

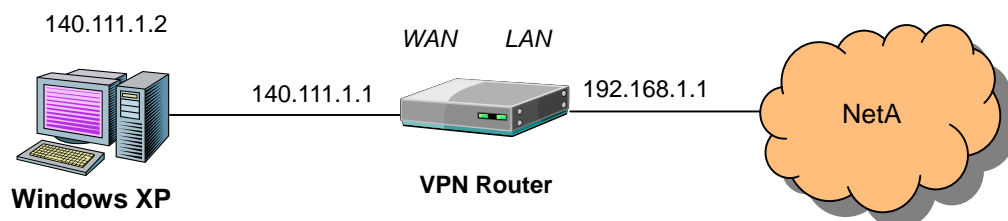
# Configuring IPsec between a Microsoft Windows XP Professional (1 NIC) and the VPN router

## Introduction

This document demonstrates how to establish an IPsec tunnel with preshared keys to join a private network inside a VPN router and a Microsoft Windows XP Professional. You can find detailed information on configuring the Microsoft Windows 2k at the Microsoft web site:

<http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP>

## Environment

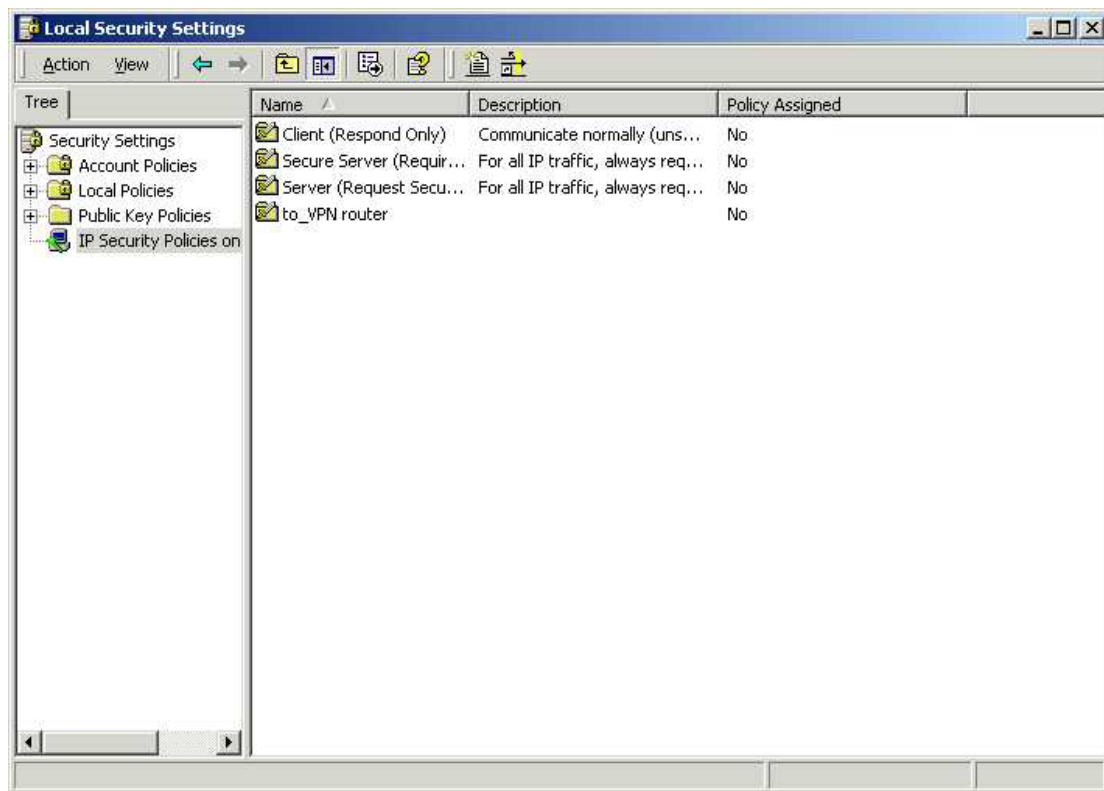


## Step-by-Step

[Windows XP]

### Create IPsec Policy

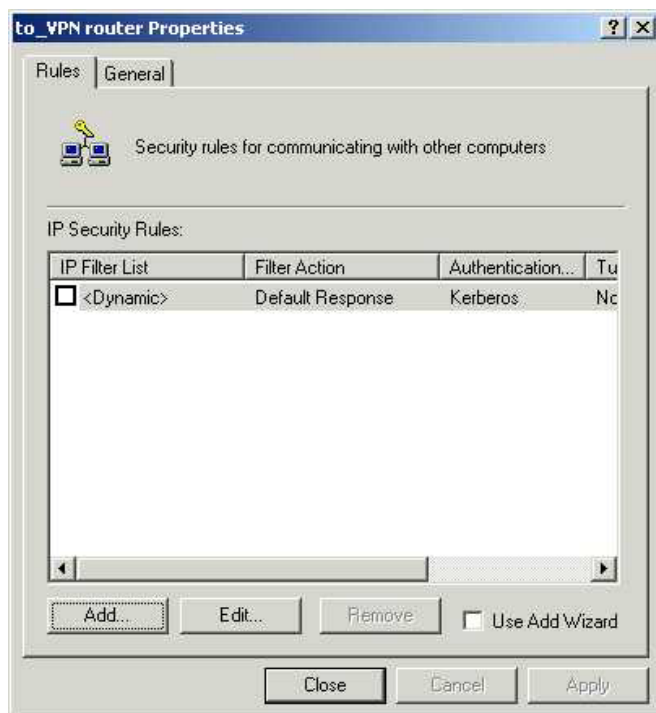
1. Click **Start > Run > secpol.msc** on the Microsoft Windows XP.
2. Right-click **IP Security Policies on Local Computer**, and then click **Create IP Security Policy**.
3. Click **Next**, and then type a name for your policy (for example, “**to\_vpn router**”).
4. Click to clear the **Activate the default response rule** check box, and then click **Next**.
5. Click **Finish** (keep the **Edit** check box selected).



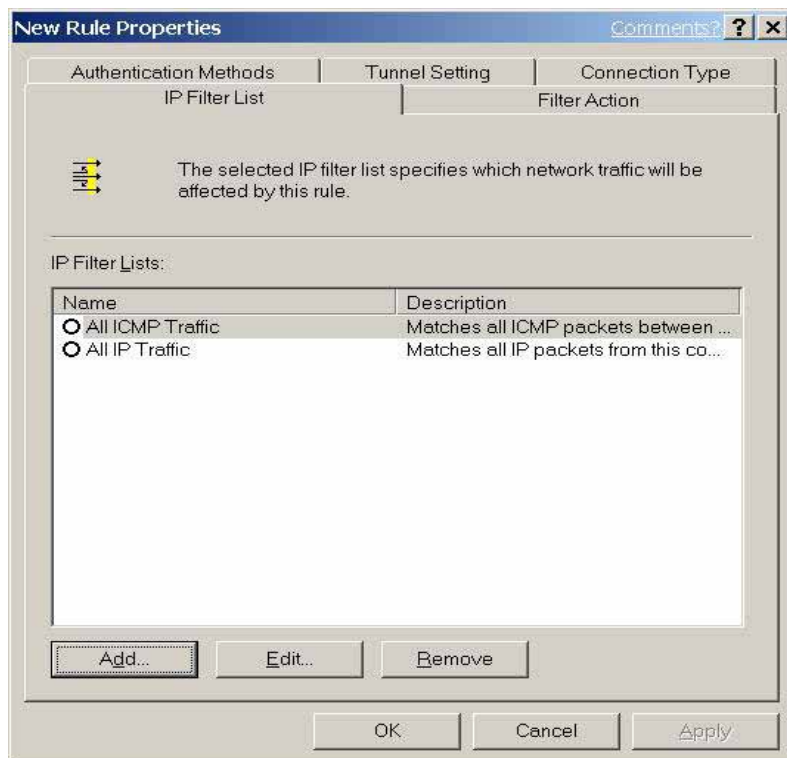
## Build 2 Filter Lists: “WinXP→VPN router” and “VPN router →WinXP”.

### Filter List 1: WinXP→VPN router

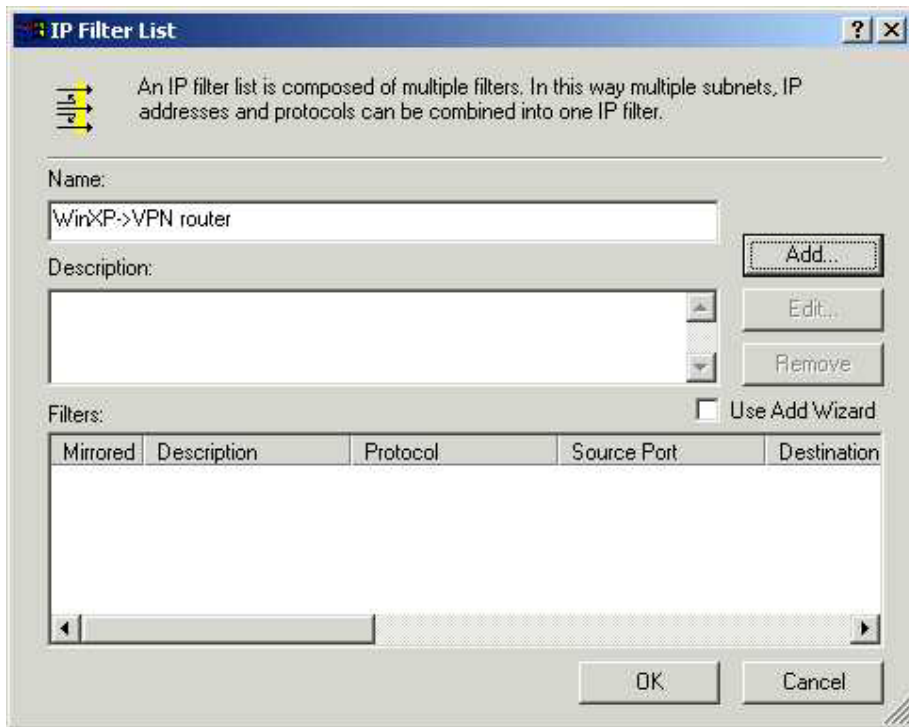
1. In the new policy properties, click to clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.



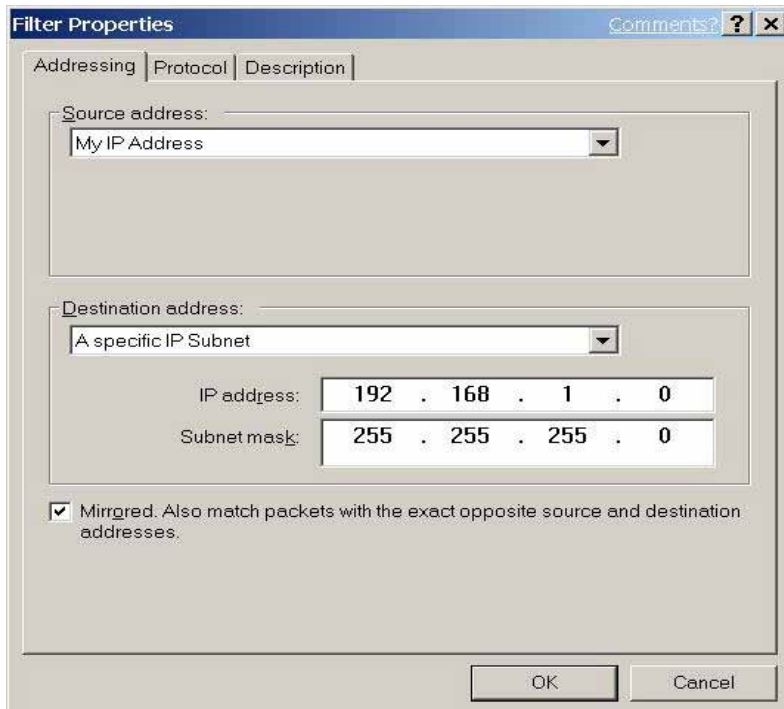
2. On the **IP Filter List** tab, click **Add**.



3. Type an appropriate name “**WinXP→VPN router**” for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.



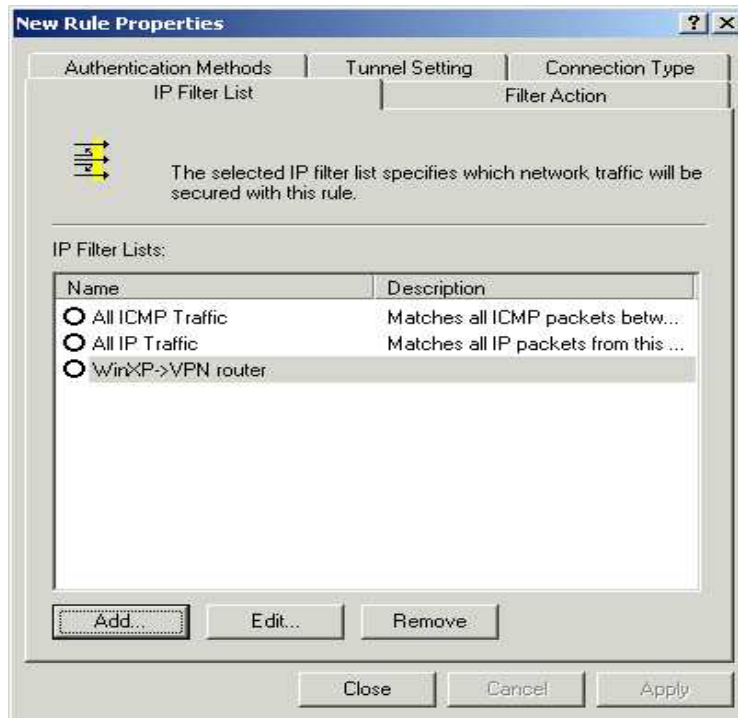
4. In the **Source address** area, click **My IP Address**.
5. In the **Destination address** area, click **A specific IP Subnet**, and fill in the **IP Address** “**192.168.1.0**” and **Subnet mask** “**255.255.255.0**” to reflect NetA.



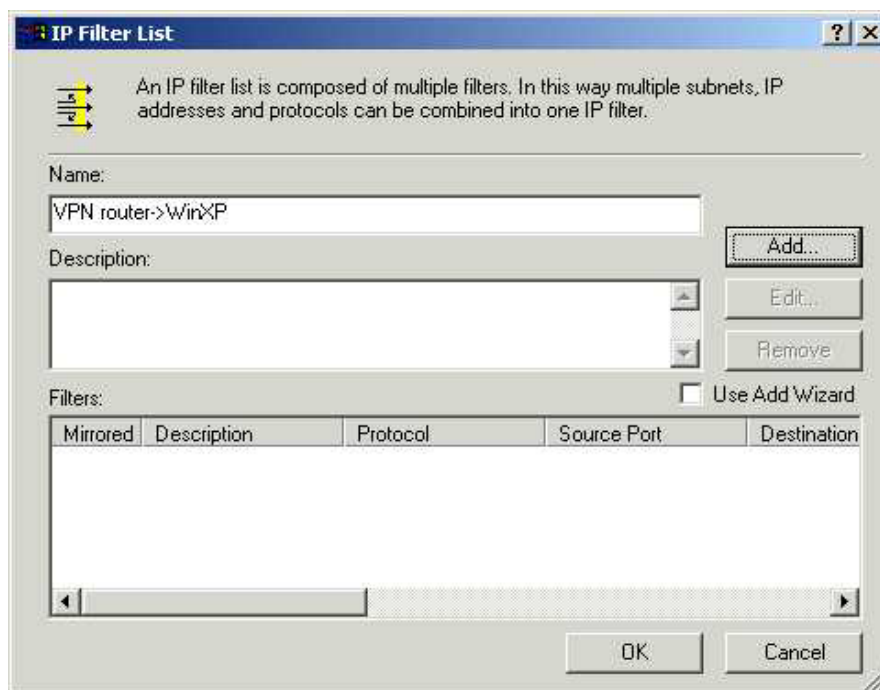
6. If you want to type a description for your filter, click the **Description** tab.
7. Click **OK**, and then click **Close**.

### Filter List 2: VPN router→WinXP

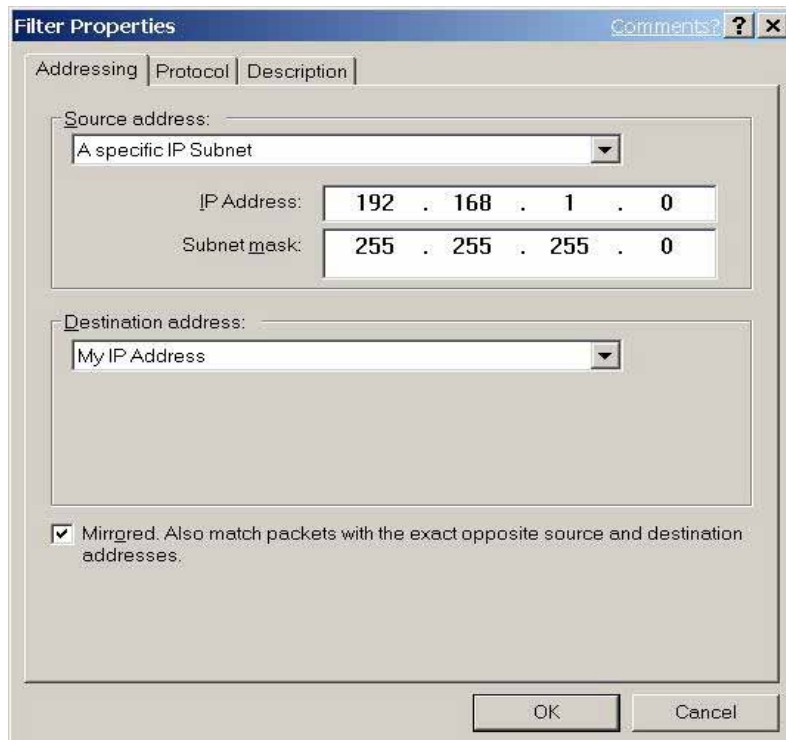
8. On the **IP Filter List** tab, click **Add**.



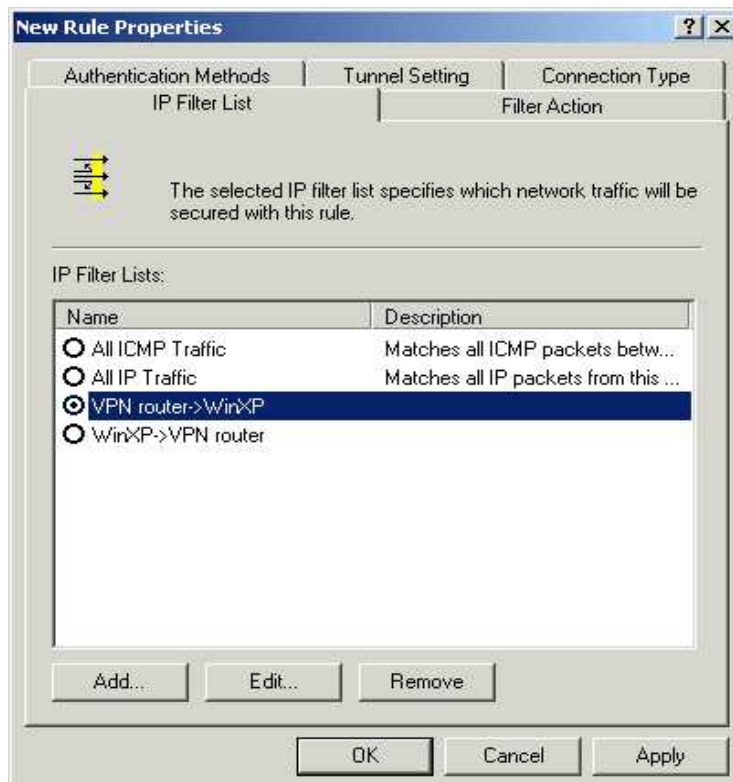
9. Type an appropriate name "VPN router→WinXP" for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.



- In the **Source address** area, click **A specific IP Subnet**, and fill in the **IP Address** “192.168.1.0” and **Subnet mask** “255.255.255.0” to reflect NetA.
- In the **Destination address** area, click **My IP Address**.



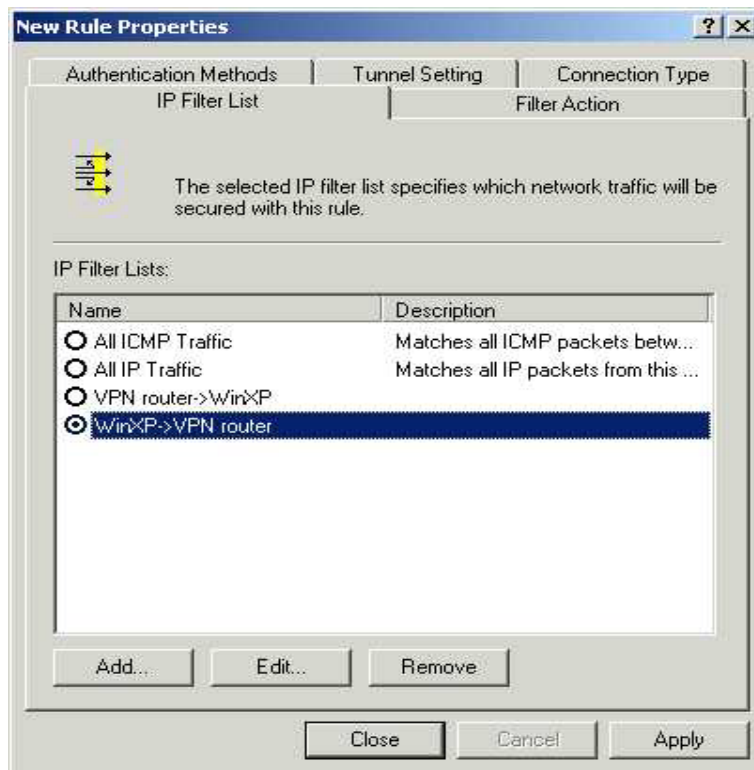
- If you want to type a description for your filter, click the **Description** tab.
- Click **OK**, and then click **Close**.



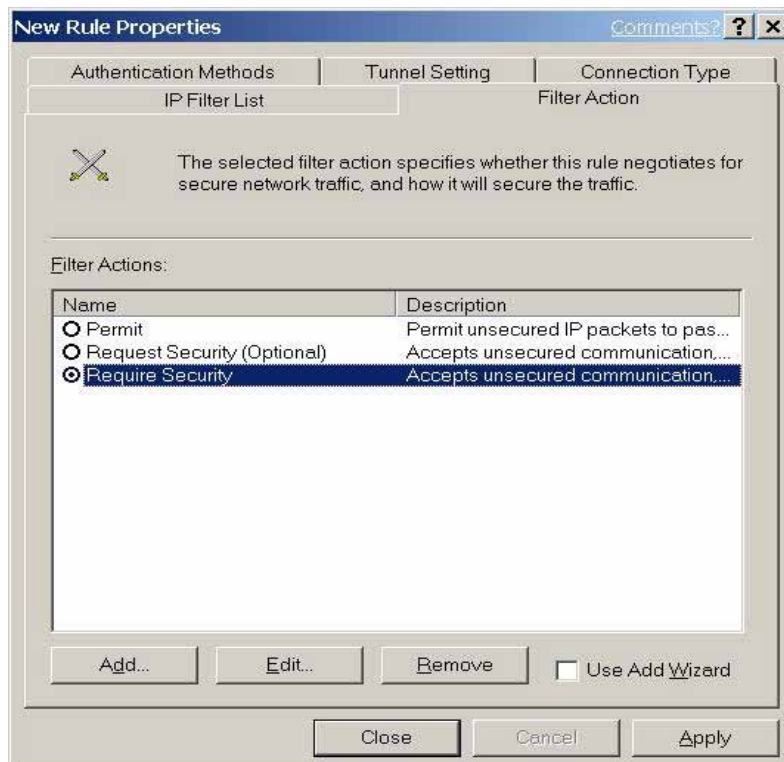
## Configure Individual Rule of 2 Tunnels.

Tunnel 1: WinXP→VPN router

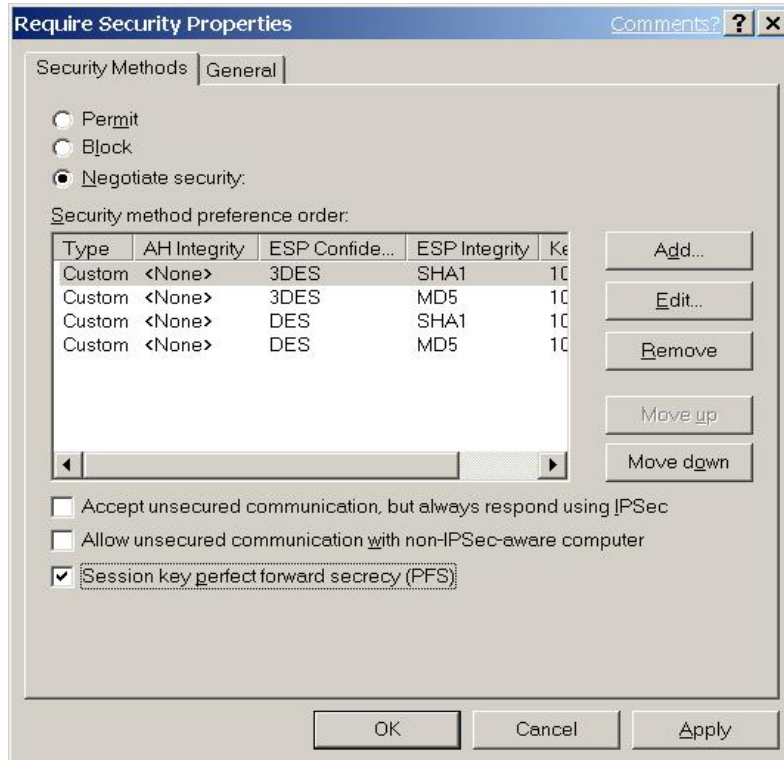
1. On the **IP Filter List** tab, click the filter list "**WinXP→VPN router**".



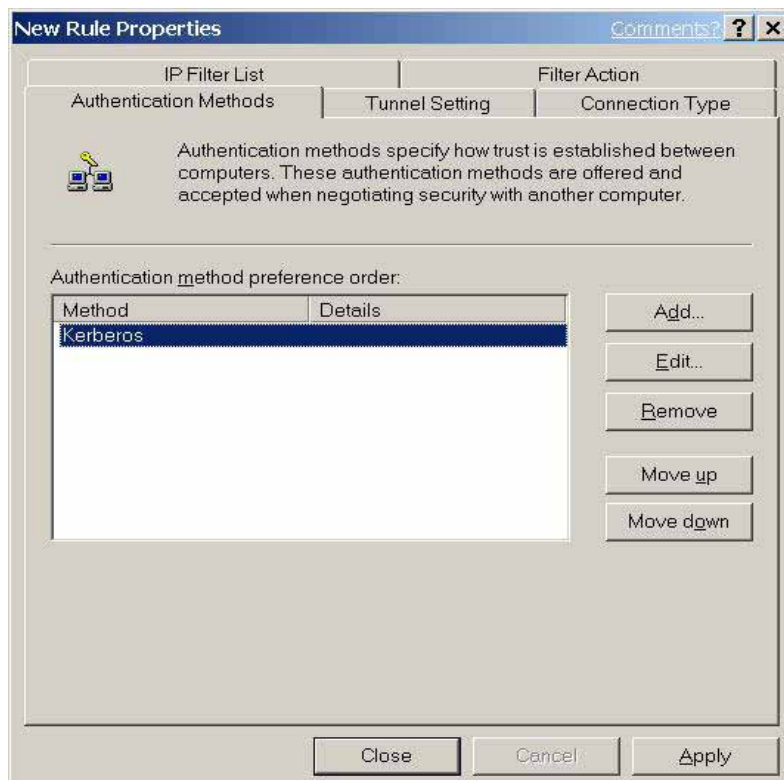
2. On the **Filter Action** tab, click the filter action "**Require Security**", and click **Edit**.



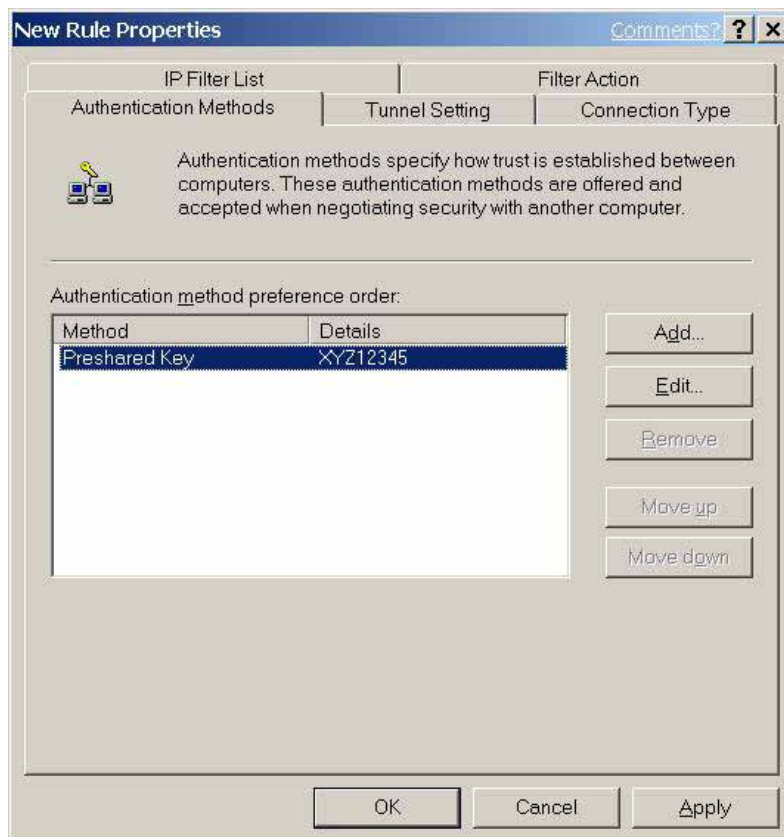
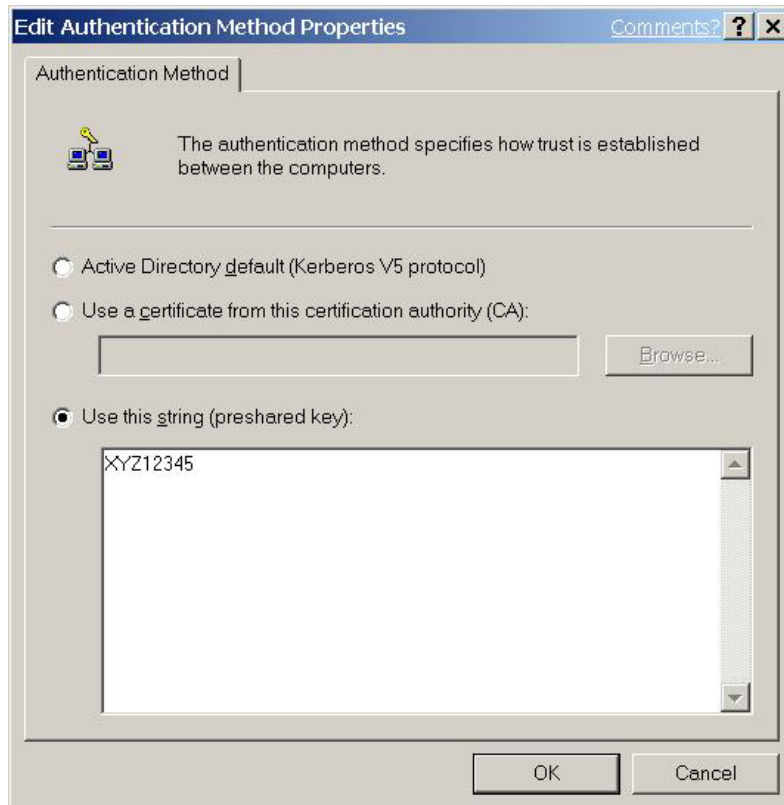
- Keep the **Negotiate security** option enabled, and click to clear the **Accept unsecured communication**, but always respond using IPsec check box.
- You can check the **Session key perfect forward secrecy (PFS)** or not, if you checked it, remember to check the **PFS** option on the **BEFVP41**, and then click **OK**.



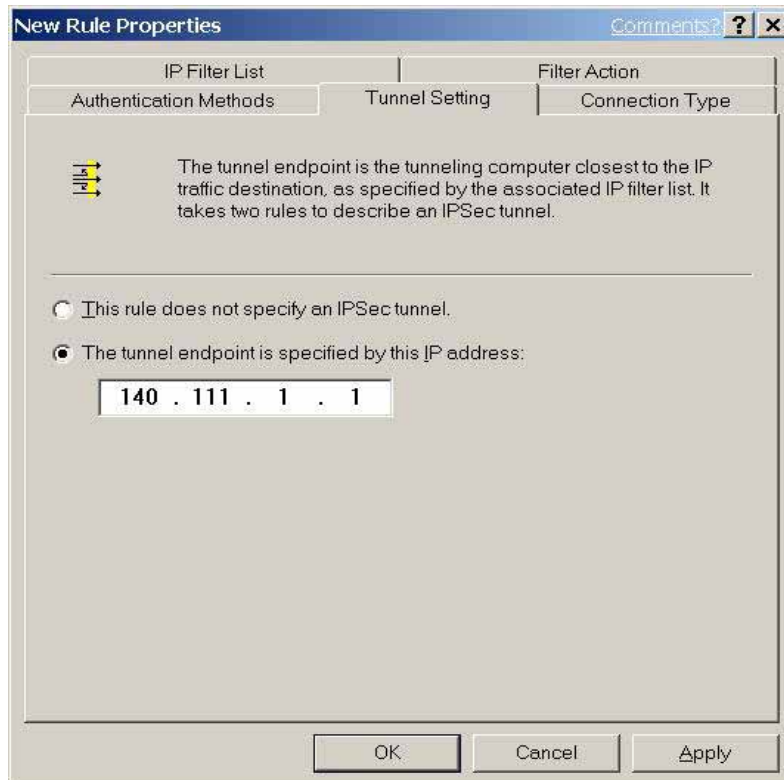
- On the **Authentication Methods** tab, click **Edit**.



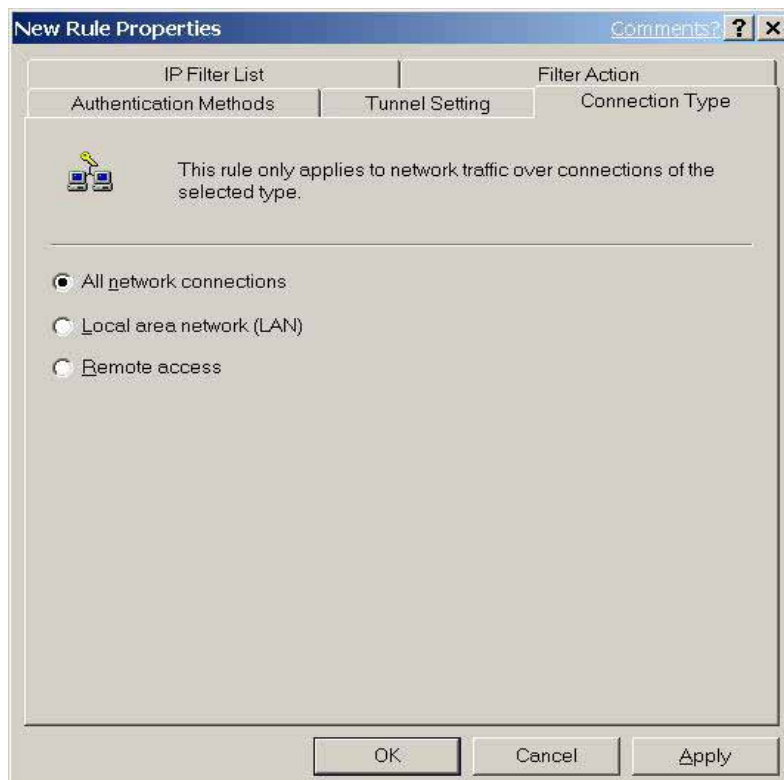
6. Change the authentication method to **“Use this string (preshared key)”**, enter the string **“XYZ12345”**, and then click **OK**.



7. On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the WAN IP Address “140.111.1.1” of VPN router.

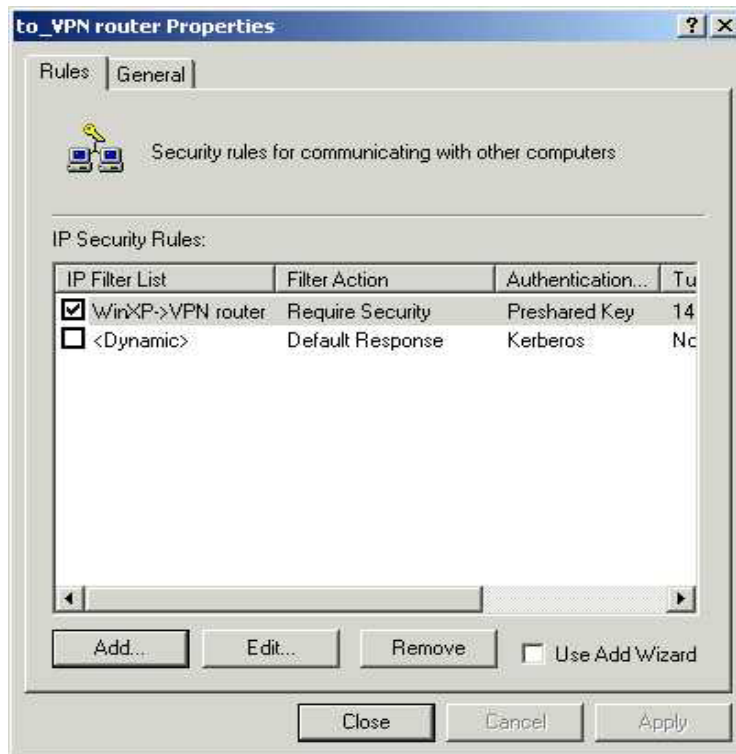


8. On the **Connection Type** tab, click **All network connections**, and then click **OK** to finish this rule.

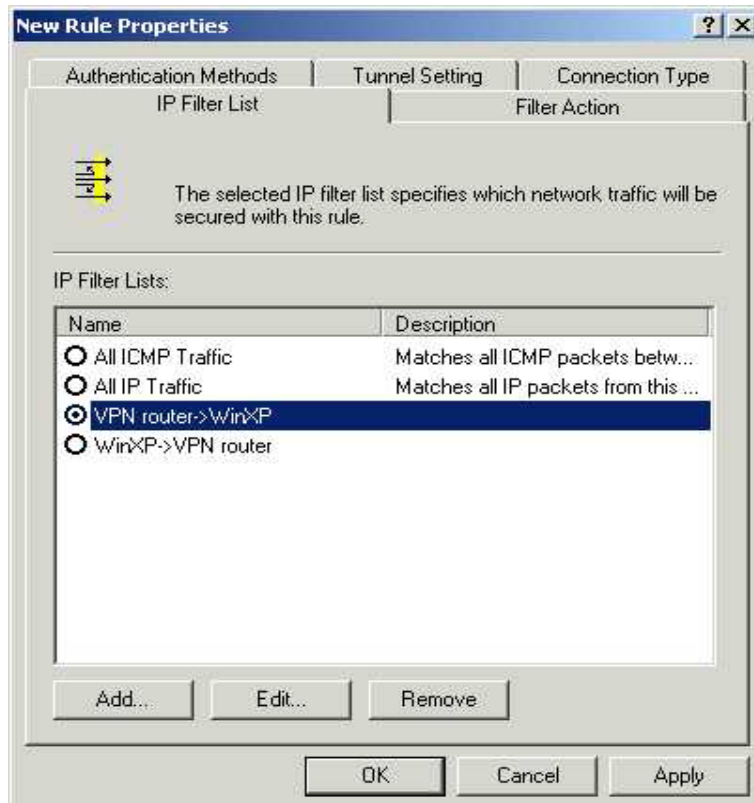


## Tunnel 2: VPN router→WinXP

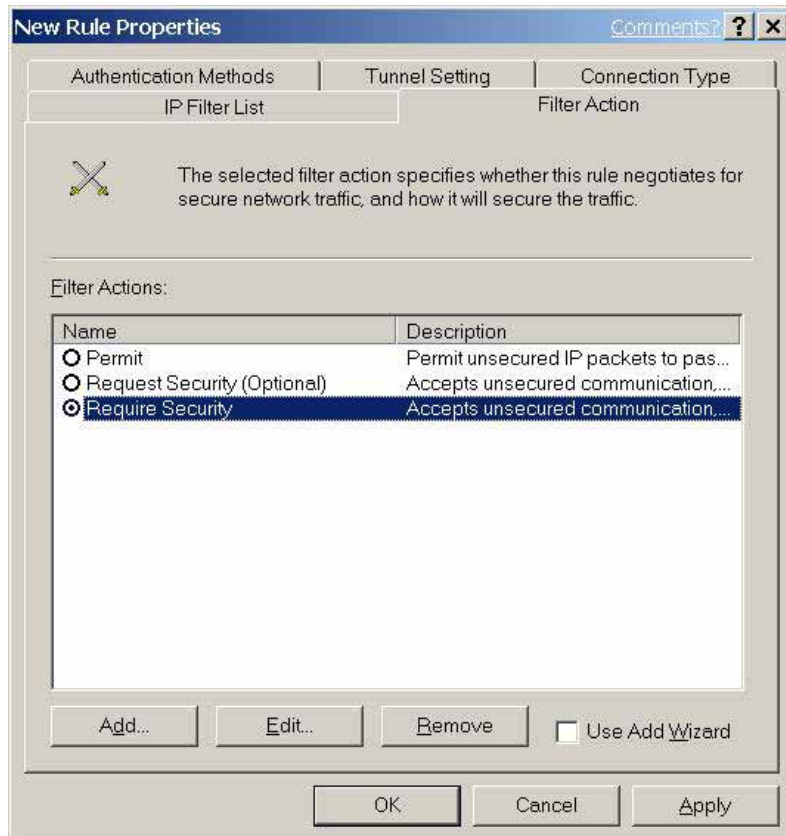
9. In the new policy properties, click to clear the **Use Add Wizard** check box, and then click **Add** to create the other one.



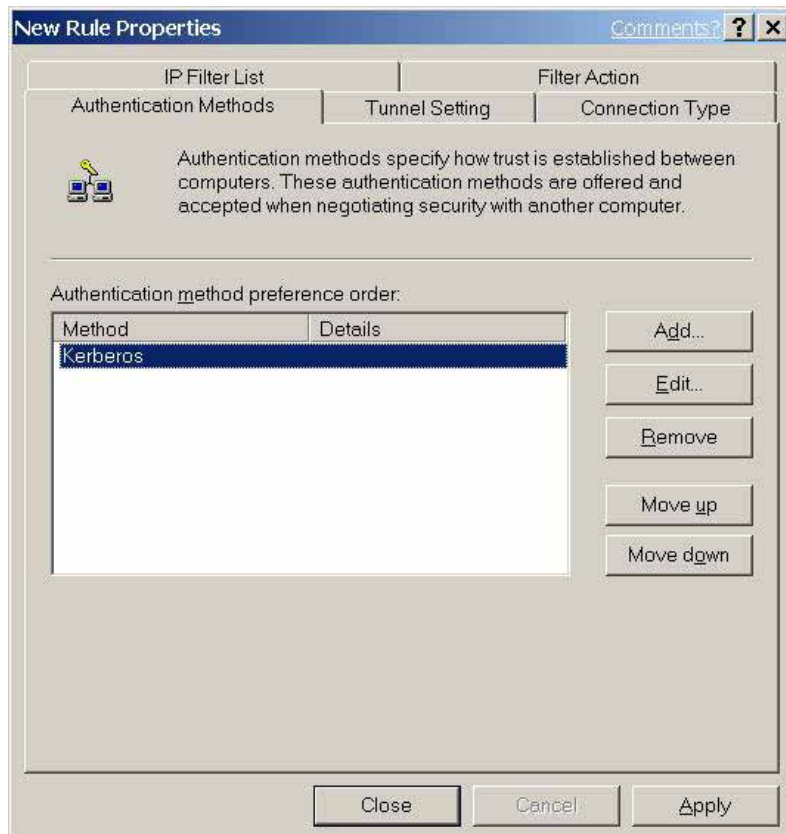
10. On the **IP Filter List** tab, click the filter list "**VPN router→WinXP**".



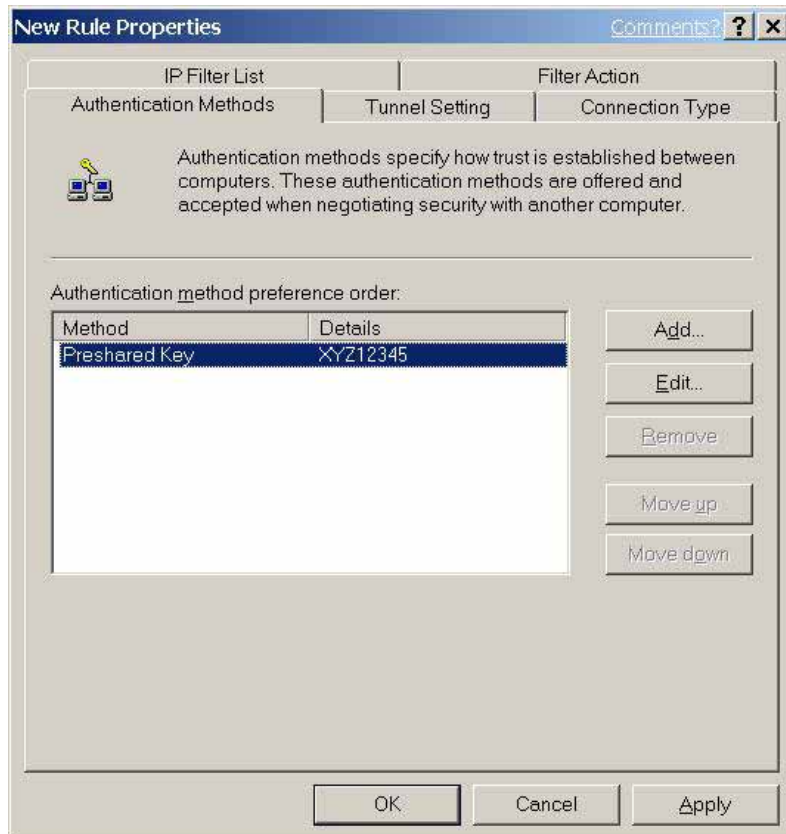
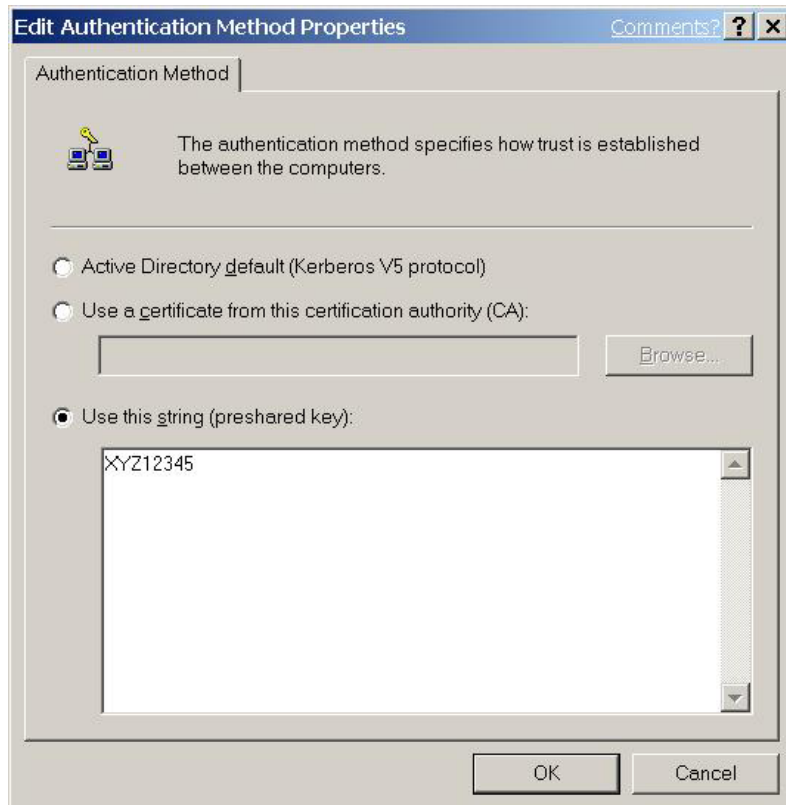
11. On the **Filter Action** tab, click the filter action “**Require Security**” (no need to edit again).



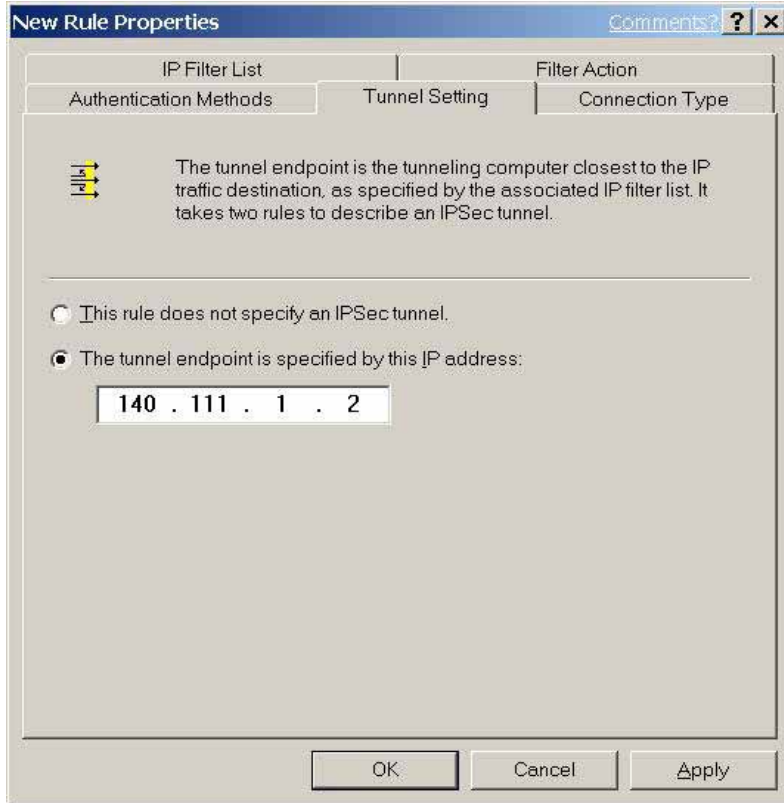
12. On the **Authentication Methods** tab, click **Edit**.



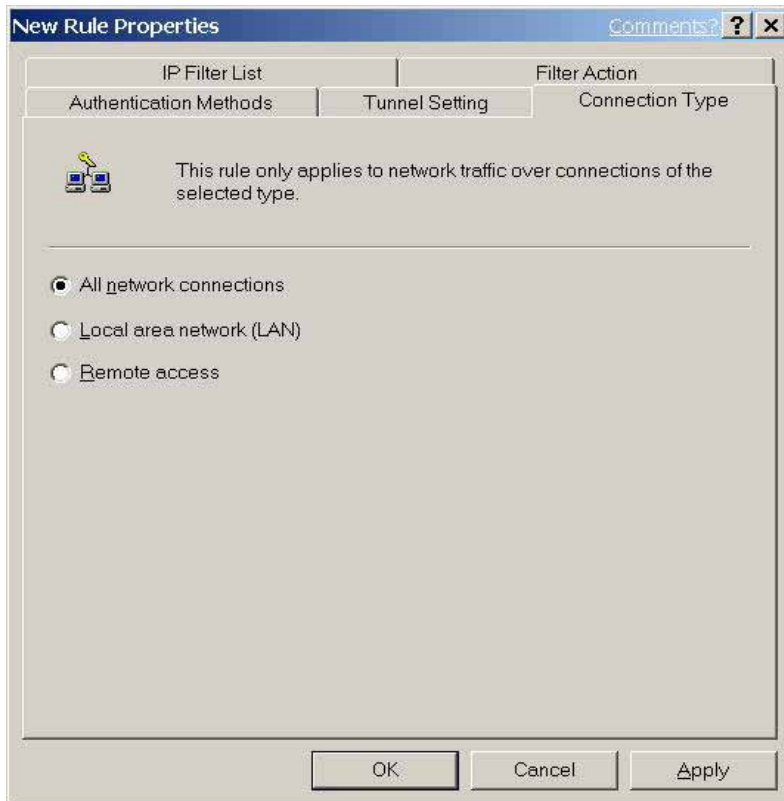
13. Change the authentication method to **“Use this string (preshared key)”**, enter the string **“XYZ12345”**, and then click **OK**.



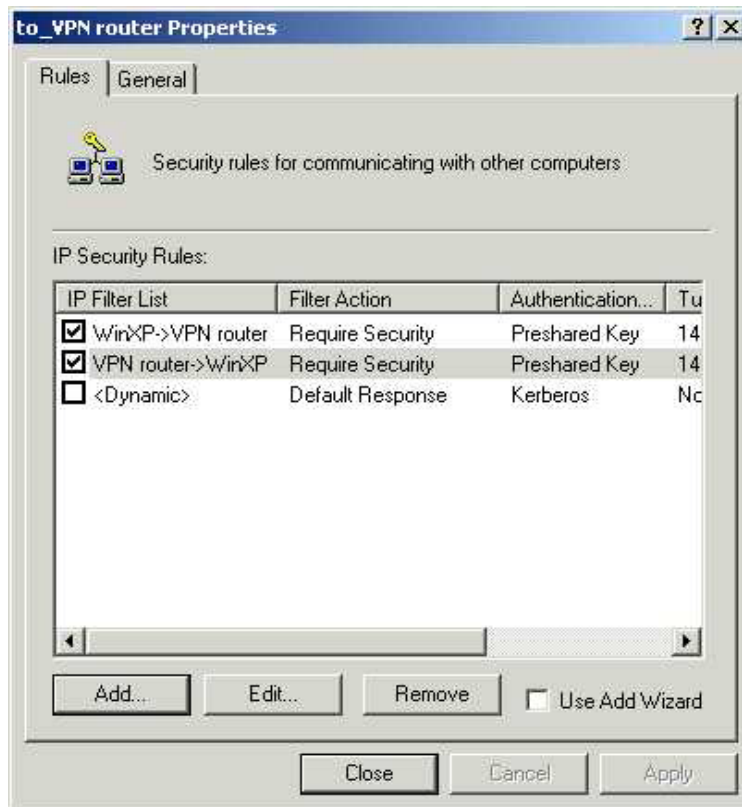
14. On the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the IP Address “**140.111.1.2**” of Windows XP.



15. On the **Connection Type** tab, click **All network connections**, and then click **OK** to finish .

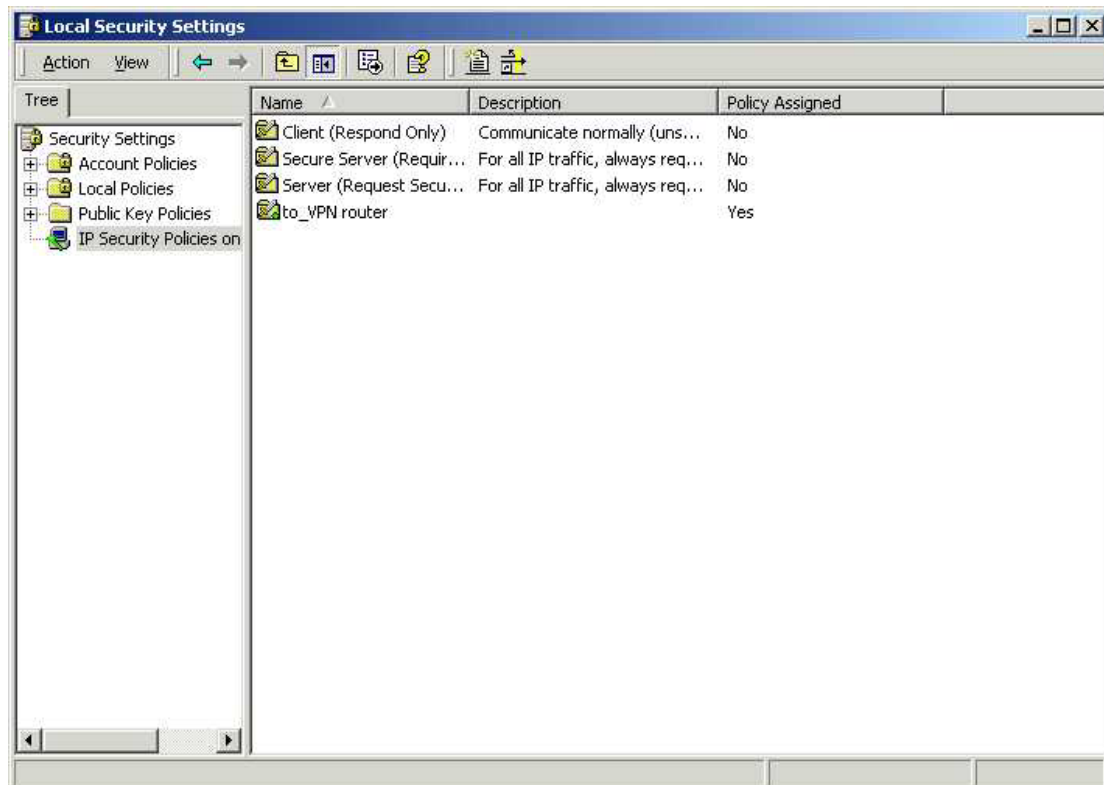


16. Click **OK**.



## Assign New IPsec Policy

1. In the **IP Security Policies on Local Computer** MMC snap-in, right-click policy named **"to\_VPN router"**, and then click **Assign**. A green arrow appears in the folder icon.



[VPN router]  
- OnePage Setup Screen

**Main Menu**

- OnePage Setup

**Advanced**

- Firewall
- VPN
- DHCP Settings
- Web Control
- ToD Control
- Access Control
- Virtual Server
- Special Application
- DMZ Host
- Dynamic Routing
- Static Routing
- DDNS

**Management**

- Device Admin.
- Status Monitor
- Log
- Backup & Restore
- Upgrade Firmware
- Diagnostic-Ping/Tracert

Log Out

## OnePage Setup

**Host Name:**  (Required by some ISPs)

**Domain Name:**  (Required by some ISPs)

**Time Zone:** (GMT+08:00) Singapore, Taiwan, Russia

**Private IP Address** (MAC Address: 00-00-00-11-11-14)

**Device IP Address:** 192 . 168 . 1 . 1

**Subnet Mask:** 255.255.255.0

**WAN Connection Type:** Static IP

Select the Internet connection type you wish to use

**Specify WAN IP Address:** 140 . 111 . 1 . 1

**Subnet Mask:** 255 . 255 . 255 . 0

**Default Gateway Address:** 140 . 111 . 1 . 2

**DNS(Required) 1:** 168 . 95 . 1 . 1

**DNS 2:** 0 . 0 . 0 . 0

**DNS 3:** 0 . 0 . 0 . 0

Apply    Cancel

- VPN Setting Screen

**Main Menu**

- OnePage Setup

**Advanced**

- Firewall
- VPN
- DHCP Settings
- Web Control
- ToD Control
- Access Control
- Virtual Server
- Special Application
- DMZ Host
- Dynamic Routing
- Static Routing
- DDNS

**Management**

- Device Admin.
- Status Monitor
- Log
- Backup & Restore
- Upgrade Firmware
- Diagnostic-Ping/Tracert

Log Out

## VPN Settings

Tunnel 1 (to\_win2k) (Select Tunnel entry)

Delete This Tunnel    Summary

**This Tunnel:**  Enable  Disable

**Tunnel Name:** to\_win2k

**Local Secure Group:** Subnet: IP: 192 . 168 . 1 . 0    Mask: 255.255.255.0

**Remote Secure Group:** IP Addr.: IP: 140 . 111 . 1 . 2

**Remote Security Gateway:** IP Addr.: IP: 140 . 111 . 1 . 2

**Encryption:**  DES  3DES  Disable

**Authentication:**  MD5  SHA  Disable

**Key Management:** Auto. (IKE)

PFS (Perfect Forward Secrecy)

**Pre-shared Key:** XYZ12345 (0x58595a3132333435)

**Key Lifetime:** 3600    Sec.

**Status:** Disconnected

Connect    View Logs    Advanced Setting

## Reference

1. Microsoft Corporation, "How to Configure IPSec Tunneling in Windows 2000 (Q252735)", by <http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP>
2. Cisco Systems, Inc, "Configuring IPSec Between a Microsoft Windows 2000 Server and a Cisco Device", by <http://www.cisco.com/warp/public/707/2000.html>