DI-804V With Windows XP IPSec VPN Configuration Procedures

I. Configuring D-Link DI-804V VPN Router

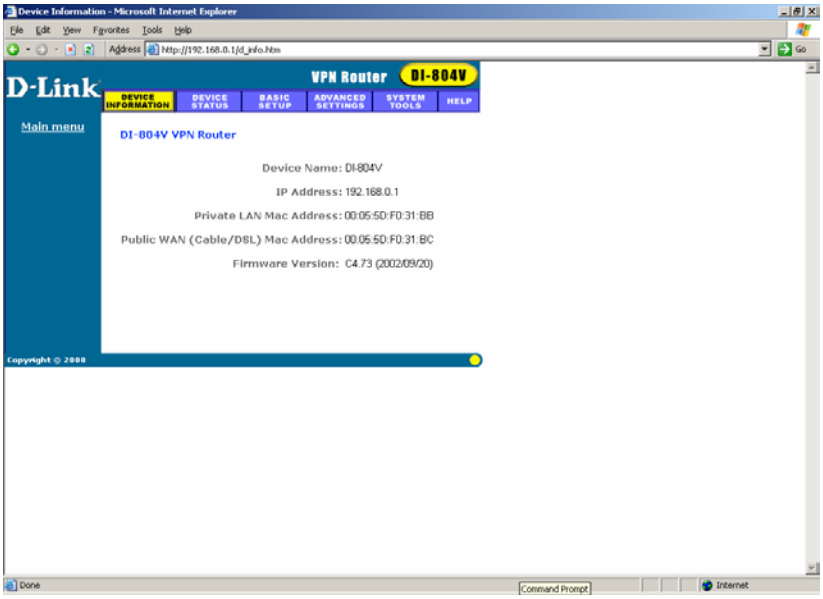
First of all you should login into your D-Link VPN Router. Please connect your PC to any of the Ethernet ports of the VPN Router.

By default the IP address of DI-804V is 192.168.0.1 255.255.255.0, thus you should configure your PC, so it would be in the same subnet as VPN router. For example, you can configure it for the IP address of 192.168.0.2 255.255.255.0 and default gateway of 192.168.0.1. The default gateway should always point to VPN Router. You can also use the dynamic IP settings on your PC, so VPN Router will give you the address automatically.

Try to ping the VPN Router to check if your PC can communicate with VPN Router. If ping is unsuccessful, that probably means that your VPN Router is configured with some other IP address. In order to get the Router back to default settings press Factory Reset button on the back of unit. After resetting, the IP address of the unit will be 192.168.0.1 255.255.255.0.

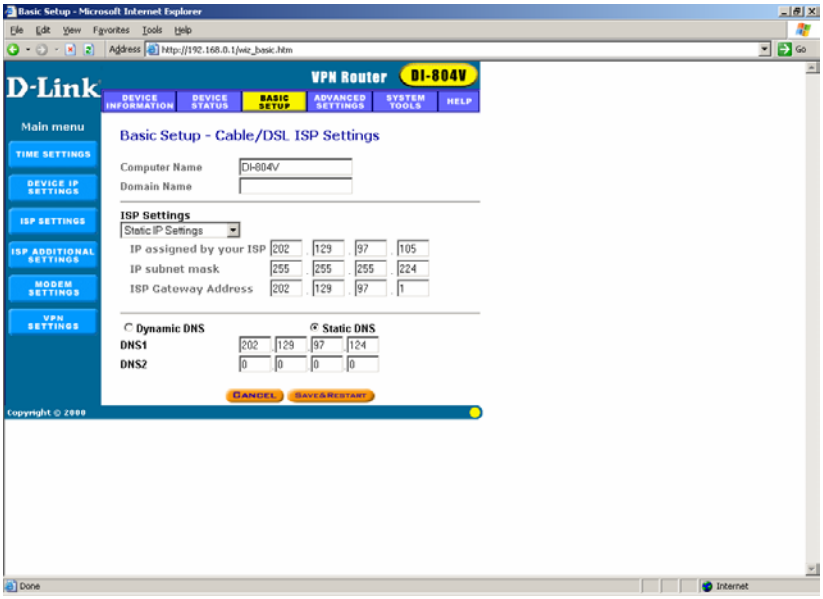
Now you should open your Internet Explorer and type http://192.168.0.1 in the Address bar. The login prompt will appear. You should use the login name “admin” and leave the password blank. You can set up the password later on. If you cannot log into the Router with blank password, that means that the password was changed. You should Factory Reset the unit in order to login into it. After you have logged in, you will see the following screen:

Now, let's go to the Device Information. You will see the following screen there:

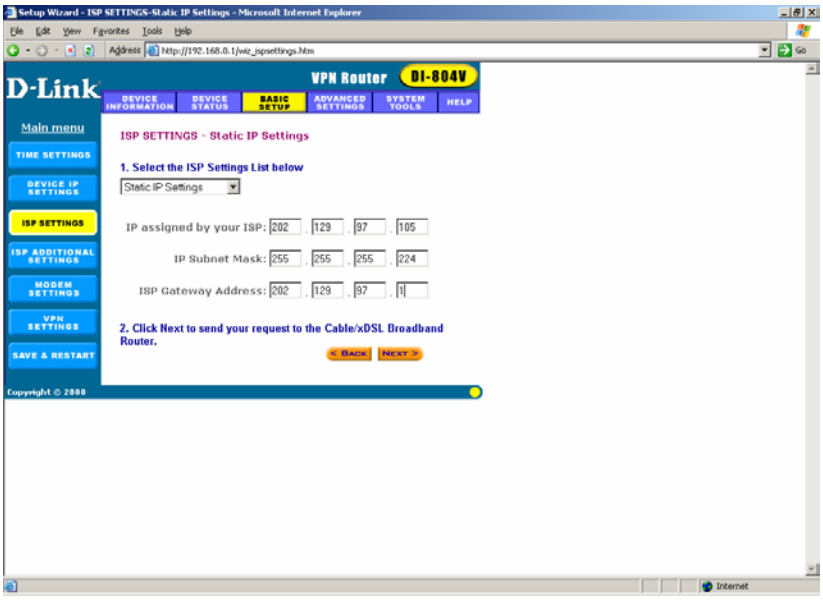


You will see the device name, IP address of the unit, Private and Public MAC addresses as well as firmware version. It is always recommended that you use the latest firmware available. By the time of this writing the latest firmware version available is 4.73.

Now you should go to the Basic Setup menu and configure Cable/DSL ISP Settings. It can be a Static IP, PPPoE, PPTP or Telstra. For PPPoE, PPTP and Telstra you must specify the user name and the password. Let's configure a static IP for our example. We will use the IP address of 202.129.97.105 255.255.255.224 for our WAN interface and the default gateway of 202.129.97.1 255.255.255.224. For DNS server we use 202.129.97.124. Your Internet service provider must give your IP address, default gateway address and DNS server address. When you are done with Static IP configuration, you will see the following screen:

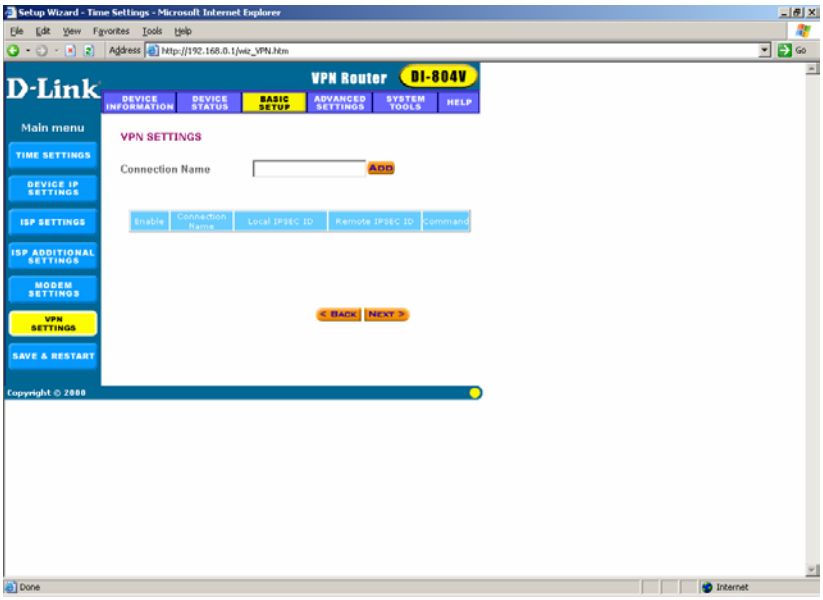


Click Save & Restart, so the unit will save the new ISP settings. After the unit is restarted, go to the Basic Setup again. Choose ISP Settings, you will see the following screen:



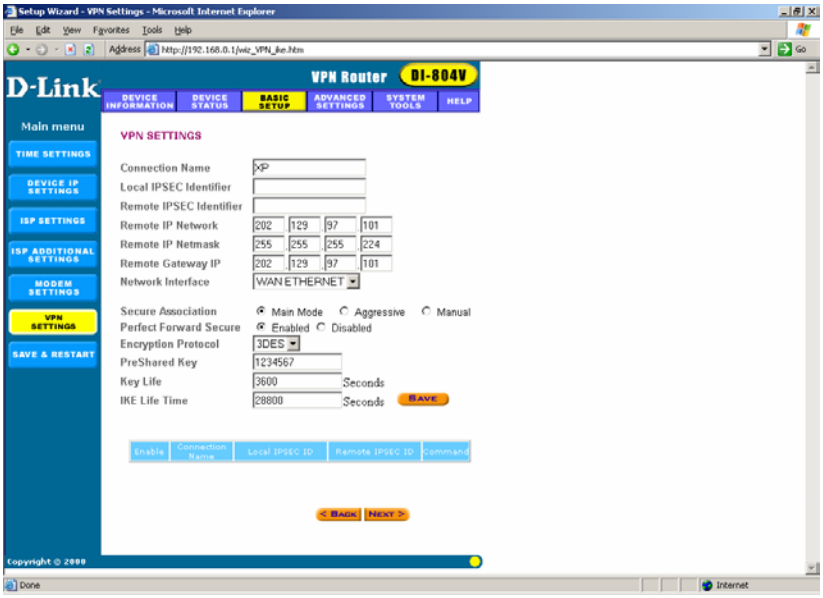
Click Next, so your VPN Router will to access Cable/xDSL Broadband Router. The connection is established now and we can go to the next step. If you have problems with the connection, check the IP (PPPoE, PPTP, Telstra) settings with your Internet service provider.

Let's go to VPN settings menu now:



Type the name of your new VPN connection and click Add. We will use VPN_Client for our example. In the next menu, you will be asked for Remote IP settings. Put the IP address of Remote IP Network, i.e. the network from which the clients will be connecting. If you want many clients from the same network to connect to your VPN Router, then put all zeros in Remote Gateway field. Otherwise, you must specify the static IP address of your client. If your client gets the IP dynamically, than you should also use 0.0.0.0 address. If you want to allow any client to connect, then put 0.0.0.0 for Remote IP Network, Remote IP Netmask and Remote Gateway.

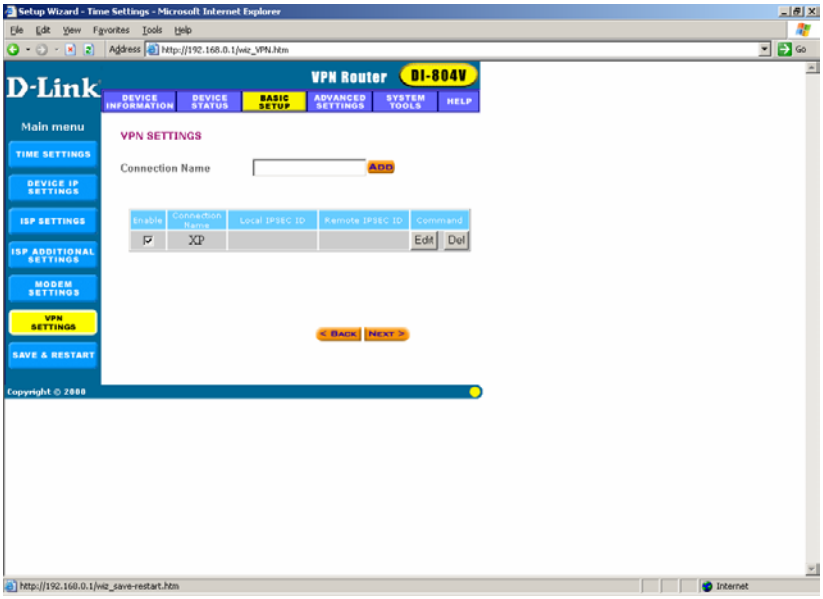
Let's look at what we have got:



You should type in the PreShared Key, which is going to be used by remote Client as well. So, don't forget the key, you will use it later, while configuring the remote Client. Be sure to remember the Key Life and IKE Life Time settings as well, they must be the same on your VPN Router and VPN Client. You may change them to whatever amount is suitable for you, but be sure to use equal settings for your client.

You can use Main, Aggressive and Manual modes for Secure Association, but be sure to use the same mode on the VPN Client. The default mode is a Main mode for VPN Router as well as for VPN Client. You have two choices for the Encryption Protocol: 3DES or DES in Main mode, you can choose Key Group in Aggressive mode and Authentication protocol in Manual mode, as well as Encryption and Authentication Keys. Once again, make sure to use equal settings for you VPN Client and VPN Router.

Now, when we are done with VPN settings, you may safely click on Save.



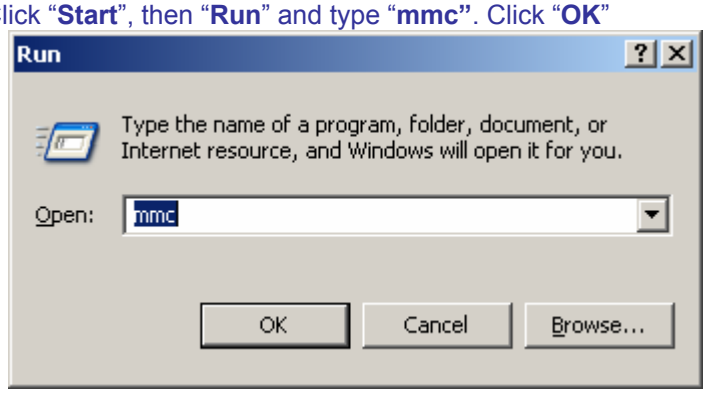
You will see the Connection we have just created. You can add more connections if you would like a client with another IP address or from the other remote network to access your internal network. The maximum amount of clients, which are supported by D-Link DI-804V VPN Router is 8.

Now you can either click on Save & Restart in the left bottom corner of the screen, or you can click Next and the system will offer you to Save & Restart the router itself. Your VPN Router is ready to get the VPN Client request.

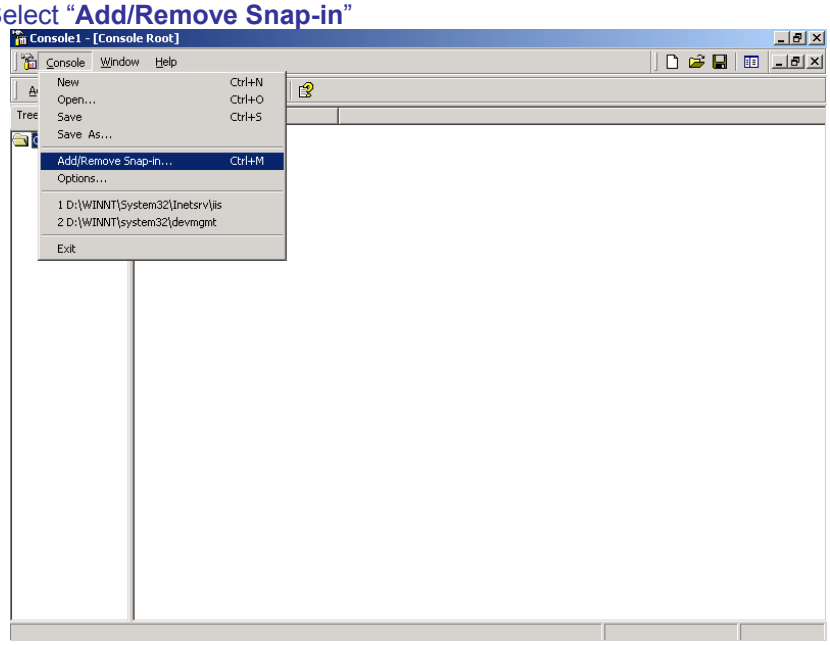
II. Configuring Windows XP IPSec Client

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.

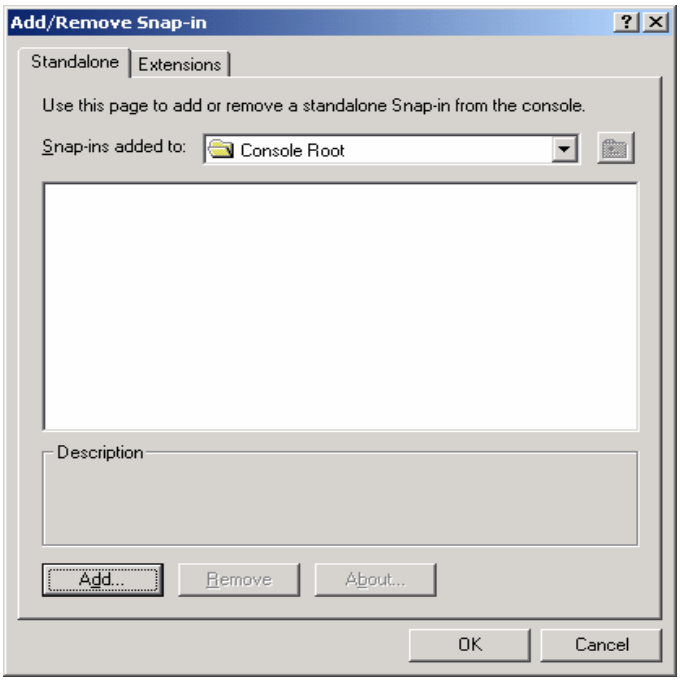
1.Click "**Start**", then "**Run**" and type "**mmc**". Click "**OK**"



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

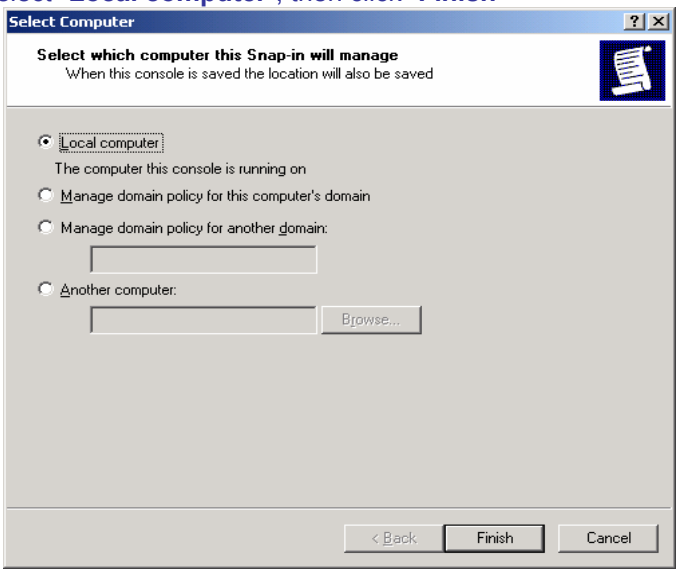


3.Click "**Add**"

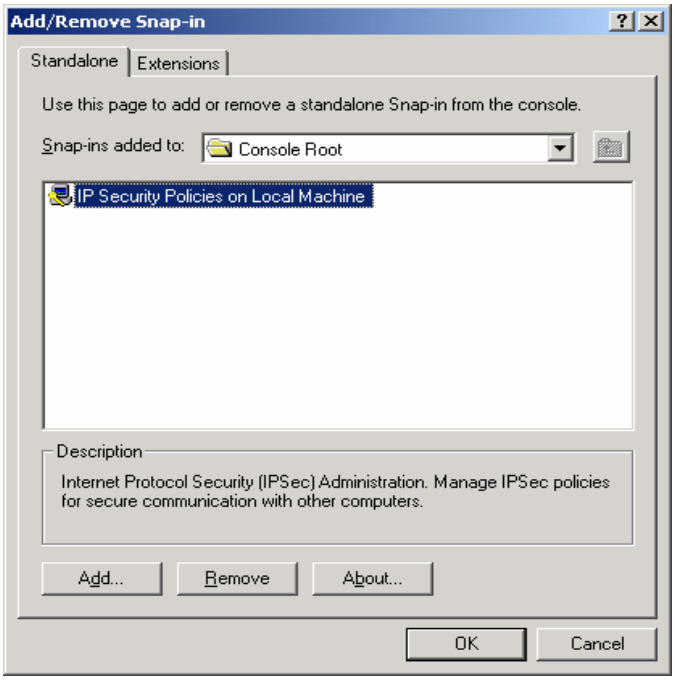


4.Select and Add "**IP Security Policy Management**"

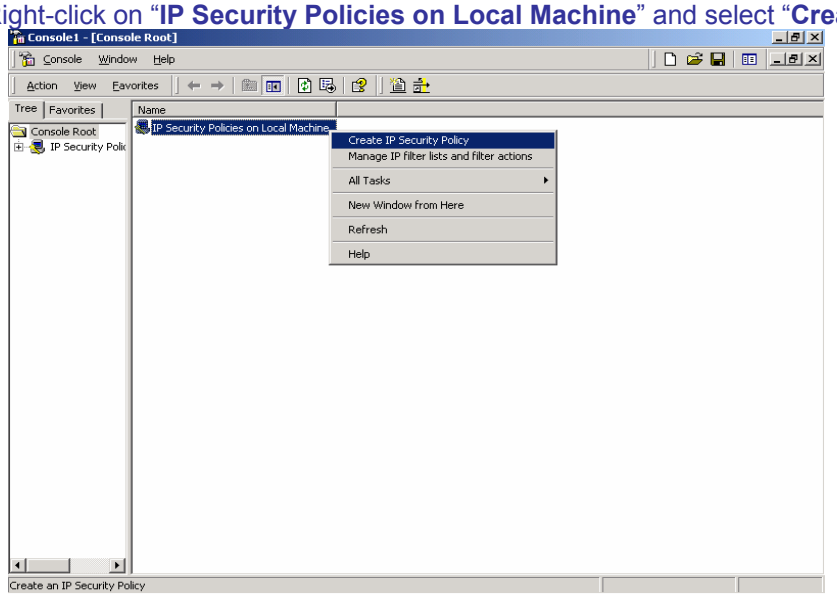
5.Select "**Local computer**", then click "**Finish**"



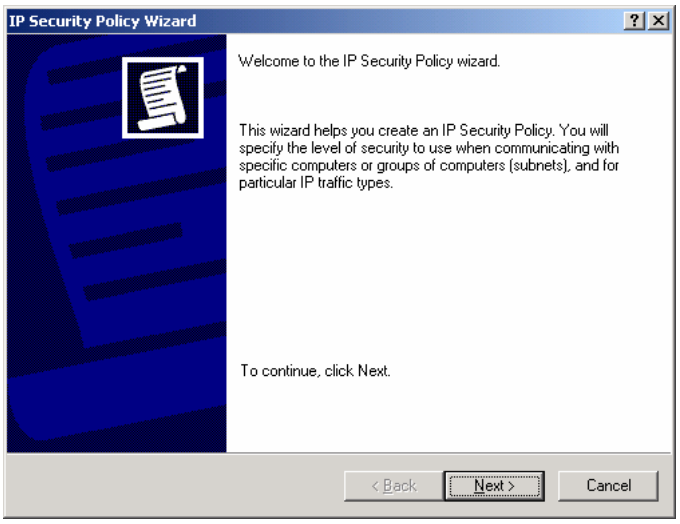
6.Click "**OK**"



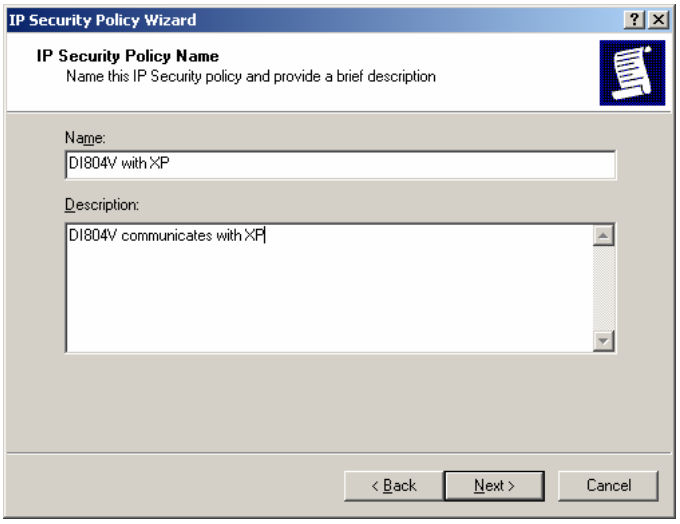
7.Right-click on “**IP Security Policies on Local Machine**” and select “**Create IP Security Policy**”



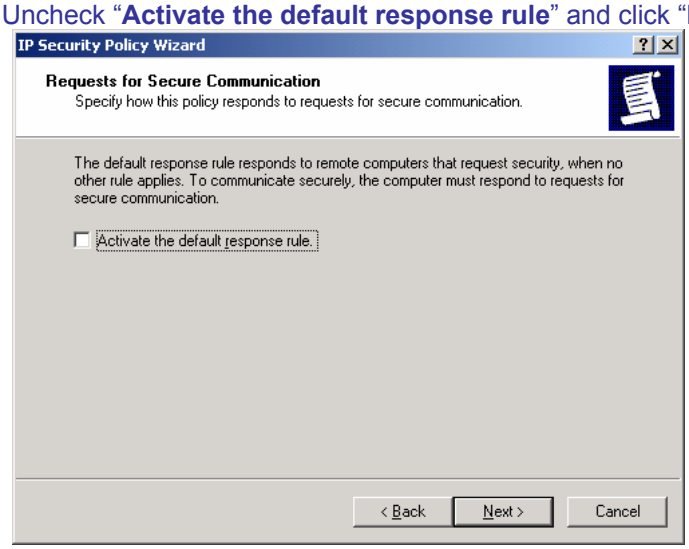
8.Click “**Next**”



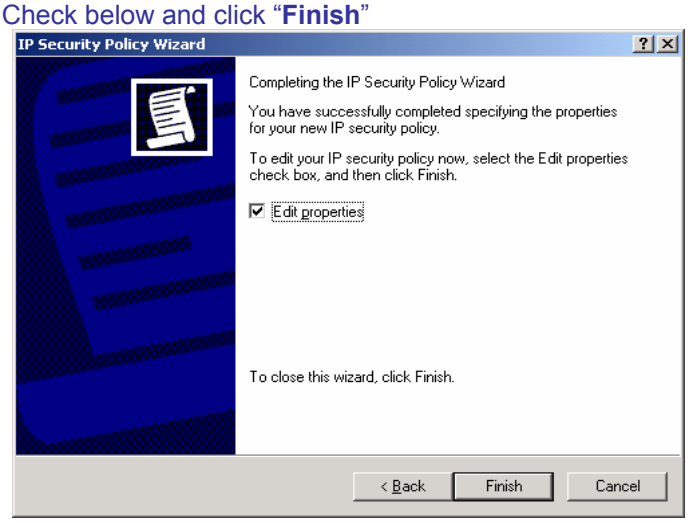
9.Enter the details below and click “**Next**”



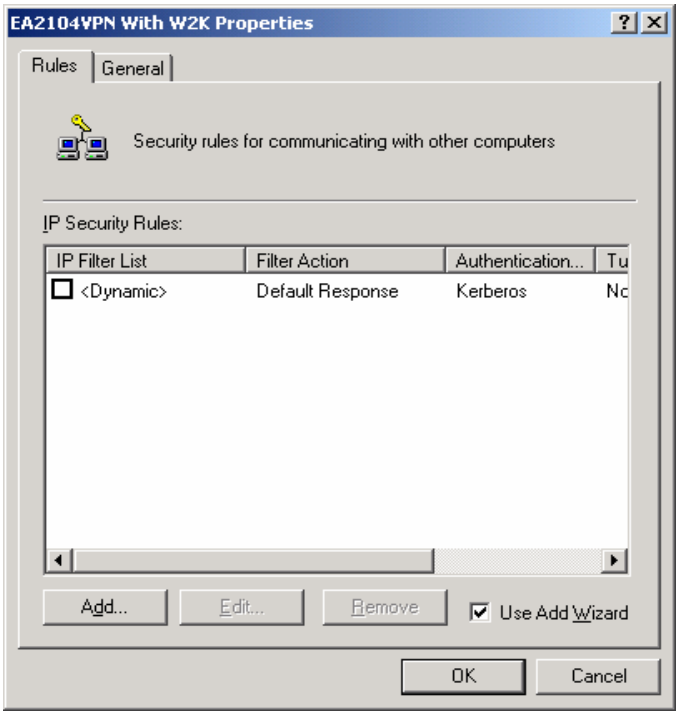
10.Uncheck “**Activate the default response rule**” and click “**Next**”



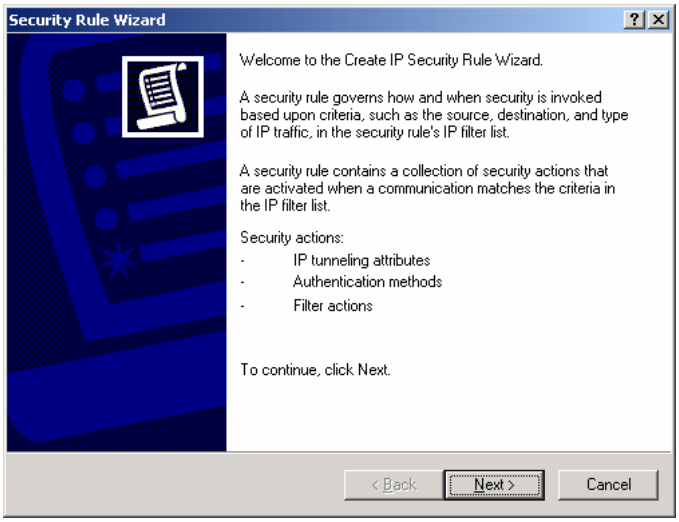
11.Check below and click “**Finish**”



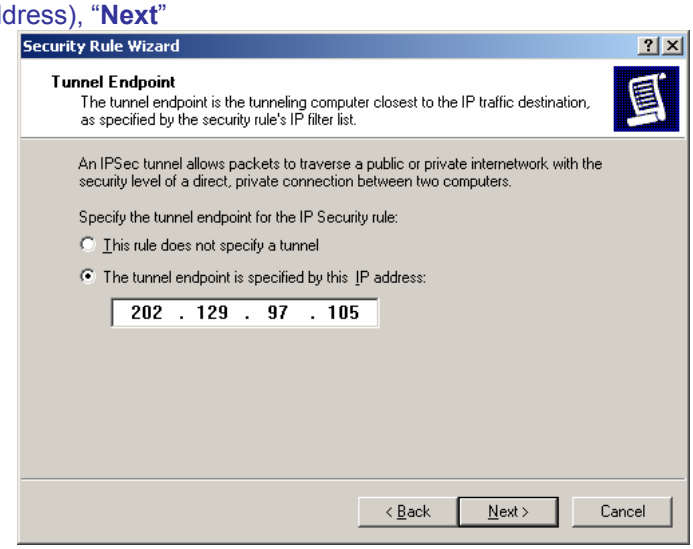
12.Select “**Add**”



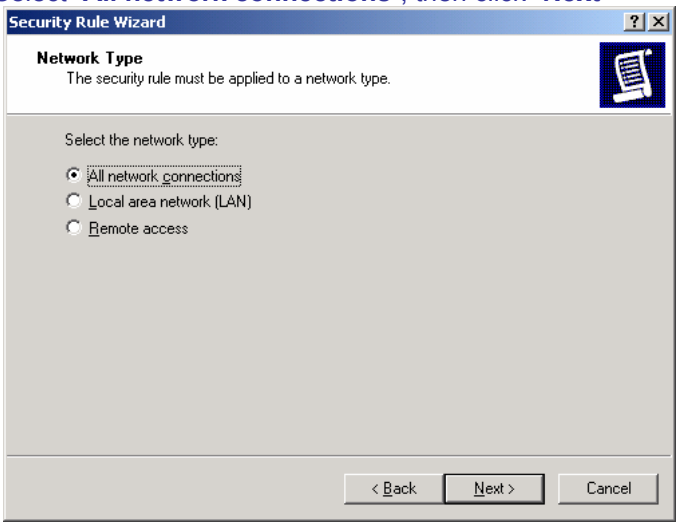
13.Click “Next”



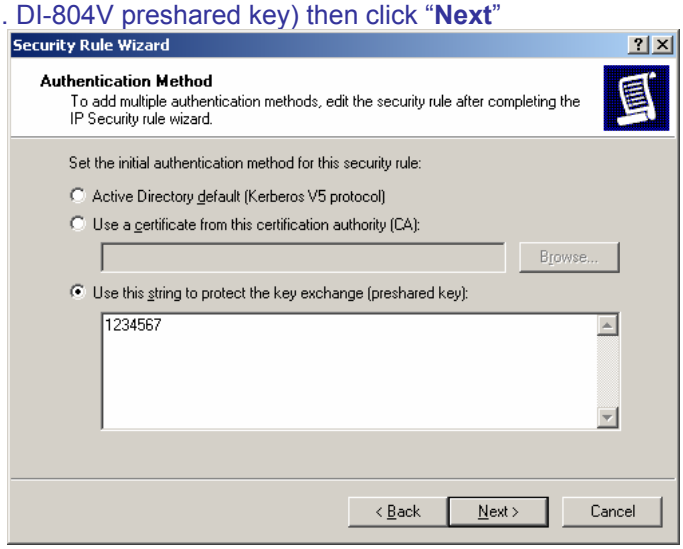
14. Input the IP Address into “**The tunnel endpoint specified by this IP address:**” (Eg. DI-804V WAN IP Address), “**Next**”



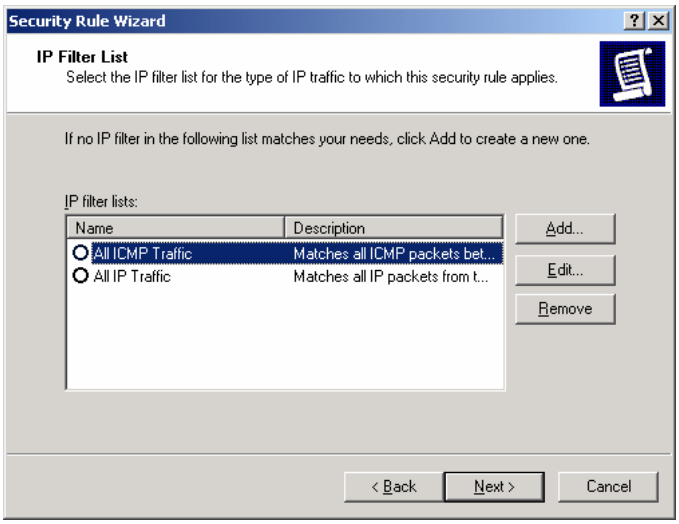
15.Select “**All network connections**”, then click “**Next**”



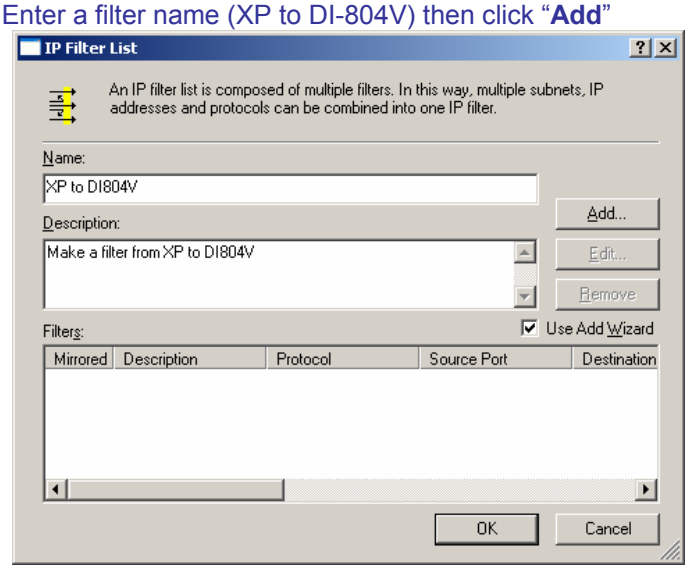
16.Select “**Use this string to protect the key exchange (preshared key)**” (Eg. DI-804V preshared key) then click “**Next**”



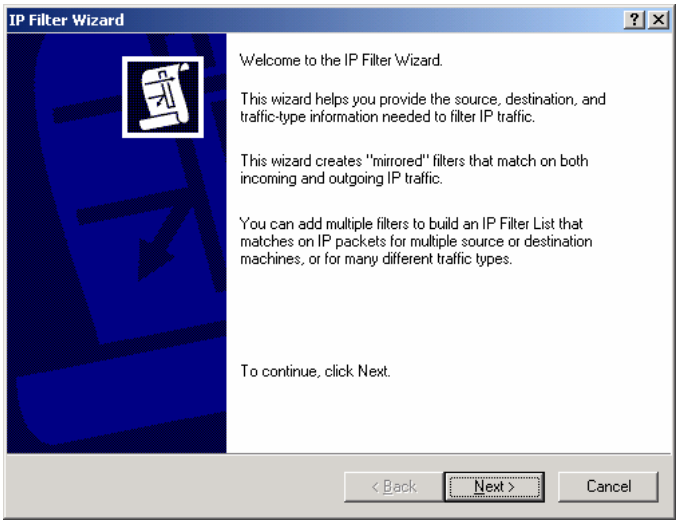
17.Select “**Add**”



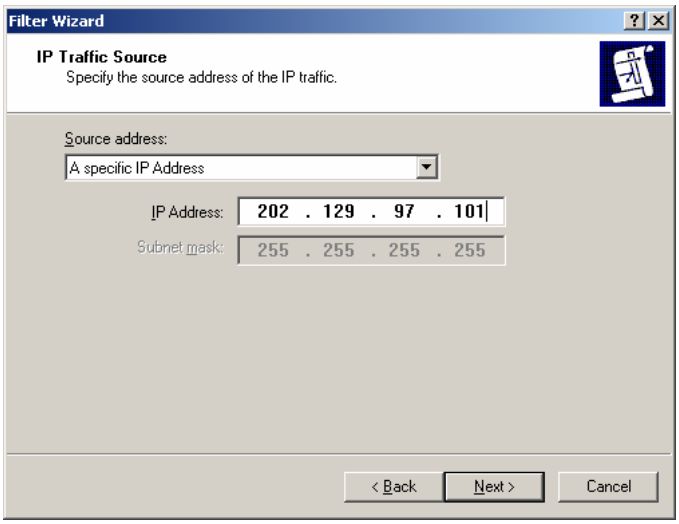
18.Enter a filter name (XP to DI-804V) then click “**Add**”



19.Click “**Next**”

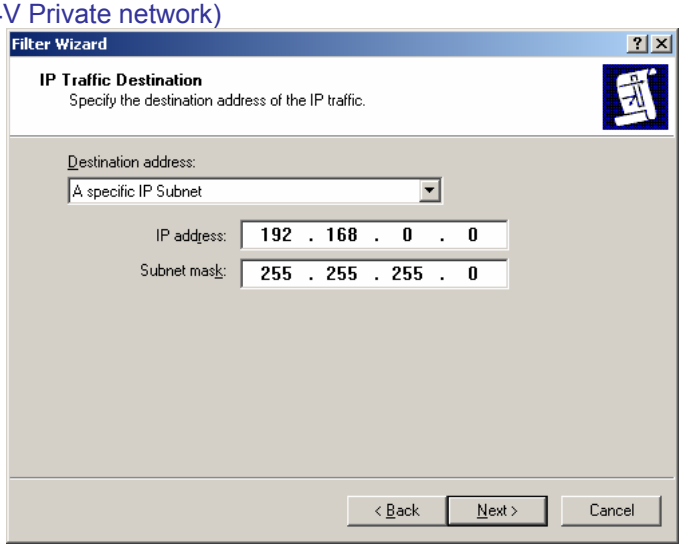


20.Select “**A specific IP Address**” and input the Source address, then “**Next**” to continue (Eg. Windows XP IP) *

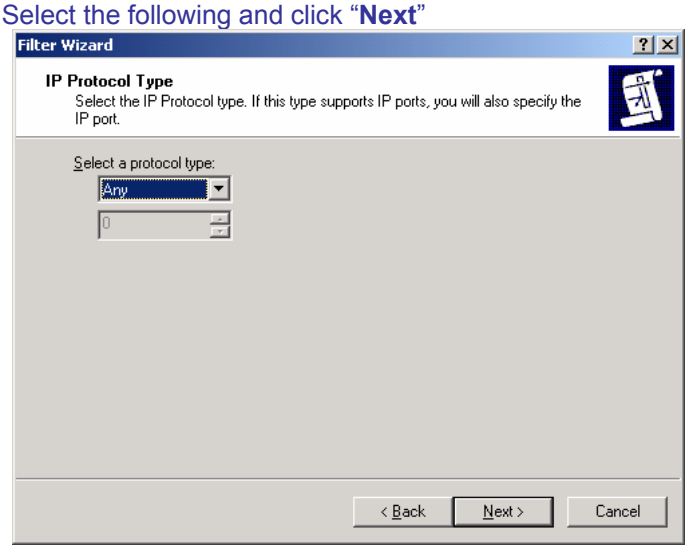


* If your client gets IP address dynamically choose “My IP address”.

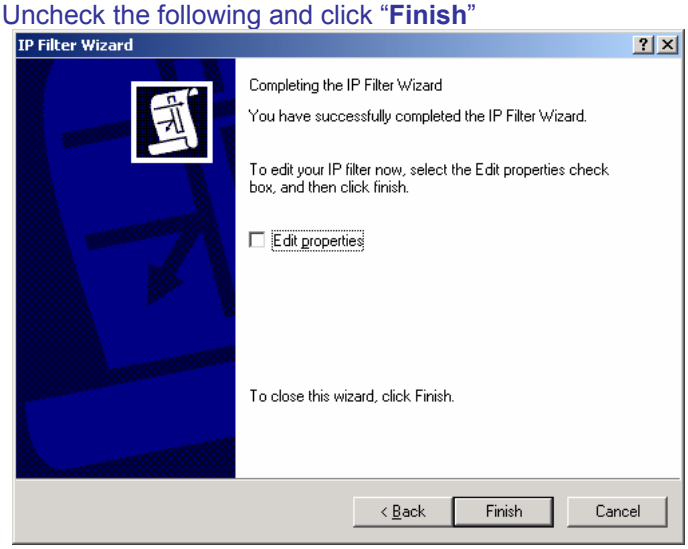
21. Select “**A specific IP Subnet**” and input the Destination subnet address, then “**Next**” to continue (Eg. DI-804V Private network)



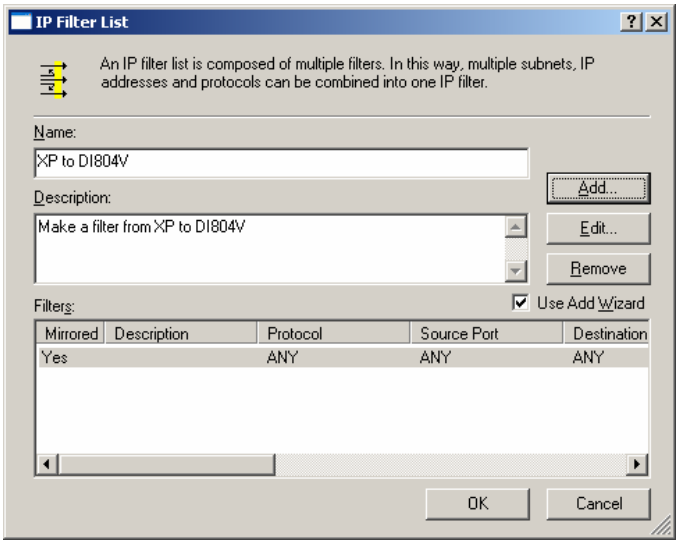
22.Select the following and click “**Next**”



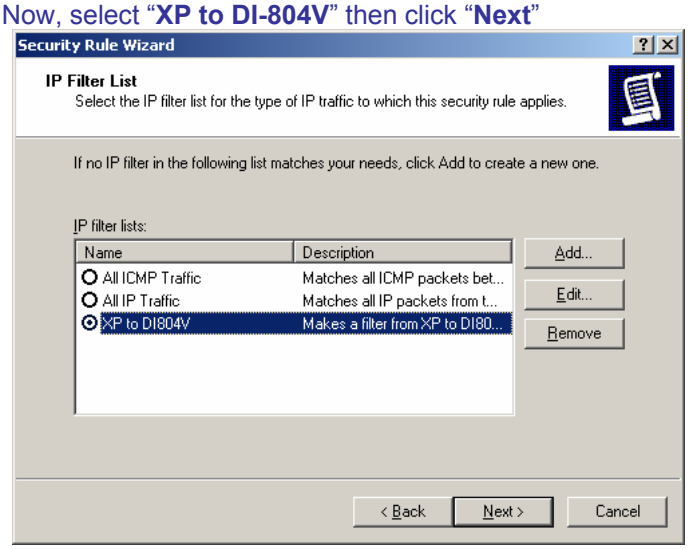
23.Uncheck the following and click “**Finish**”



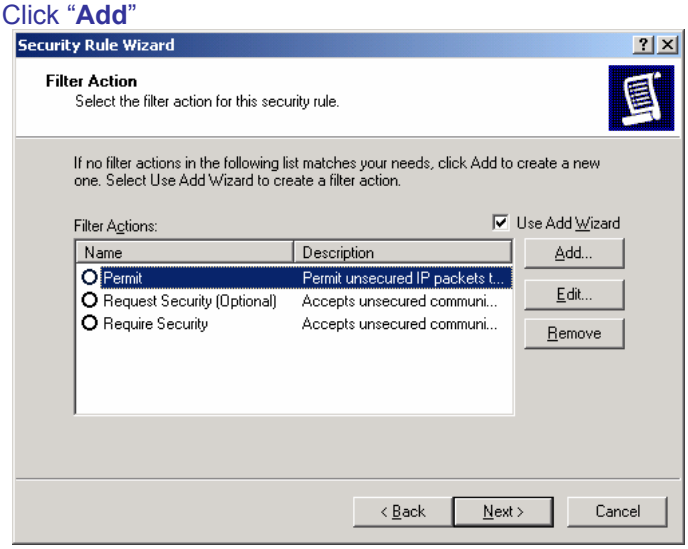
24.Click “**Ok**”



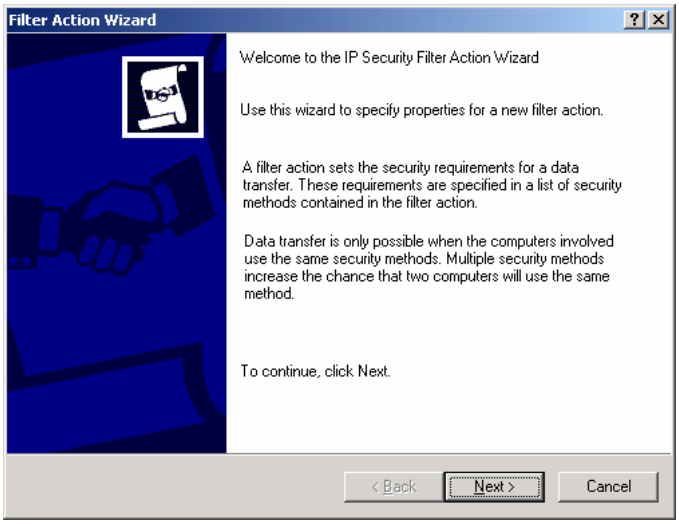
25.Now, select “**XP to DI-804V**” then click “**Next**”



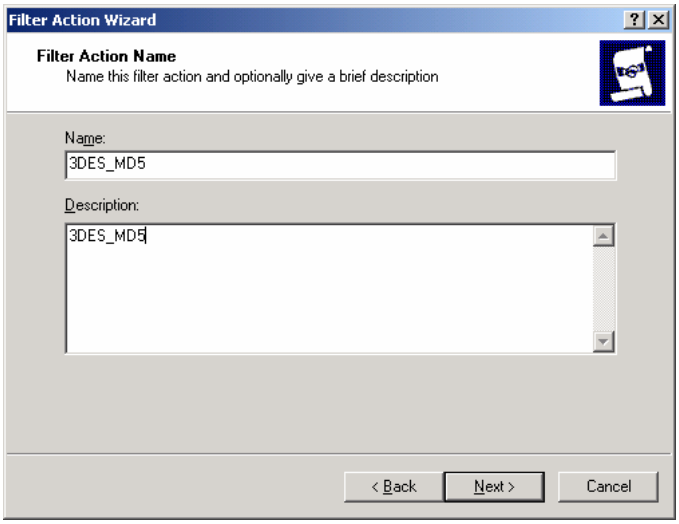
26.Click “**Add**”



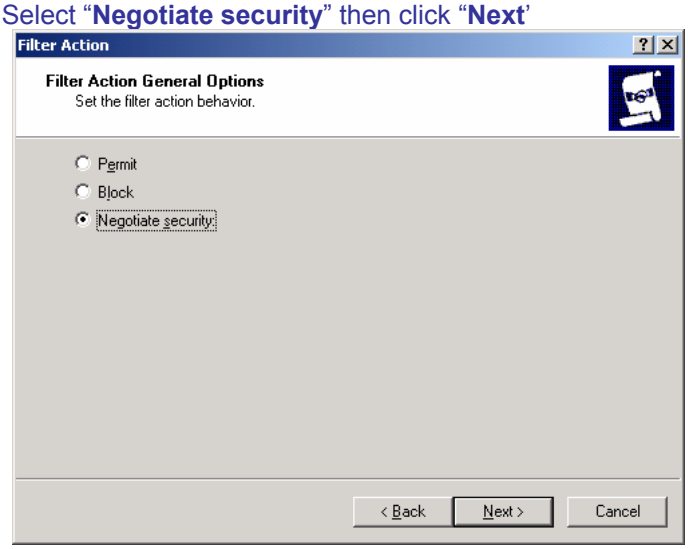
27.Click “**Next**”



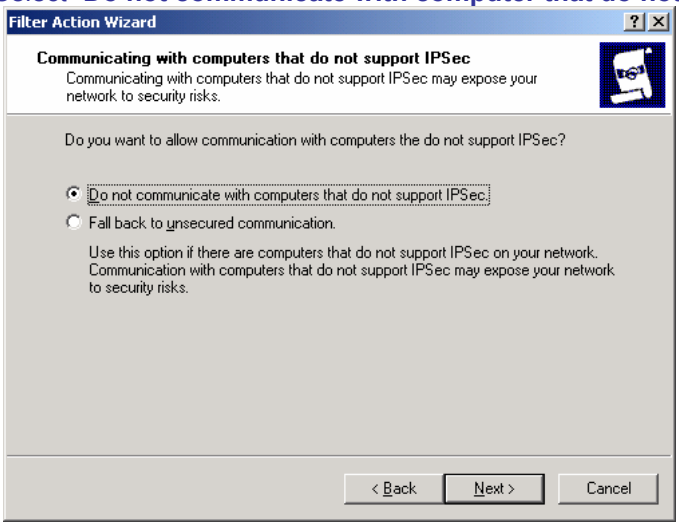
28. Enter a filter action name then click “**Next**”



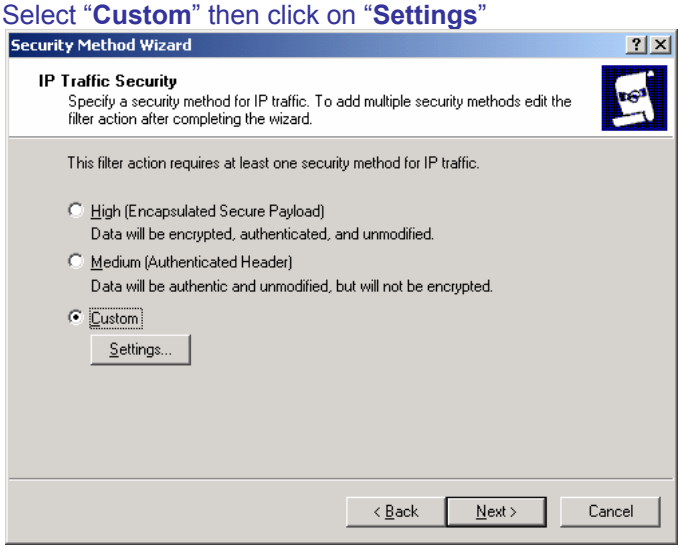
29.Select “**Negotiate security**” then click “**Next**’



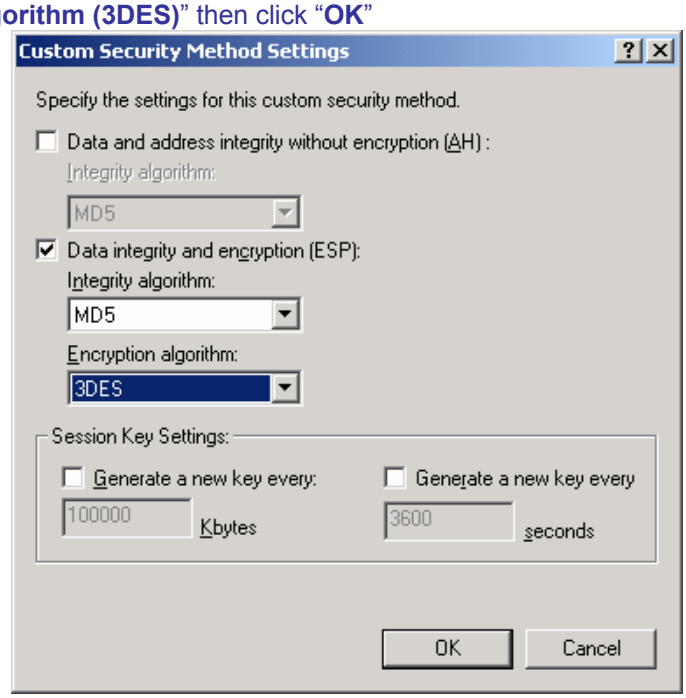
30.Select “**Do not communicate with computer that do not support IPSec**” then click “**Next**”



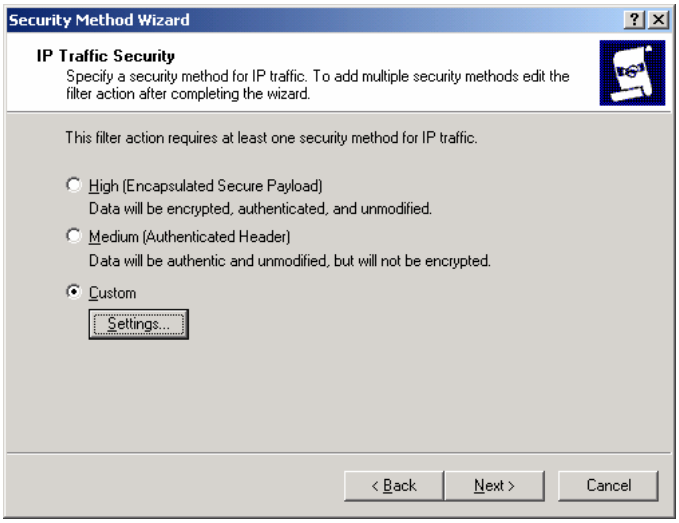
31. Select “**Custom**” then click on “**Settings**”



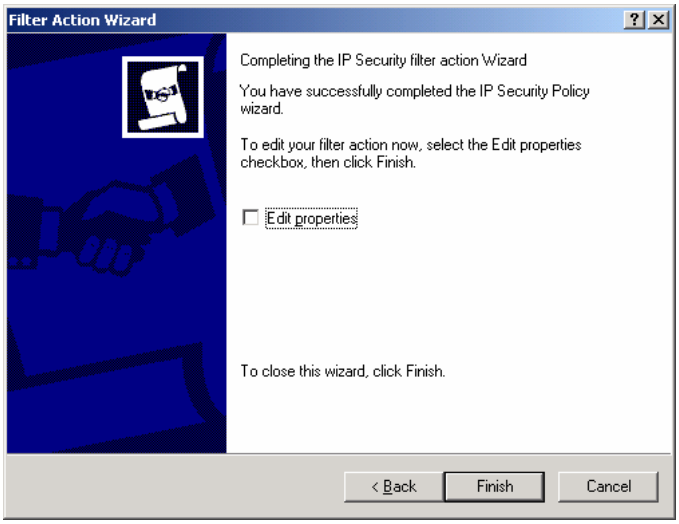
32.Check “**Data integrity and encryption (ESP)**”, select the “**Integrity algorithm (MD5)**” and “**Encryption algorithm (3DES)**” then click “**OK**”



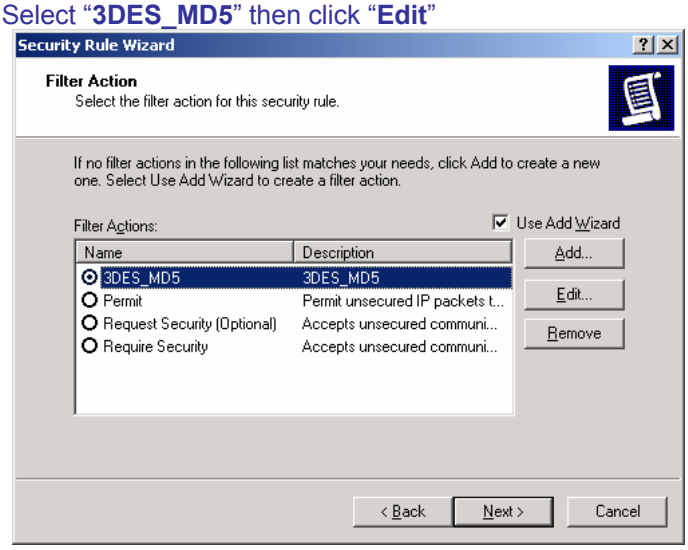
33.Click “**Next**”



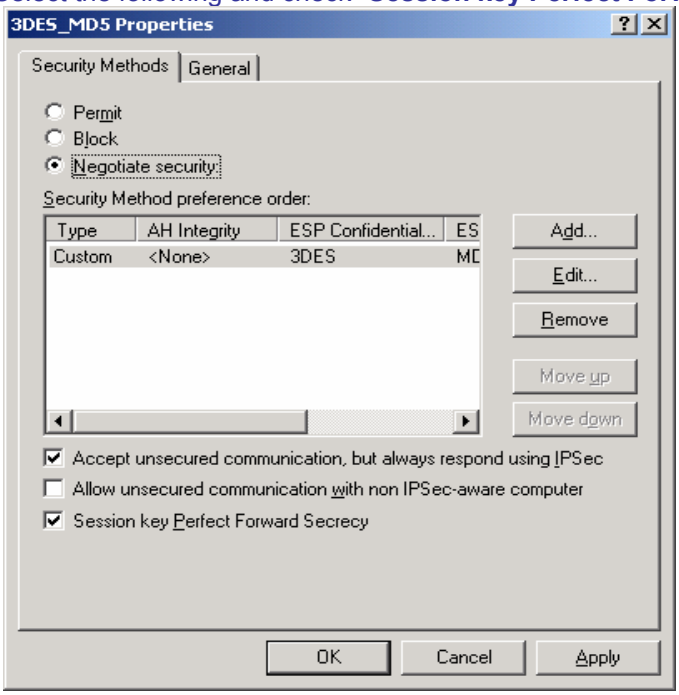
34.Click “**Finish**”



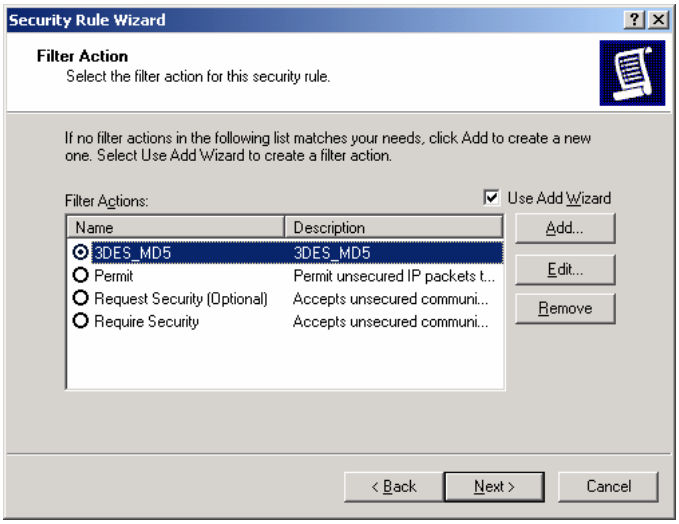
35.Select “**3DES_MD5**” then click “**Edit**”



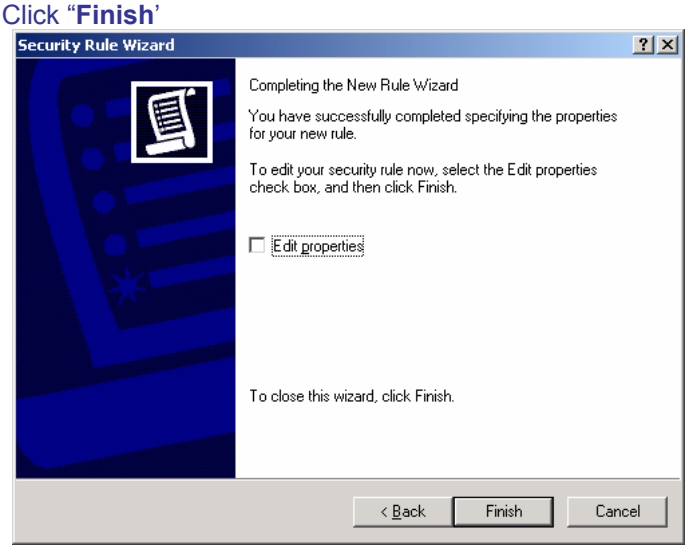
36.Select the following and check “**Session key Perfect Forward Secrecy**” then click “**OK**”



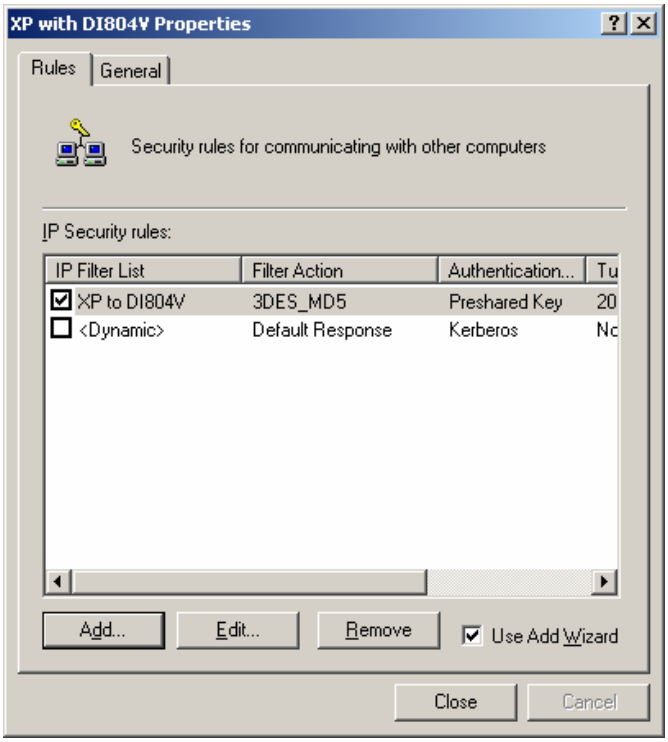
37.Click “**Next**”



38.Click “**Finish**’

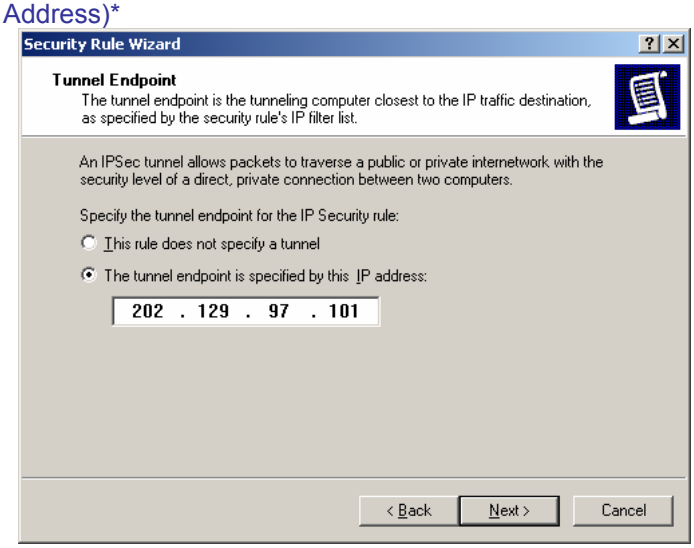


39.Click “**Add**”



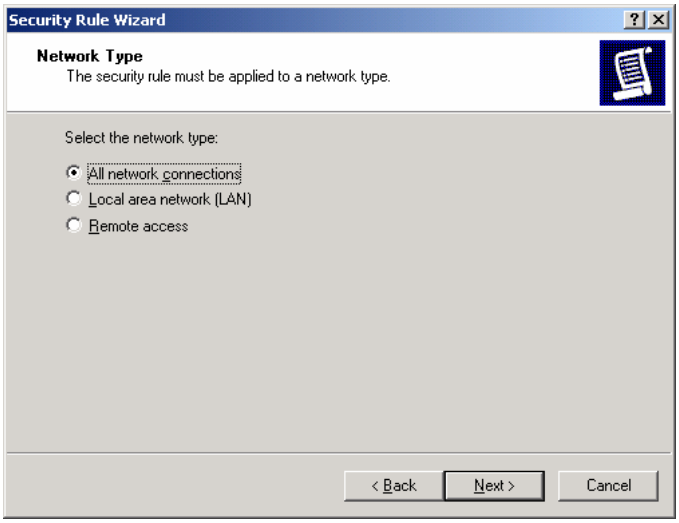
40.Click “**Next**”

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

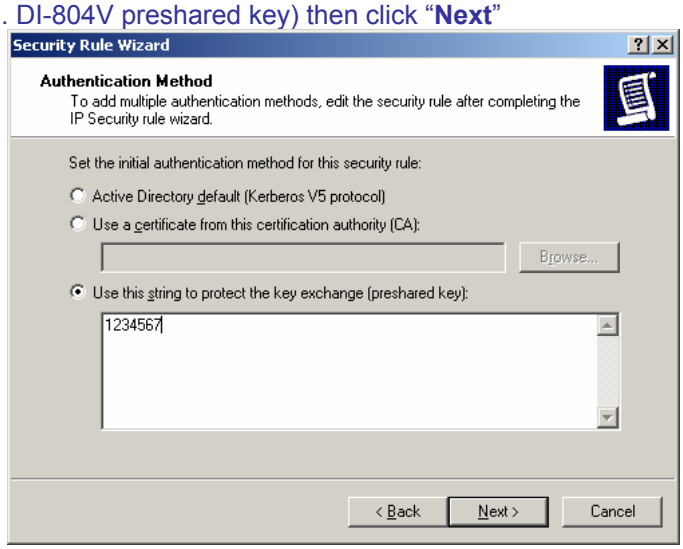


* If your client gets IP address dynamically, put the dynamic IP address here! You will have to change this setting every time you connect to the Internet. Unfortunately, this is the limitation of XP/2000 IPSec client. If your XP/2000 IPSec client is connected to the Internet through the router, use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

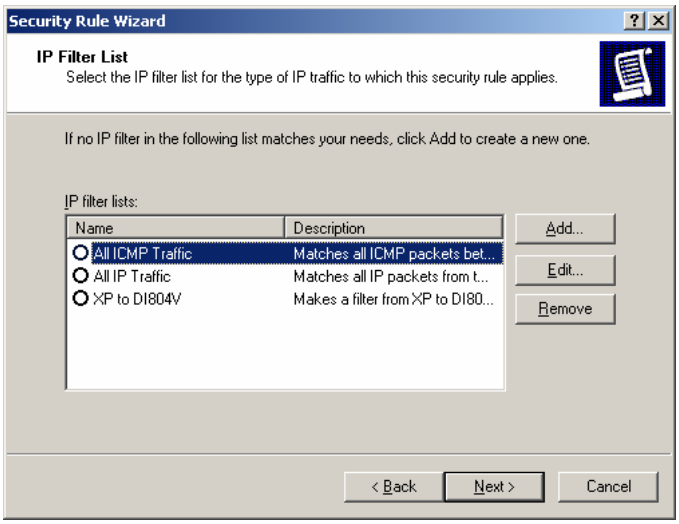
42. Select “**All network connections**” then click “**Next**”



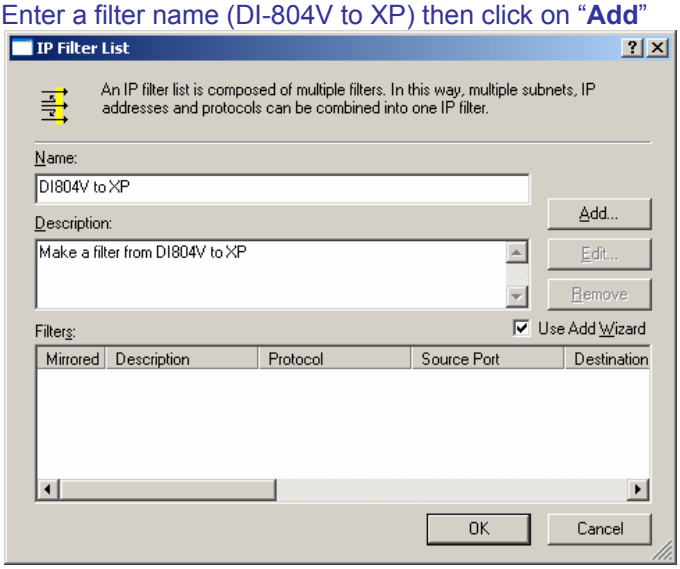
43. Select "**Use this string to protect the key exchange (preshared key)**" (Eg. DI-804V preshared key) then click "**Next**"



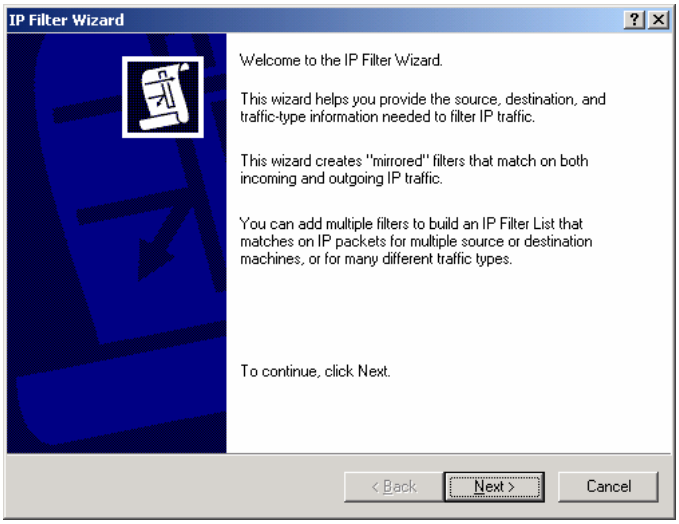
44. Click "**Add**"



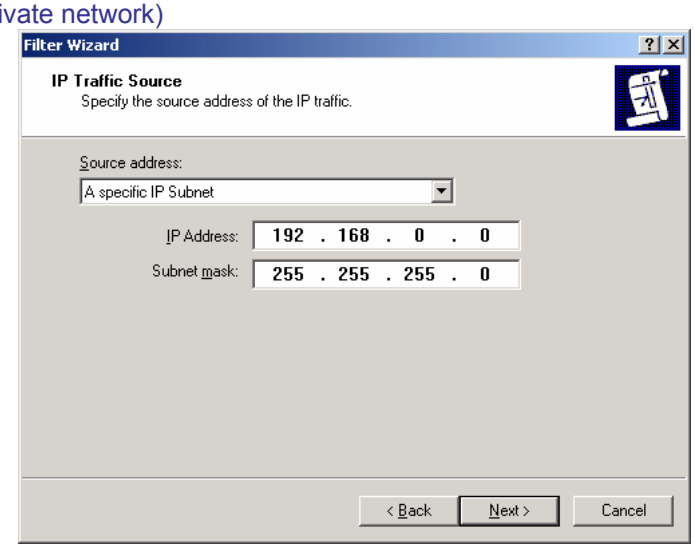
45. Enter a filter name (DI-804V to XP) then click on "**Add**"



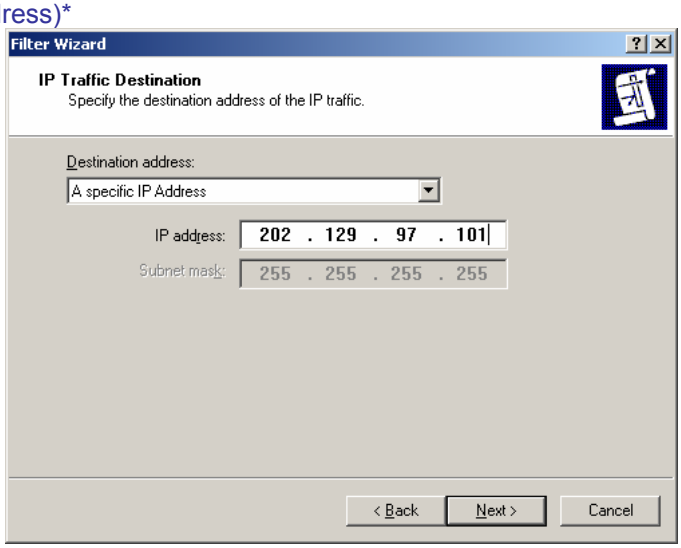
46.Click “**Next**”



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

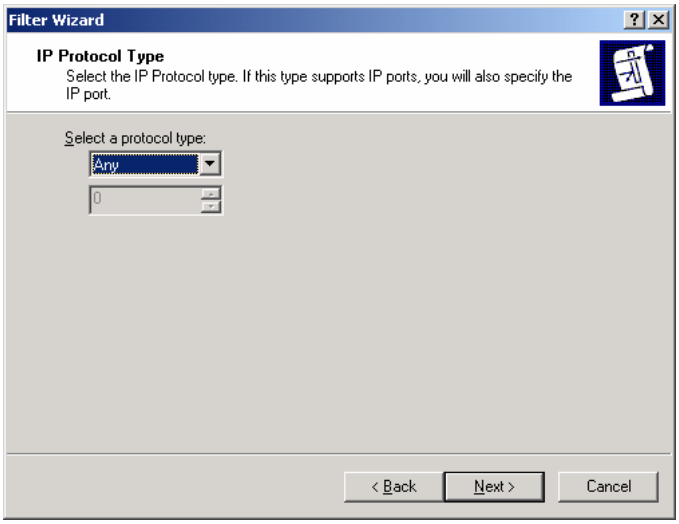


48. Select “**A specific IP Address**” and input the Destination address then click “**Next**” (Eg. Windows XP IP address)*

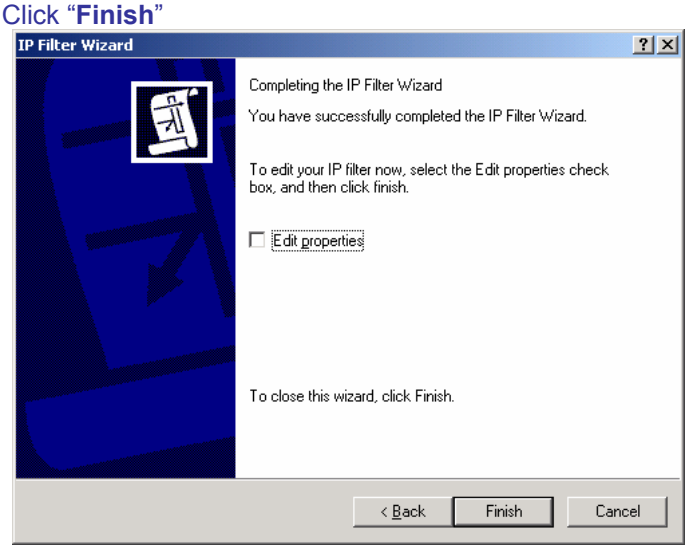


* If your client gets IP address dynamically choose “My IP Address”.

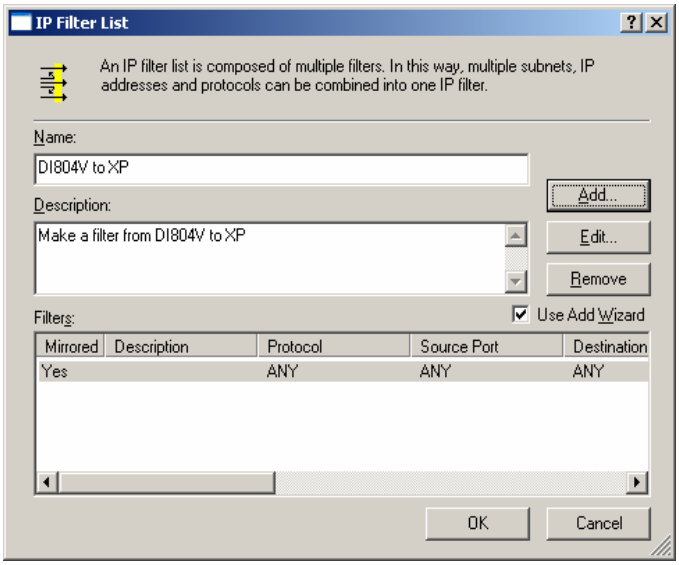
49.Click “**Next**”



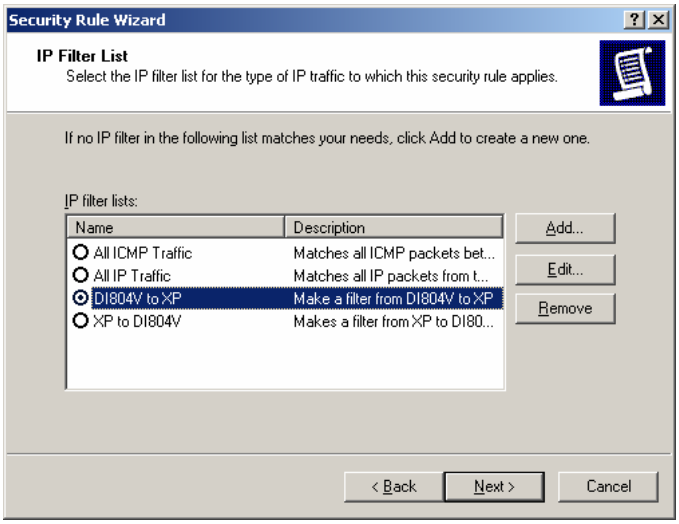
50.Click “**Finish**”



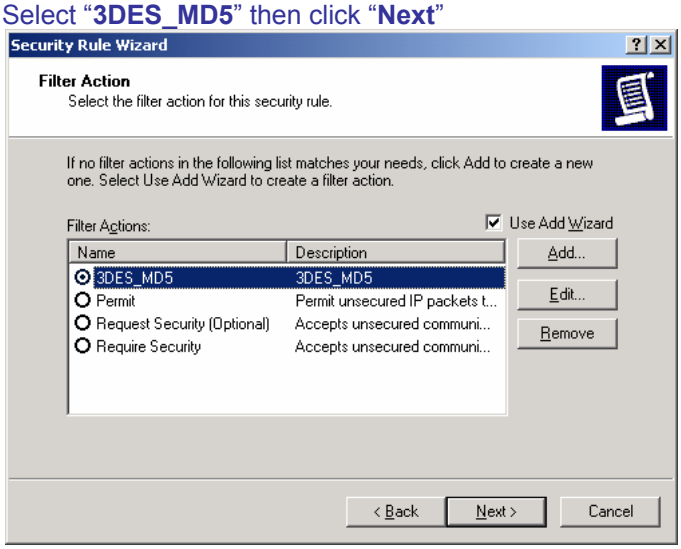
51.Click on “**Close**”



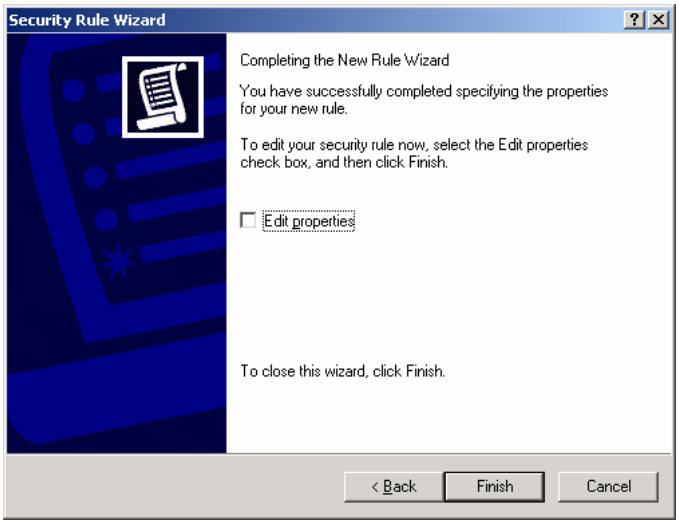
52.Select “**DI-804V to XP**” then click “**Next**”



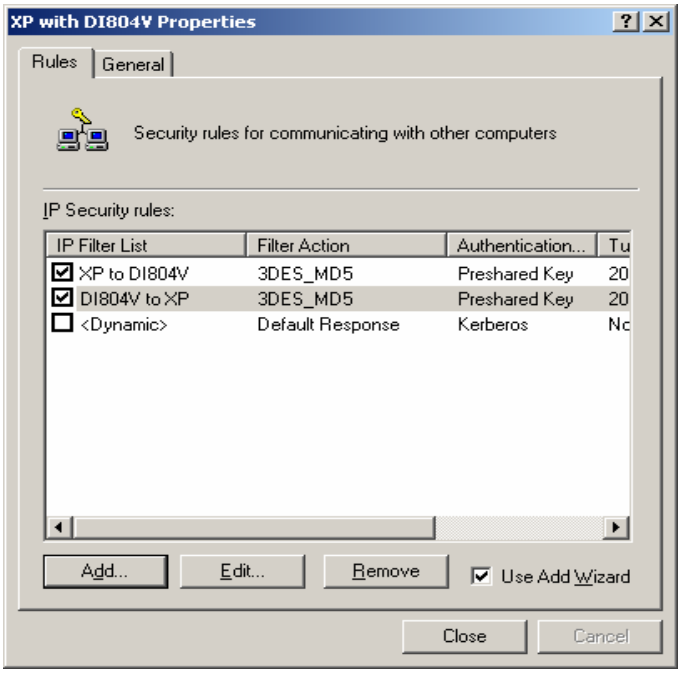
53. Select “**3DES_MD5**” then click “**Next**”



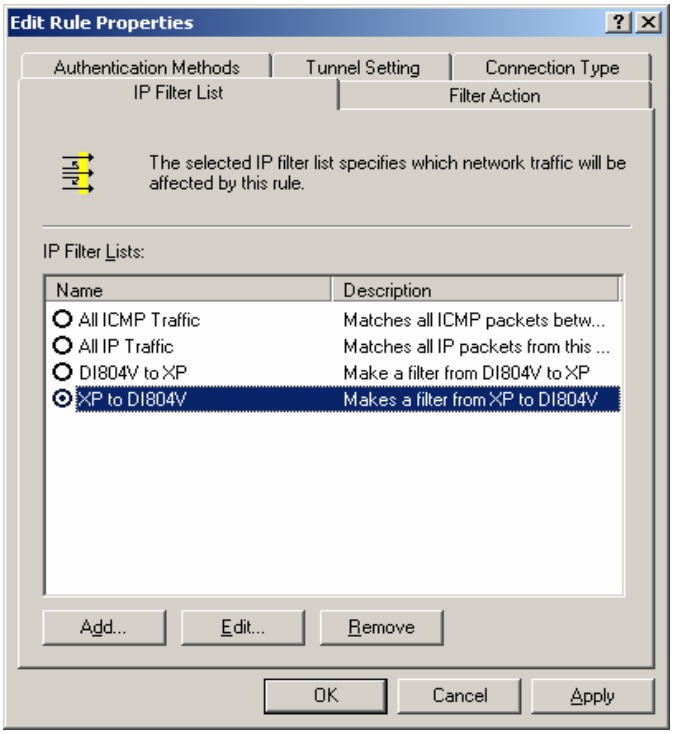
54.Click “**Finish**”



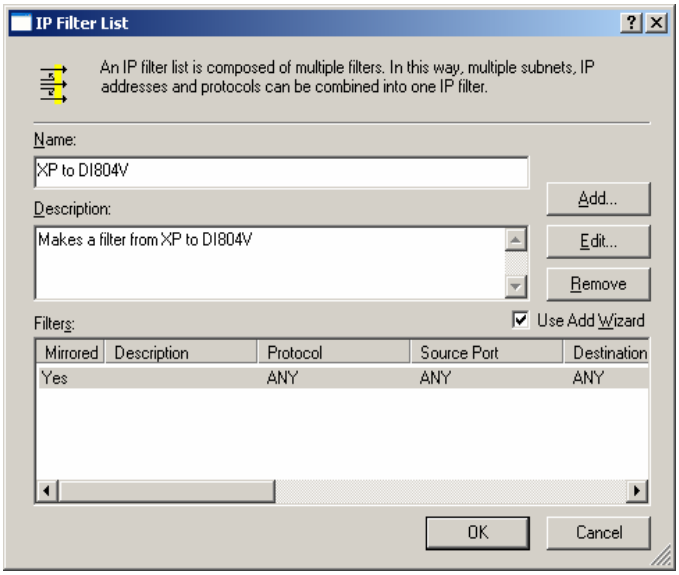
55.Select “**XP to DI-804V**” then click on “**Edit**”



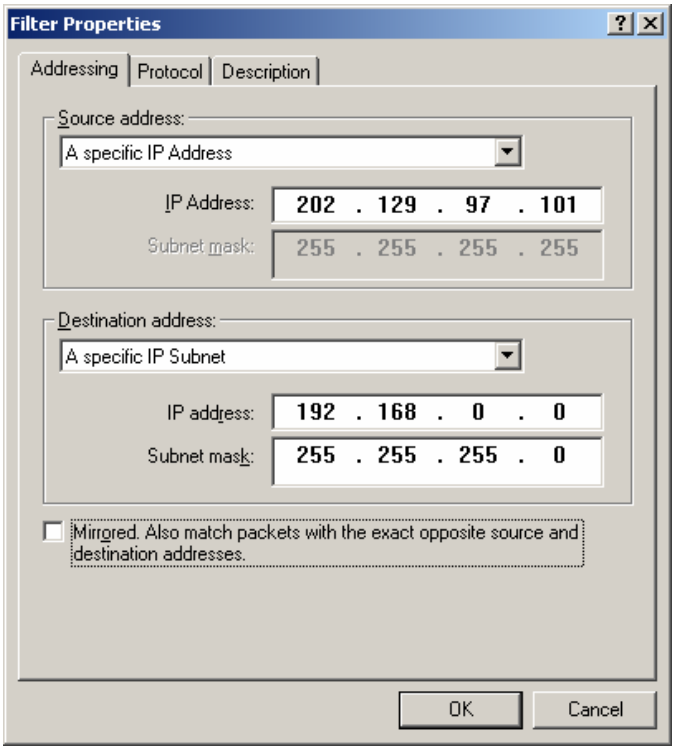
56.Select “**XP to DI-804V**” then click on “**Edit**”



57.Click “**Edit**”

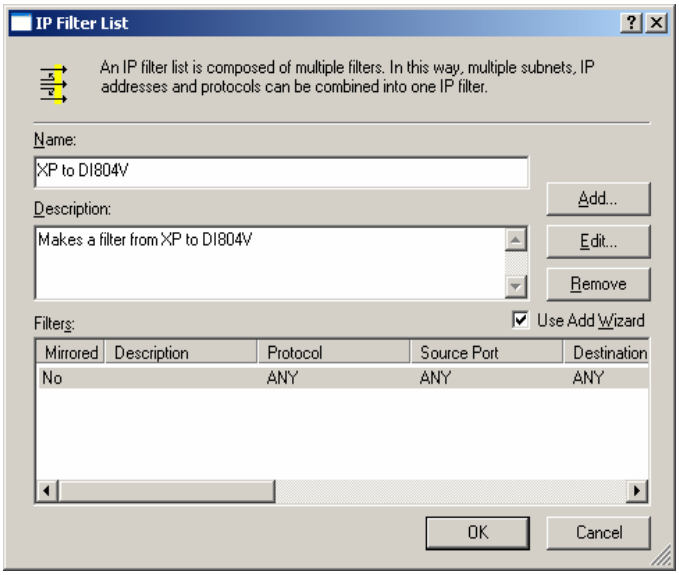


58.Uncheck “**Mirrored. Also match packets with exact opposite source and destination address**” then click “**OK**” *

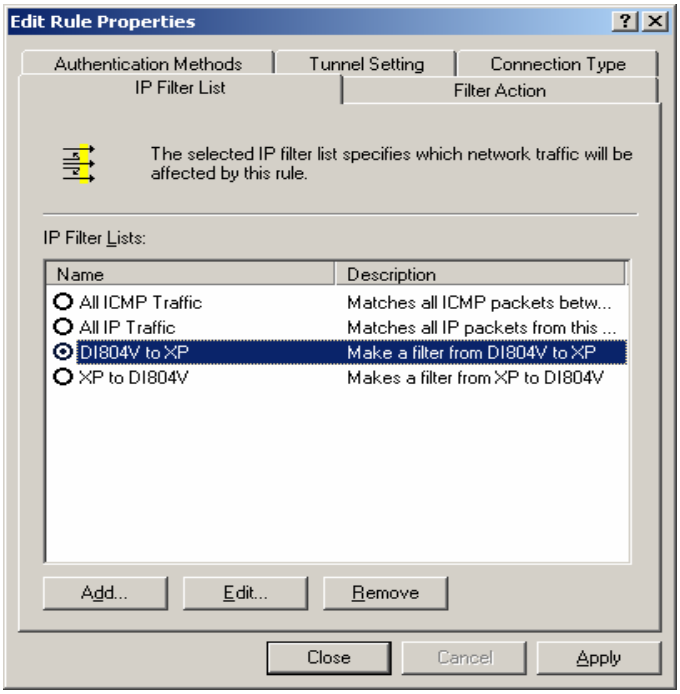


* If your client gets IP address dynamically you will see “My IP Address” in Source address field.

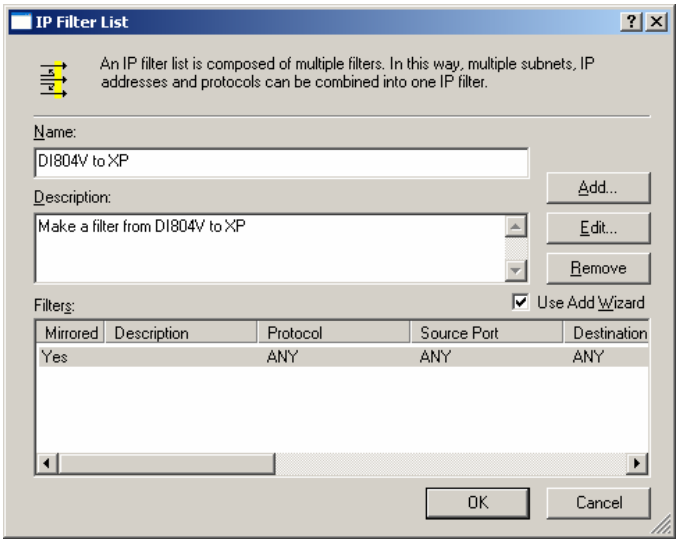
59.Click “**Close**”



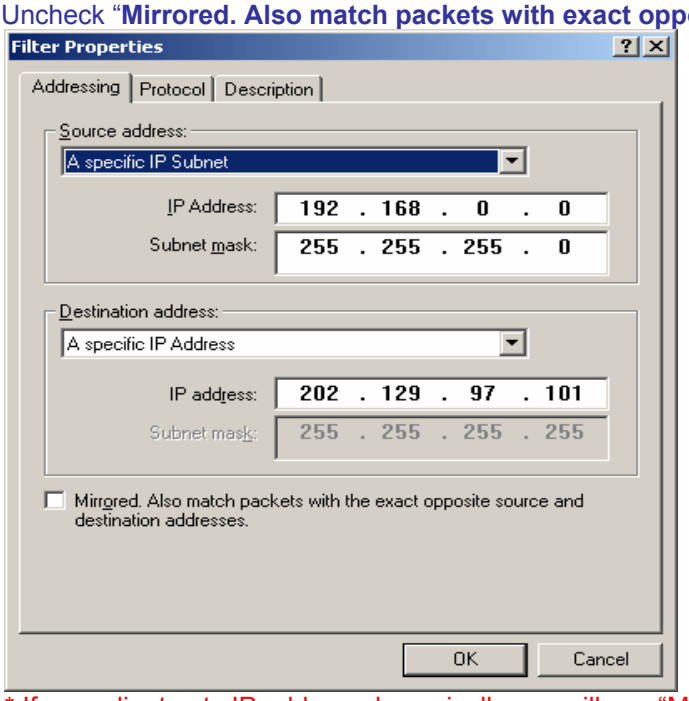
60. Select “**DI-804V to XP**” then click on “**Edit**”



61.Click “**Edit**”

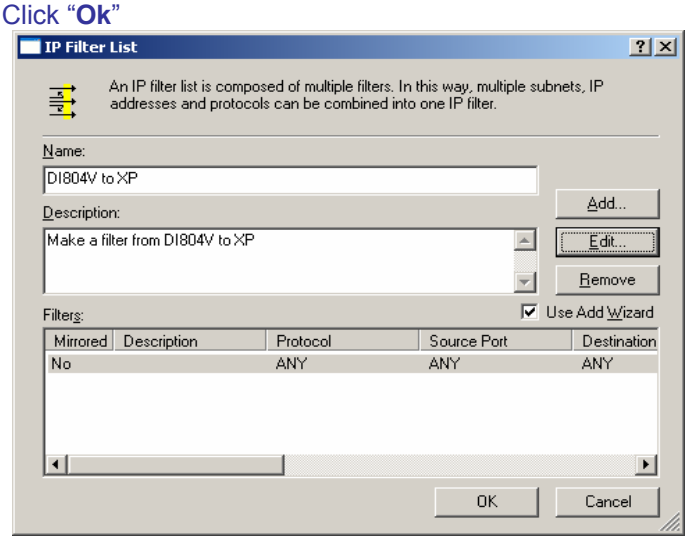


62. Uncheck “**Mirrored. Also match packets with exact opposite source…**” then click “**OK**” *

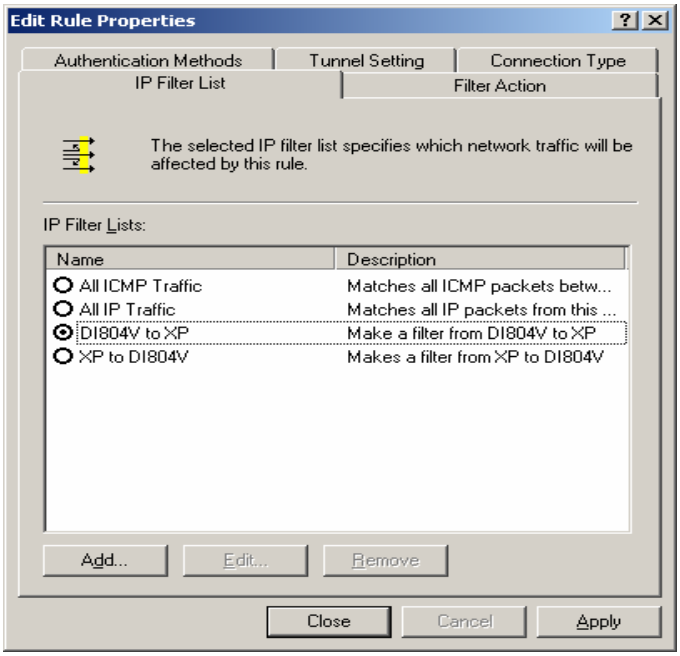


* If your client gets IP address dynamically you will see “My IP Address” in Destination address field.

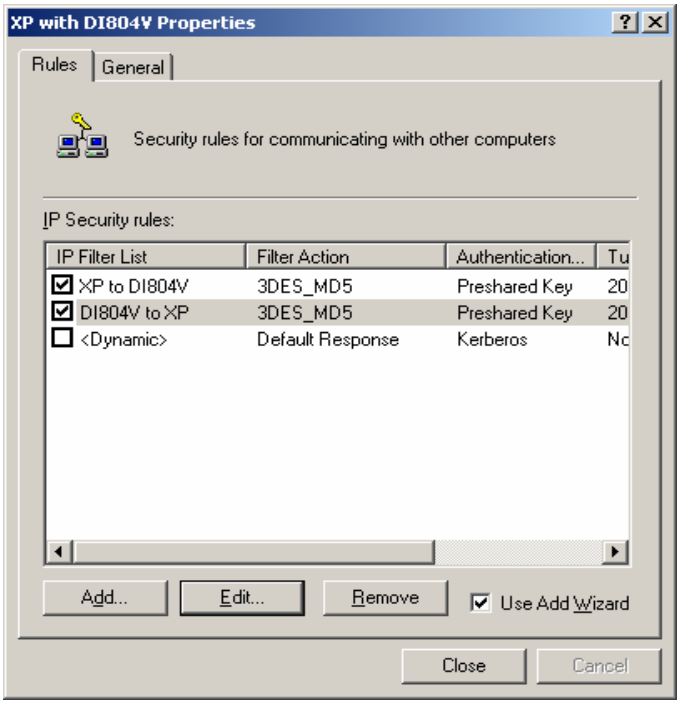
63.Click “**Ok**”



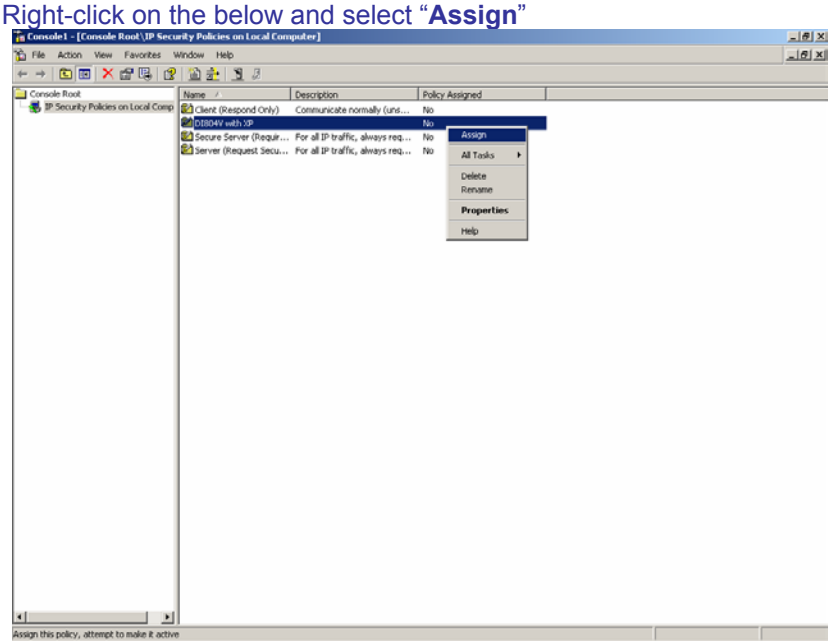
64.Click “**Close**”



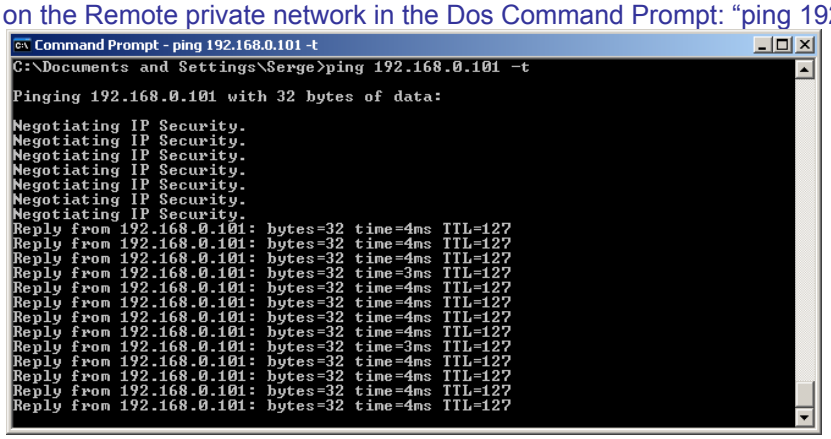
65.Click “**Close**”



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

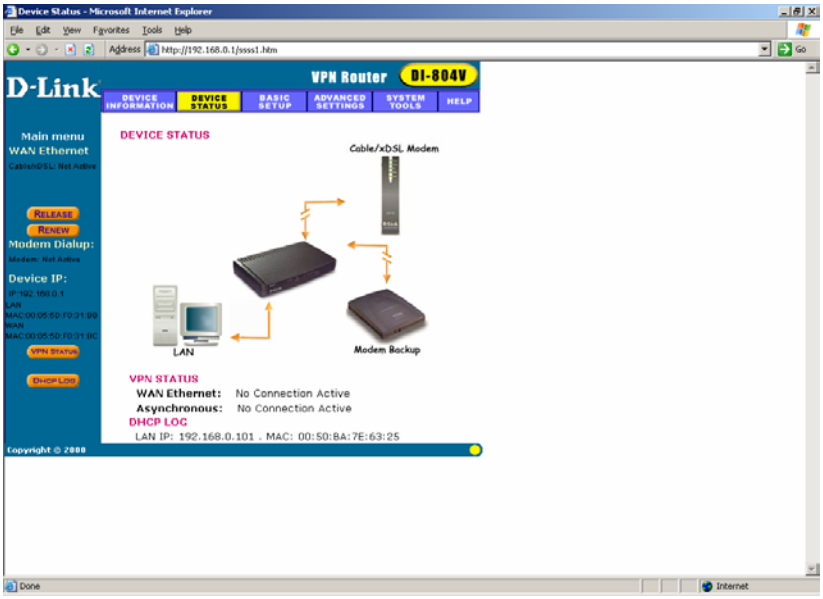


67. On XP/2000 IPSec client machine do a **PING** to a valid machine (which HAS the default gateway pointing to DFL-500 internal IP address and NO anti-virus or ANY other blocking software installed) on the Remote private network in the Dos Command Prompt: “ping 192.168.0.101 –t”

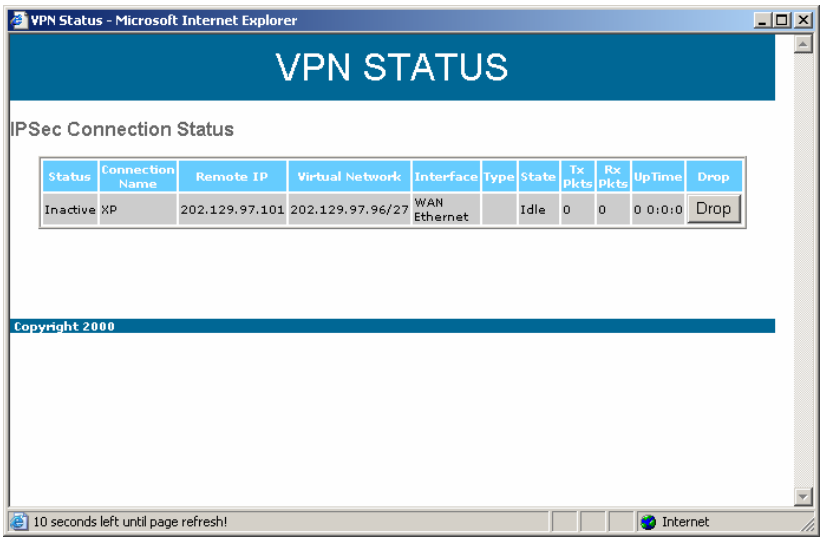


III. Monitoring and managing the VPN connection

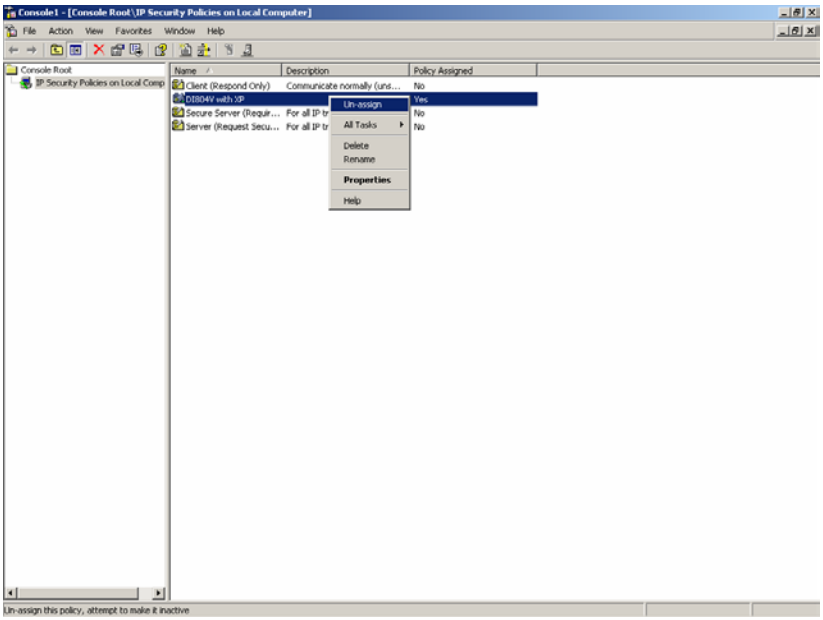
You can use two tools to monitor your VPN connection. It is Microsoft IP Security Monitor and D-Link DI-804V VPN Router Device Status Monitor. Let's go to the VPN Client menu first and check out the VPN Connection status. Go to Device Status, then click VPN Status in the bottom left corner of the screen:



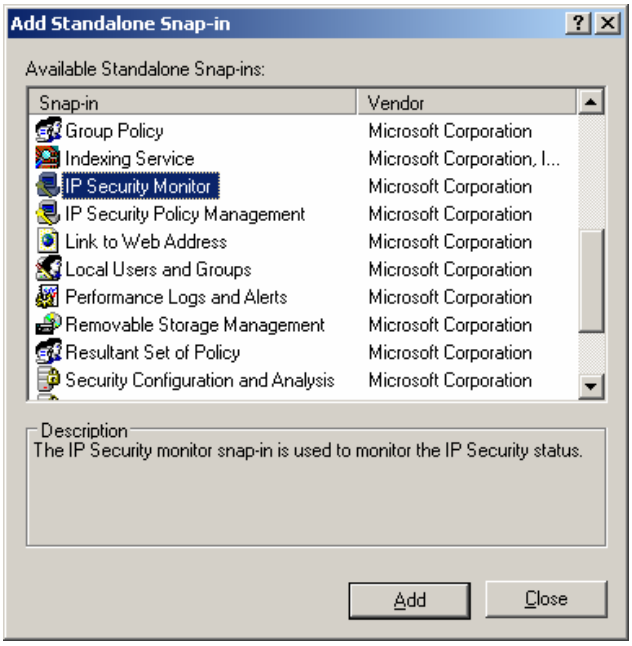
You will see the connection, which we have just created:



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:

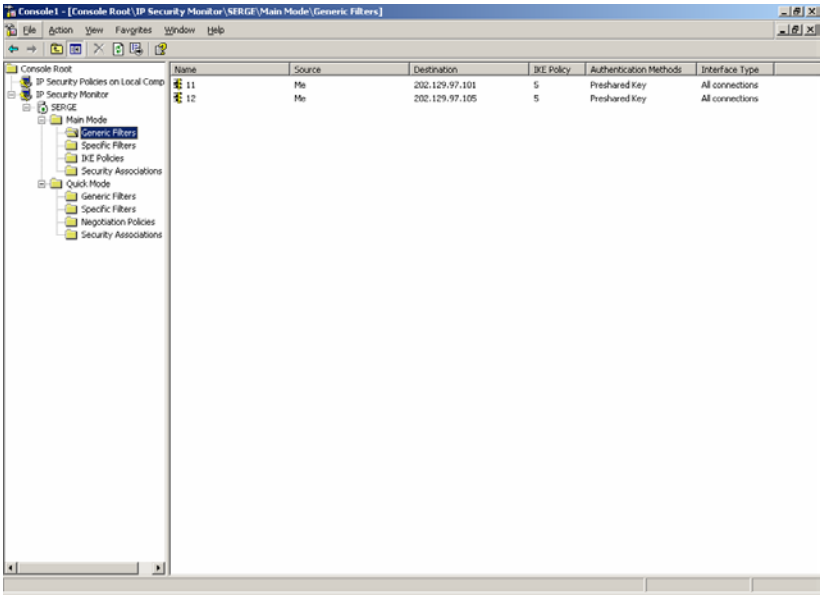


Now let's go back to Microsoft Management Console. We need to add one more Snap-in there. Go to File, then to Add/Remove Snap-in and choose IP Security Monitor:

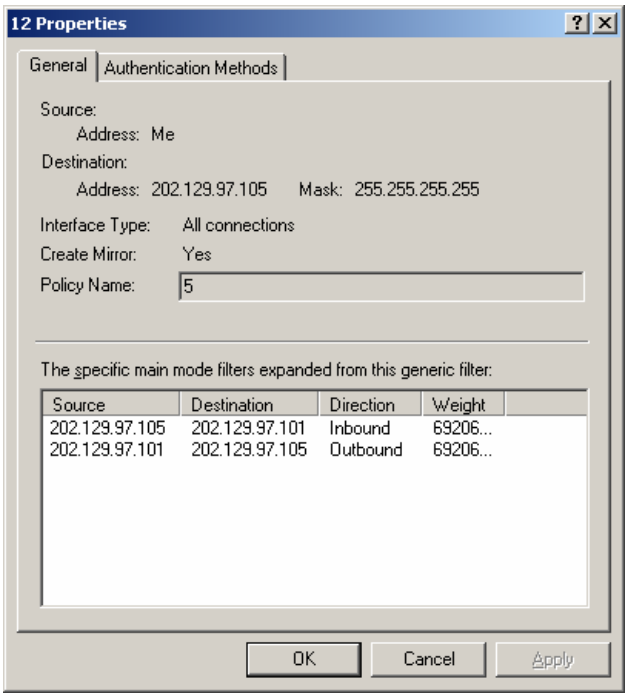


You have a choice of Generic Filters, Specific Filters, IKE Policies and Security Associations in Quick and Main modes.

Let's look at Generic Filters in Main mode:

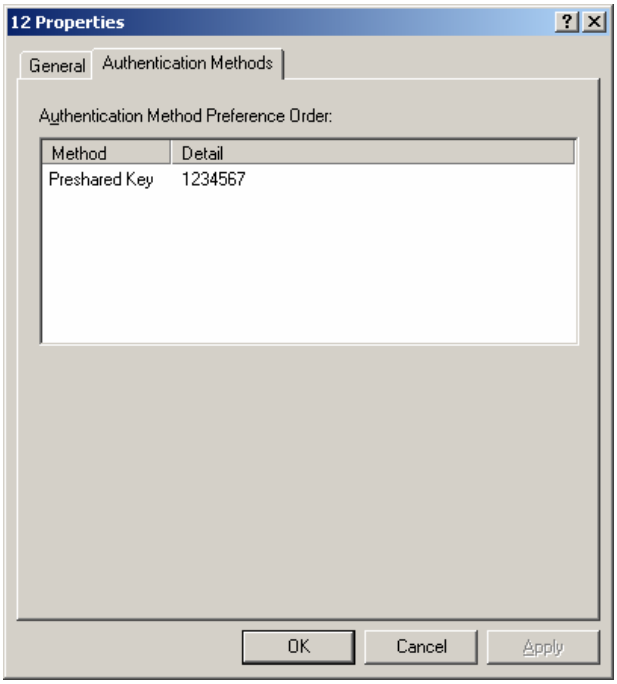


You can see two connections there: one with a destination of 202.129.97.105 and another one with a destination of 202.129.97.101. Those are our "XP to DI804V" and "DI804V to XP" connections. Now click on to the one with 202.129.97.105 connection. You will see the following:

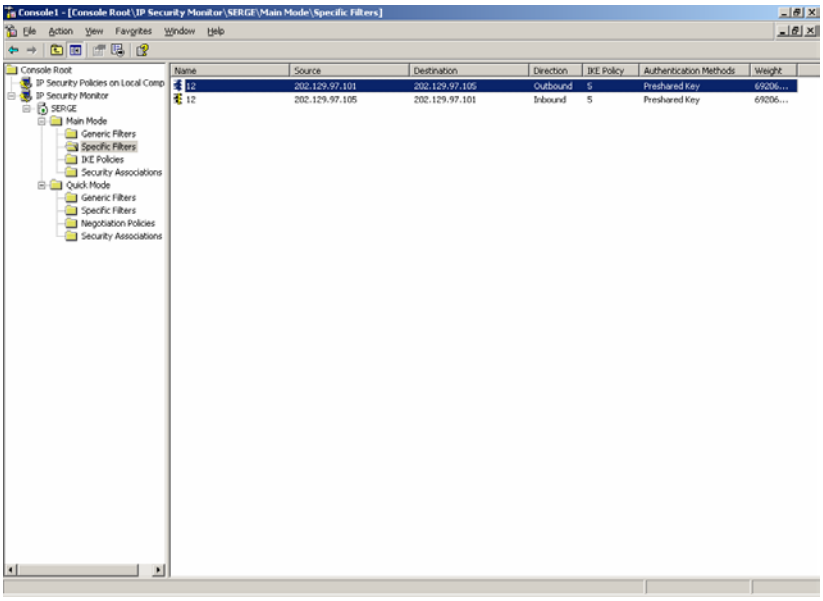


It basically tells you the source and destination of connections as well as a weight of the connection.

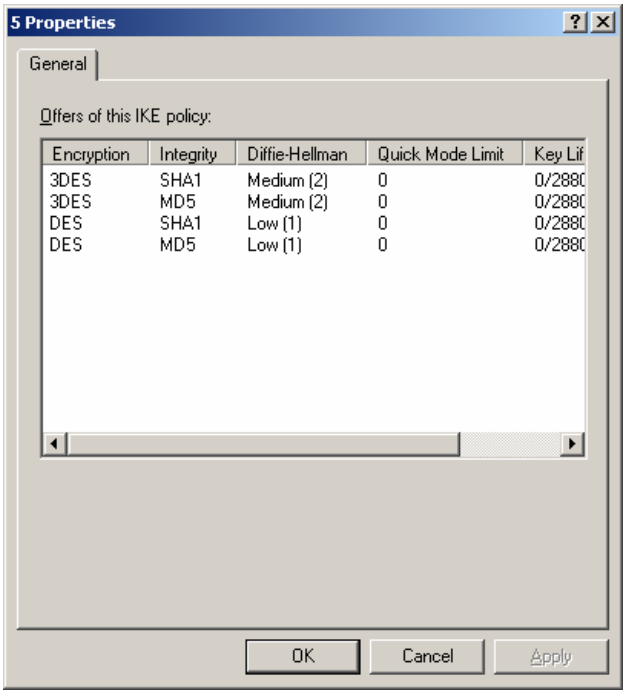
Now click on Authentication Methods:



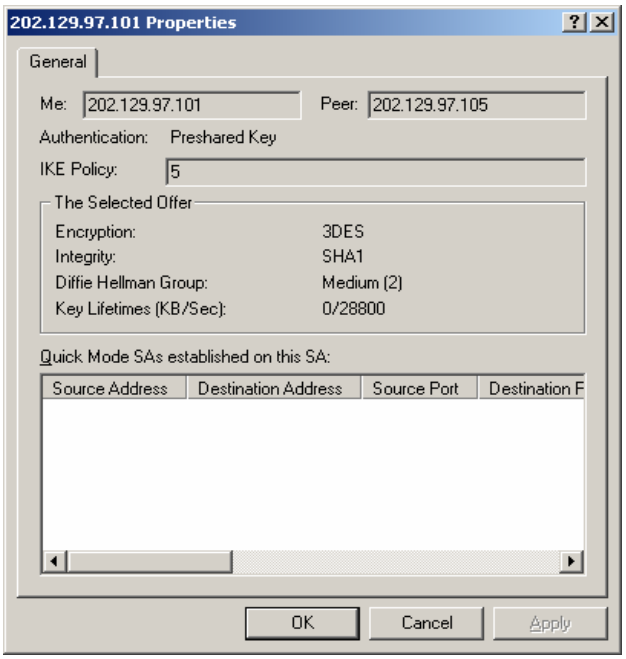
What you see there is the Preshared Key used in this connection. In Specific Filters, we basically see the same information, but in a bit different order:



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

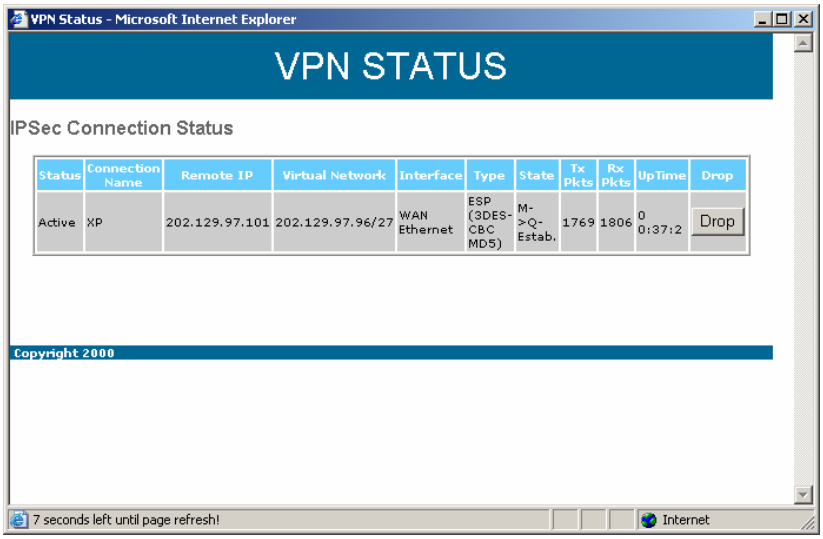


And finally, in the Security Associations you will see the following:



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.

Now let's go back to VPN Router and check the VPN Status there:



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.