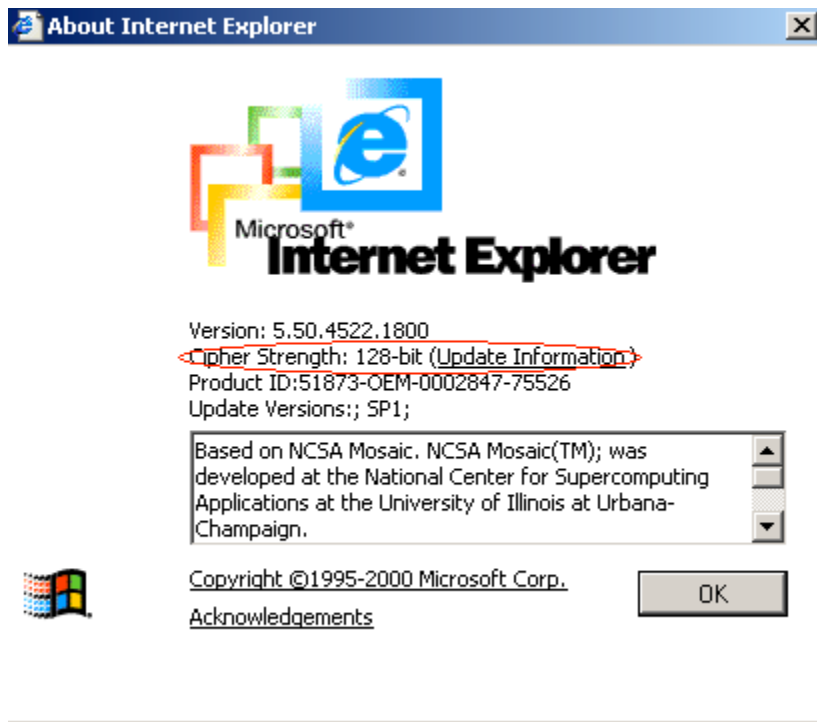


Window 2000 Professional Settings Procedure

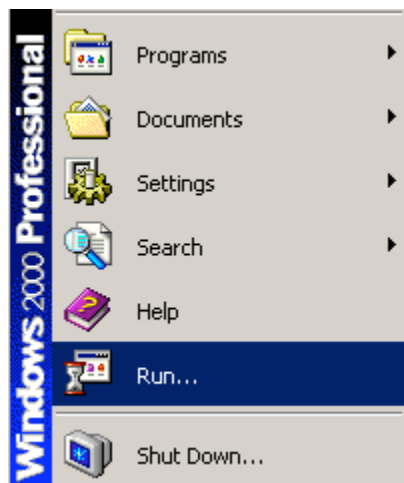
1. Check the encryption of window 2000 professional

Open IE and click on Help – About Internet Explorer, check the cipher strength

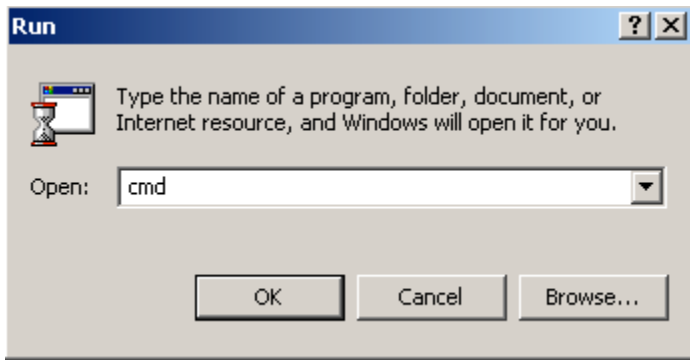


If it is 56-bit, need install Encryption Packet: Encpack_win2000_en.

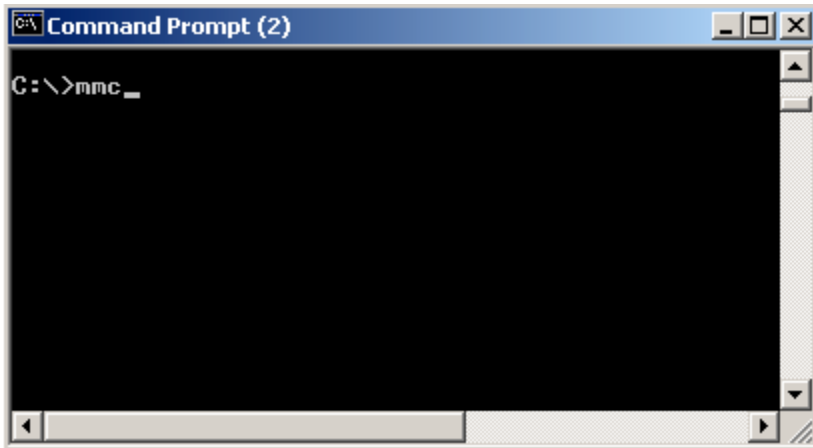
2. Press “Run” of Start Menu



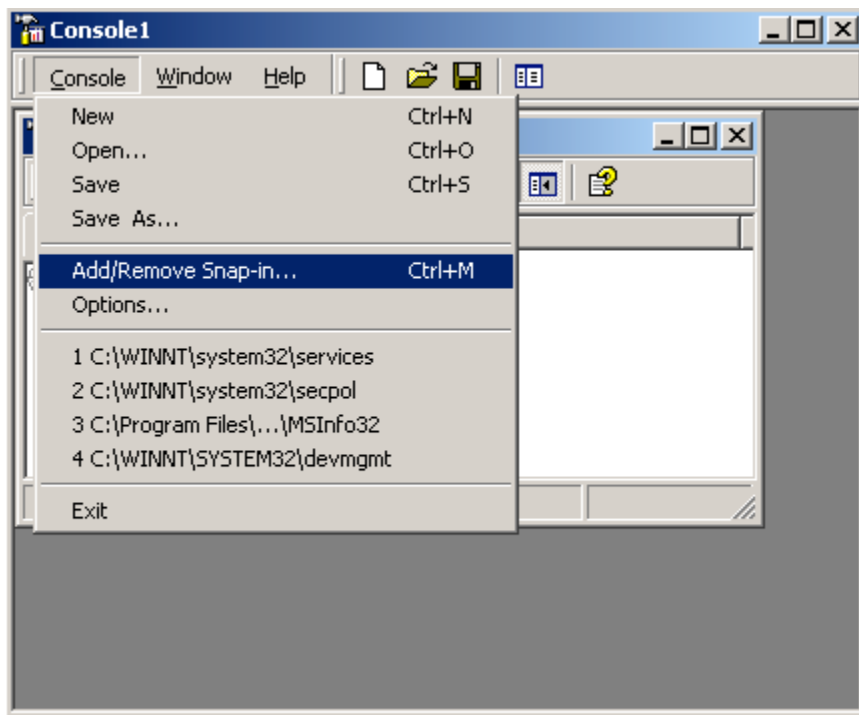
3. Type “cmd” into DOS command mode



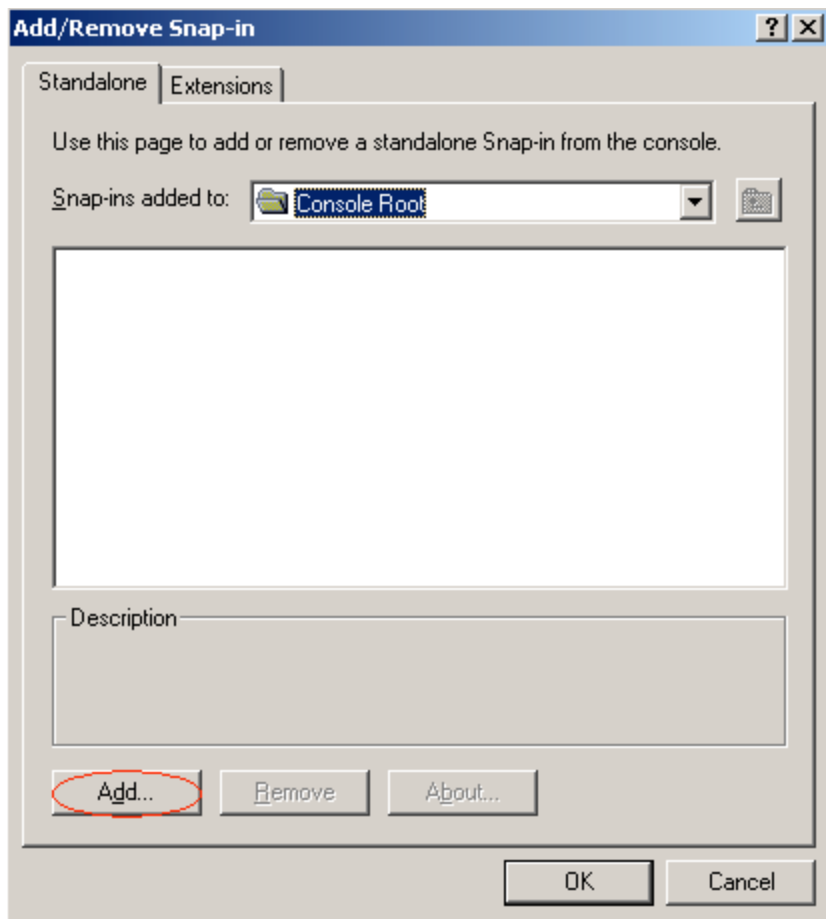
4. Type “**mmc**” on DOS command mode



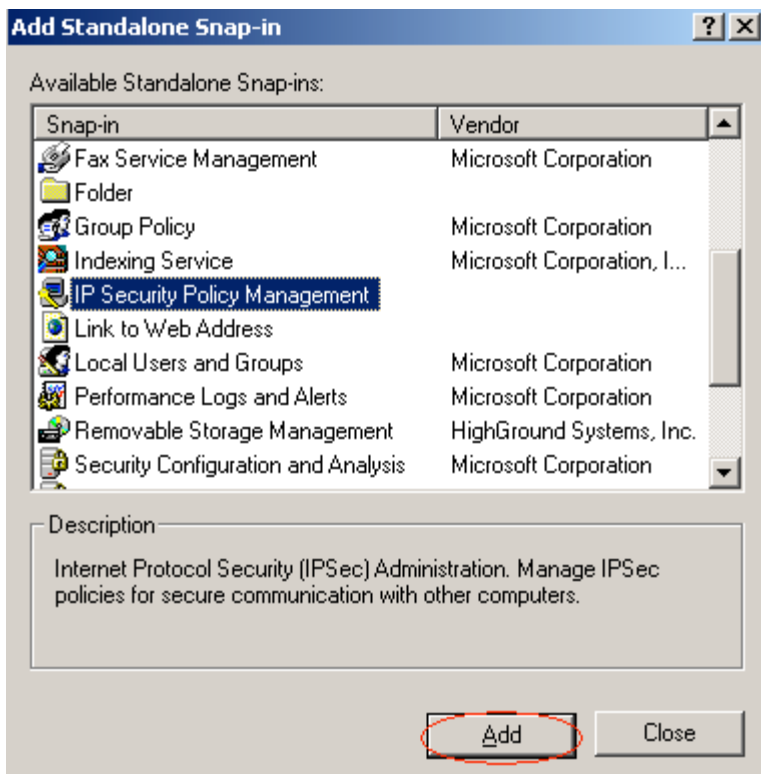
5. Click on **Console**, then **Add/Remove Snap-in ...**



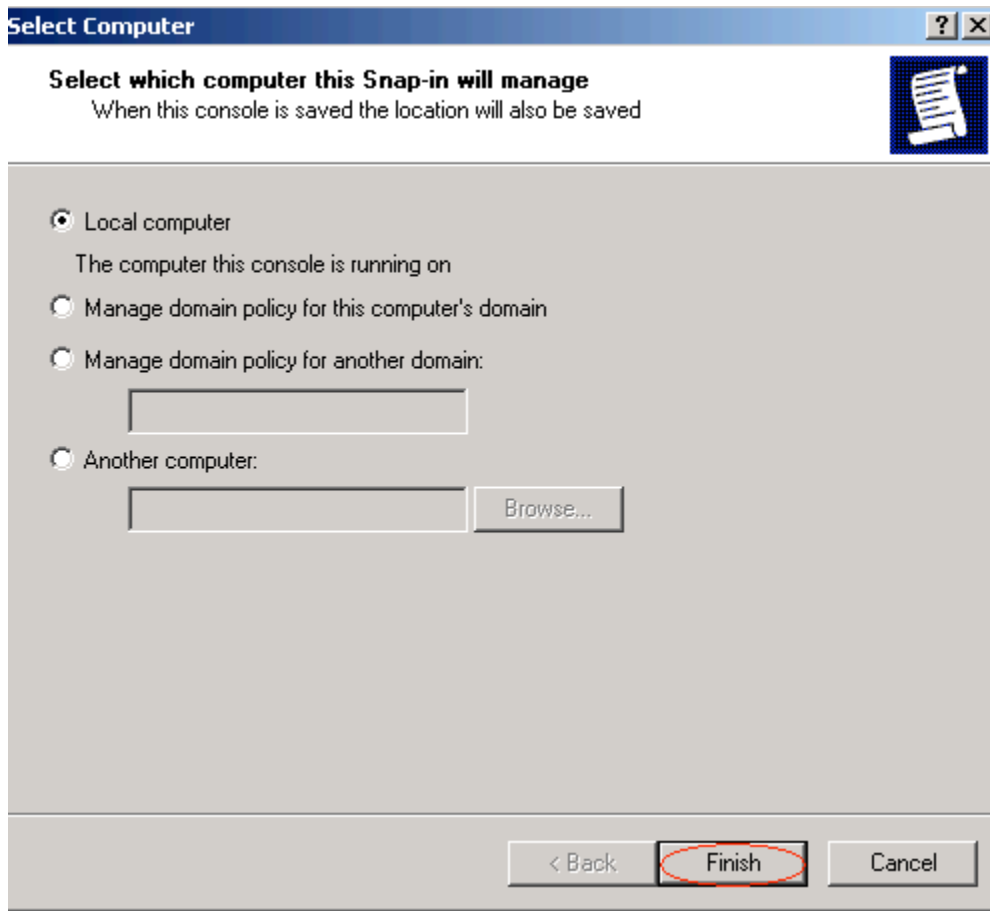
6. Click “**Add**”



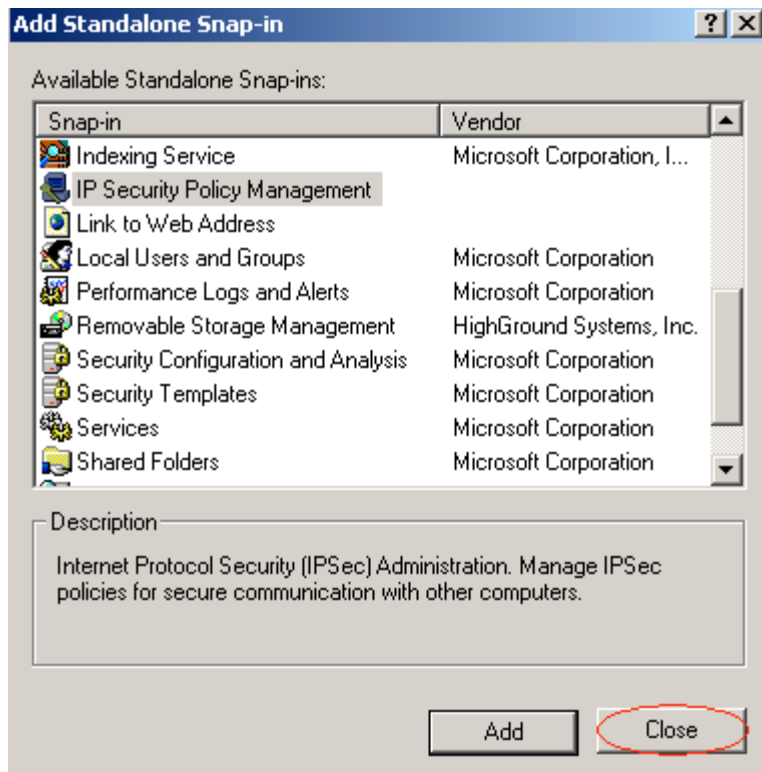
7. Select “IP Security Policy Management” the click “Add”



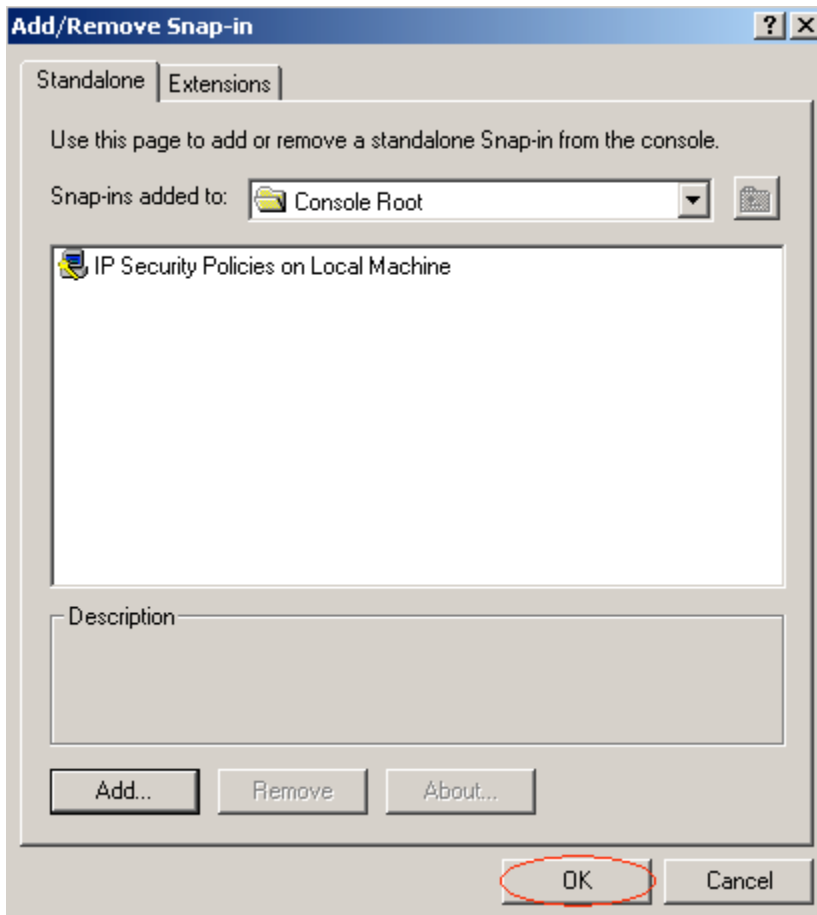
8. Click “Finish”



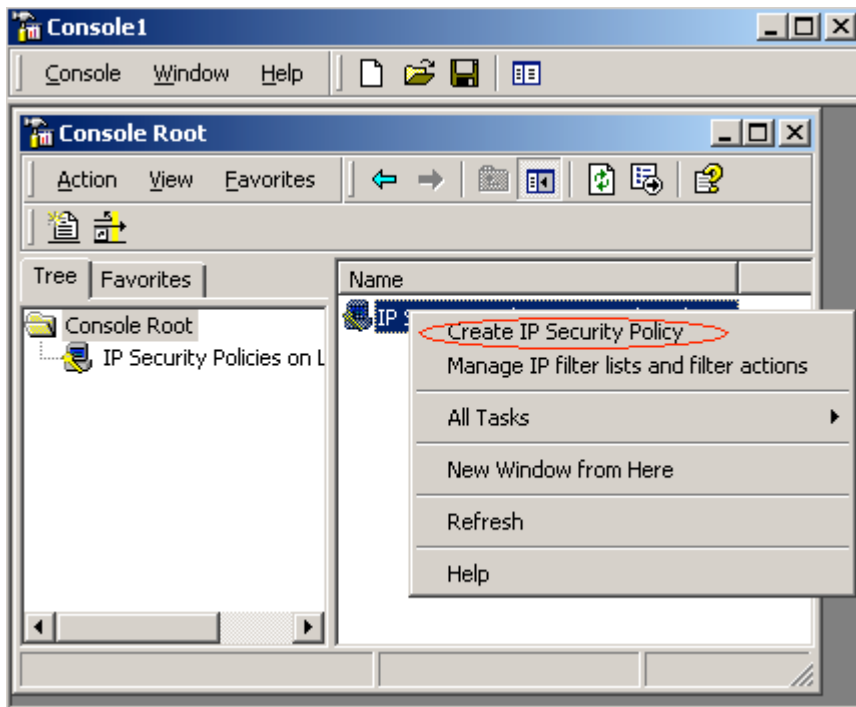
9. Click “Close”



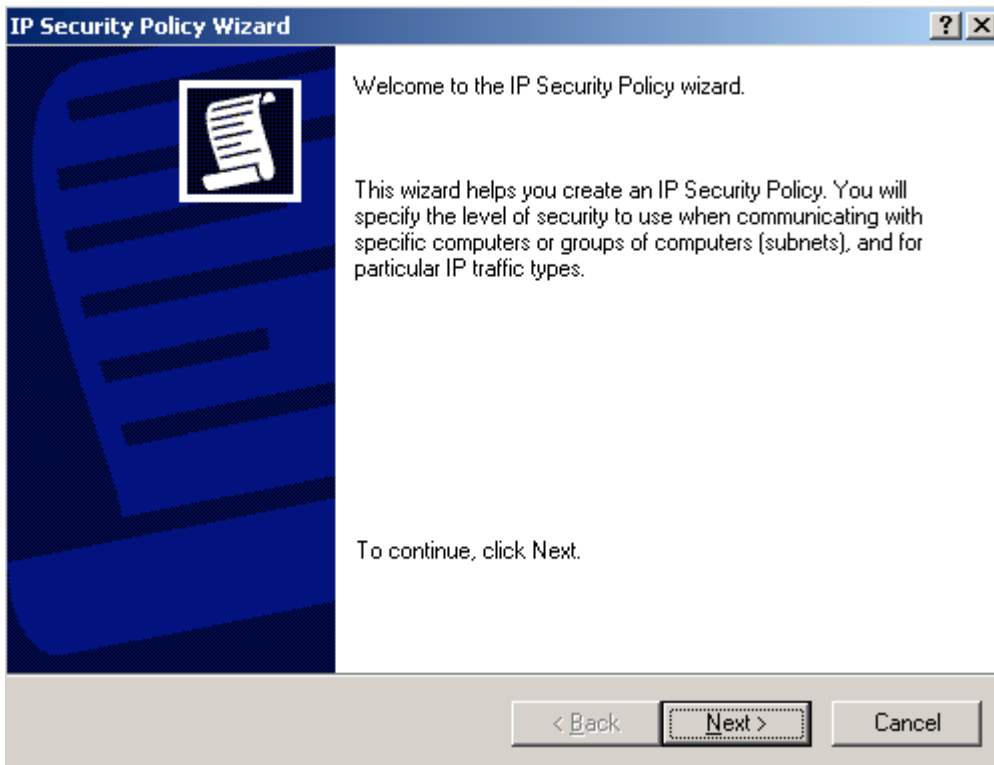
10. Click “OK”



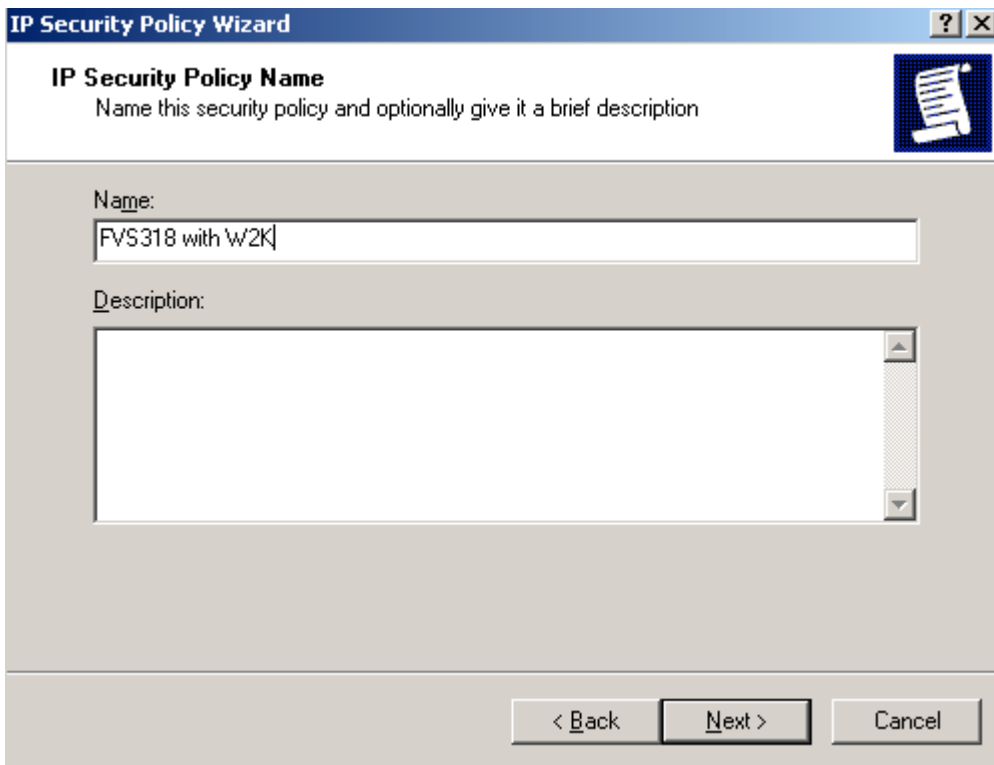
11. Click right button on **“IP Security Policies on Local Machine”** and select **“Create IP Security Policy”**



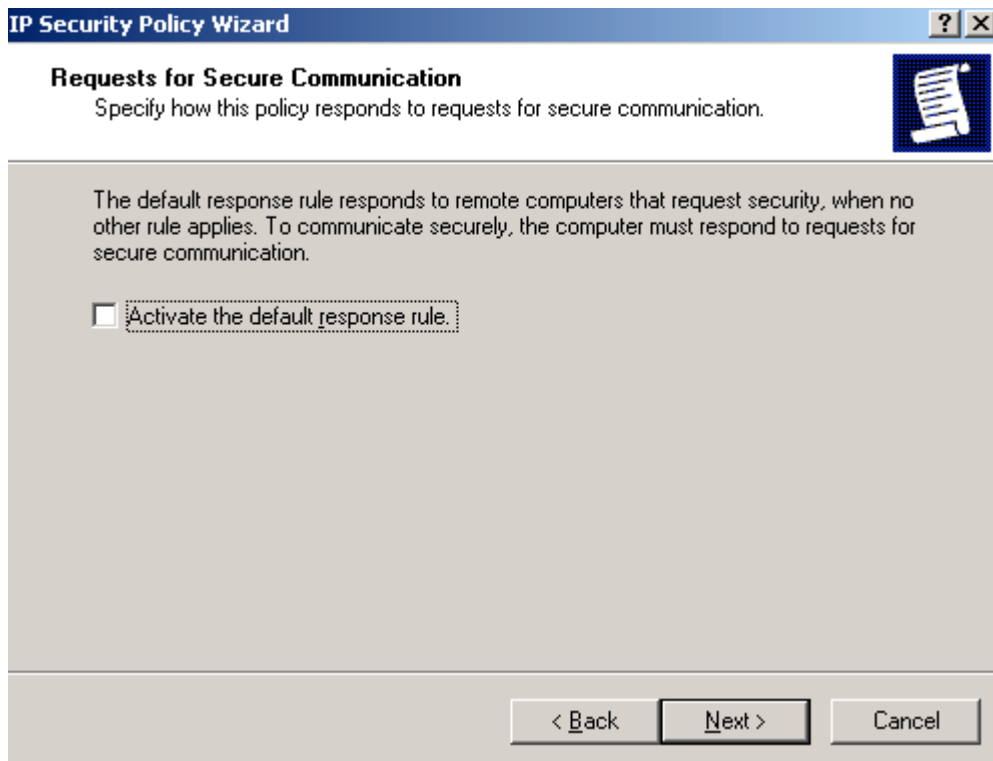
12. Click **“Next”**



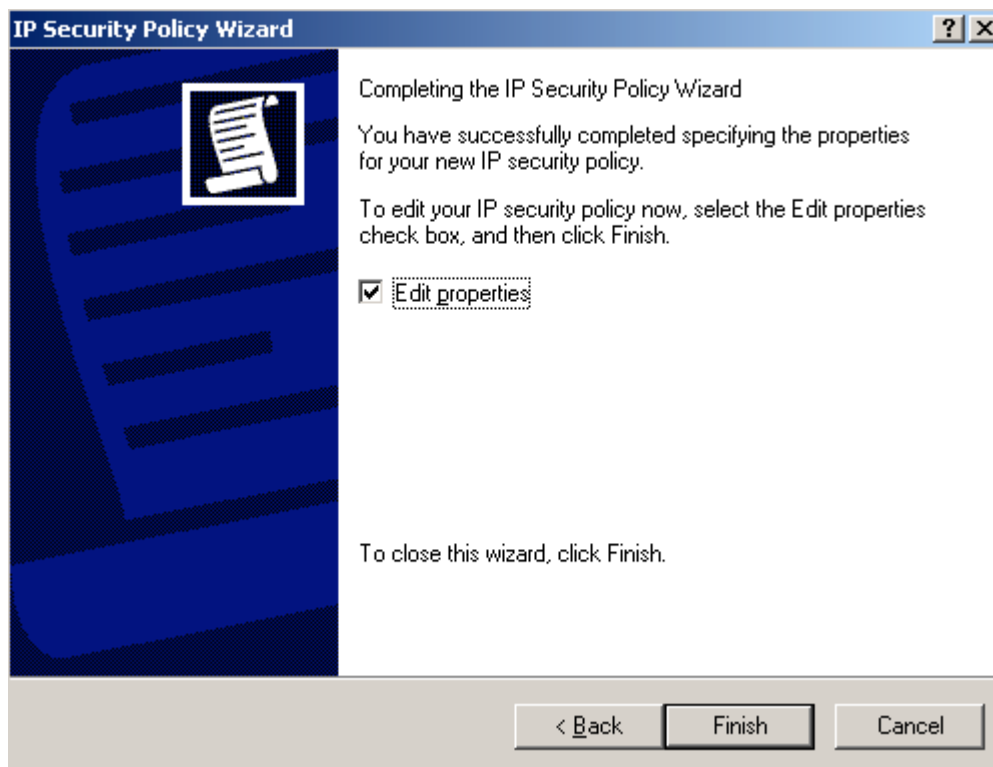
13. Type the IP Security Policy Name (ex: FVS318 with W2K) then click “Next”



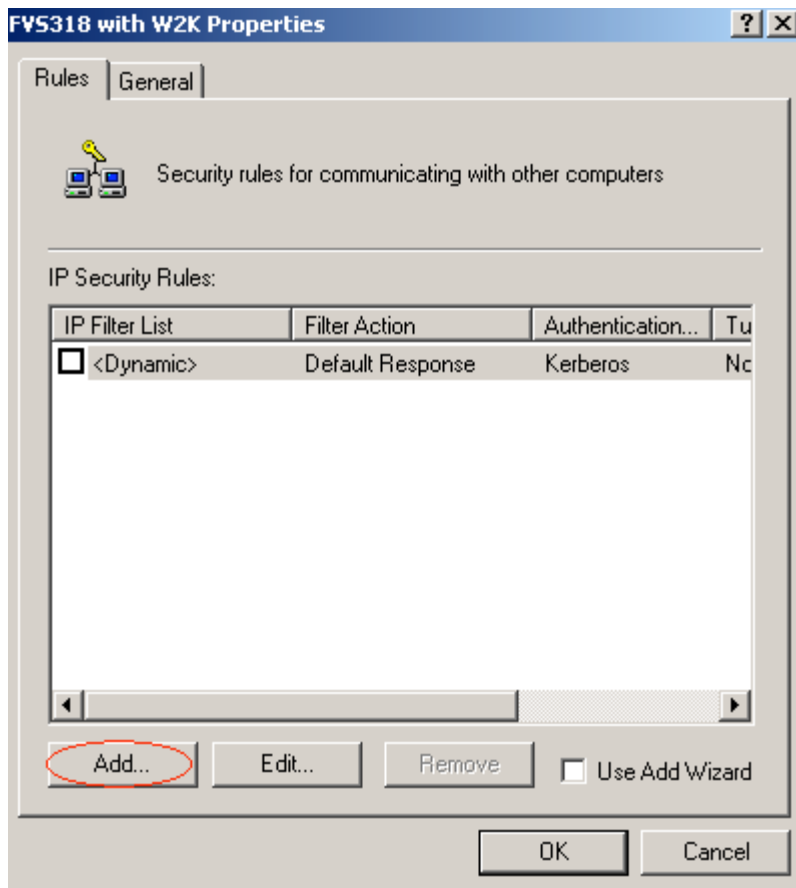
14. Uncheck “Activate the default response rule” and click “Next”



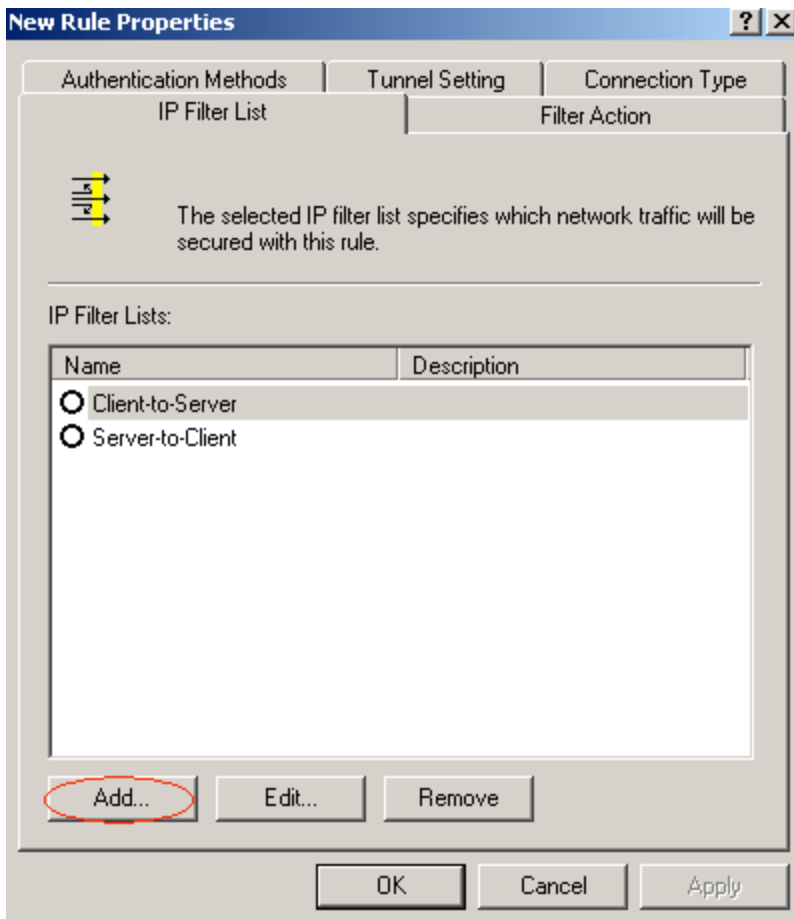
15. Click "Finish"



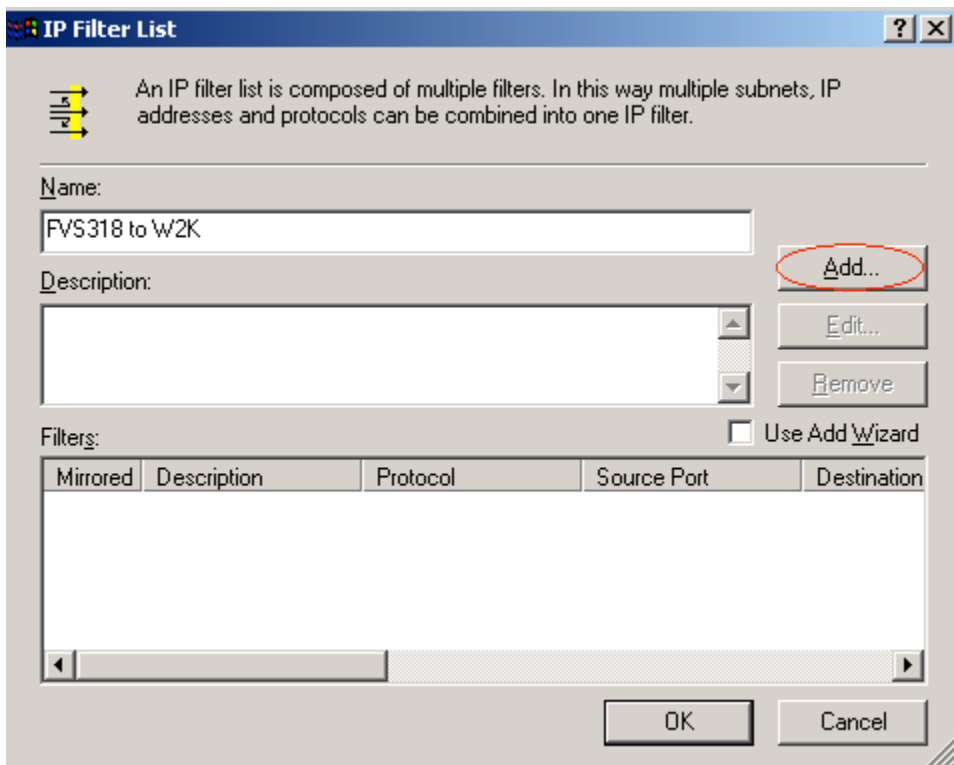
16. Click "Add" and uncheck "Use Add Wizard"



17. Click “Add”



18. Type the “IP Filter Name” (ex: FVS318 to W2K), uncheck “Use Add Wizard” and then click “Add”



19. Input the settings then uncheck “Mirrored. Also...” and click “Apply”, “OK” “Close”

Filter Properties [?] [X]

Addressing | Protocol | Description

Source address: [A specific IP Subnet ▼]

IP Address: 192 . 168 . 0 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address: [A specific IP Address ▼]

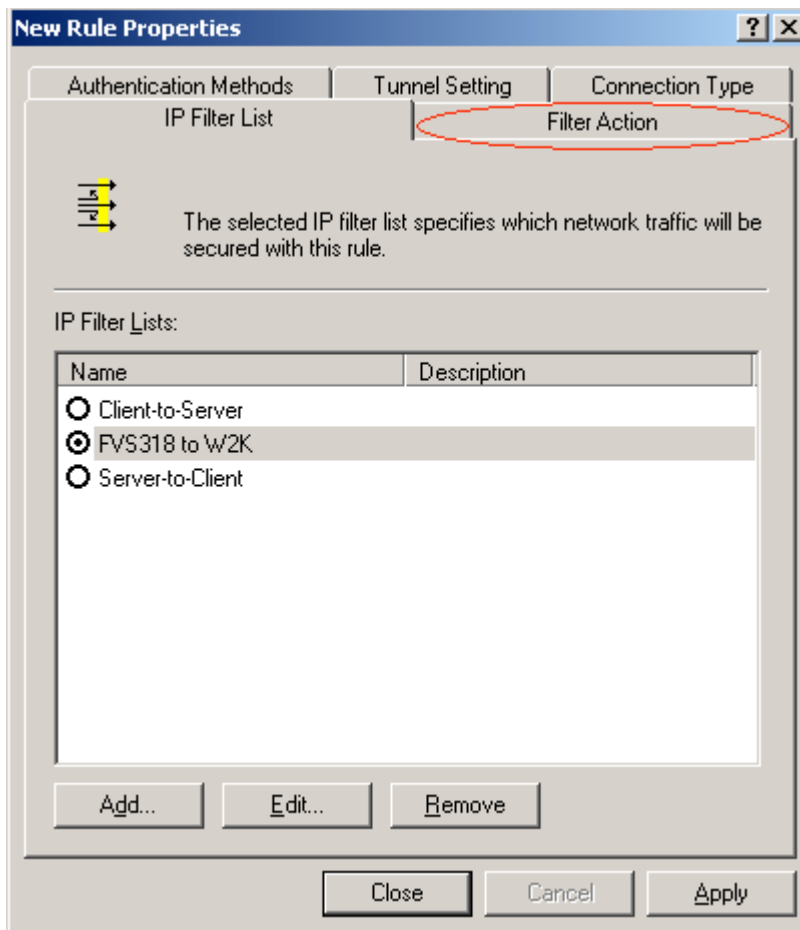
IP Address: 192 . 168 . 10 . 2

Subnet mask: 255 . 255 . 255 . 255

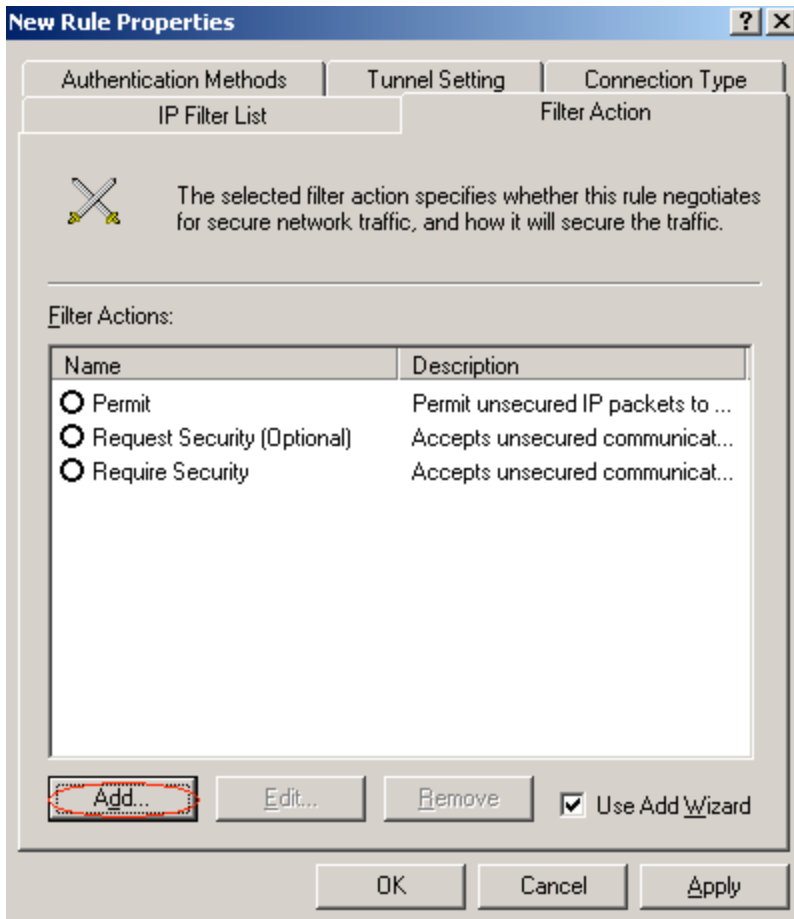
Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel **Apply**

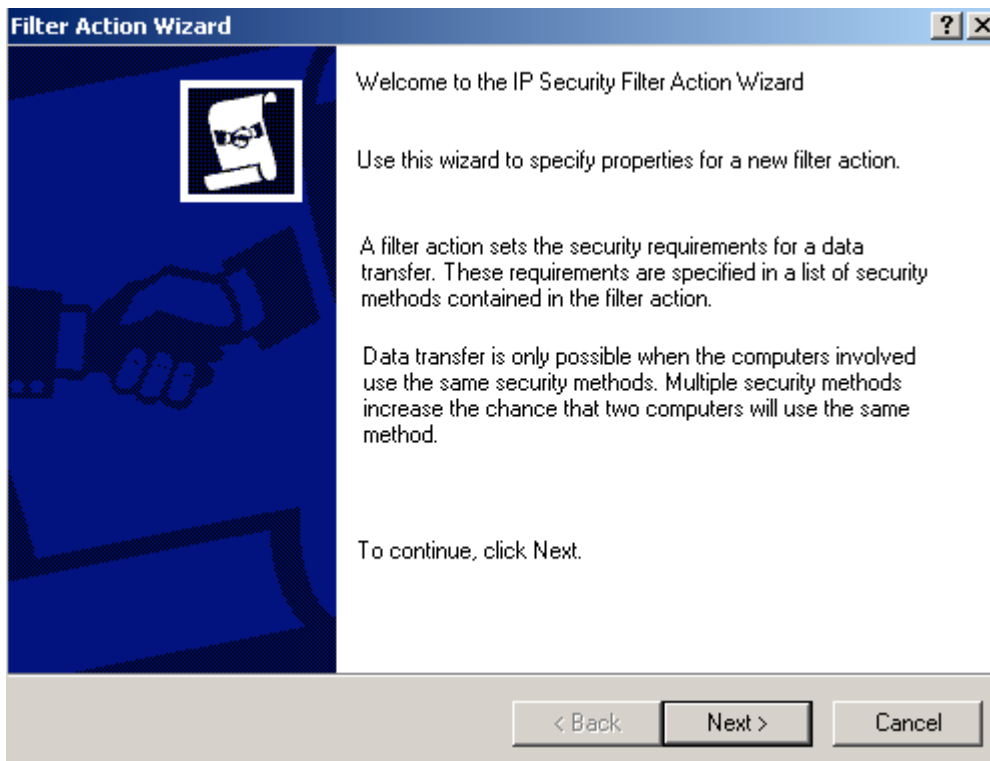
19. Select “IP Filter List” (ex: FVS318 to W2K) then click “Filter Action”



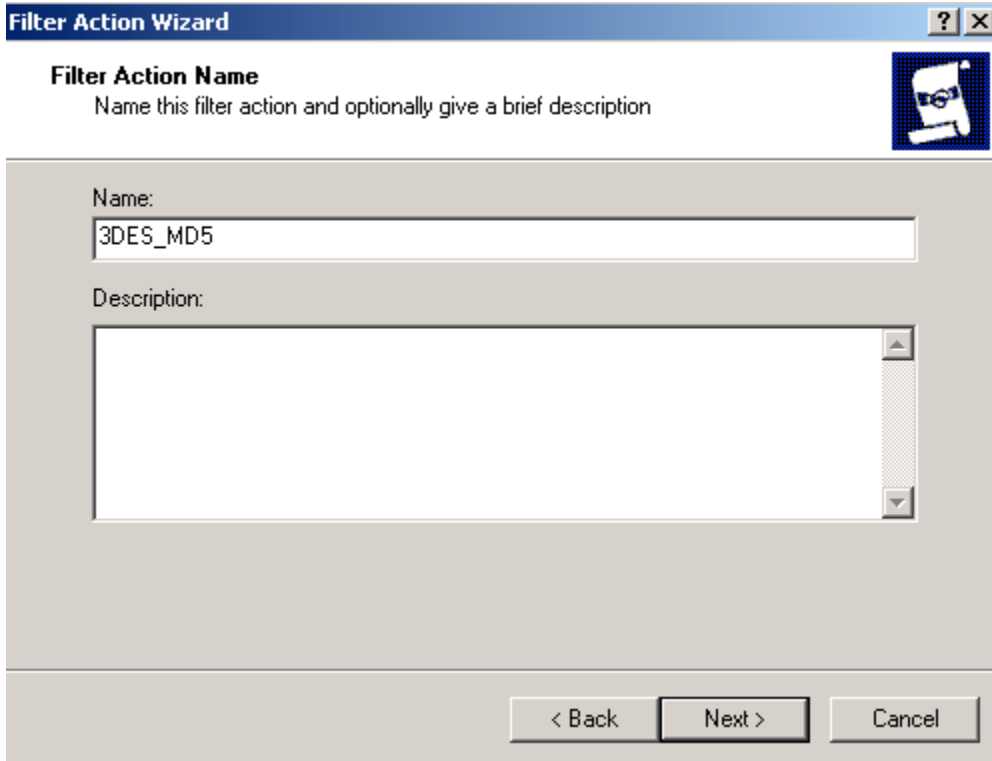
20. Check “User Add Wizard” and click “Add”



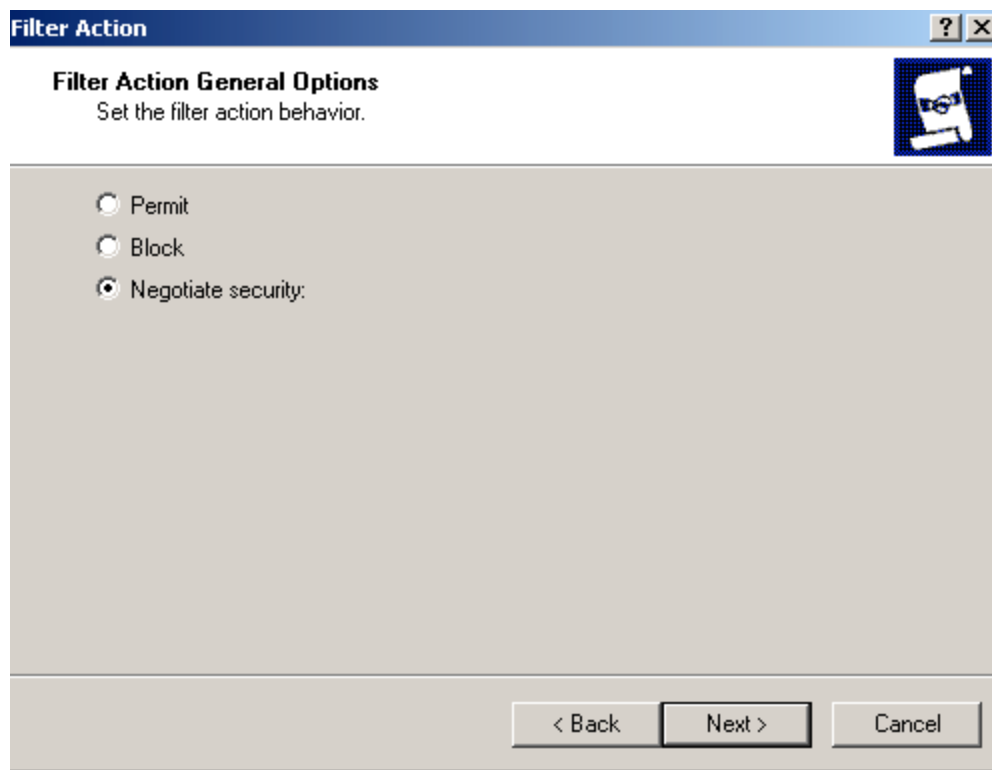
21. Click “Next”



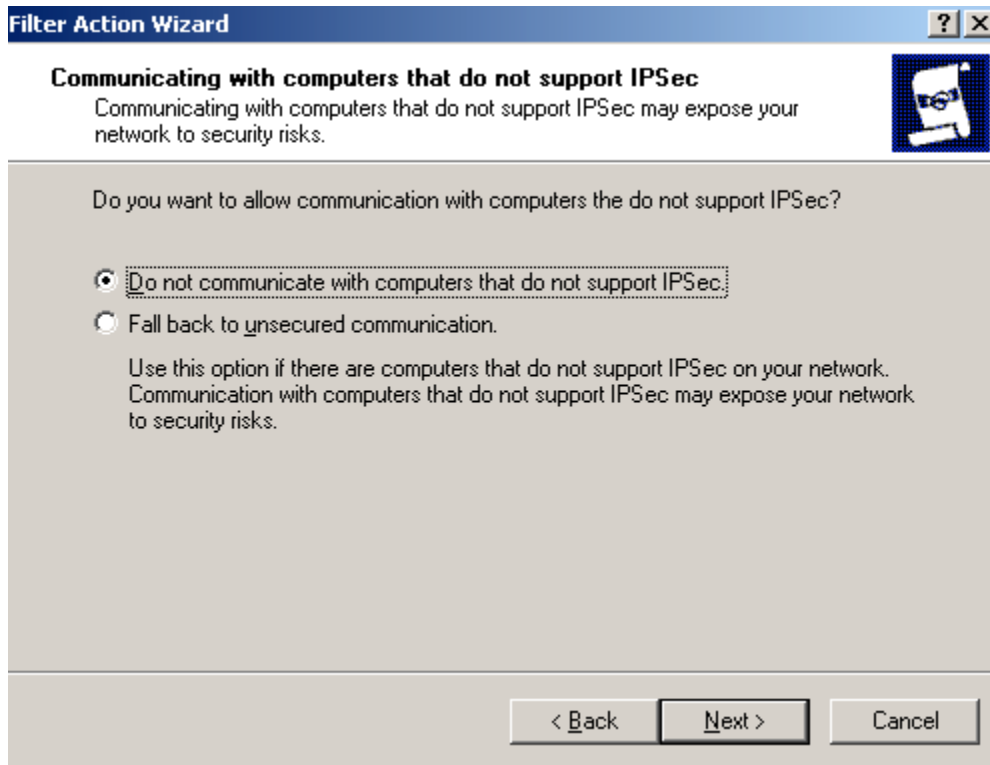
22. Type “**Filter Action Name**” (ex: 3DES_MD5)



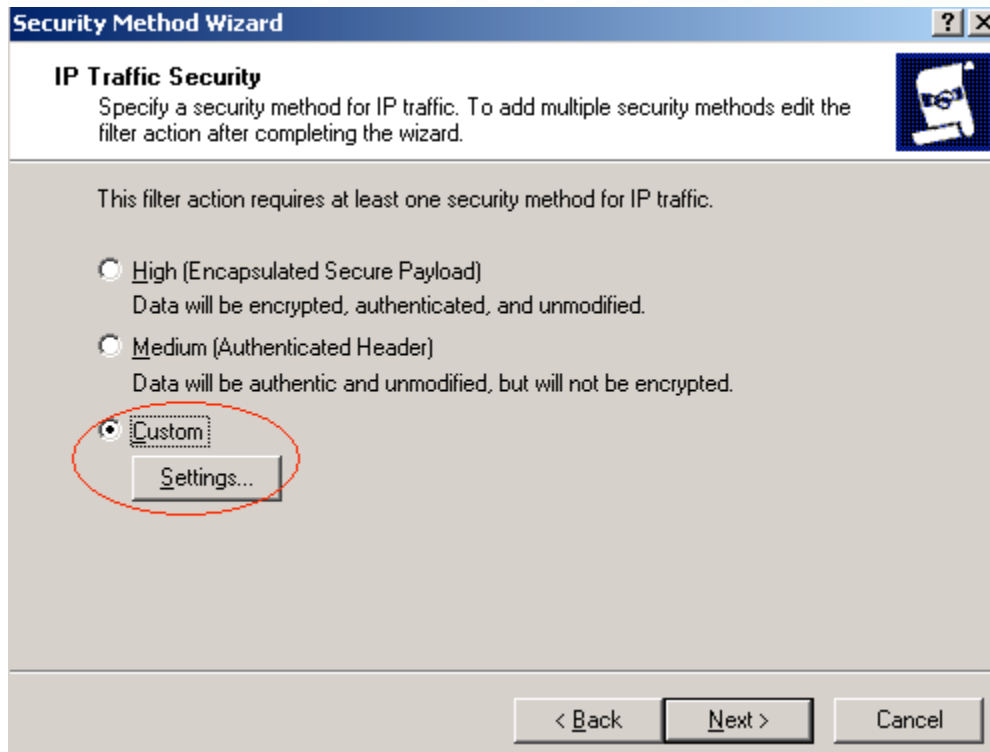
23. Click “Next”



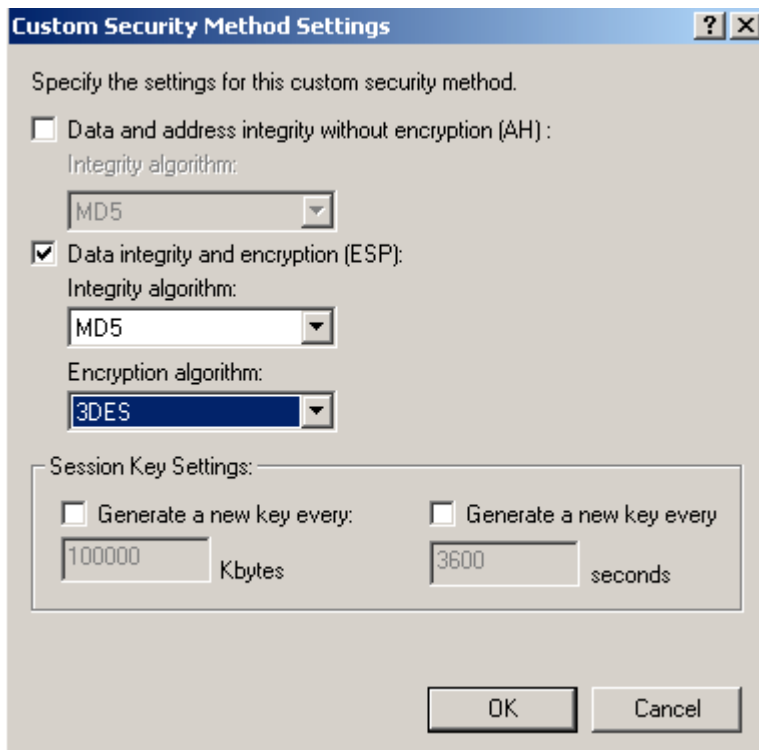
24. Click “Next”



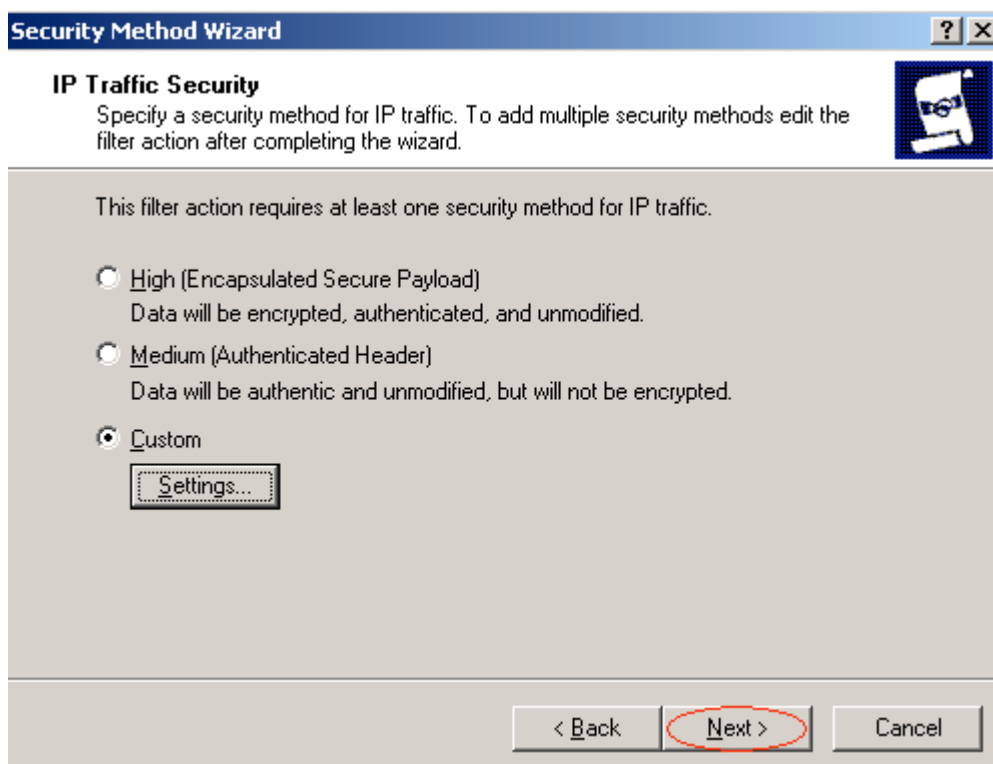
25. Select the “Custom Settings” then click “Next”



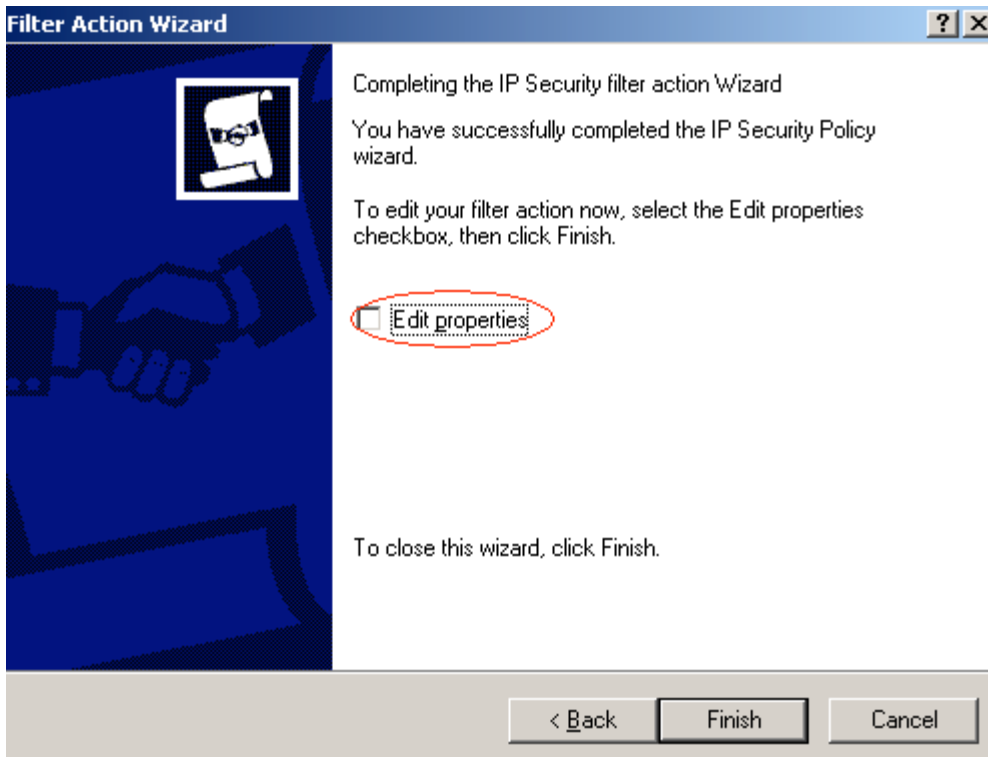
26. Select “MD5 & 3DES” then click “OK”



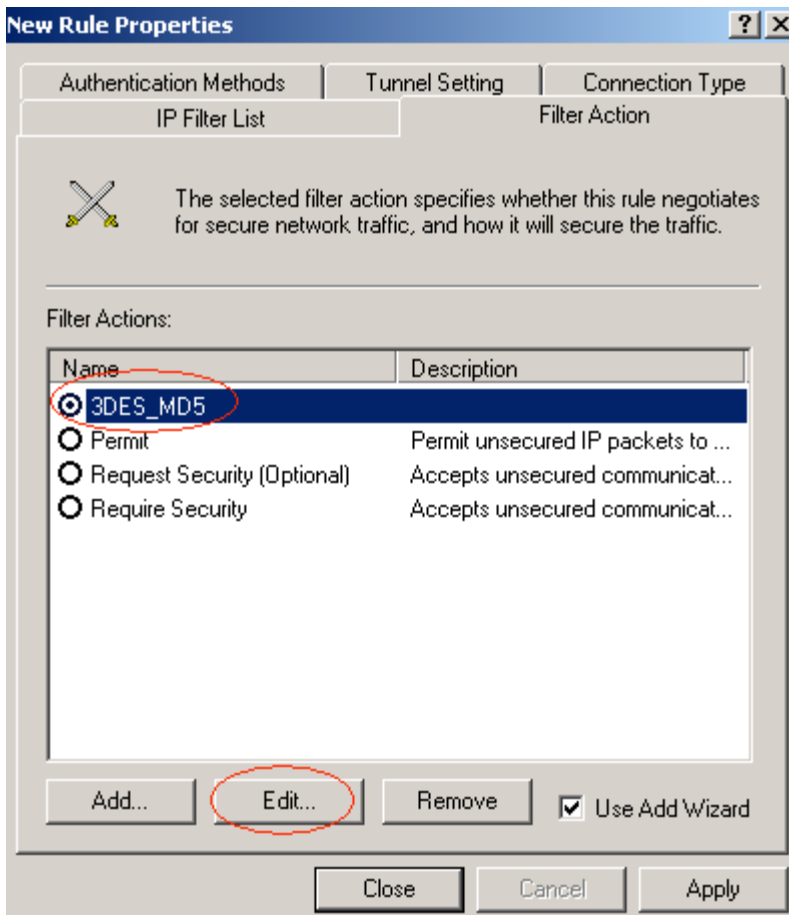
27. Click “Next”



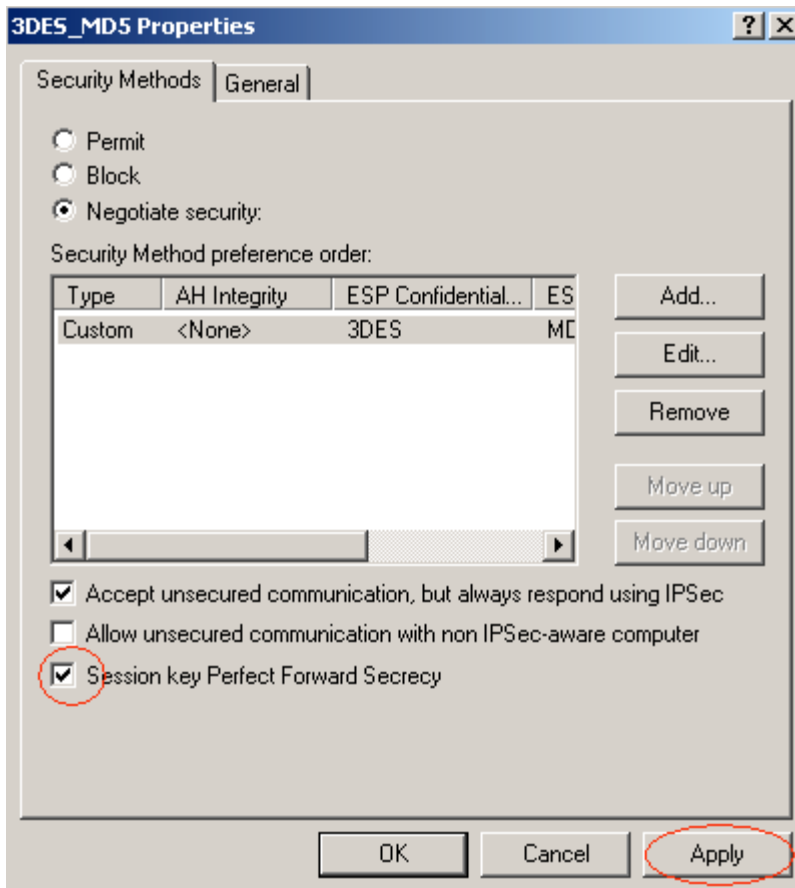
28. Click “Finish” (uncheck Edit properties)



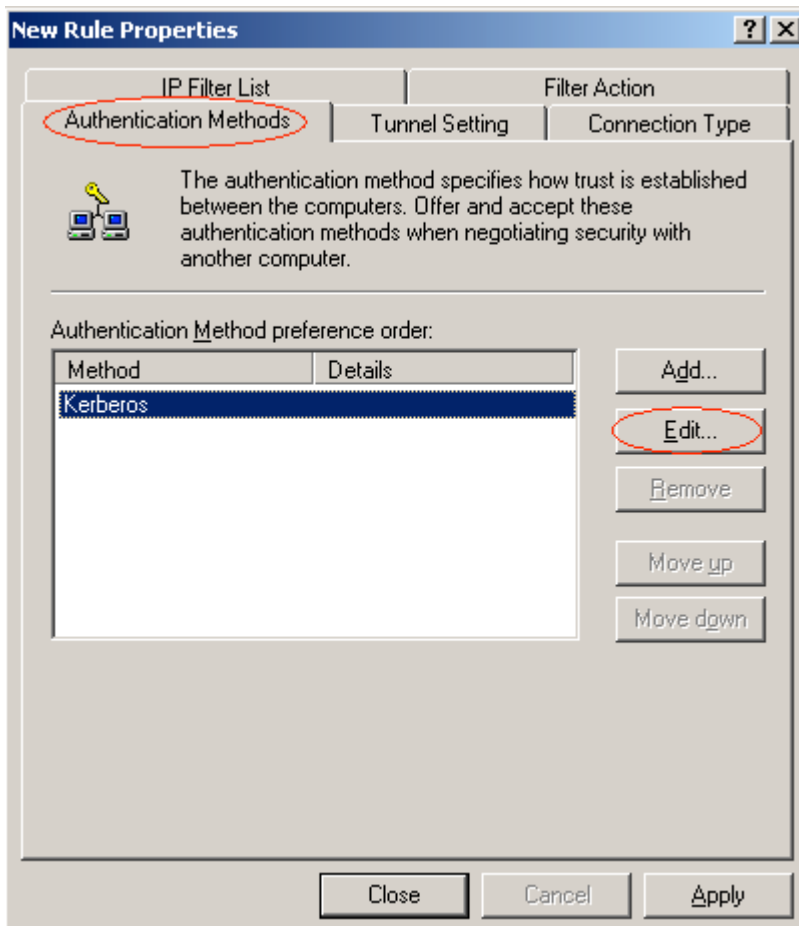
29. Select “3DES_MD5” then click “Edit”



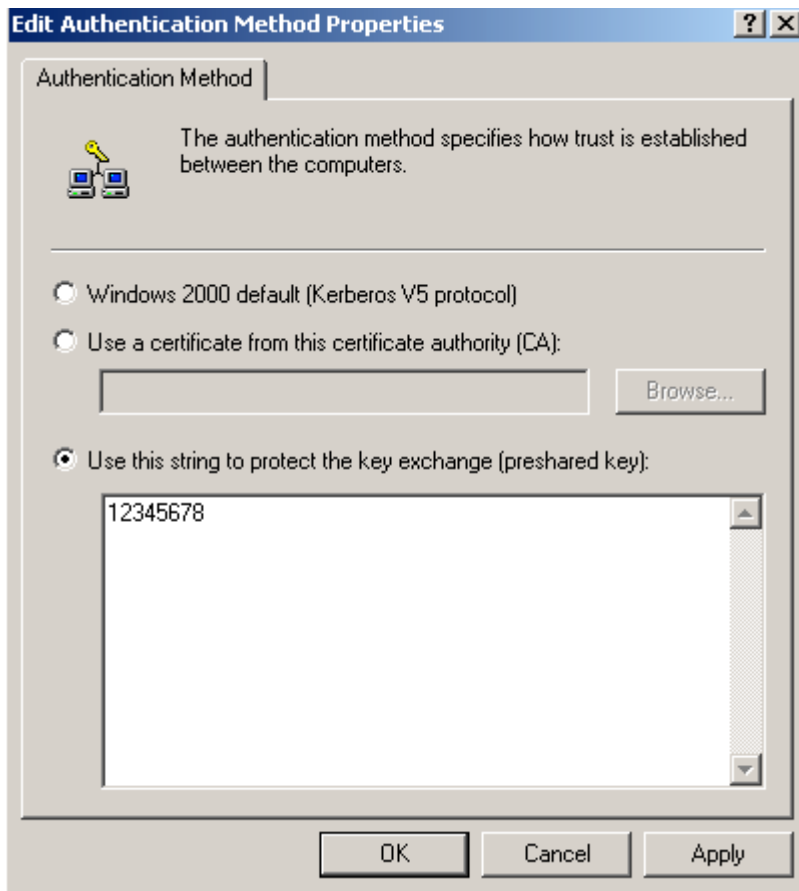
30. Check on “Session key Perfect Forward Secrecy” and click “Apply” then click “OK”



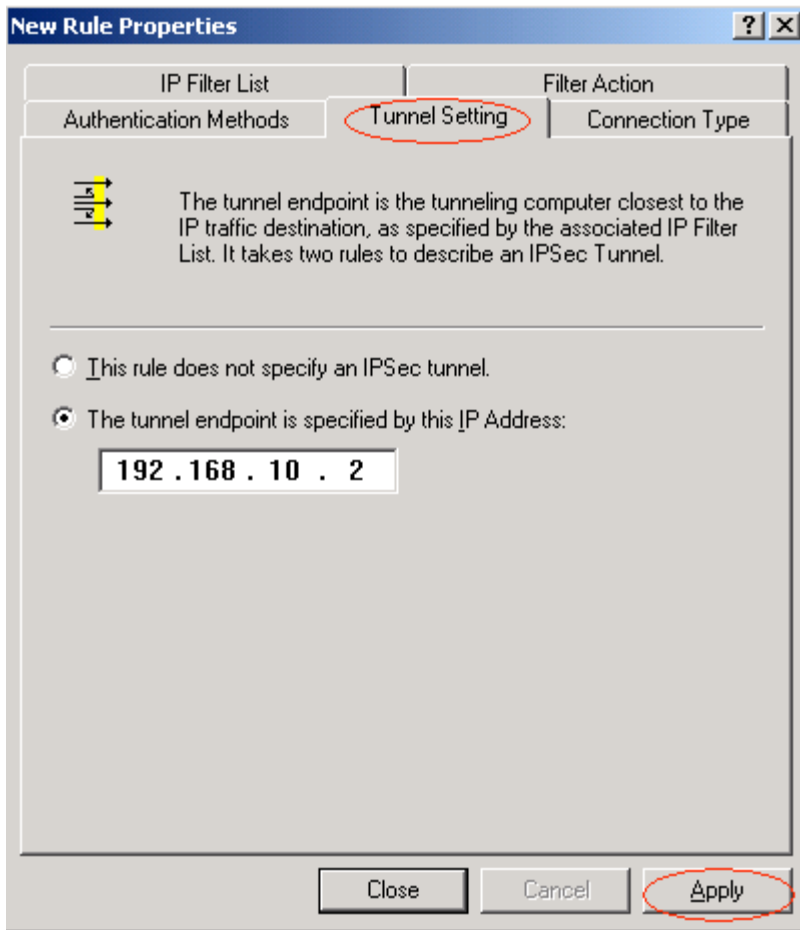
31. Select “**Authentication Methods**” then click “**Edit**”



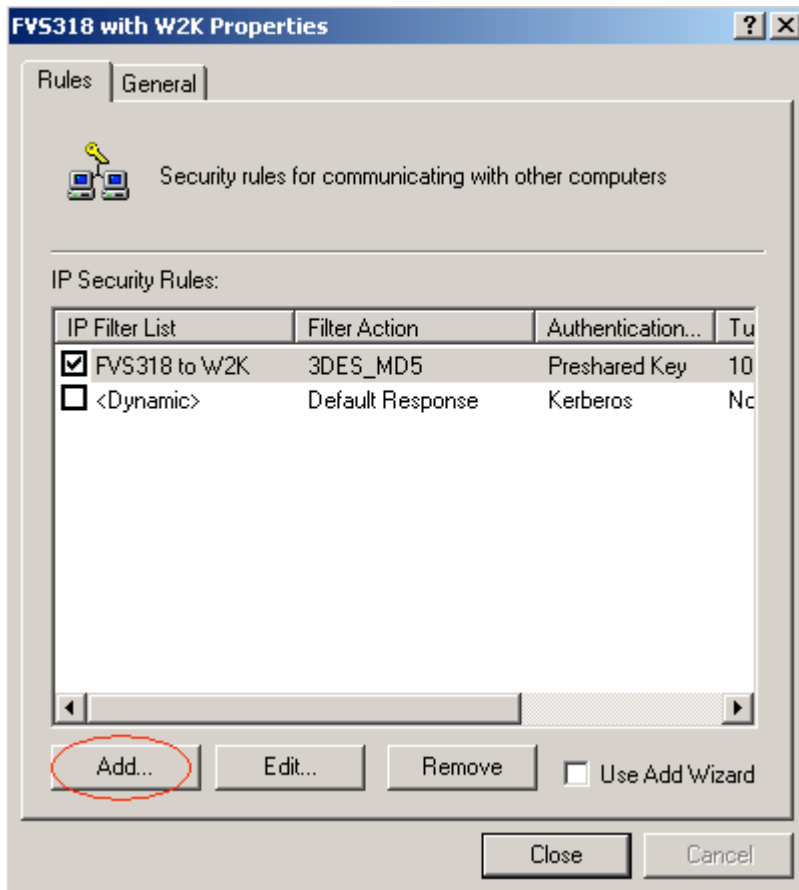
32. Select “Use this string ...(preshared key)” then input the key (ex: 12345678), and click “Apply” and “OK”



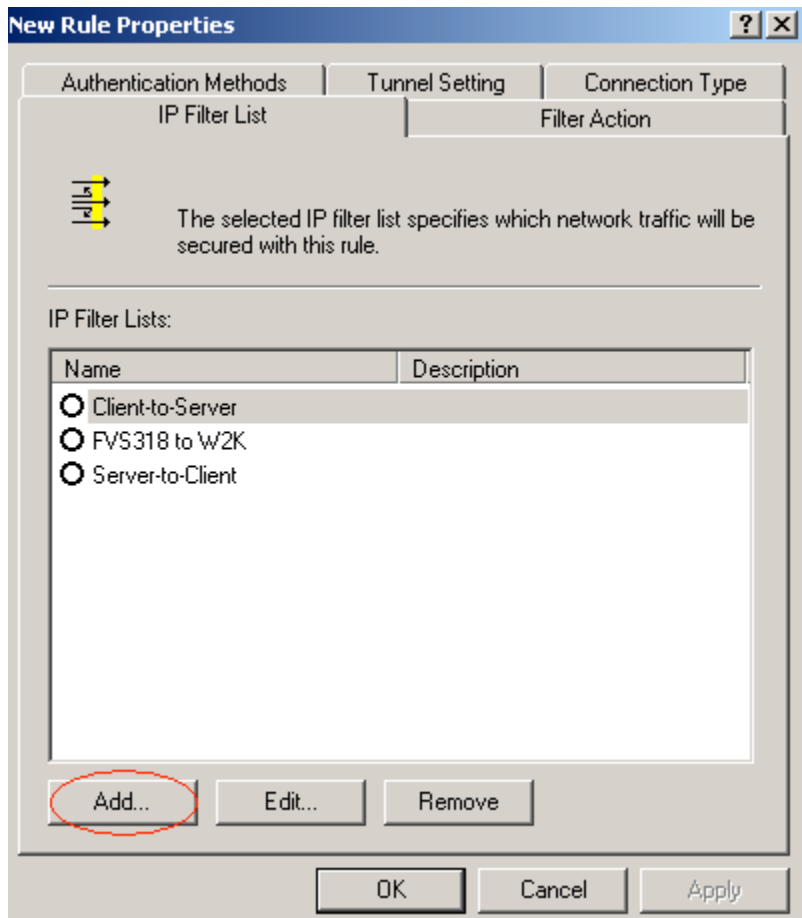
33. Select “**Tunnel Setting**” and input “**The tunnel endpoint specified by this IP Address**” (ex: 10.10.10.1) then click “**OK**”



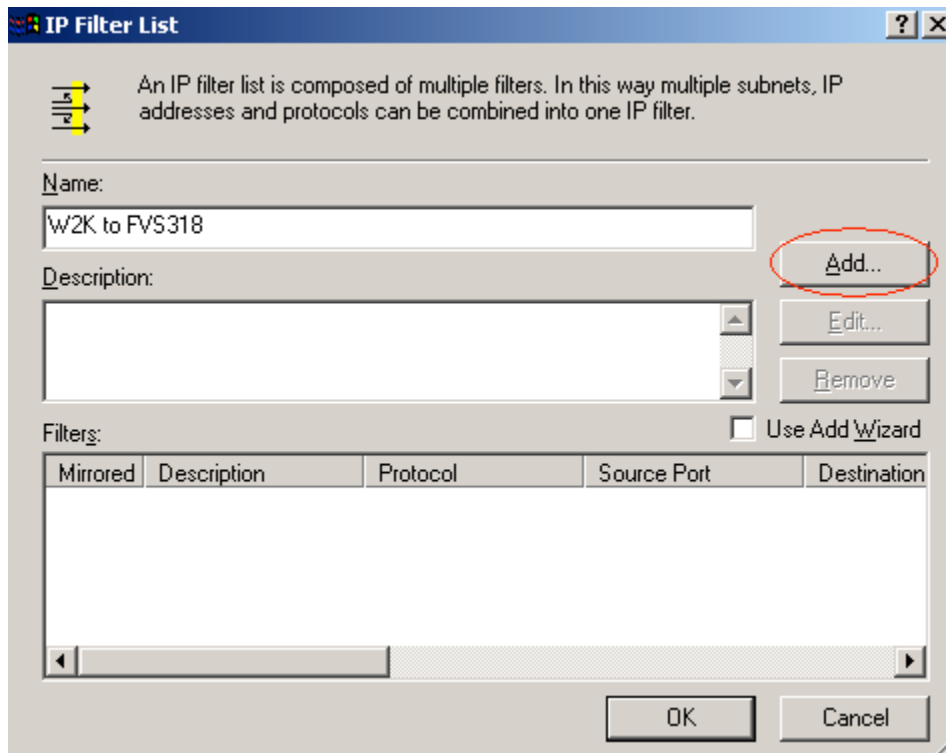
34. Click “**Add**” (uncheck “Use Add Wizard”)



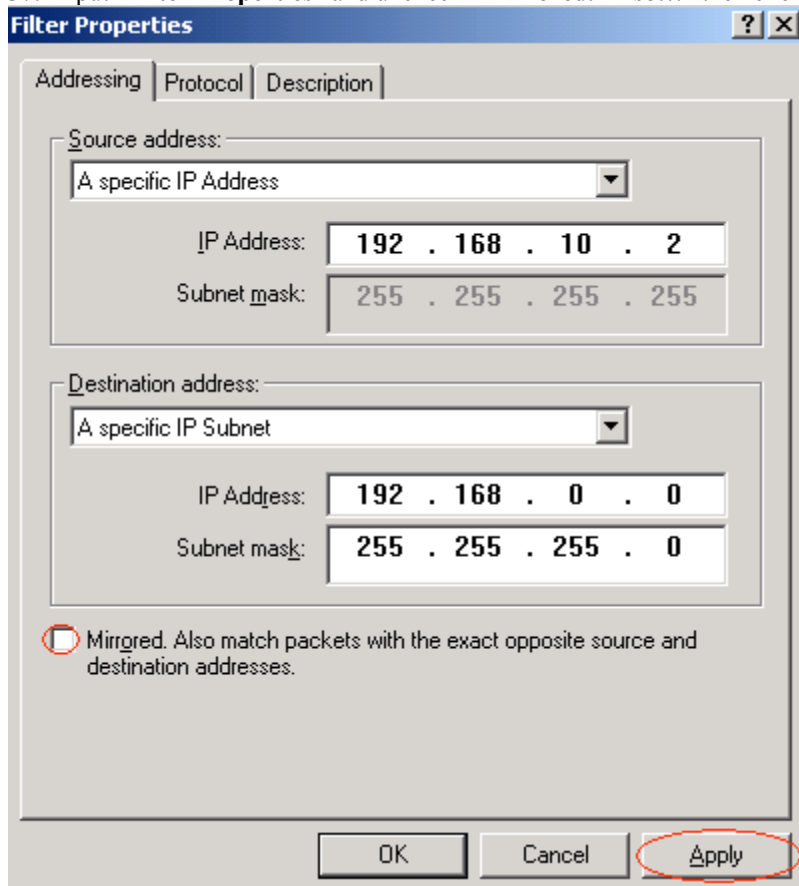
35. Click "Add"



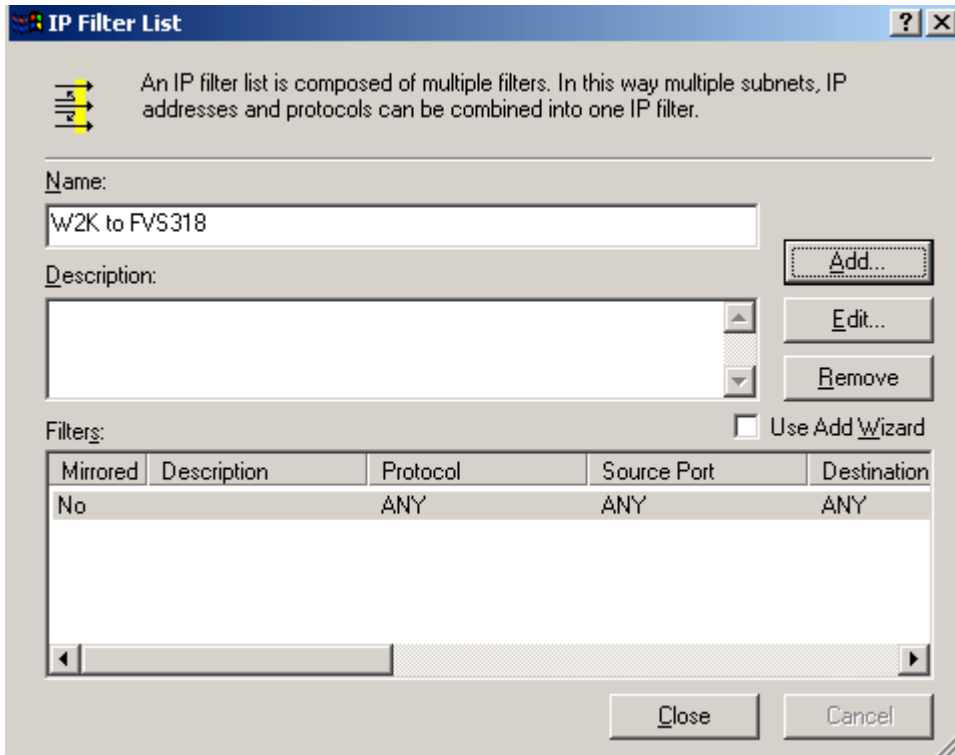
36. Input “IP Filter List Name” (ex: W2K to FVS318) and click “Add” (uncheck Use Add Wizard)



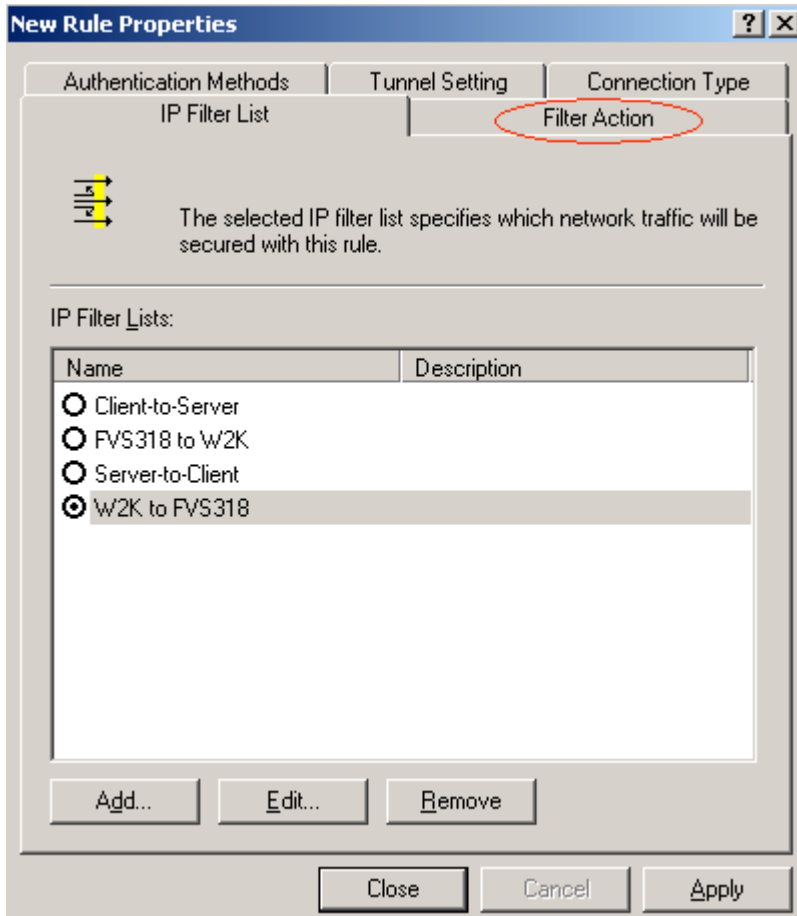
37. Input “Filter Properties” and uncheck “Mirrored. Also...” then click “Apply” “OK”



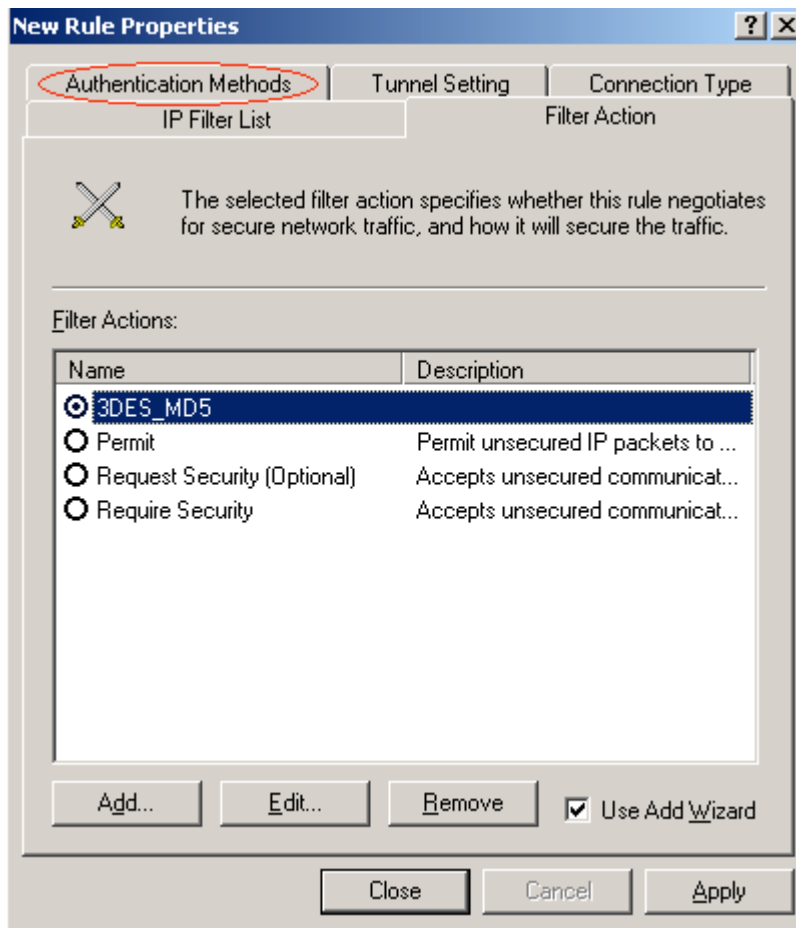
38. Click “Close”



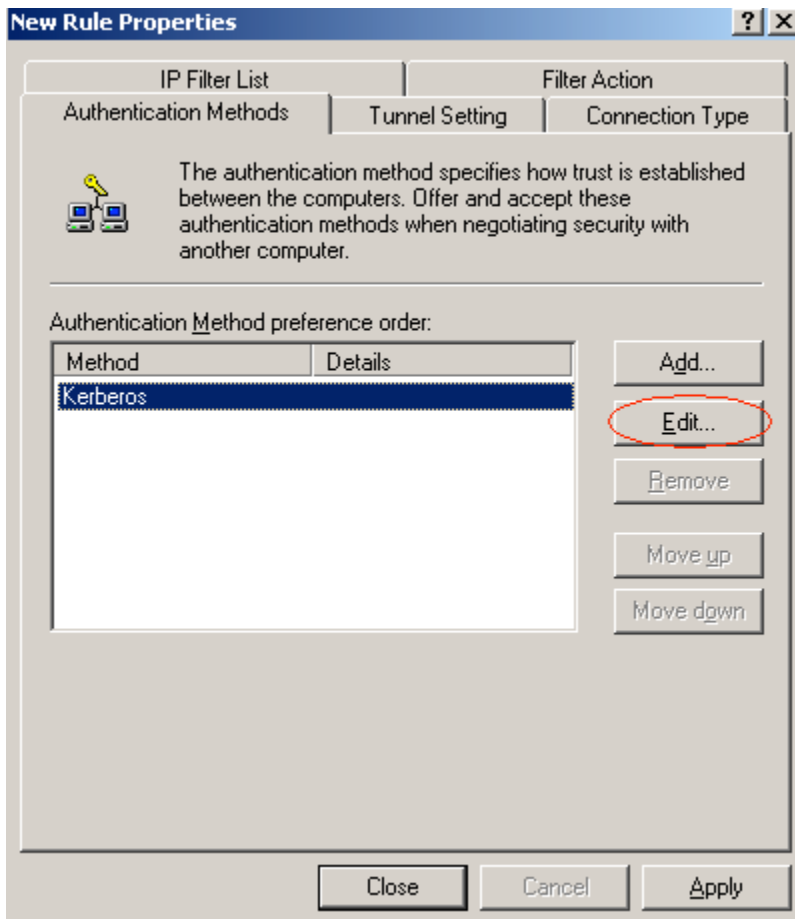
39. Select “W2K to FVS318” then click “Filter Action”



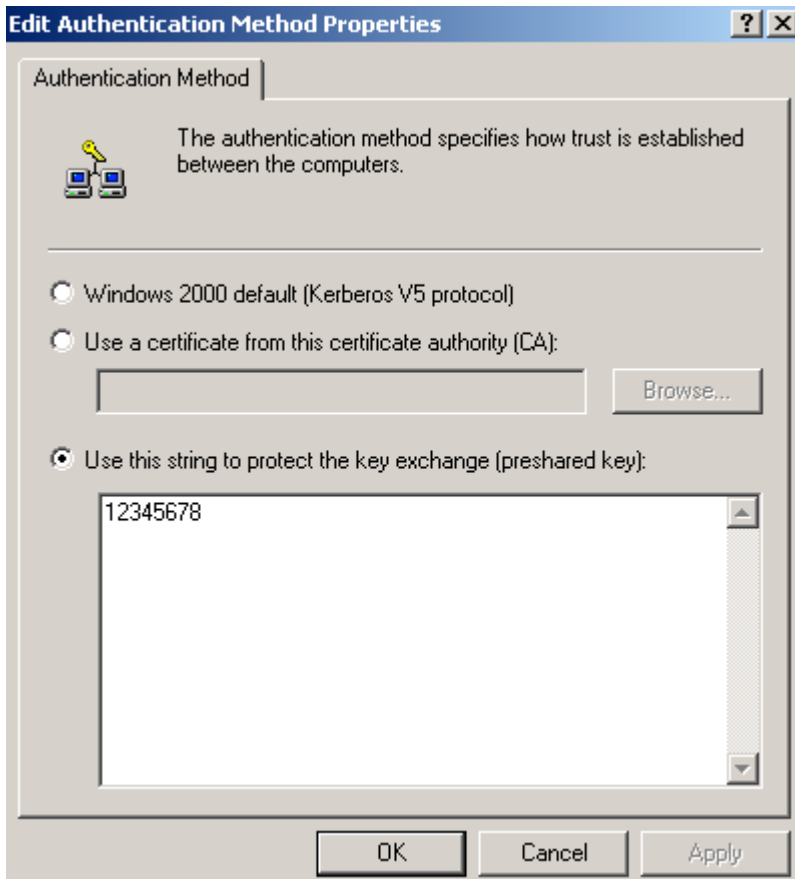
40. Select “3DES_MD5” then click “Authentication Methods”



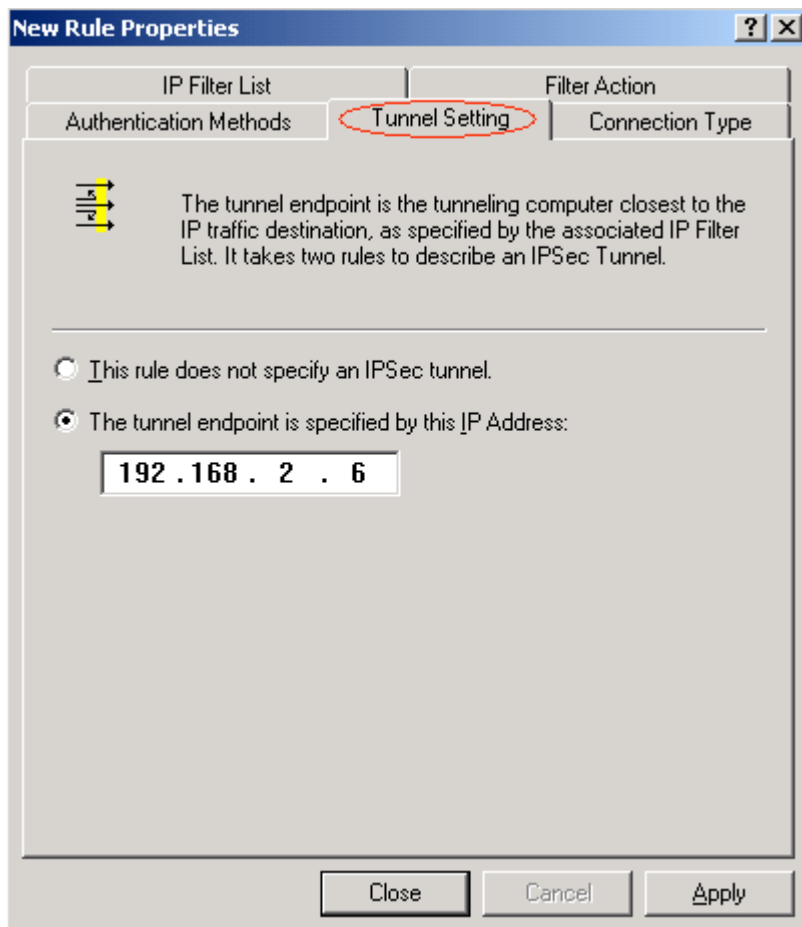
41. Click “**Edit**”



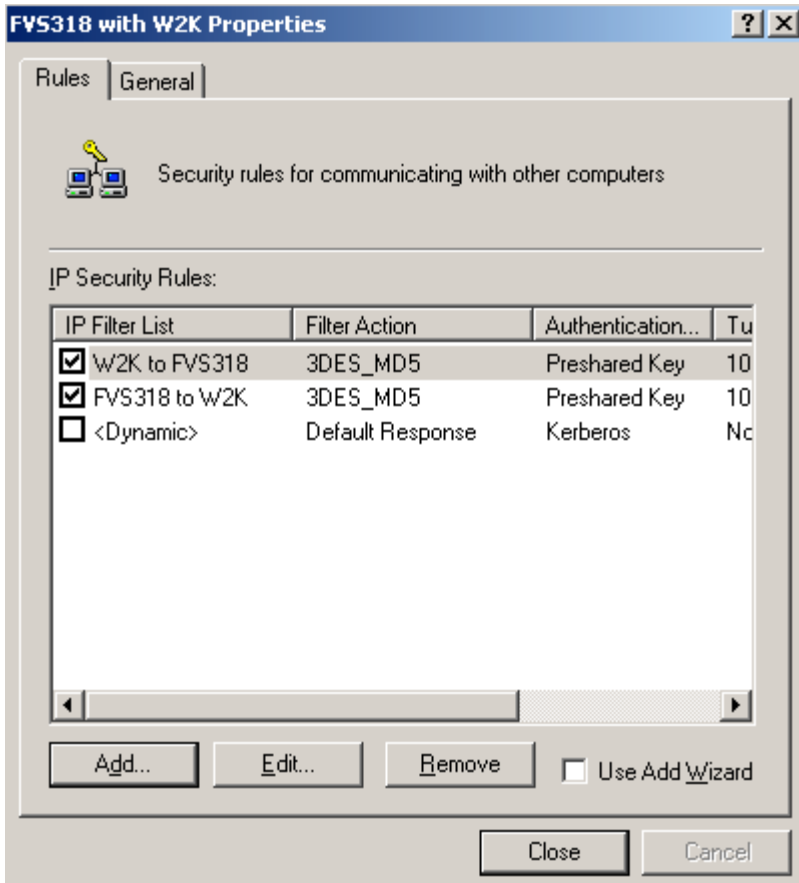
42. Select “Use this string ... (preshared key)” then input the key (ex: 12345678)



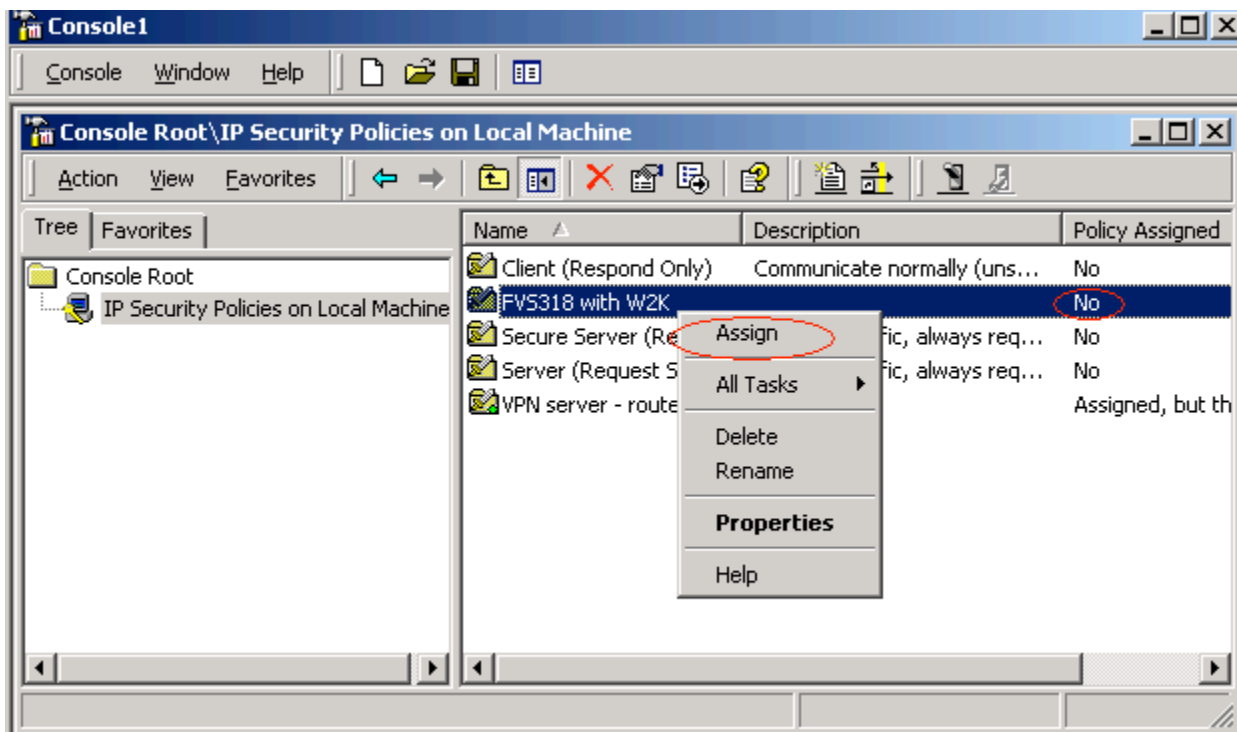
43. Select “**Tunnel Setting**” then input “**The tunnel ...**” (ex: 10.10.10.2) and click “**Apply**” and “**OK**”



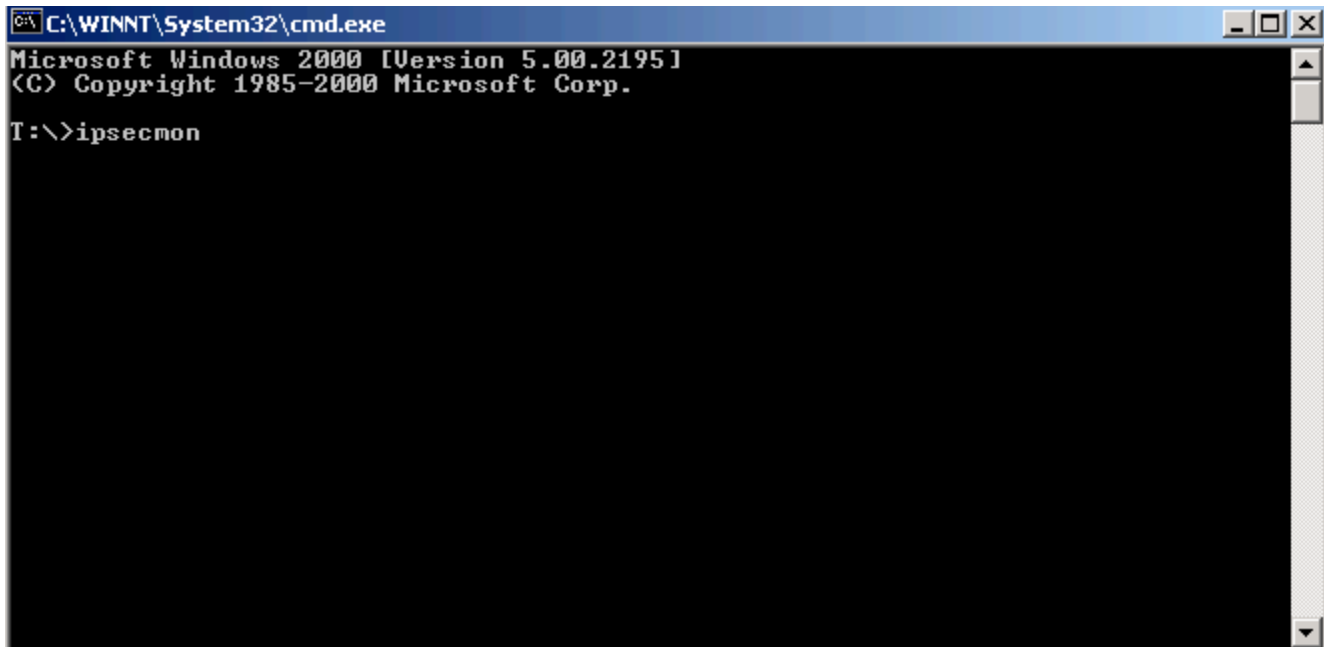
44. Click “Close”



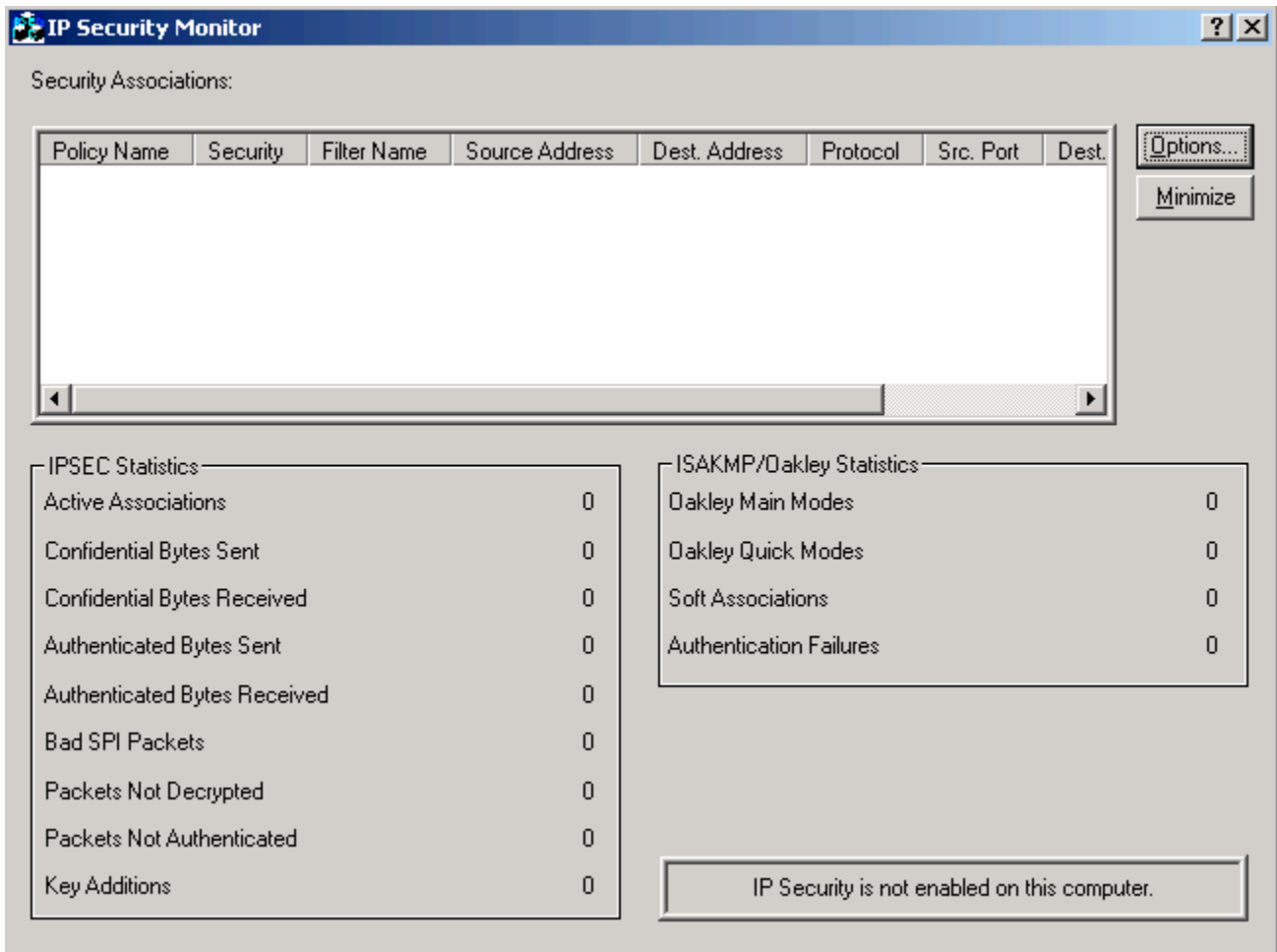
45. Select “IP Security Policy” and click right button on the policy name (ex: FVS318 with W2K) and click “Assign” (after assign, the No will change to Yes)



46. Type "ipsecmon" on DOS command mode



48. Check the IPsec tunnel status



FVS318 LAN/WAN and VPN Settings

FVS318 LAN: 192.168.0.1 subnet mask 255.255.255.0
WAN: 192.168.2.6 subnet mask 255.255.255.0 gateway: 192.168.2.1

FVS318 VPN Settings

- Connection Name: FVS318_W2K
- Local IPSec Identifier: 0.0.0.0
- Remote IPSec Identifier: 0.0.0.0
- Remote IP Network: 192.168.10.2
- Remote IP Subnet mask: 255.255.255.255
- Remote Gateway IP: 192.168.2.3
- Secure Association: IKE
- Perfect Forward Secure: Enabled
- PreShared Key: 12345678
- Key Life: 3600
- IKE Life Time: 28800

VPN client _W2K Settings

W2K is connected to a NAT router.

W2K: ip: 192.168.10.2
Netmask: 255.255.255.0
gateway: 192.168.10.1

NAT router:

LAN: 192.168.0.1/24
WAN 192.168.2.3
Gateway: 192.168.2.1