Module 12 Lab Securing Remote Access IPSec

Background: This lab reinforces the concepts of IPSec and securing local traffic via IPSec.

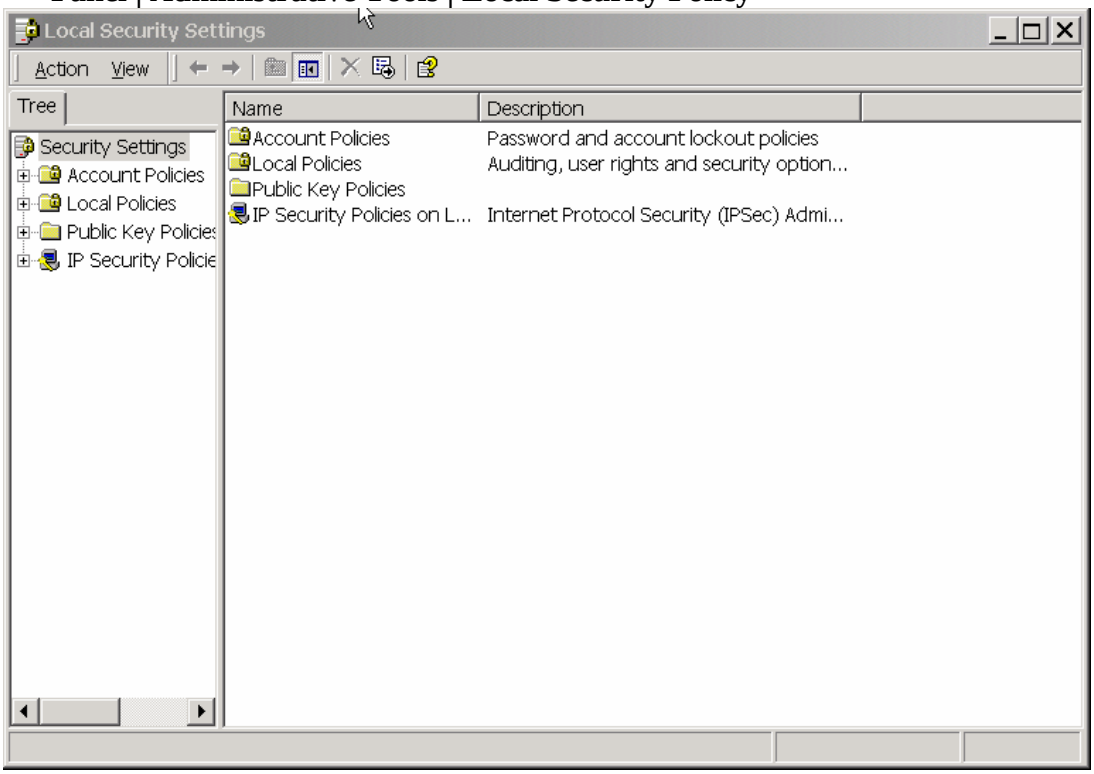
Requirements/assumptions:

- Workstation with Windows 2000 Professional
- Local administrative privileges

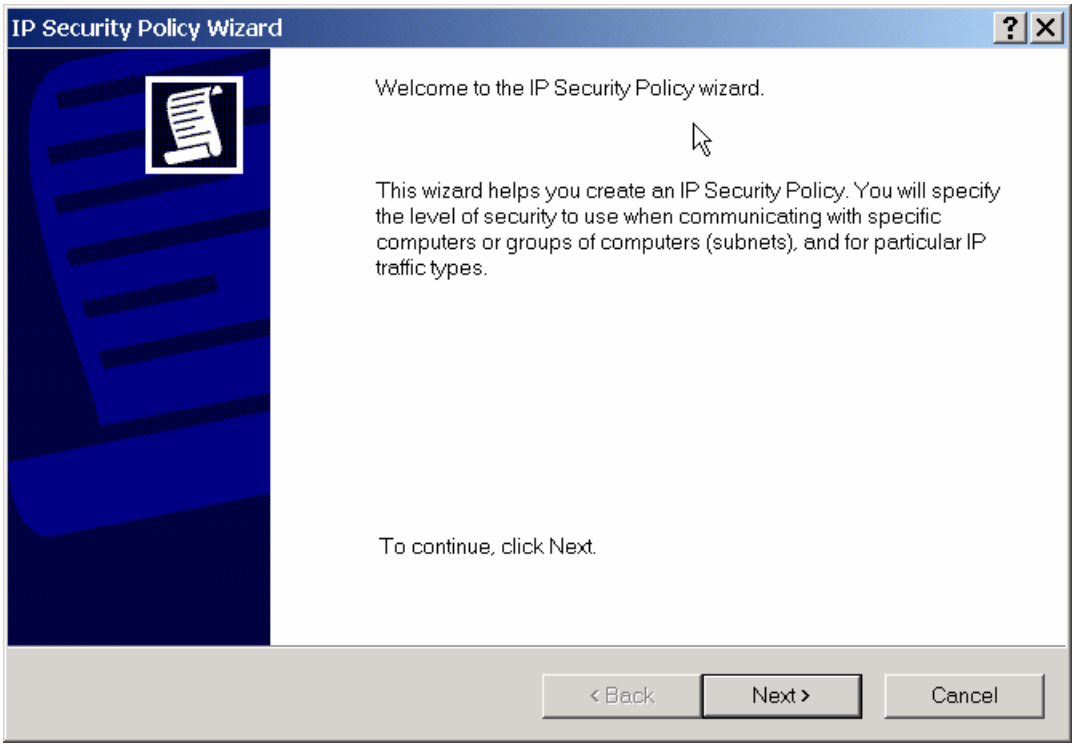
Scenario**:** Some IT staff within the company are concerned that traffic on the local network is at risk of being sniffed, either by wireless eavesdroppers or by unauthorized systems on the network. Therefore, they have decided to implement IPSec on the local network through a Windows 2000 Local Security Policy on each client system. This will secure local traffic, both wired and wireless, and will make it more difficult to sniff the packets.

Configuring an IPSec Security Policy

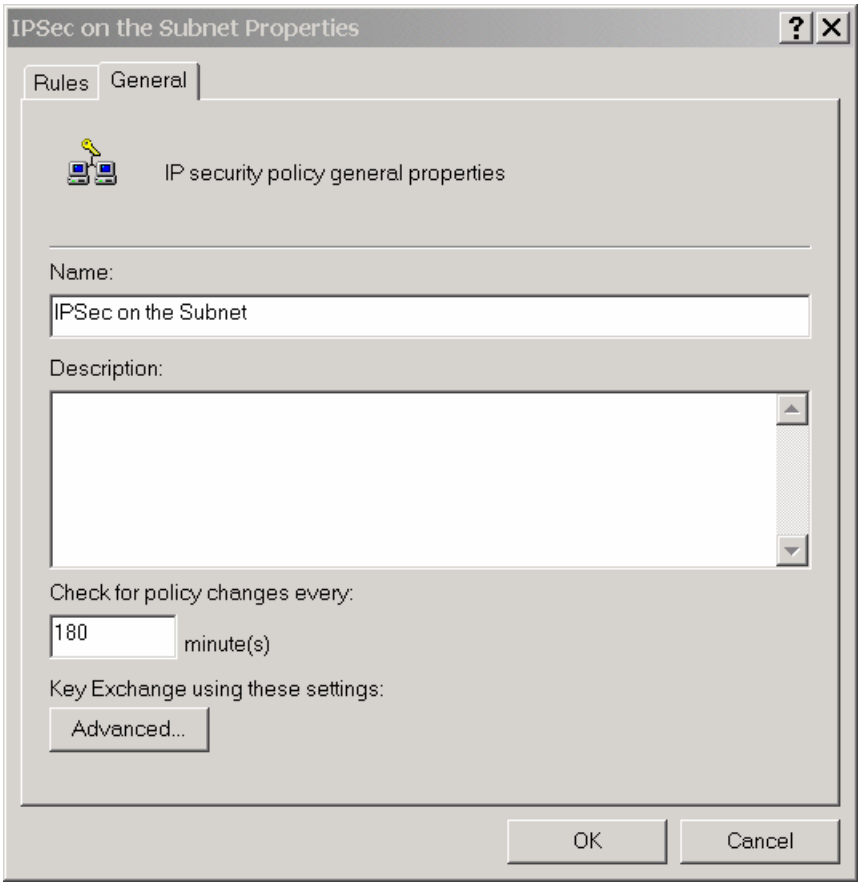
1. Boot to Windows 2000
2. Login as Administrator
3. Open the Local Security Policies Console by selecting **Start | Settings | Control Panel | Administrative Tools | Local Security Policy**



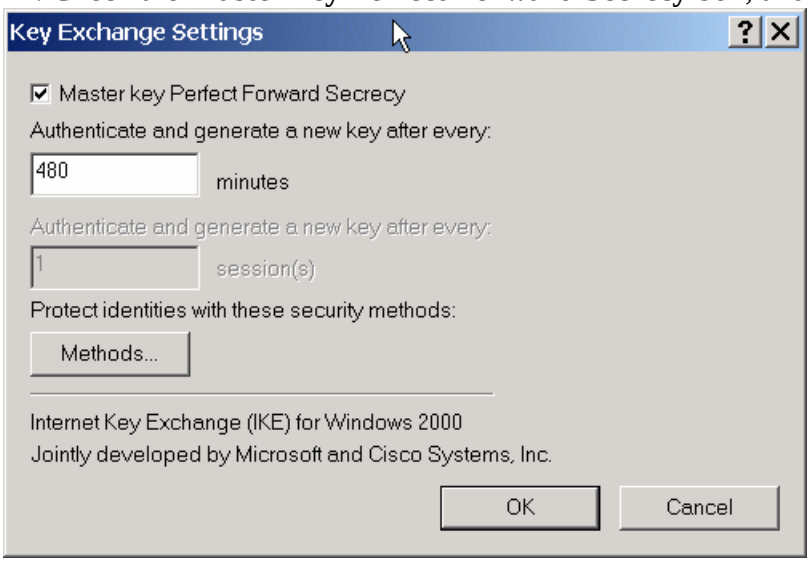
4. Right click on **IP Security Policies on Local Machine** and select **Create IP Security Policy**, which will bring up the following wizard:



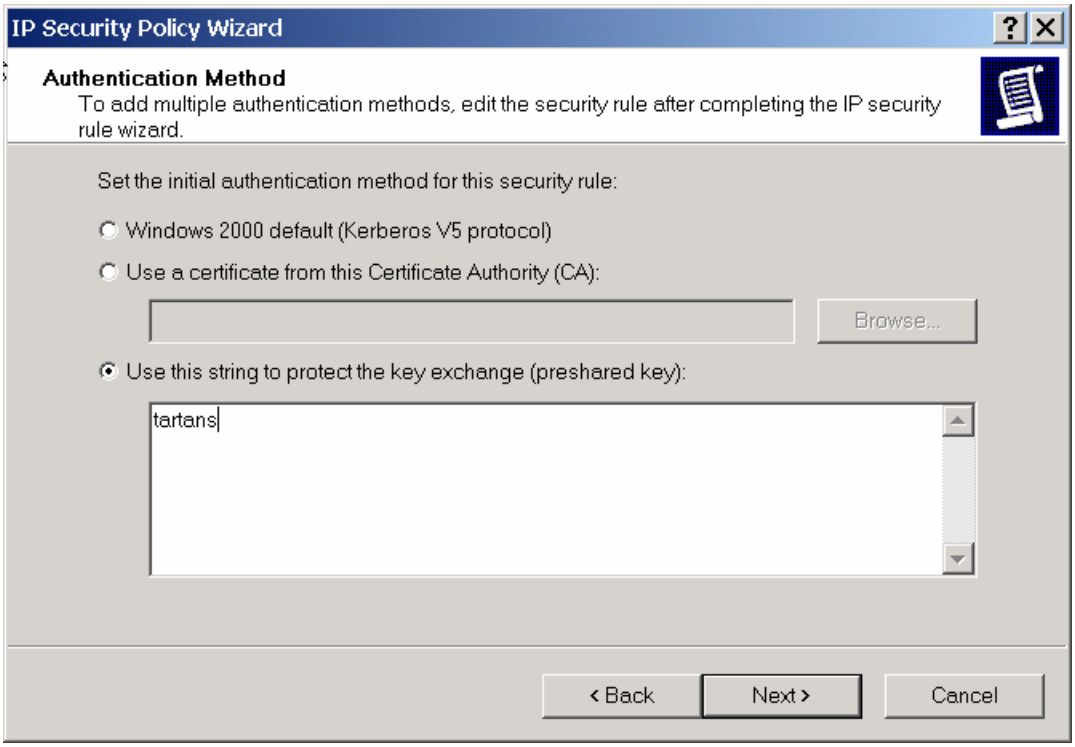
5. Click **Next**
6. Enter **IPSec on the Subnet** as the name of the rule, and click **Next**
7. Uncheck the **Activate the default response rule** and click **Next**
8. Leave the **Edit properties** box checked and click **Finish**
9. Click on the **General** tab, which will bring up this window:



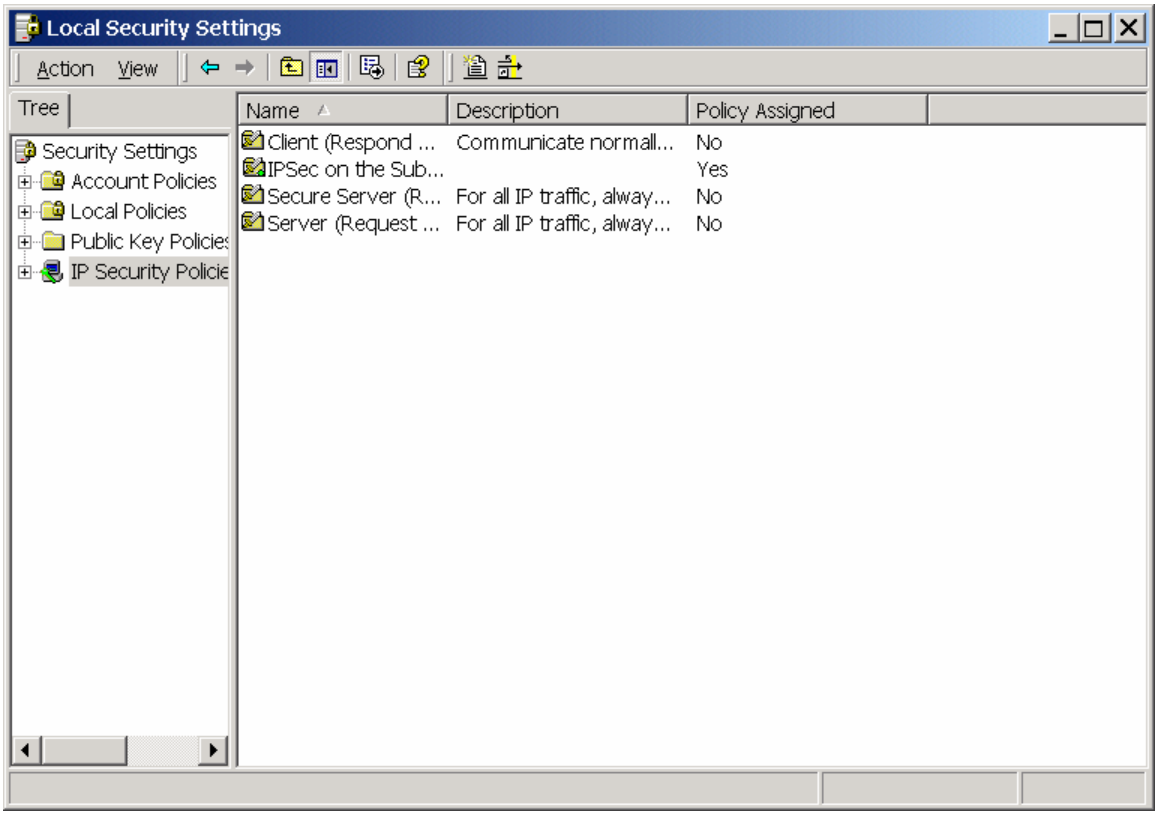
10. Click the **Advanced** button
11. Check the **Master key Perfect Forward Secrecy** box, and click **OK**



12. Go back to the **Rules** tab
13. Click the **Add…** button to start the Security Rule Wizard
14. Click **Next** to start the wizard
15. Leave **This rule does not specify a tunnel** selected and click **Next**
16. Leave **All network connections** selected, and click **Next**
17. Select **Use this string…** and enter **tartans** as the string, and click Next



18. On the **IP Filter List** screen, click **Add…**
19. On the next IP Filter List screen, click **Add…**
20. Click **Next** to start the **IP Filter Wizard**
21. On the Filter Wizard screen, leave Source Address as **My IP Address** and click **Next**
22. Select A Specific Subnet on the following wizard screen, and enter the subnet (192.168.30.0, 255.255.255.0)
23. Leave **Protocol Type** set to **Any**, and click **Next**
24. Leave **Edit Properties** unchecked and click **Finish**
25. Click **Close** to close the IP Filter List
26. Click **Close** to get back to the Security Rule Wizard
27. Click the button next to **New IP Filter List**
28. Click **Next**
29. Click **Require Security**, and click **Next**
30. Uncheck the **Edit Properties** box and click **Finish**
31. Close the **Manage Filter Lists and Filter Actions** window
32. Get back to the Local Security Settings screen
33. Double click **IP Security Policies on the Local Computer** (if not expanded already)
34. Right click on the **IPSec on the Subnet** policy and select **Assign**



35. Close the **Local Security Settings** window
36. Open a command prompt
37. Ping another student's system
38. You should get **Negotiating IP Security** as the response on your first ping attempt, and actual replies the second attempt.
39. Capture packets with Ethereal or Etherpeek to see the type of traffic that is generated through the IPSec connection—which IPSEC protocol is used?
40. After the connections have been completed, the instructors will demonstrate attempting connectivity from a system which does not have IPSec enabled

