

# OvisLink

[www.ovislink.com.tw](http://www.ovislink.com.tw)

## WMU/MU9000VPN

### VPN Setup Guide



# Table of Contents

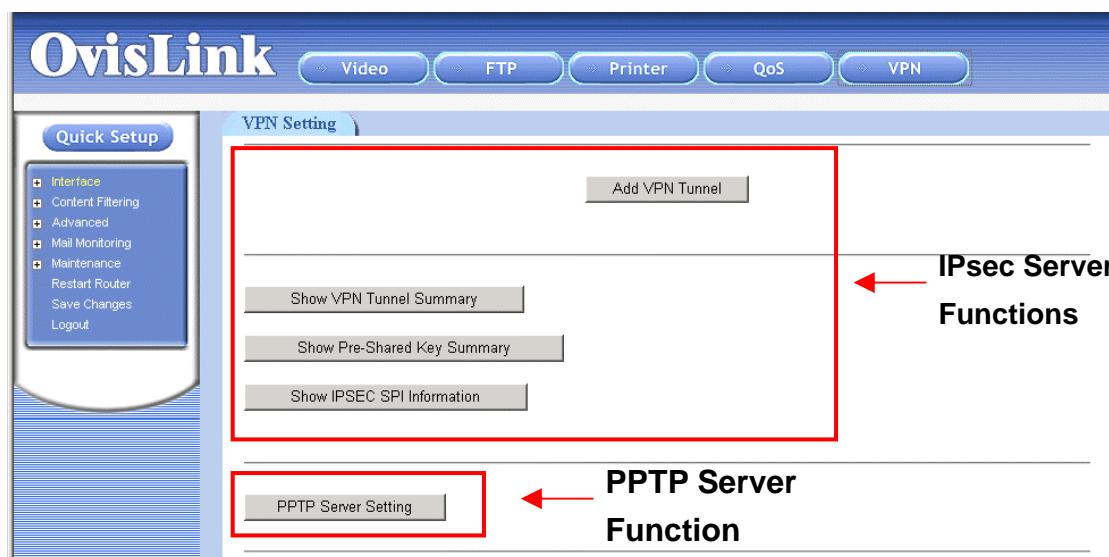
<b>VPN EXAMPLES.....</b>	<b>3</b>
EXAMPLE 1: USING IPSEC TO CONNECT 2 LAN TOGETHER.....	3
<i>USA Router Setup</i> .....	4
<i>Germany Router Setup</i> .....	6
EXAMPLE 2: USING PPTP TO CONNECT REMOTE PC TO LOCAL LAN .....	8
<i>Router Setup</i> .....	8
<i>Remote PC Setup (Using WinXP VPN Client)</i> .....	10
EXAMPLE 3: IPSEC CONFIGURATION EXAMPLE.....	17
<i>Router's IPsec Setup</i> .....	18
<i>PC's IPsec Setup (WinXP)</i> .....	21

# VPN Examples

In this Guide, we will provided setup guide for 3 VPN applications example:

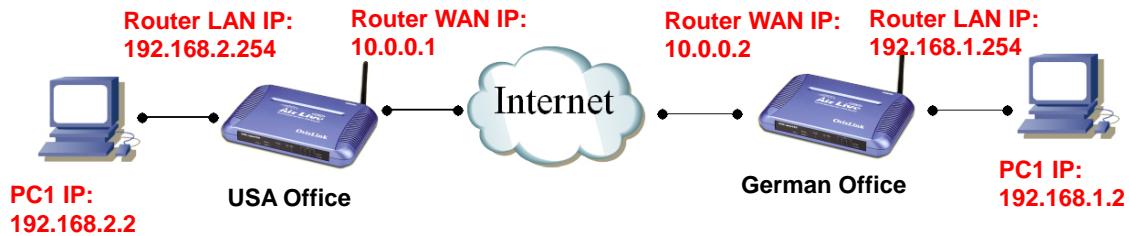
1. Using IPsec protocol to connect 2 remote LAN together using 2 WMU/MU9000VPN Routers.
2. Using PPTP protocol to connect 1 remote PC with WMU/MU-9000VPN
3. Using IPsec protocol to connect a remote mobile PC with WMU/MU-9000VPN

To setup a VPN connection, it involves set up in both the router and the PC side. As you will notice, the setup for the VPN server on the router is very simple. But the setup on the client side depends on what type of VPN client software you use on the PC. Once you take time to go through the step-by-step example, it will become clear and easier to setup.



---

## Example 1: Using IPsec to connect 2 LAN together



In this example, we will connect the USA office and German office together using IPsec VPN server (WMU-9000VPN on both side). The goal is to let both office's network together and operate as if they are on the same LAN. Please note that for security purpose, IPsec require that the IP subnet on both side of the VPN tunnel must be different. Therefore, in this example, the USA office's local IP subnet is 192.168.2.x. The German office's local IP subnet is 192.168.1.x.

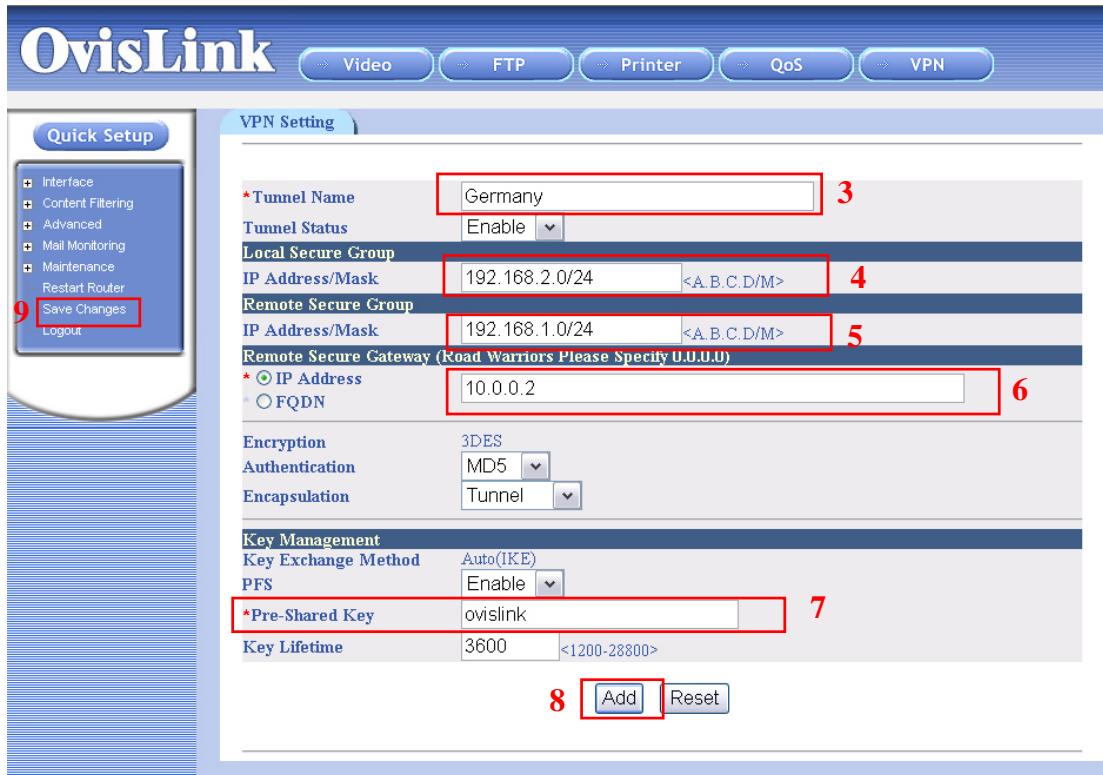
*After firmware version .40, the router can support VPN over dynamic DNS. If the remote VPN server is using Dynamic DNS, please select "FQDN" for the Remote Secure gateway, then enter the remote server's DDNS domain name.*

Please check the above diagram to get a clear idea of how the connect and IP addresses.

## USA Router Setup

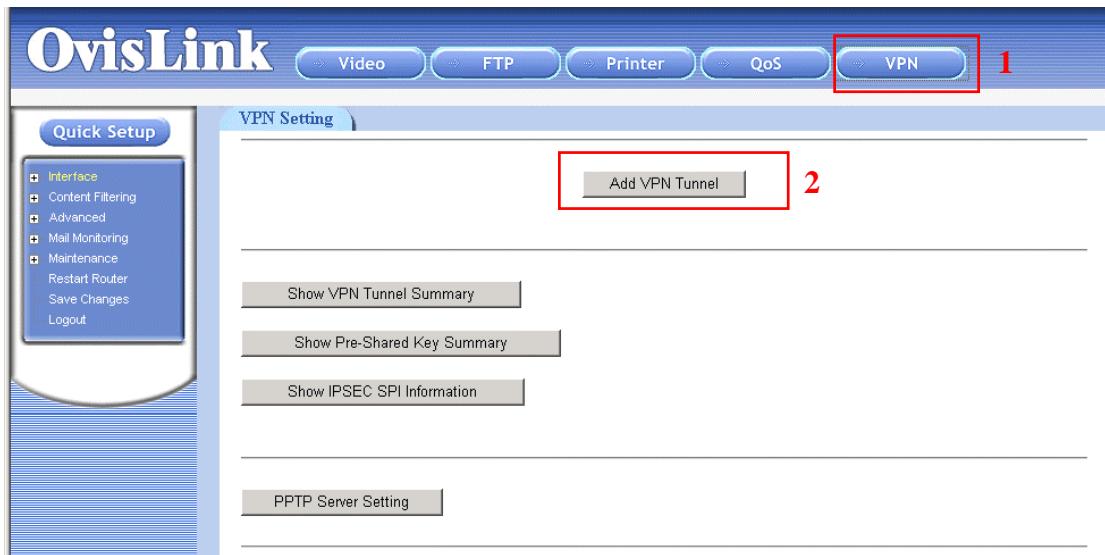
1. Click on the VPN button on the top menu

2. Click on “Add VPN Tunnel”



3. On the VPN setting page above. For the Tunnel name, please enter “Germany” for this case.
4. For the local secure Group. Enter the local IP subnet and the mask in this field. For USA office, the LAN IP subnet is 192.168.2.0, enter “24” for mask if you want the entire LAN to have access to the tunnel.
5. For the remote secure Group. Enter the remote LAN IP subnet and the mask in this field. For the remote Germany office, the LAN IP subnet is 192.168.1.0, enter “24” for mask if you want the entire remote LAN to have access to the tunnel.
6. Enter the IP address of the Germany’s WAN IP address. In this case, it is “10.0.0.2”. **If the remote VPN server is using Dynamic, please select “FQDN” and enter the remote server’s DDNS address.**
7. Please enter a Pre-Shared Key which is the key that the VPN tunnel use for data encryption. The key must set to the same on both side. In this case, we use “ovislink”
8. Press the Add button
9. Press “save changes” on the left menu bar.

## Germany Router Setup



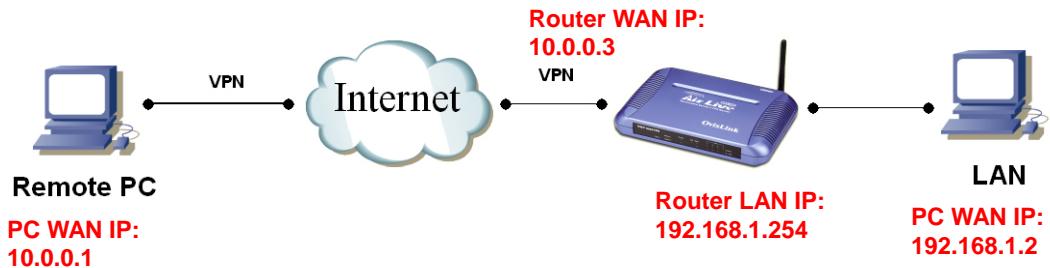
1. Click on the VPN button on the top menu
2. Click on “Add VPN Tunnel”

<b>*Tunnel Name</b>	USA	3
<b>Tunnel Status</b>	Enable	
<b>Local Secure Group</b>		
<b>IP Address/Mask</b>	192.168.1.0/24	<A.B.C.D/M>
<b>Remote Secure Group</b>		
<b>IP Address/Mask</b>	192.168.2.0/24	<A.B.C.D/M>
<b>Remote Secure Gateway (Road Warriors Please Specify 0.0.0.0)</b>		
<input checked="" type="radio"/> IP Address	10.0.0.1	6
<input type="radio"/> FQDN		
<b>Encryption</b>	3DES	
<b>Authentication</b>	MD5	
<b>Encapsulation</b>	Tunnel	
<b>Key Management</b>		
<b>Key Exchange Method</b>	Auto(IKE)	
<b>PFS</b>	Enable	
<b>*Pre-Shared Key</b>	ovislink	7
<b>Key Lifetime</b>	3600	<1200-28800>
<b>8</b> <input type="button" value="Add"/> <input type="button" value="Reset"/>		

3. On the VPN setting page above. For the Tunnel name, please enter “USA” for this case.
4. For the local secure Group. Enter the local IP subnet and the mask in this field. For the Germany office, the LAN IP subnet is 192.168.1.0, enter “24” for mask if you want the entire LAN to have access to the tunnel.
5. For the remote secure Group. Enter the remote LAN IP subnet and the mask in this field. For the remote USA office, the LAN IP subnet is 192.168.2.0, enter “24” for mask if you want the entire remote LAN to have access to the tunnel.
6. Enter the IP address of the USA's WAN IP address. In this case, it is “10.0.0.1”. **If the remote VPN server is using Dynamic, please select “FQDN” and enter the remote server's DDNS address.**
7. Please enter a Pre-Shared Key which is the key that the VPN tunnel use for data encryption. The key must set to the same on both side. In this case, we use “ovislink”
8. Press the Add button
9. Press “save changes” on the left menu bar.

After the settings is done on both side, the routers should built tunnels to connect the 2 sides together.

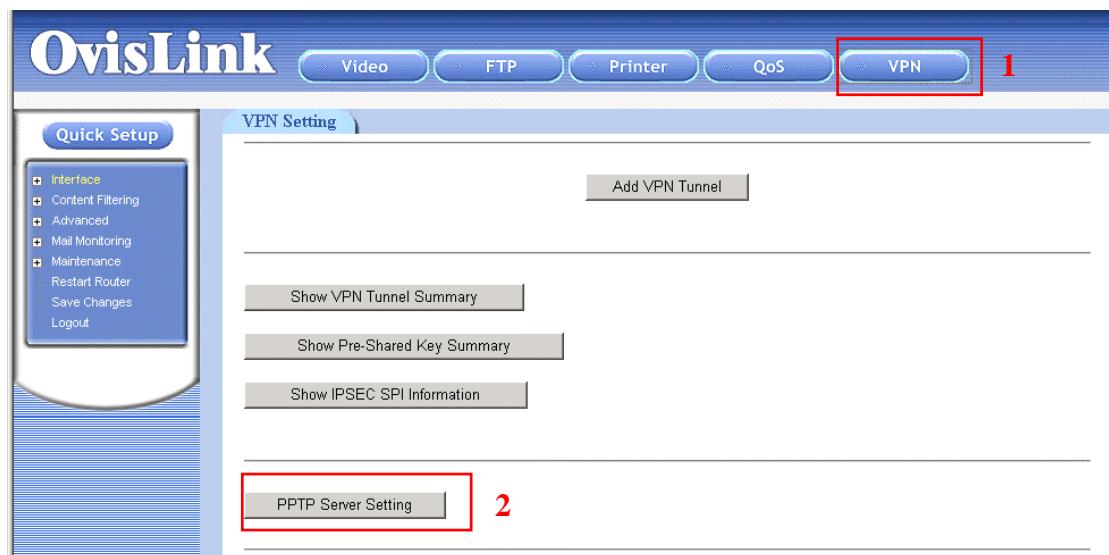
## Example 2: Using PPTP to connect remote PC to Local LAN



In this example, we will demonstrate how to setup a VPN connection between a remote PC and the WMU-9000VPN using the PPTP server function. Looking at the diagram above, the Remote PC has real IP address of 10.0.0.1. If this remote PC is connected to Internet through an IP sharing router, please make sure that router supports PPTP pass through function. In this example, the WMU-9000VPN's WAN IP address is 10.0.0.3. You can also register the WMU-9000VPN with dynamic DNS if you don't have fixed IP address. Finally, the local LAN has IP address 192.168.1.x. Please note that if the Remote PC is under a router, the remote PC's IP subnet must be different from the local IP subnet.

The Router's PPTP server can support 10 PPTP VPN user's account.

### Router Setup



- Click on the VPN button on the top menu

4. Click on “PPTP Server Settings”

PPTP Server

PPTP Server Status: **Enable**

Local IP Address: 192.168.33.101-100 <A.B.C.D[-E]>

Remote IP Address: 192.168.1.101-100 <A.B.C.D[-E]>

**6** Set Reset

Account Management

User Name	Password

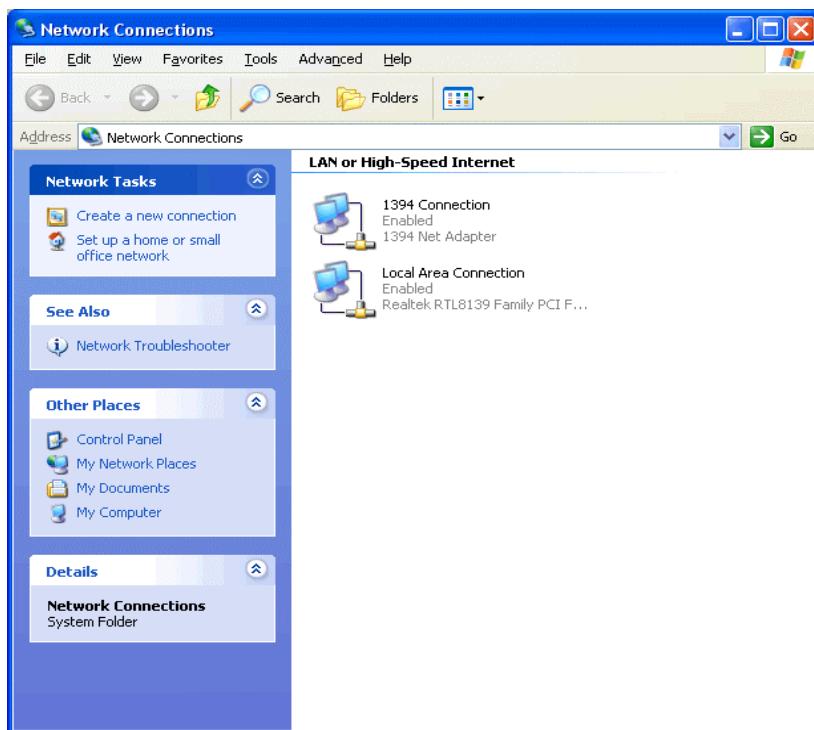
Set Reset

3. Enable the PPTP Server Status
4. The local IP address field is the internal IP address range used by VPN server to keep track of the IP translation. It must be on a different subnet from the local LAN. In this case, we put “192.168.33.101-110” for all 10 possible account.
5. The Remote IP address field is where you put the local IP address assignment to the remote PC when they login. They must be in the same subnet as the local LAN. In this case, since the local LAN’s IP subnet is 192.168.1.x. We will put “192.168.1.101-110” for the IP address assignment to the 10 accounts (from .101 to .110).
6. Place the “Set” button to turn on the PPTP server

7. Now Enter the User's Name and Password in the account management. In this example, please put "vpnone" for the user's name.
8. Press "Set" button to create VPN account.
9. Press "Save Changes" on the left hand menu bar.

### **Remote PC Setup (Using WinXP VPN Client)**

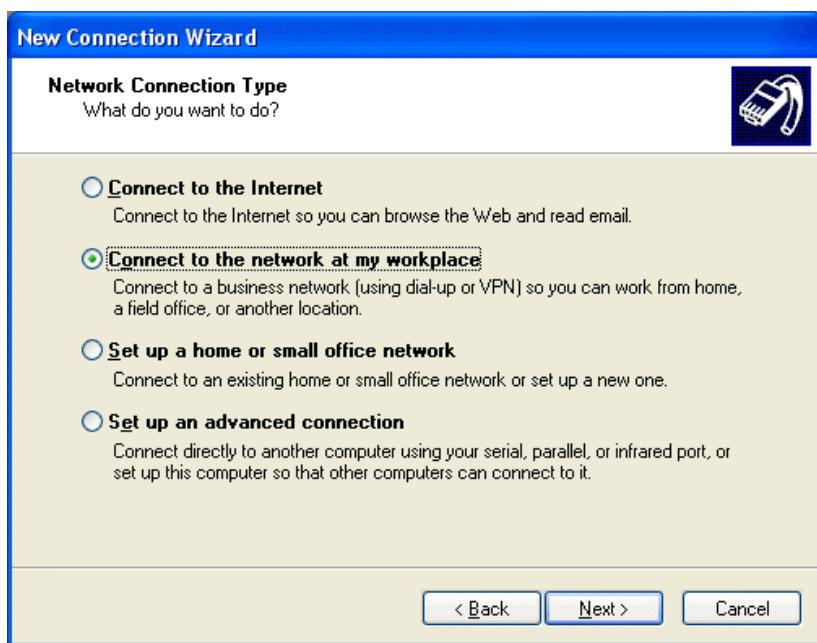
In case of WINXP, the following steps shows PPTP client setting.



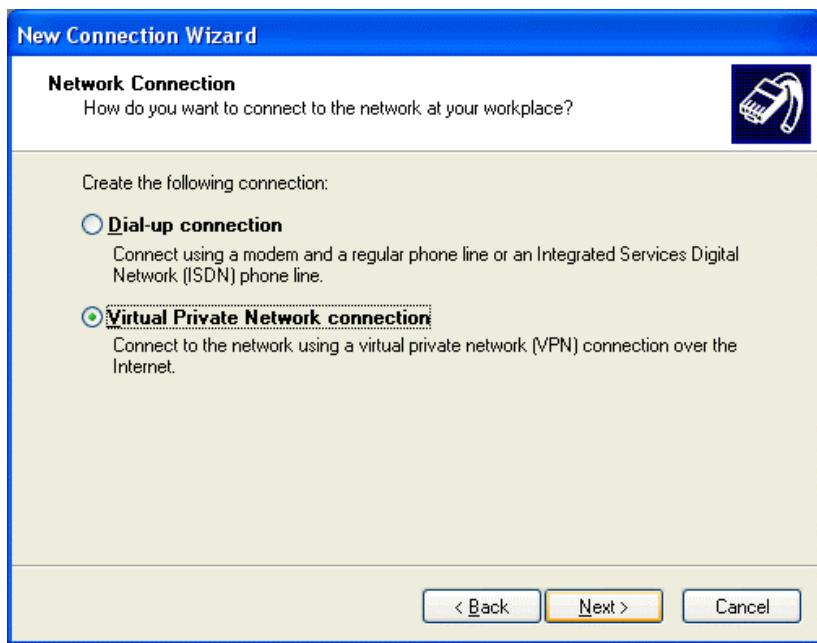
1. Go to **Network Connection** on Control Panel
2. Click on **Create a new connection**.



3. Click on **Next** button



4. Click on **Connect to the network at my workplace**.
5. Click on **Next** button

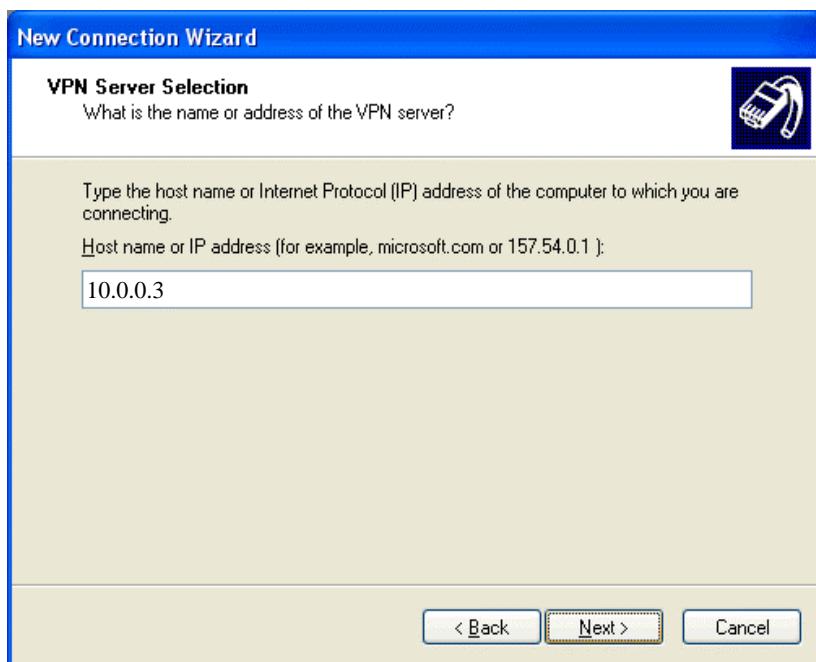


6. Click on **Virtual Private Network connection**
7. Click on **Next** button



8. Enter the name of this VPN connection. In this case, the name is To VPN router.
9. Click on **Next**

Then, enter Matrix's domain IP address. If you're using static IP and already applied for a domain name, or if you are using dynamic IP with DDNS domain name applied and activated built-in DDNS function in this router. Then you can enter the domain name in this section.



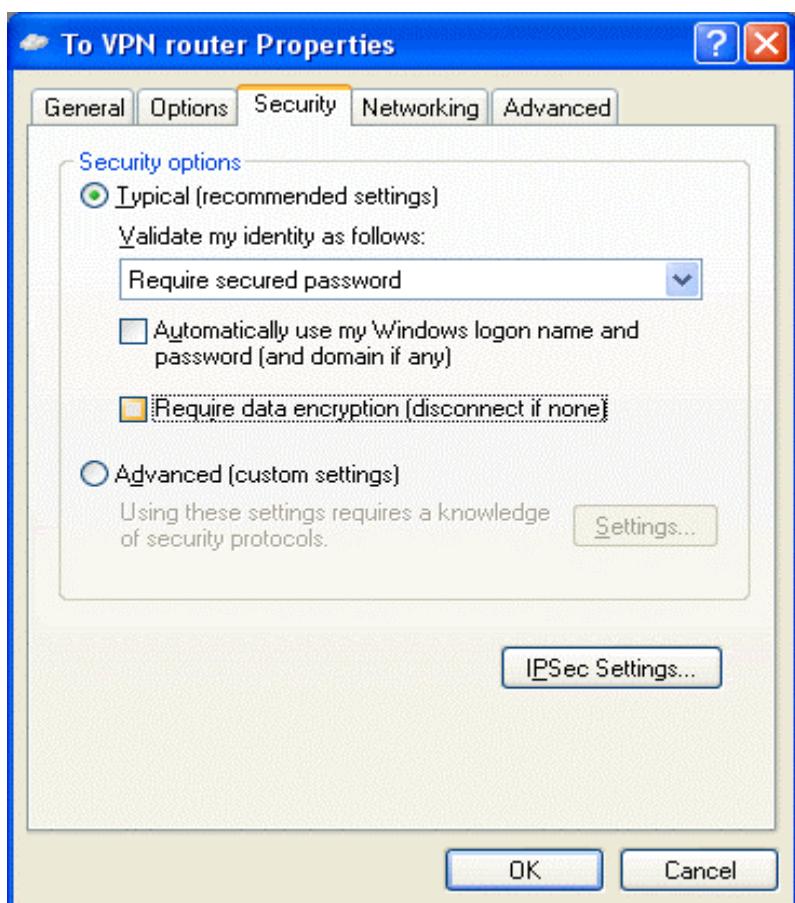
10. Enter the WAN IP address or DDNS domain name of your VPN router.
11. Click on **Next**



12. If you would like this connection to appear on your desktop. Please do so by ticking the check box of **Add a shortcut to the connection to my desktop.**
13. Click on **Finish** button.



14. Click on **Properties** button



15. Un-tick or cancel the check box of **Require data encryption** (disconnect if none)

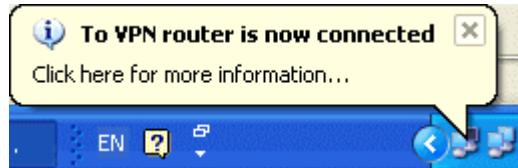
16. Click on **OK**



17. Enter your **User name** and **Password**

18. Click on **Connect** button.

**Once the successful connection is made, your WINXP connection logo will appear on the bottom of your Window to confirm the successful connection.**



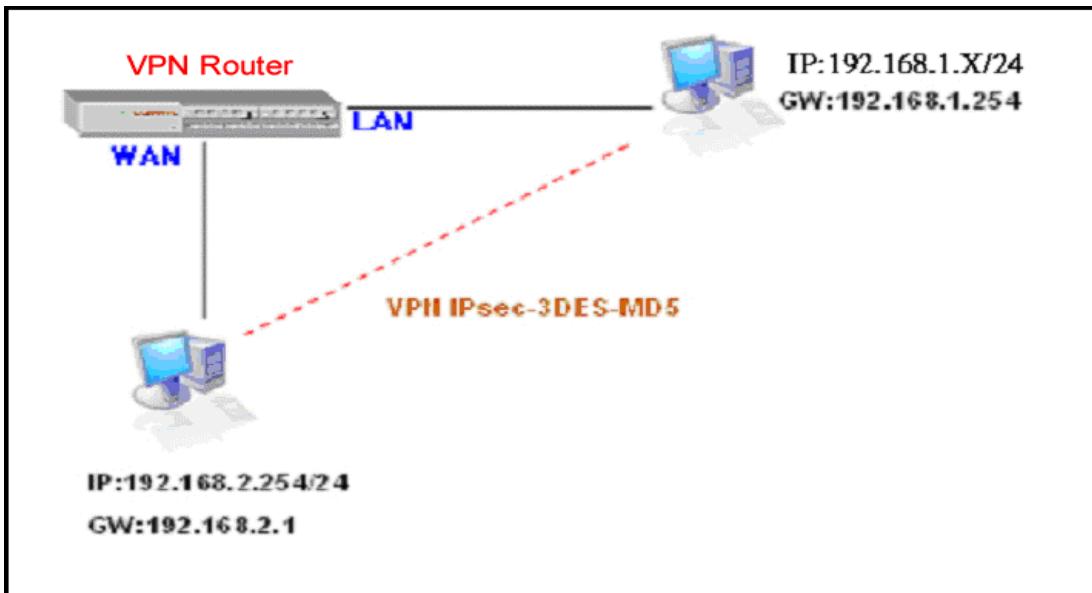
You can also access to your web-based management page from your router and go to PPTP server setting page. From the bottom of the page, you will see the current PPTP VPN connection status from Client Management section.

On Client Management section, if Disconnect check box is ticked and click on Set, it will allow PPTP disconnection. If the Reset button is clicked, PPTP disconnection will be cancelled and the PPTP will be reconnected again.

Now the remote PC can access the Local LAN. It should be able to ping the PC at 192.168.1.2 directly.

## Example 3: IPSEC Configuration Example

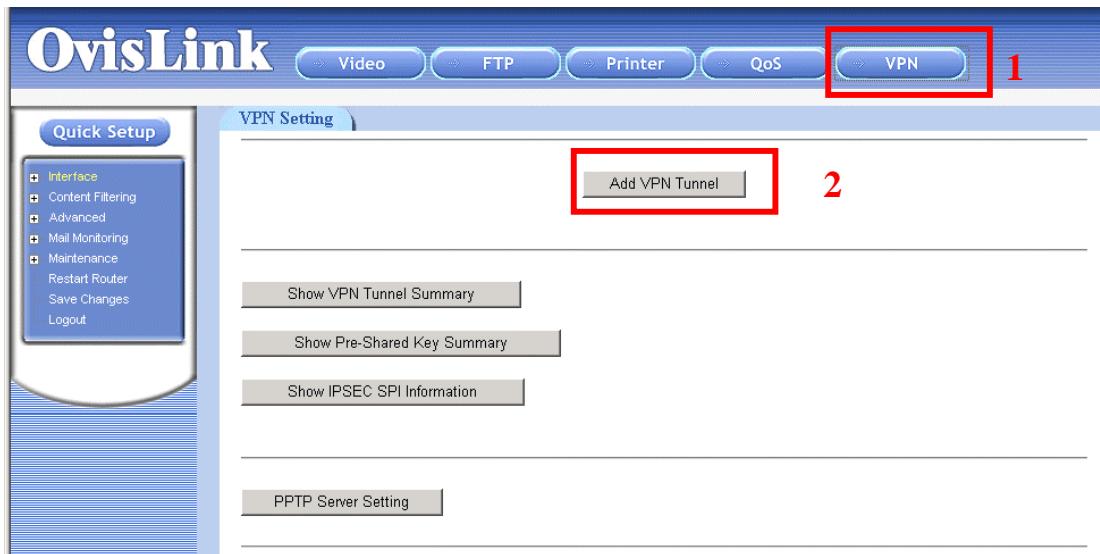
IPSec provide tunneling, authentication, and encryption technique so it ensure your data is safely transmitted on Internet without been attack by hackers. In order to create a secure VPN tunnel or channel between two endpoints by IPSEC, please take the following steps.



The above diagram provides simple illustration of how to connect two end points via your router by VPN technique. In this case, a PC with IP address of 192.168.2.254/24 is trying to connect with another PC with its IP address of 192.168.1.x/24 via your VPN router with it's IP address of 192.168.1.254/24.

The above diagram is the basis for the configuration environment of our VPN router.

## Router's IPsec Setup



1. Click on **VPN** button on top manual bar of your web page.
2. Click on **Add VPN Tunnel**.

**VPN Setting**

**Tunnel Name:** ForWinXP 3

**Tunnel Status:** Enable 4

**Local Secure Group**

**IP Address/Mask:** 192.168.1.0/24 <A.B.C.D/M>

**Remote Secure Group**

**IP Address/Mask:** <A.B.C.D/M>

**Remote Secure Gateway (Road Warriors Please Specify 0.0.0.0)**

**\* IP Address:** 0.0.0.0

**\* FQDN:**

**Encryption:** 3DES

**Authentication:** MD5

**Encapsulation:** Tunnel

**Key Management**

**Key Exchange Method:** Auto(IKE)

**PFS:** Enable

**\*Pre-Shared Key:** vpntest

**Key Lifetime:** 3600 <1200-28800>

**Add** **Reset**

3. Enter the name of the tunnel in the **Tunnel name** field. It allows you to identify multiple tunnels from your tunnel group. It does not have to match the name used at the other end of the tunnel. **For this example, please enter “ForWinXP”**
4. Select **Enable** from Tunnel Status field to activate the tunnel.
5. The **Local Secure Group** is the computer (s) on your LAN that can access the tunnel. Enter the IP address and subnet mask of your local VPN router in the field. **For this example, enter “192.168.1.0/24”**
6. The **Remote Secure group** is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the IP address and subnet mask of the computer at the other end of the tunnel in this field. **Since in this example, we leave the option open for any PC with correct authentication key. Therefore, we leave the option blank.**
7. The Remote Security Gateway is the VPN device, such as a second VPN router on the remote end of the VPN tunnel. Enter the IP address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN router, a VPN server, or a computer with VPN client software that supports IPSec. The IP address may either be static or dynamic, depending on the settings of the remote VPN device. Make sure that you have entered the IP address correctly, or the connection cannot be made. **In this example, since the connection is for any remote PC with correct authentication key, we leave it at “0.0.0.0”.**
8. Currently you have only one option to select one type of **Encryption** as **3DES**. This is the most secure type of encryption and it is set as the default value.
9. From **Authentication**, you have option to select either **MD5** or **SHA1**. It is recommended to select SHA1 as it is more secure than MD5.
10. From **Key Management** section, select Auto (IKE) as default value and select PFS (Perfect Forward Secrecy) and enter a series of numbers or letters in the **Pre-Shared Key** field. Based on this word, which must be entered at both ends of the tunnel. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the **Key Lifetime** field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you like the key to be useful. The default value if Key Lifetime is 3600 seconds. In this example, we use **“vpntest”**
11. Click on **add** to confirm your VPN tunnel settings.

After the VPN tunnel has been established, you should see the name of VPN tunnel and status from the first page as following:

VPN Setting

---

VPN Tunnel

Tunnel Name	Status
<a href="#">ForWinXP</a>	Enable

---

[Add VPN Tunnel](#)

---

[Show VPN Tunnel Summary](#)

---

[Show Pre-Shared Key Summary](#)

---

[Show IPSEC SPI Information](#)

---

[PPTP Server Setting](#)

---

### Show VPN Tunnel Summary

To view IPsec VPN tunnel setting values, please click on **Show VPN Tunnel Summary** button to access the information.

VPN Tunnel Summary

---

```
Interface wan crypto map detail:

Crypto map "ForWinXP" ipsec-isakmp
  Match address 192.168.1.0/24
  Current peer: 0.0.0.0
  Transform-set=(ForWinXP)
  Security association lifetime: 28800 seconds
  PFS (Y/N): Y
  ISAKMP authentication : Pre-share
  ISAKMP Security association lifetime: 3600 seconds
  Passive mode(Y/N) : N
```

---

### Show Pre-Shared Key Summary

To view all Pre-shared Key configuration information, please click on Show

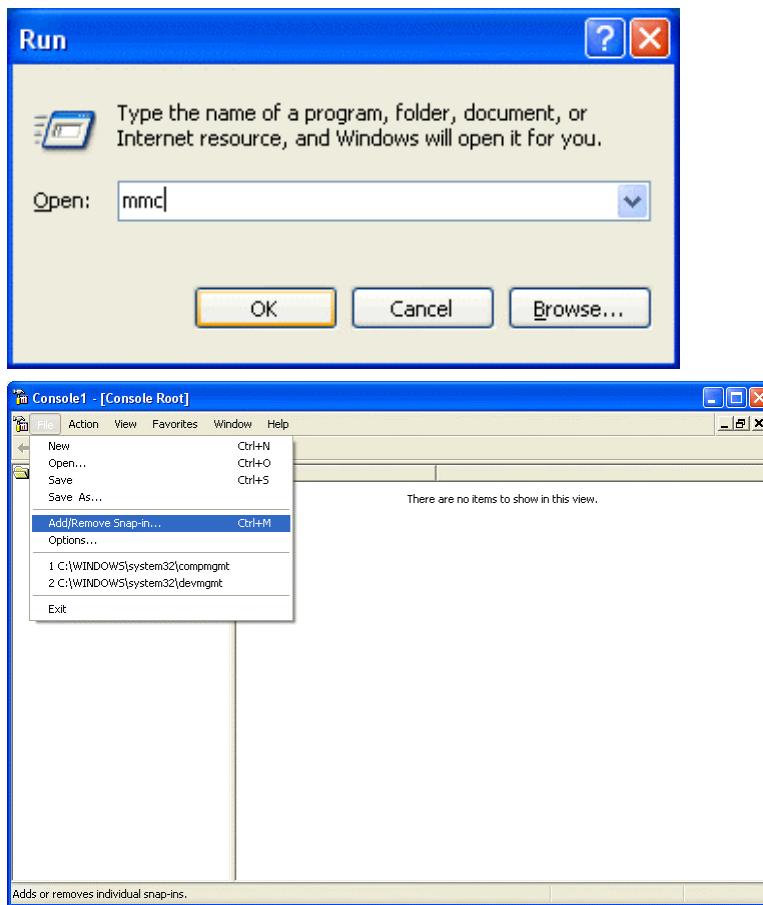
Pre-Shared Key Summary button.

ISAKMP Preshared Keys	
IP Address/Hostname	Preshared Key
0.0.0.0	vpntest

Since the VPN has not yet established, therefore if you click on “**Show IPSec SPI Information**” then it will show no values.

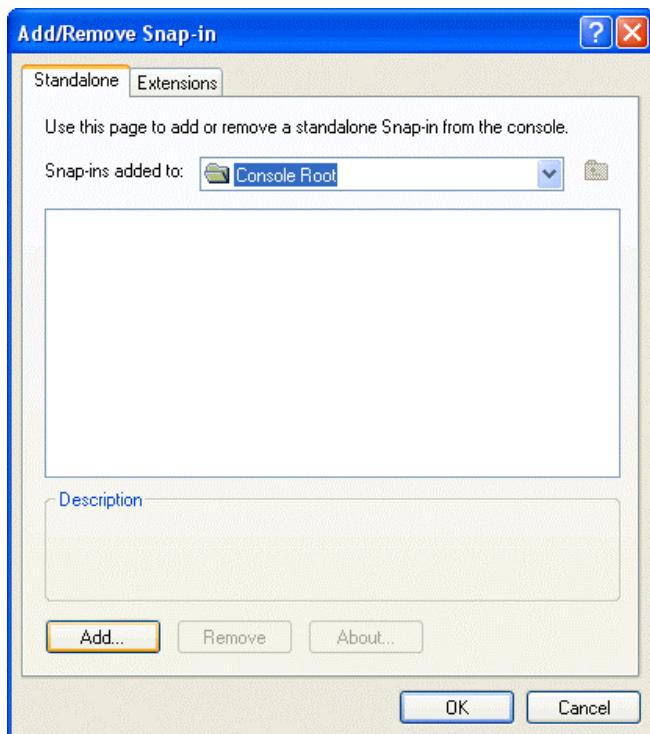
### PC's IPsec Setup (WinXP)

The following section will explain the configuration steps on how to connection VPN tunnels between your PC (WinXP) with your VPN router.

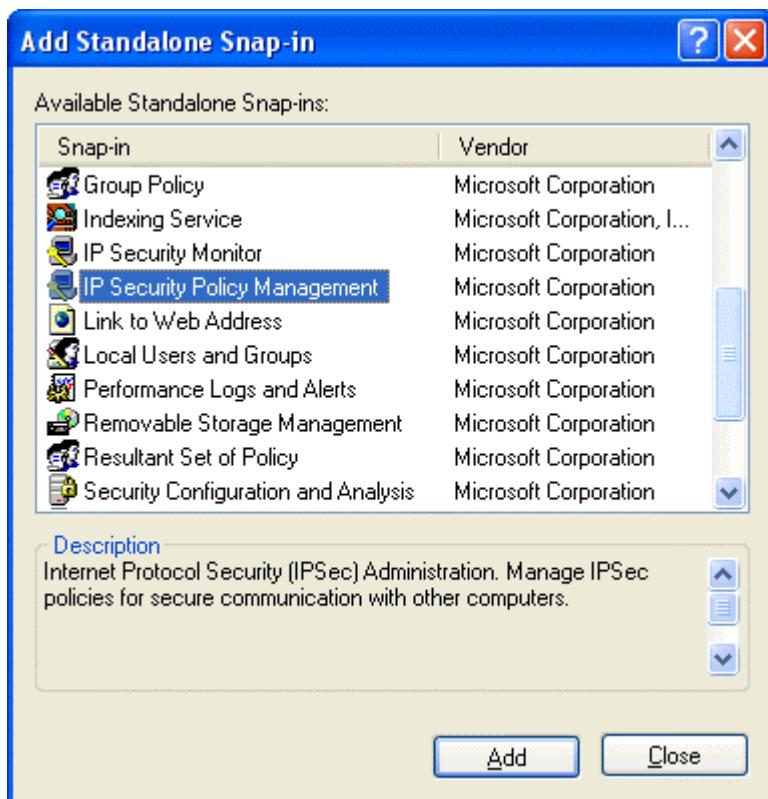


19. Go to **Start** button and select **Run**
20. Type **mmc** in **open** field
21. Click **Ok**.

22. From **File** pull-down window, select **Add/Remove Snap-in**

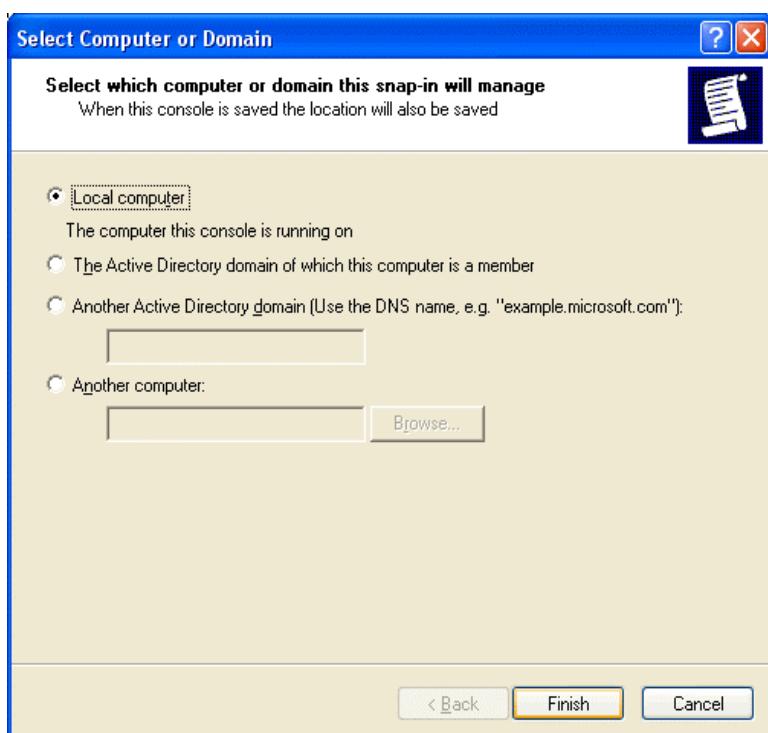


23. Click on **Add** button



24. Click on **IP Security policy management**

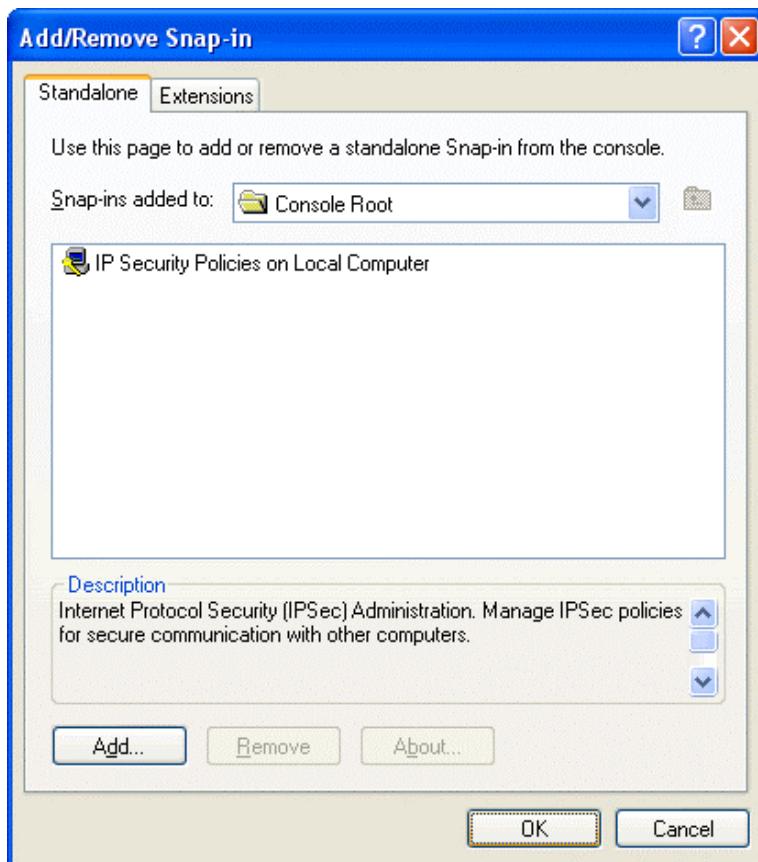
25. Click on **Add** button



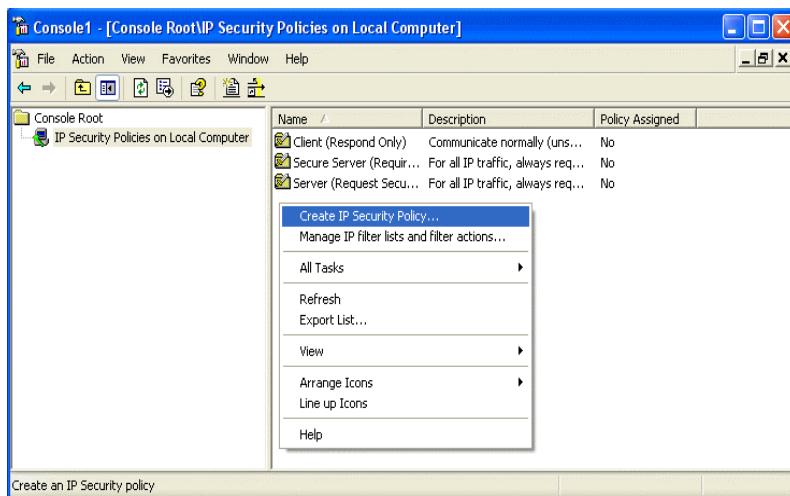
26. Select Local Computer  
27. Click on Finish button



28. Click on Close button



29. Click on **OK** button



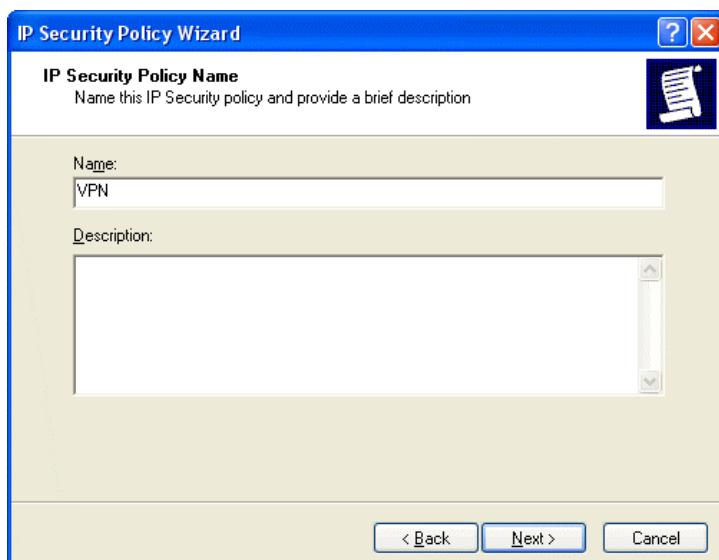
30. Click on **IP Security Policies on Local Computer** on the left screen

31. On the right screen, move your mouse cursor to the blank area and hit a single click on the right hand button of your mouse.

32. Select **Create IP Security Policy** from the pull-down window.



33. Click on **Next** button

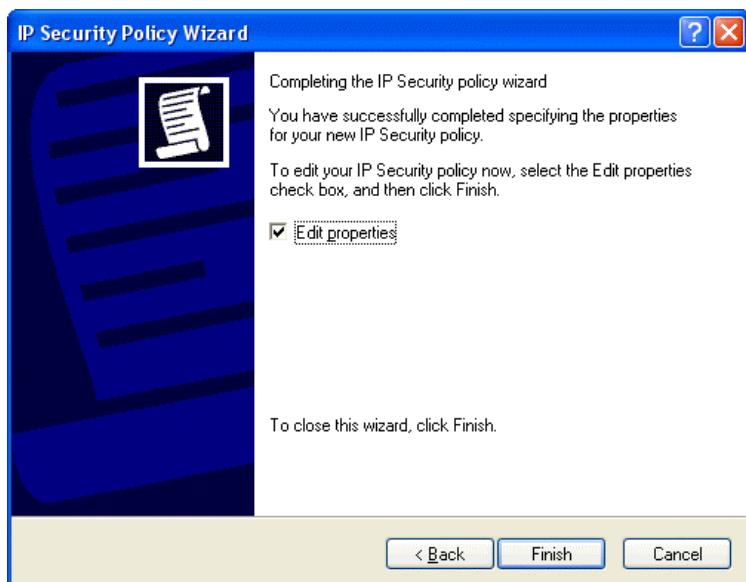


34. From the **Name** field, enter the name of VPN tunnel. (in this case, the name is called VPN)

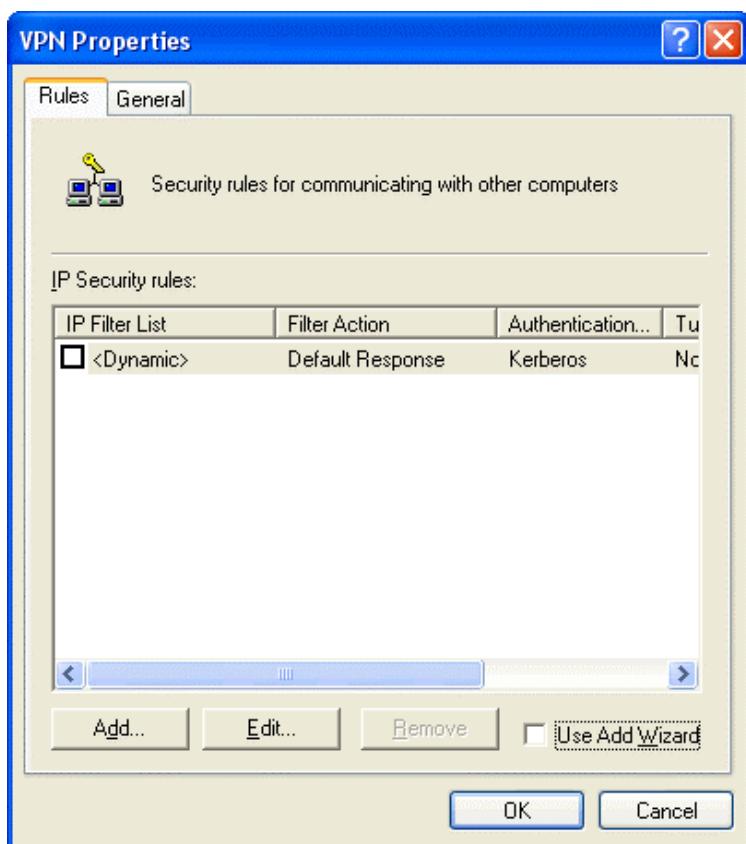


35. Un-check or cancel the square box next to **Activate the default response rule**.

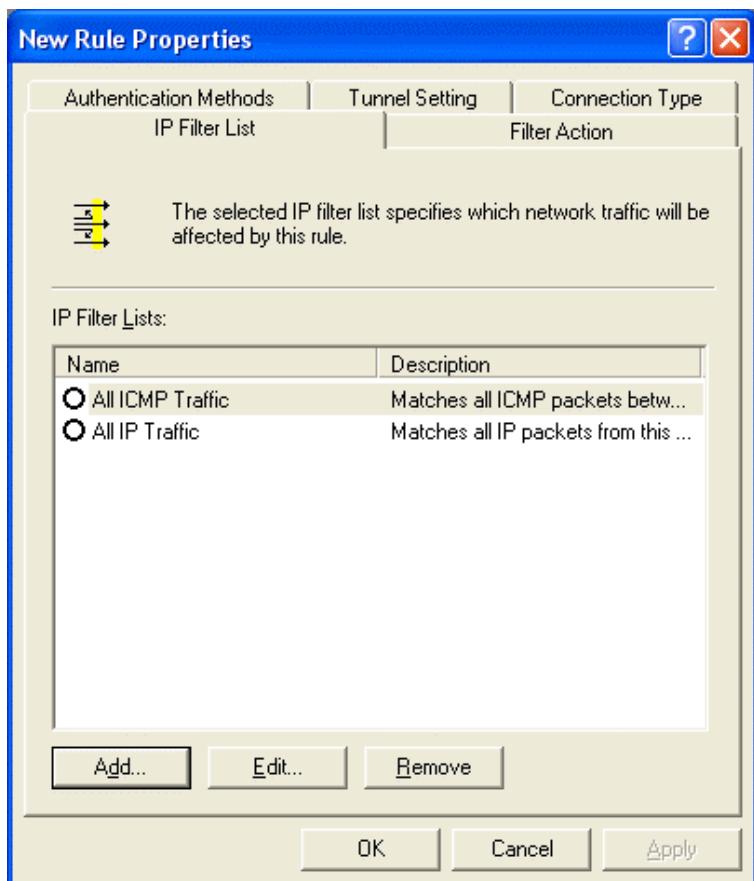
36. Click on **Next** button



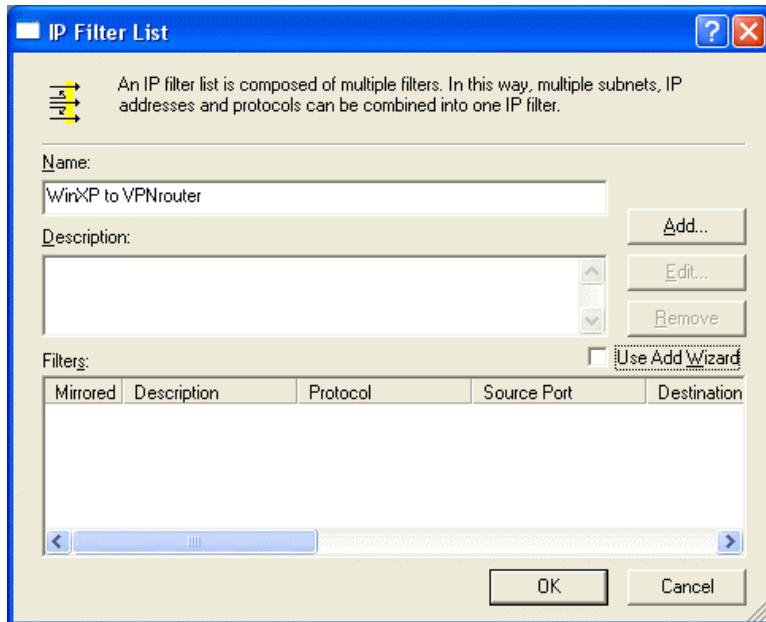
37. Tick on the square box next to **Edit properties**
38. Click on **Finish** button



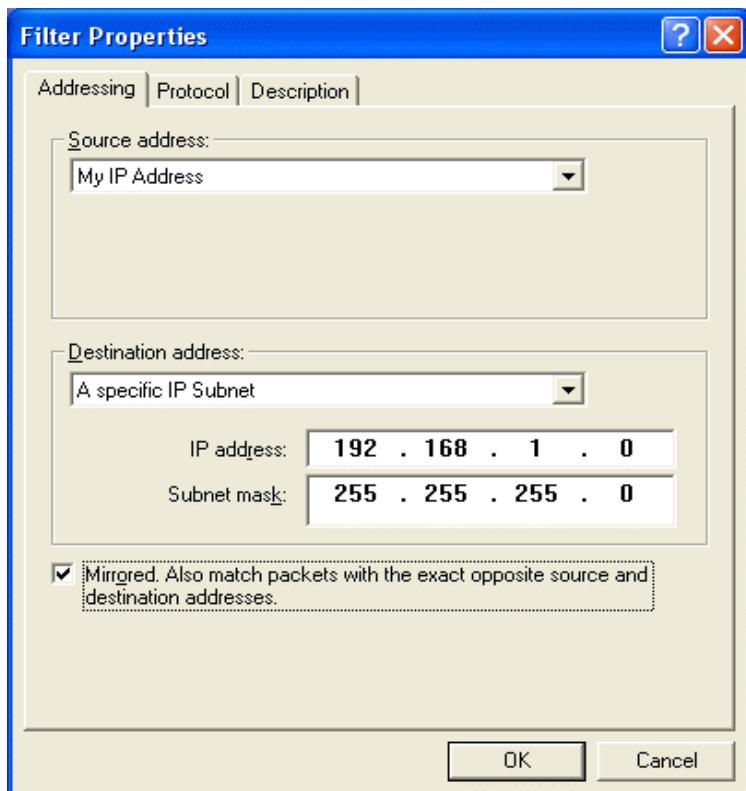
39. Un-tick or cancel **Use Add Wizard**
40. Click on **Add** button



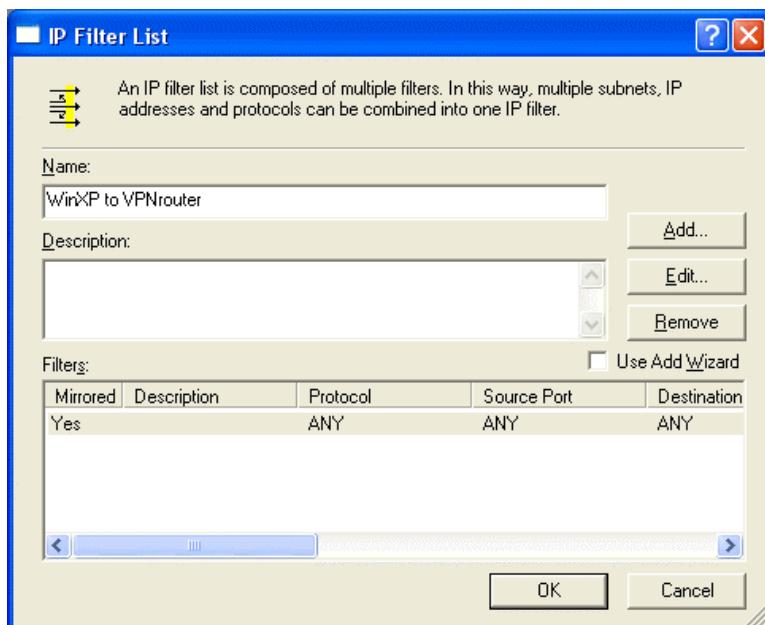
41. Click on **Add** button



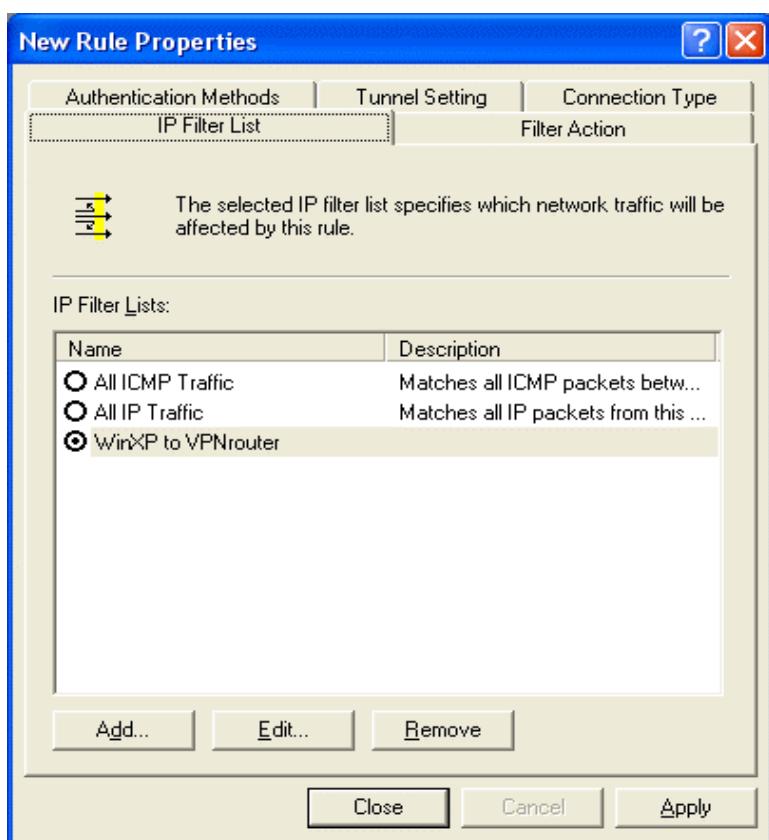
42. Enter the **name** of the **IP Filter List**.  
(In this case, the name is WinXP to VPNrouter)



43. From **Source address** pull-down window, select **My IP Address**
44. From **Destination address** pull-down window, select **A specific IP Subnet**. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255.255.0)
45. Check the box of **Mirrored. Also match packets with the exact opposite source and destination addresses.**
46. Click on **OK** button

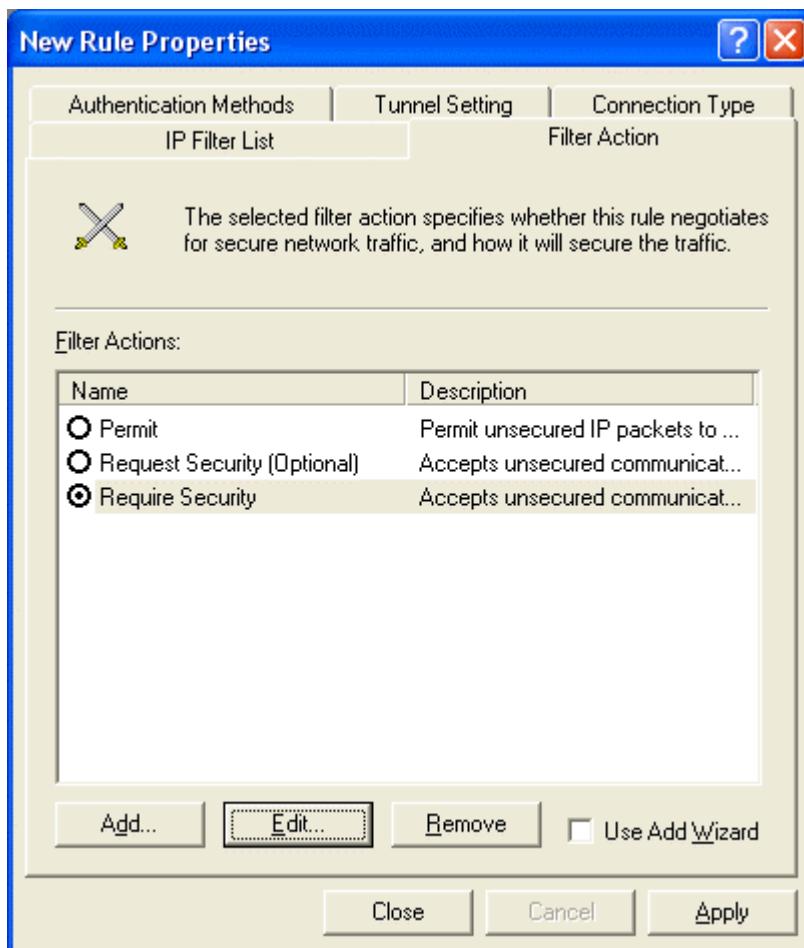


47. Click on **OK** button

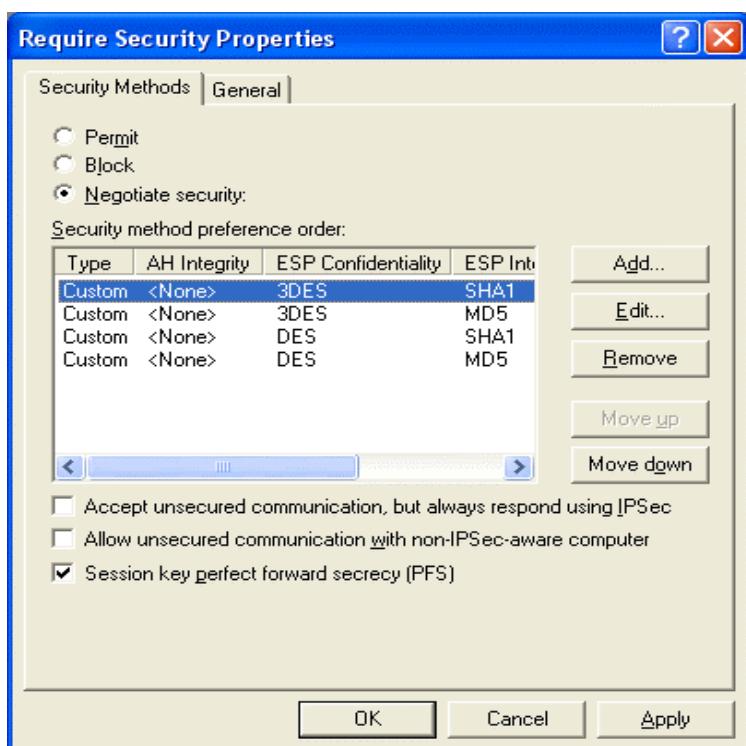


48. Click on IP Filter name of your previous setting. (in this case, it's WinXP to VPNrouter)

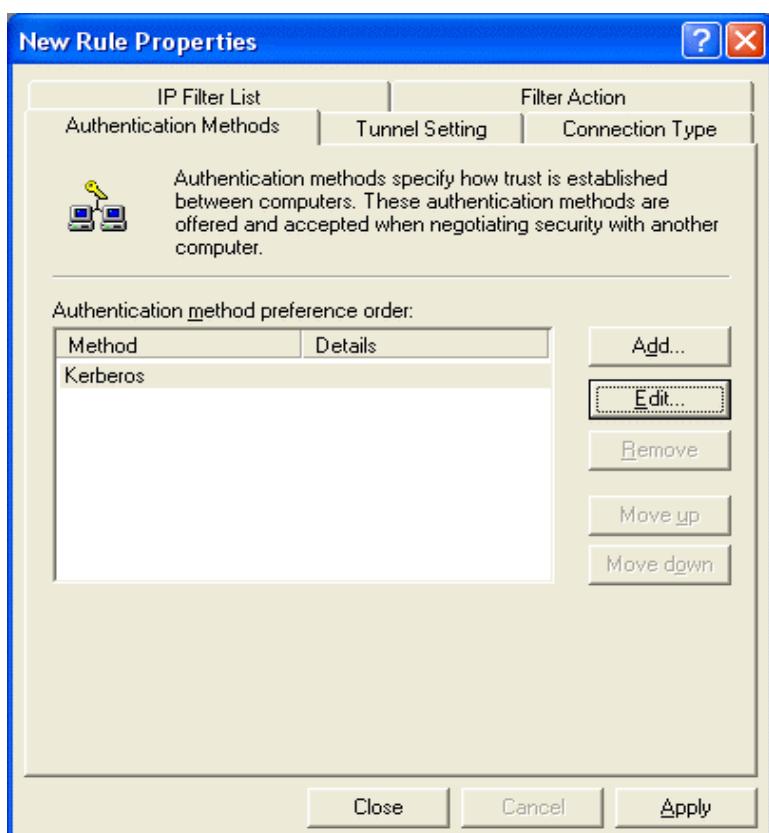
49. Click on **Filter Action** tab from the top.



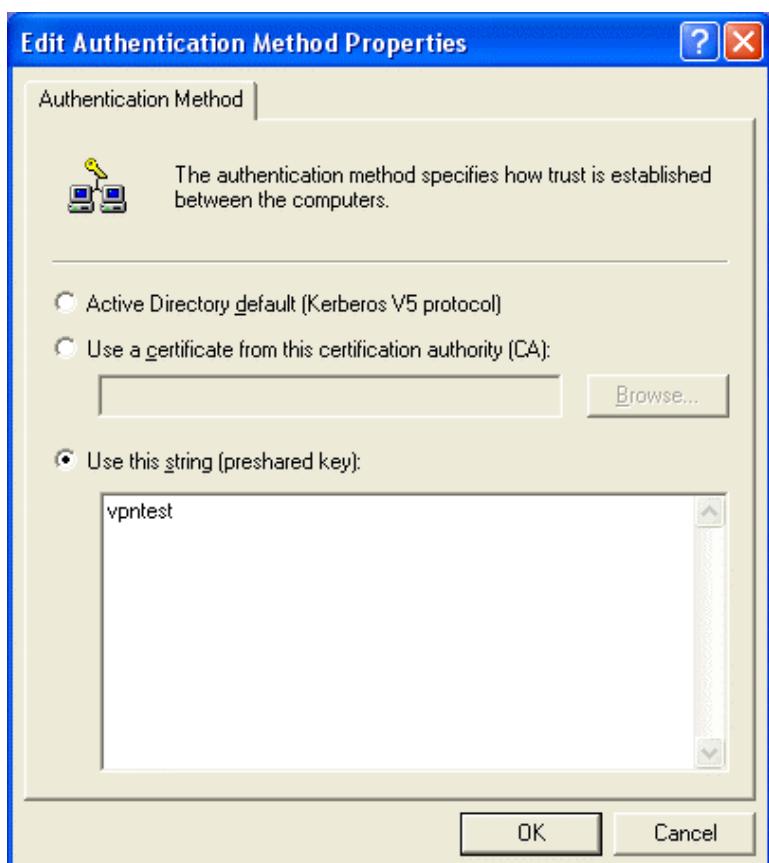
50. Click on **Require Security**  
 51. Click on **Edit** button



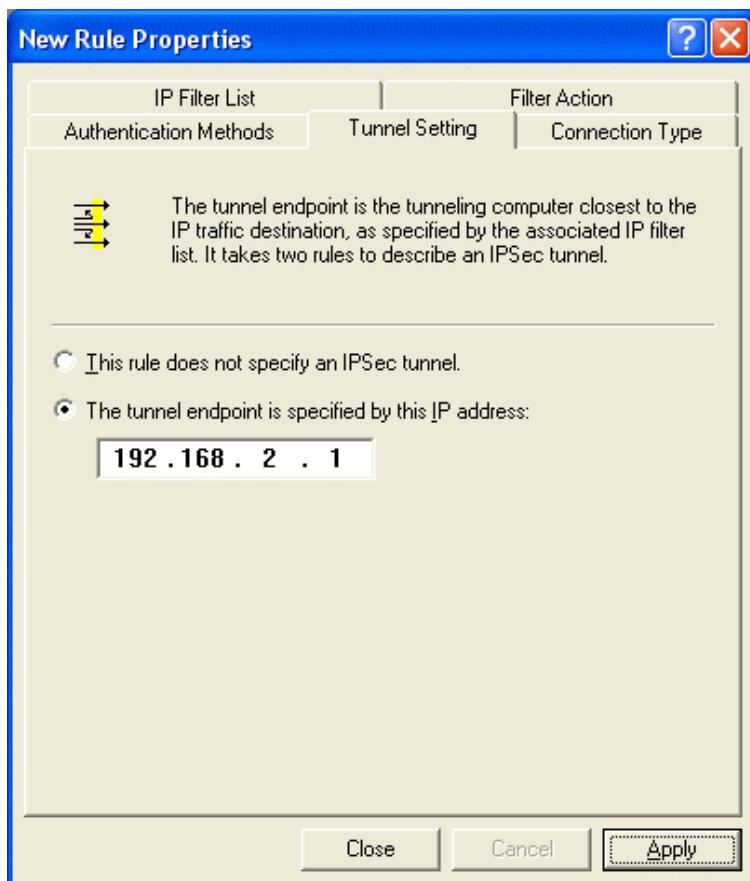
52. Click on **Negotiate security**  
 53. Cancel the check box of **Accept unsecured communication, but always respond using IPSec**  
 54. Tick the box of **session key perfect forward secrecy (PFS)**.  
 55. Click on **OK** button



56. Click on **Edit** button



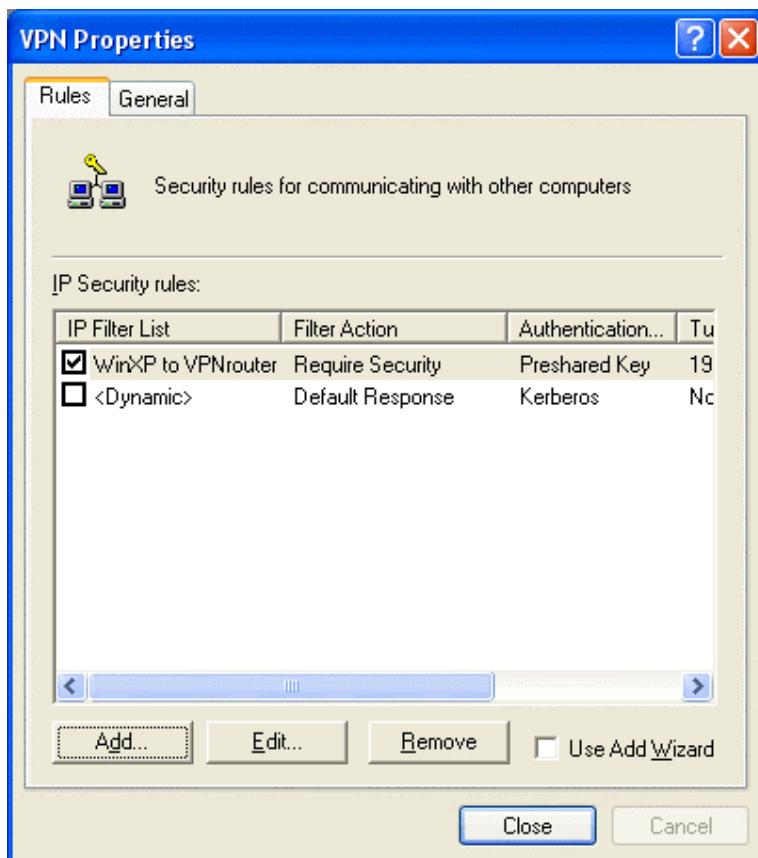
57. Click on **Use this string** (preshared key)
58. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting.
59. Click on **OK** button



60. Click on **The tunnel endpoint is specified by this IP address**

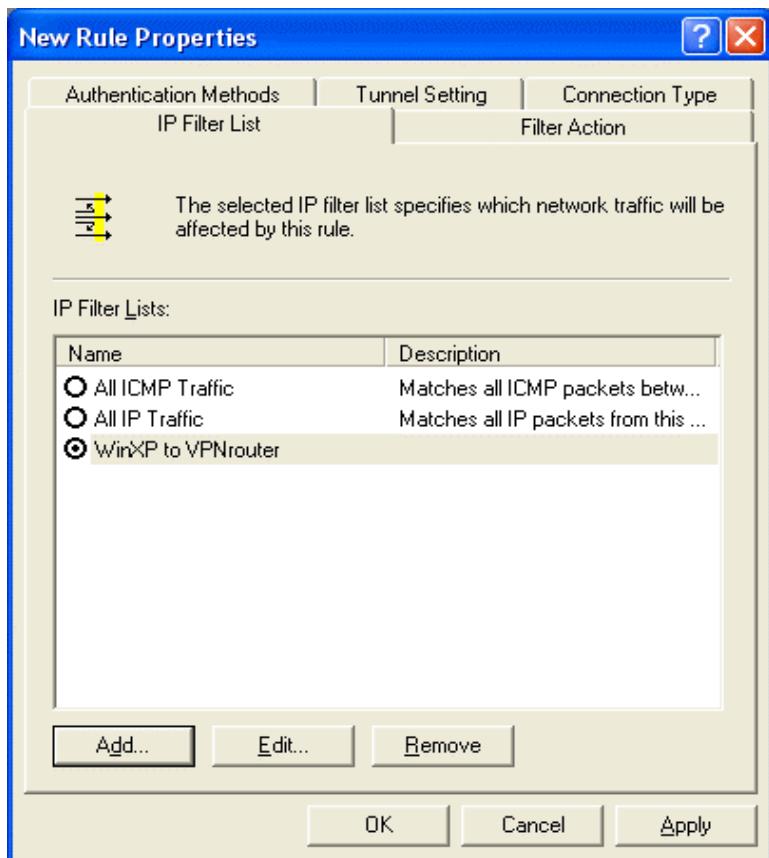
61. Enter the **WAN IP address** of destination endpoint of VPN tunnel. (in this case, it's 192.168.2.1)

62. Click on **Apply** button

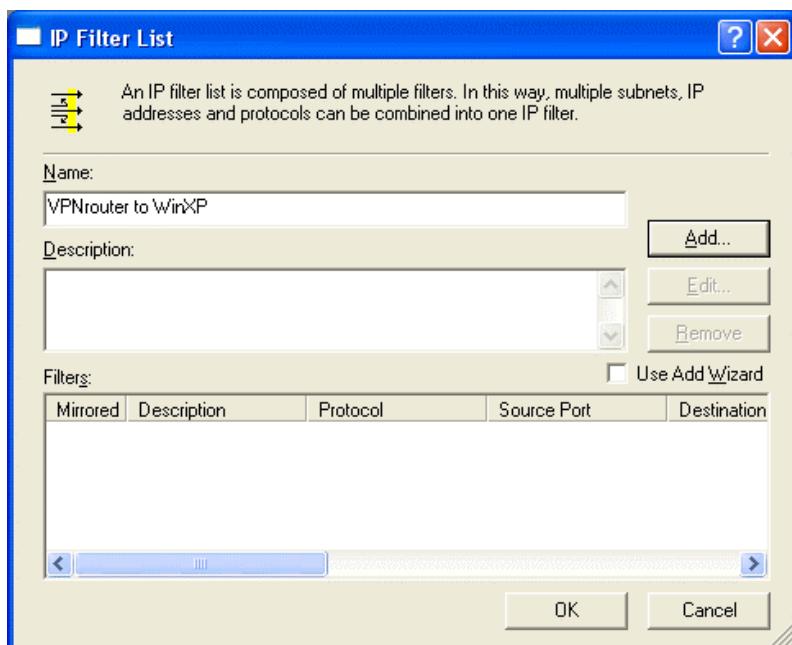


63. Click on pre-defined IP Security rules. (in this case it's WinXP to VPNTunnel)

64. Click on **Add** button

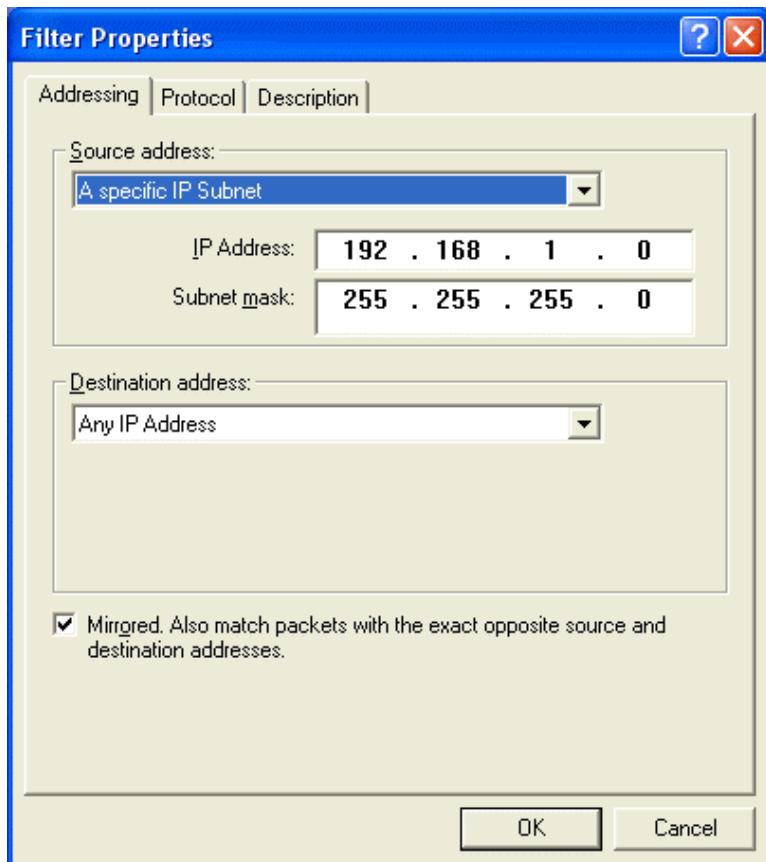


65. Click on **Add** button



66. Enter the name of IP filter list in opposite direction. In this case, it's VPNrouter to WinXP.

67. Click on **Add** button



68. From **Source address** pull-down window, select **A specific IP Subnet**

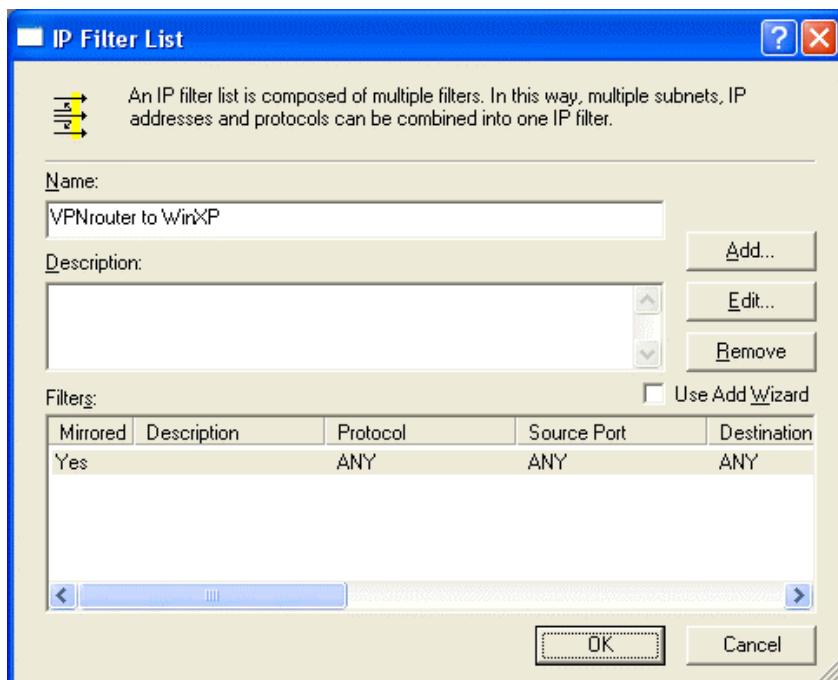
69. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255.255.0).

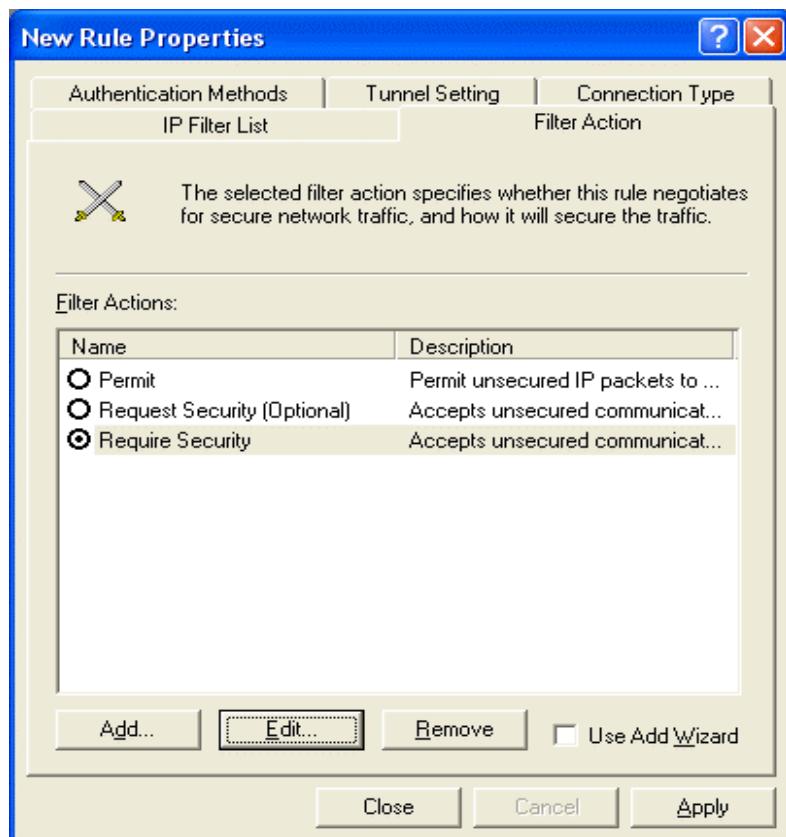
70. From **Destination address** pull-down window, select **Any IP Address**.

71. Check the box of **Mirrored. Also match packets with the exact opposite source and destination addresses.**

72. Click on **OK** button

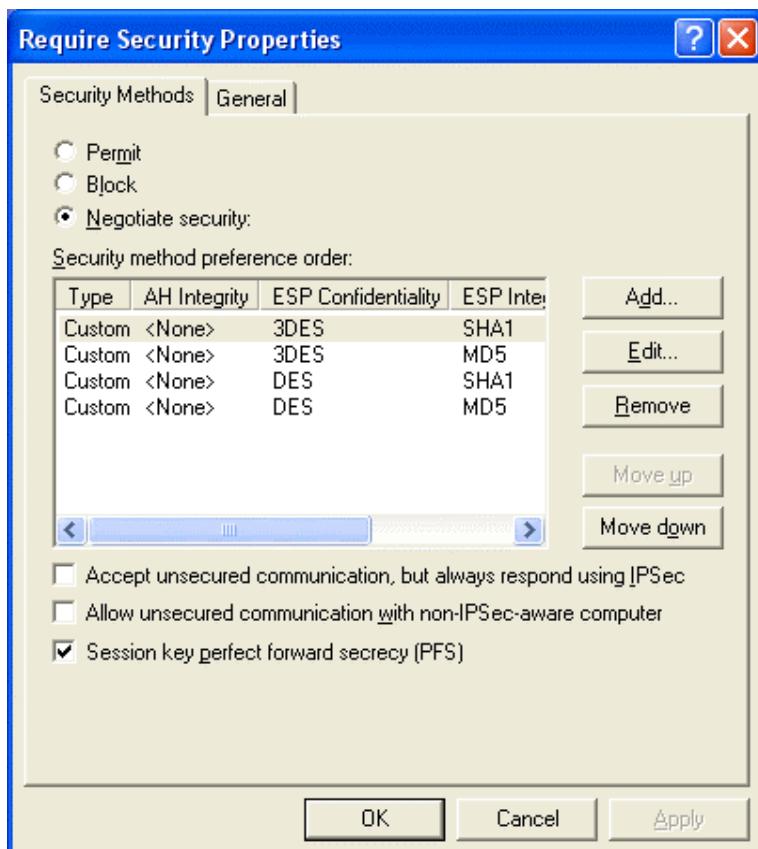
73. Click on **OK** button





74. Click on **Require Security**

75. Click on **Edit** button

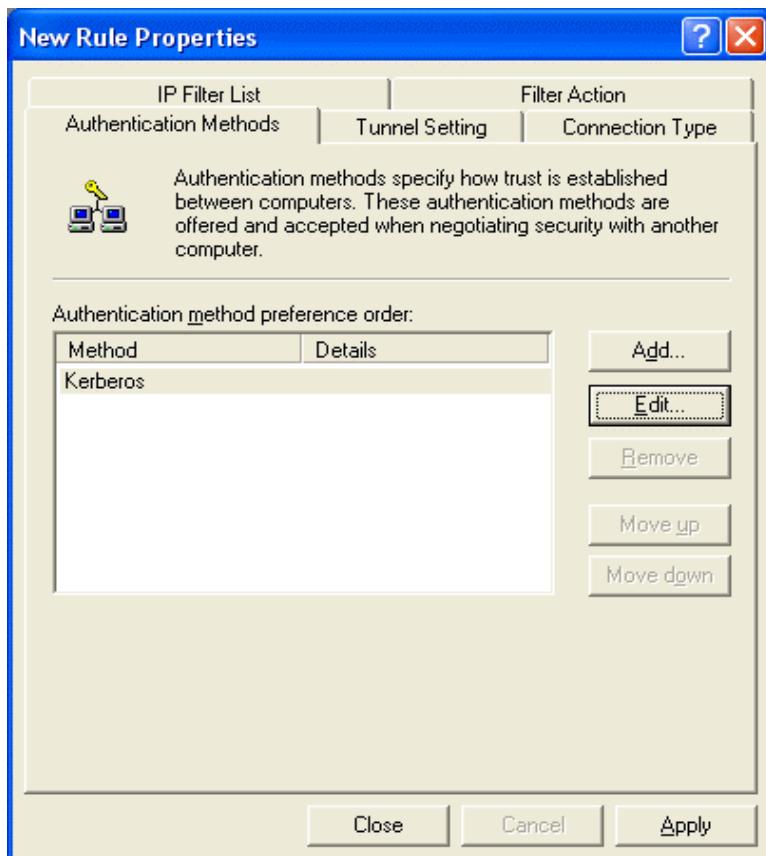


76. Click on **Negotiate security**

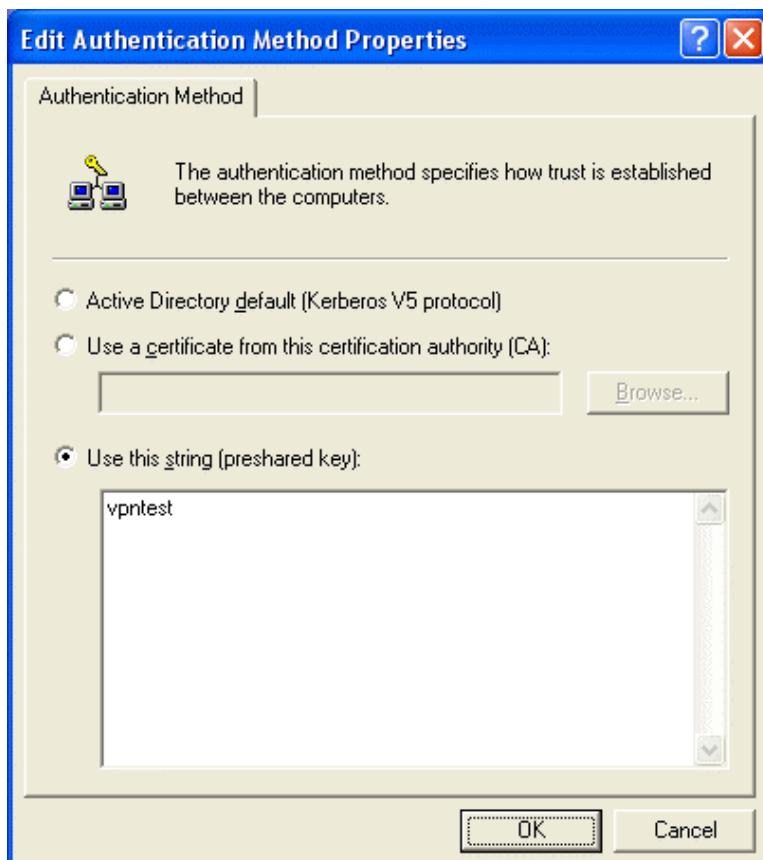
77. Cancel the check box of **Accept unsecured communication, but always respond using IPSec**

78. Tick the box of **session key perfect forward secrecy (PFS)**.

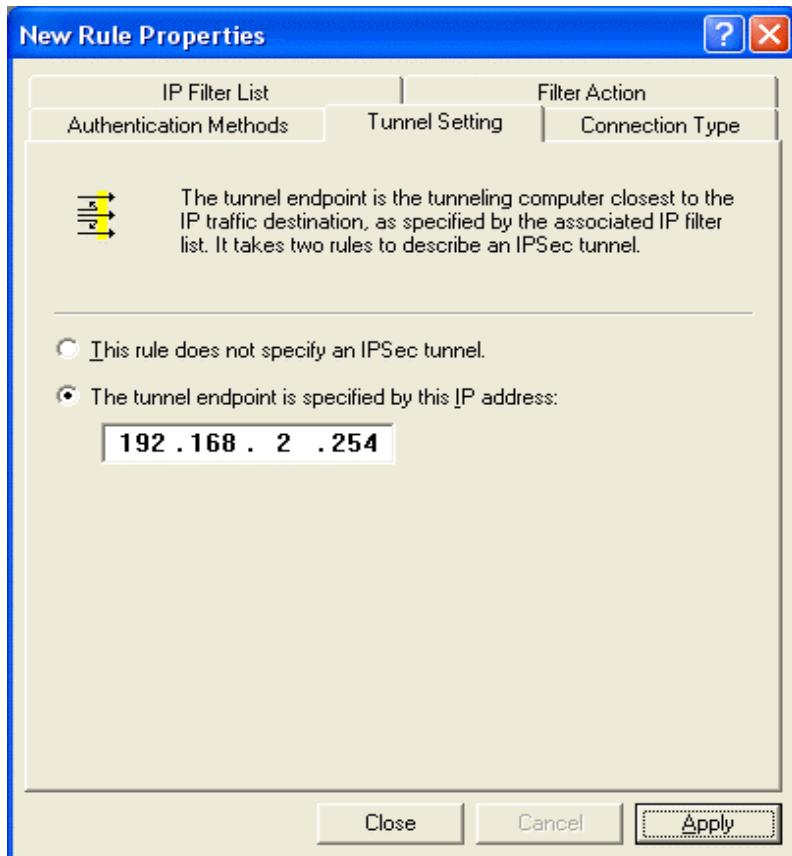
79. Click on **OK** button



80. Click on **Edit** button



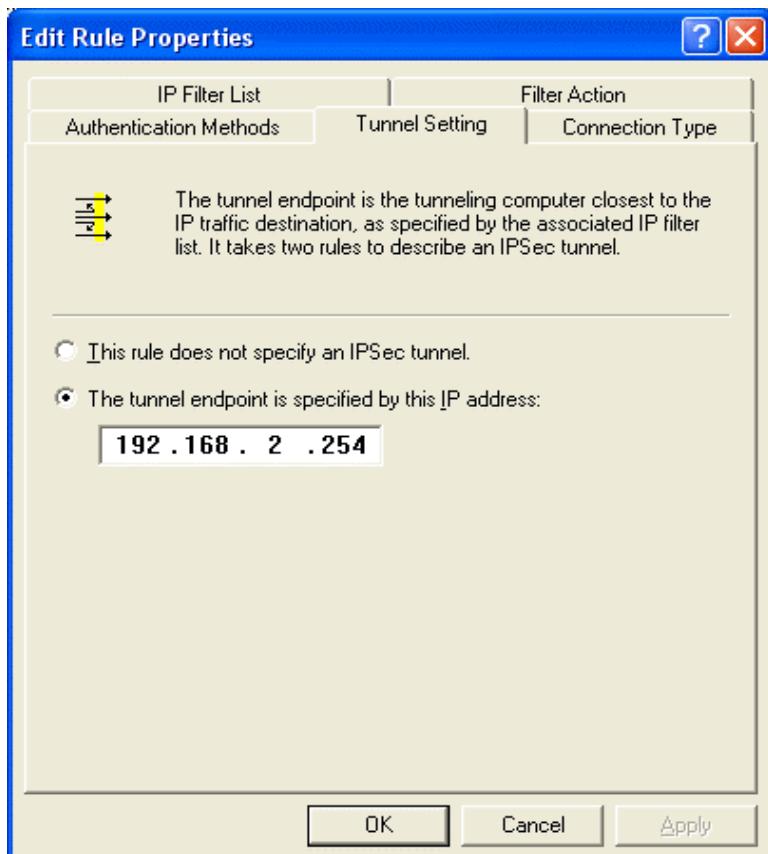
81. Click on **Use this string** (preshared key)  
 82. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting.  
 83. Click on **OK** button



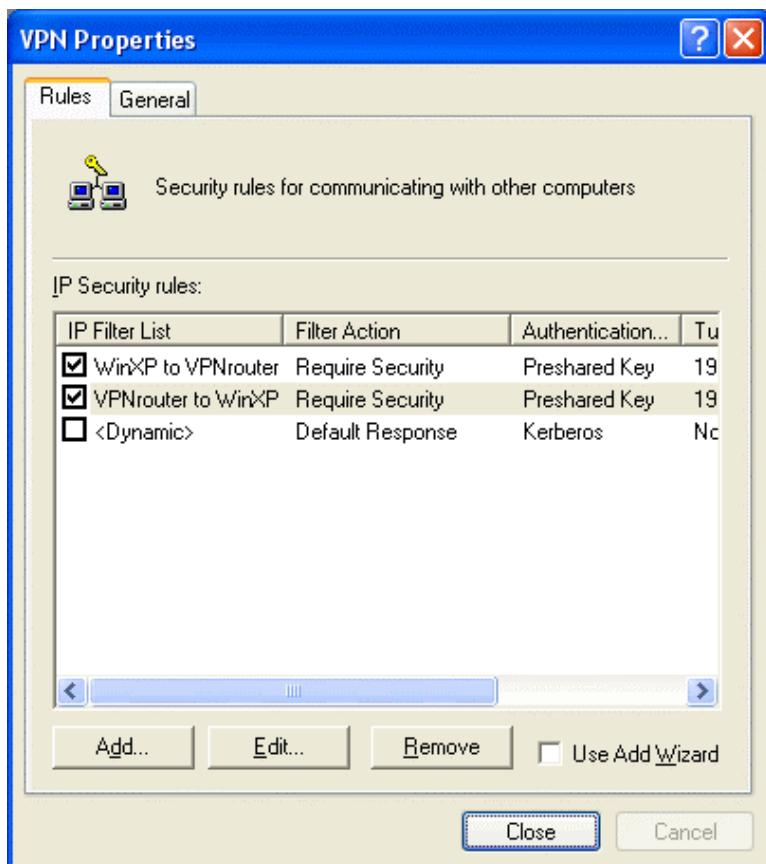
84. Click on **The tunnel endpoint is specified by this IP address**

85. Enter the **WAN IP** address of your WINXP PC (in this case, it's 192.168.2.254)

86. Click on **Apply** button

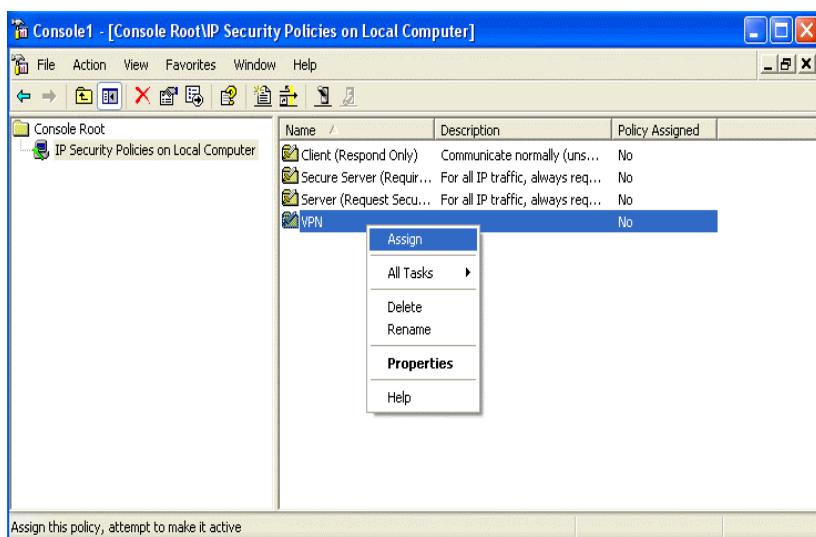


87. Click on **OK** button



88. Make sure you have checked the box of both IP Security rules you configured in previous section. In this case, they are WinXP to VPNrouter and VPNrouter to WinXP.

89. Click on **Close** button



90. From IP Security Policy, click on the name of your VPN tunnel setting and click on the right hand button of your mouse.

91. Click on **Assign** from pull-down window.

Now, you have successfully established the VPN tunnel. In Web-Based management page of your router, go to **VPN > Show IPSEC SPI information**. The information page will appear and show all relevant information regards to your VPN connection.