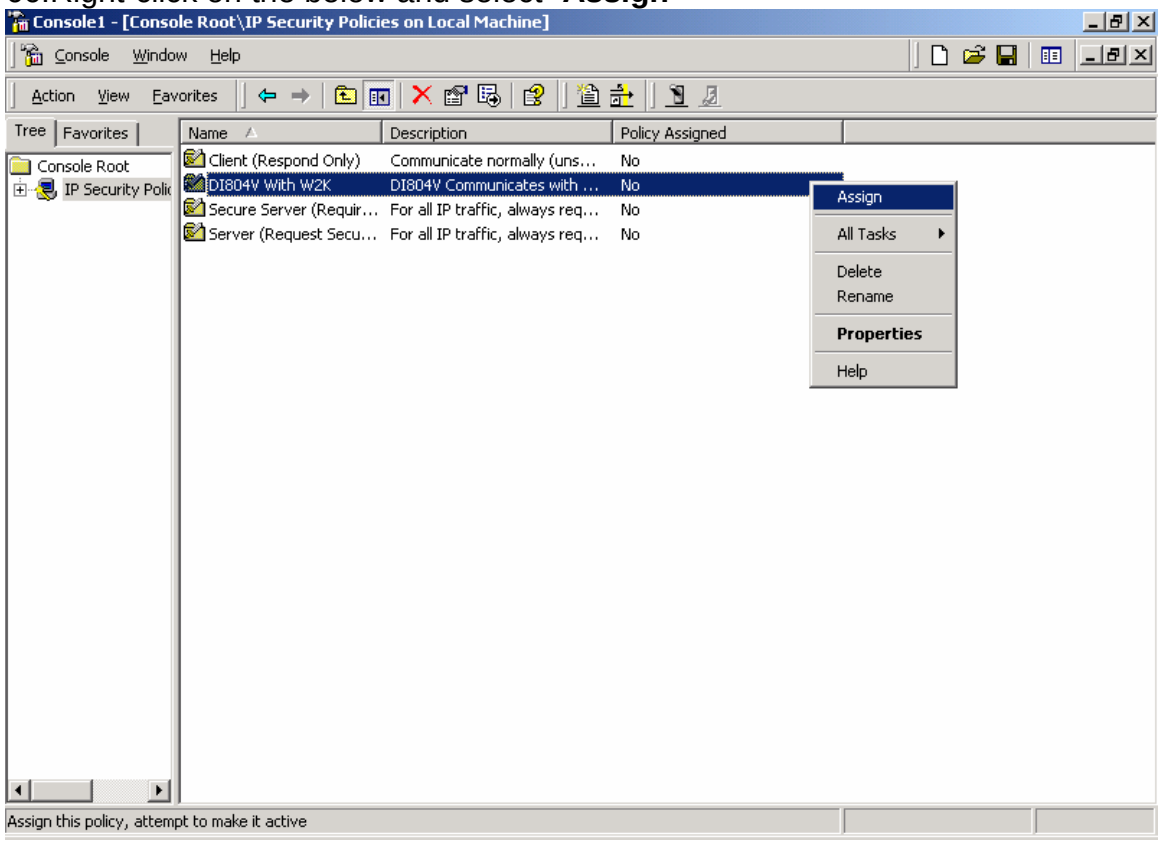
64.Click “**Close**”



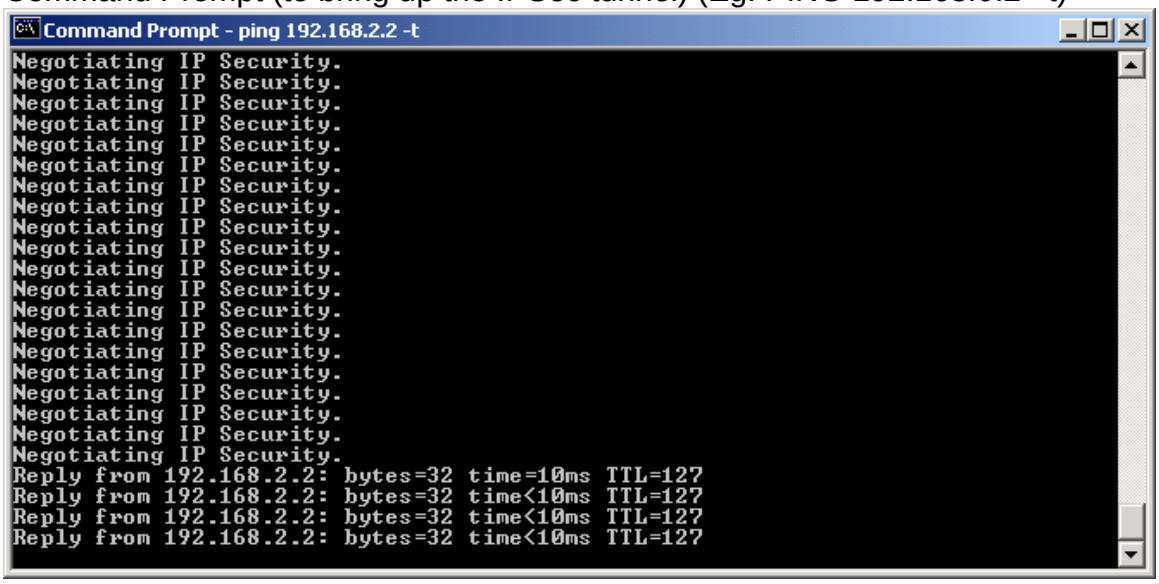
65.Click “**Close**”



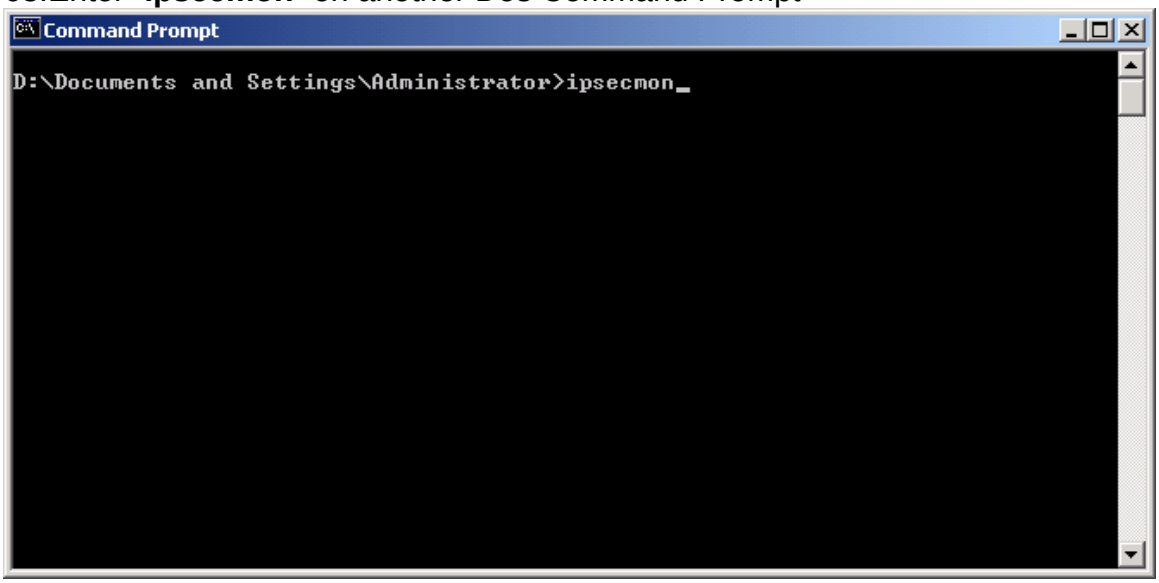
66.Right-click on the below and select “**Assign**”



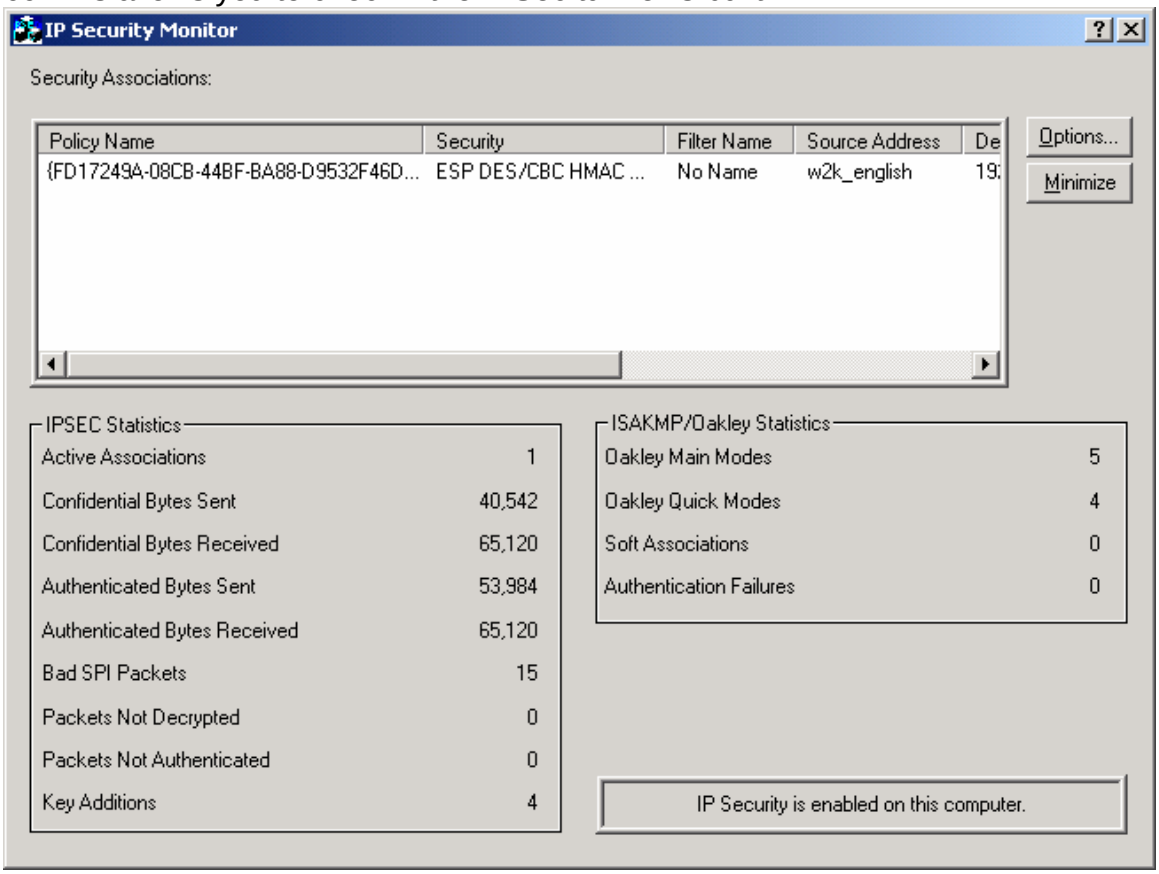
67.Do a **PING** to a valid machine on the Remote private network on the Dos Command Prompt (to bring up the IPSec tunnel) (Eg. PING 192.168.0.2 –t)



68.Enter "**ipsecmon**" on another Dos Command Prompt



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



~ End of Document. Thank you for reading ~