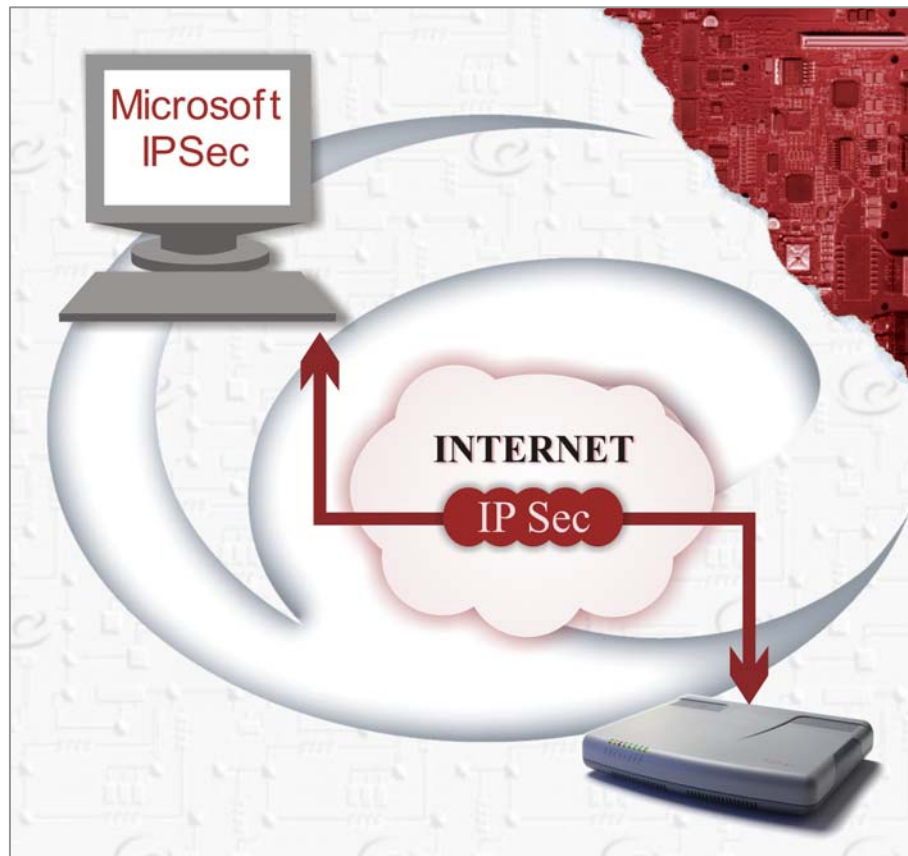

How to configure Quadro IPSec with MS IPSec



Abstract: This document describes the configuration settings for Quadro while creating VPN between Quadro and MS Windows 2000.

Table of Contents:

- 1 Introduction.....3**
- 2 How to configure.....3**
 - 2.1 Quadro IPSec ↔ MS IPSec3
 - 2.2 The Windows 2000 IPSec setup.....6
- 3 Useful Links27**

1 Introduction

This document describes the configuration settings for Quadro while creating VPN between Quadro and MS Windows 2000.

2 How to configure

2.1 Quadro IPSec ↔ MS IPSec

To configure IPSec on Quadro the follow the steps below:

1. Go to **Internet Uplink**→**VPN Configuration**→**IPSec Configuration** page.
2. Add a new connection.
3. Fill in the connection name and select **Windows 2000/XP** from the Peer type drop-down list and go to the next page of the wizard.

The screenshot shows the 'IPSec Connection Wizard' interface. At the top, there is a navigation menu with tabs: Main, System, Users, Telephony, Internet Uplink, and LAN Services. The 'Internet Uplink' tab is selected. In the top right corner, the Epygi logo and 'TQuadro225' are visible. The main heading is 'IPSec Connection Wizard'. Below this, there is a section titled 'Add IPsec Connection'. This section contains three input fields: 'Connection Name' with the value 'Quadro_MSWin2k', 'Peer type' with a dropdown menu showing 'Windows 2000/XP', and 'VPN Network Topology' with a dropdown menu showing 'Quadro<->Peer'. At the bottom of the wizard, there are four buttons: 'Previous', 'Next', 'Cancel', and 'Help'.

Figure 1

- 4. The basic parameters are already set on this page. Enter the peer's IP in the **Remote Gateway** IP Address field. MS peer should use 3DES/MD5 Keying type.

The screenshot displays the 'IPsec Connection Wizard' interface. At the top, there are navigation tabs: Main, System, Users, Telephony, Internet Uplink, and LAN Services. The Epygi logo and 'TQuadro225' are in the top right corner. The main title is 'IPsec Connection Wizard'. Below it, the specific configuration is titled 'IPsec Connection Properties - Quadro_MSWin2k'. On the left, there are two radio buttons: 'Dynamic IP / Roadwarrior' (unselected) and 'Static IP / Remote Gateway' (selected). Below this, the 'Remote Gateway' field contains the IP address '207.151.222.2'. There are four checkboxes for connection types: 'Quadro <-> Remote Gateway' (unchecked), 'Local Subnet <-> Remote Gateway' (checked), 'Quadro <-> Remote Subnet' (unchecked), and 'Local Subnet <-> Remote Subnet' (unchecked). Below these are fields for 'Remote Subnet IP' (192.168.1.0/24) and 'Local Subnet IP' (172.168.2.0/24), each with an 'IP-Clipboard' button. At the bottom left, there is a checkbox 'Stop connection if not successful' (unchecked). On the right side, there are two sections for keying. The top section is 'Internet Key Exchange (IKE)' with 'Auto Keying' selected. It includes dropdown menus for 'Encryption' (Triple DES), 'Authentication' (MD5), and 'Diffie-Hellman Group' (Group 2 (1024 bit)). Below this is the 'Encapsulated Security Payload (ESP)' section with 'Encryption' (Triple DES) and 'Authentication' (MD5) dropdowns. The bottom section is 'Manual Keying' (unselected) with 'Encryption' (Single DES) and 'Authentication' (MD5) dropdowns. At the very bottom, there are four buttons: 'Previous', 'Next', 'Cancel', and 'Help'.

Figure 2

- 5. The same shared secret key must be used on both Quadro and MS peer sides. Also MS peer should have the same state of PFS (Perfect Forward Secrecy) as Quadro.

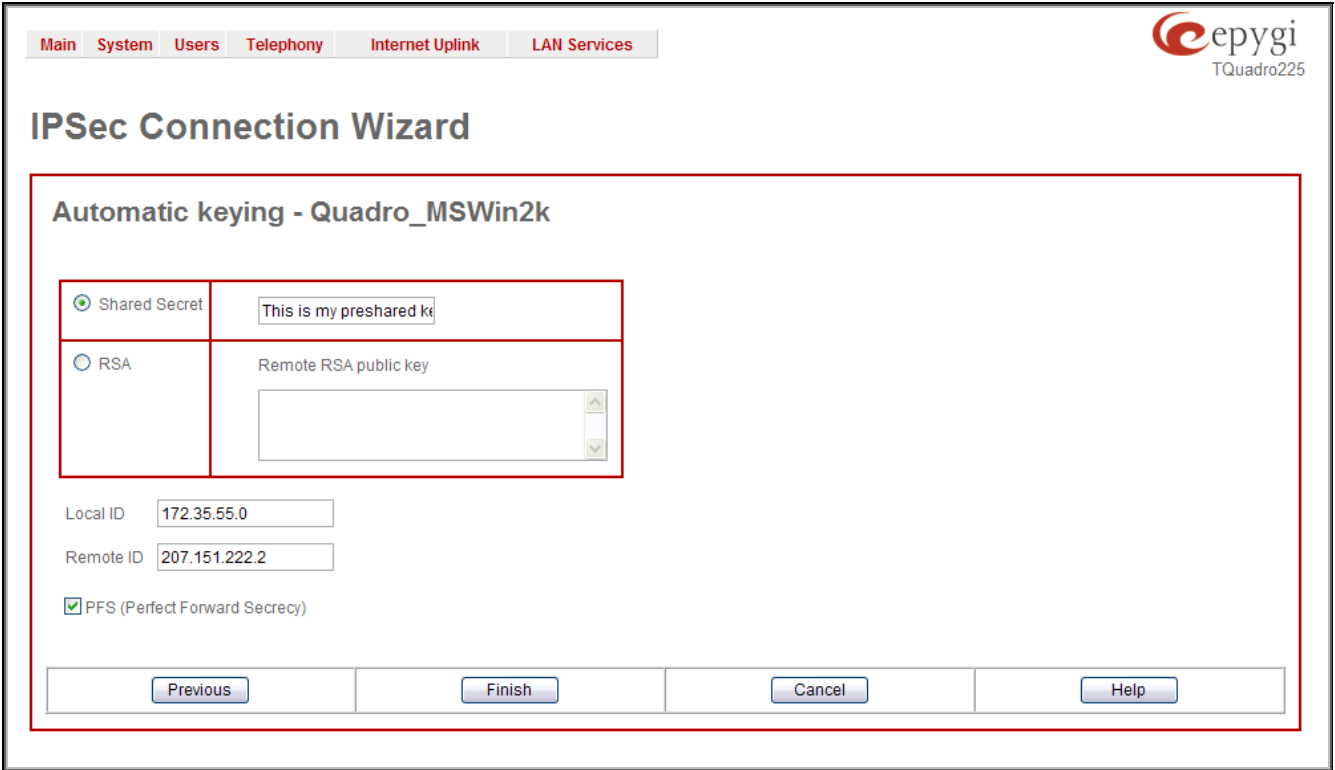


Figure 3

- 6. Press **Finish** and **Start** connection.
- 7. Configure **MS peer** and enjoy connection.

2.2 The Windows 2000 IPSec setup

1. Run MMC from **Start** ->**Run** window.

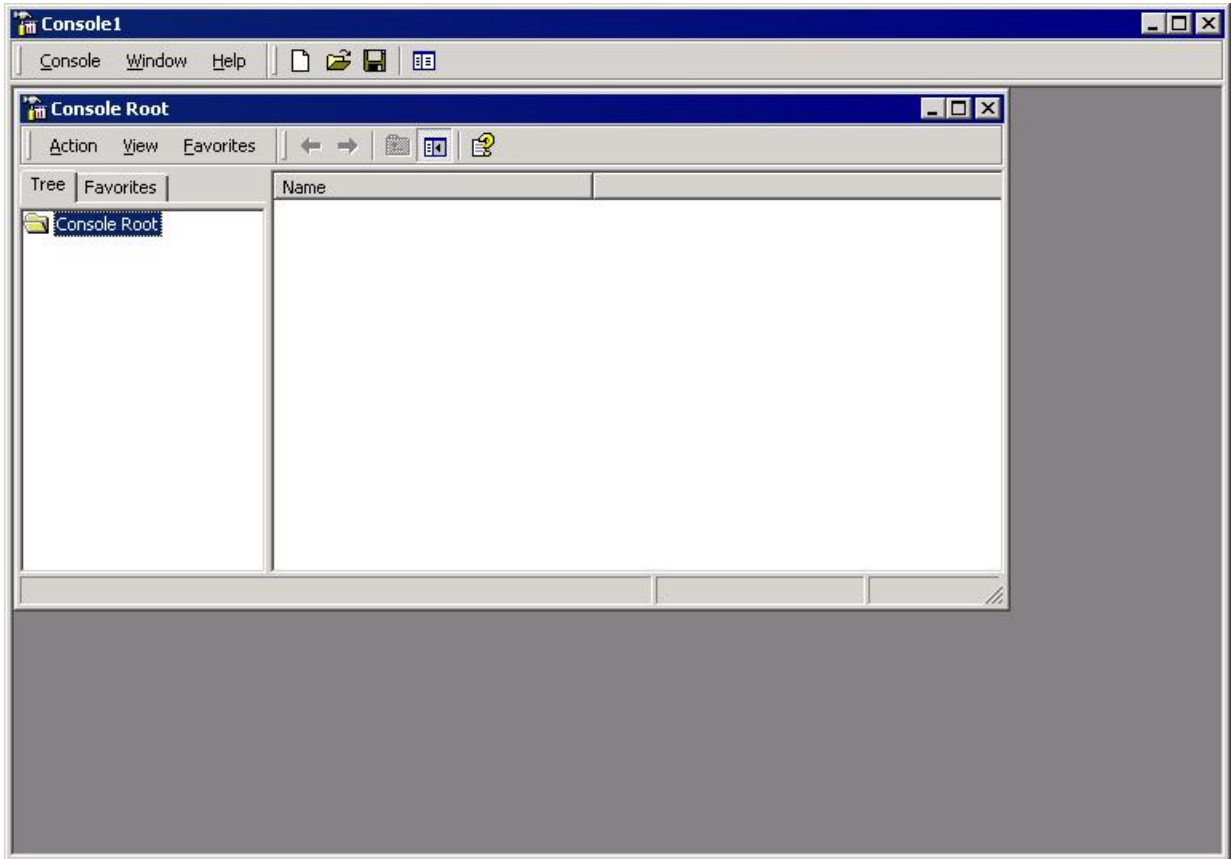


Figure 4

- 2. Go to **Console** -> **Add/Remove Snap-in**. Add **IP Security Policy Management**.

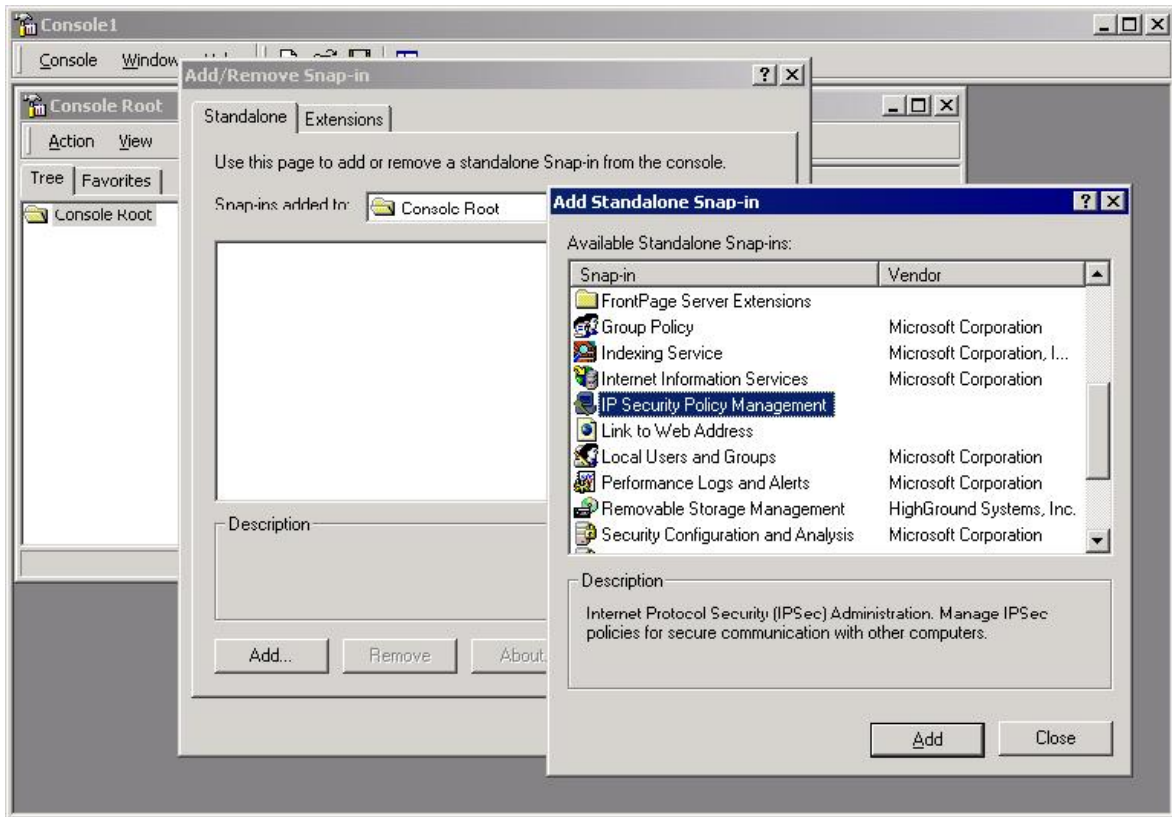


Figure 5

- 3. Choose **Local Computer** and press **Finish**.

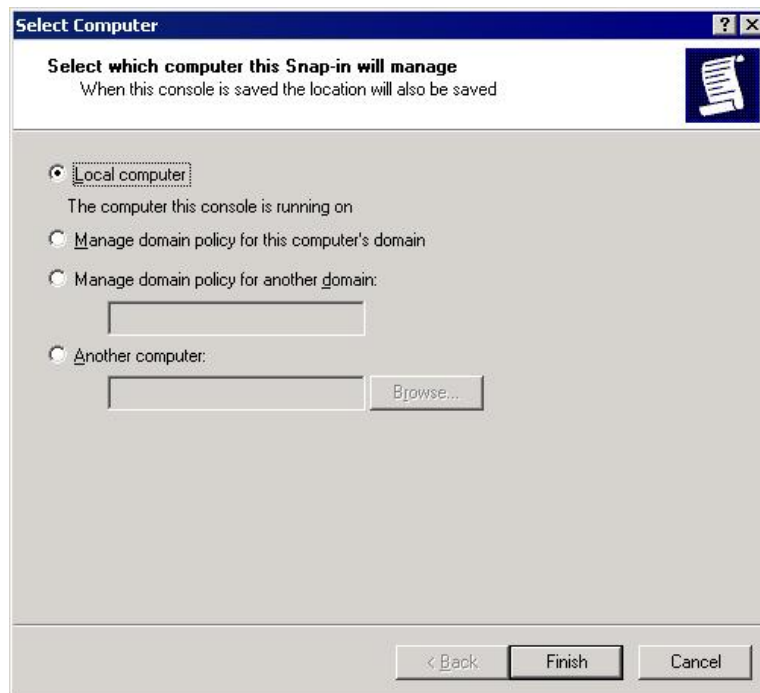


Figure 6

4. Create a new **IPSec Security Policy**.

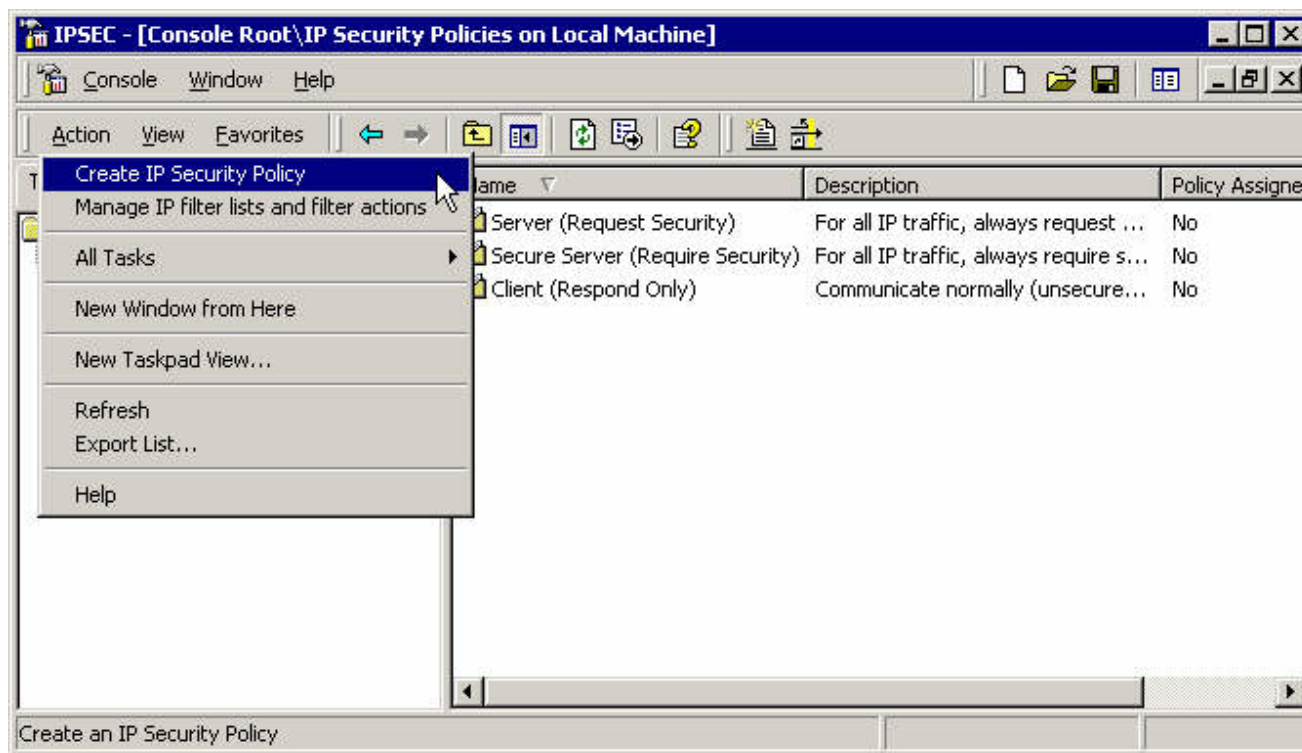


Figure 7

5. Press **Next**.



Figure 8

- 6. Enter a name for the new policy.

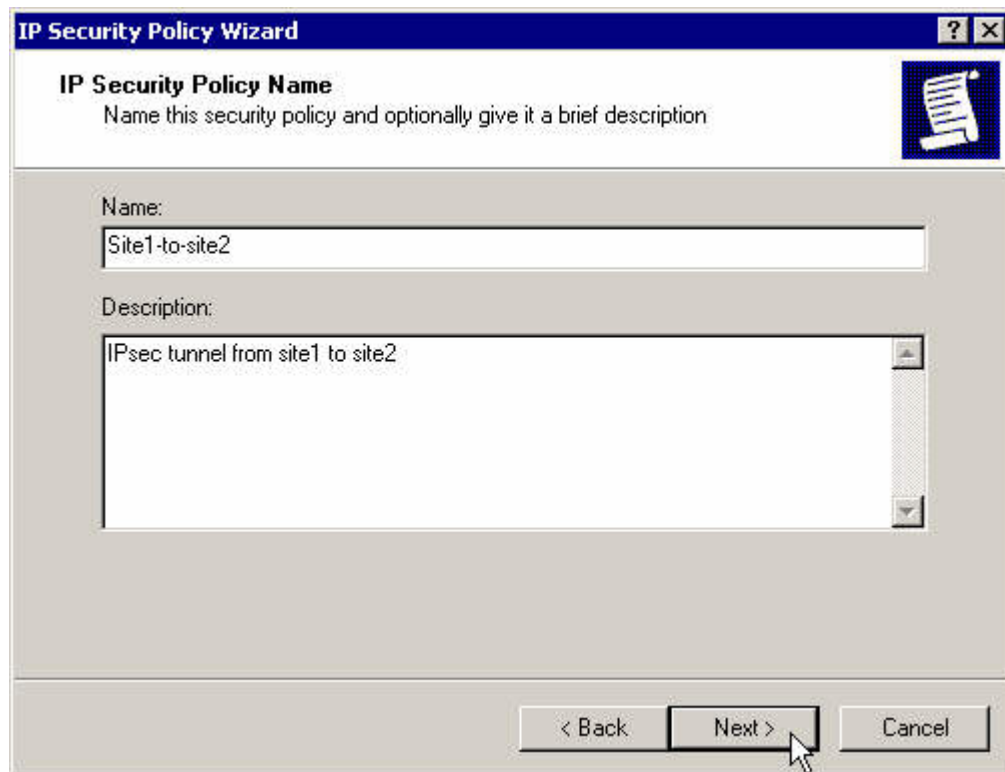


Figure 9

- 7. Deactivate the default response rule and press **Next**.

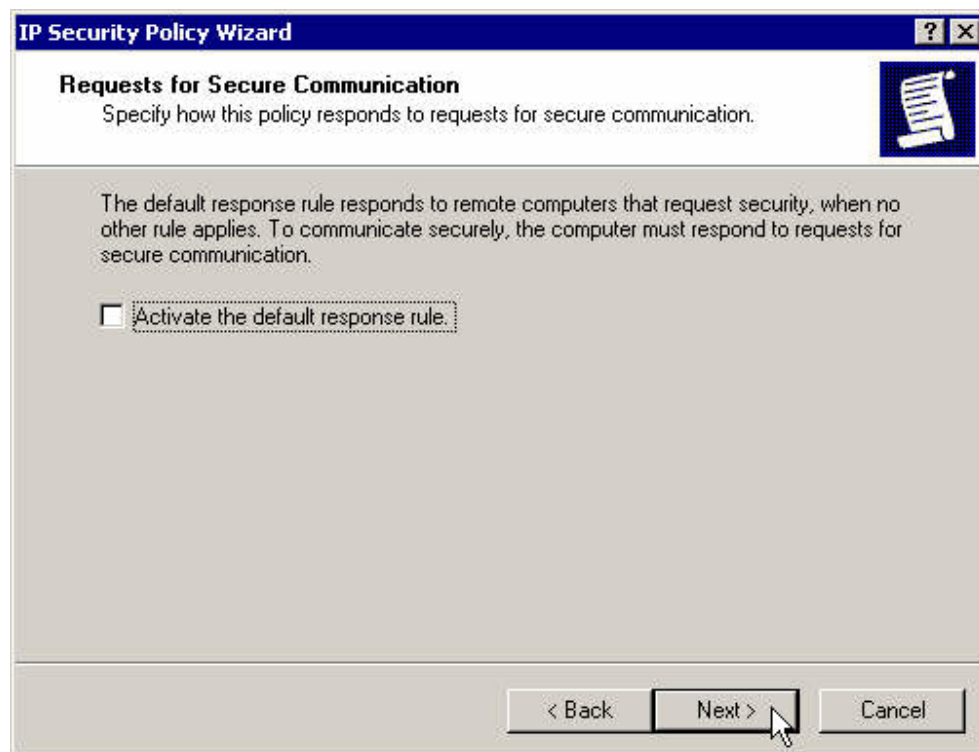


Figure 10

- 8. Click **Finish**.

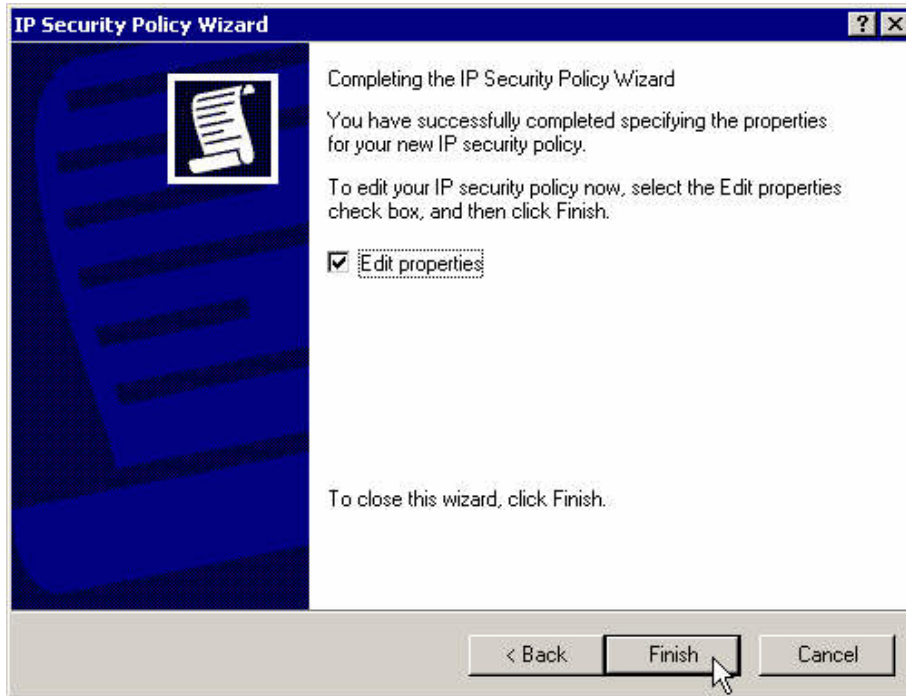


Figure 11

- 9. Create the first IP filter for the traffic from the left subnet to the right subnet. Uncheck **Use Add Wizard** checkbox.

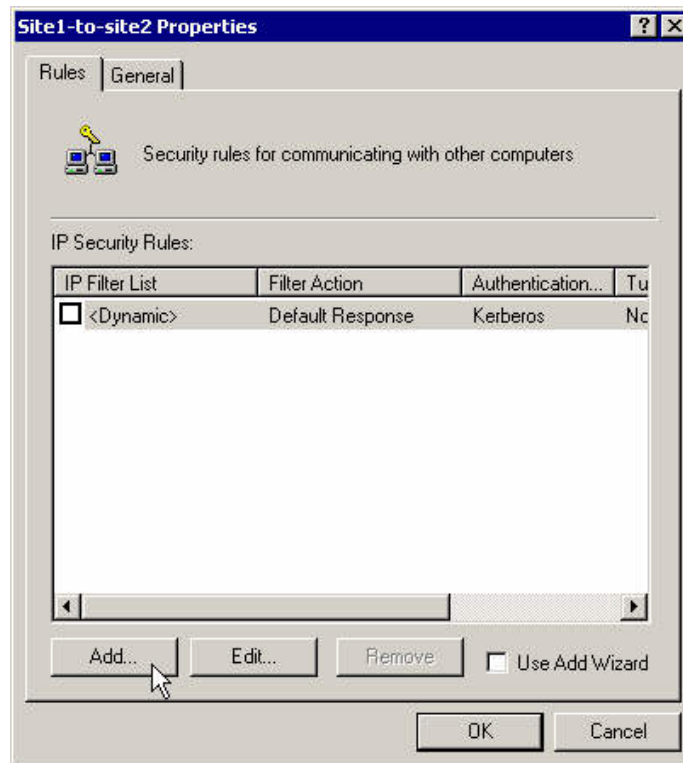


Figure 12

10. Press **Add**.

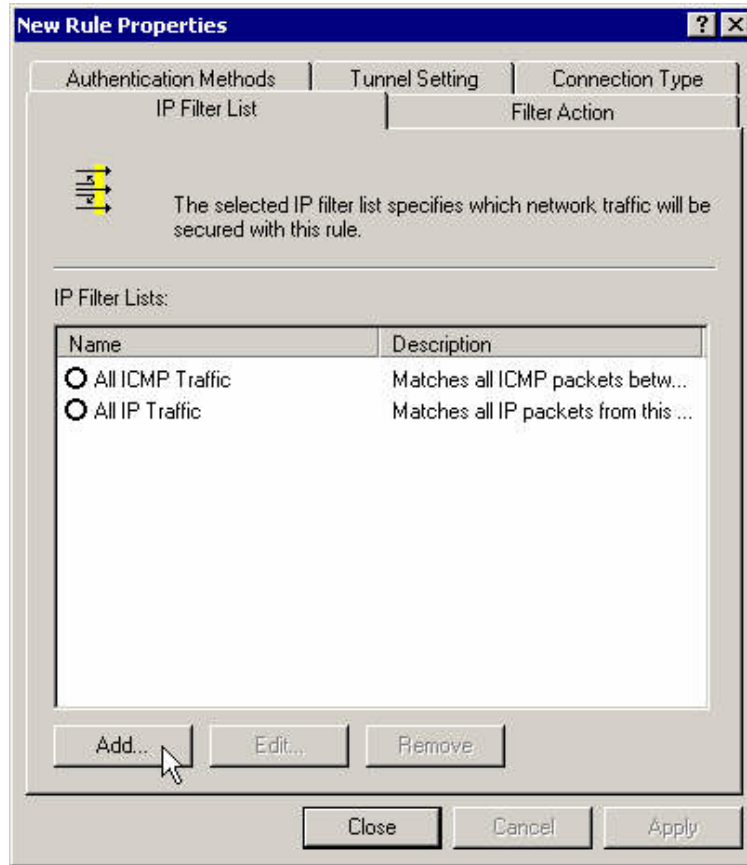


Figure 13

11. Enter a name, description and add the filter.

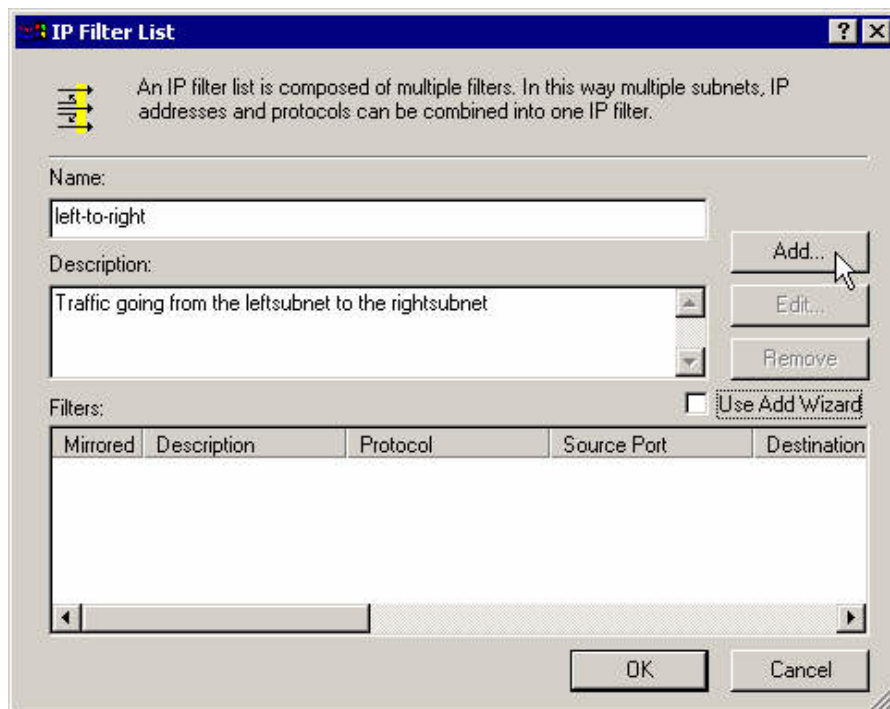


Figure 14

- Enter the left subnet as the source address and the right subnet as the destination address.

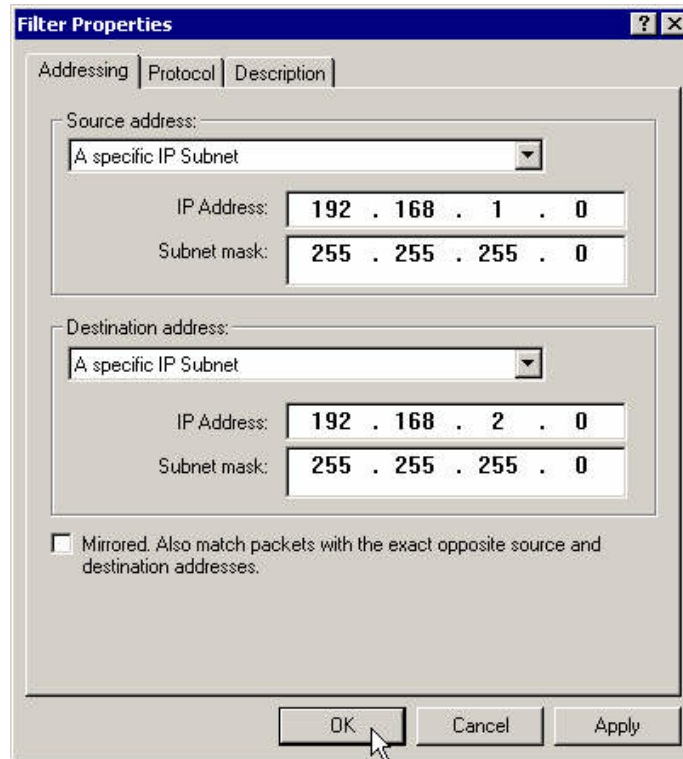


Figure 15

- Close that filter's properties box.

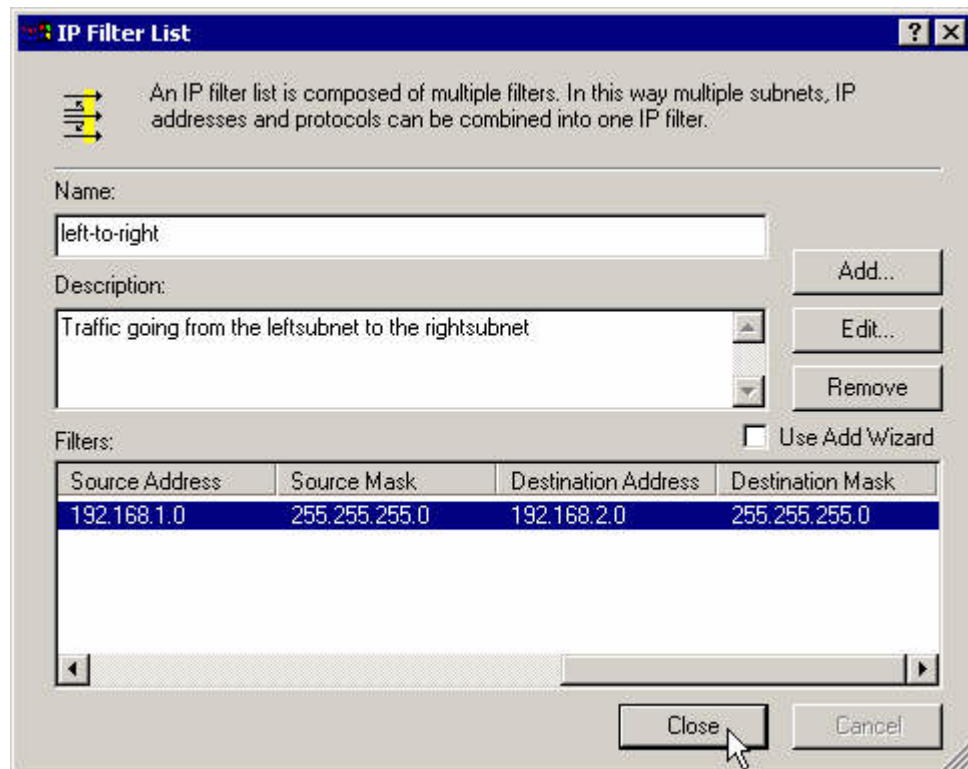


Figure 16

14. Assign the newly created filter to the current rule.

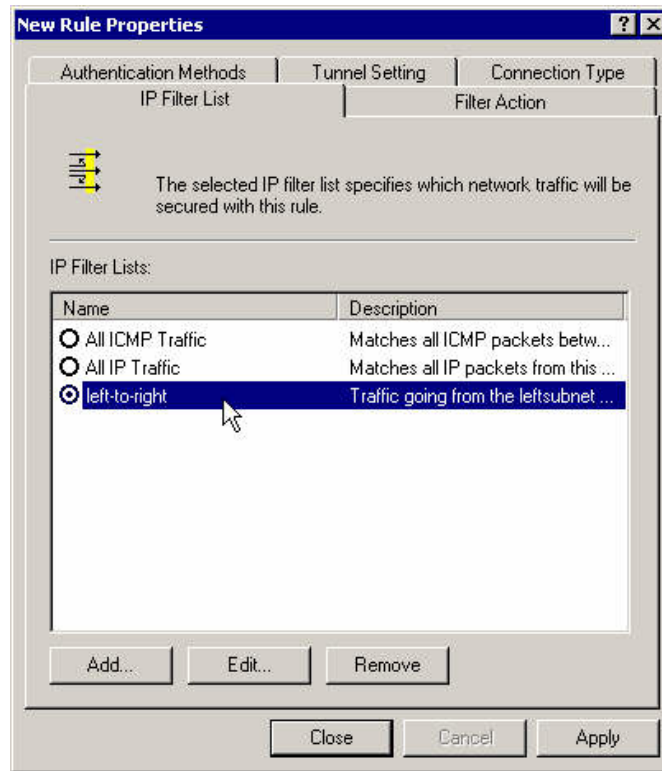


Figure 17

15. Set the filter action to the **Require Security** action.

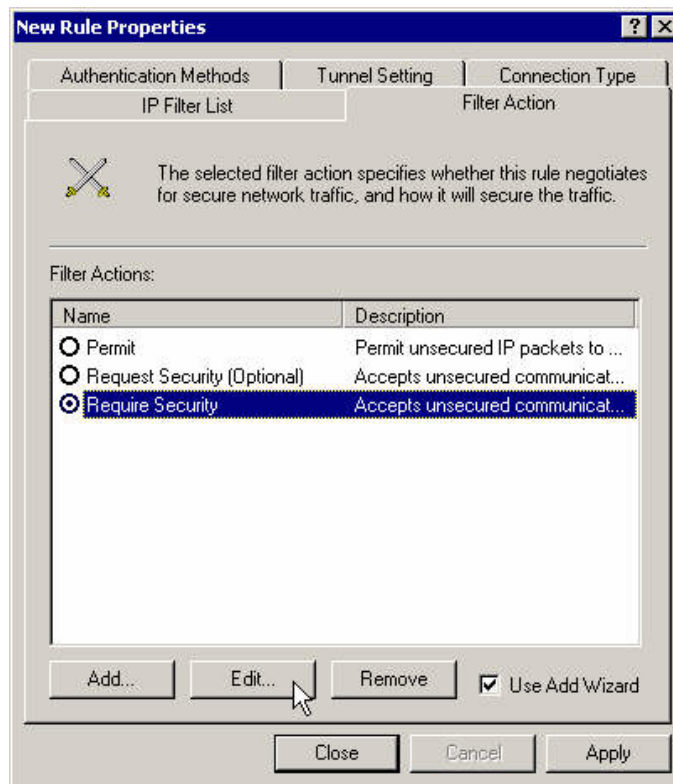


Figure 18

16. Set these action properties and move the proposal 3DES-MD5 to the top of the list. Select **Session Key Perfect Forward Secrecy** checkbox.

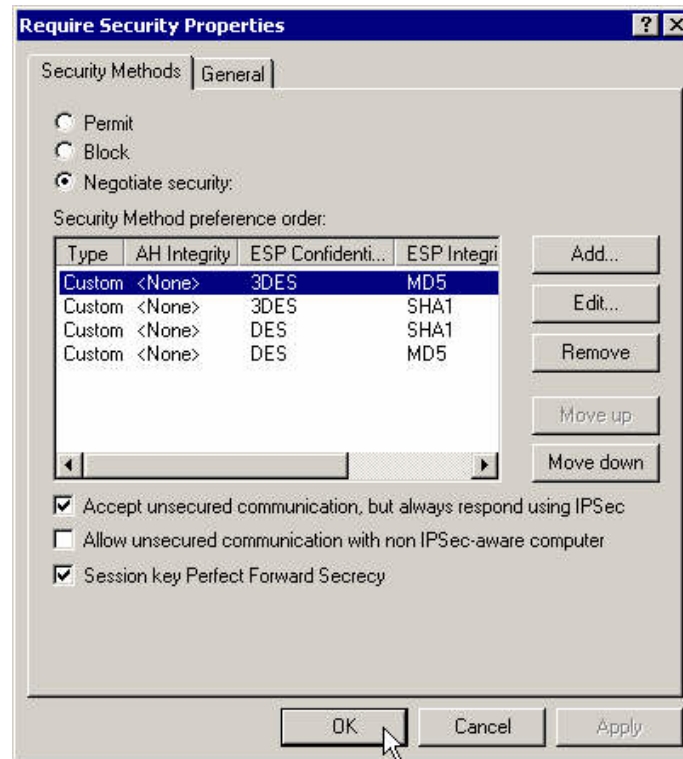


Figure 19

17. Set the connection type for LAN.

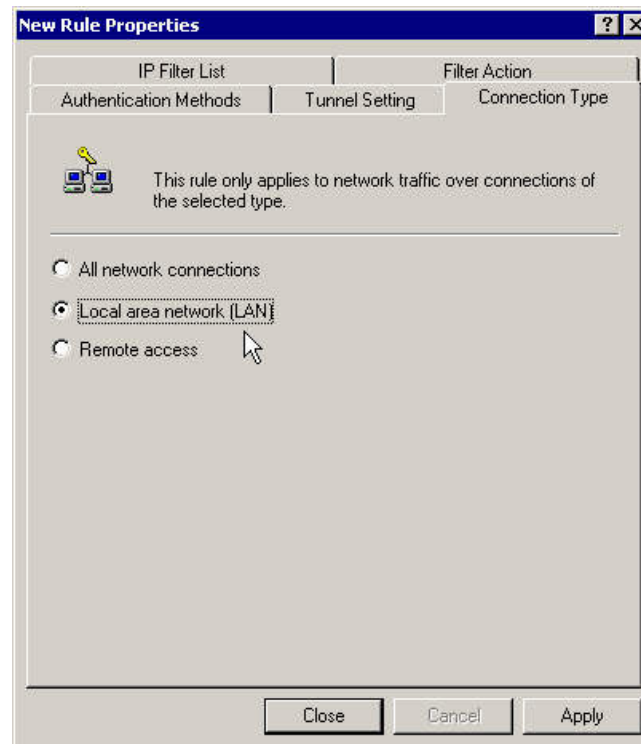


Figure 20

18. Specify the right gateway IP address.

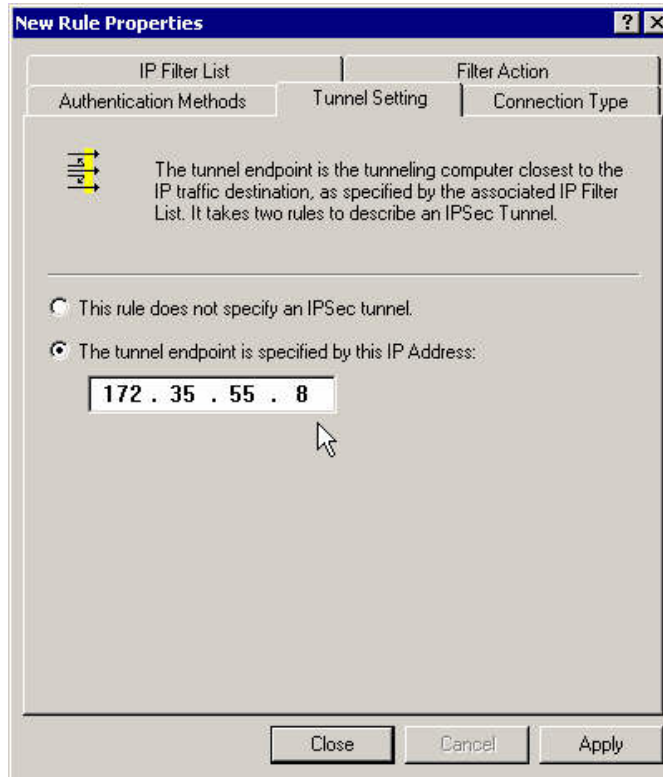


Figure 21

19. Modify the authentication method.

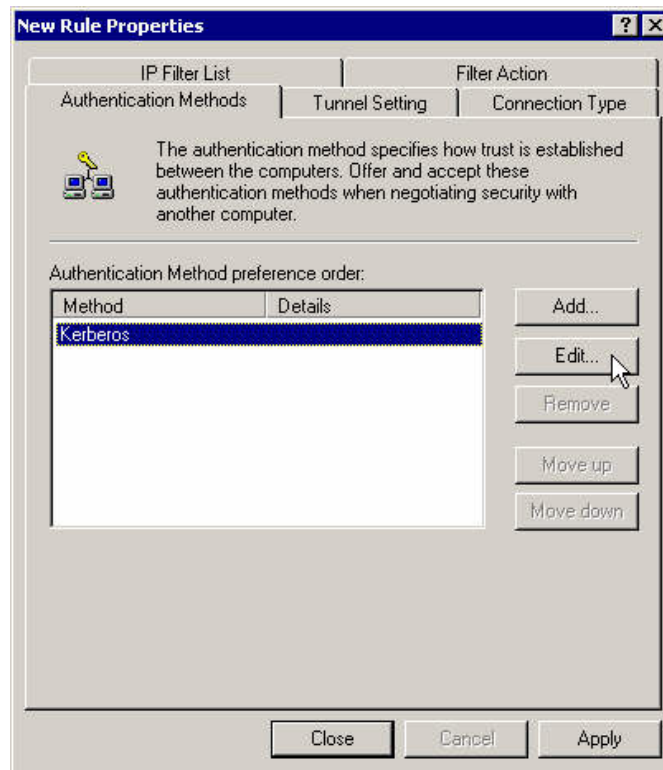


Figure 22

20. Set it to pre-shared key and enter it there.

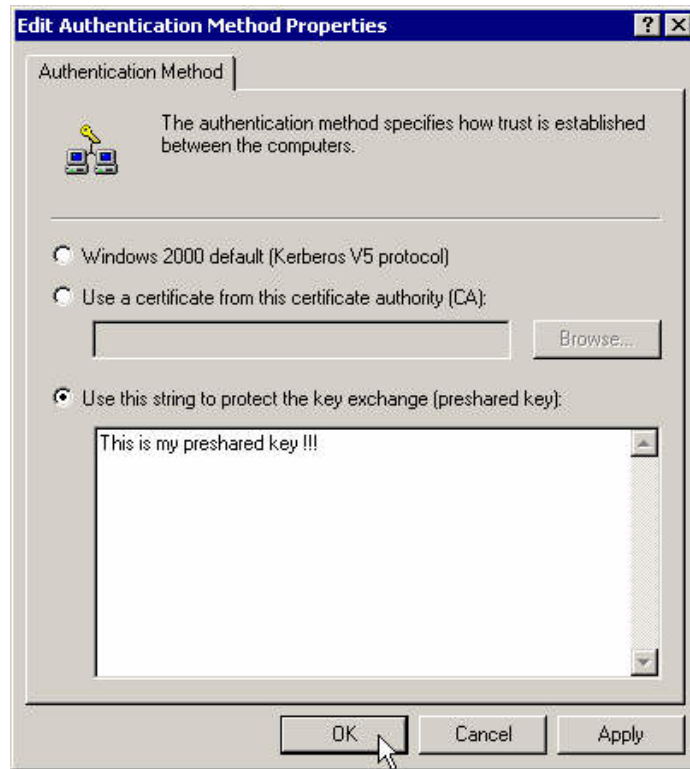


Figure 23

21. Close the first rule's properties box.

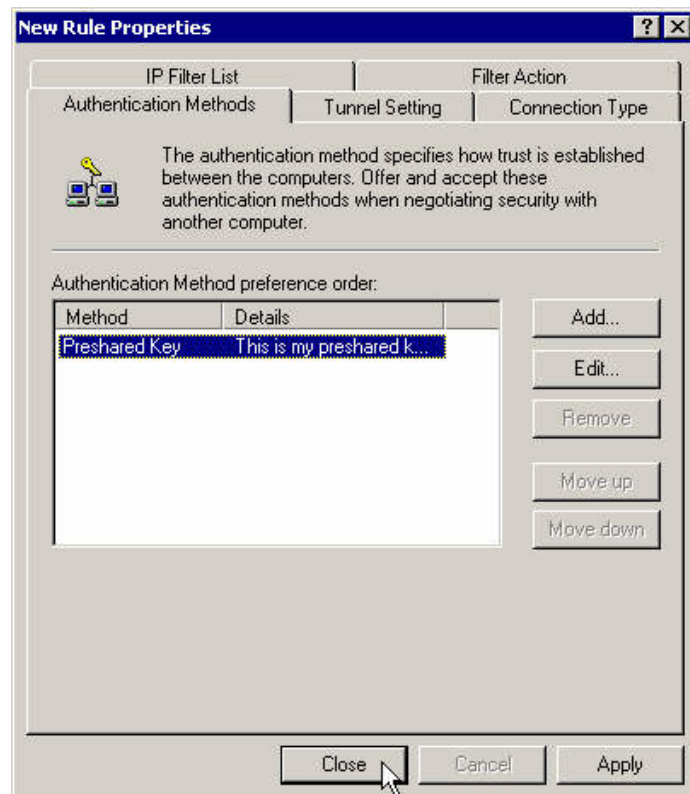


Figure 24

22. Create a second rule for the traffic from the right subnet to the left subnet.

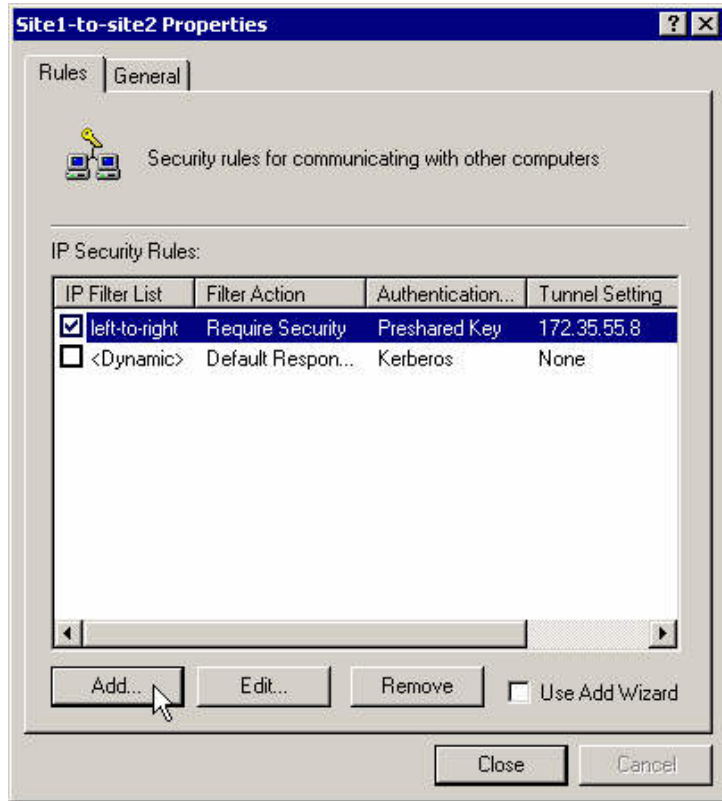


Figure 25

23. Create a new filter for that rule.

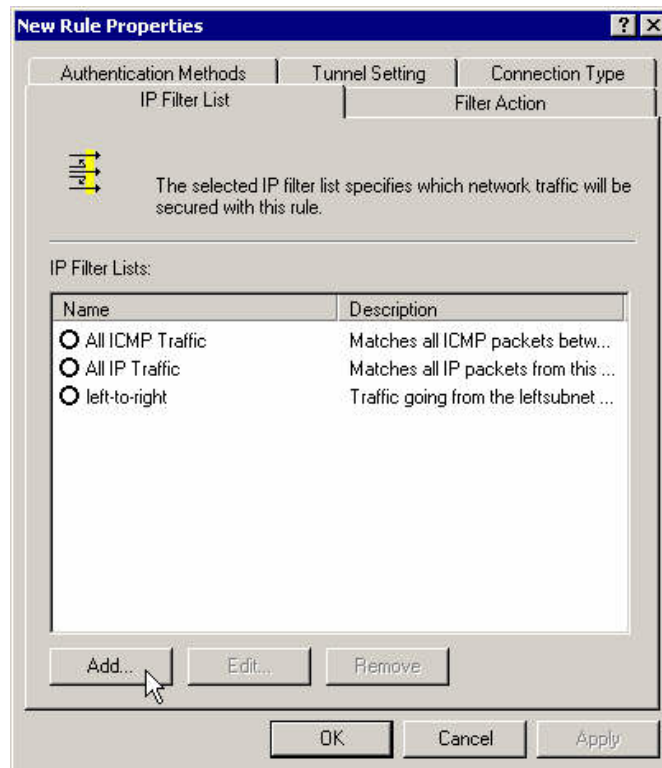


Figure 26

24. Enter a name, description and add the filter.

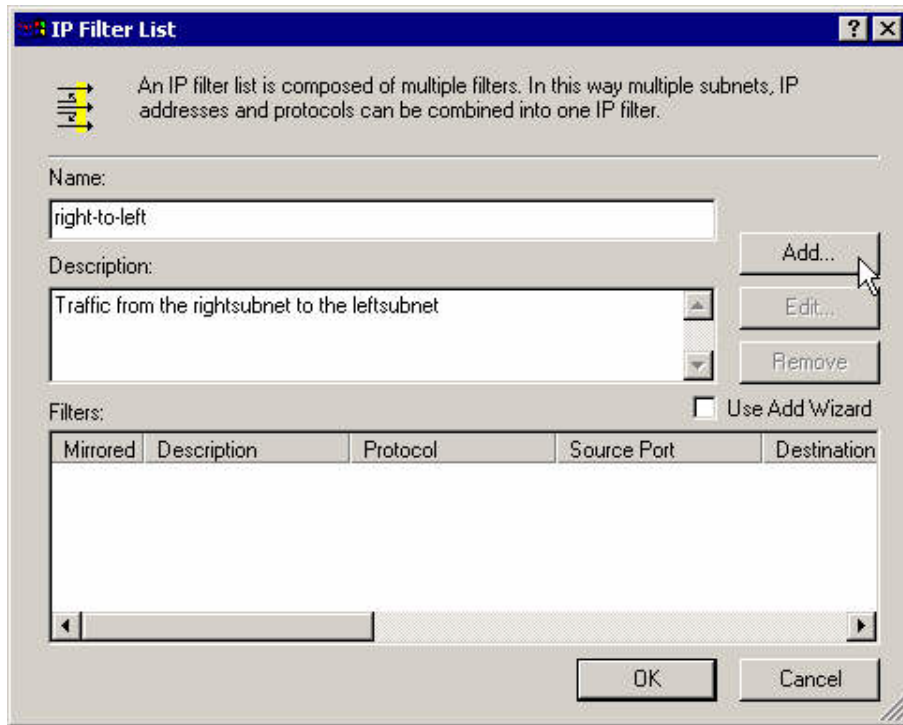


Figure 27

25. Enter the right subnet as the source address and the left subnet as the destination address.

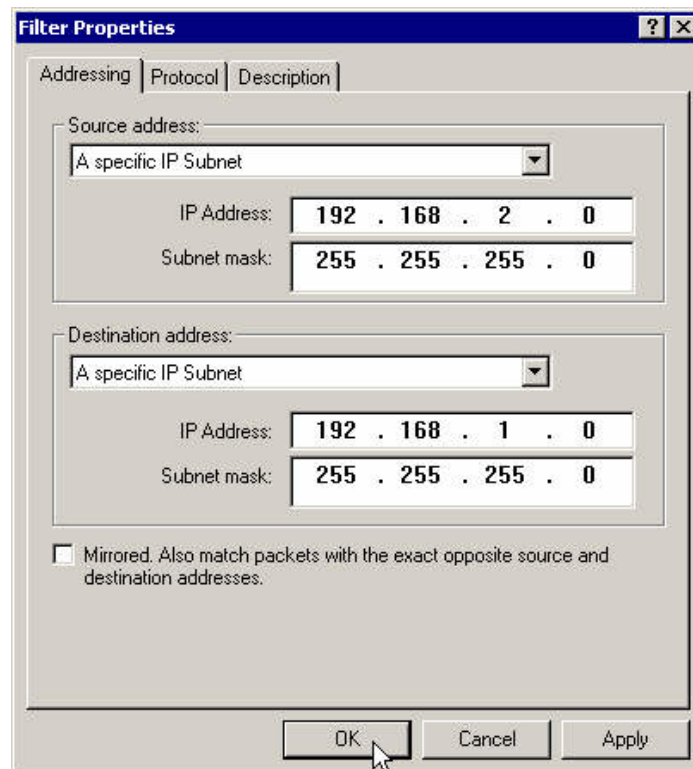


Figure 28

26. Close the IP filter's properties box.

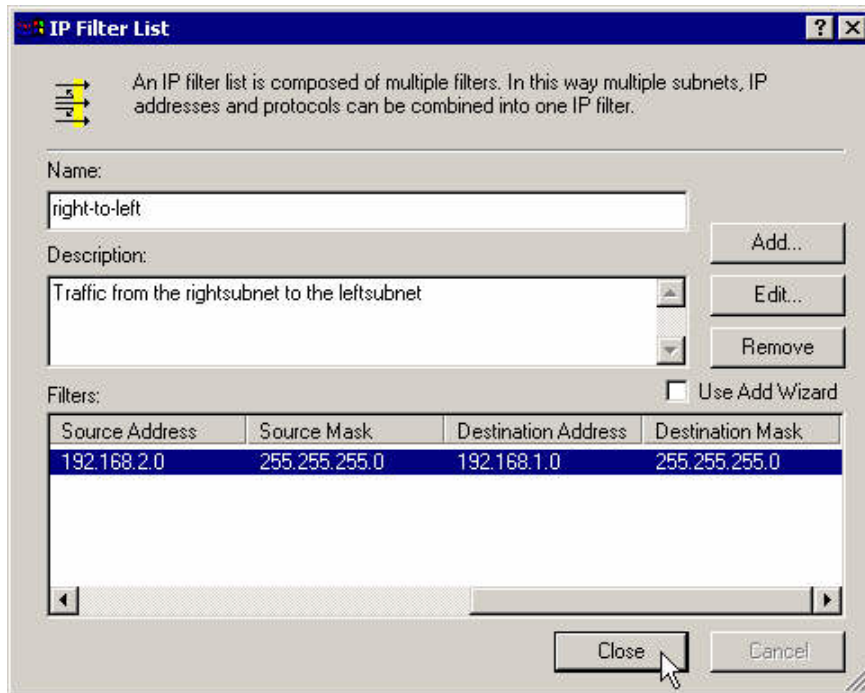


Figure 29

27. Assign the newly created filter to that rule.

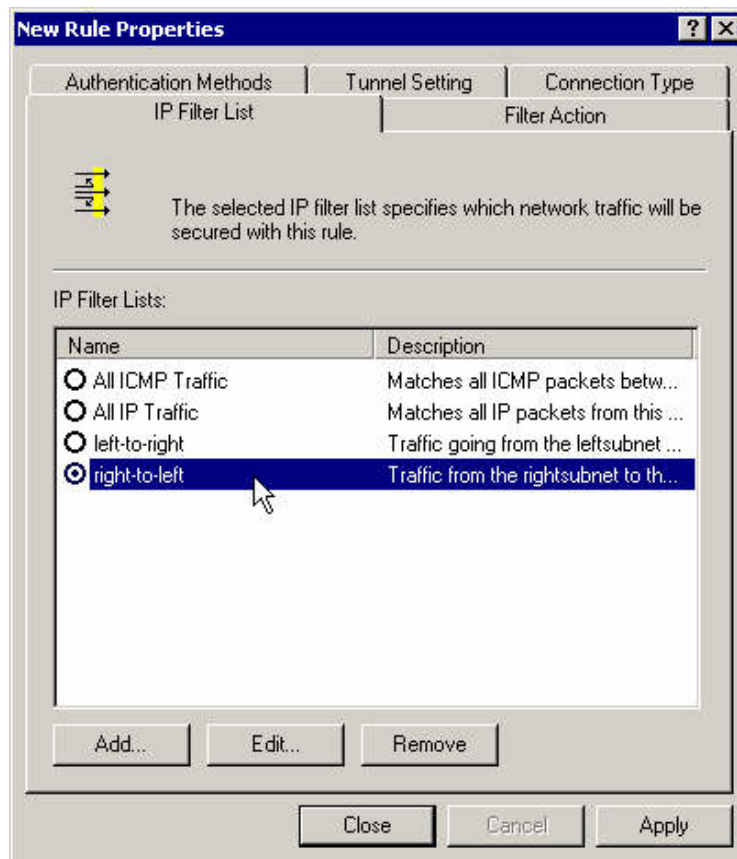


Figure 30

28. Select the **Require Security** radio button (no need to edit it again).

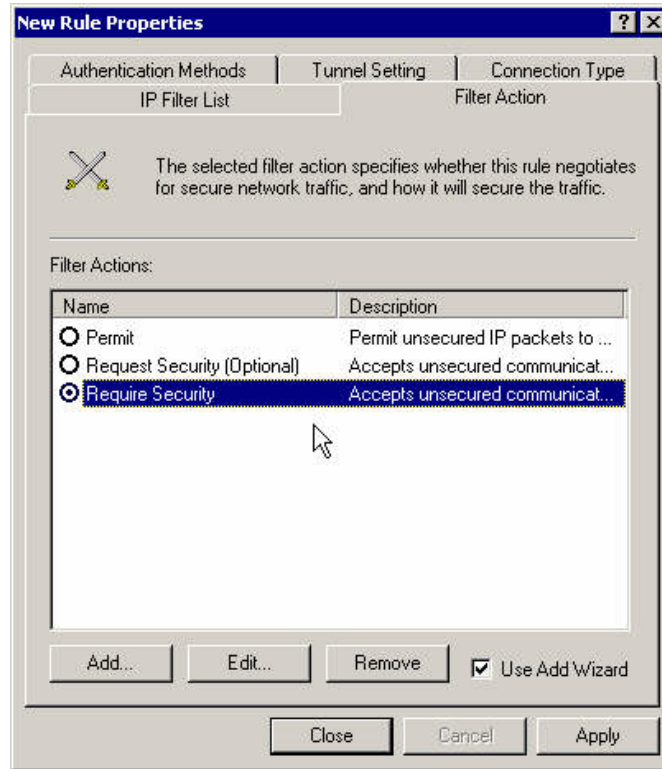


Figure 31

29. Set the connection's type to LAN.

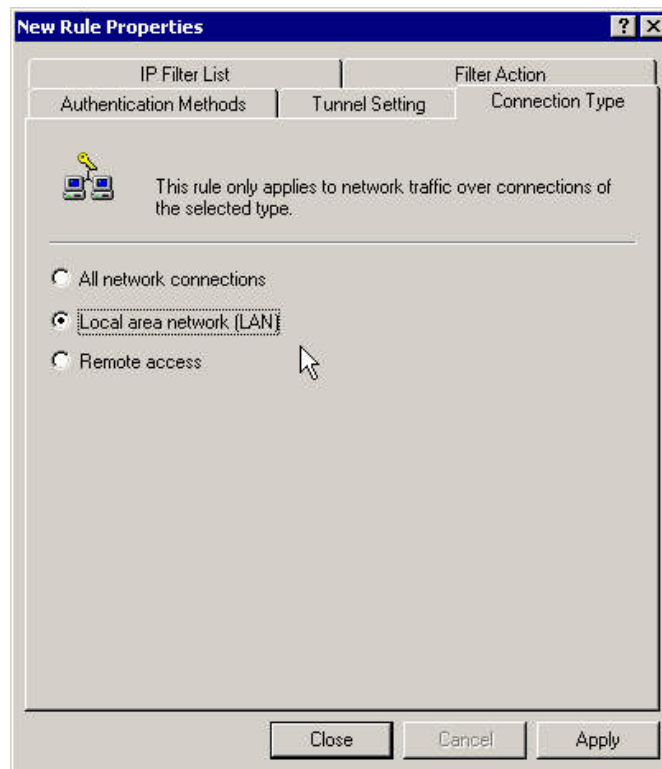


Figure 32

30. Enter the left gateway (your side) as the tunnel endpoint.

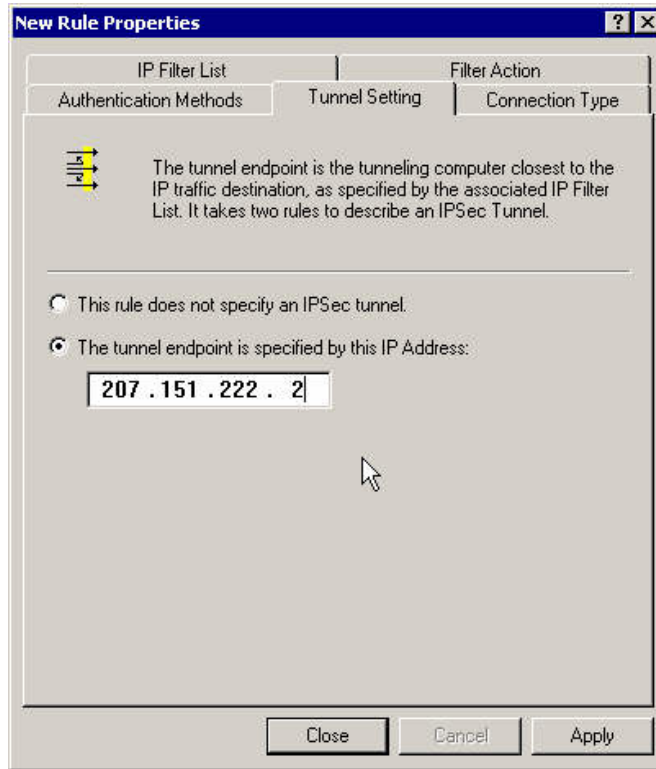


Figure 33

31. Modify the authentication method.

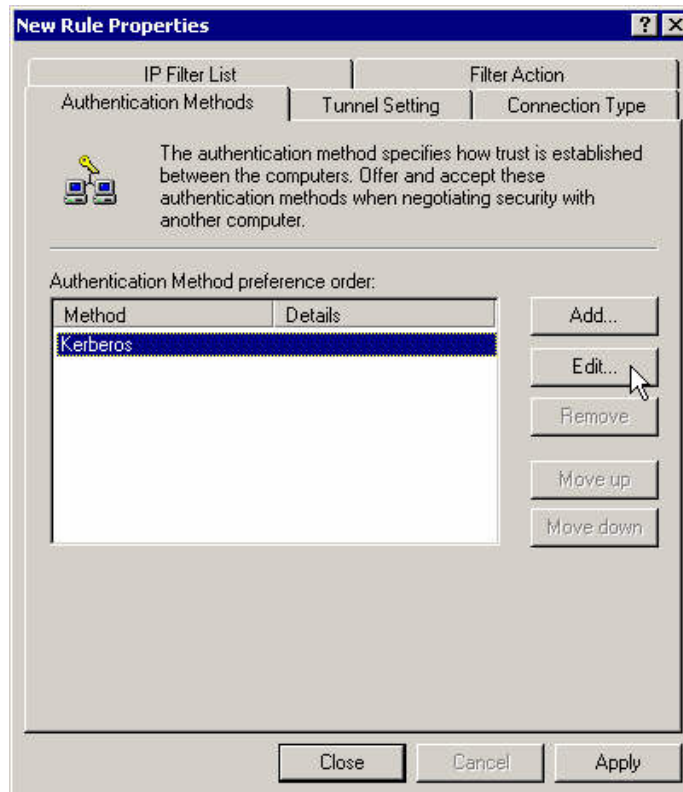


Figure 34

32. Enter your pre-shared key again.

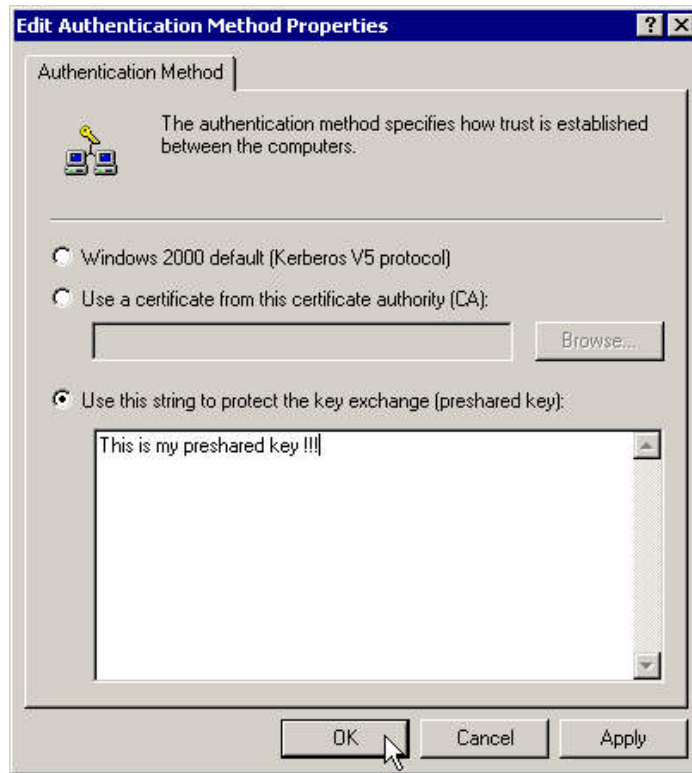


Figure 35

33. Close that rule's properties box.

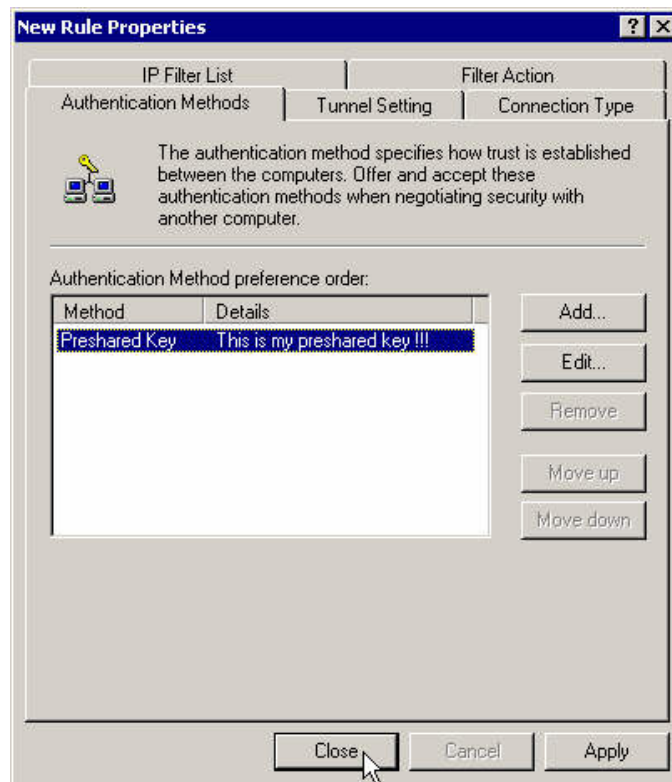


Figure 36

34. Select the 2 rules to apply on that policy.

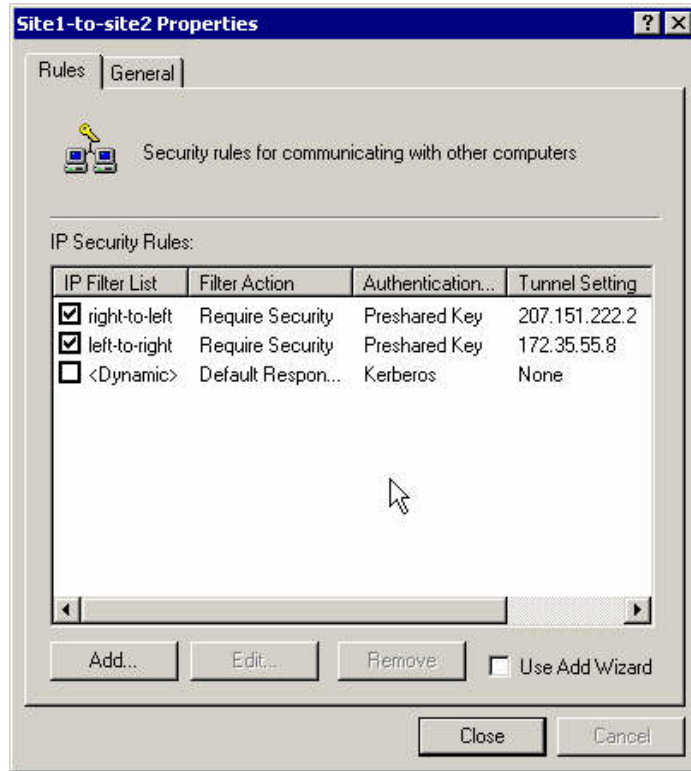


Figure 37

35. On the general tab, press the **Advanced** button.

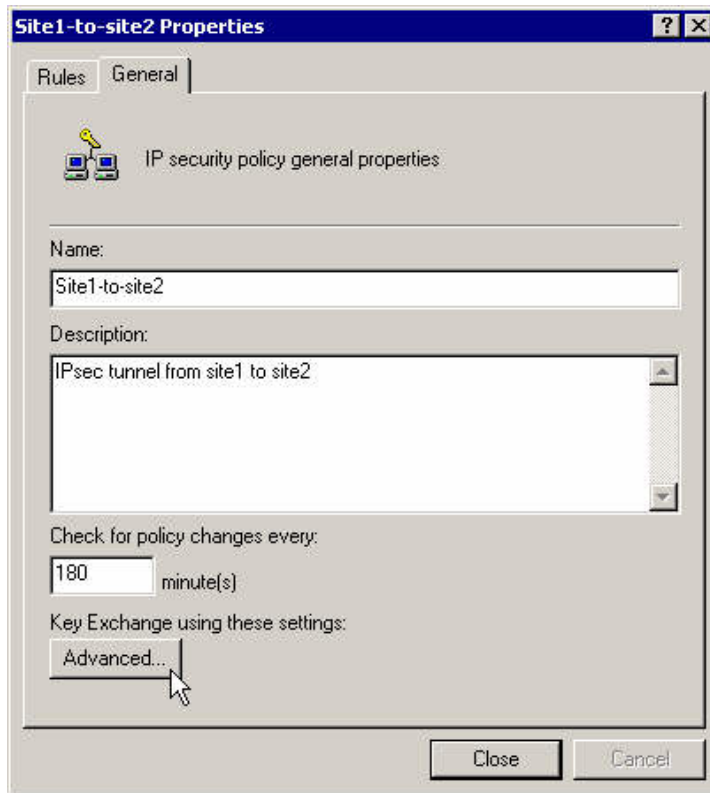


Figure 38

- 36. Select **Master Key Perfect Forward Secrecy** checkbox and press the **Methods** button.

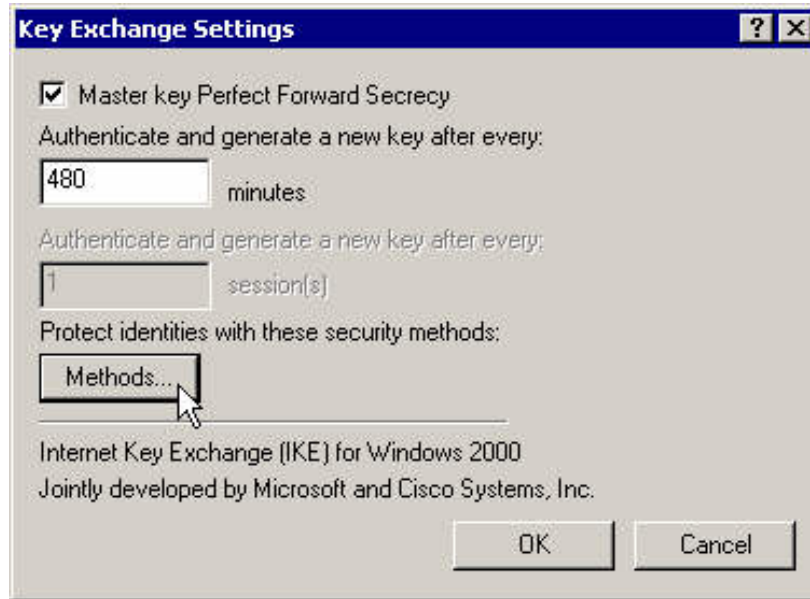


Figure 39

- 37. Move the proposal **3DES-MD5** to the top of the list and close that policy.

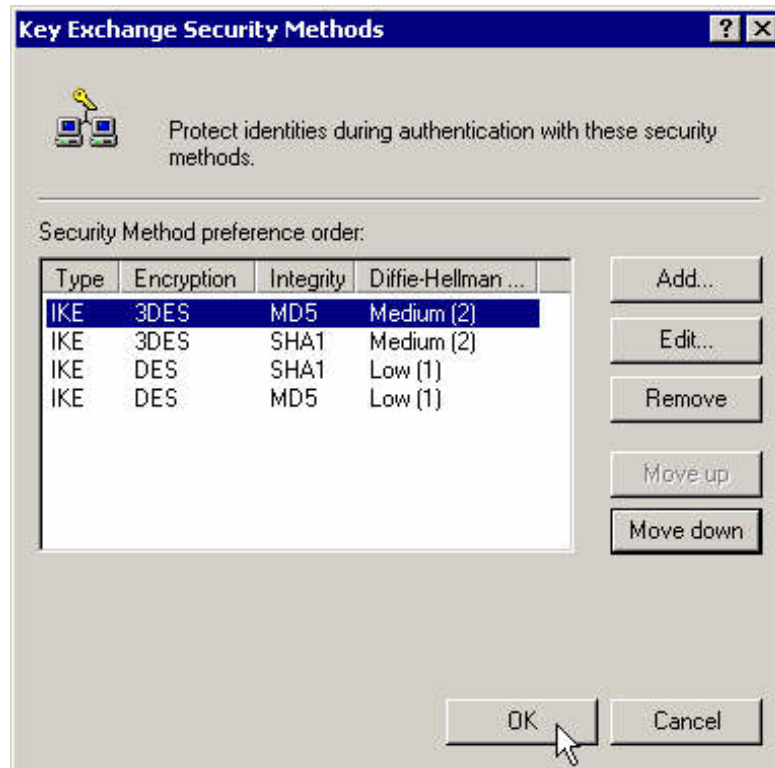


Figure 40

38. Select **Assign** for that policy to make it active.

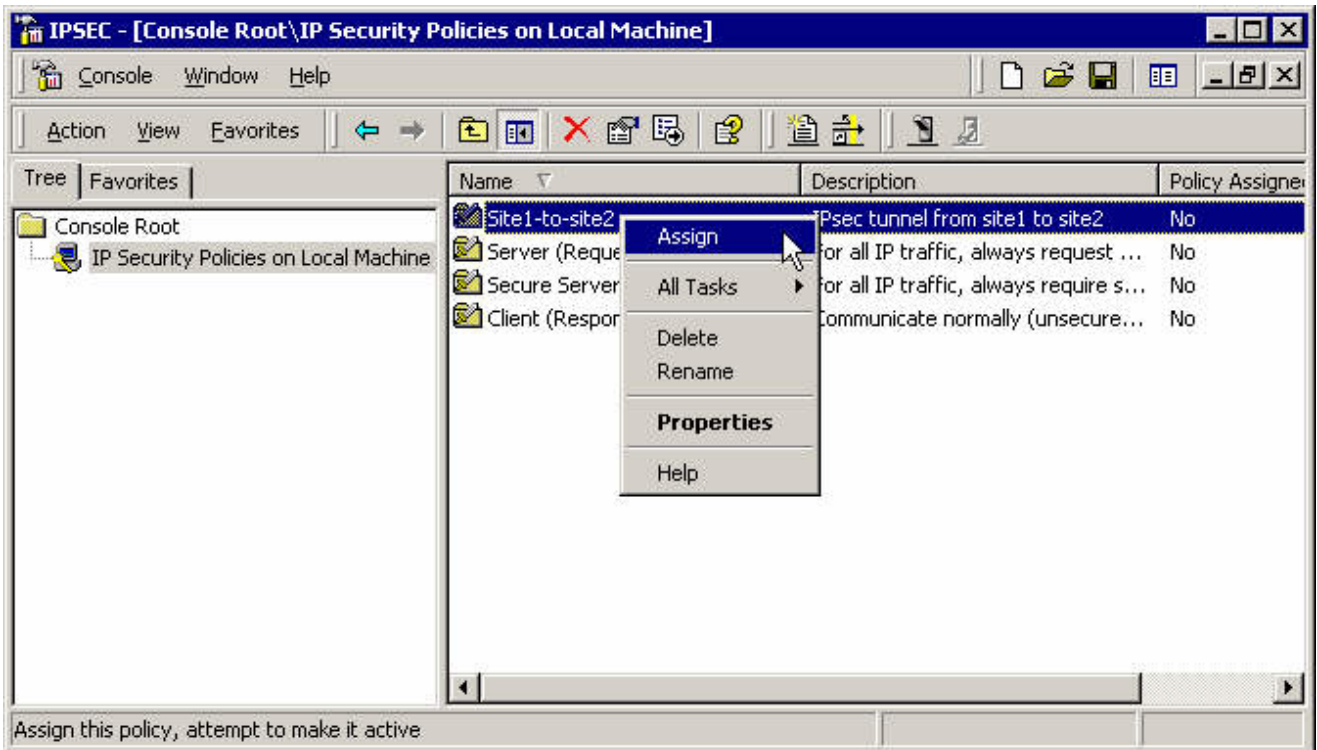


Figure 41

39. Test it. Wait and ping it again. Then check the events log because it never works the first time.

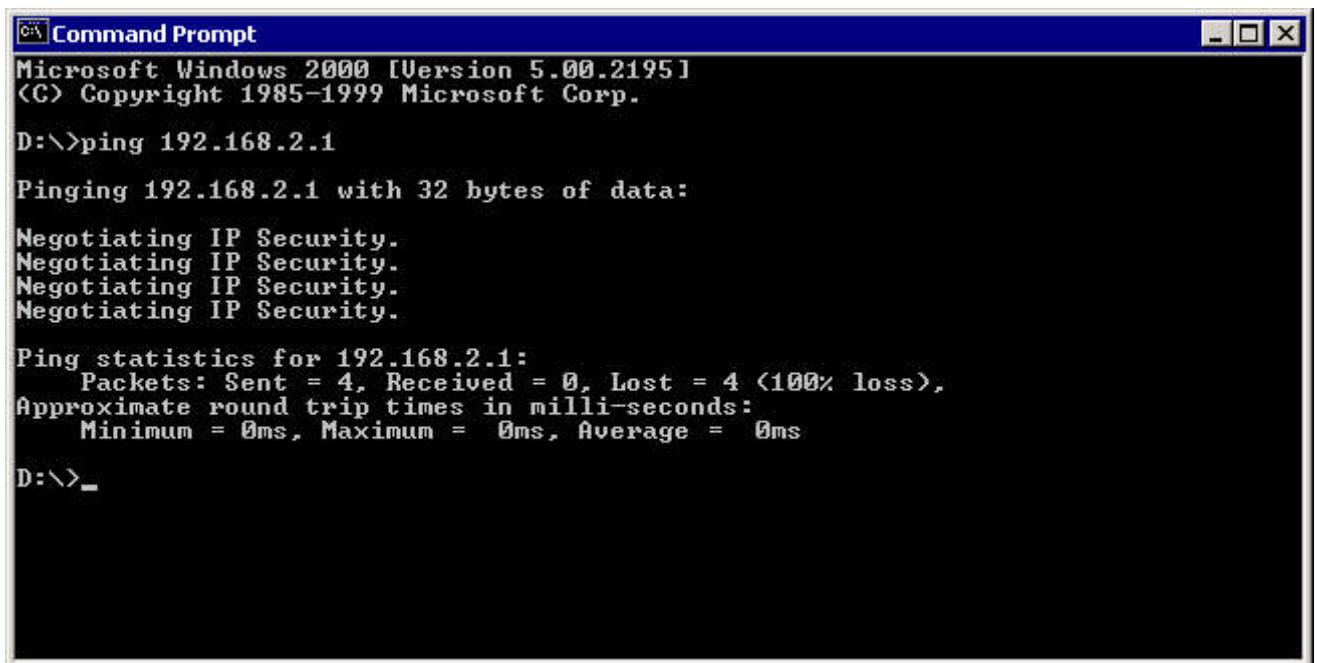


Figure 42

- 40. You'll have to modify your policy to correct what's wrong. Restart the **Ipsec** service before testing it again.

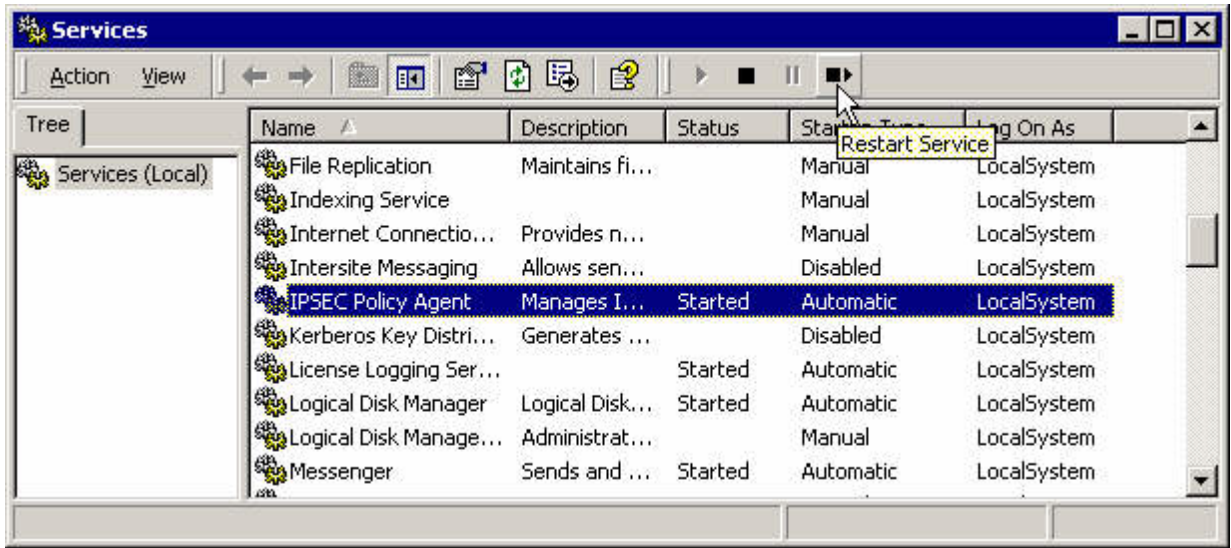


Figure 43

- 41. When it works you can monitor the tunnel with the **ipsecmon** program.

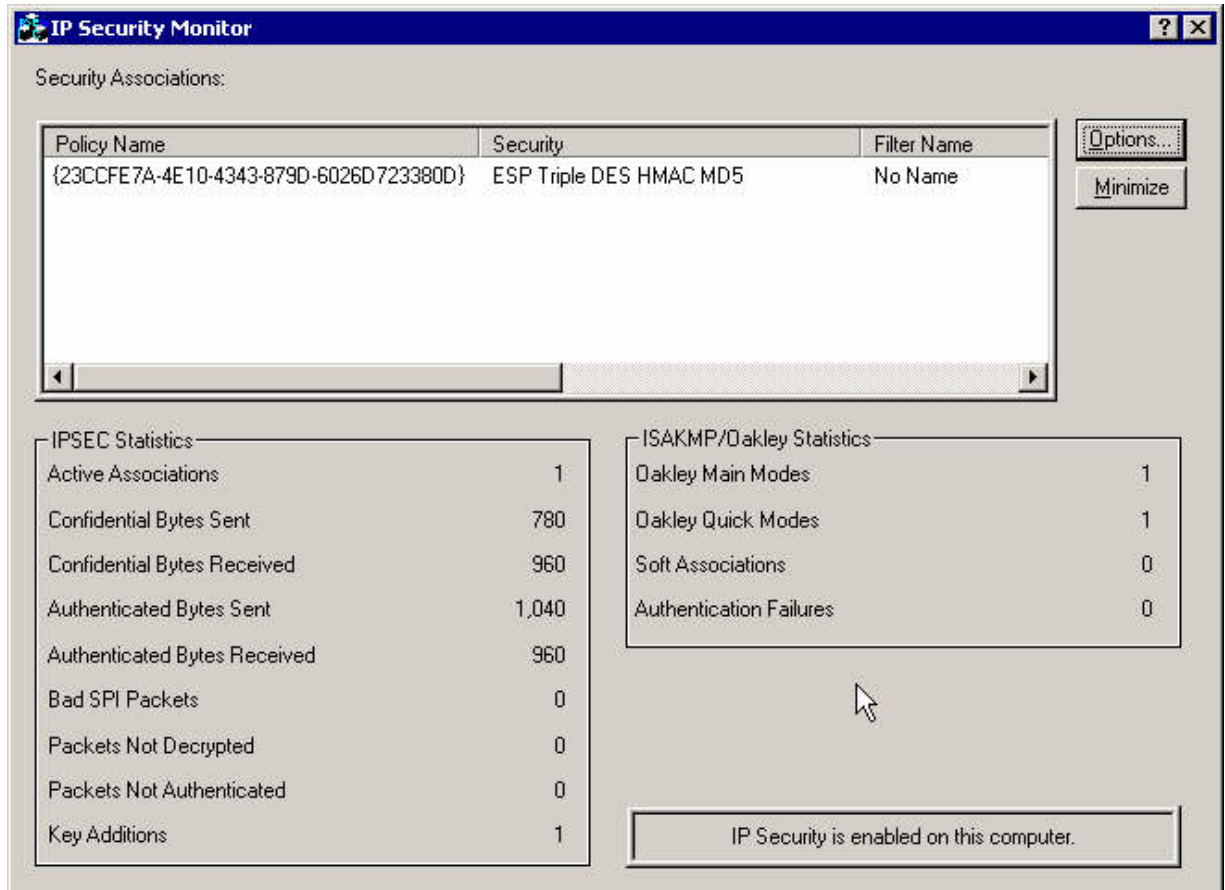


Figure 44

3 Useful Links

- The Quadro home site!
<http://www.epygi.com>
- The Windows 2000 IPSec setup!
<http://jixen.tripod.com/win2k-screen.html>
- Windows 2000 PPTP-client configuration!
http://poptop.sourceforge.net/dox/pptp_win2k/