DFL-600 With Windows XP IPSec VPN Configuration Procedures

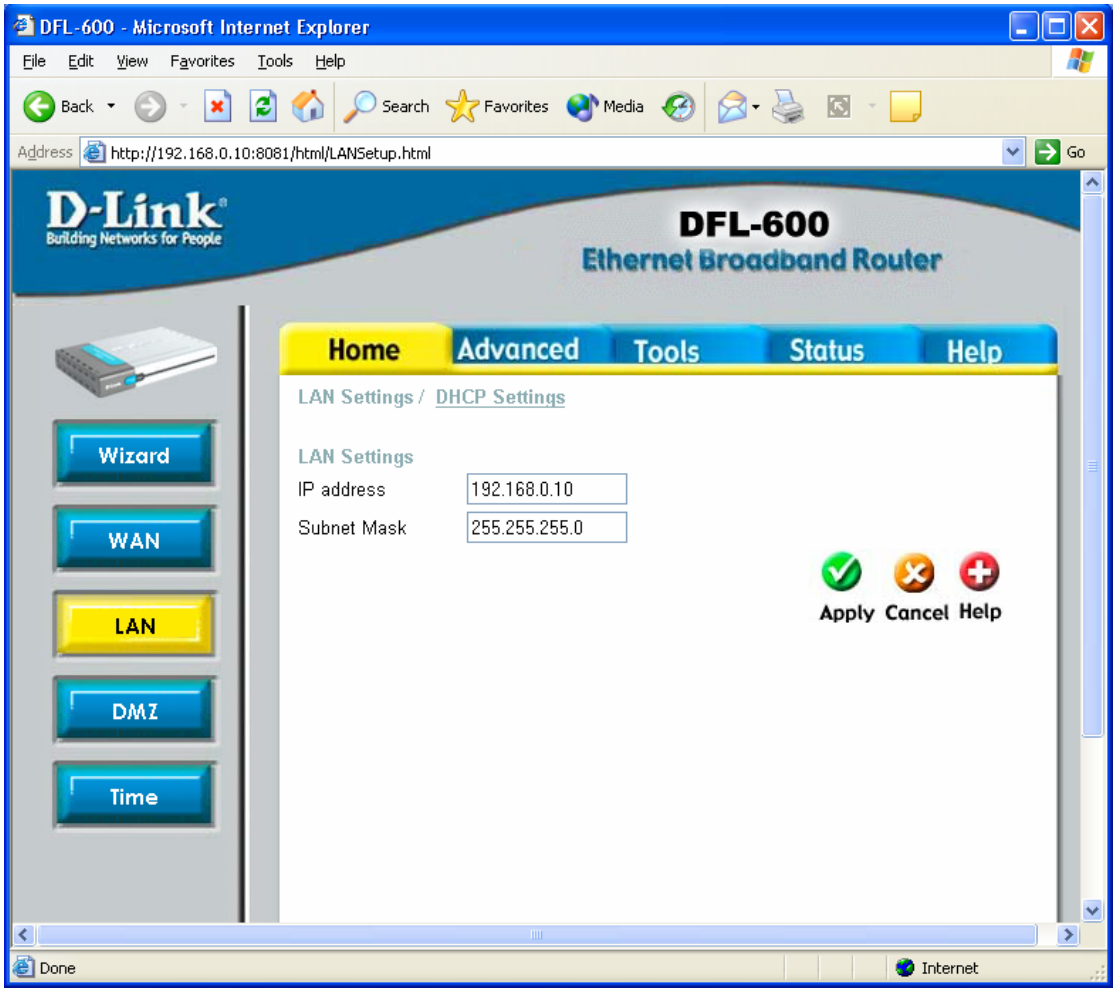
Beta version of the setup, please note the IP address's used are example use only.

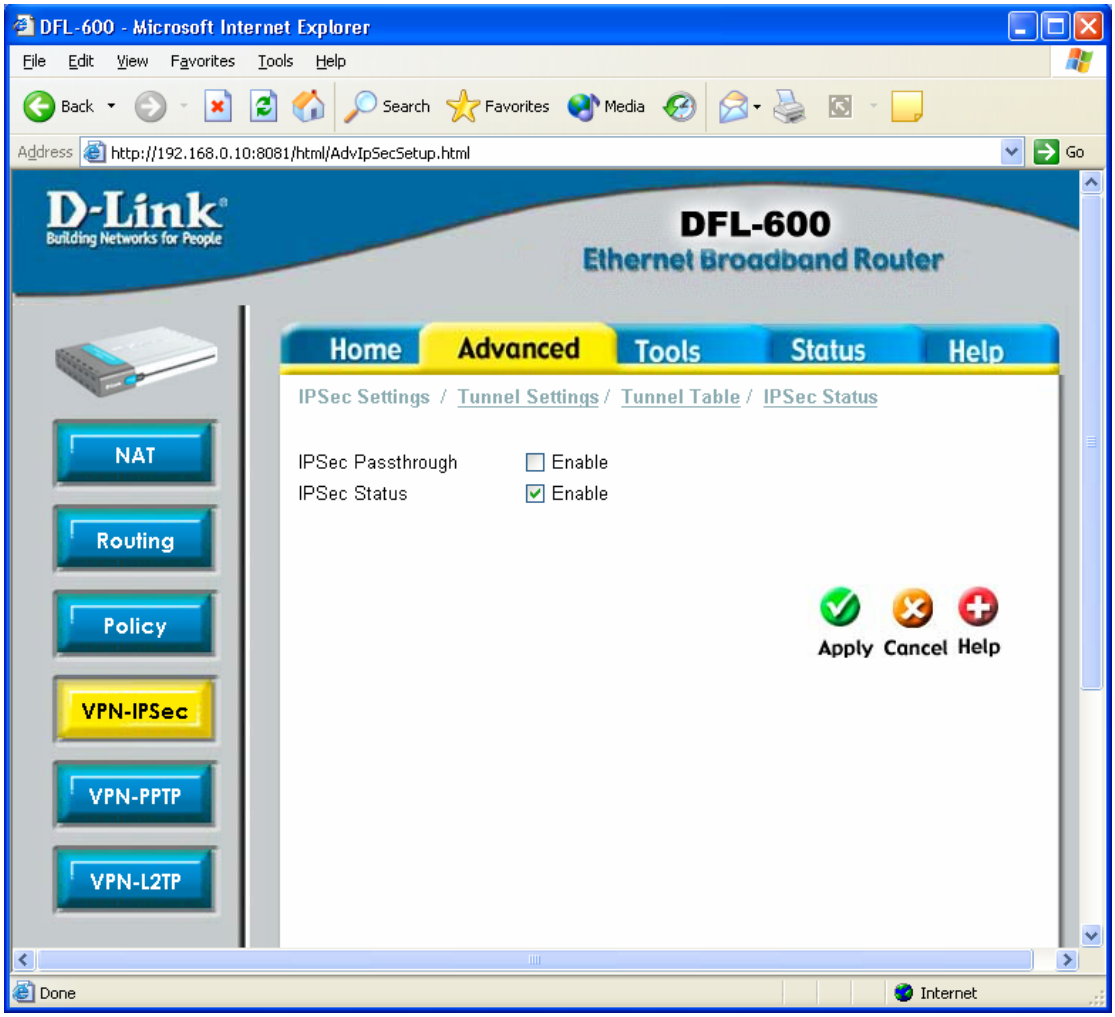
I. Configuring D-Link DFL-600 VPN Router

DFL-600 Settings:

This is the page you need to go into to change the IP, once you have change it make sure your PC has the same subnet.

Remember to Access the unit with the default IP 192.168.0.1:8081
In the below the IP was changed.




DFL-600 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.10:8081/html/AdvIpSecSetup.html
Go
D-Link
Building Networks for People
DFL-600
Ethernet Broadband Router
Home
Advanced
Tools
Status
Help
NAT
Routing
Policy
VPN-IPSec
VPN-PPTP
VPN-L2TP
IPSec Settings / Tunnel Settings / Tunnel Table / IPSec Status
IPSec Passthrough
Enable
IPSec Status
Enable
Apply
Cancel
Help
Done
Internet

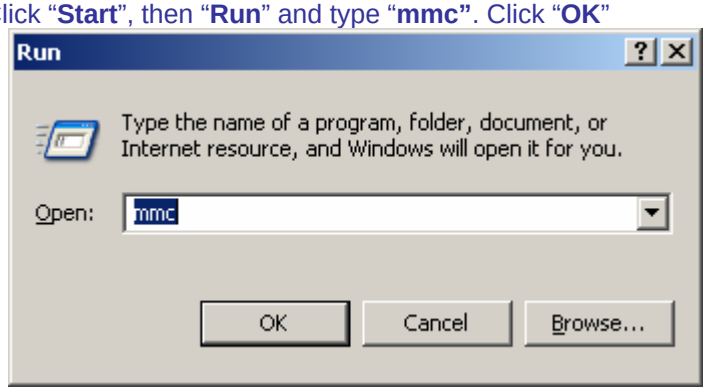

DFL-600 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.10:8081/html/AdvTunnelSetup.html?0,0,0,0,0
Go
D-Link
Building Networks for People
DFL-600
Ethernet Broadband Router
Home
Advanced
Tools
Status
Help
NAT
Routing
Policy
VPN-IPSec
VPN-PPTP
VPN-L2TP
IPSec Settings / Tunnel Settings / Tunnel Table / IPSec Status
Add/New Tunnel
Tunnel ID
Remote Gateway
Termination IP
10.44.13.10
Shared Key
password
Tunnel Type
Public
Phase 1 Proposal
Mode
Main
Aggressive
DH Group
Group 1
IKE Life Duration
28800
seconds
IKE Hash
MD5
IKE Encryption
DES
Phase 2 Proposal
PFS Mode
Group 1
IPSec Operation
ESP
IPSec Life Duration
14400
seconds
ESP Transform
3DES
ESP Auth
HMAC-MD5
AH Transform
MD5
Target Host Range
Type
Subnet
Starting Target Host
192.168.2.1
Subnet Mask
255.255.255.0
Apply
Cancel
Help
Done
Internet

II. Configuring Windows XP IPSec Client

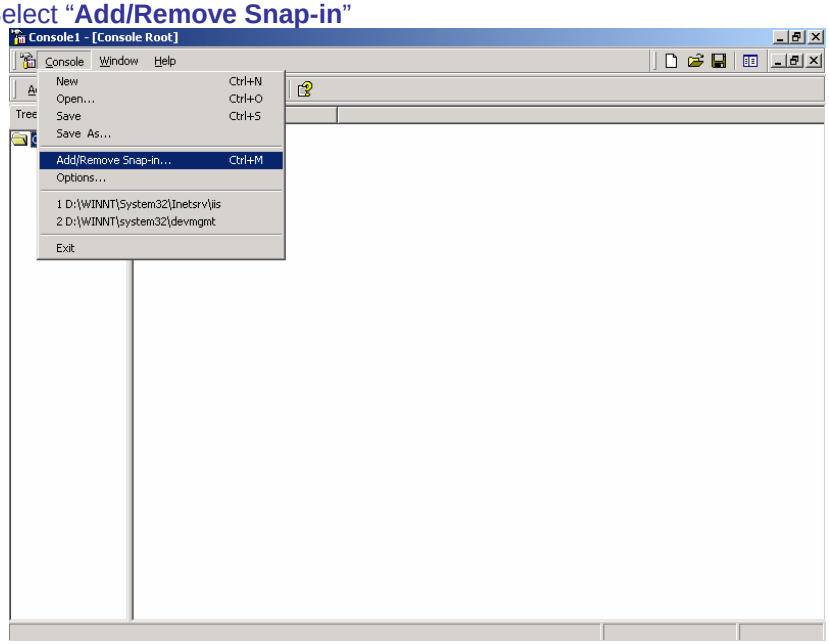
Technical Requirement: Customer is required to understand their network and the Windows XP well for this configuration. Please consult Microsoft certified professional if unsure. The information provided here is for your reference only. D-Link will not be held responsible for any consequences arise from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

Please change DI-804V to DFL-600 in the below shots.

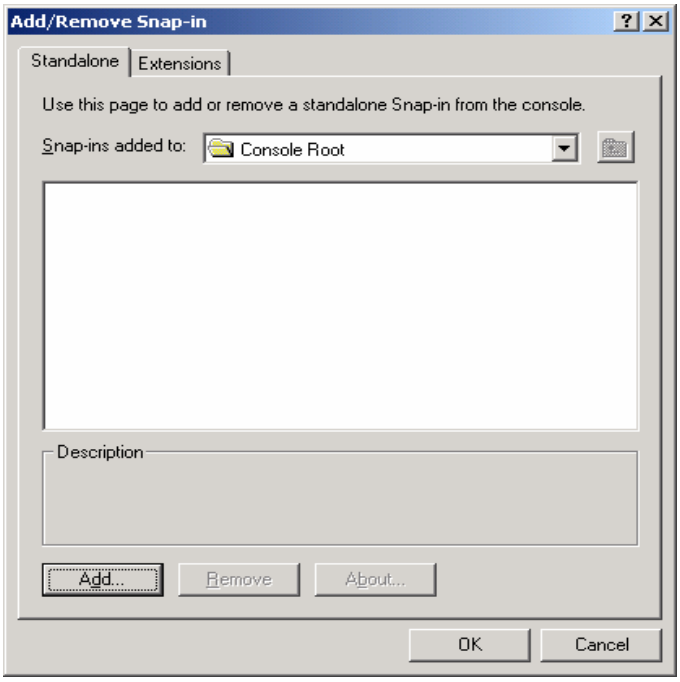
1.Click "**Start**", then "**Run**" and type "**mmc**". Click "**OK**"



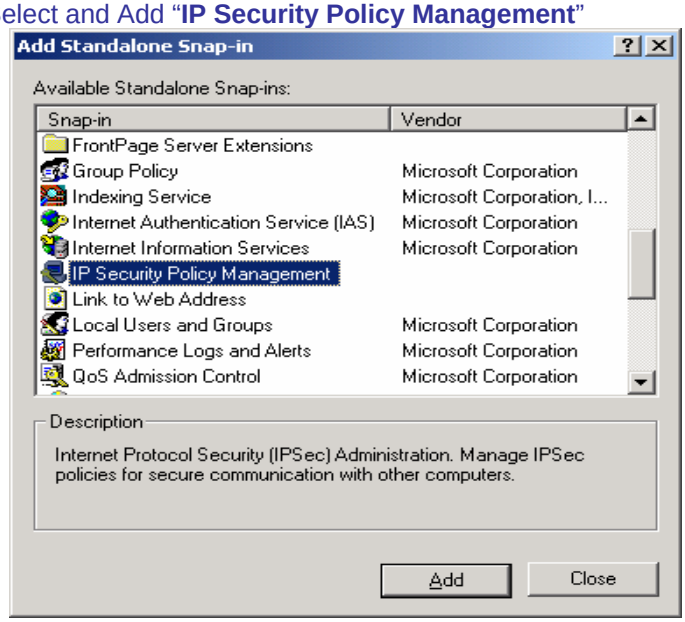
2.Select "**Add/Remove Snap-in**"



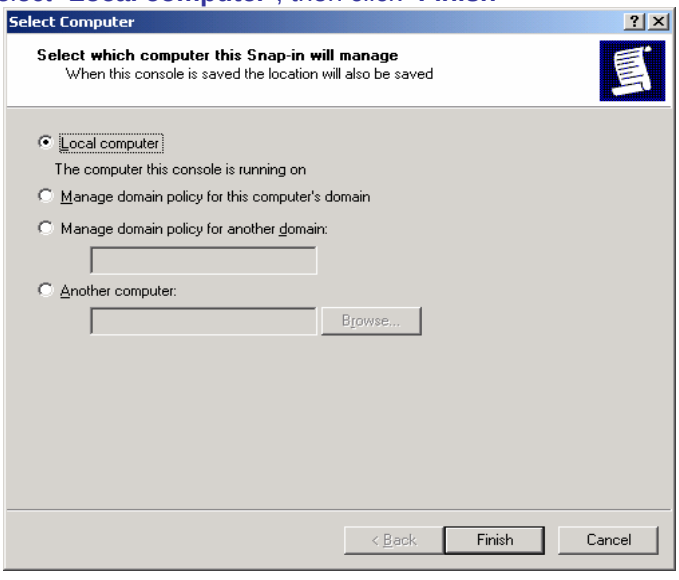
3.Click "**Add**"



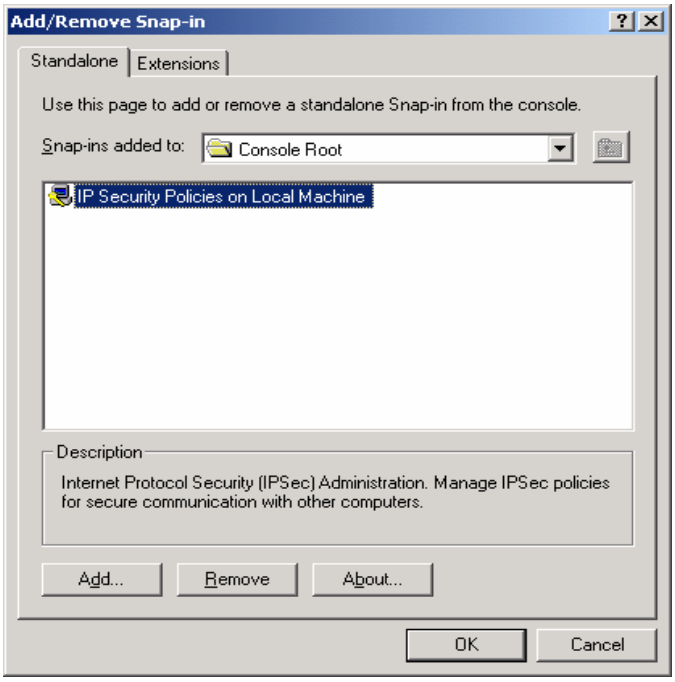
4.Select and Add "**IP Security Policy Management**"



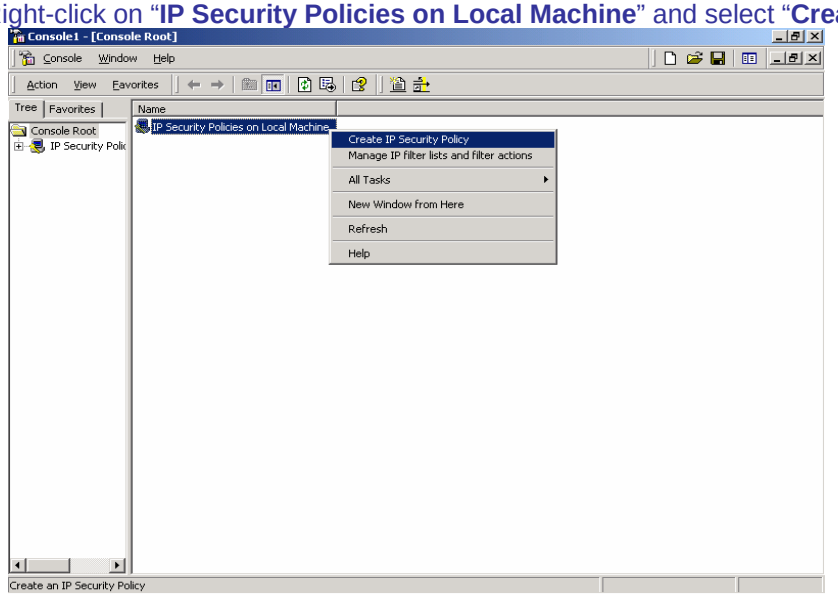
5.Select "**Local computer**", then click "**Finish**"



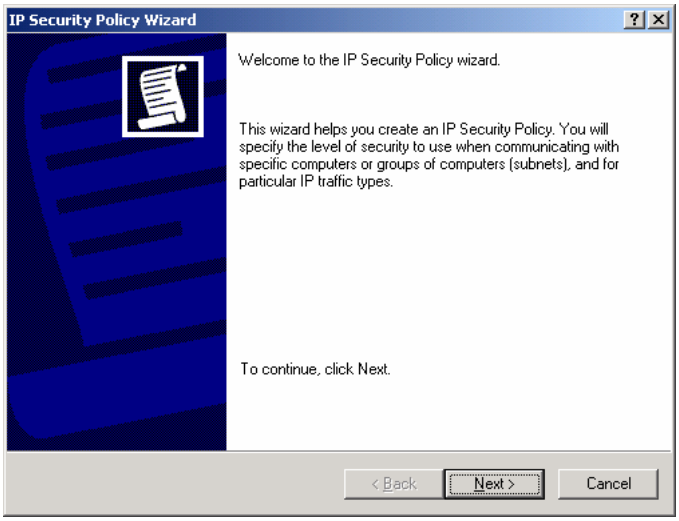
6.Click "**OK**"



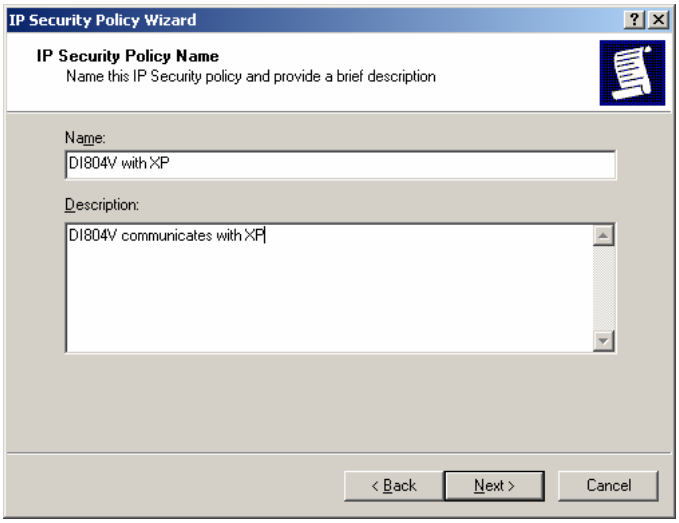
7.Right-click on "**IP Security Policies on Local Machine**" and select "**Create IP Security Policy**"



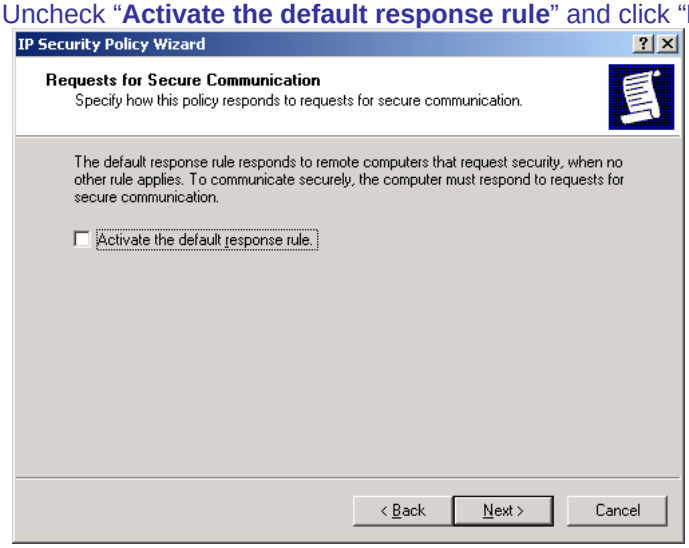
8.Click "**Next**"



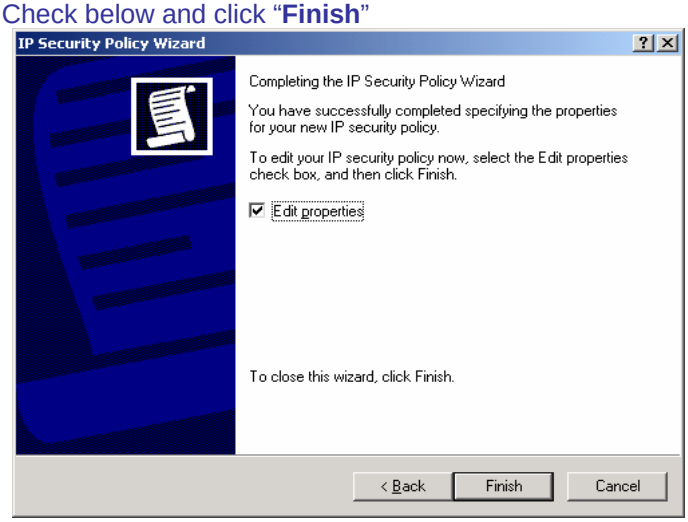
9.Enter the details below and click "**Next**"


IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
DI804V with XP
Description:
DI804V communicates with XP
< Back
Next >
Cancel

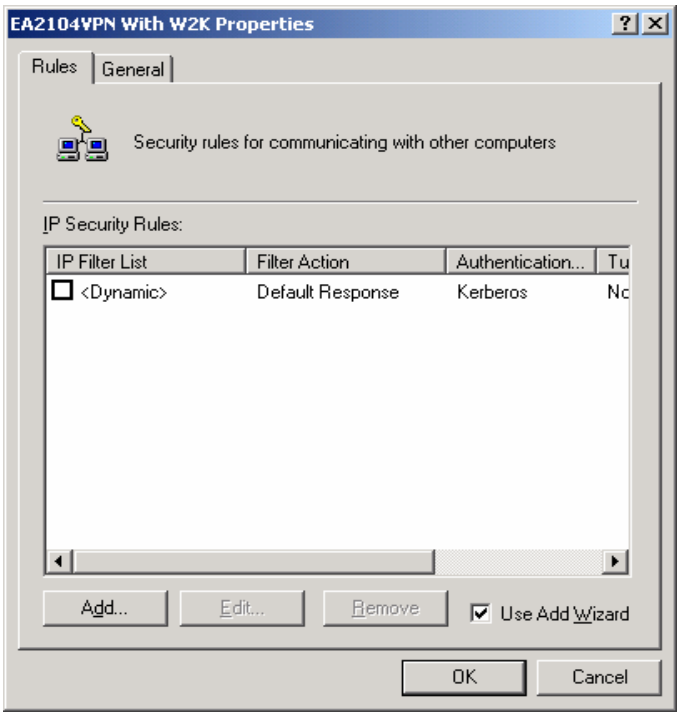
10.Uncheck “**Activate the default response rule**” and click “**Next**”



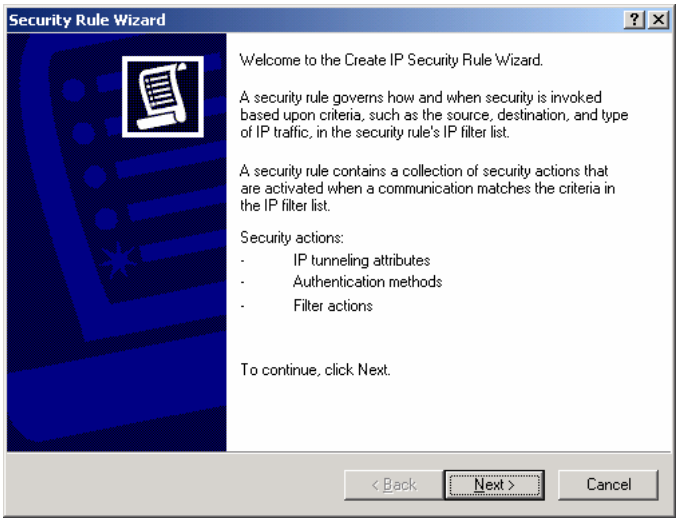
11.Check below and click “**Finish**”



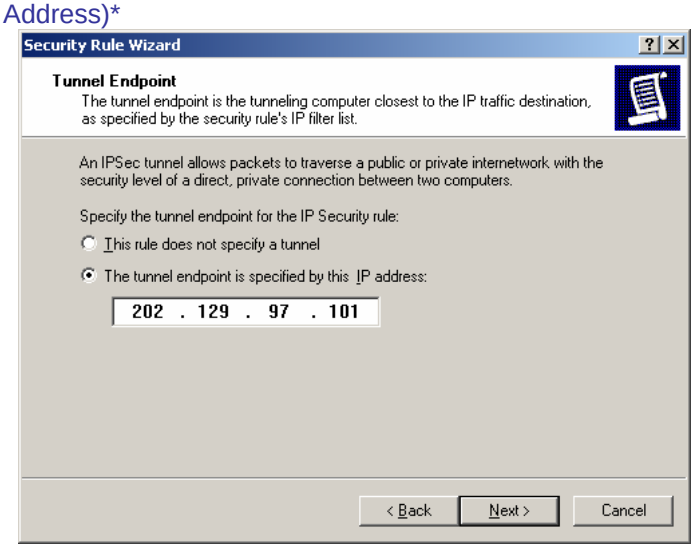
12.Select “**Add**”



13.Click “Next”

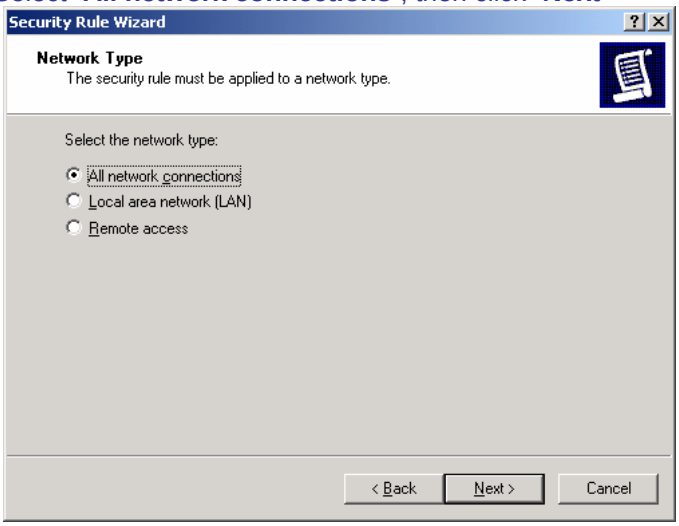


14.Enter the IP Address detail into “**The tunnel endpoint specified by this IP address:**” (Eg. Windows XP IP Address)*

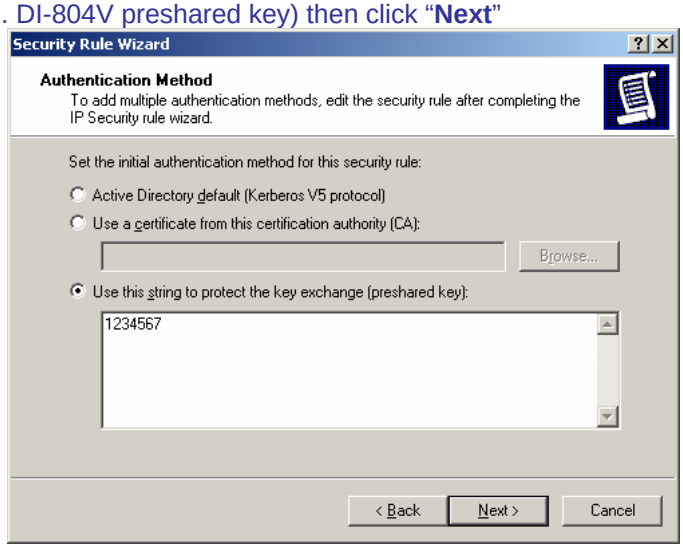


* If your client gets IP address dynamically click to “This rule does not specify a tunnel”.

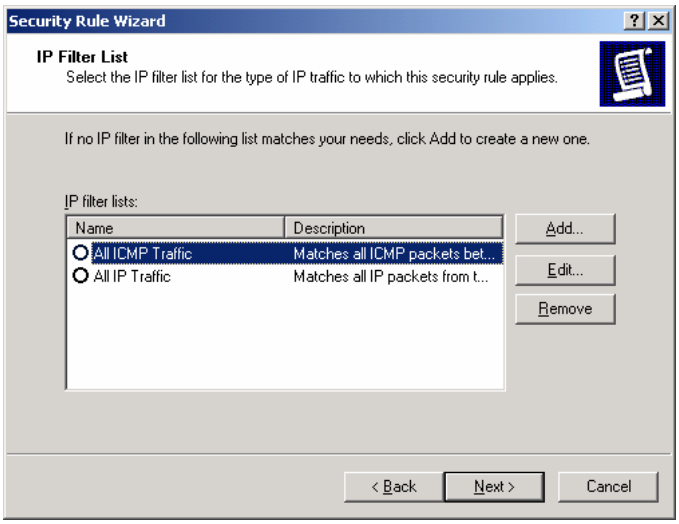
15.Select “**All network connections**”, then click “**Next**”



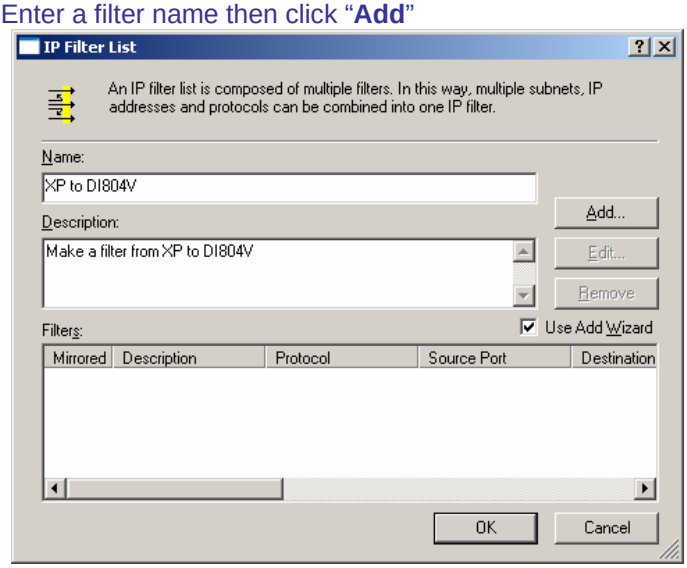
16.Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DI-804V preshared key) then click “**Next**”



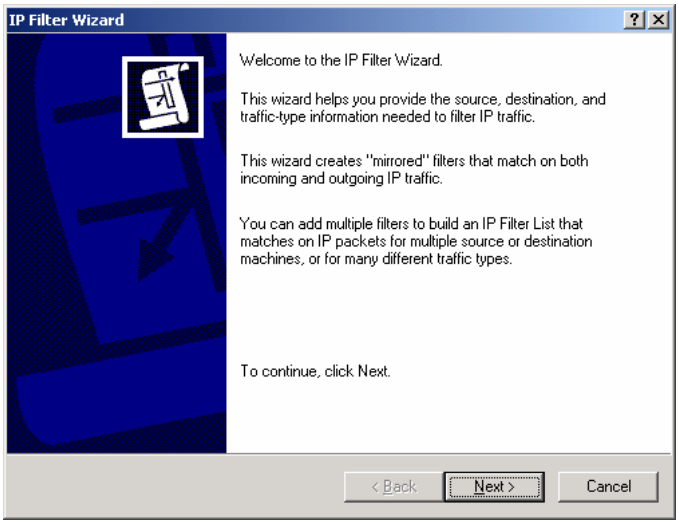
17.Select “**Add**”



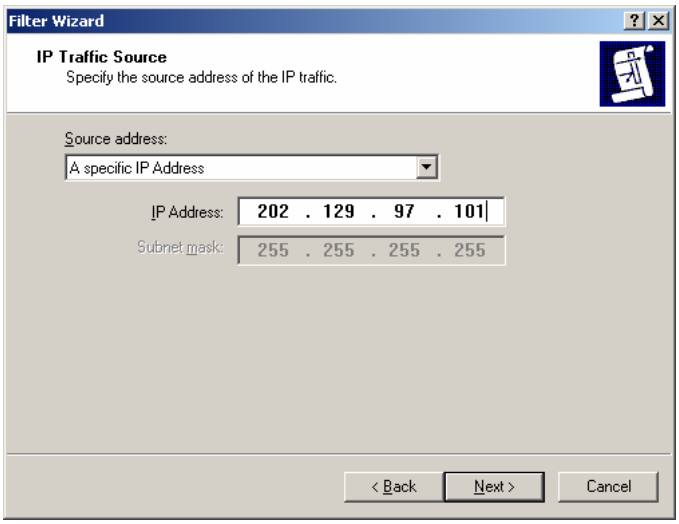
18.Enter a filter name then click “**Add**”



19.Click “**Next**”

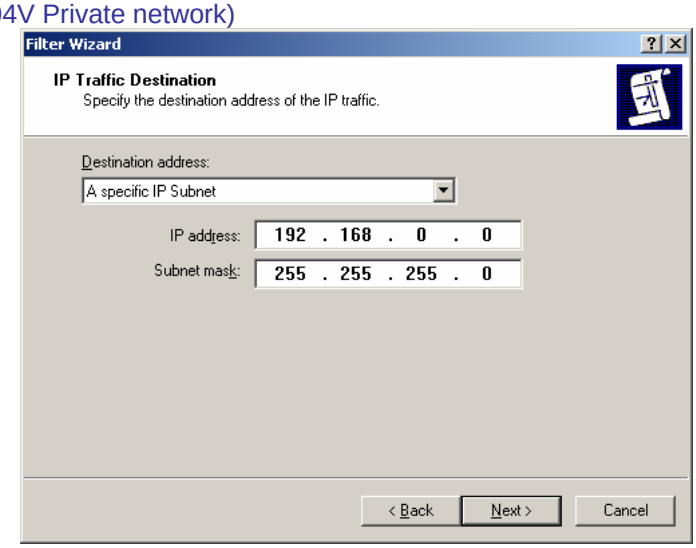


20.Select “**A specific IP Address**” and input the Source address, then “**Next**” to continue (Eg. Windows XP IP) *

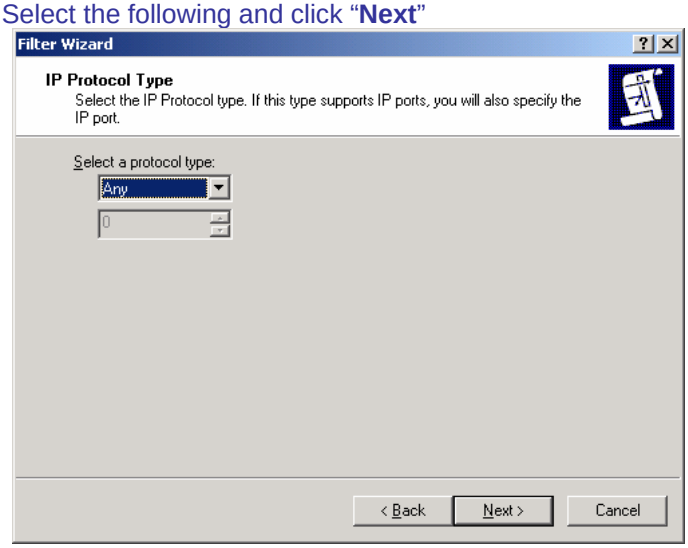


* If your client gets IP address dynamically choose “My IP address”.

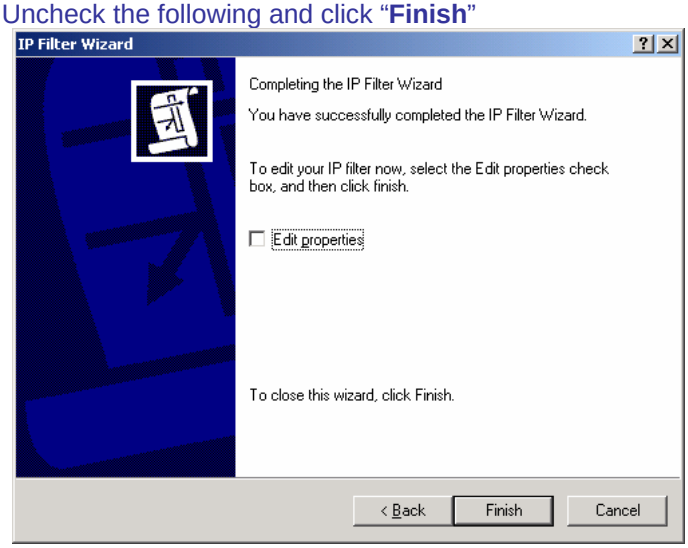
21. Select “**A specific IP Subnet**” and input the Destination subnet address, then “**Next**” to continue (Eg. DI-804V Private network)



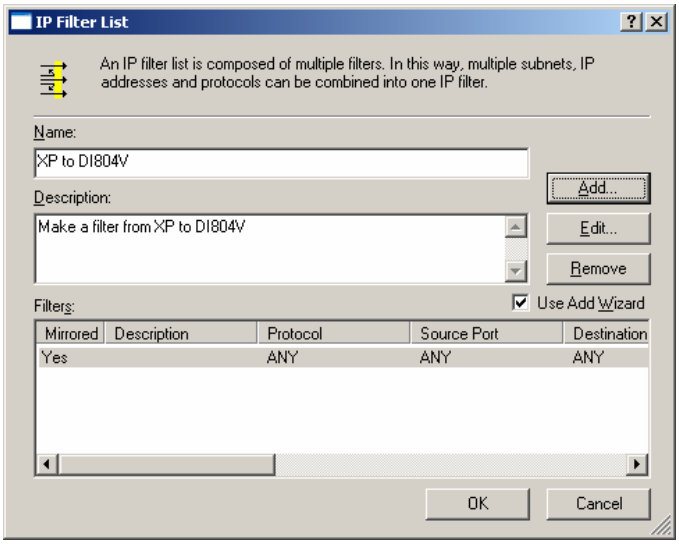
22.Select the following and click “**Next**”



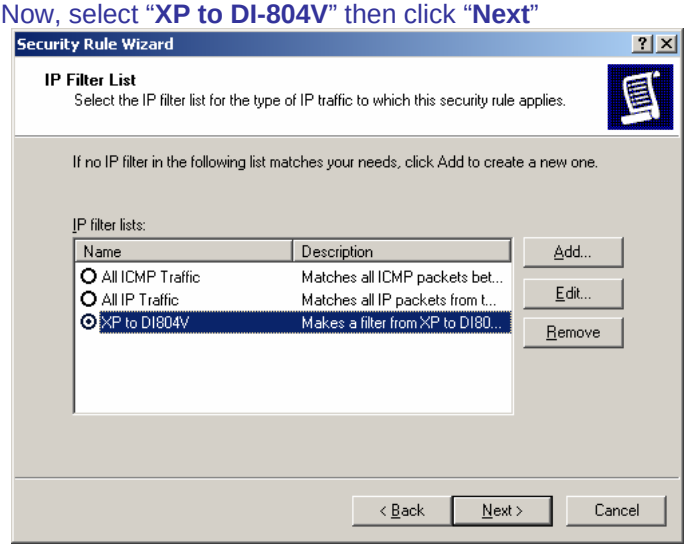
23.Uncheck the following and click “**Finish**”



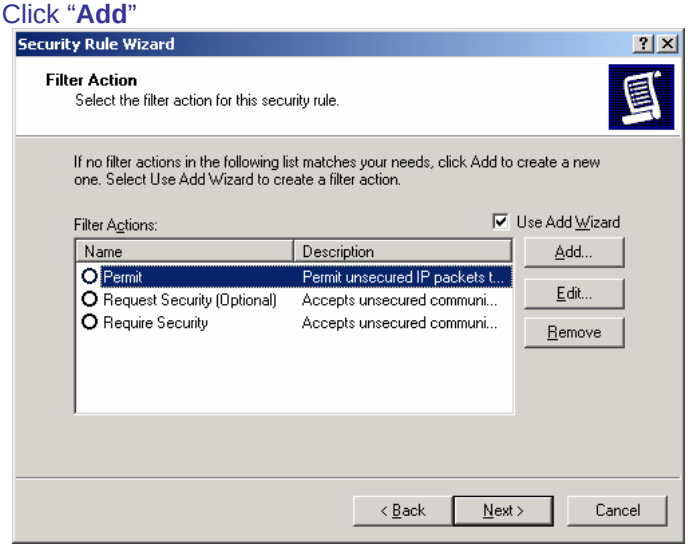
24.Click “**Ok**”



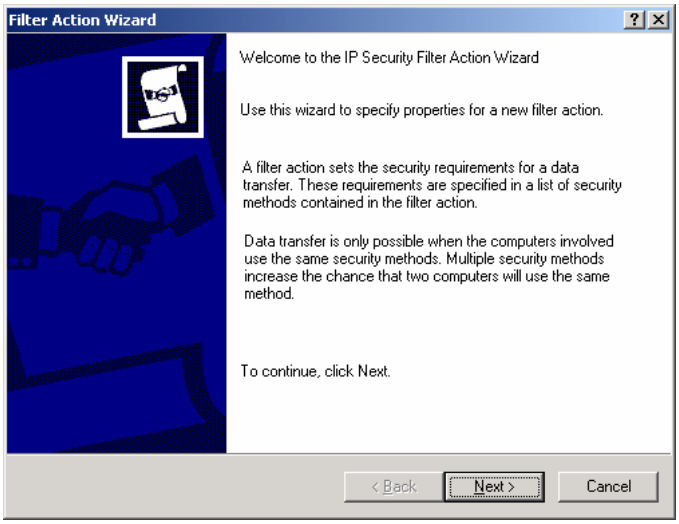
25.Now, select “**XP to DI-804V**” then click “**Next**”



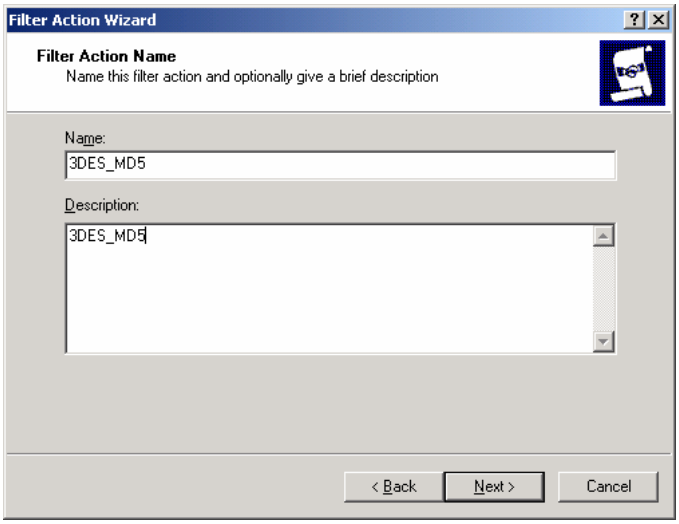
26.Click “**Add**”



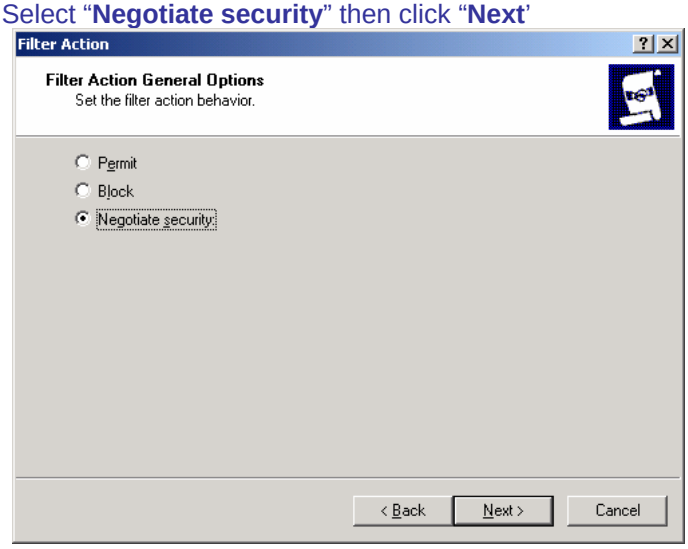
27.Click “**Next**”



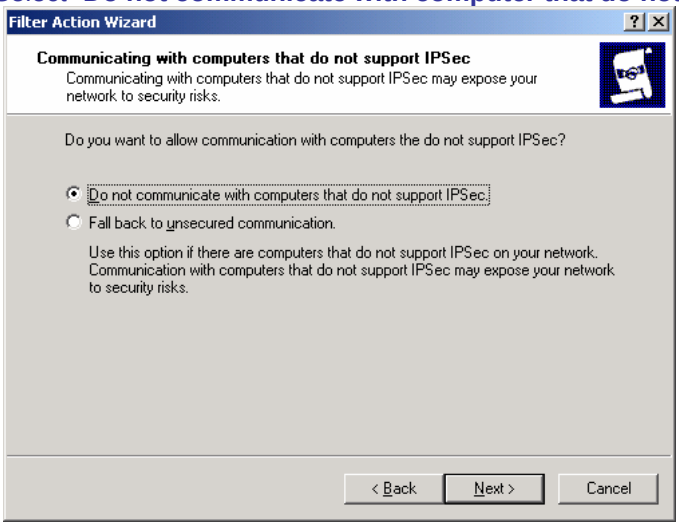
28. Enter a filter action name then click “**Next**”



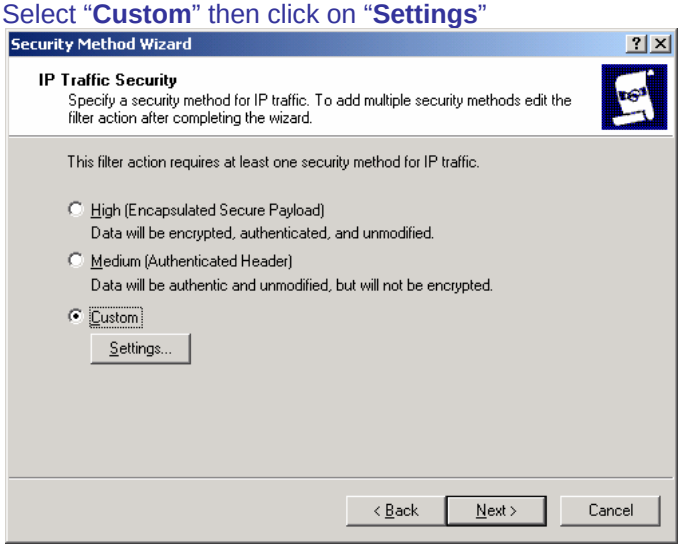
29.Select “**Negotiate security**” then click “**Next**’



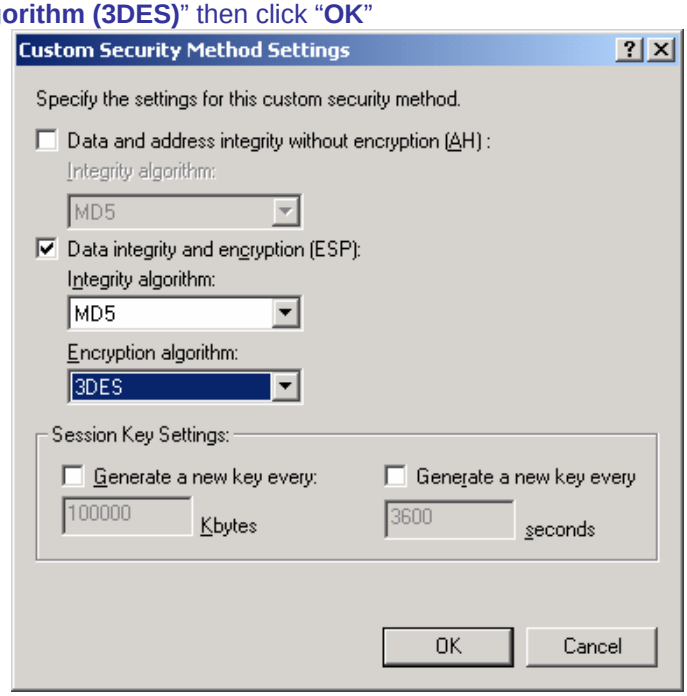
30.Select “**Do not communicate with computer that do not support IPSec**” then click “**Next**”



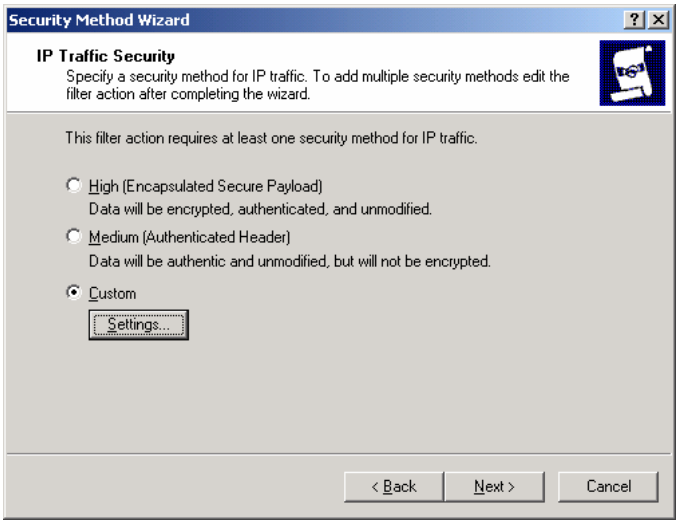
31. Select “**Custom**” then click on “**Settings**”



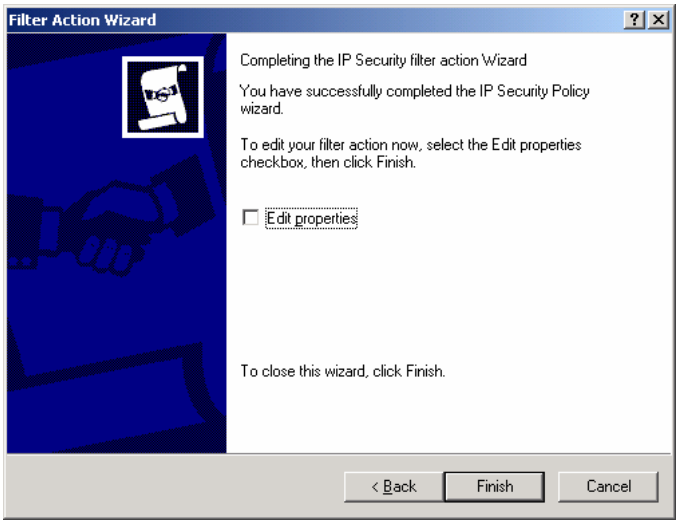
32.Check “**Data integrity and encryption (ESP)**”, select the “**Integrity algorithm (MD5)**” and “**Encryption algorithm (3DES)**” then click “**OK**”



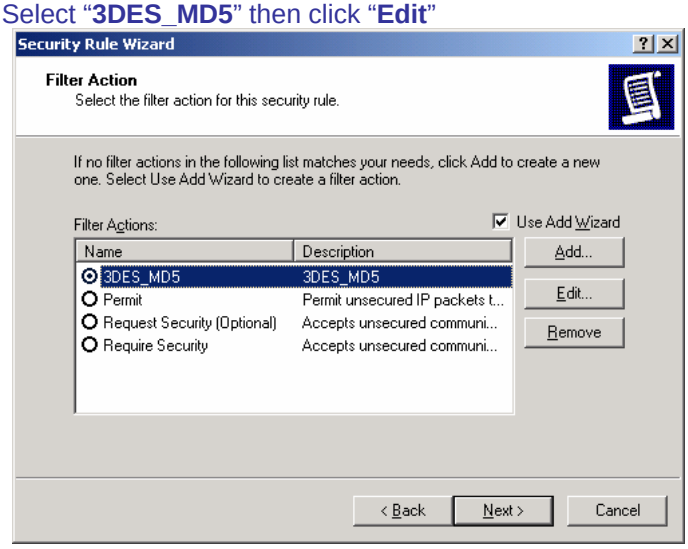
33.Click “**Next**”



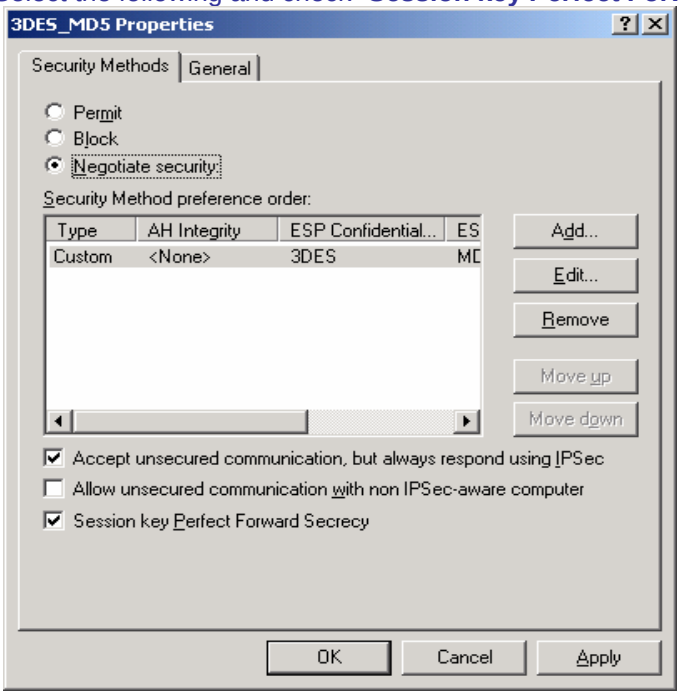
34.Click “**Finish**”



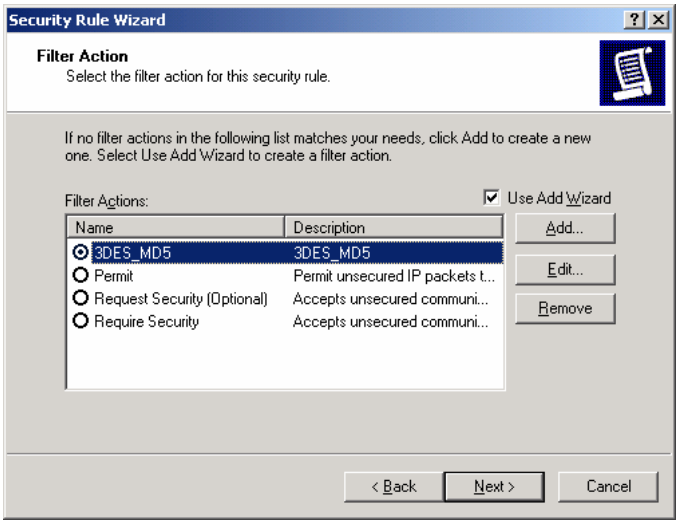
35.Select “**3DES_MD5**” then click “**Edit**”



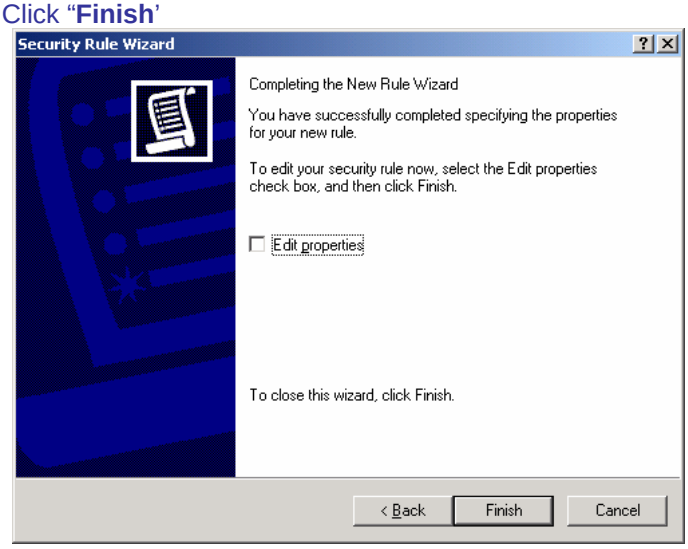
36.Select the following and check “**Session key Perfect Forward Secrecy**” then click “**OK**”



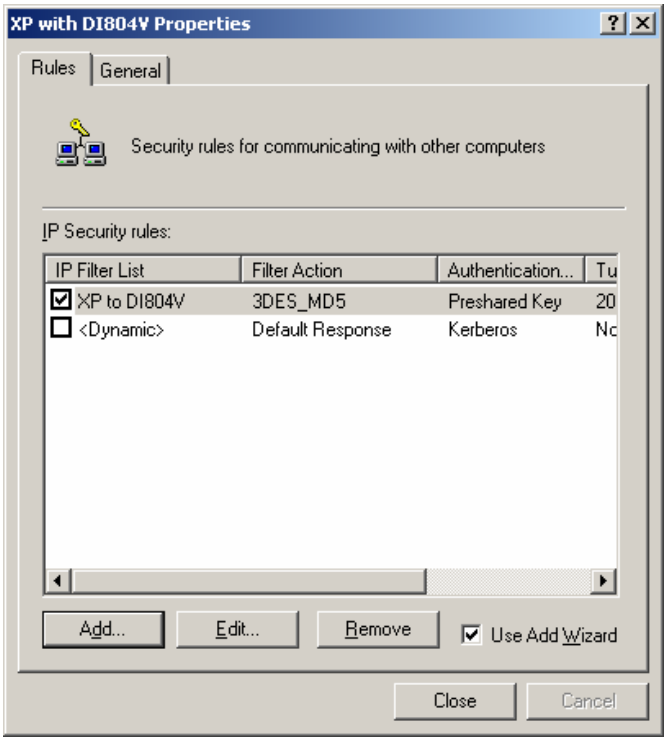
37.Click “**Next**”



38.Click “**Finish**’

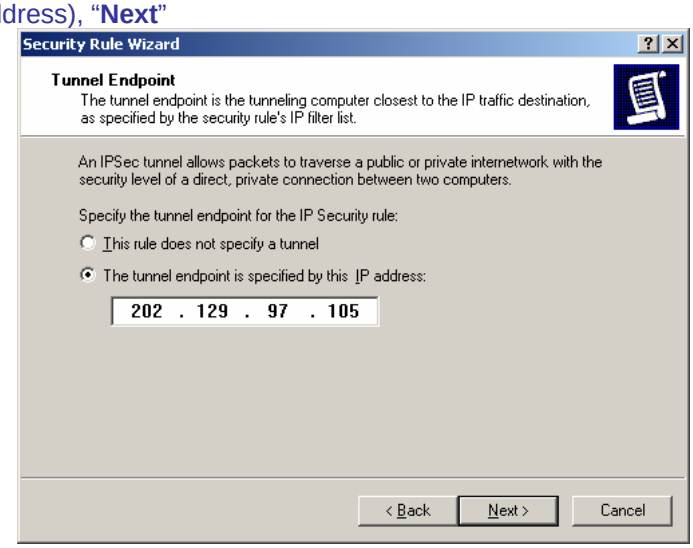


39.Click “**Add**”

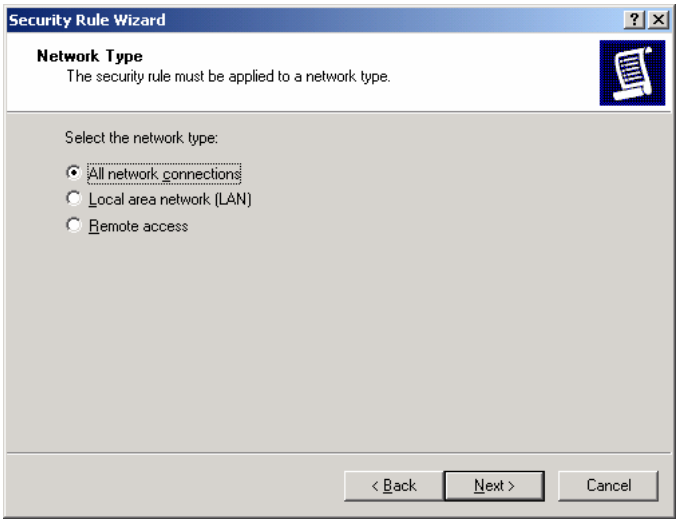


40.Click “**Next**”

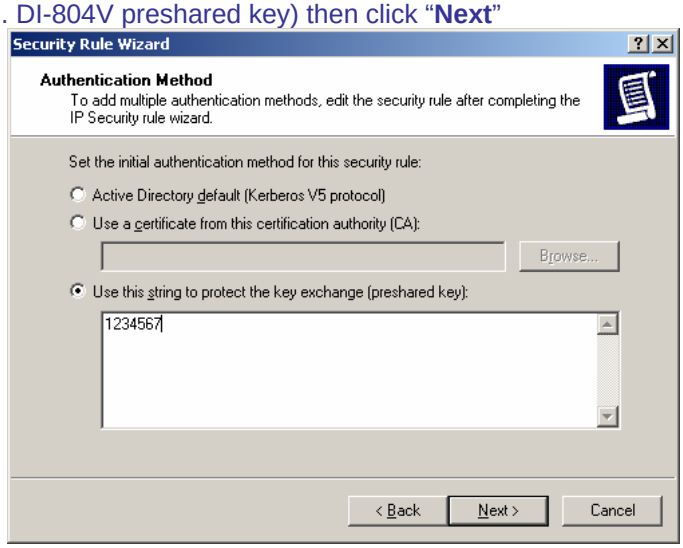
41. Input the IP Address into “**The tunnel endpoint specified by this IP address:**” (Eg. DI-804V WAN IP Address), “**Next**”



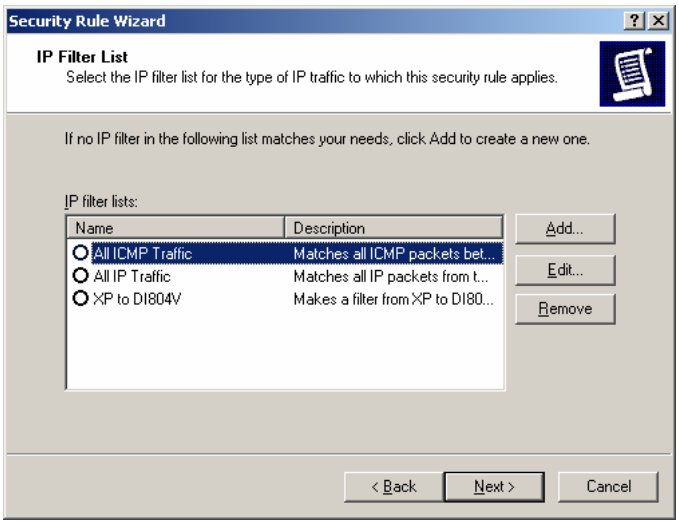
42. Select “**All network connections**” then click “**Next**”



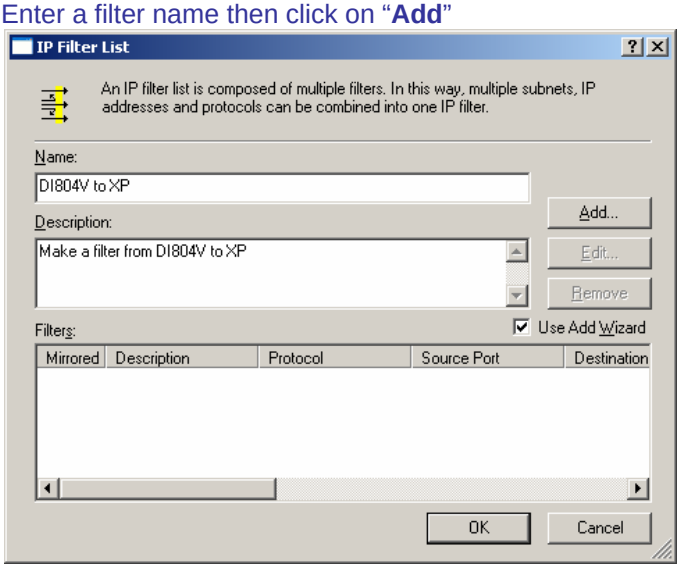
43. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DI-804V preshared key) then click "**Next**"



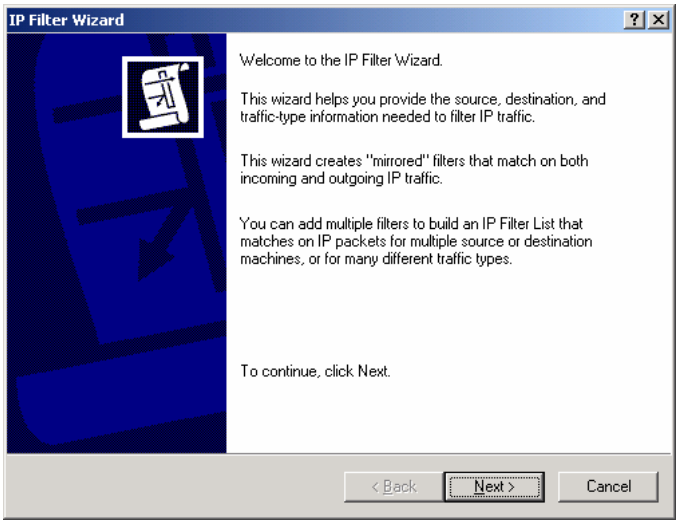
44. Click "**Add**"



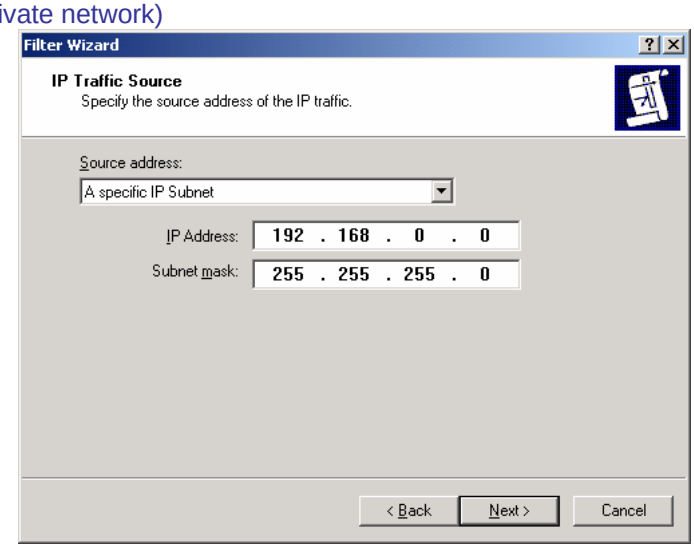
45. Enter a filter name then click on "**Add**"



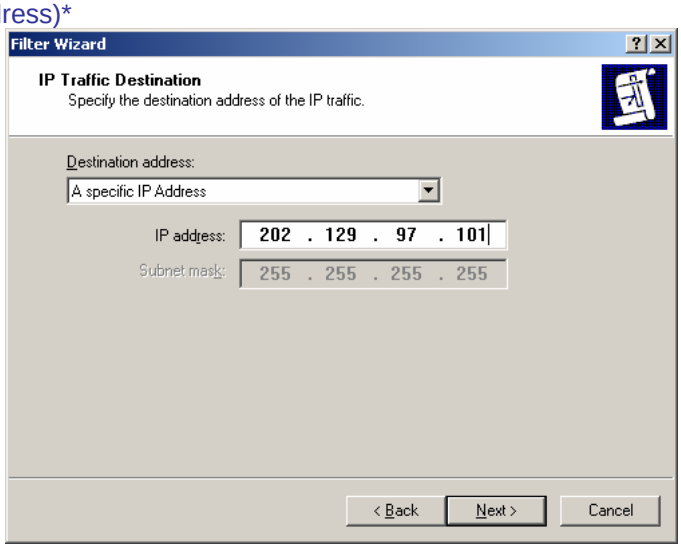
46.Click “**Next**”



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

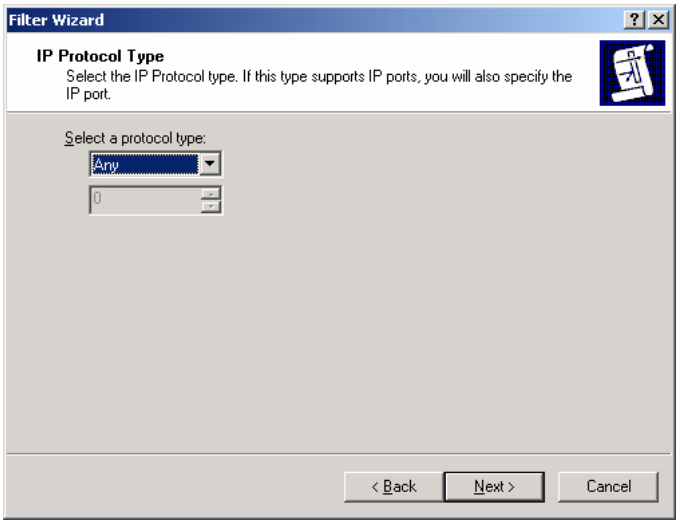


48. Select “**A specific IP Address**” and input the Destination address then click “**Next**” (Eg. Windows XP IP address)*

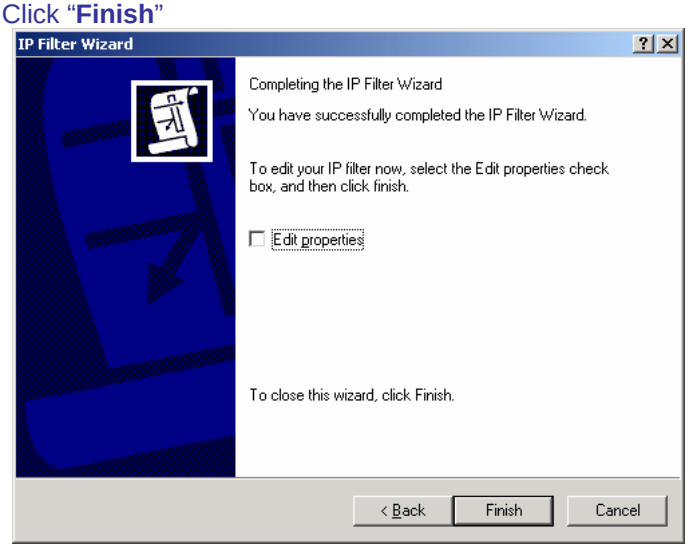


* If your client gets IP address dynamically choose “My IP Address”.

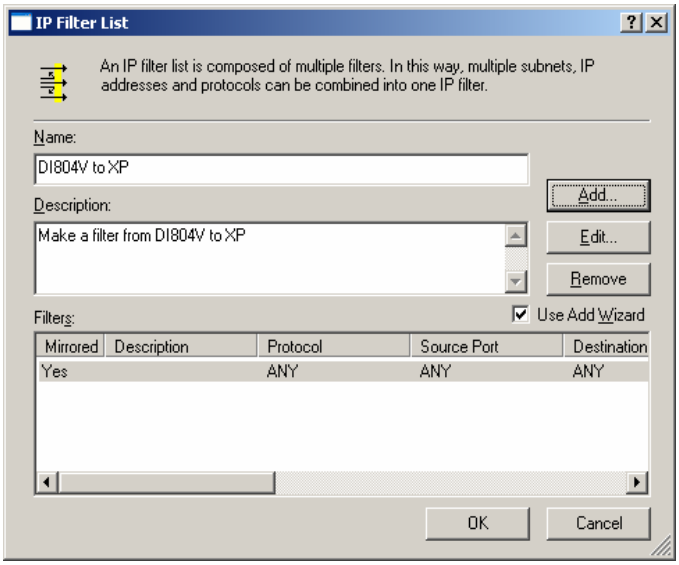
49.Click “**Next**”



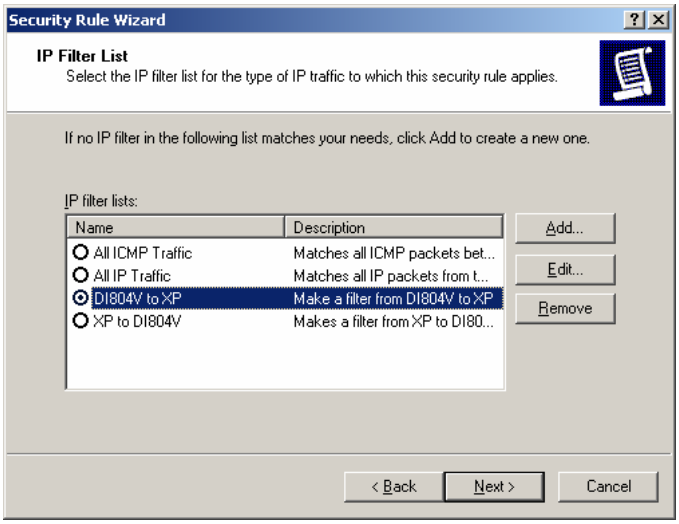
50.Click “**Finish**”



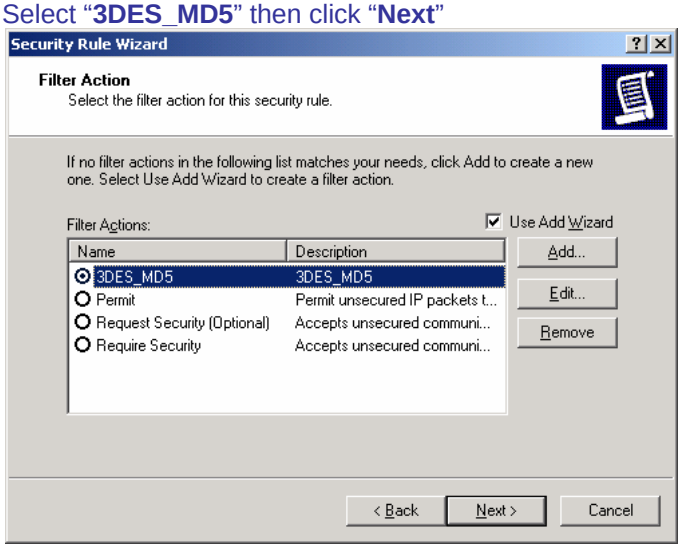
51.Click on “**Close**”



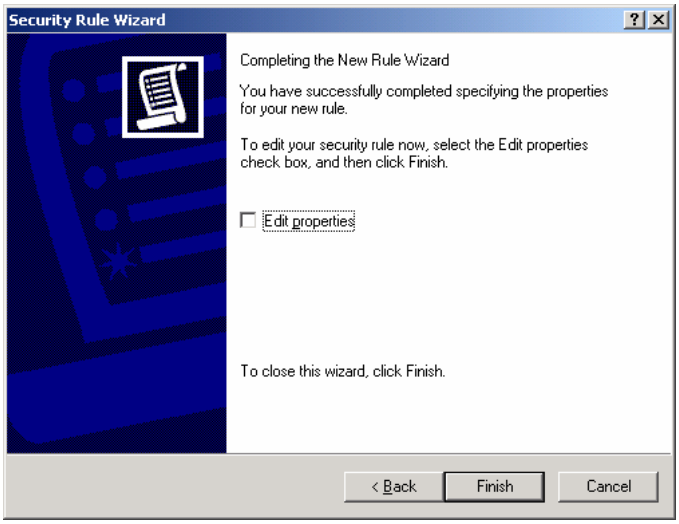
52.Select “**DI-804V to XP**” then click “**Next**”



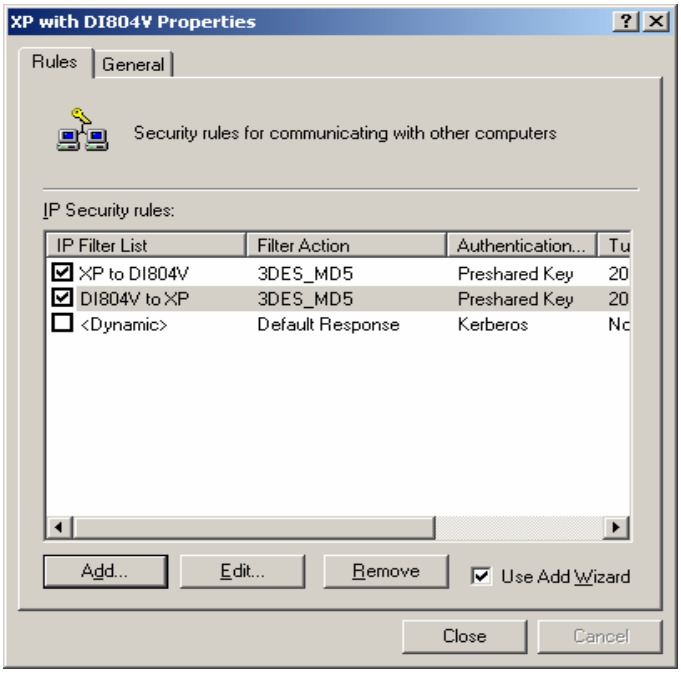
53. Select “**3DES_MD5**” then click “**Next**”



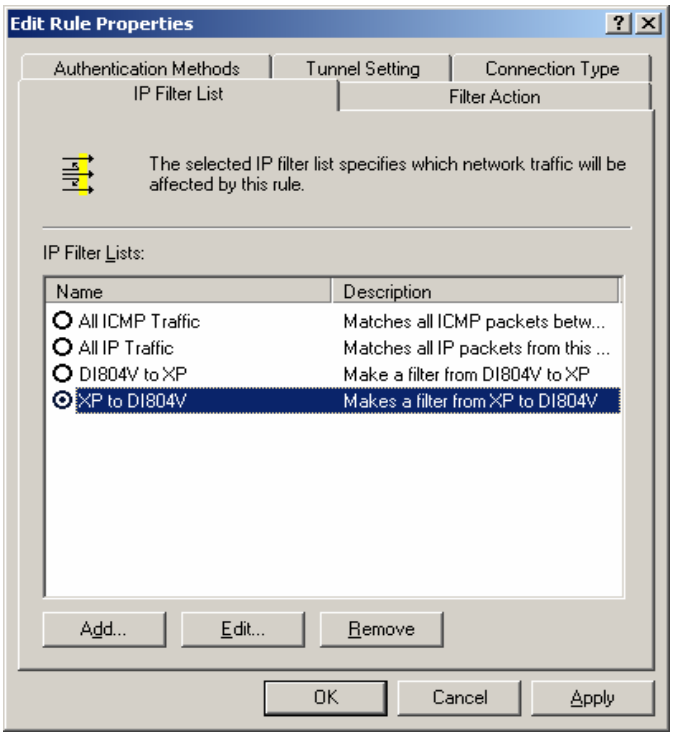
54.Click “**Finish**”



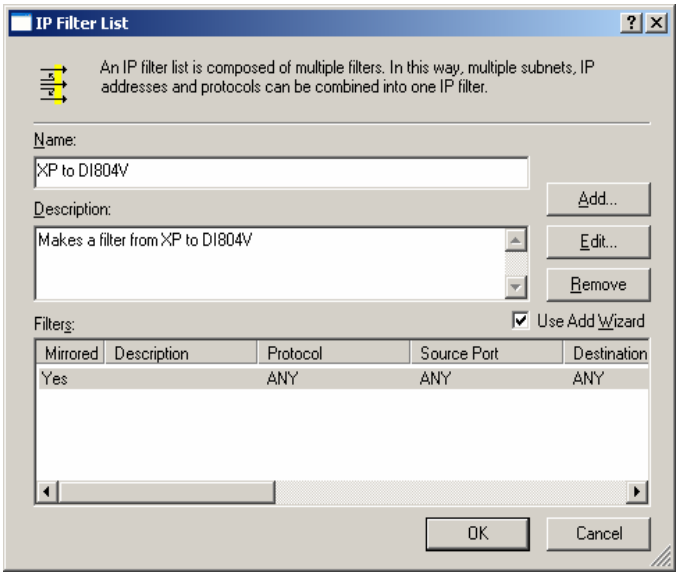
55.Select “**XP to DI-804V**” then click on “**Edit**”



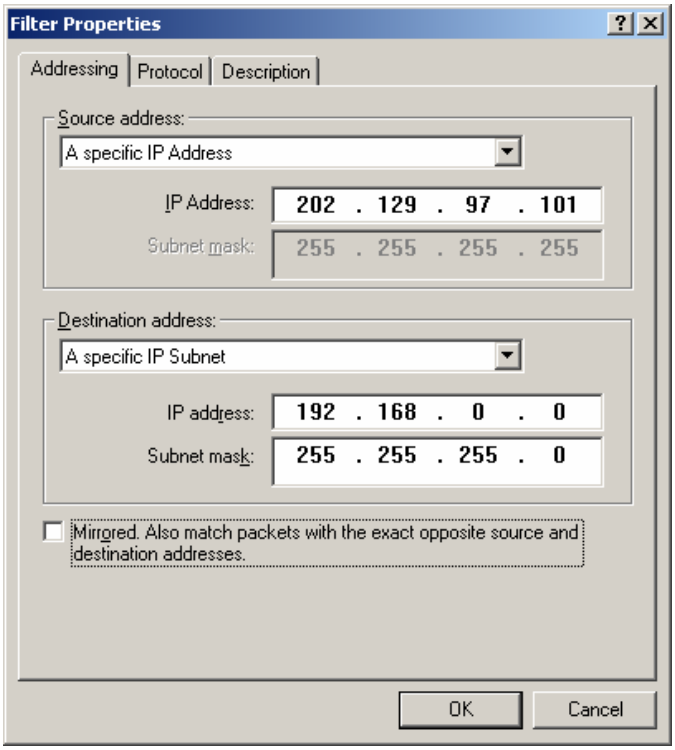
56.Select “**XP to DI-804V**” then click on “**Edit**”



57.Click “**Edit**”

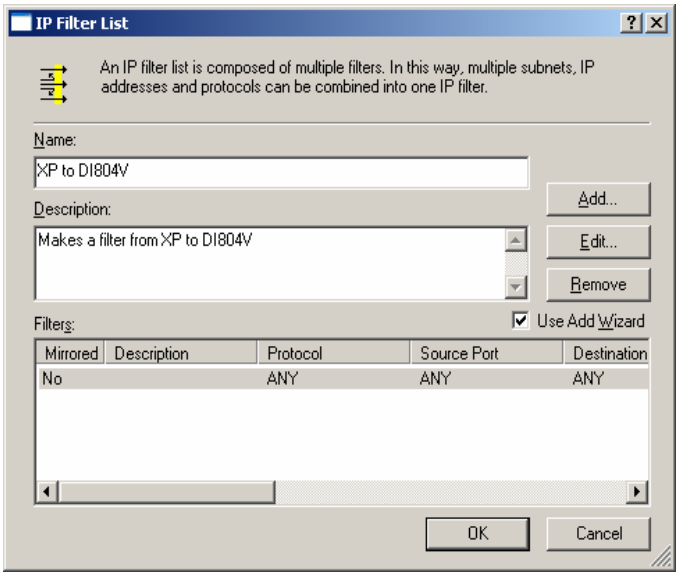


58.Uncheck “**Mirrored. Also match packets with exact opposite source and destination address**” then click “**OK**” *

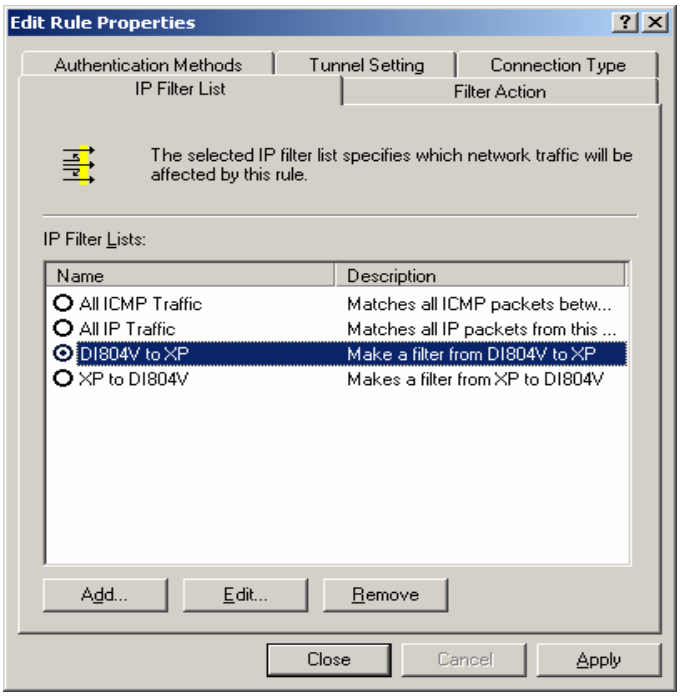


* If your client gets IP address dynamically you will see “My IP Address” in Source address field.

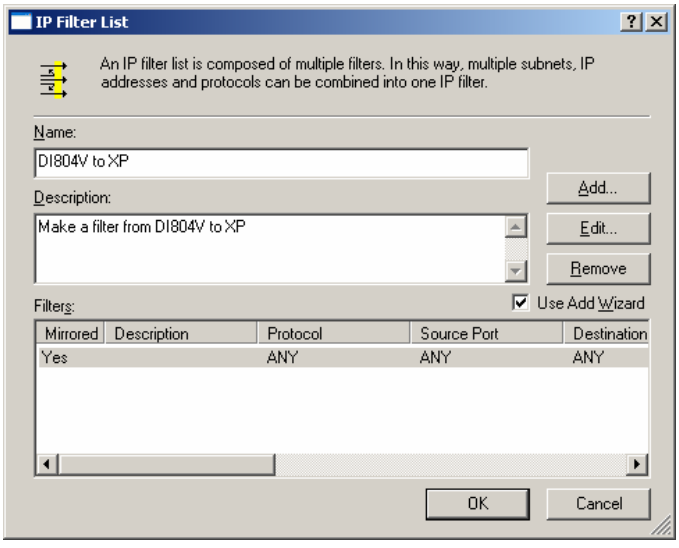
59.Click “**Close**”



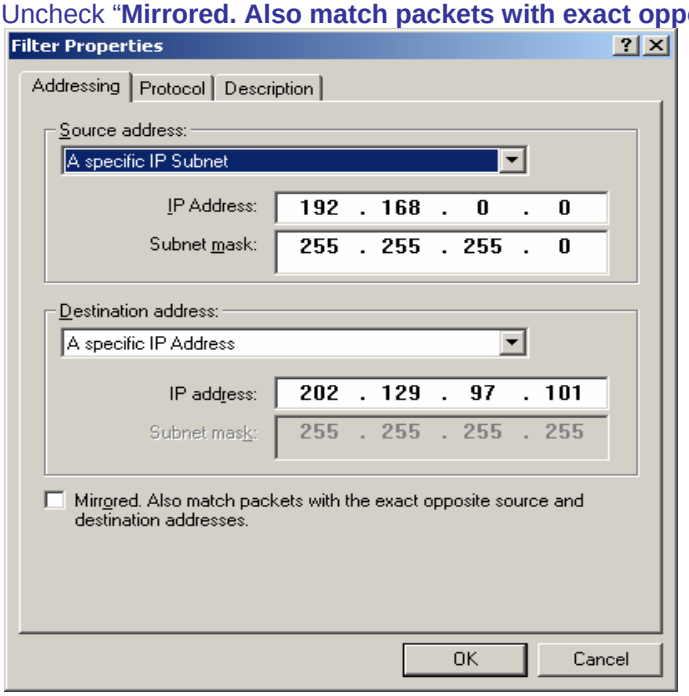
60. Select “**DI-804V to XP**” then click on “**Edit**”



61.Click “**Edit**”

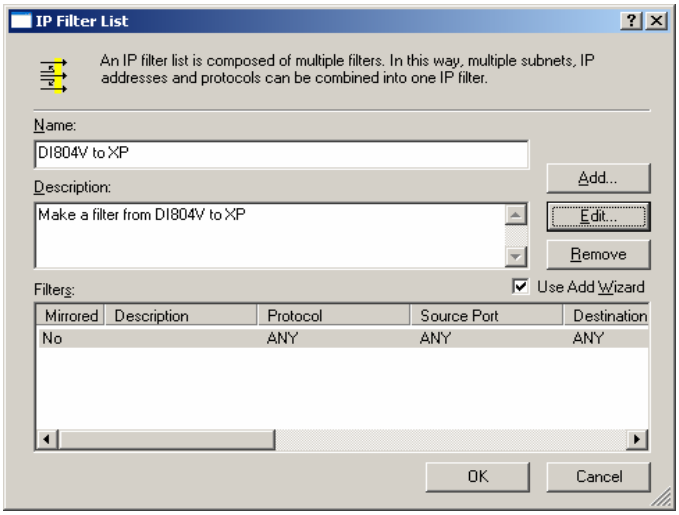


62. Uncheck “**Mirrored. Also match packets with exact opposite source…**” then click “**OK**” *

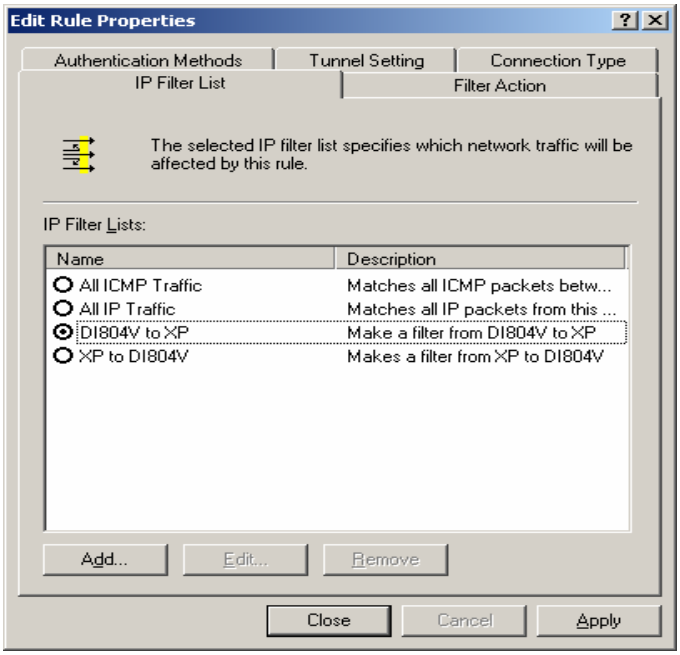


* If your client gets IP address dynamically you will see “My IP Address” in Destination address field.

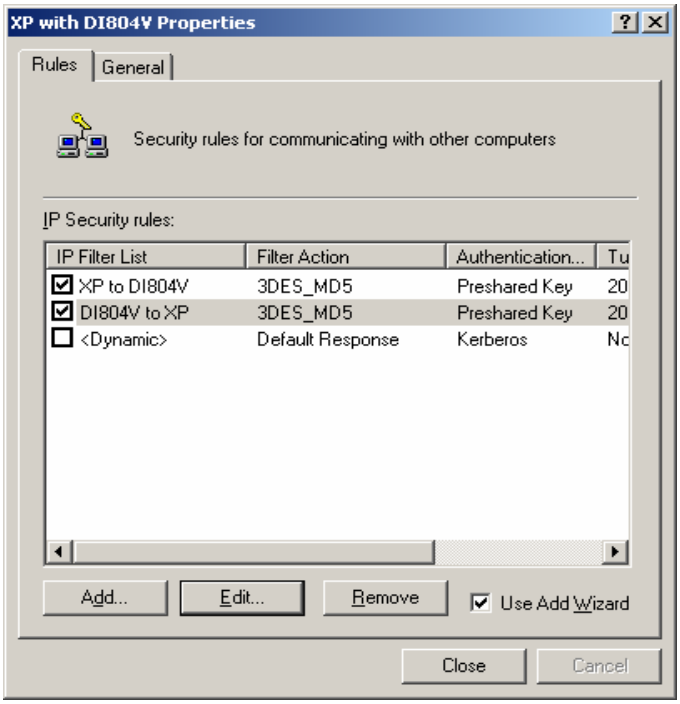
63.Click “**Ok**”



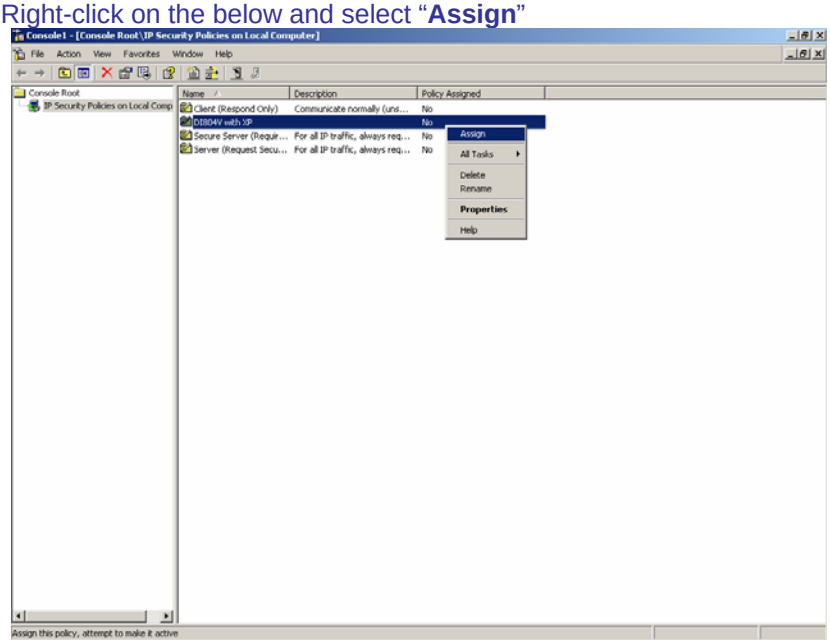
64.Click “**Close**”



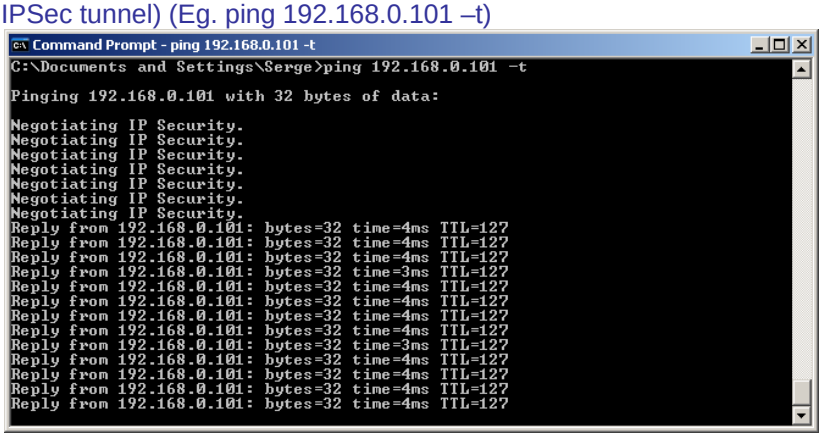
65.Click “**Close**”



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

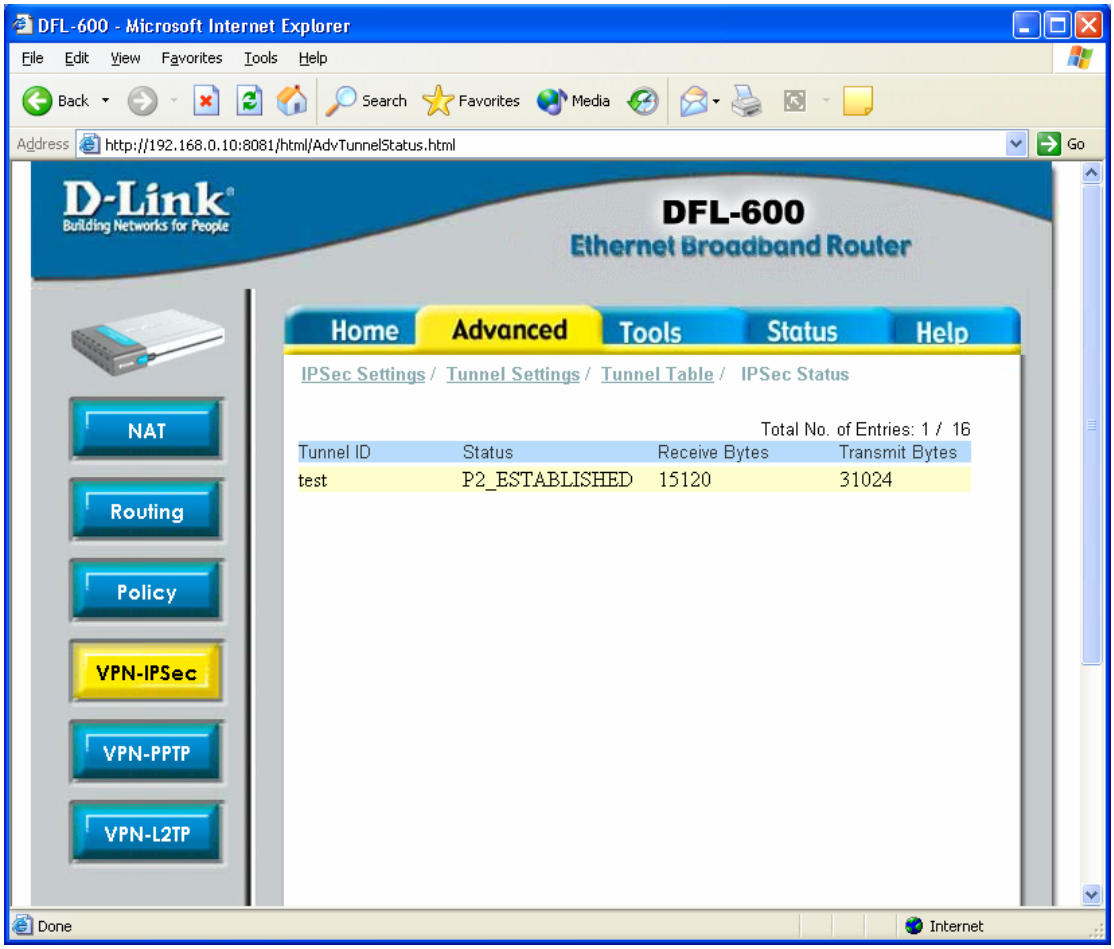


67.Do a **PING** to a valid machine on the Remote private network on the Dos Command Prompt (to bring up the IPSec tunnel) (Eg. ping 192.168.0.101 –t)

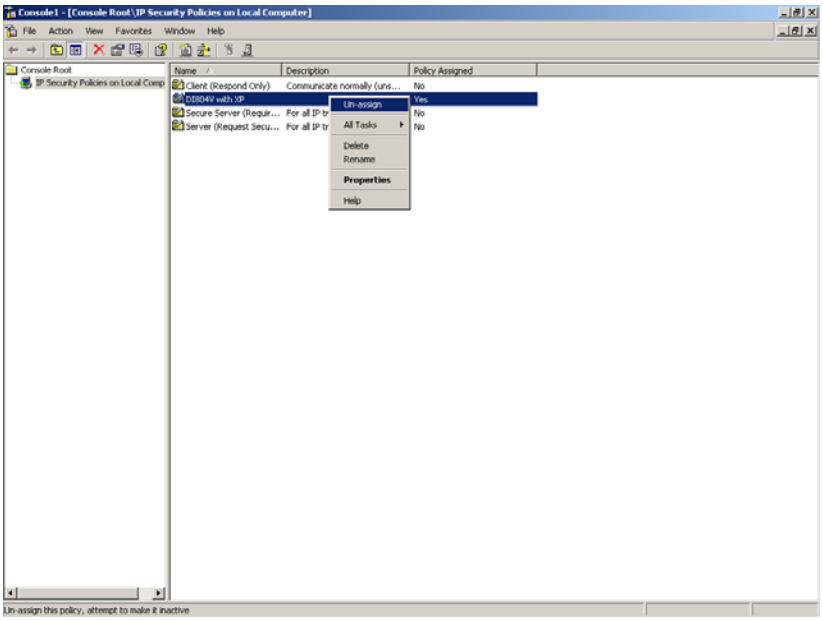


III. Monitoring and managing the VPN connection

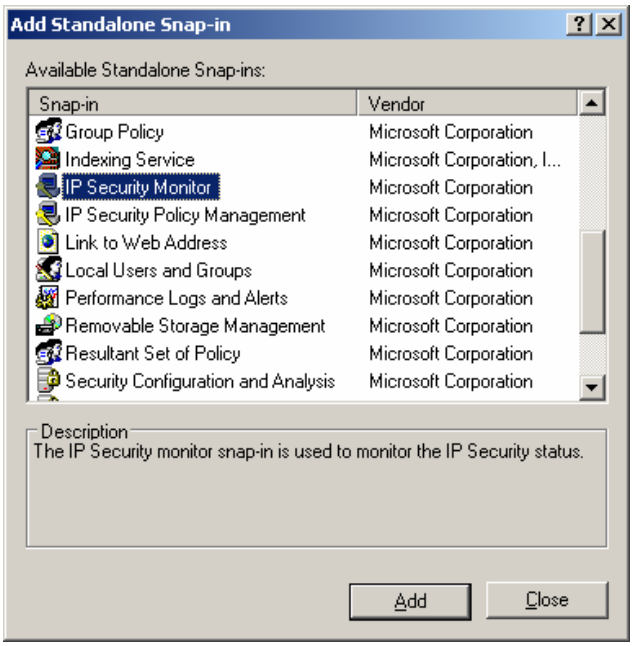
You can use two tools to monitor your VPN connection. It is Microsoft IP Security Monitor and D-Link DFL-600 VPN Router Device Status Monitor. Let's go to the VPN server menu first and check out the VPN Connection status. Go to Advanced, then click VPN-IPSec then IPSec Status. You should see something like the below.



The status of the connection is Inactive or Idle, it means, that there is no active VPN connections at this time, however the VPN connection itself is created. Later on, you will be able to drop the unnecessary or suspecting connections by clicking Drop button. You can also drop the connection by clicking the right-mouse button in Microsoft Management Concole (MMC), while pointing onto the active connection:

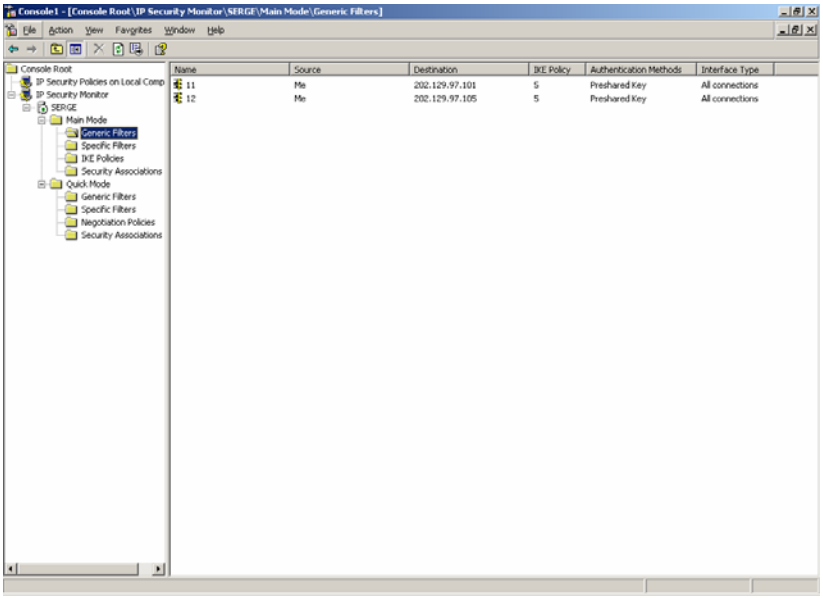


Now let's go back to Microsoft Management Console. We need to add one more Snap-in there. Go to File, then to Add/Remove Snap-in and choose IP Security Monitor:

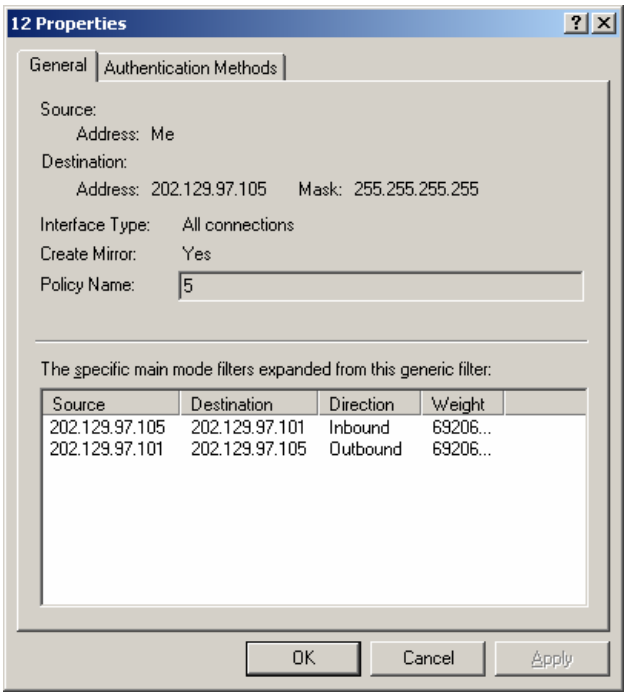


You have a choice of Generic Filters, Specific Filters, IKE Policies and Security Associations in Quick and Main modes.

Let's look at Generic Filters in Main mode:

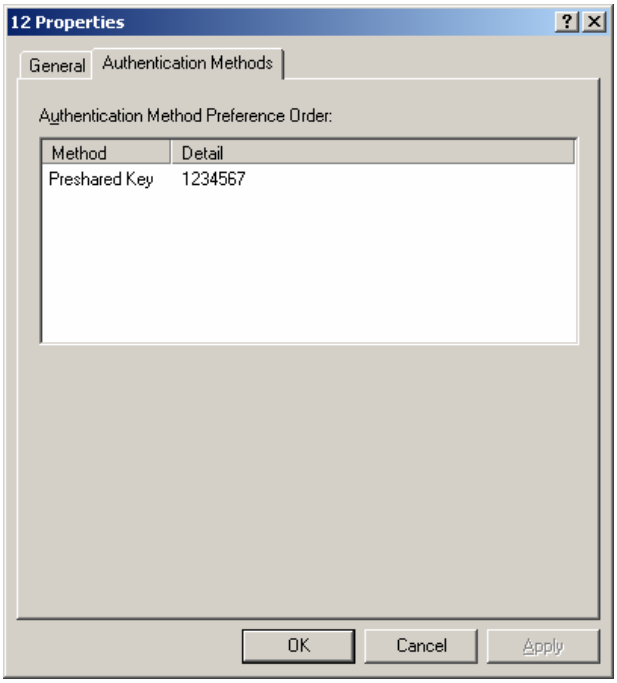


You can see two connections there: one with a destination of 202.129.97.105 and another one with a destination of 202.129.97.101. Those are our "XP to DI804V" and "DI804V to XP" connections. Now click on to the one with 202.129.97.105 connection. You will see the following:

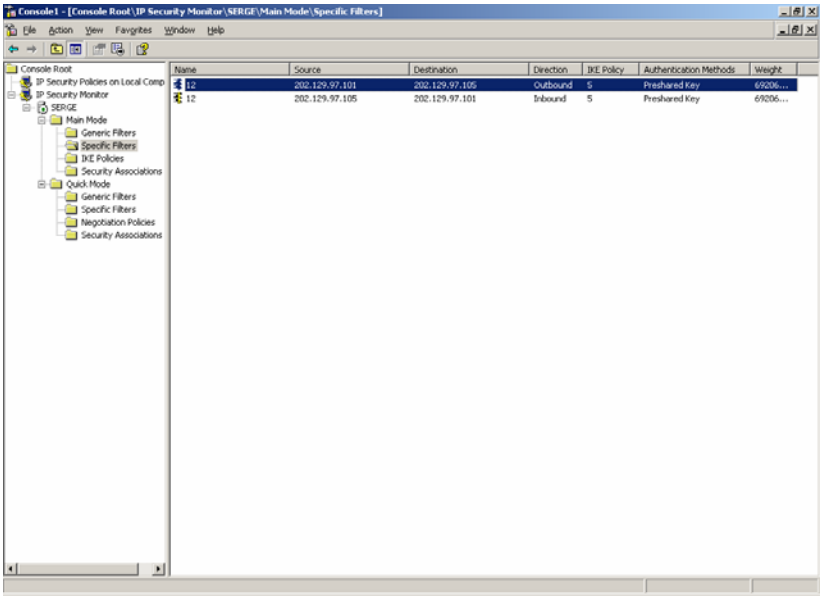


It basically tells you the source and destination of connections as well as a weight of the connection.

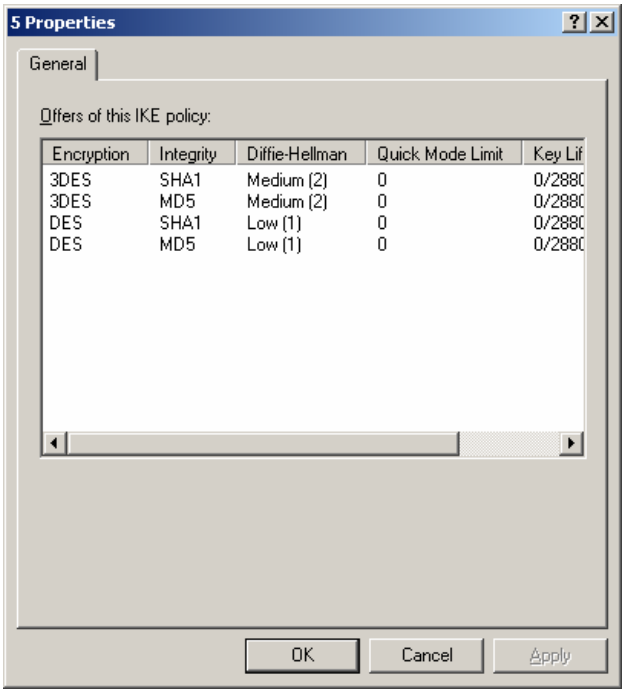
Now click on Authentication Methods:



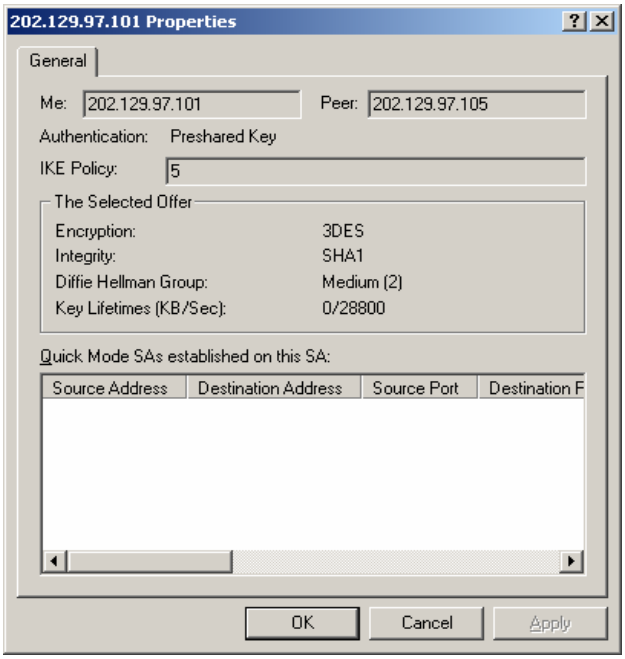
What you see there is the Preshared Key used in this connection. In Specific Filters, we basically see the same information, but in a bit different order:



In IKE Policies you can see the authentication and encryption modes available:



And finally, in the Security Associations you will see the following:



What we see here is the encryption and integrity algorithms, which were actually chosen from the options we had in IKE Policy window. The algorithms are chosen during the negotiation phase. In our example, we have a IKE Policy 5 chosen. You can also see the Key Lifetimes here.

What you see now is that the VPN connection is active. You can also see the Encryption and Integrity modes used. The state of the VPN Connection is M->Q-Established. You can also see the amount of packets received and send as well as up time. As previously told, you can drop the connection by clicking Drop on the VPN Router, or Un-assigning the IPSec policy in XP MMC.

That’s basically it and now you can use your VPN connection with ease.

~ End of Document ~