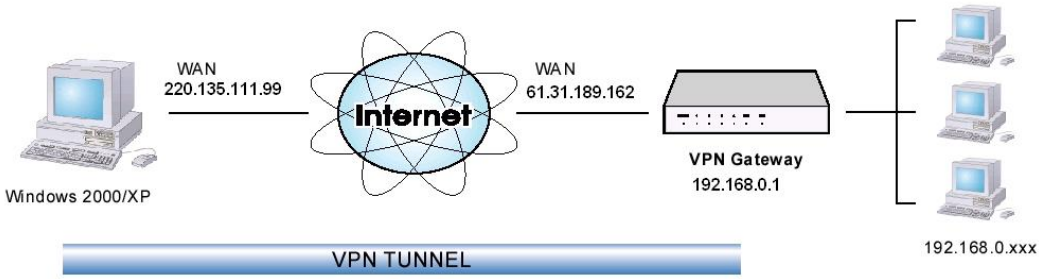
WBR-3460 IPSec VPN vs. Win XP IPSec VPN

Windows 2000/XP client with public IP connects to WBR-3460 Broadband VPN Gateway and gains access to the local LAN.

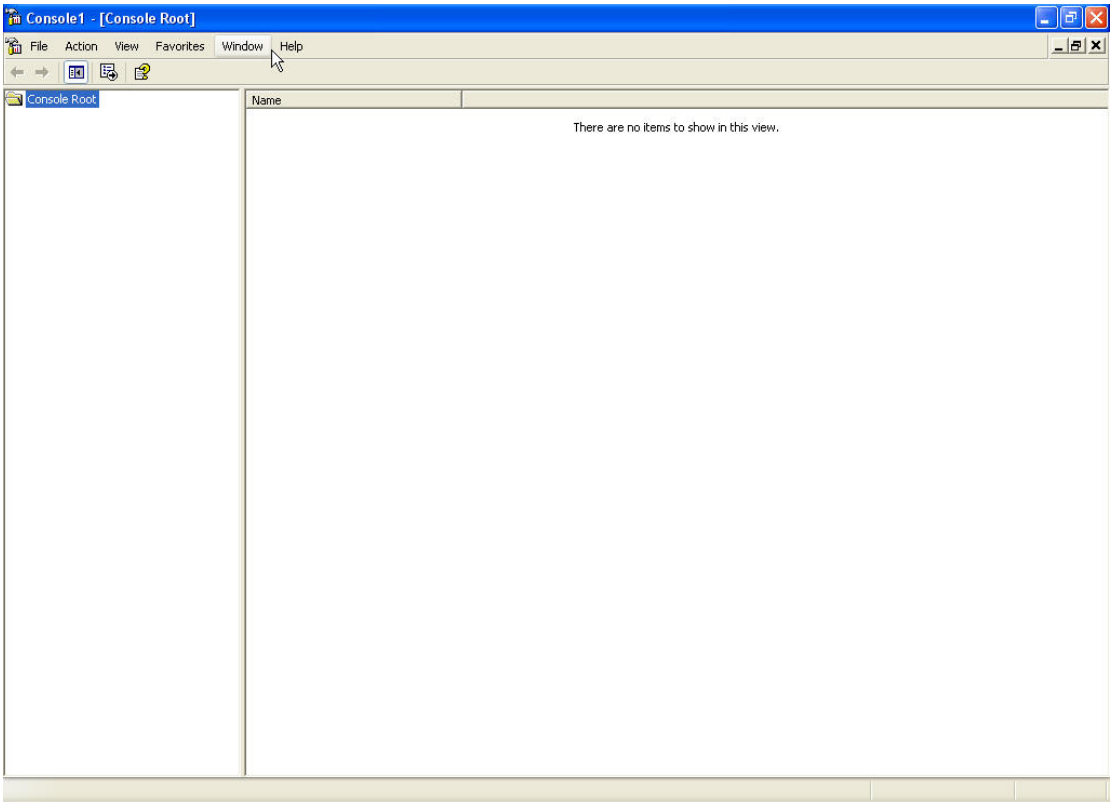


Windows 2000/XP Client to Broadband VPN Gateway

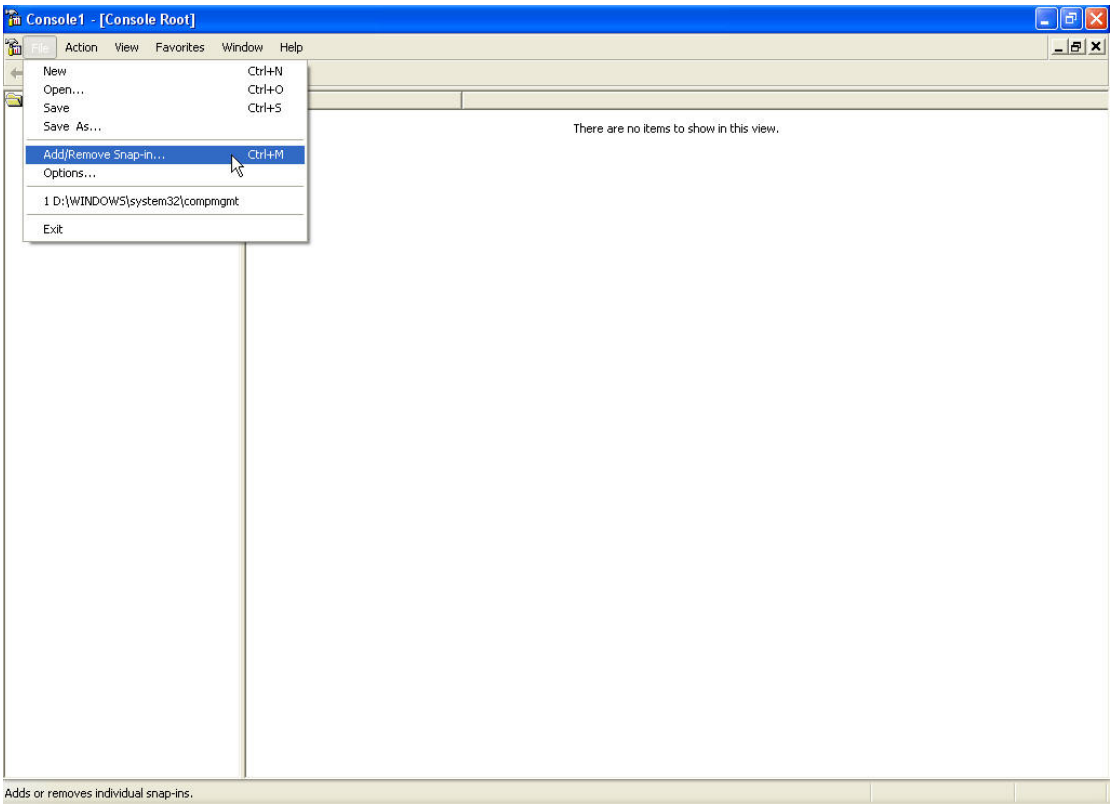
Windows 2000/XP IPSec client configuration can be a little bit confusing for the first time. Basically you will need to create an IP Sec security policy in Windows and set both “way to the router” and “back from the router”. Below is a step by step guidance.

1. Start → Run → <mmc>

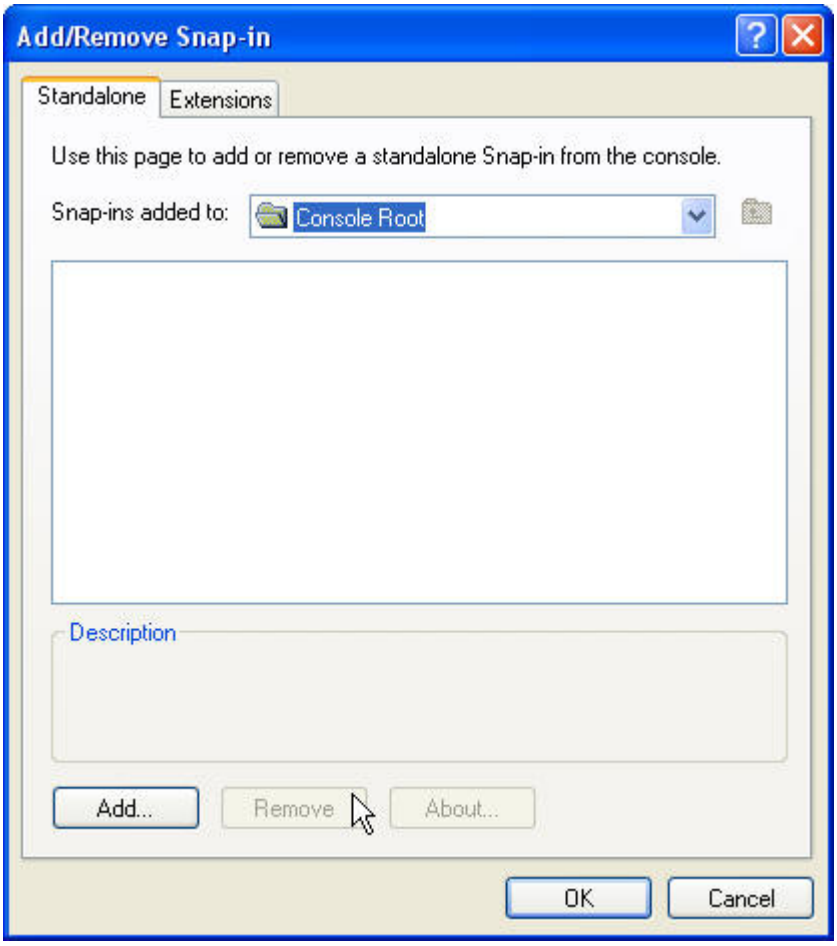
2. You should see the console screen.



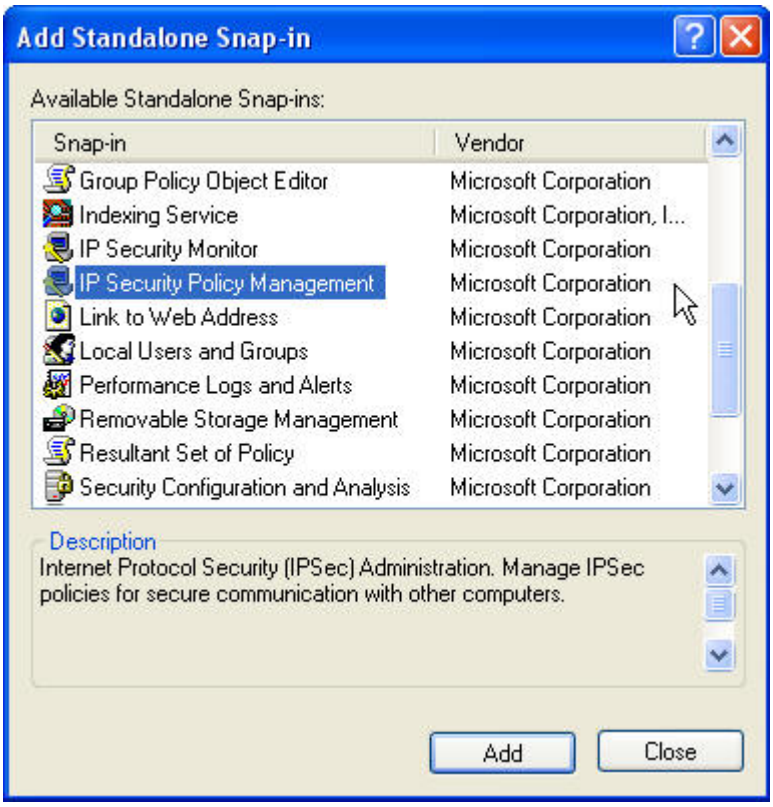
3. Under file, select “Add/Remove Snap-in”.



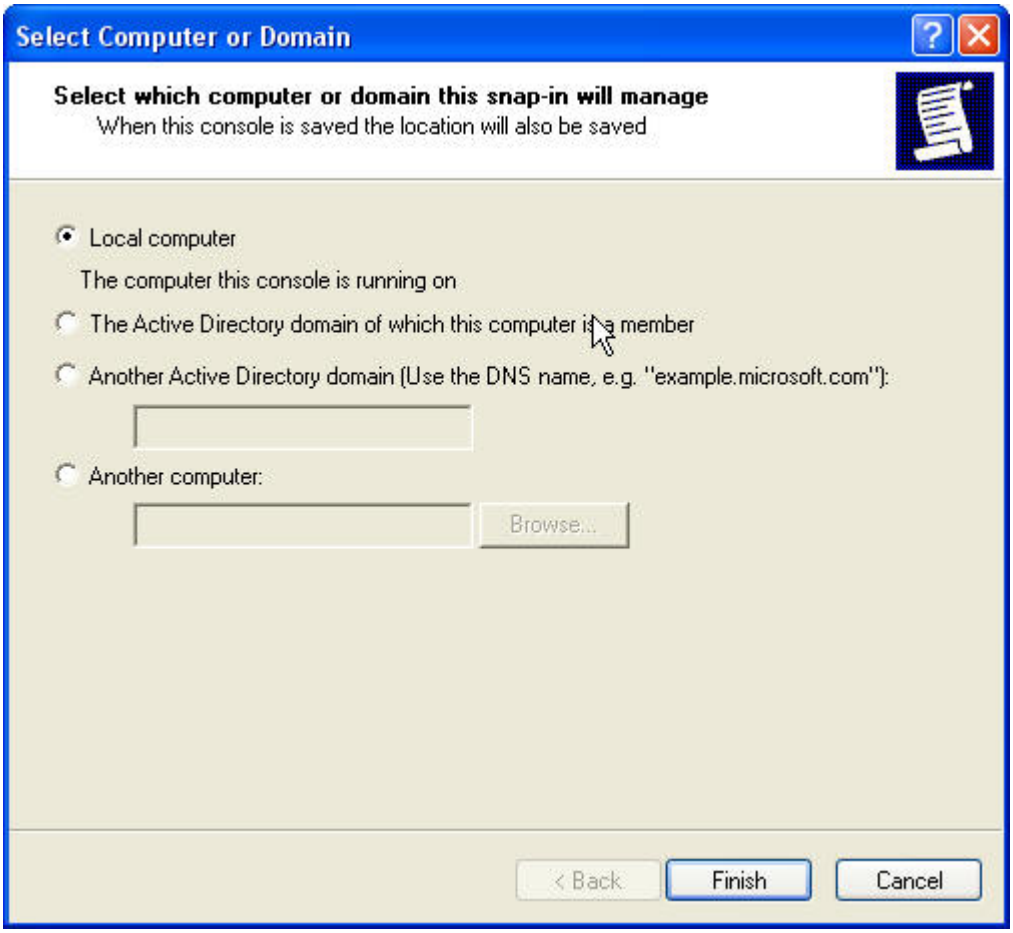
4. Click on “Add”.



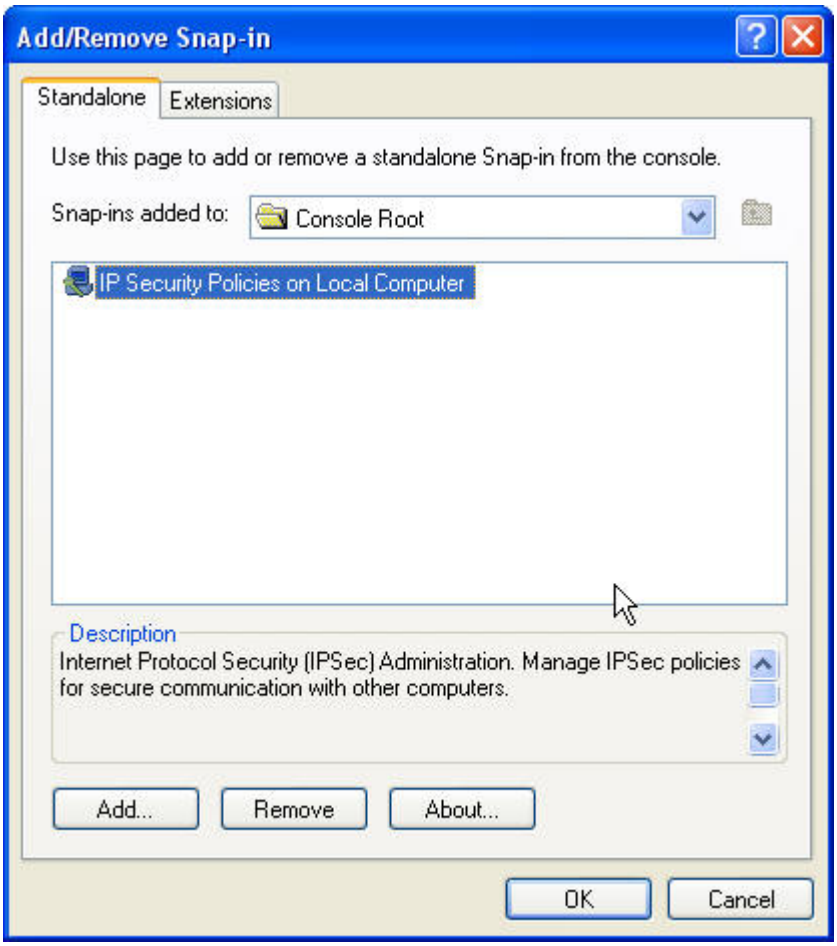
5. Select “IP Security Policy Management”.



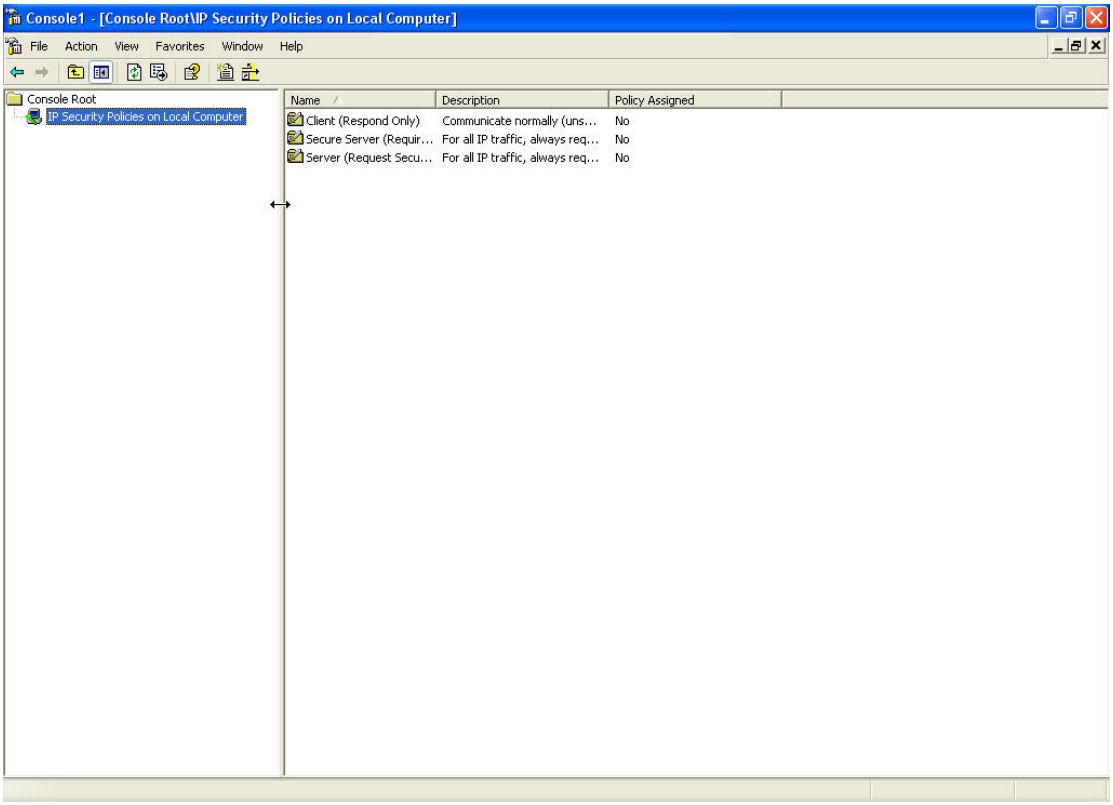
6. Select “Local Computer” then finish.



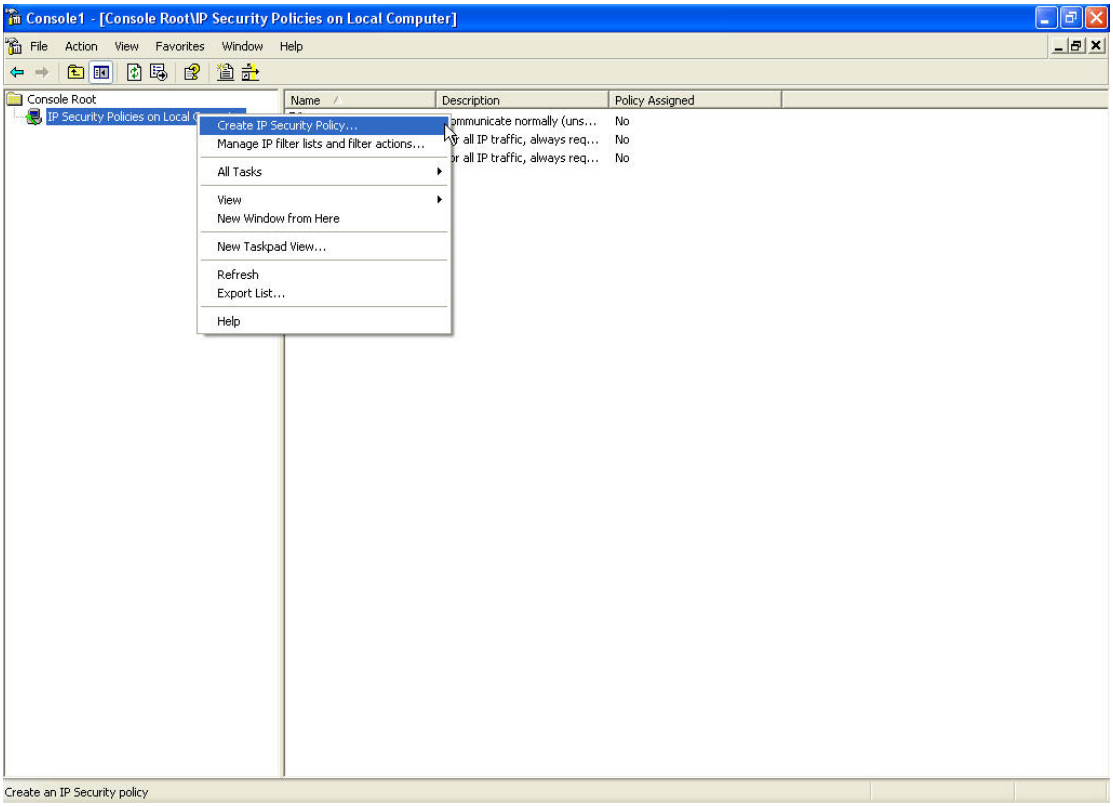
7. Click on “Add”.



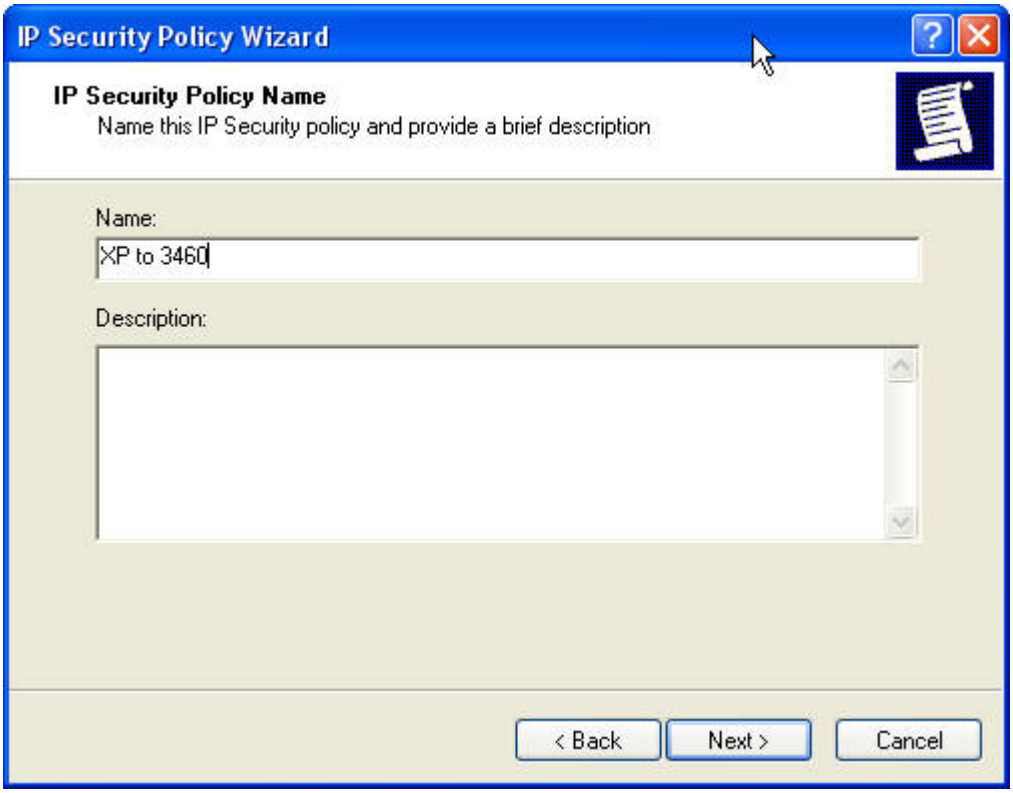
8. You will see the console screen with security policy added.



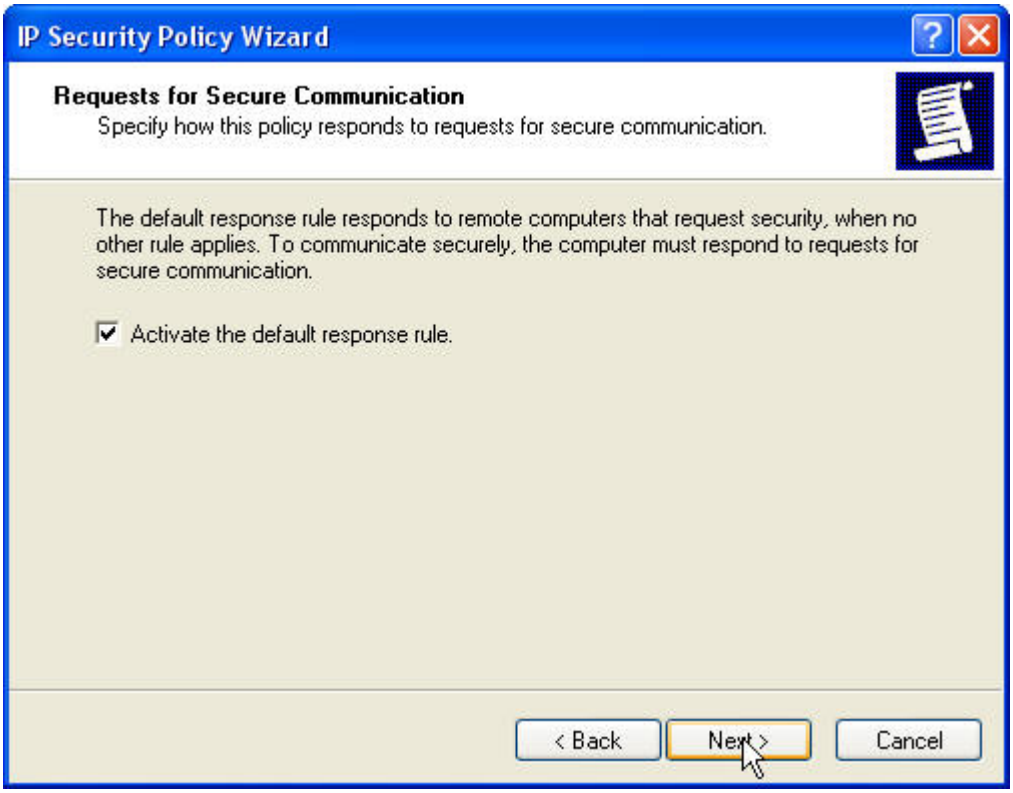
9. Right click on IP Security Policy on Local Computer → Create IP Security Policy.



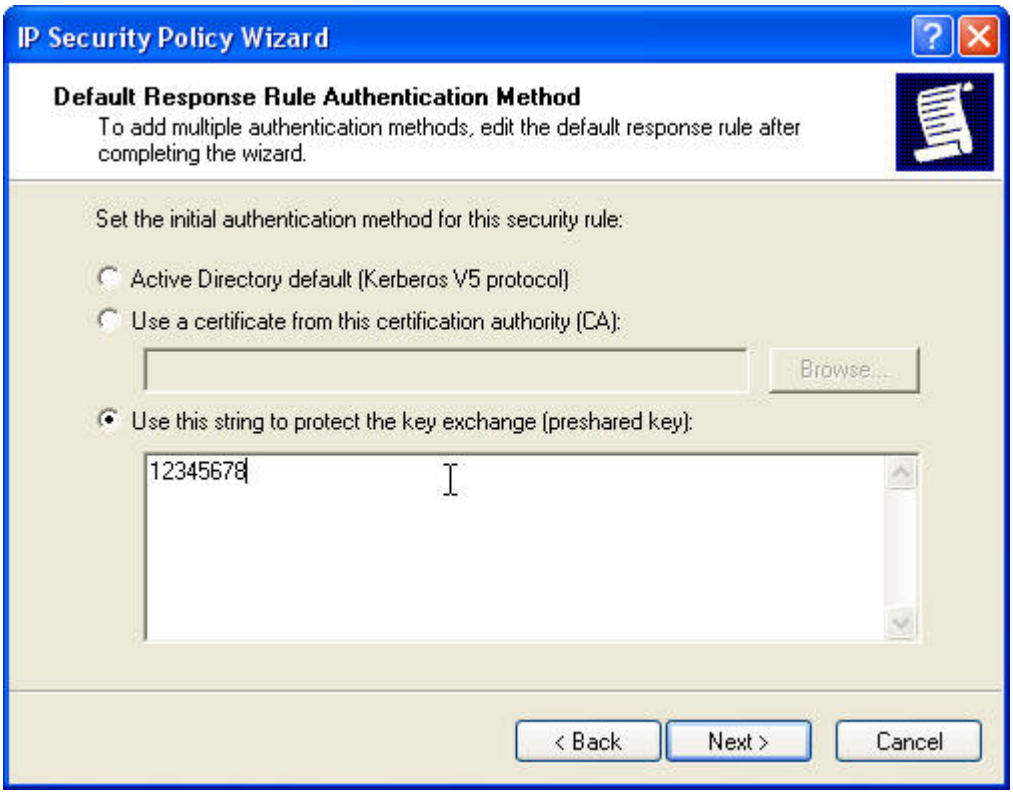
10. Please name the policy.



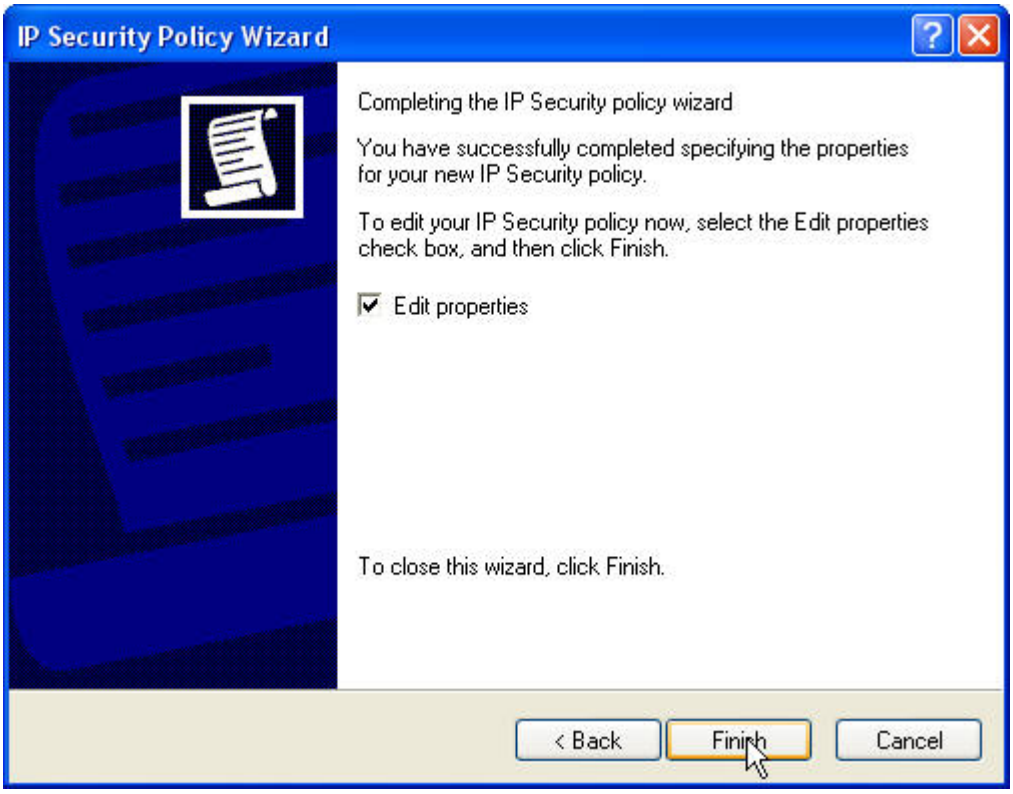
11. Next.



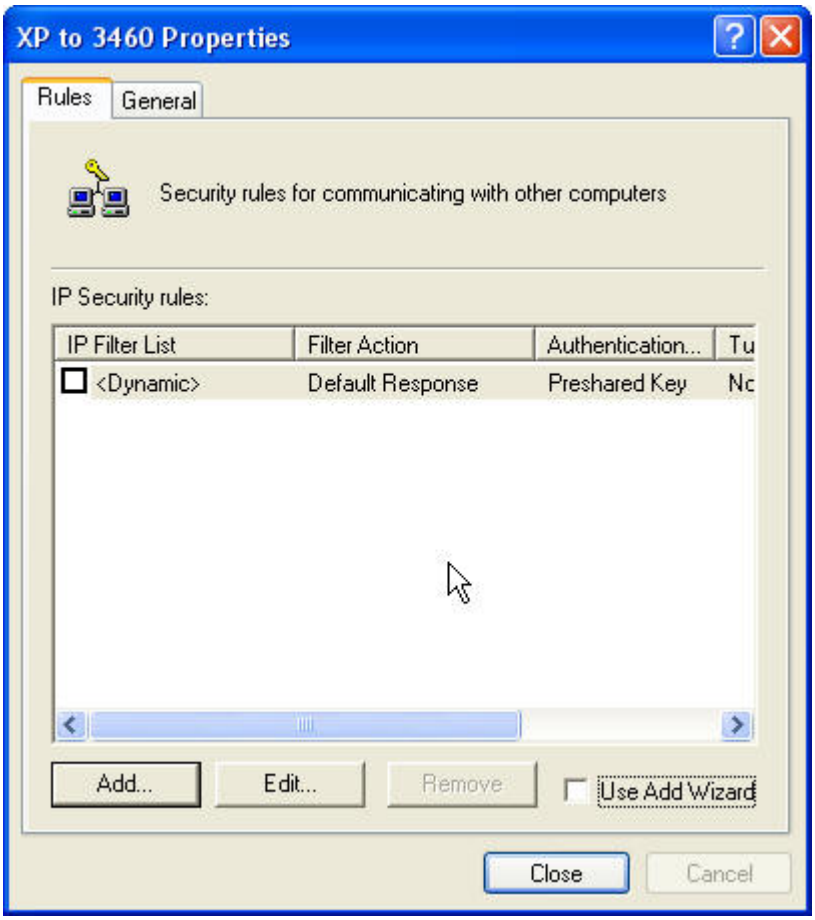
12. Use the Preshared Key, in this example we use “12345678”.



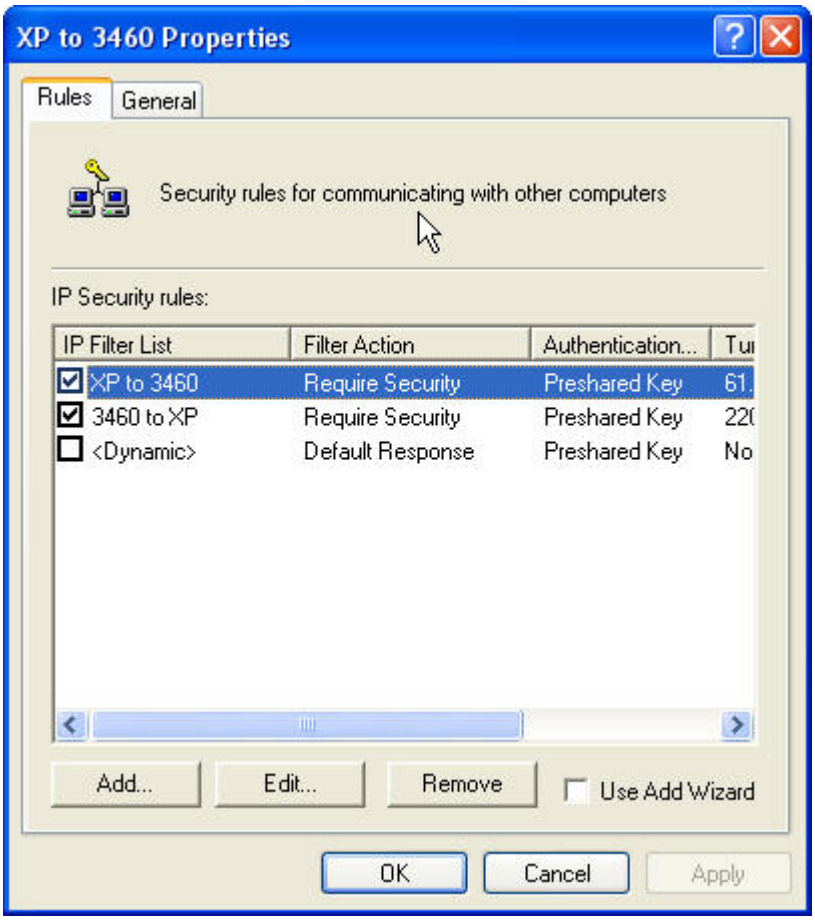
13. Click on Finish.



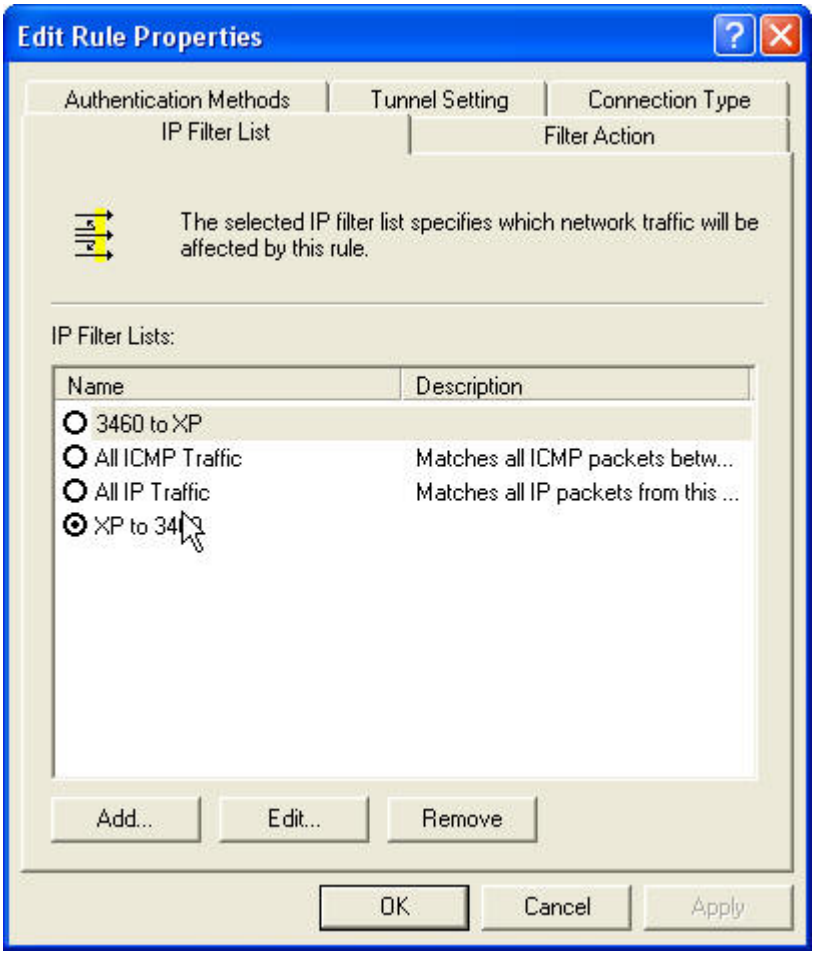
14. In this screen, please disable “use add wizard” and “dynamic”. Then click on add button.

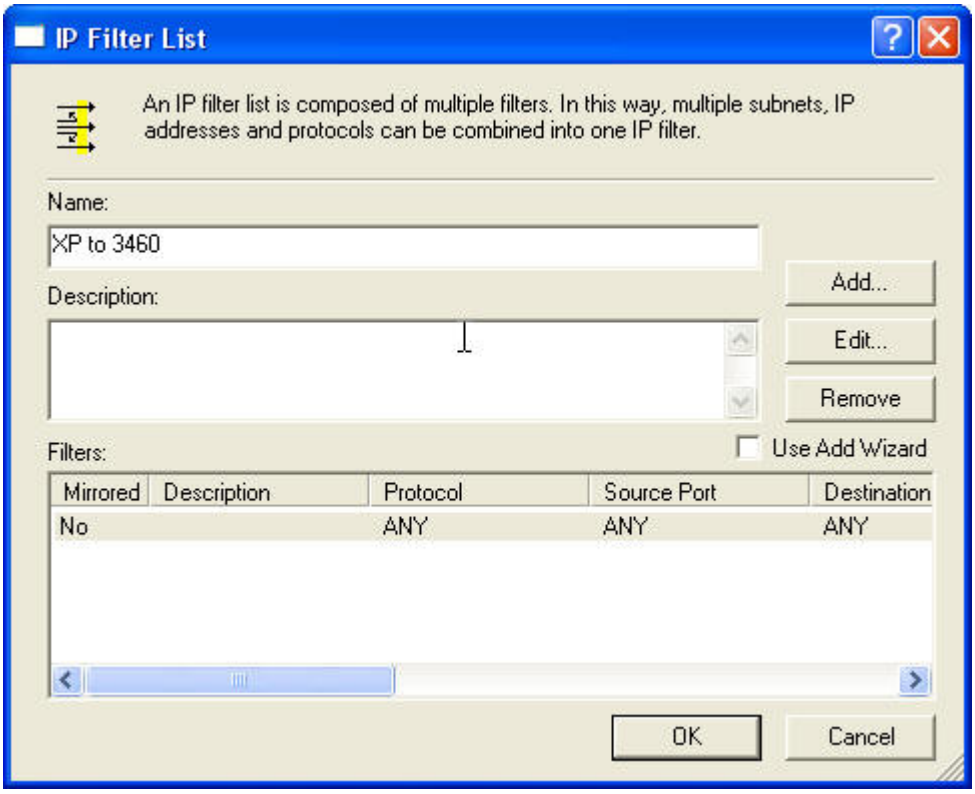


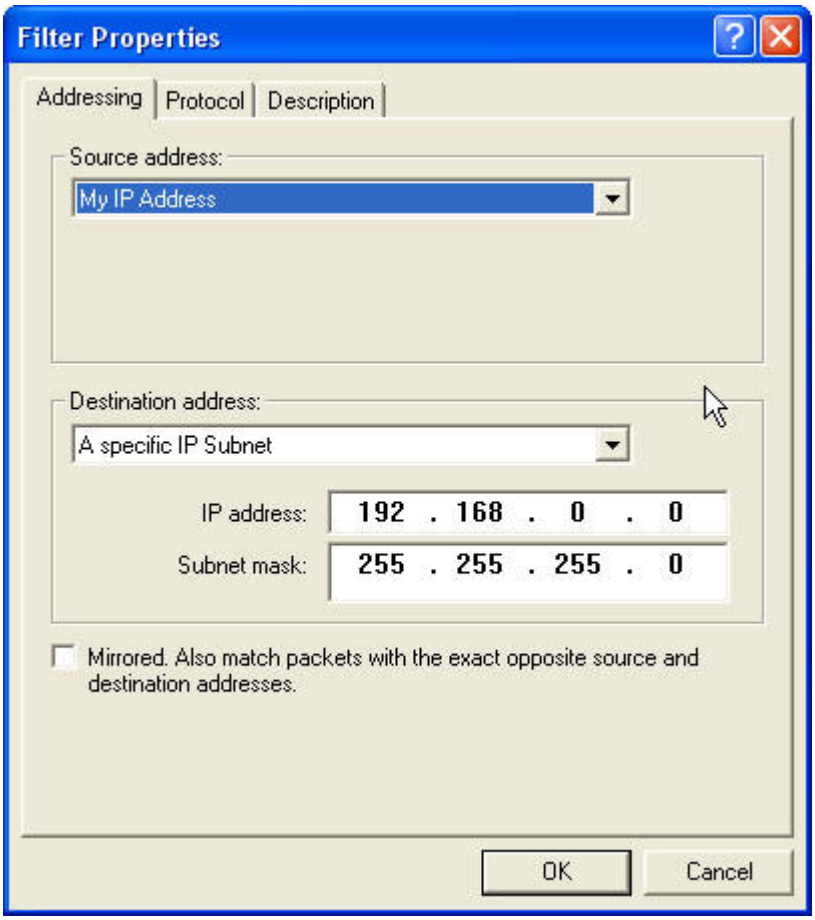
15. From this step, the snapshots show the finished setting. Please follow the same configuration as shown. You will need to create XP to 3460 and 3460 to XP 2 policies.

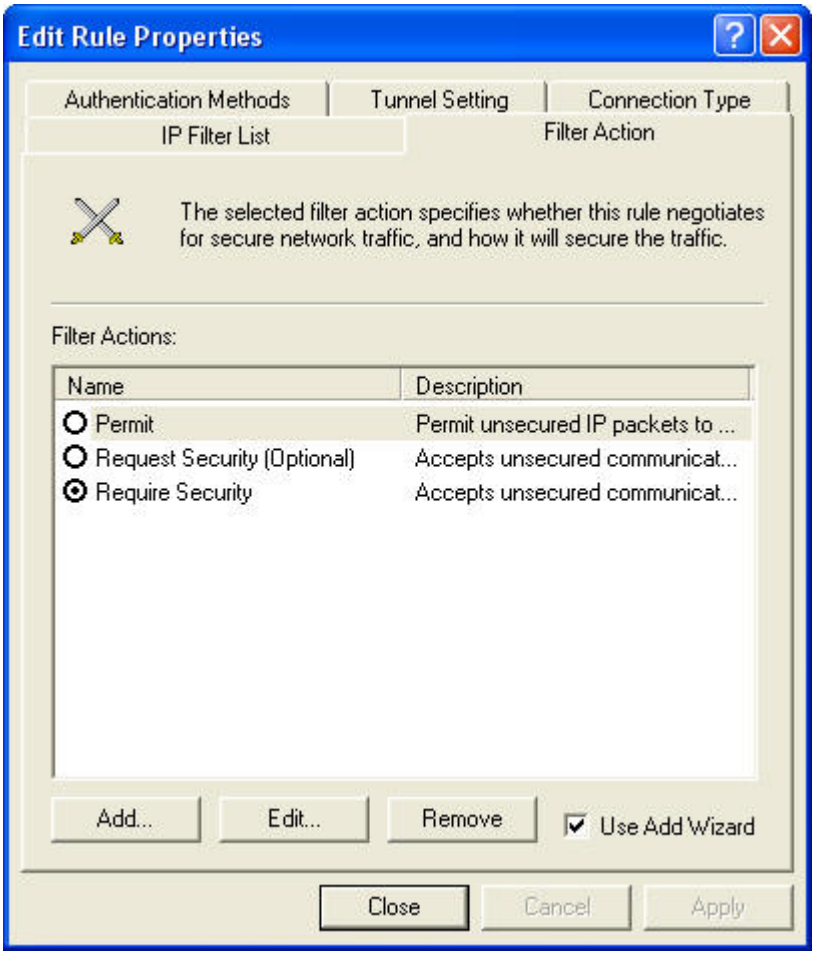


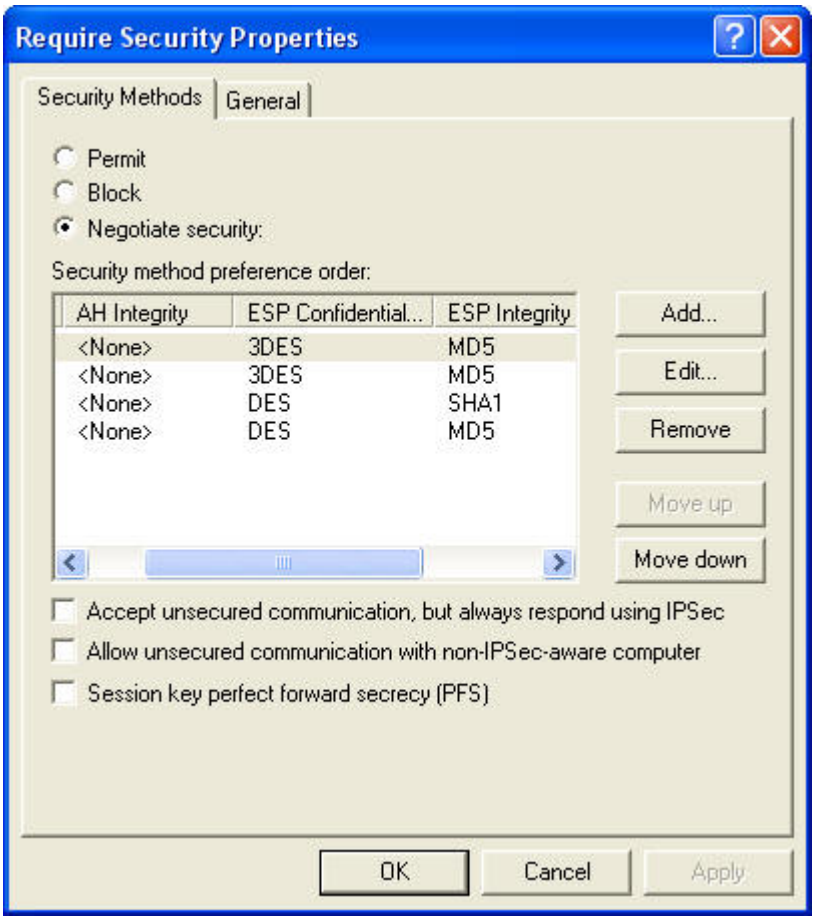
16. We can start with XP to 3460 first. Please configure as shown below.


Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be affected by this rule.
IP Filter Lists:
Name
Description
3460 to XP
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
XP to 34
Add...
Edit...
Remove
OK
Cancel
Apply

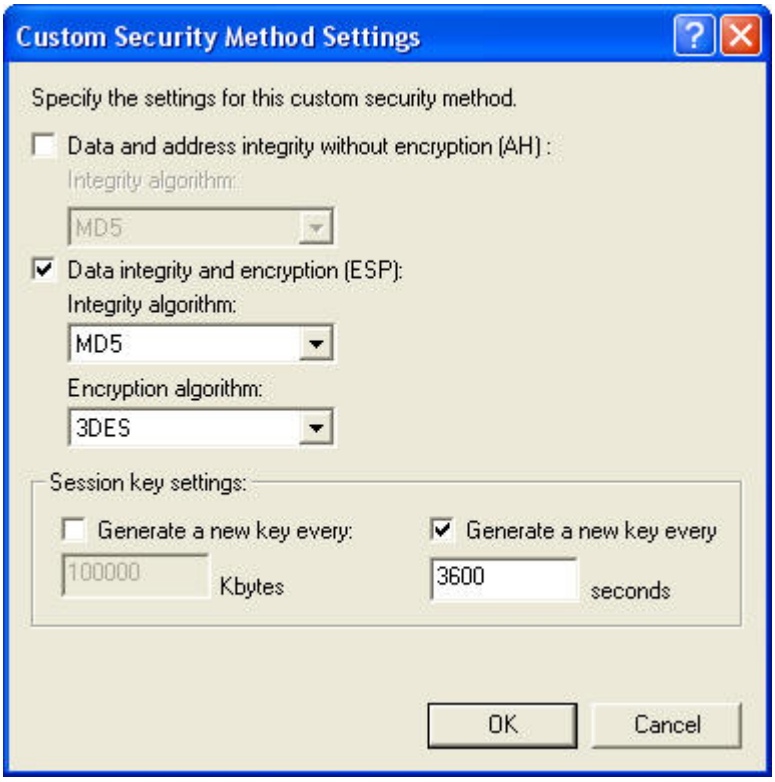

IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
XP to 3460
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
No
ANY
ANY
ANY
OK
Cancel


Filter Properties
Addressing
Protocol
Description
Source address:
My IP Address
Destination address:
A specific IP Subnet
IP address:
192 . 168 . 0 . 0
Subnet mask:
255 . 255 . 255 . 0
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK
Cancel

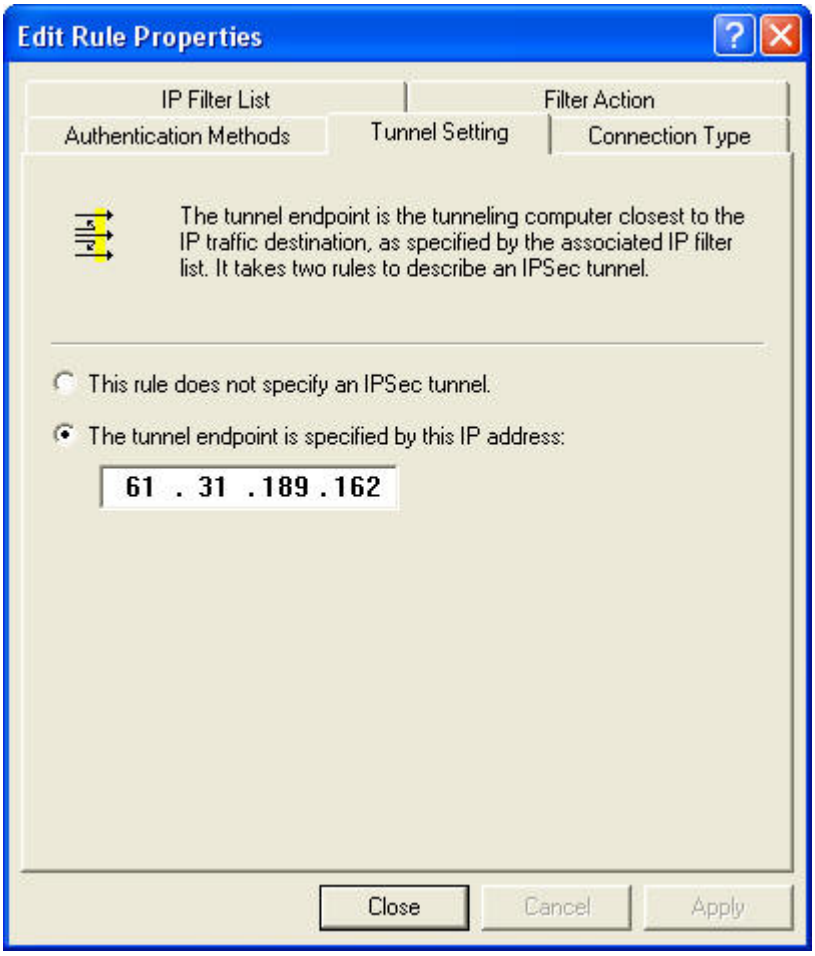

Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.
Filter Actions:
Name
Description
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicat...
Require Security
Accepts unsecured communicat...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

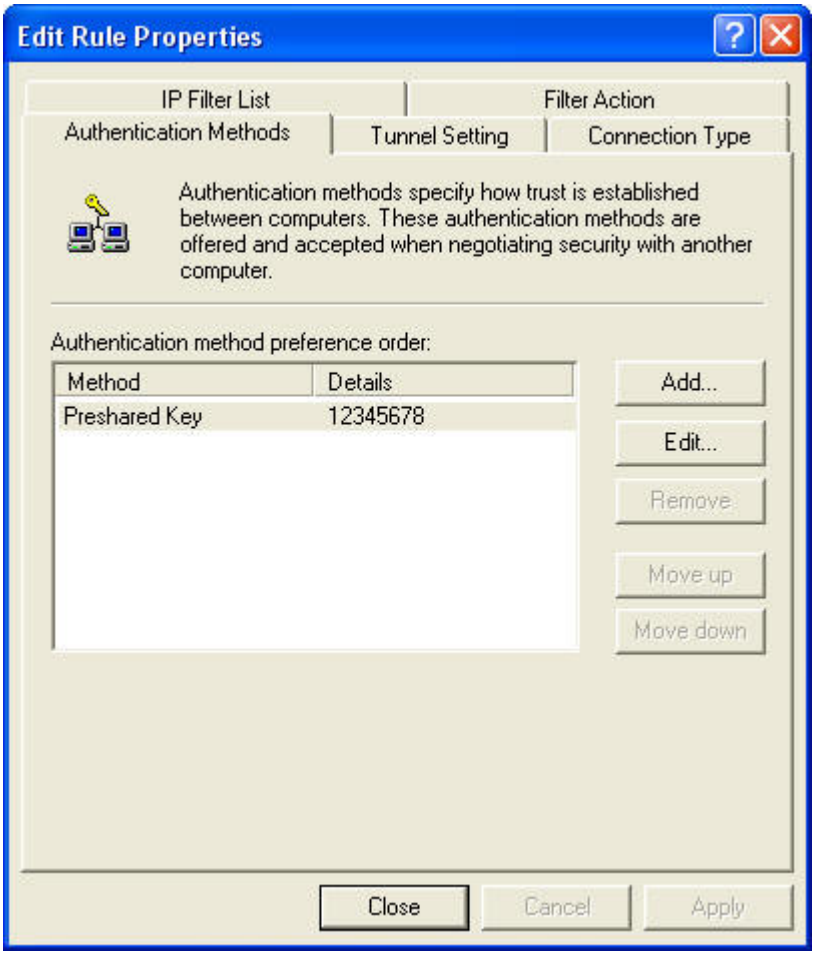

Require Security Properties
Security Methods
General
Permit
Block
Negotiate security:
Security method preference order:
AH Integrity
ESP Confidential...
ESP Integrity
<None>
3DES
MD5
<None>
3DES
MD5
<None>
DES
SHA1
<None>
DES
MD5
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non-IPSec-aware computer
Session key perfect forward secrecy (PFS)
OK
Cancel
Apply

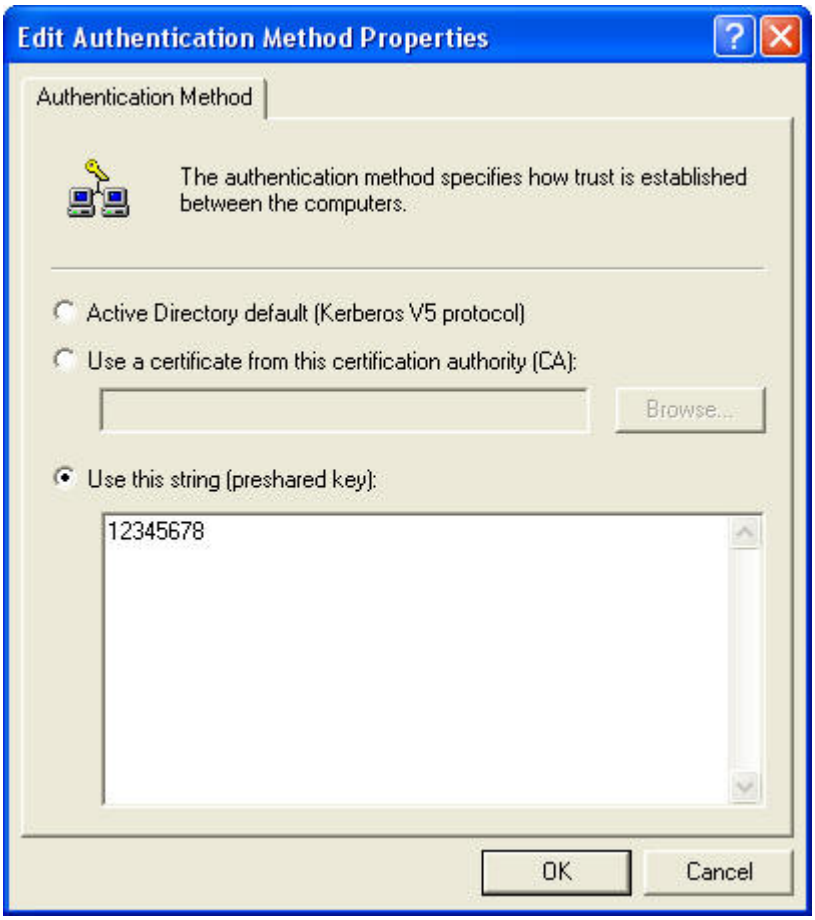

Modify Security Method
Security Method
Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified
Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted
Custom
Settings...
OK
Cancel


Custom Security Method Settings
Specify the settings for this custom security method.
Data and address integrity without encryption (AH) :
Integrity algorithm:
MD5
Data integrity and encryption (ESP):
Integrity algorithm:
MD5
Encryption algorithm:
3DES
Session key settings:
Generate a new key every:
100000
Kbytes
Generate a new key every
3600
seconds
OK
Cancel

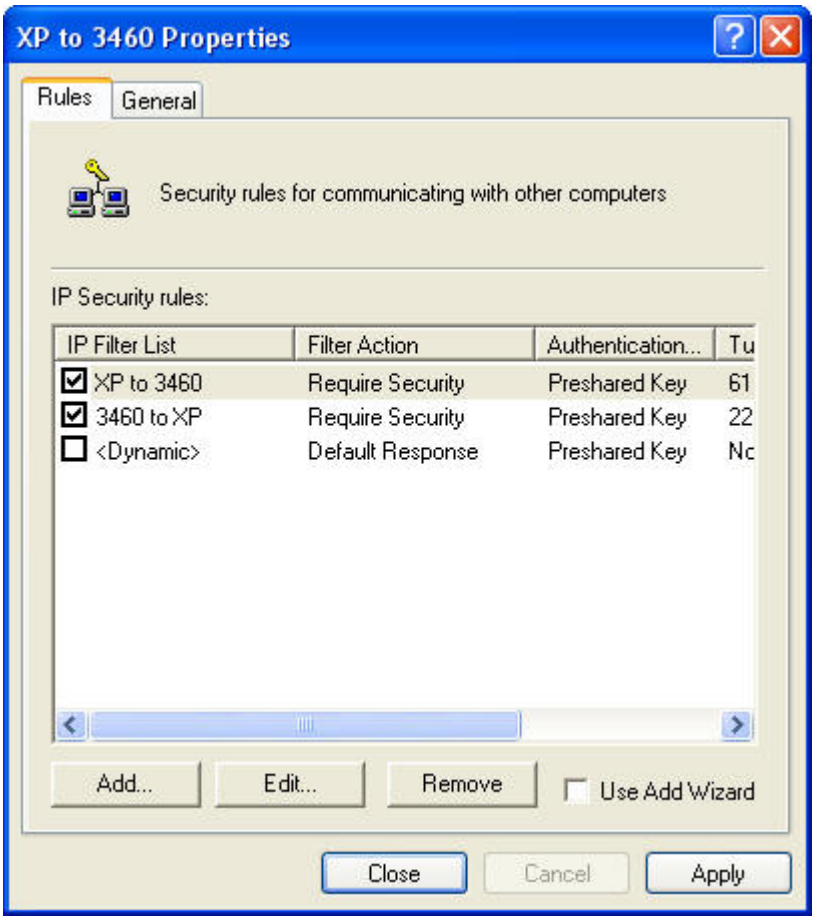
17. The end point is the WAN IP address of WBR-3460.



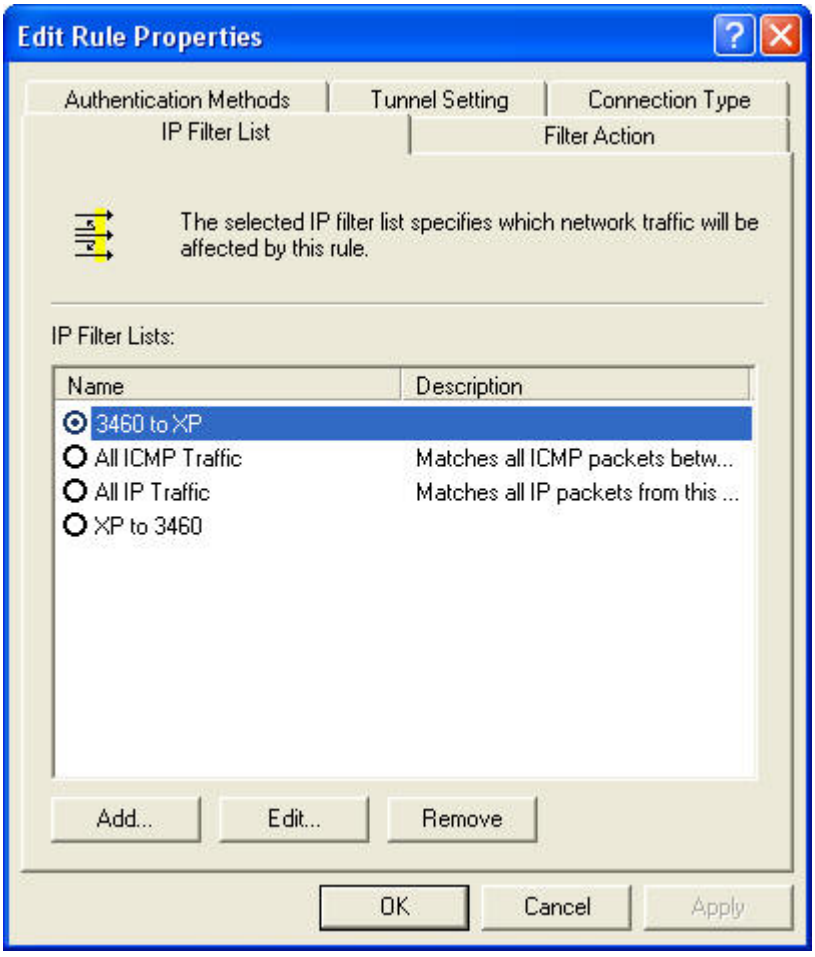

Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.
Authentication method preference order:
Method
Details
Preshared Key
12345678
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply

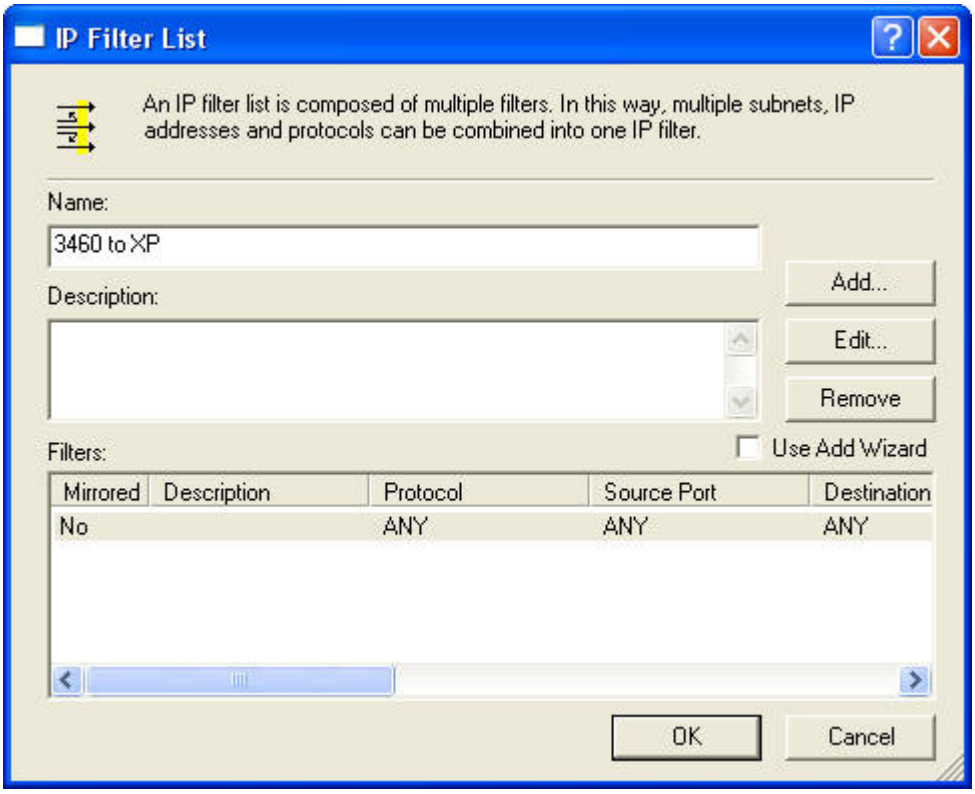


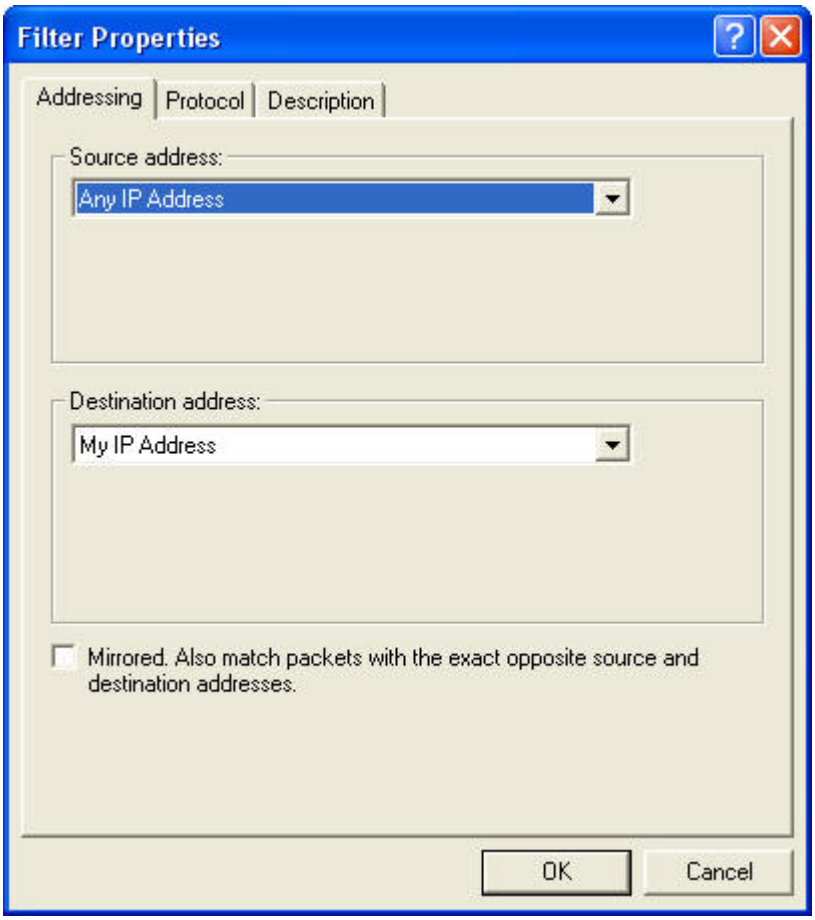
18. Finish XP to 3460.

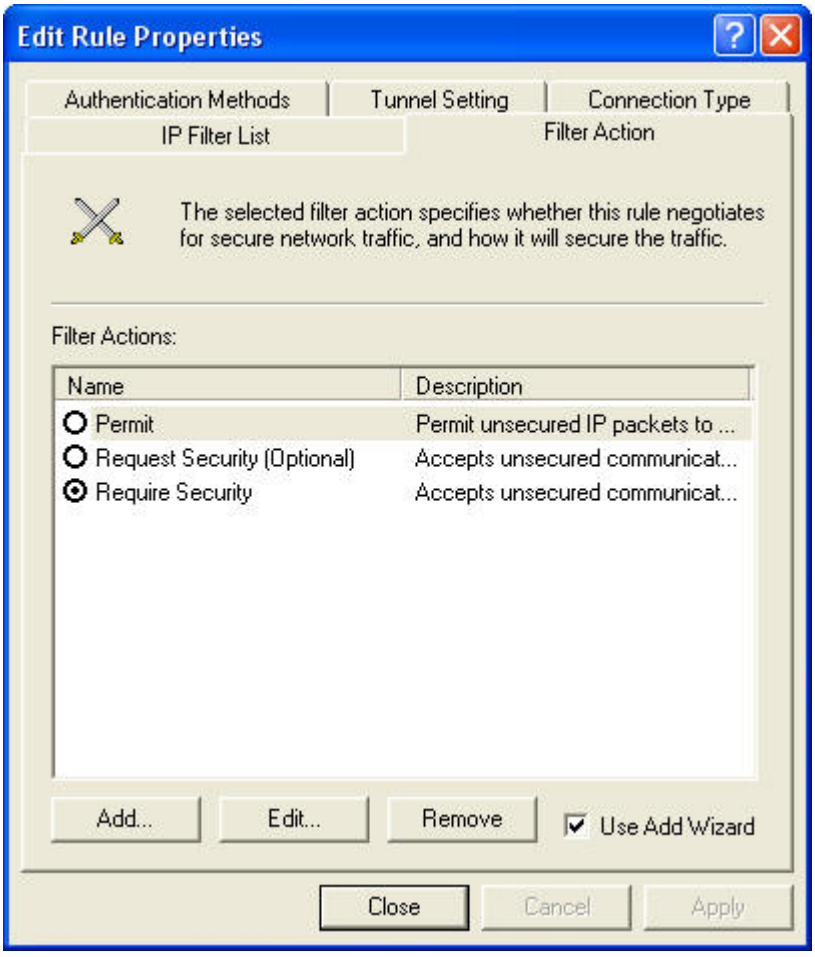


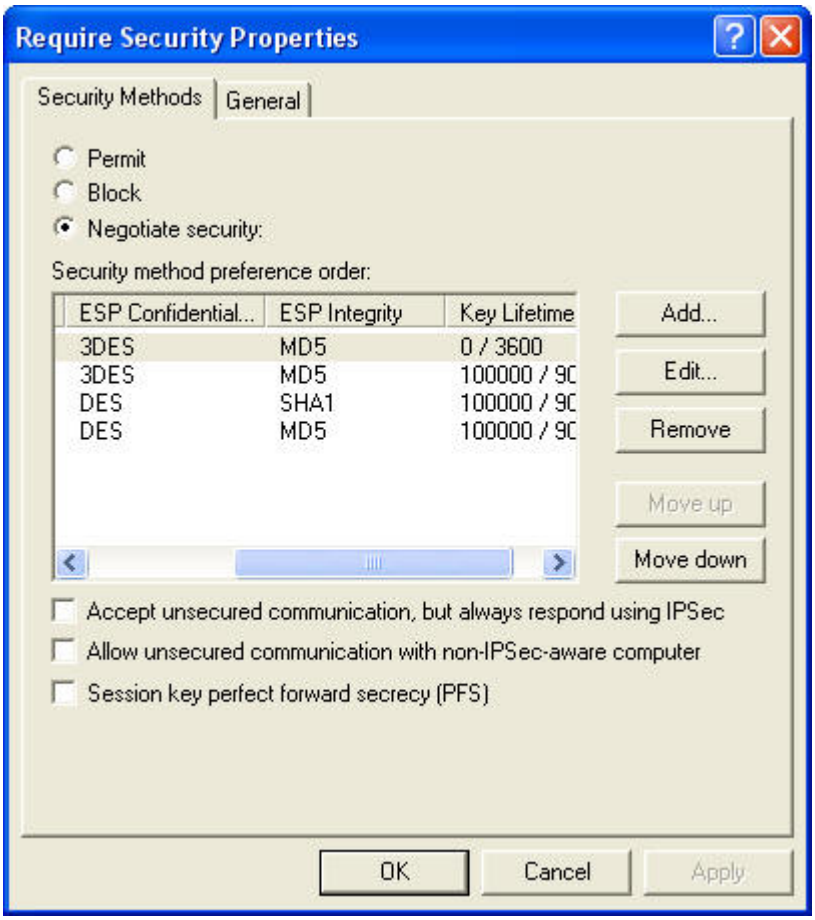
19. Configure 3460 to XP.


Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected IP filter list specifies which network traffic will be affected by this rule.
IP Filter Lists:
Name
Description
3460 to XP
All ICMP Traffic
Matches all ICMP packets betw...
All IP Traffic
Matches all IP packets from this ...
XP to 3460
Add...
Edit...
Remove
OK
Cancel
Apply

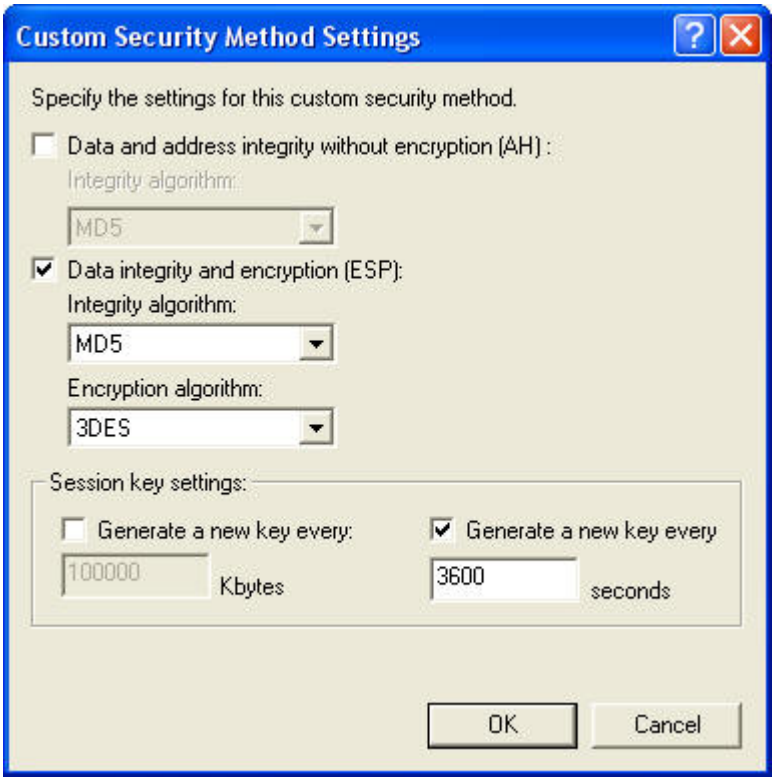

IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
3460 to XP
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
No
ANY
ANY
ANY
OK
Cancel


Filter Properties
Addressing
Protocol
Description
Source address:
Any IP Address
Destination address:
My IP Address
Mirrored. Also match packets with the exact opposite source and destination addresses.
OK
Cancel

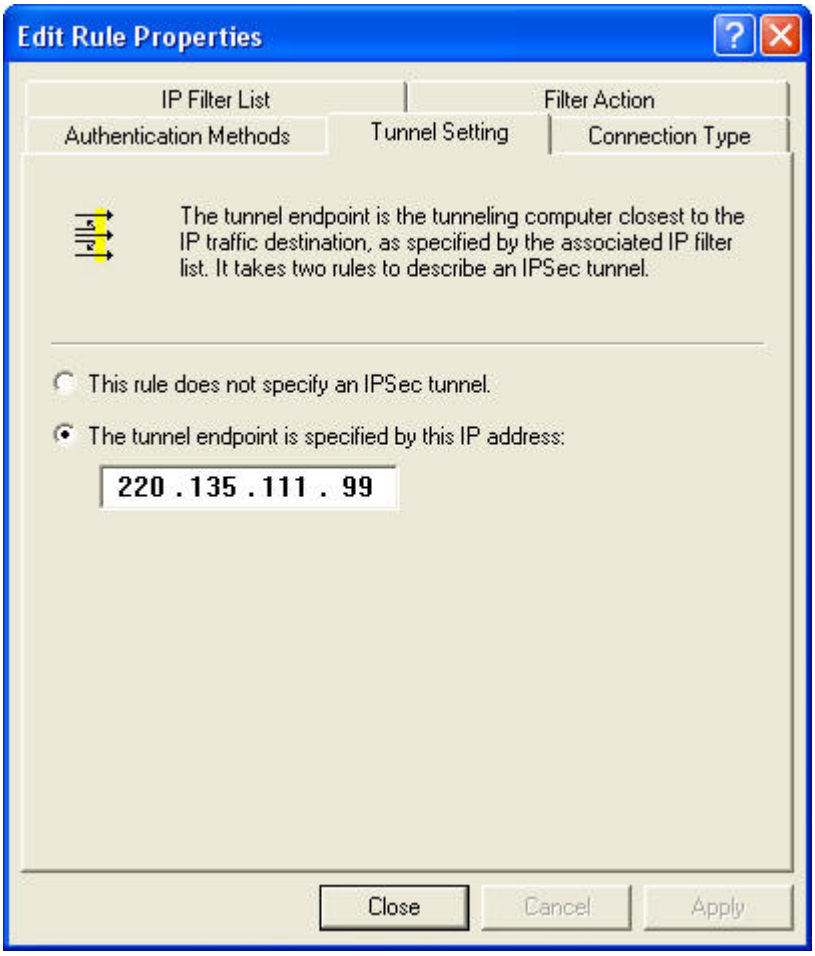

Edit Rule Properties
Authentication Methods
Tunnel Setting
Connection Type
IP Filter List
Filter Action
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.
Filter Actions:
Name
Description
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicat...
Require Security
Accepts unsecured communicat...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

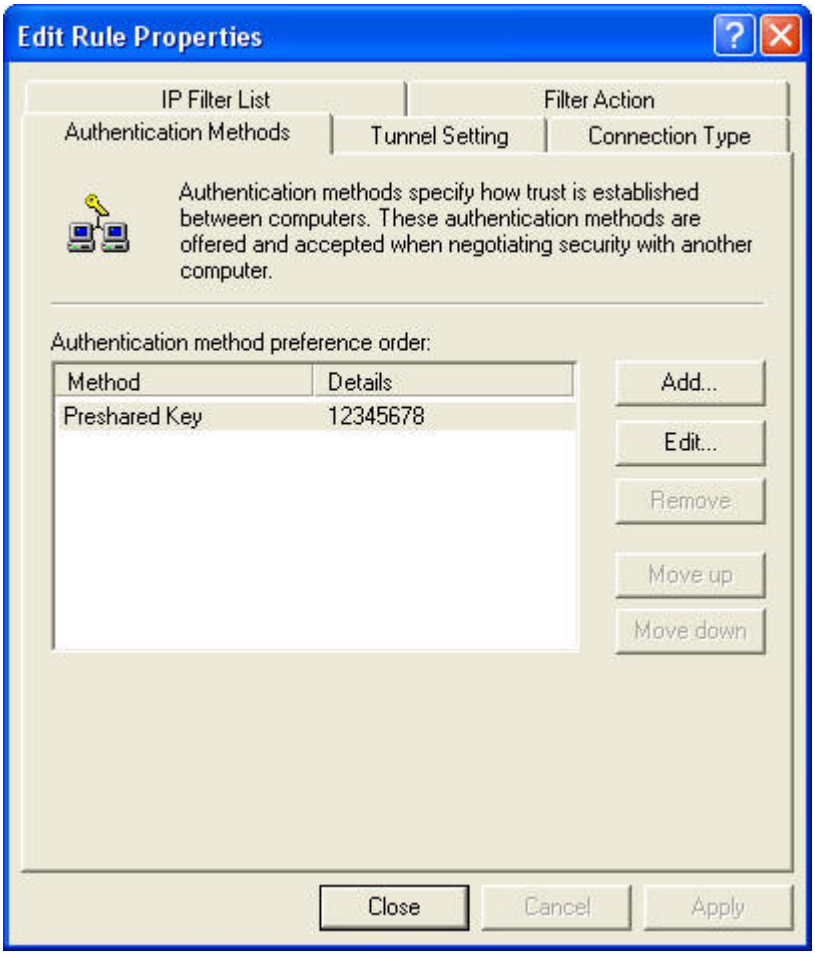

Require Security Properties
Security Methods
General
Permit
Block
Negotiate security:
Security method preference order:
ESP Confidential...
ESP Integrity
Key Lifetime
3DES
MD5
0 / 3600
3DES
MD5
100000 / 90
DES
SHA1
100000 / 90
DES
MD5
100000 / 90
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non-IPSec-aware computer
Session key perfect forward secrecy (PFS)
OK
Cancel
Apply

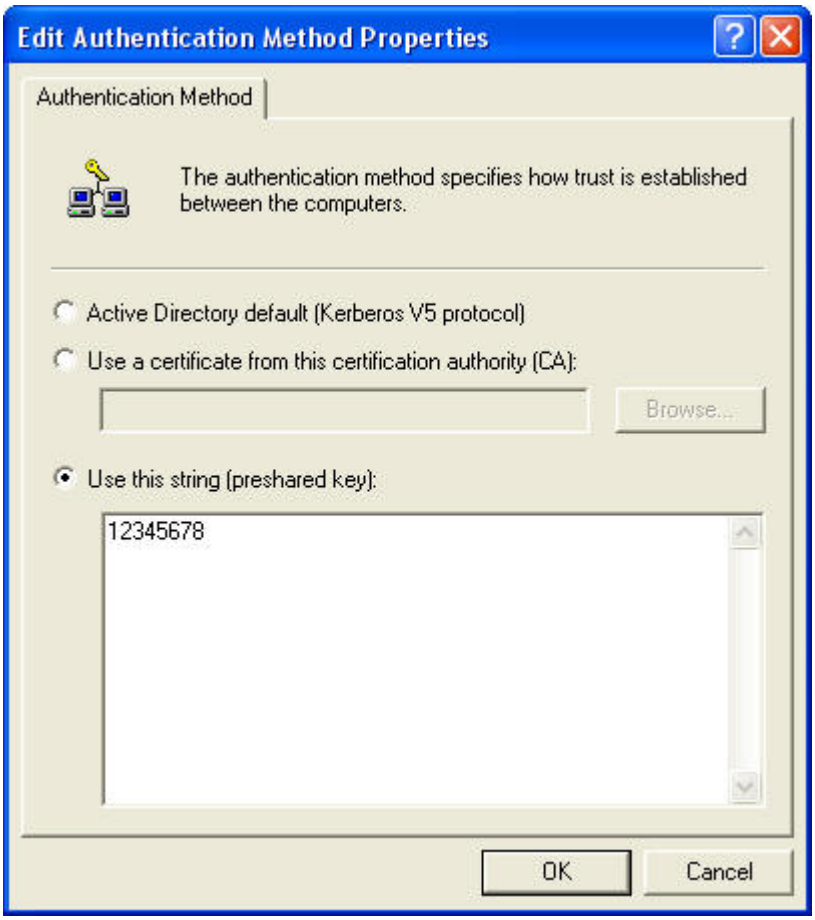

Modify Security Method
Security Method
Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified
Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted
Custom
Settings...
OK
Cancel

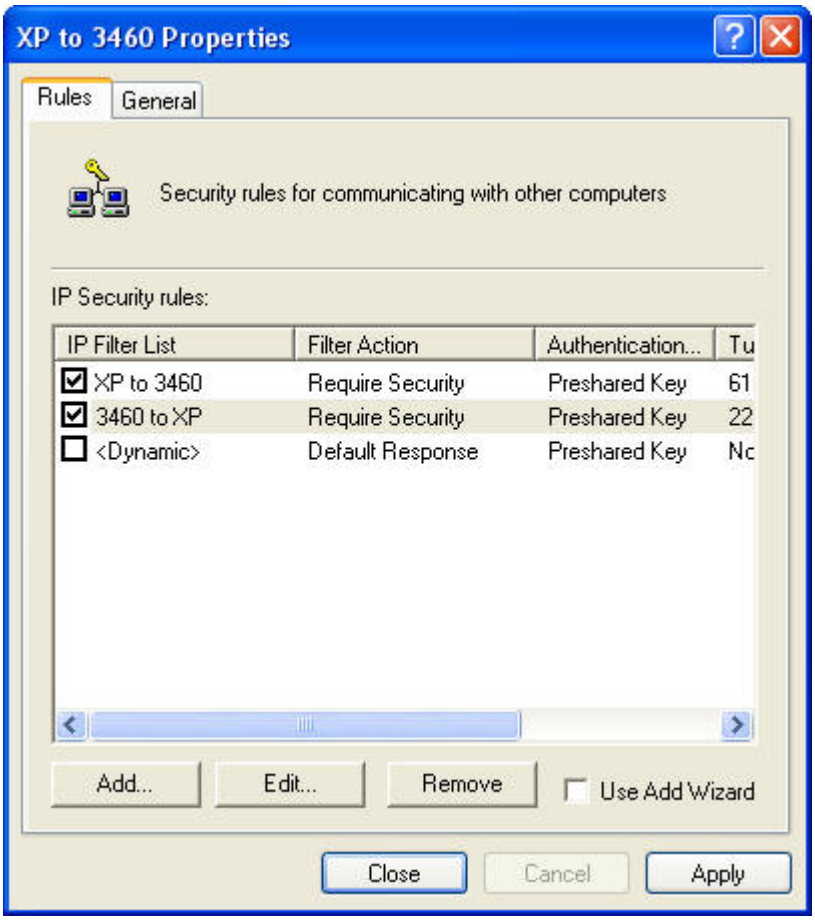

Custom Security Method Settings
Specify the settings for this custom security method.
Data and address integrity without encryption (AH) :
Integrity algorithm:
MD5
Data integrity and encryption (ESP):
Integrity algorithm:
MD5
Encryption algorithm:
3DES
Session key settings:
Generate a new key every:
100000
Kbytes
Generate a new key every
3600
seconds
OK
Cancel

20. The end point is the WAN IP address of Windows 2000/XP.

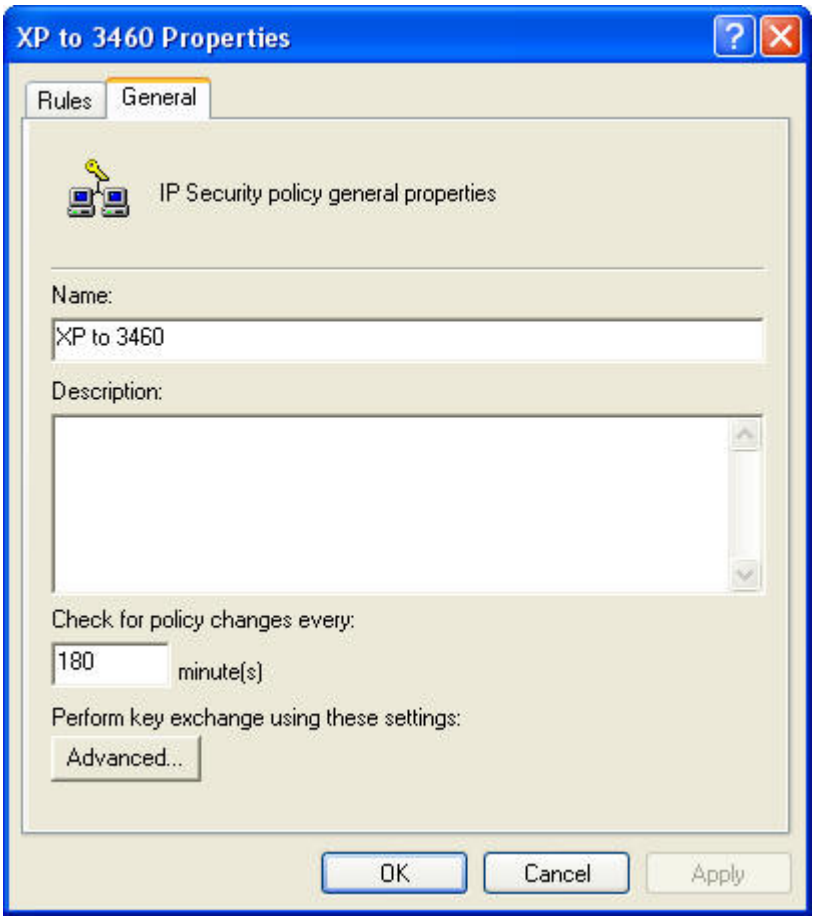



Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.
Authentication method preference order:
Method
Details
Preshared Key
12345678
Add...
Edit...
Remove
Move up
Move down
Close
Cancel
Apply

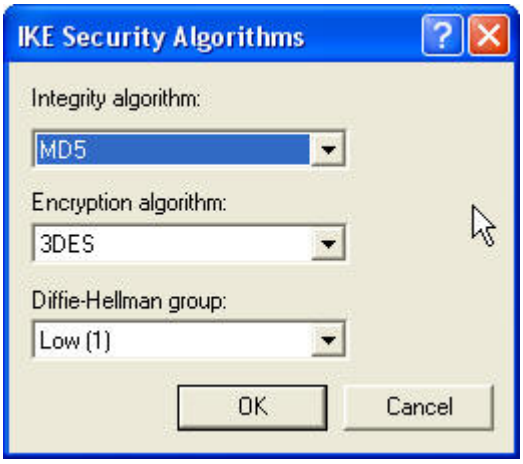

Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Active Directory default (Kerberos V5 protocol)
Use a certificate from this certification authority (CA):
Browse...
Use this string (preshared key):
12345678
OK
Cancel



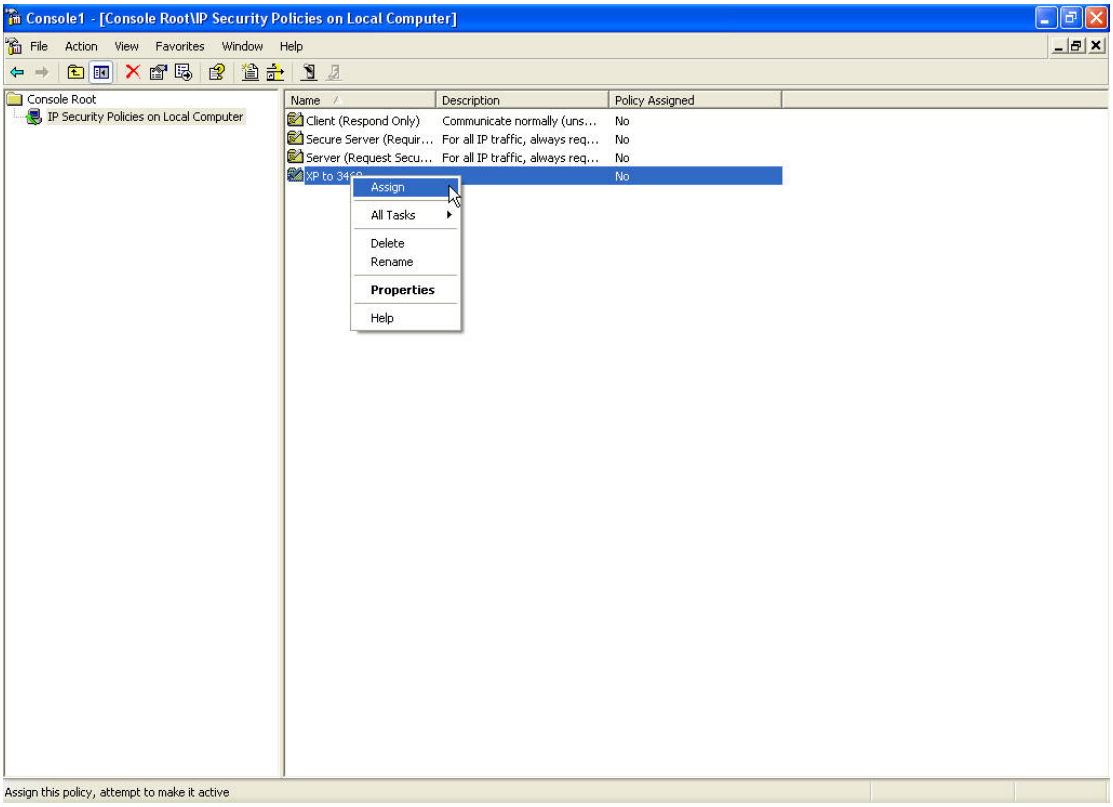
21. Click on General Tab. Configure as below.


XP to 3460 Properties
Rules
General
IP Security policy general properties
Name:
XP to 3460
Description:
Check for policy changes every:
180
minute(s)
Perform key exchange using these settings:
Advanced...
OK
Cancel
Apply


Key Exchange Security Methods
Protect identities during authentication with these security methods.
Security method preference order:
Encryption
Integrity
Diffie-Hellman
3DES
MD5
Low (1)
3DES
MD5
Medium (2)
DES
SHA1
Low (1)
DES
MD5
Low (1)
Add...
Edit...
Remove
Move up
Move down
OK
Cancel

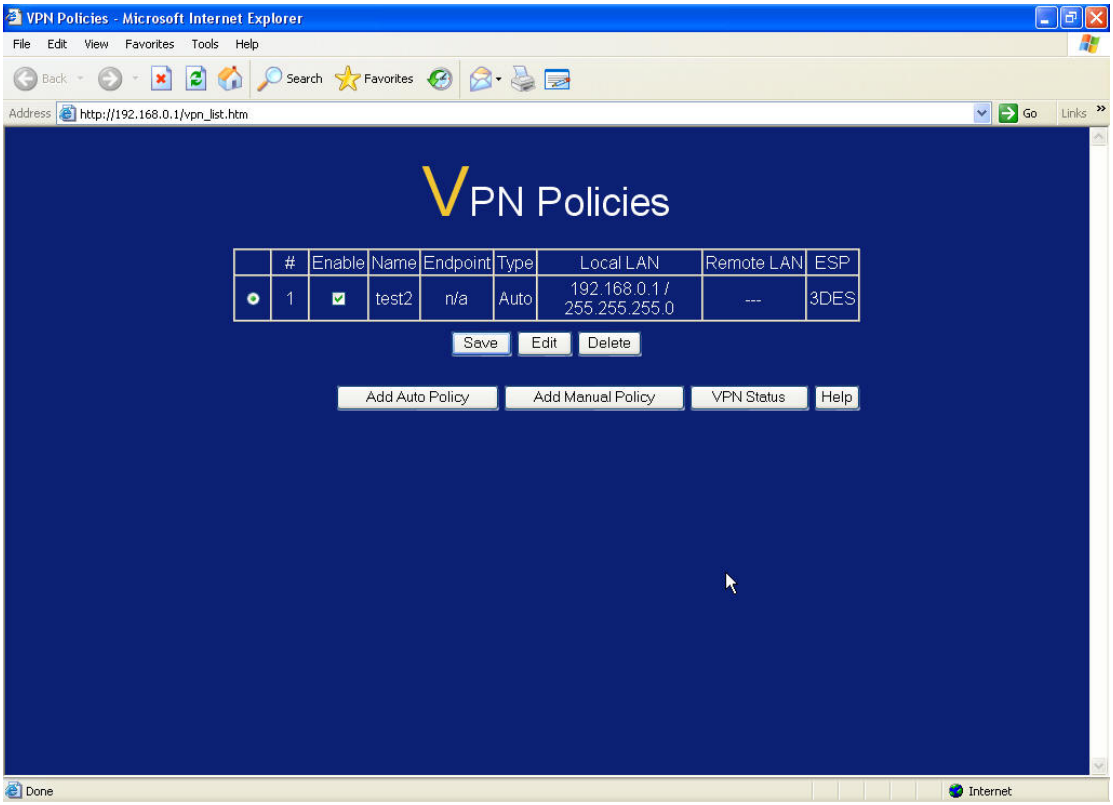


22. Once complete, return to the console screen, right click on the policy and select “assign” to activate.



Below is the sample configuration for WBR-3460 VPN server

23. Please do not forget to enable the VPN tunnel.



24. Sample configuration of WBR-3460 VPN.

25. Ping from Windows 2000/XP VPN Client to WBR-3460 via VPN tunnel.