Configure IPSec policy on Windows Server to protect HTTP Server traffic

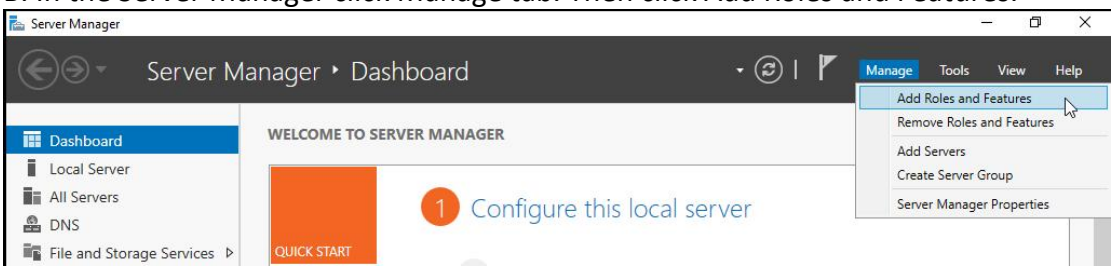
This lab will demonstrate the steps to configure IPSec between two Windows Server. For this lab Windows 2016 Server standard evaluation version is used. One Windows Server will be configured to host the web server. The other server will be the client.

This document assumes that you already have two Windows server 2012 R2 or higher version of Windows already installed on physical servers or virtual machines. In case of VM's keep network card in NAT mode in VMWare and in Host only for VirtualBox. The client can be any Windows version except home basic.

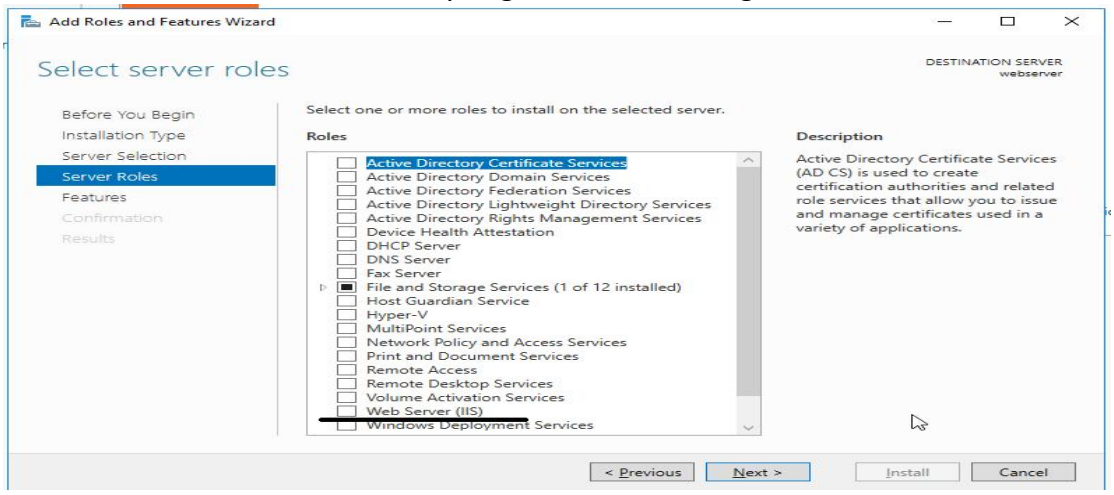
1. **Configure IIS web server on one of the server.**

A. Login as administrator.

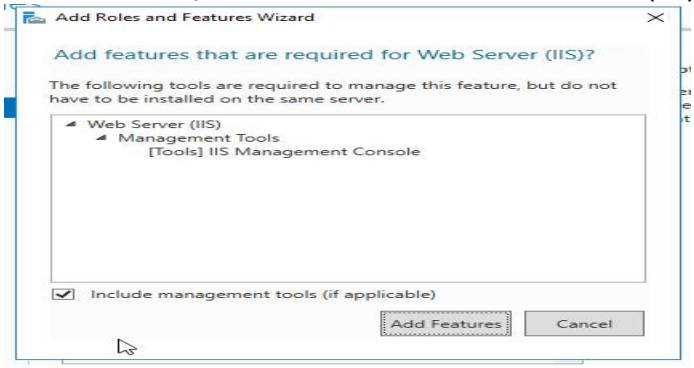
B. In the Server Manager click Manage tab. Then click Add Roles and Features.



Click Next on all the Windows, till you get to the following window.

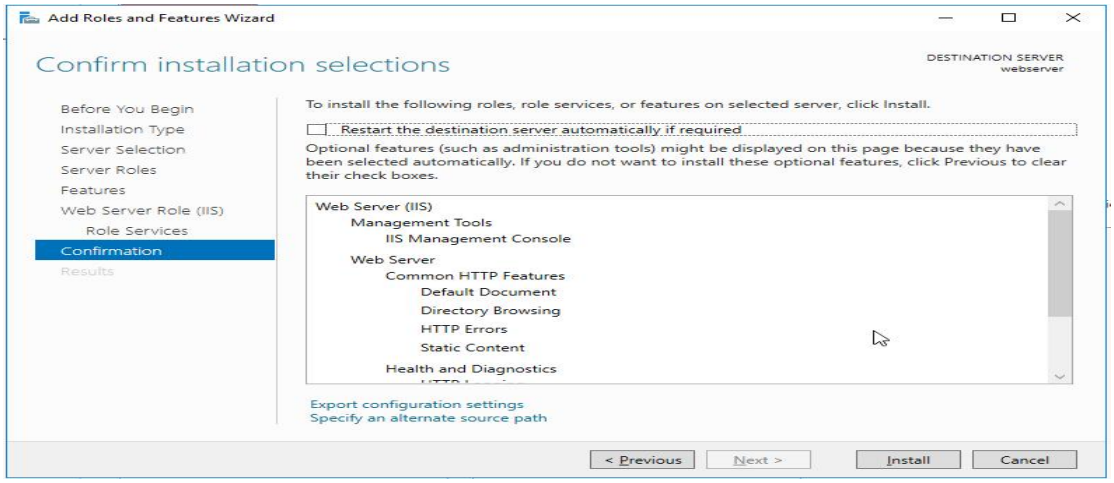


In this window, click the check box of Web Server(IIS).

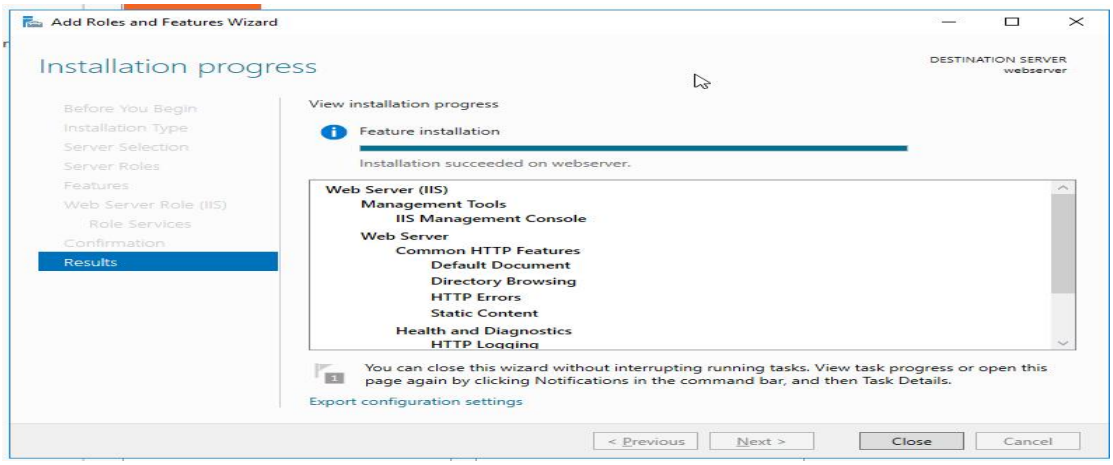


Click Add Features on the window that opens when you click the check box.

Click Next on all windows till you get following window.



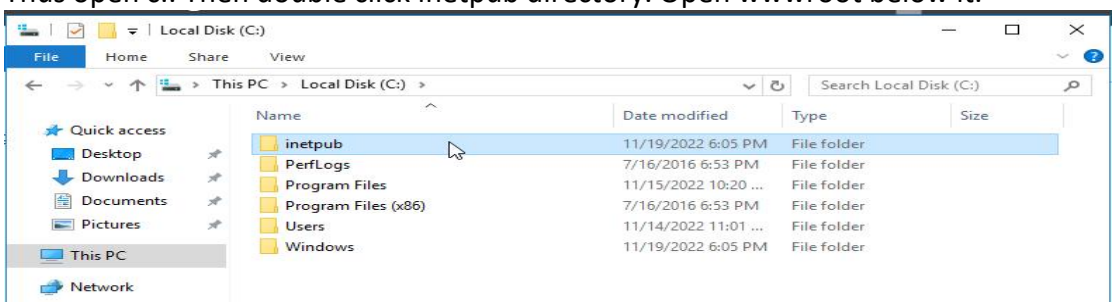
Click Install. This will install the web server on the Windows server.



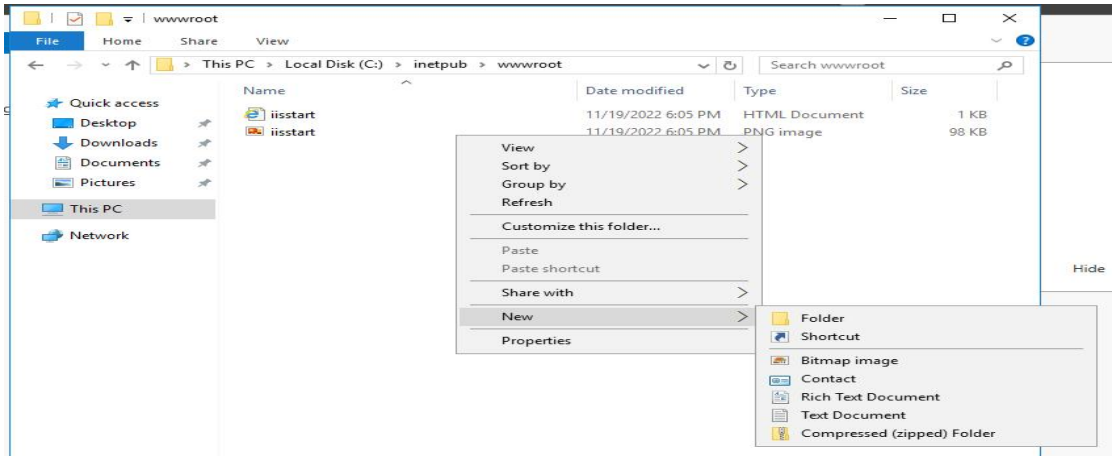
Once the installation is successful, click Close.

Now a default web site is automatically created by IIS. This website runs on TCP port 80 (HTTP port). This website displays the web pages from the c:\inetpub\wwwroot directory. There is a default welcome page. We will create our web page in this directory.

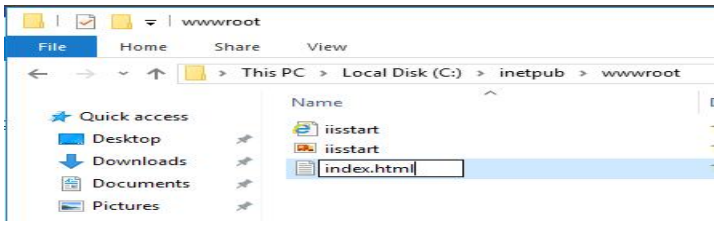
Thus open c:. Then double click inetpub directory. Open wwwroot below it.



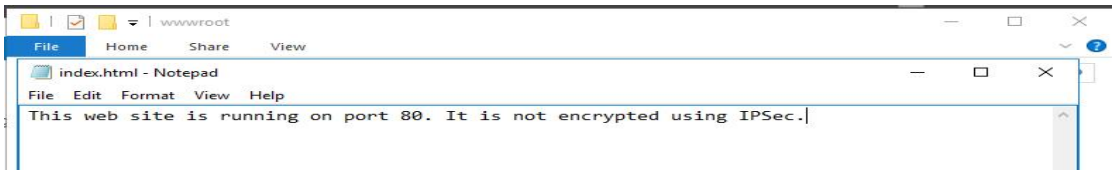
In the wwwroot directory, right click and click New. Then select Text Document. As shown below.



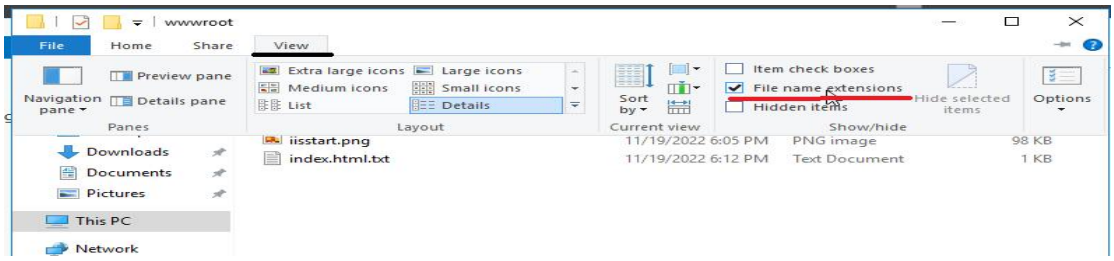
Provide the file name as **index.html**. The web server is designed to show the first web page by this name.



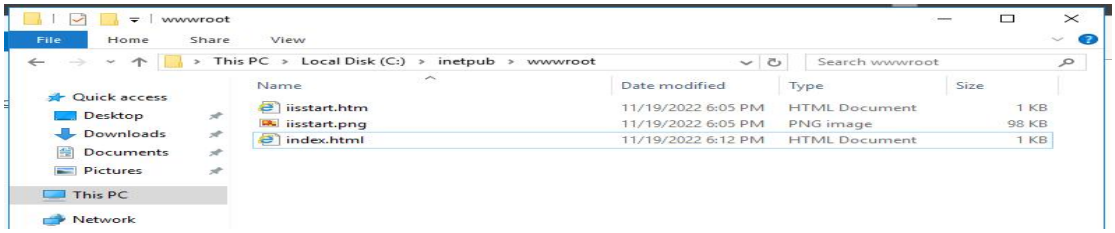
Edit file and type any text. This will be displayed in the client browser.



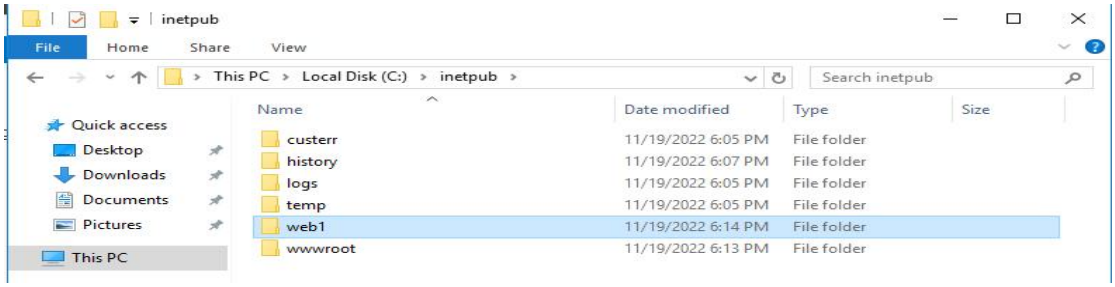
Save and close the file. Actually the file name becomes index.html.txt. However Windows hides the file extension. Thus to configure Windows to display file extensions, click View. Then click the check box of File name extensions. This will display the file name extensions.



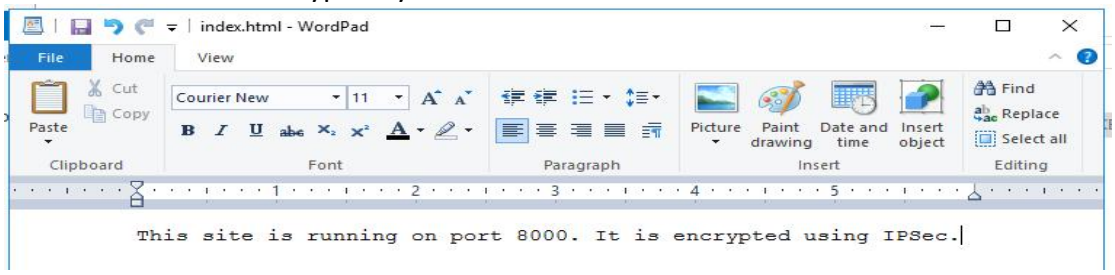
Rename the file. Remove the .txt extension. The file will be index.html as shown below.



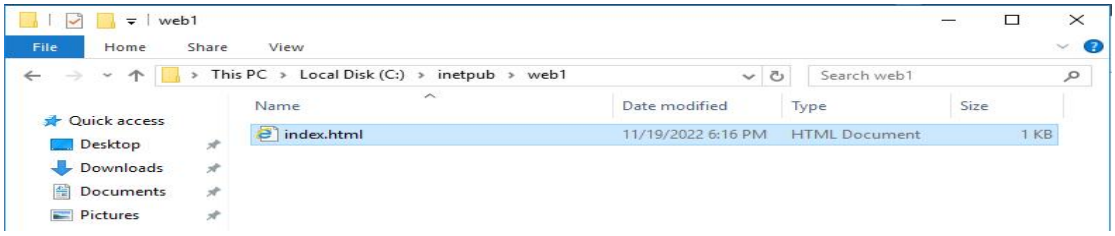
Now we will create a directory for the second web site. Go back to inetpub directory. Create a new directory by any name. Here the name given is **web1** as shown below.



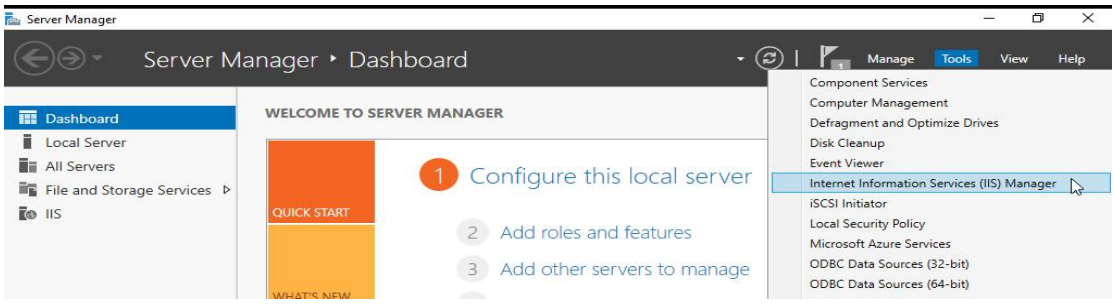
Now go into that directory. Right click and create a text document. Name the file as index.html. Edit it and type any text in it as shown below.



Save the file. Rename the file. Remove the .txt extension. The file will be as shown below.

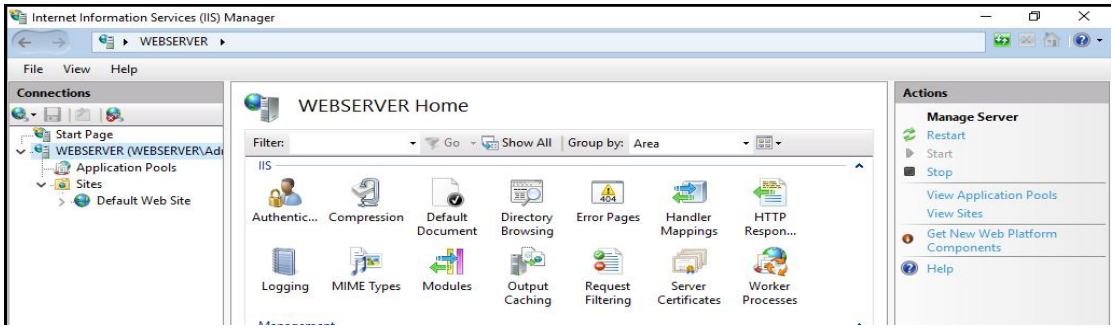


Now we will create the second website. For this go to Server Manager. Click Tools. In the list displayed, click Internet Information Service (IIS) Manager as shown below.

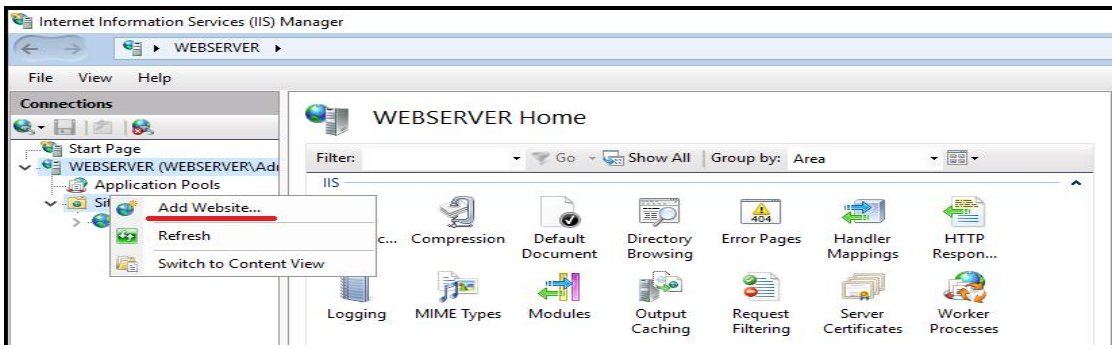


Following window opens. Server name will be displayed on the left side. Click the expand button. It will display Application Pool and Sites.

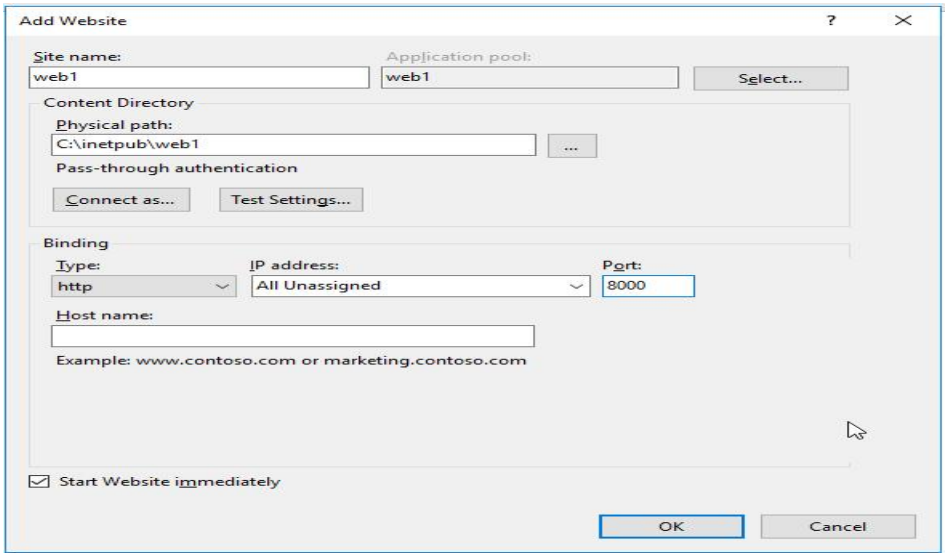
Expand sites. This will display the Default Web Site created as shown in the below scrrenshot.



Now right click on the sites. It shows Add Website option as shown below.

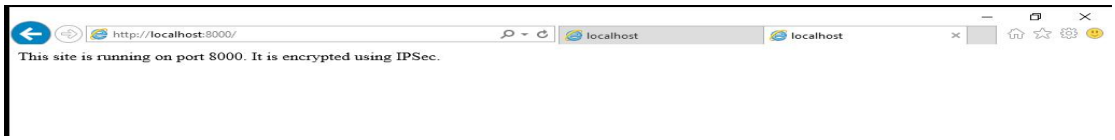


Click Add Website. A new window opens as shown below.

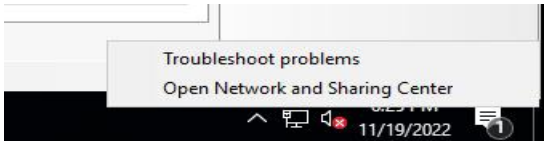


Type some name in the Site name field. Click three dots in front of Physical Path. Select the web1 directory created below C:\inetpub.
In the port field type 8000.
Thus this website will run on port 8000. Click OK. This will create our second website. Now open browser on the server and type http://localhost. This will open the Default web site.

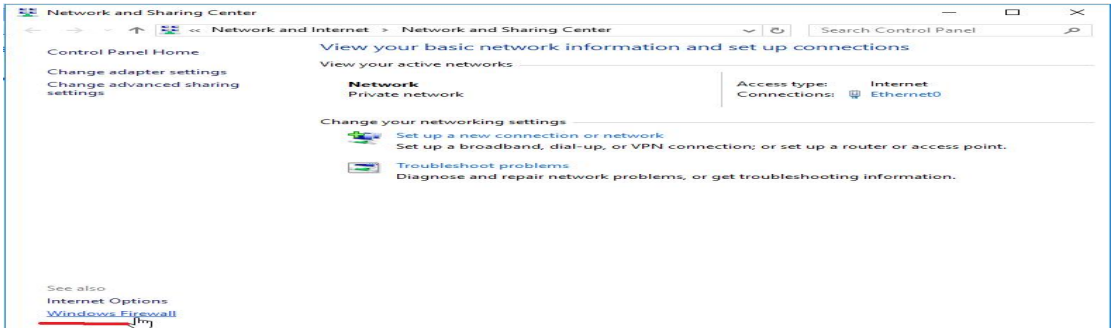
Open another tab and type http://localhost:8000. This will open the second web site.



Thus both websites are working properly. Now we will open the ports in the Windows firewall. This will allow other computers in the network to open websites as by default firewall blocks access to all ports.
To open firewall configuration, right click on the computer icon displayed near date and time. This will display following options.

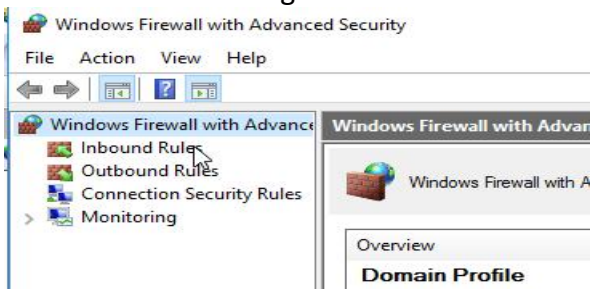


Click Open Network and Sharing Center. Following window will open.



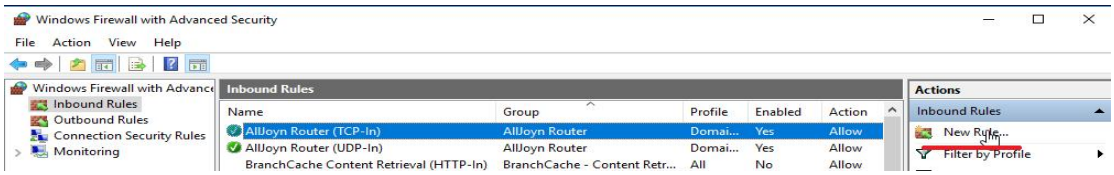
Click Windows Firewall option, displayed on the left bottom of the screen. Following window is displayed.

Click Advanced settings on the left side as shown above. Following window opens.

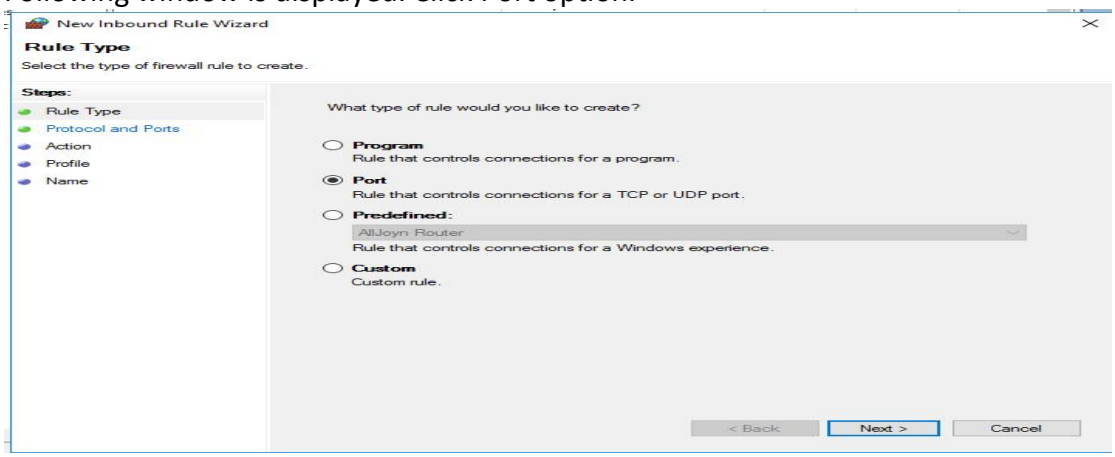


Click Inbound Rules.

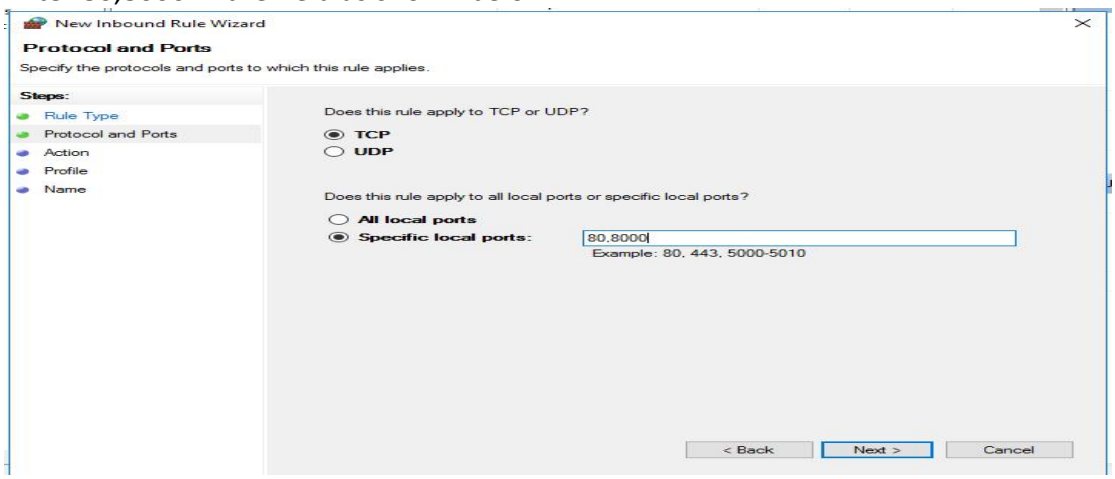
Now click New Rule option on extreme right side as shown below.



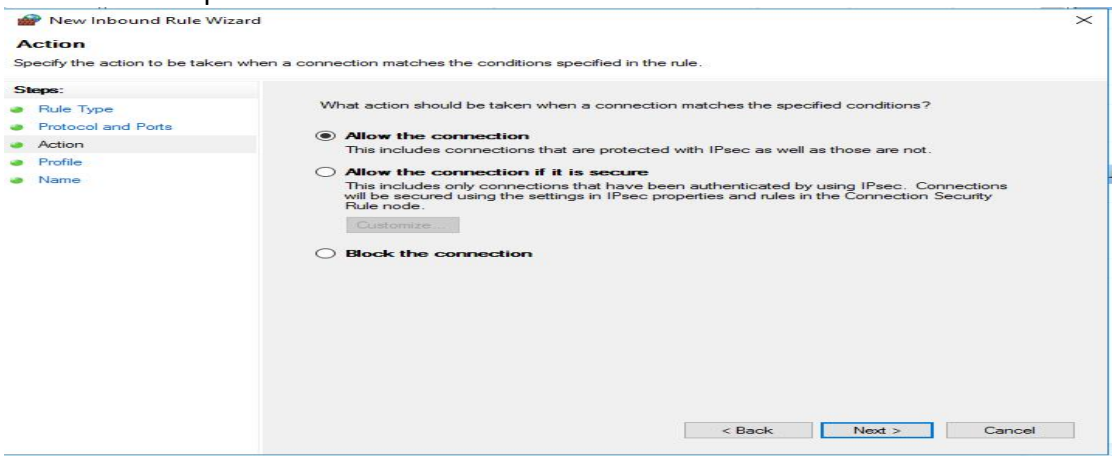
Following window is displayed. Click Port option.



Click Next. On the following window keep TCP selected. Then click Specific local ports. Enter 80,8000 in the field as shown below.

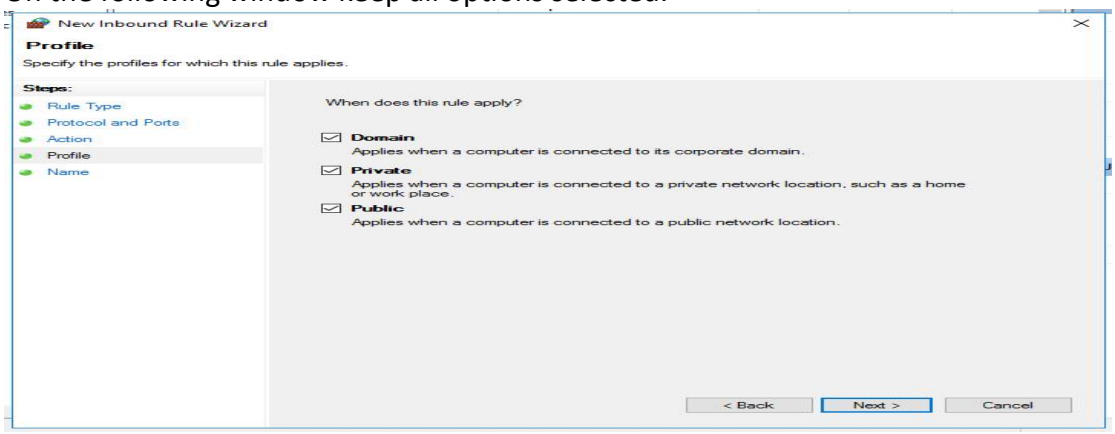


Click Next. Keep Allow the Connection.

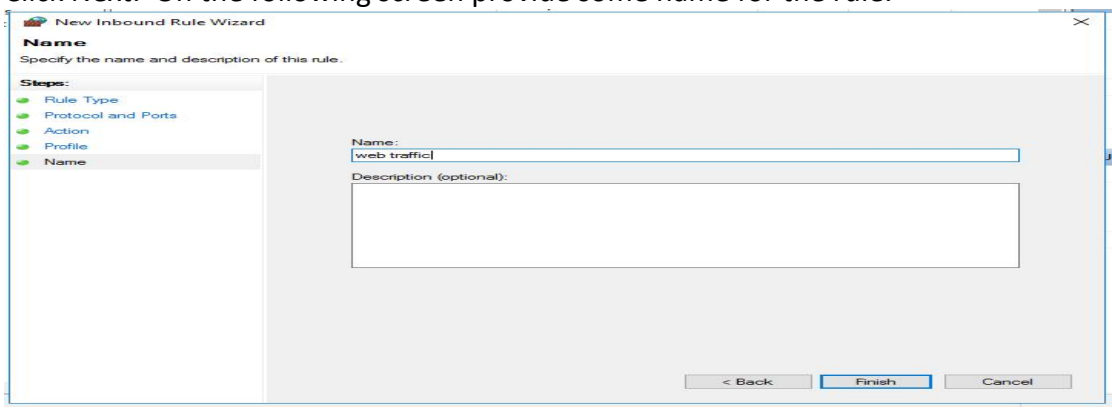


Click Next.

On the following window keep all options selected.



Click Next. On the following screen provide some name for the rule.

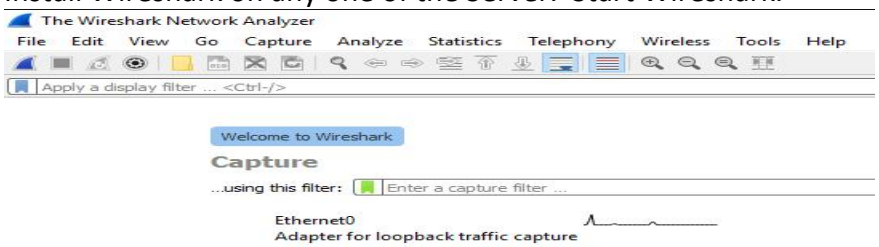


Click Finish to add the rule to the firewall.

2. Capture traffic using Wireshark

Now we will capture the traffic on one of the server to check that http traffic is sent in plain text. This will show the web page content in the Wireshark. Later we will configure IPSec to secure this traffic.

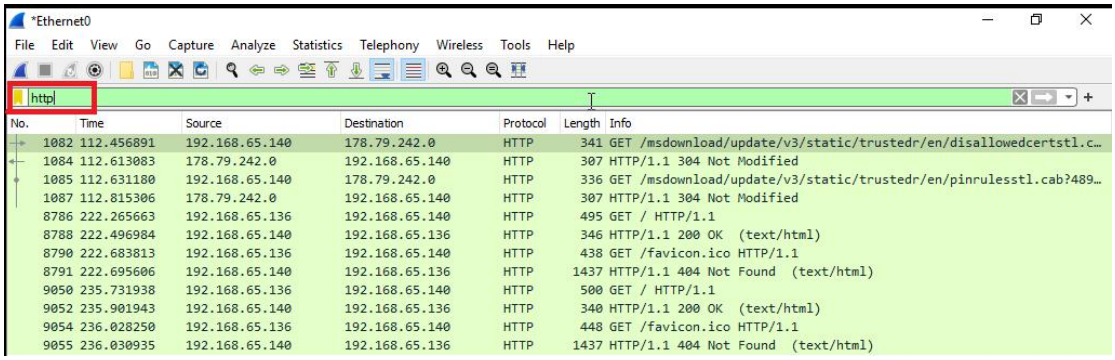
Install Wireshark on any one of the Server. Start Wireshark.



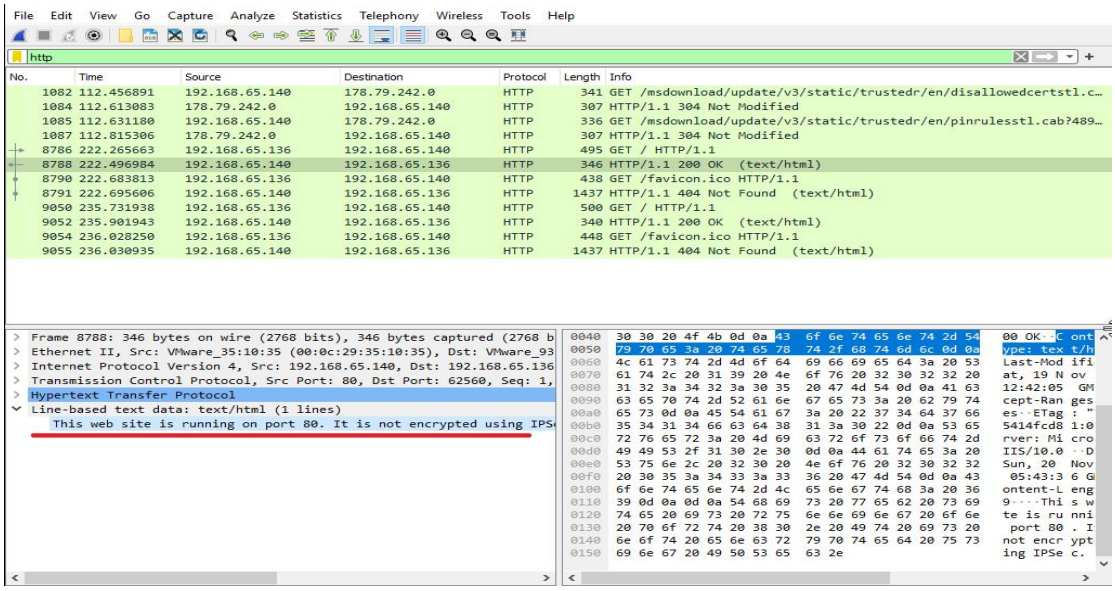
Click Ethernet0 to start capturing Frames.

Now open browser. Type http://(IP address of the Web Server). This will open the first web site. Then type http://(Web server ip):8000 to open second website.

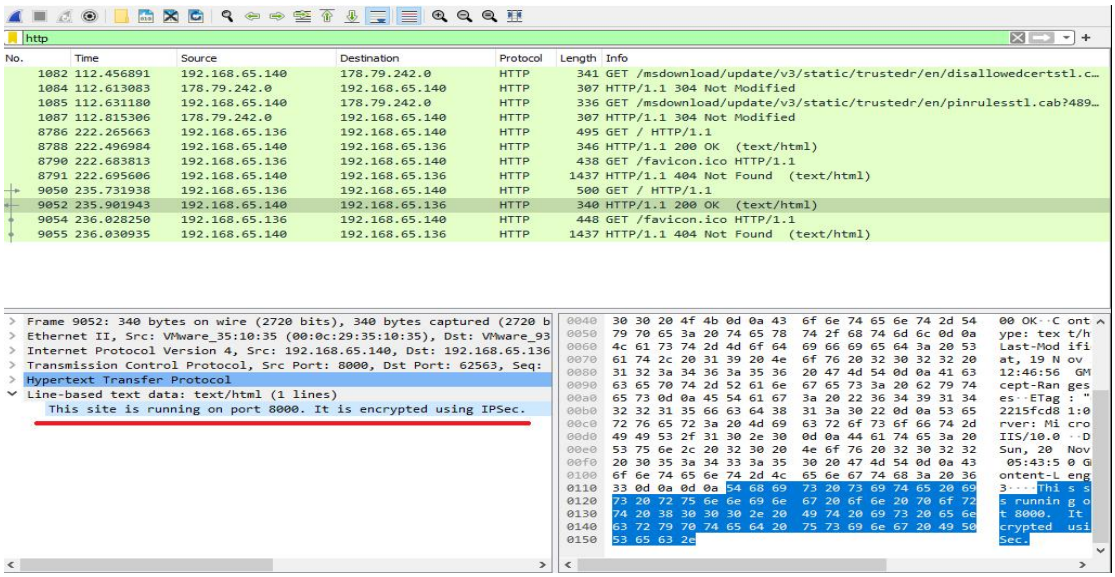
Then go to wire shark.



Stop capturing. In the filter box type http to display HTTP traffic as show above. Now select **HTTP/1.1 200 OK (text/html)** frames.



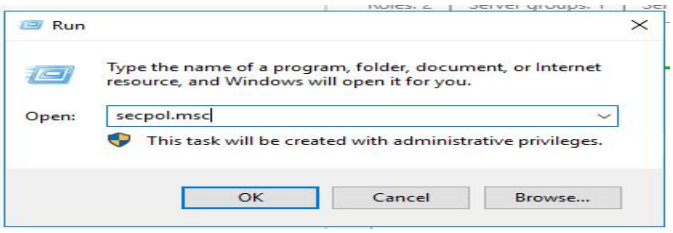
This displays the contents of the first web site. Similarly select the second frame.



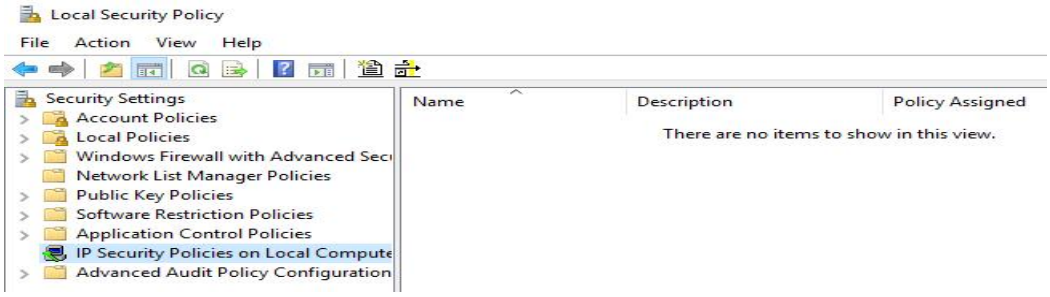
The above frame displays the contents of the second website.

3. **Configure IPSec policy on the web server**.

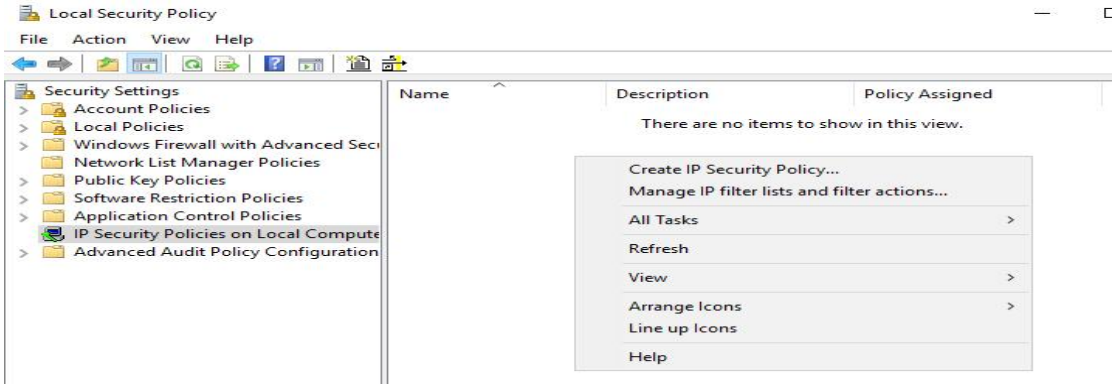
On the server where we configured web sites, go to run and type secpol.msc as shown below.



This will open the security policy of the server as shown below.



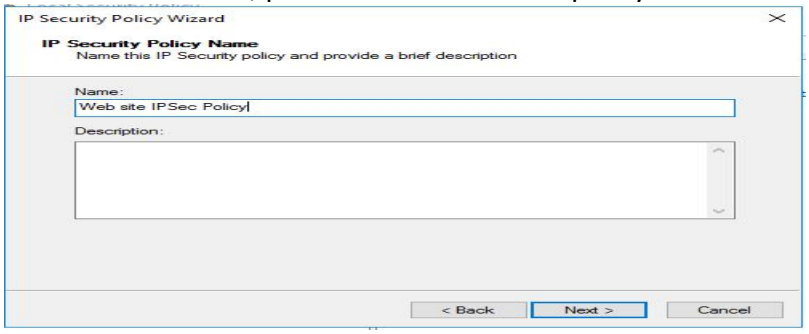
Click to select IP Security Policies on Local Computer. By default there is no policy. Right click and then click Create IP Security Policy option.



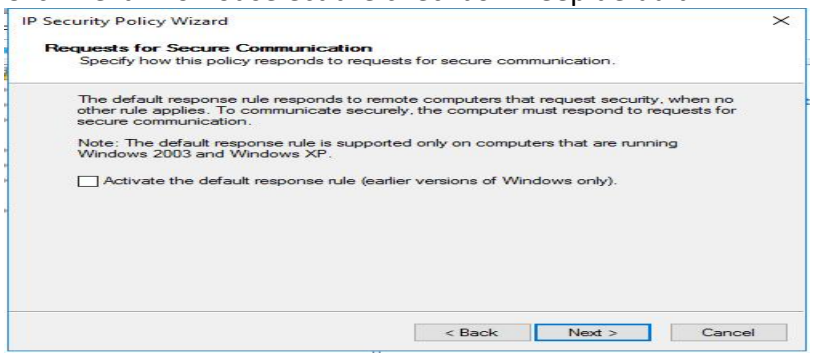
This will stat the following Wizard.

Click Next.

On the next screen, provide a name for the policy as shown below.

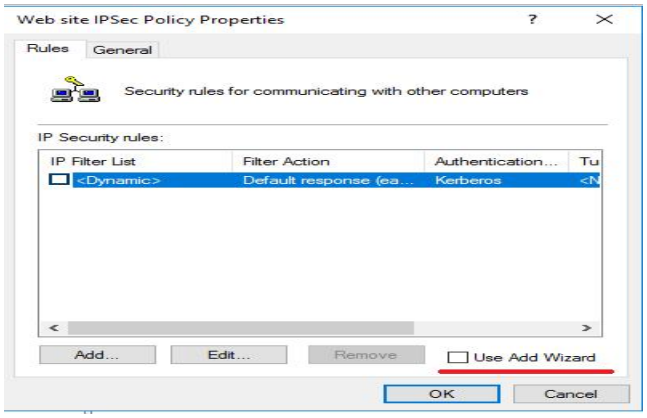


Click Next. Do not select the checkbox. Keep default.

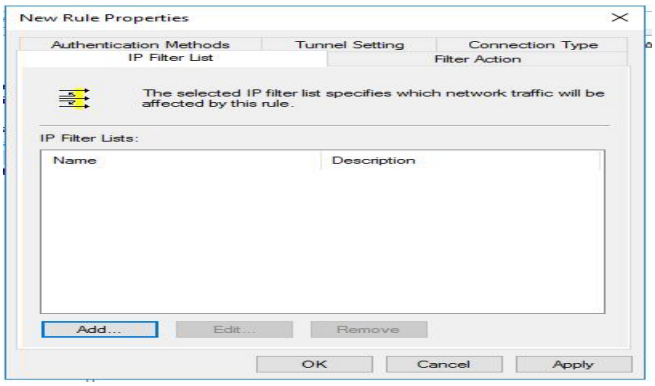


Click Next.

N the above screen keep Edit properties checkbox selected. Click Finish. This will create a policy and edit its properties as shown below.

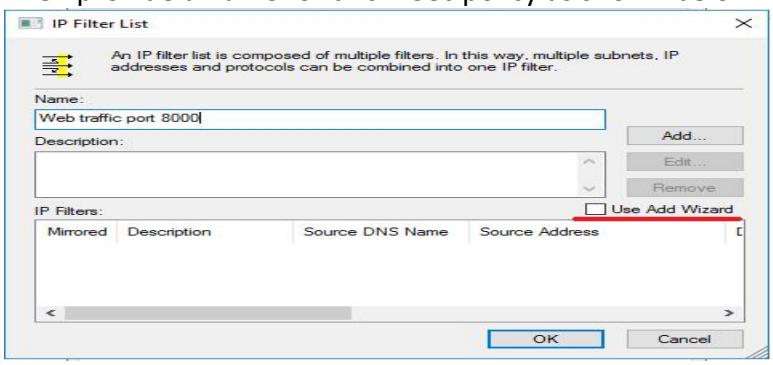


Remove the tick from the check box for Use Add Wizard . Click Add button.

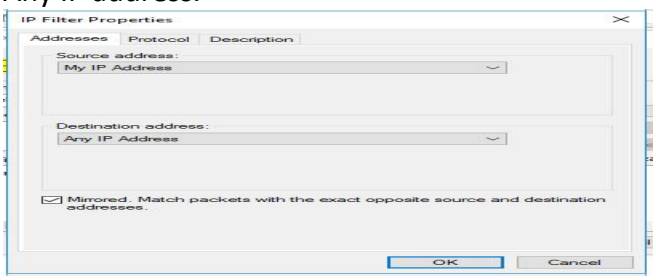


On the window that opens, click Add.

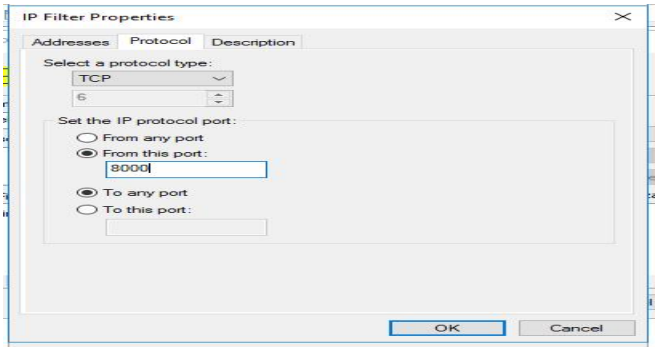
On the following window that opens, first remove the tick from Use Add Wizard. Then provide a name for this IPSec policy as shown below.



Click Add button. Following window opens. Here we need to identify the traffic that will be encrypted by the applied IPSec policy. In this lab we are going to apply IPSec policy for the traffic between web server TCP port 8000 to any client port.
As we are defining policy on the Web server, My IP Address in the source will be the web server IP address. Destination address will be client IP address. Thus keep as Any IP address.



Click Protocol tab on the same window.

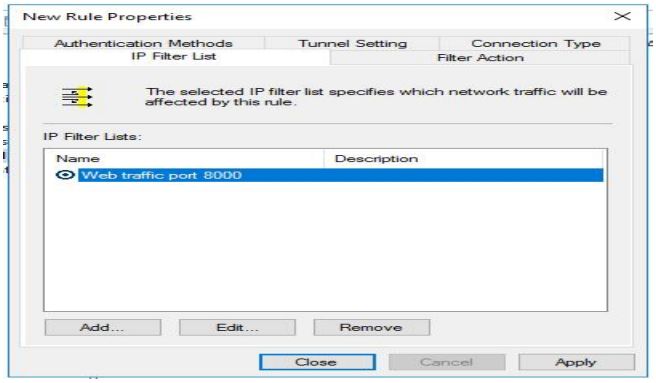


On this tab in the Protocol type select TCP.

In the From the port field type 8000.

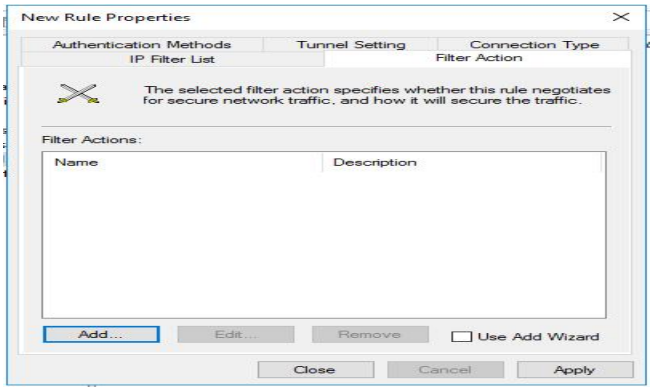
Keep To any port as it is. Click Ok to close the window.

Thus here we identified the traffic going from web server IP and TCP port 8000 to Any client IP address and any port on client.



Click OK to close the window.
The adjacent window should appear.
Make sure you click the circle in front of the Web traffic port 8000.
A dot should appear in the circle as shown.

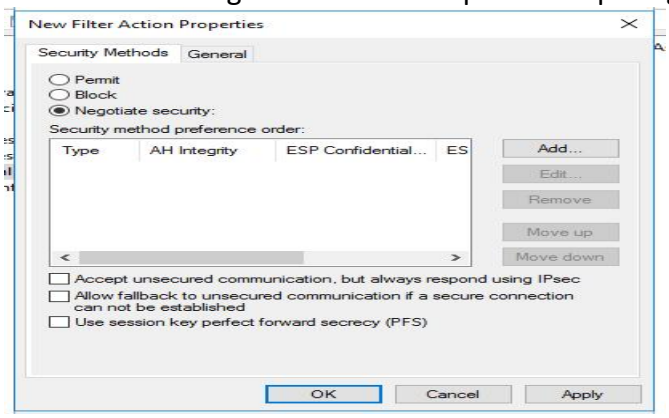
Next click the Filter Action tab on the above window.



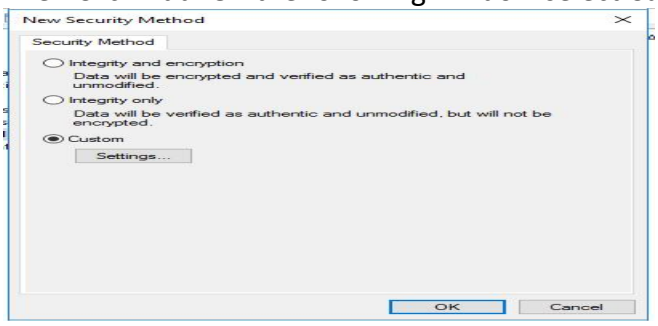
On the Filter Action tab, first remove the tick from the check box of **Use Add Wizard**.

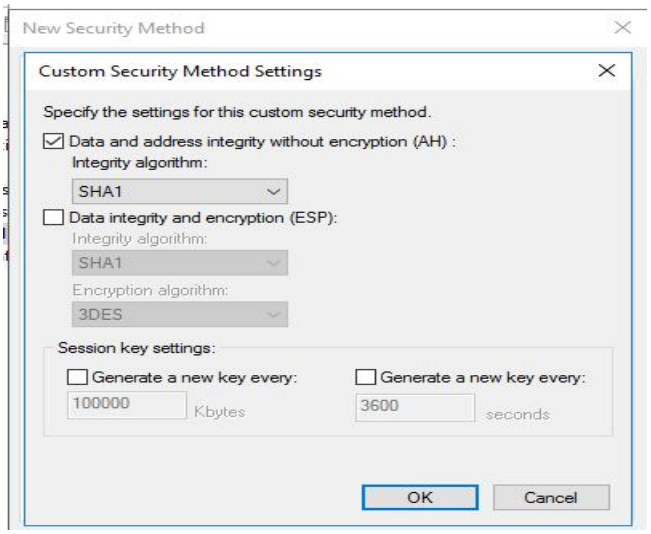
Then Click Add.

On the Following window that opens. Keep Negotiate Security option selected.



Then Click Add. On the following window select Custom and click Settings button.





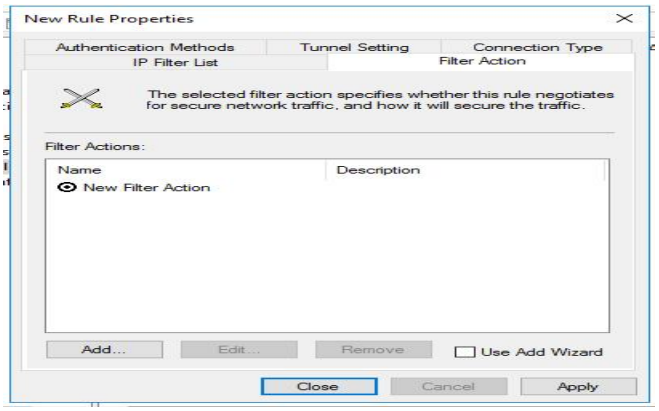
On this Screen Select Data and address integrity without encryption check box.

Select SHA1 from the drop down list.

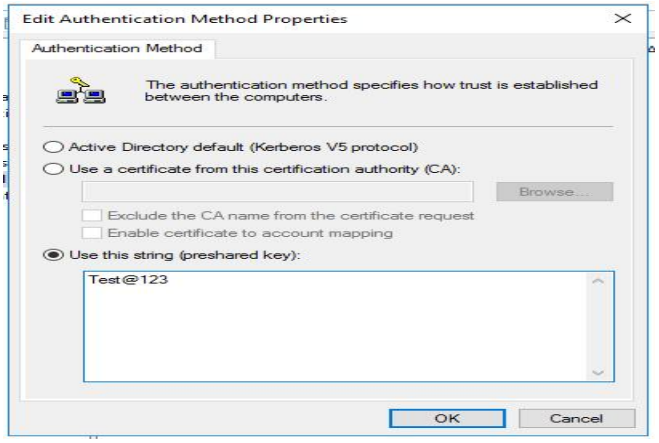
First we will implement AH protocol of IPSec and check the frames.

Click OK.

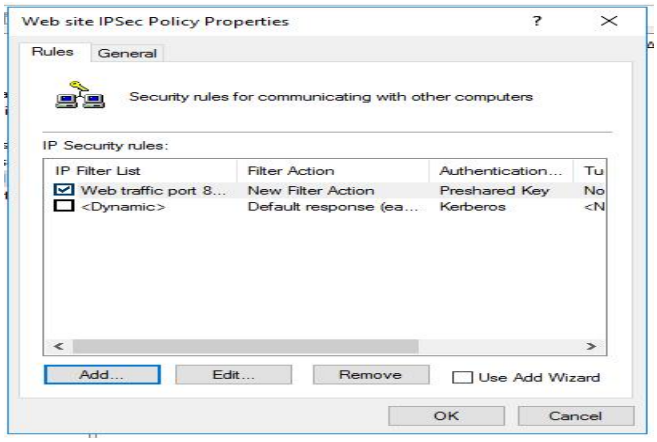
Click OK. Click OK and finally Click Apply button. Then click OK . Following screen is displayed. Click the circle in front of New Filter Action. Make sure the dot is shown inside the circle.



Click **Authentication Methods** tab in the above window. Click Edit button. Following window is displayed.
Select Use this string (preshared key) option. Then type a string. This string needs be same on the client. Thus remember the string. It is case sensitive.

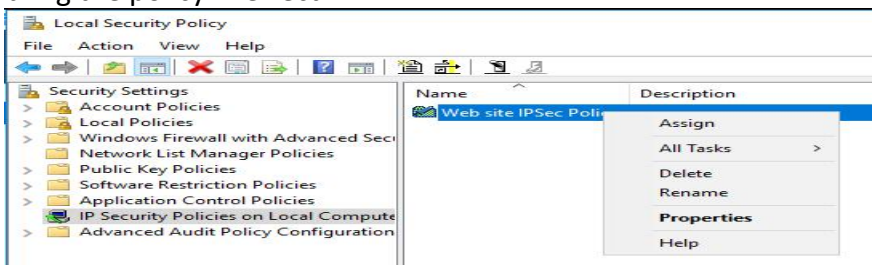


Click OK. Then Click Apply. Again Click OK on the window.
Finally following window is displayed.



On the above window make sure the Web traffic port check box is selected. Click OK.

This will create the IPSec policy. Right click on the IPSec policy name. Click Assign to bring the policy in effect.

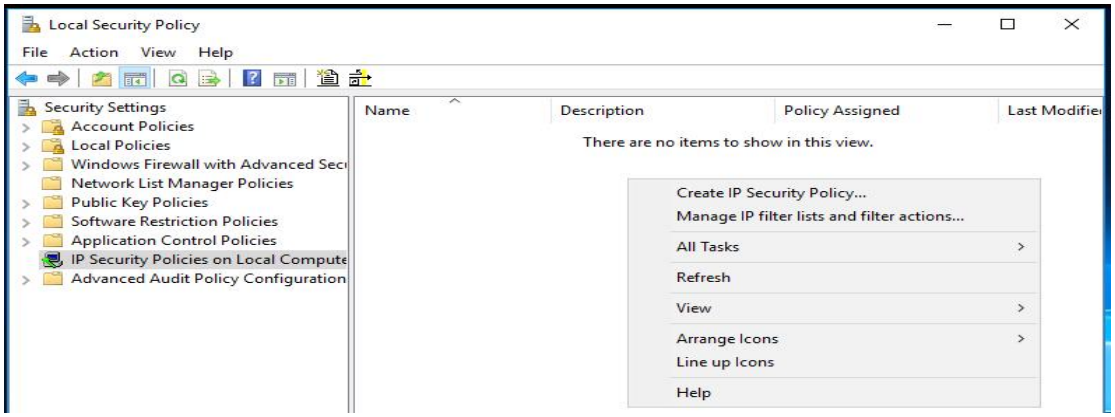


4. **Configure IPSec policy on the client.**

Now if you try to open the website from the client, the web site running on port 8000 will not open. This is because IPSec on Web sever is active and requires the client also to perform IPSec.

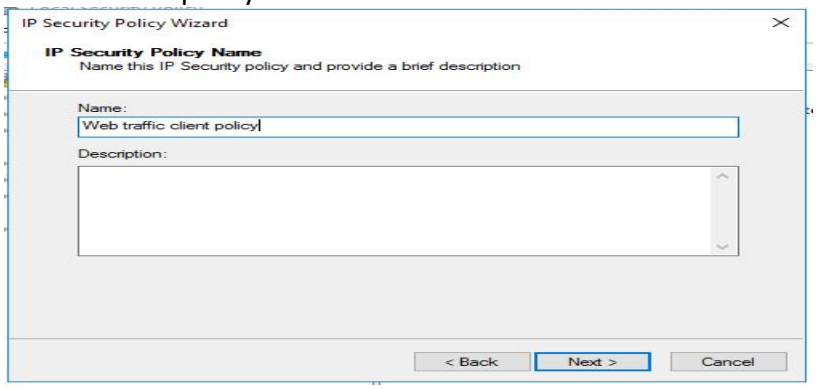
Now we will create the IPSec policy on the client.

Go to Run and type **secpol.msc**.

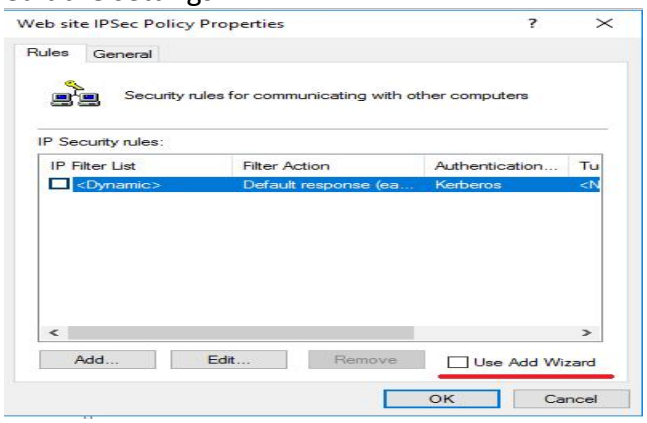


Select IP Security Policies on Local Computer. Right click and select Create IP Security Policy.

Click Next on the Policy creation Wizard page. On the following screen Provide a name for the policy.

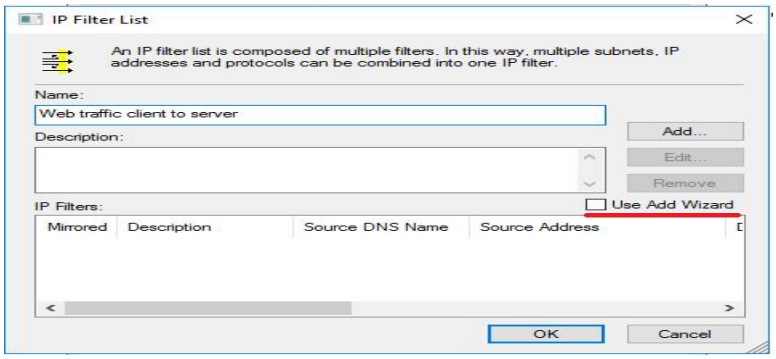


Click Next. Click Next on next window. Finally click Finish to create the policyand edit the settings.

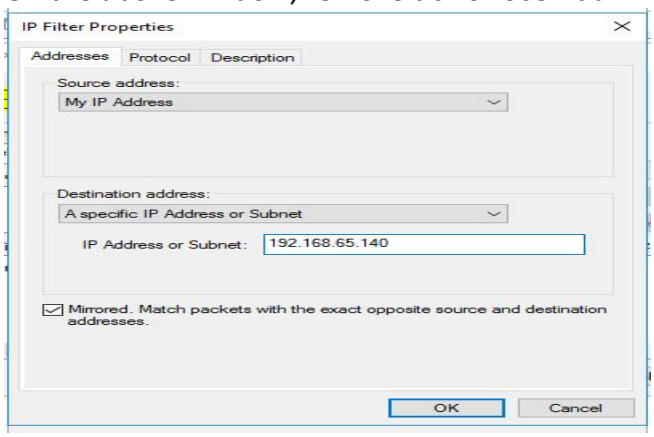


Remove Use Add Wizard tick.

Click Add. On the next window also click Add.

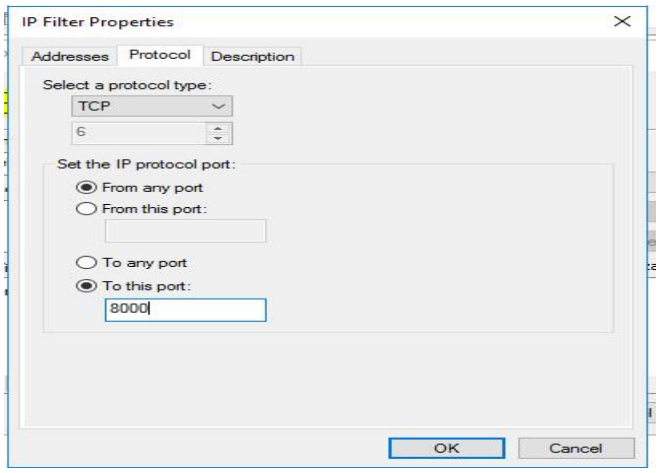


On the above window, remove tick of Use Add Wizard. Provide a name. Click Add.



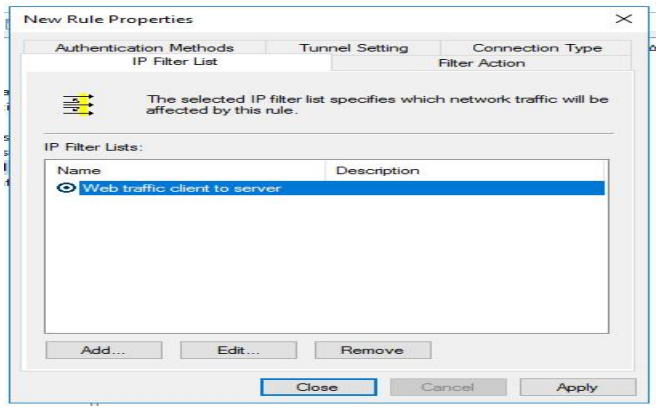
On this window we identify the traffic from client to Web server. Thus Source address will be My IP address means client IP. Destination address will be your web server IP address.

Click Protocol tab.



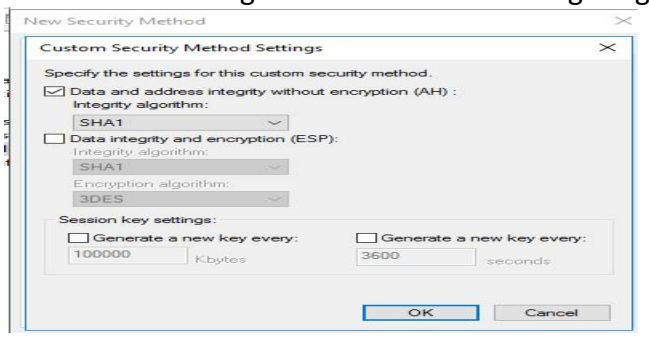
As we are identifying the traffic from client to Web server, select protocol as TCP.
As client will open a random port, From any port will be selected.
Destination will be the Web server port, thus select To this port and type 8000.
Click OK

Click OK again. The following window is displayed.

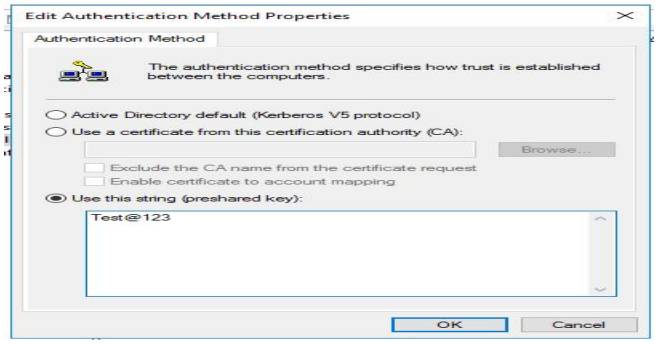


Make sure you click the circle in front of filter list name and a dot appears.

Click Filter Action tab.
On this window make sure you remove tick from the Use Add Wizard check box.
Then Click Add.
On the New window that opens select Negotiate Security. Click Add.
On the next Window select Custom and Click Settings tab.
(***** These steps are same as the IPSec configuration on the web server. Thus you can refer to those screen shots or steps.**)
Select same settings as selected while configuring the web server policy.



Click OK. Click OK again. Then click Apply.
Then click Authentication Methods. Click Edit. Select preshared key option. Typethe same key as typed on the Web server as shown below.



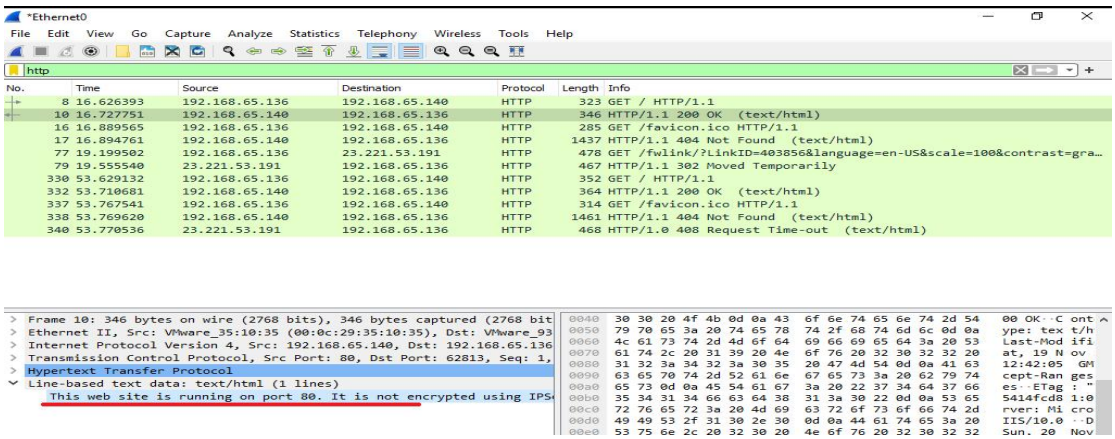
Click OK.
Click OK on all windows to close the policy properties.
This will display the policy. Right Click on the policy and assign.

Thus Client side IPSec policyis created and applied.
Now both server and client sould be able t create an IPSec tunnel.

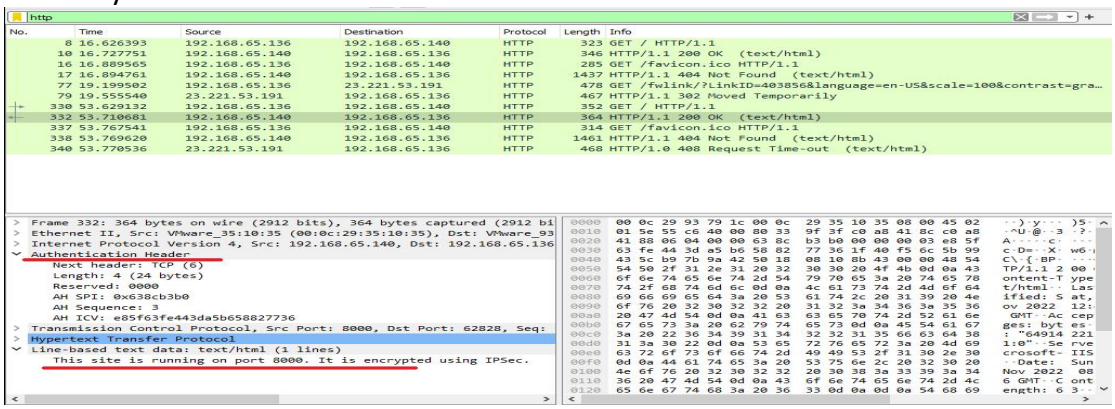
5. Checking if IPSec is working.

Ope Wireshark. Start Capturing. Open Browser. Clear history. Then open both web sites. Stop wireshark. Again apply http filter and check 200 OK frames.

For website running on port 80, there is no difference as IPSec is not applied to this traffic.



But for the website running on port 8000, an additional Authentication Header is added by IPSec.

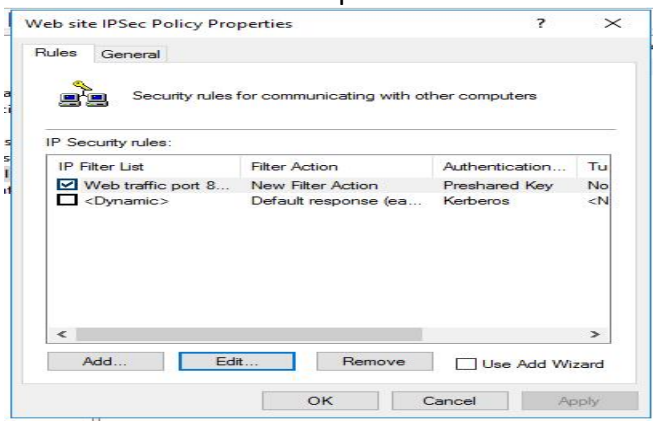


You are able to see the contents of the web page. Thus AH protocol of IPSec is not encrypting the data. It is just calculating hash and attaching it. Thus it provides authentication and integrity.

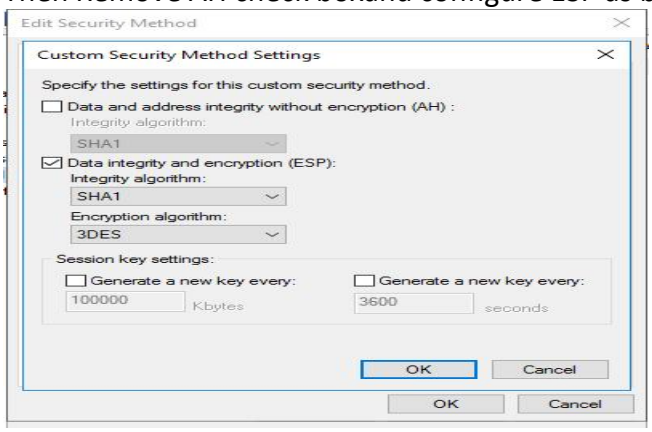
6. Changing from AH to ESP in IPSec.

Now we will shift to ESP and check if encryption happens.

On the Web Server go to secpol.msc. Select IP Security policy. Double click the policy name that we created earlier.
In the new window that opens click Edit.



Then click the **Filter Action** tab. Click Edit. Again Click Edit. ThenBelow Customs option click Settings tab.
Then Remove AH check boxand configure ESP as below.



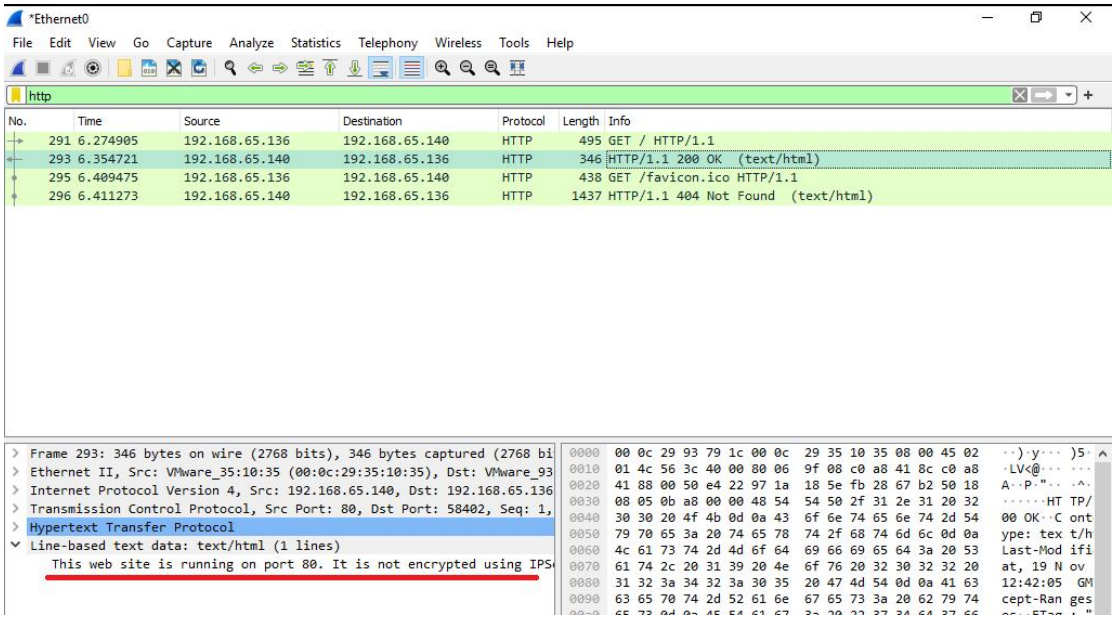
Click OK. Click OK if any message is displayed. Click Apply and then Click OK.
Then click close. On the final window click Apply and close.

Follow the same steps on the client server and change from AH to ESP.

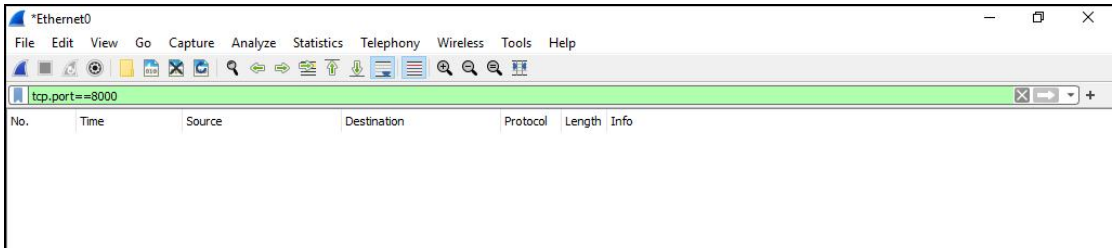
7. Test ESP Configuration.

Start Wireshark. Start capture. Open browser. Clear History. Then open both the web sites.

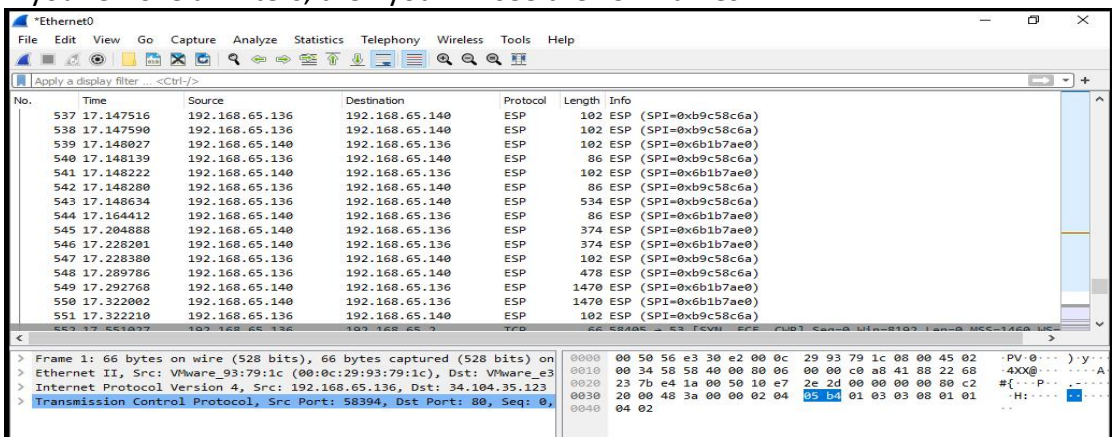
Now when you apply filter http in Wireshark, you will get HTTP traffic only for the web site running on port 80.



But you can see that now there are no http frames for port 8000 web site traffic.
Try applying a filter for TCP port 8000. (tcp.port==8000)



No frames are shown.
This is because ESP encrypts the entire thing.
If you remove all filters, then you will see the ESP frames.



This is how the IPSec policy is tested successfully.

Make sre you delete IPSec policy from both the servers.