**LAB 8: Using IPsec in Windows**

**Materials and Setup**

You will need the following:

• Windows 7

• Windows Server 2008

**Lab Steps**

**Step 1: Start the Windows Server 2008 and Windows 7 PCs. Log on to the Windows 7 and Windows Server 2008 PC’s.**

**Step 2: Ping the server and connect with FTP.**

You are going to ping the Windows Server 2008 and connect with FTP to establish that you can in fact communicate with both of these utilities.

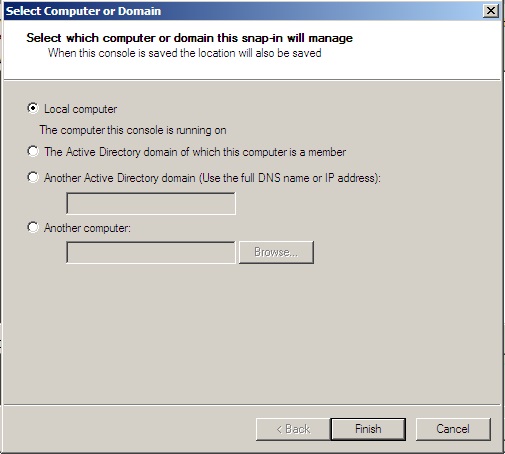
From the Windows 7 machine:

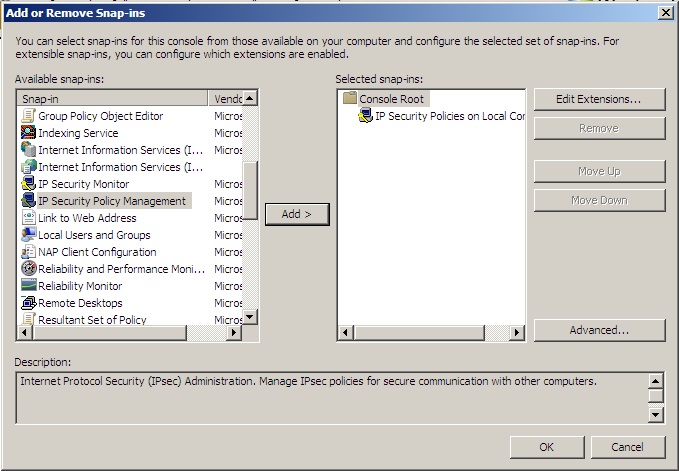
1. Choose Start | Run.
2. In the Open field, type **cmd** and press enter.
3. Type **ping 10.170.14.242** and press enter.
4. Note that you can ping the server.
5. At the command line, type ftp 10.170.14.242 and press enter.
6. At User (10.170.14.242:none), type **administrator** and press enter.
7. At the password prompt, type **password** and press enter.
8. At the ftp prompt, type **ls** and press enter.
9. Note that FTP is working properly.
10. At the prompt, type **quit** and press enter.

**Step 3: Set the IPsec policy for the Windows 7 PC.**

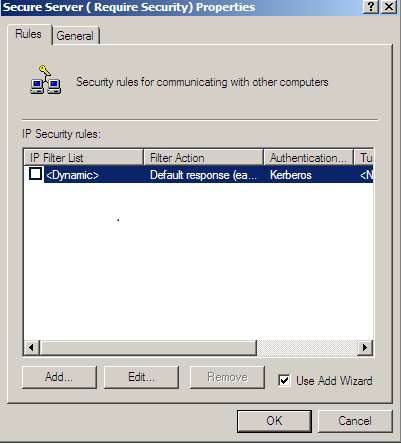
You will now configure IPsec on the Windows 7 computer.

1. Choose Start | Run.
2. In the Open field, type **mmc** and press enter.
3. Maximize the **Console1** and **Console Root** window.
4. Click the **Console** tab, choose **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, shown in Figure below, click **Add**.
6. Select **IP Security Policy Management** and click **Add**.
7. On the Select Computer or Domain screen, select **Local Computer** and click **Finish**.
8. In the Standalone Snap-in dialog box, click **Close**.
9. In the Add/Remove Snap-in dialog box, click **OK**.

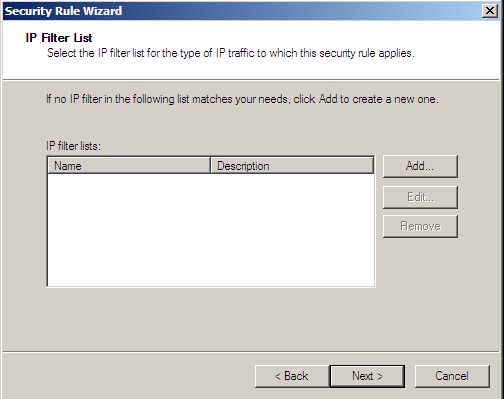




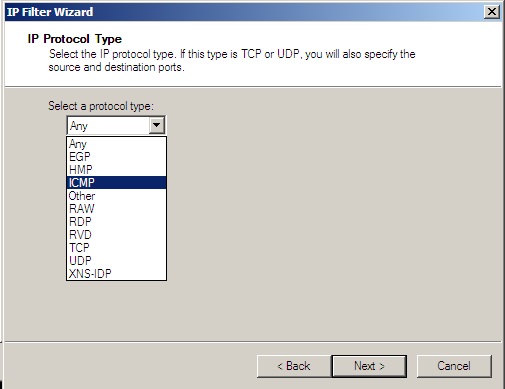
1. In the console tree pane, Right Click on **IP Security Policies on Local Machine**, select Create IP Security Policy.
   1. Follow the IP Security Wizard, Next, Then add a name for the new Policy: **Secure Server (Require Security), Next, Finish.**
   2. Uncheck the **<Dynamic>** check box.



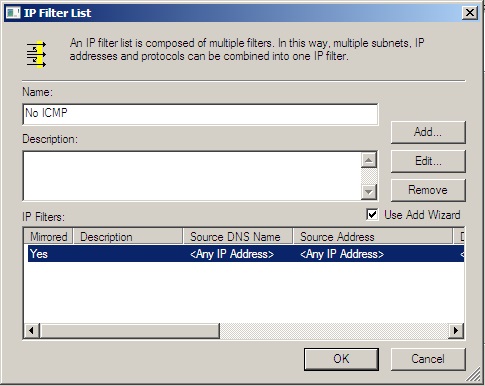
* 1. Click Add to add security Rule, Next, check this rule does not specify a tunnel. Next, check All network connection, Next. Add Filter.



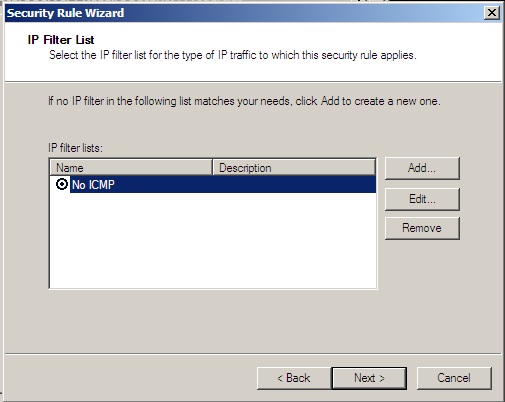
* 1. Add a name to the filter: No ICMP or No Ping, the press Add to open IP filter wizard, Next, Next. Source: Any IP Address, Destination: Any IP address, Protocol type: **ICMP**, Finish. ( for FTP connection select TCP protocol type, destination port 21)



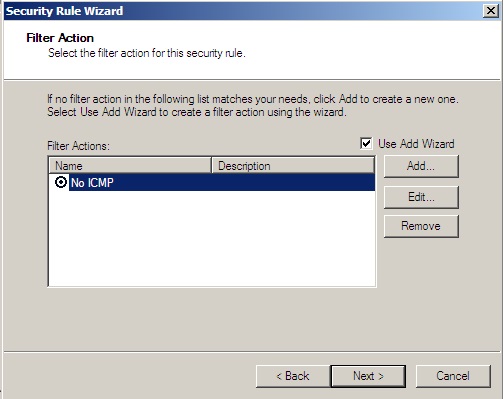
* 1. Select the IP filter added before then OK

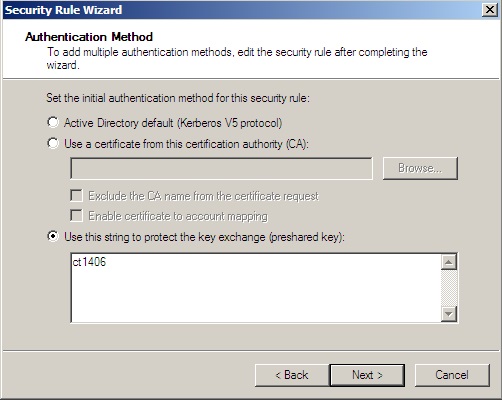


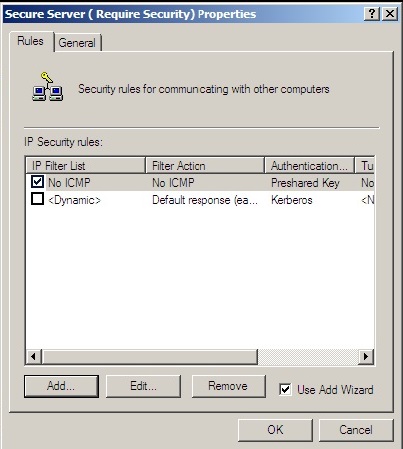
* 1. Select the Filter then Next.

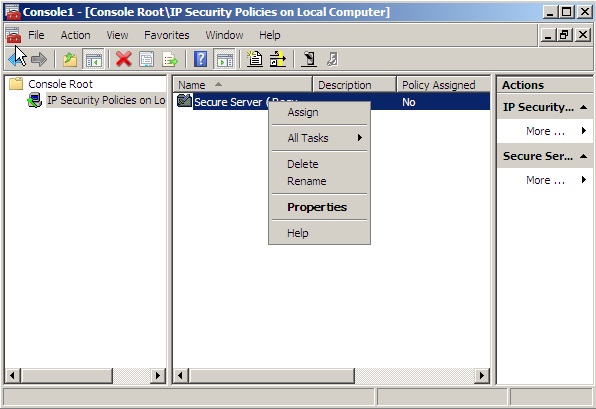


* 1. Add Filter action by pressing Add, Next, Name: No ICMP, select **negotiate security, N**ext, select **Do not allow unsecure communication**. Next, select **Integration and encryption, Next, Finish.**
  2. Check the Action address before then Next.



* 1. Check use this key to protect key exchange ( pre-shared key) then add a key (ct1406). Finish. 
  2. Make sure the rule is checked then OK.



* 1. In the details pane, right-click the **Secure Server (Require Security)** policy and select **Assign.**
  2. At the command line, type **ping 10.170.14.242** and press enter.

What response do you get?

* 1. At the command line, **type ftp 10.170.14.242** and press enter.

What error message do you get?

1. Type **quit** and press **enter**.

**Step 4: Set the IPsec policy for the Windows Server 2008 PC.**

Until IPsec is configured properly on both computers, neither computer will be able to communicate with the other. You will now configure the Windows 2000 Server PC with IPsec.

On the Windows Server 2008 computer:

1. Choose Start | Run.
2. In the Open field, type **mmc** and press **enter**.
3. Maximize the **Console1** and **Console Root** window.
4. On the **Console** tab, choose **Add/Remove Snap-in**.
5. In the **Add/Remove Snap-in** dialog box, click **Add**.
6. Select **IP Security Policy Management** and click **Add**.
7. On the Select Computer or Domain screen, select **Local Computer** and click **Finish**.
8. In the **Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the console tree pane, select **IP Security Policies** **on Local Machine**.
    1. Follow the IP Security Wizard, Next, Then add a name for the new Policy: **Secure Server (Require Security), Next, Finish.**
    2. Uncheck the **<Dynamic>** check box.
    3. Click Add to add security Rule, Next, check this rule does not specify a tunnel. Next, check All network connection, Next. Add Filter.
    4. Add a name to the filter: No ICMP or No Ping, the press Add to open IP filter wizard, Next, Next. Source: Any IP Address, Destination: Any IP address, Protocol type: **ICMP**, Finish. ( for FTP connection select TCP protocol type, source port 21)
    5. Select the IP filter added before then OK
    6. Select the Filter then Next.
    7. Add Filter action by pressing Add, Next, Name: No ICMP, select **negotiate security, N**ext, select **Do not allow unsecure communication**. Next, select **Integration and encryption, Next, Finish.**
    8. Check the Action address before then Next.
    9. Check use this key to protect key exchange ( pre-shared key) then add a key (ct1406). Finish.
    10. Make sure the rule is checked then OK.
    11. In the details pane, right-click the **Secure Server (Require Security)** policy and select **Assign**

**Step 5: Test the IPsec configuration.**

You will now see if you can communicate again with the ping command or the ftp command.

1. On the Windows 7 computer:
2. At the command line, type **ping 10.170.14.242** and press **enter**.

What response do you get? (If it does not work the first time, try again.)

1. At the command line, type **ftp 10.170.14.242** and press **enter**.

Are you able to connect?

Now configure the Windows 7 computer so that you will be able to use the ping command but not communicate with FTP.

1. Maximize the **Console1** window.
2. In the details pane, right-click the **Secure Server (Require Security)** policy and select **Properties**.
3. Uncheck the **Secure Server** check box.
4. Click **Apply** and then click **OK**.
5. At the command line, type **ping 10.170.14.242** and press **enter**.

What response do you get?

1. At the command line, type **ftp 10.170.14.242** and press **enter**.

Are you able to connect?

**Step 6: Capture and analyze the traffic.**

You will now allow IP traffic again and look at what the network traffic looks like in Wireshark.

1. Click the **Console1** window. In the details pane, right-click the **Secure Server (Require Security)** policy and select **Properties**.
2. Check the **All IP Traffic** check box.
3. Click **Apply** and then click **OK**.
4. On the **desktop**, double-click **Wireshark**.
5. On the Wireshark menu, choose Capture | Start.
6. On the Wireshark Capture Options screen, click **OK**.
7. At the command line, type **ping 10.170.14.242** and press **enter**.
8. At the command line, type **ftp 10.170.14.242** and press **enter**.
9. At **User (10.170.14.242:none),** type **administrator** and press **enter**.
10. At the password prompt, type **password** and press **enter**.
11. At the ftp prompt, type **ls** and press **enter**.
12. At the prompt, type **quit** and press **enter**.
13. In Wireshark, choose Capture | Stop.

What port number is the traffic transferring across?

Can you see any of the data in any of the packets?

**Step 7: Log off from the Windows 7 PC and also the Windows Server 2008 PC.**

To exit from the Windows 7 PC:

1. Choose Start | **Log Off**.
2. At the Log Off Windows screen, click **Log Off**.

To exit from the Windows Server 2008 PC:

1. Choose Start | **Log Off**.
2. At the Log Off Windows screen, click **Log Off**.