

Configure IPSec policy on Windows Server to protect HTTP Server traffic

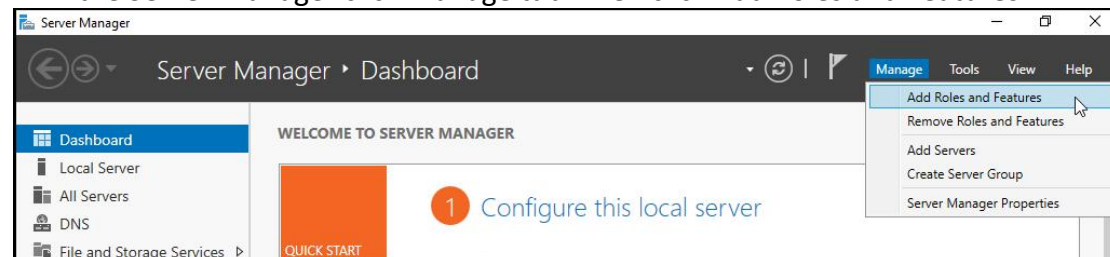
This lab will demonstrate the steps to configure IPSec between two Windows Server. For this lab Windows 2016 Server standard evaluation version is used. One Windows Server will be configured to host the web server. The other server will be the client.

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.

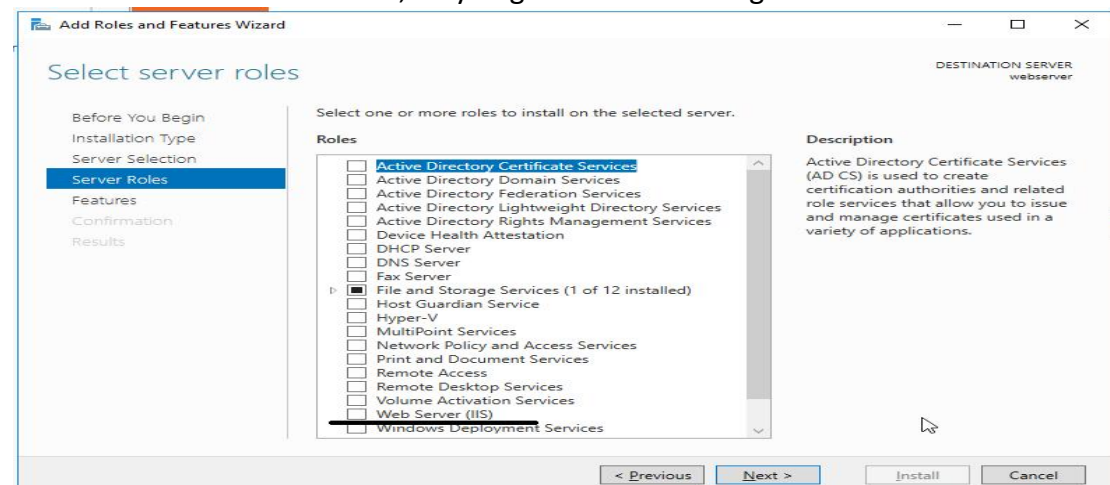
1. Configure IIS web server on one of the server.

A. Login as administrator.

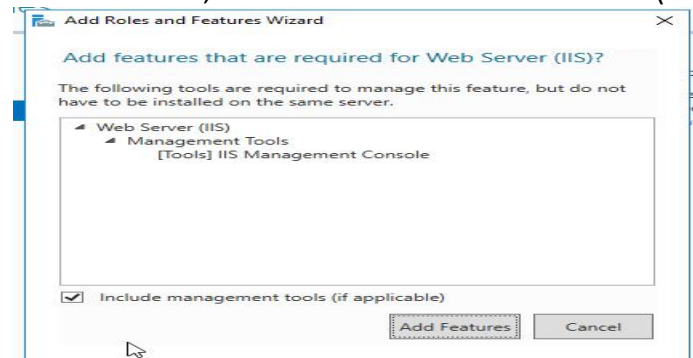
B. In the Server Manager click Manage tab. Then click Add Roles and Features.



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

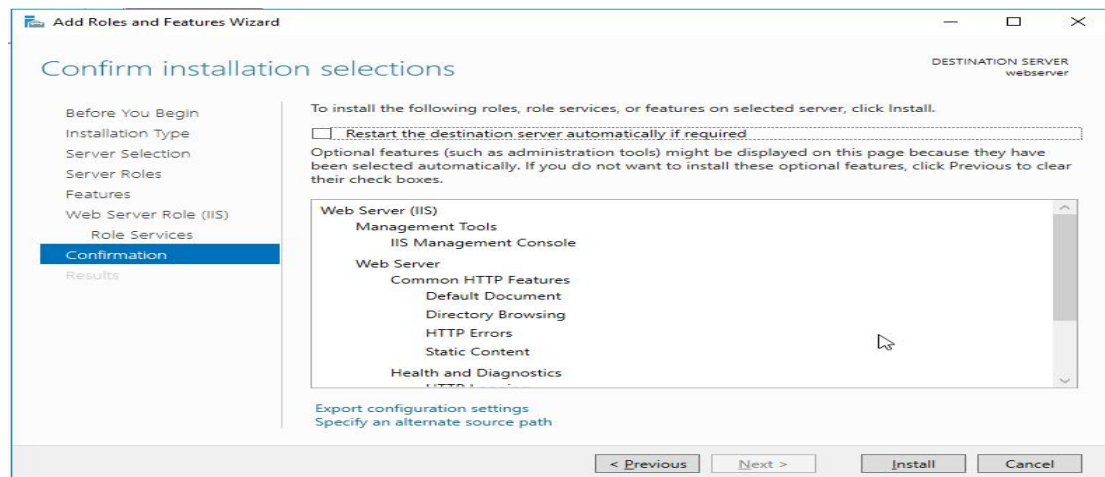


In this window, click the check box of Web Server(IIS).

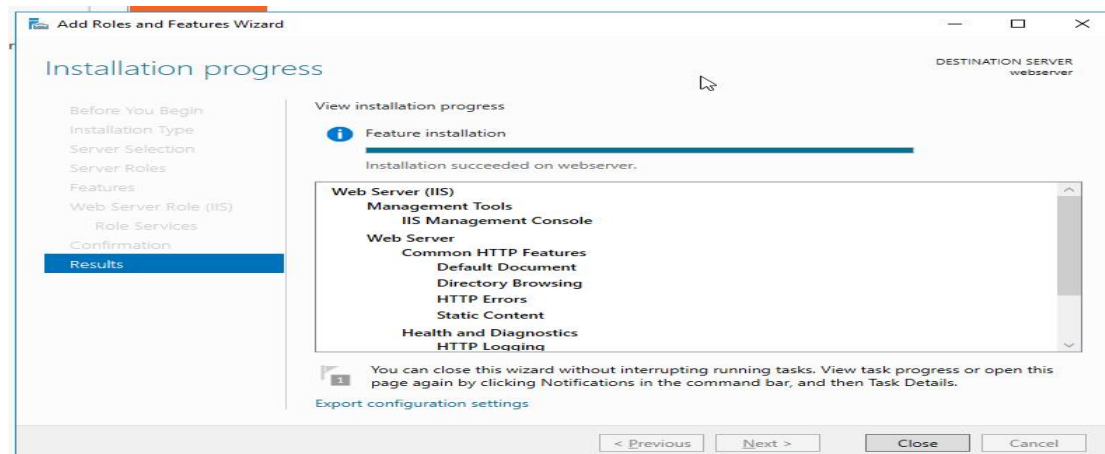


Click Add Features on the window that opens when you click the check box.

Click Next on all windows till you get following window.



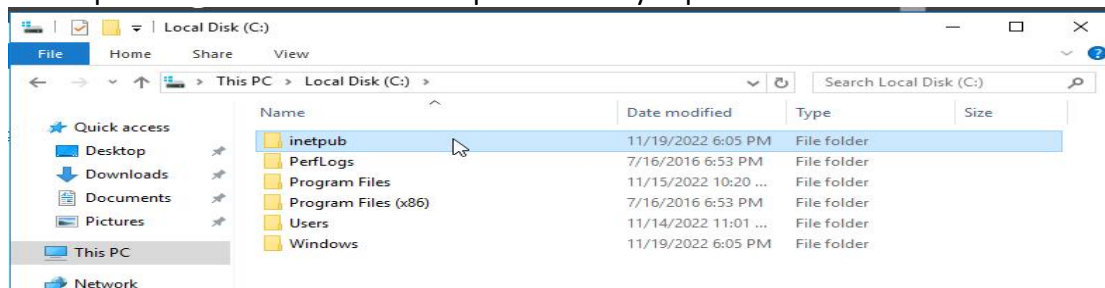
Click Install. This will install the web server on the Windows server.



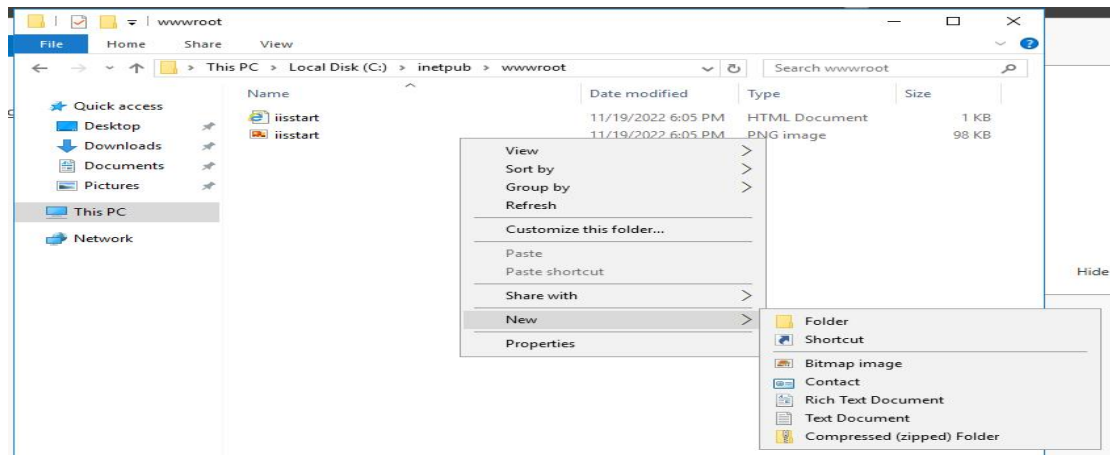
Once the installation is successful, click Close.

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.

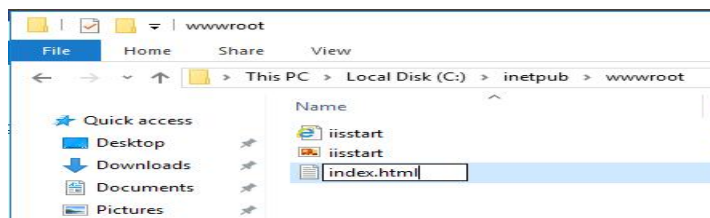
Thus open c:. Then double click inetpub directory. Open wwwroot below it.



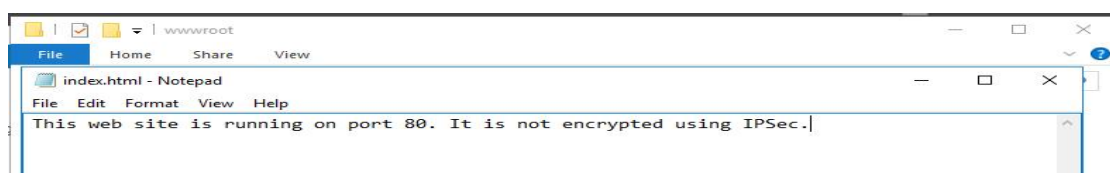
In the wwwroot directory, right click and click New. Then select Text Document. As shown below.



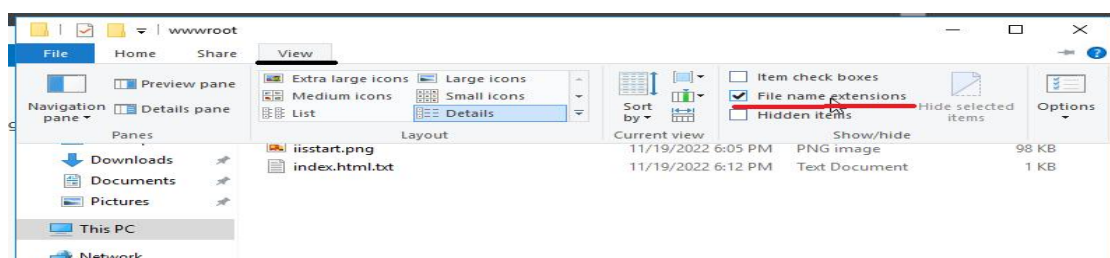
Provide the file name as **index.html**. The web server is designed to show the first web page by this name.



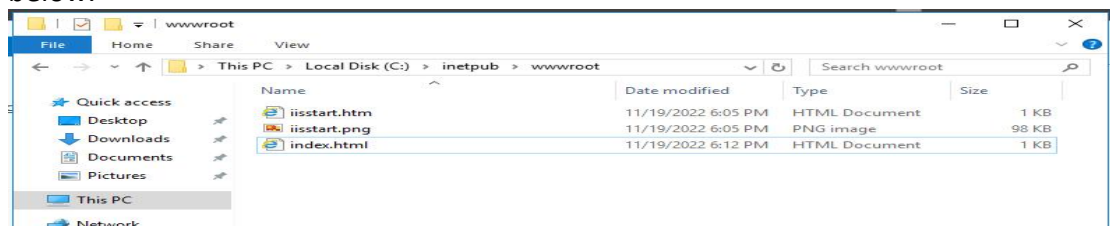
Edit file and type any text. This will be displayed in the client browser.



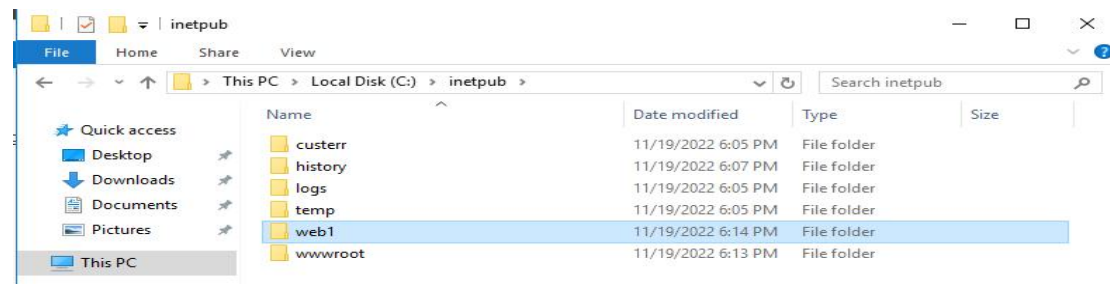
Save and close the file. Actually the file name becomes index.html.txt. However Windows hides the file extension. Thus to configure Windows to display file extensions, click View. Then click the check box of File name extensions. This will display the file name extensions.



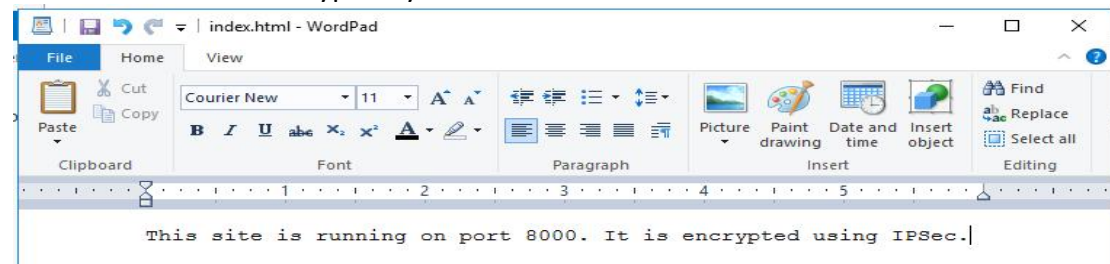
Rename the file. Remove the .txt extension. The file will be index.html as shown below.



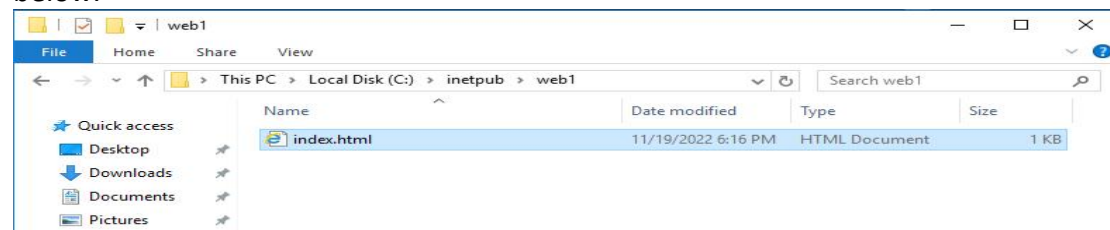
Now we will create a directory for the second web site. Go back to inetpub directory. Create a new directory by any name. Here the name given is **web1** as shown below.



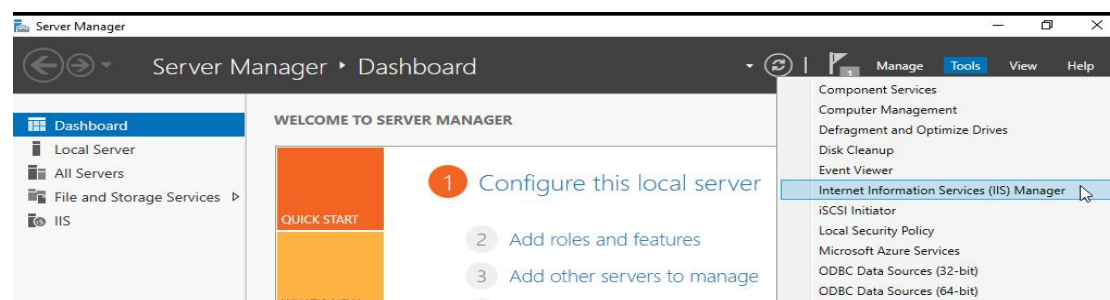
Now go into that directory. Right click and create a text document. Name the file as index.html. Edit it and type any text in it as shown below.



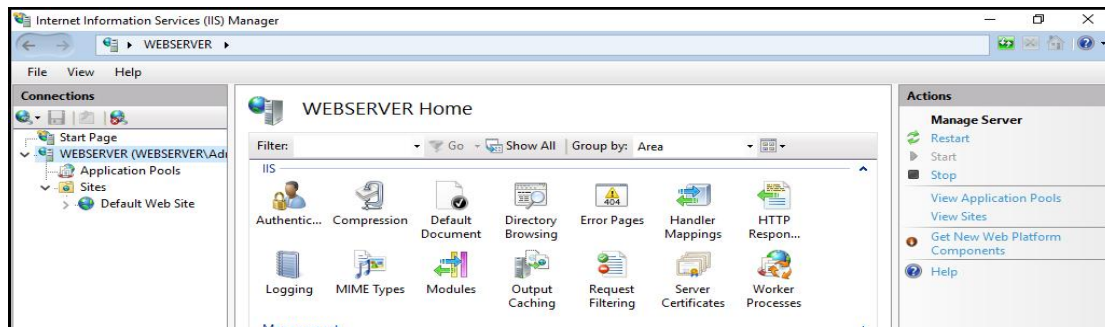
Save the file. Rename the file. Remove the .txt extension. The file will be as shown below.



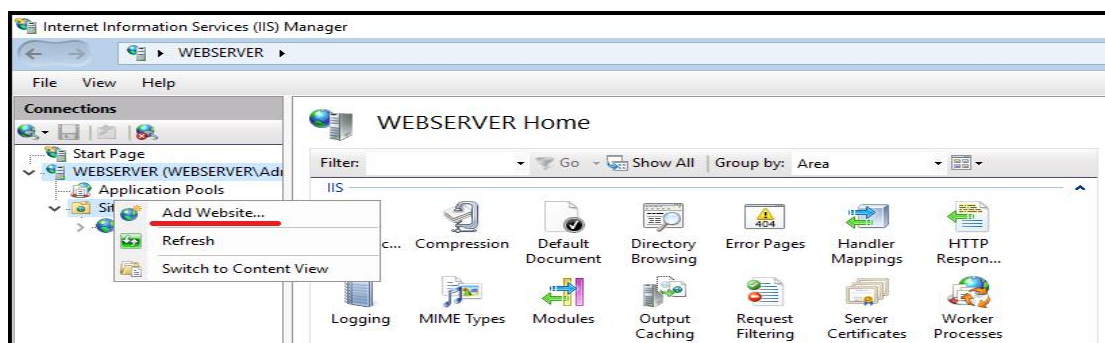
Now we will create the second website. For this go to Server Manager. Click Tools. In the list displayed, click Internet Information Service (IIS) Manager as shown below.



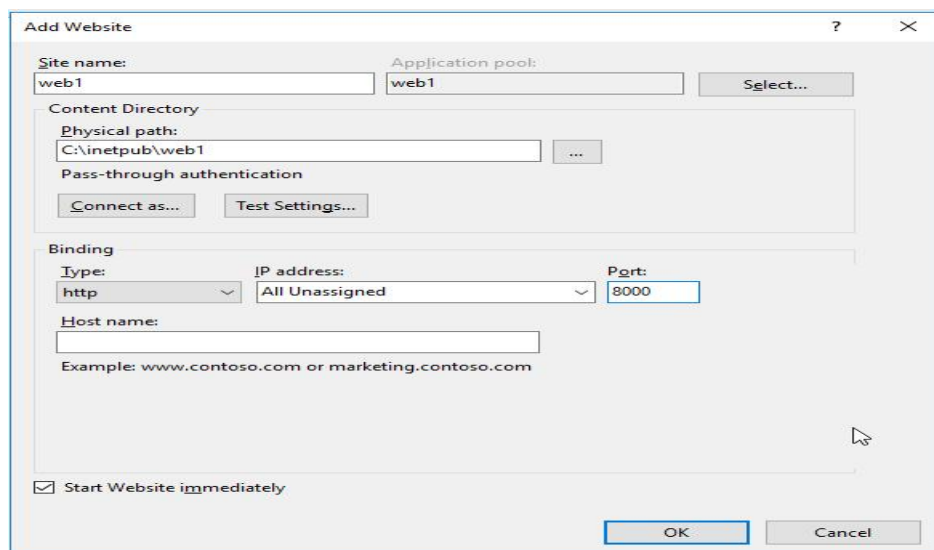
Following window opens. Server name will be displayed on the left side. Click the expand button. It will display Application Pool and Sites. Expand sites. This will display the Default Web Site created as shown in the below screenshot.



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



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



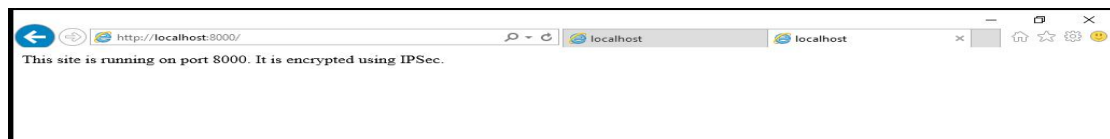
Type some name in the Site name field. Click three dots in front of Physical Path. Select the web1 directory created below C:\inetpub.

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.

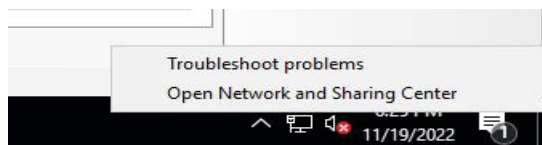


Open another tab and type <http://localhost:8000>. This will open the second web site.

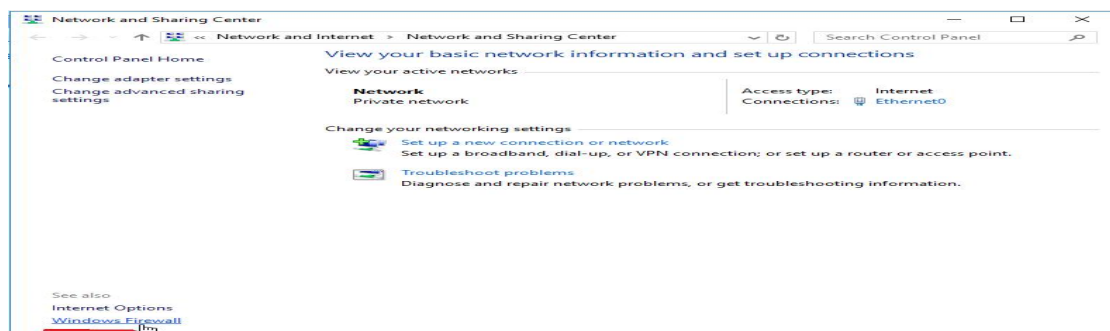


Thus both websites are working properly. Now we will open the ports in the Windows firewall. This will allow other computers in the network to open websites as by default firewall blocks access to all ports.

To open firewall configuration, right click on the computer icon displayed near date and time. This will display following options.



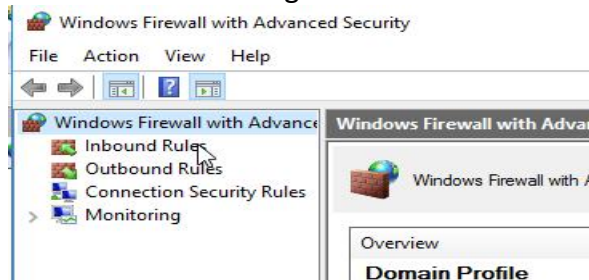
Click Open Network and Sharing Center. Following window will open.



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

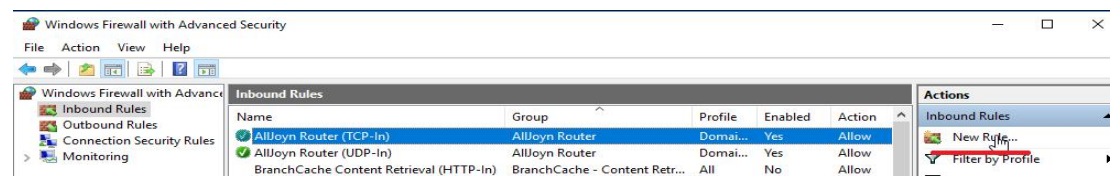


Click Advanced settings on the left side as shown above. Following window opens.

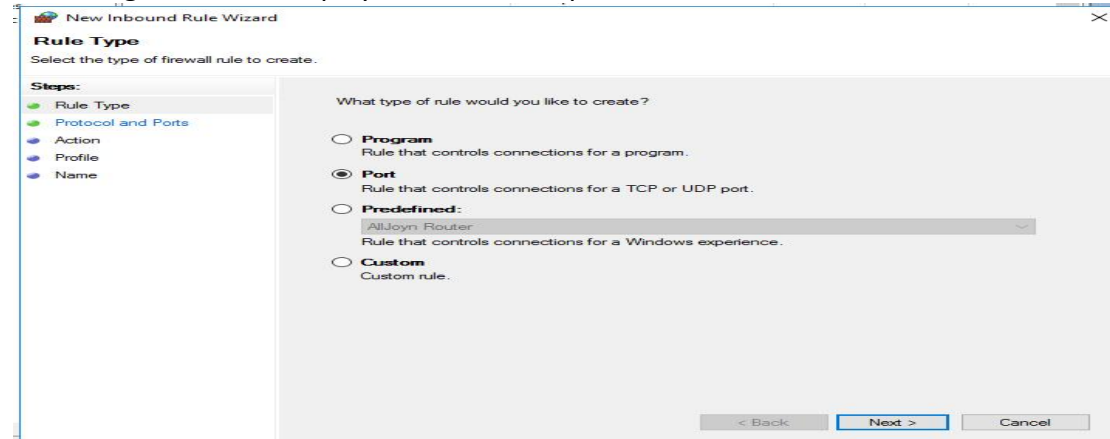


Click Inbound Rules.

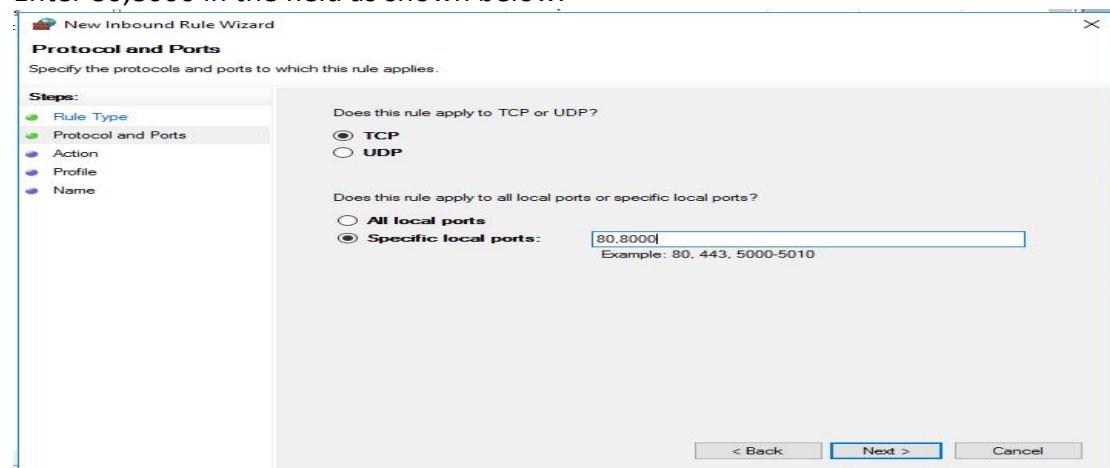
Now click New Rule option on extreme right side as shown below.



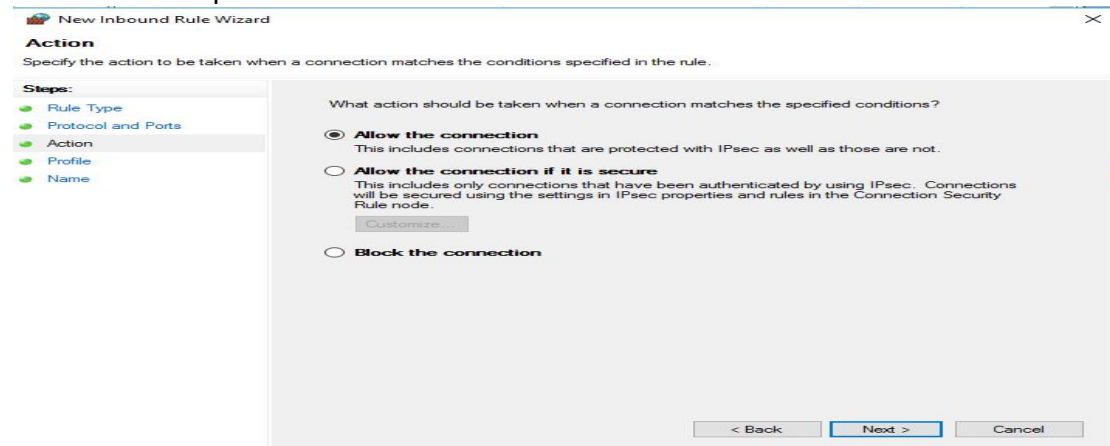
Following window is displayed. Click Port option.



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

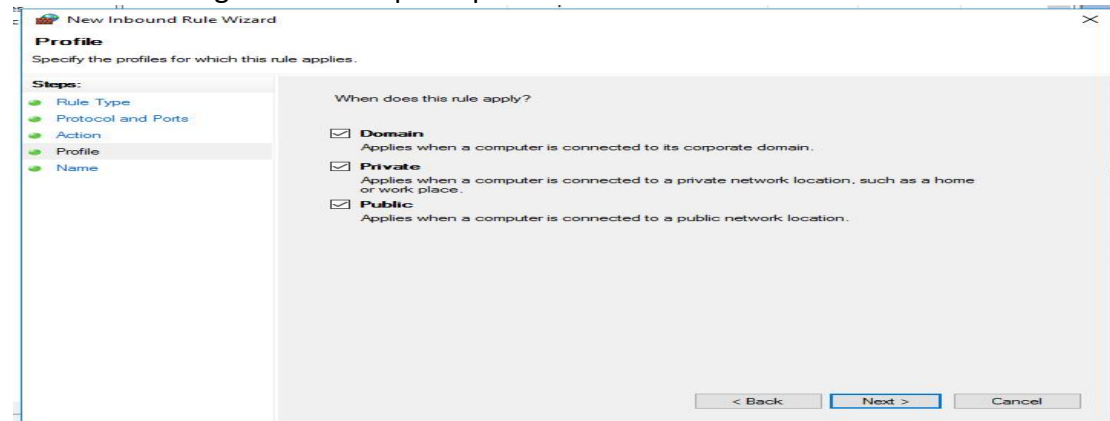


Click Next. Keep Allow the Connection.

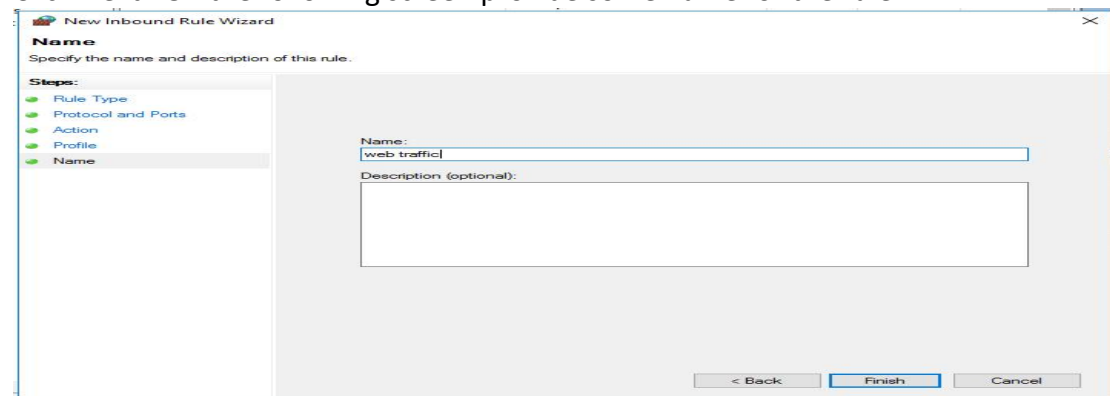


Click Next.

On the following window keep all options selected.



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

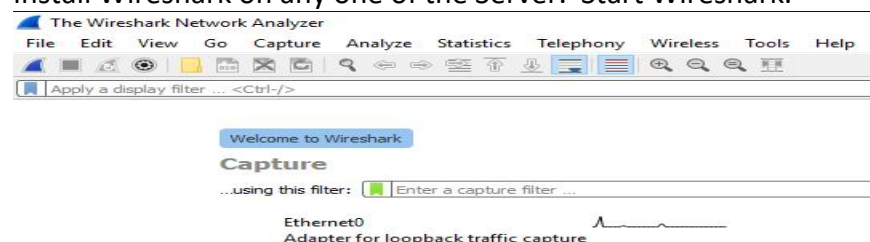


Click Finish to add the rule to the firewall.

2. Capture traffic using Wireshark

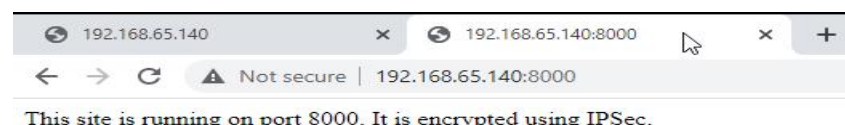
Now we will capture the traffic on one of the server to check that http traffic is sent in plain text. This will show the web page content in the Wireshark. Later we will configure IPSec to secure this traffic.

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



Click Ethernet0 to start capturing Frames.

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



Then go to wire shark.

No.	Time	Source	Destination	Protocol	Length	Info
1082	112.456891	192.168.65.140	178.79.242.0	HTTP	341	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.c...
1084	112.613083	178.79.242.0	192.168.65.140	HTTP	307	HTTP/1.1 304 Not Modified
1085	112.631180	192.168.65.140	178.79.242.0	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?489...
1087	112.815306	178.79.242.0	192.168.65.140	HTTP	307	HTTP/1.1 304 Not Modified
8786	222.265663	192.168.65.136	192.168.65.140	HTTP	495	GET / HTTP/1.1
8788	222.496984	192.168.65.140	192.168.65.136	HTTP	346	HTTP/1.1 200 OK (text/html)
8790	222.683813	192.168.65.136	192.168.65.140	HTTP	438	GET /favicon.ico HTTP/1.1
8791	222.695606	192.168.65.140	192.168.65.136	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
9050	235.731938	192.168.65.136	192.168.65.140	HTTP	500	GET / HTTP/1.1
9052	235.901943	192.168.65.140	192.168.65.136	HTTP	340	HTTP/1.1 200 OK (text/html)
9054	236.028250	192.168.65.136	192.168.65.140	HTTP	448	GET /favicon.ico HTTP/1.1
9055	236.030935	192.168.65.140	192.168.65.136	HTTP	1437	HTTP/1.1 404 Not Found (text/html)

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.

Frame 8788: 346 bytes on wire (2768 bits), 346 bytes captured (2768 b...
 Ethernet II, Src: VMware_35:10:35 (00:0c:29:35:10:35), Dst: VMware_93...
 Internet Protocol Version 4, Src: 192.168.65.140, Dst: 192.168.65.136
 Transmission Control Protocol, Src Port: 80, Dst Port: 62560, Seq: 1,
 Hypertext Transfer Protocol
 Line-based text data: text/html (1 lines)
 This web site is running on port 80. It is not encrypted using IPSec.

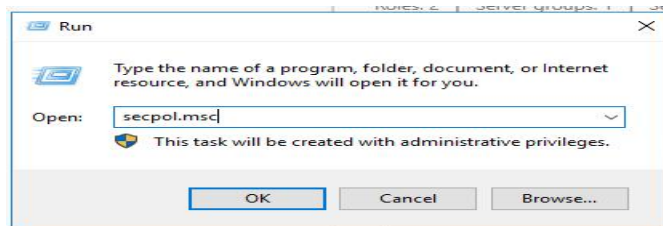
This displays the contents of the first web site. Similarly select the second frame.

Frame 9052: 340 bytes on wire (2720 bits), 340 bytes captured (2720 b...
 Ethernet II, Src: VMware_35:10:35 (00:0c:29:35:10:35), Dst: VMware_93...
 Internet Protocol Version 4, Src: 192.168.65.140, Dst: 192.168.65.136
 Transmission Control Protocol, Src Port: 8080, Dst Port: 62563, Seq: 1,
 Hypertext Transfer Protocol
 Line-based text data: text/html (1 lines)
 This site is running on port 8080. It is encrypted using IPSec.

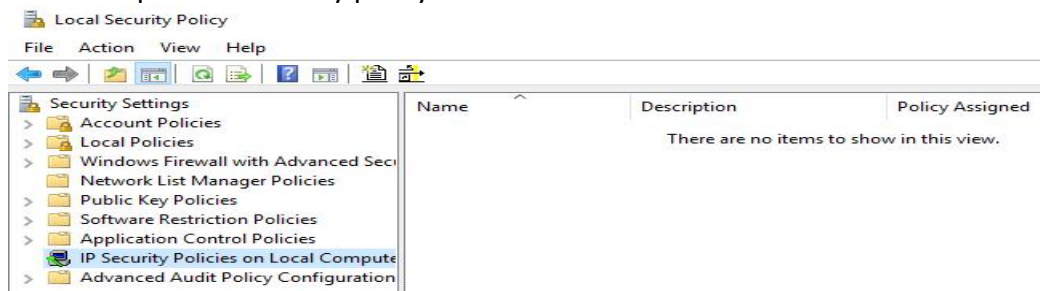
The above frame displays the contents of the second website.

3. Configure IPSec policy on the web server.

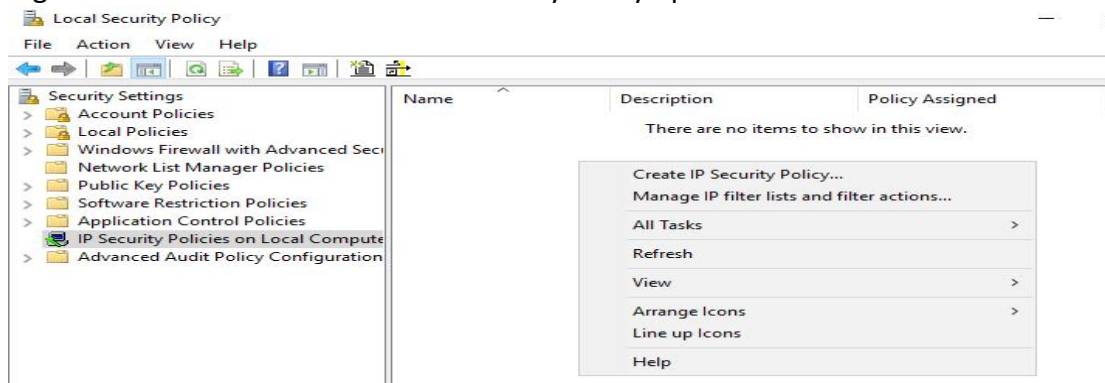
On the server where we configured web sites, go to run and type secpol.msc as shown below.



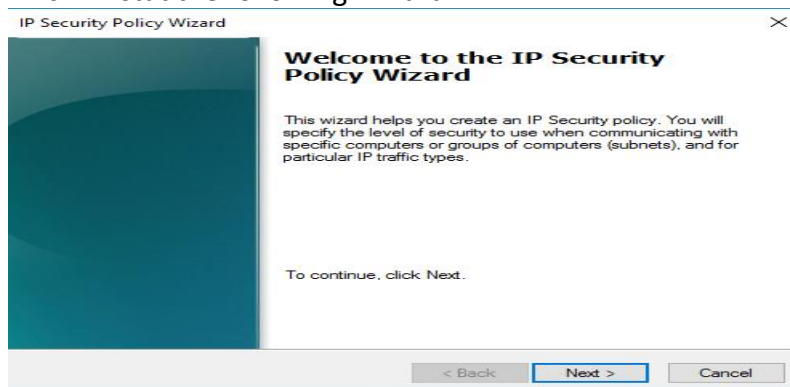
This will open the security policy of the server as shown below.



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.

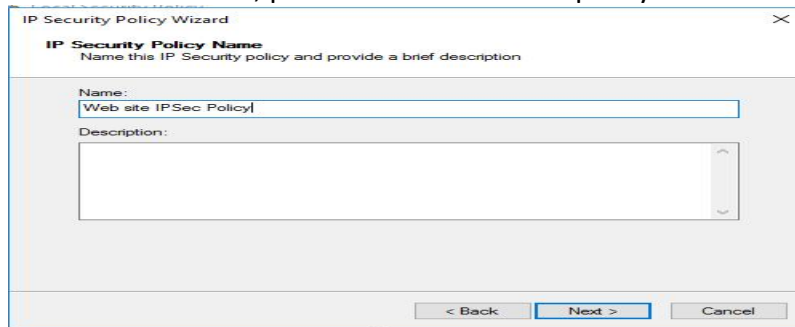


This will start the following Wizard.



Click Next.

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



IP Security Policy Wizard

IP Security Policy Name
Name this IP Security policy and provide a brief description

Name:
Web site IPSec Policy

Description:

< Back Next > Cancel

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



IP Security Policy Wizard

Requests for Secure Communication
Specify how this policy responds to requests for secure communication.

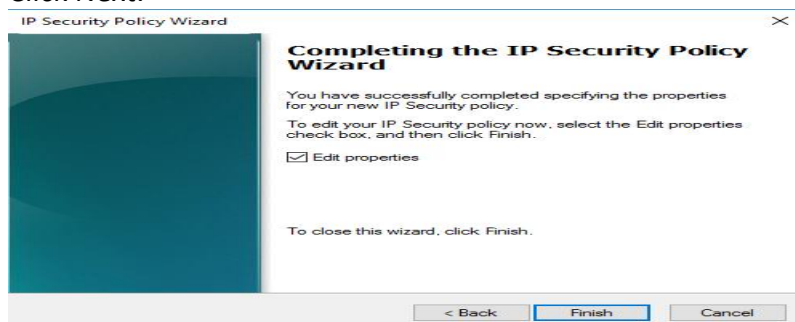
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.

☐ Activate the default response rule (earlier versions of Windows only).

< Back Next > Cancel

Click Next.



IP Security Policy Wizard

Completing the IP Security Policy Wizard

You have successfully completed specifying the properties for your new IP Security policy.

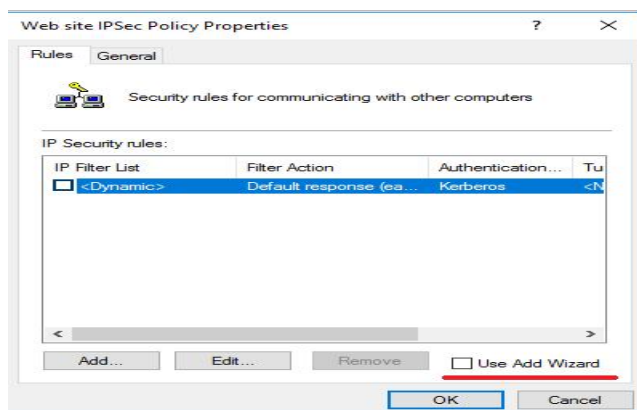
To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☒ Edit properties

To close this wizard, click Finish.

< Back Finish Cancel

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



Web site IPSec Policy Properties

Rules General

Security rules for communicating with other computers

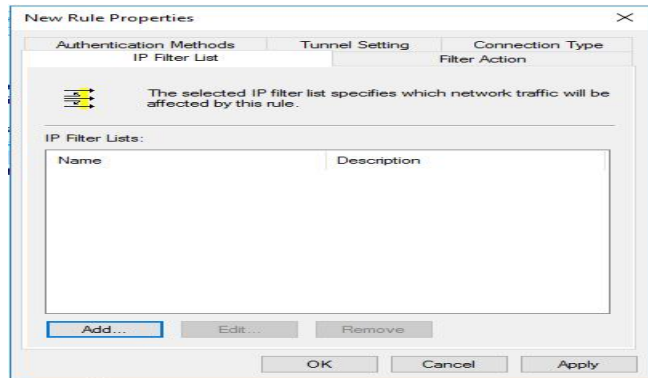
IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
<input type="checkbox"/> <Dynamic>	Default response (ea...	Kerberos	<N

Add... Edit... Remove ☐ Use Add Wizard

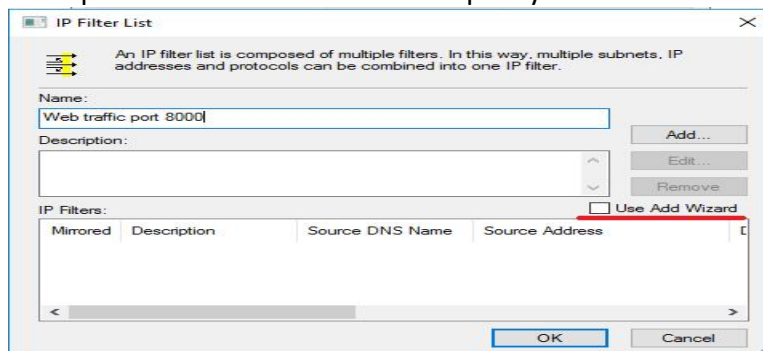
OK Cancel

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



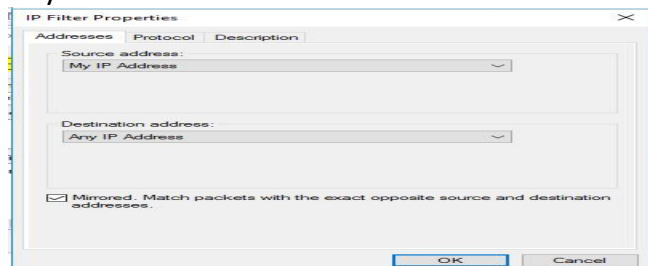
On the window that opens, click Add.

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.

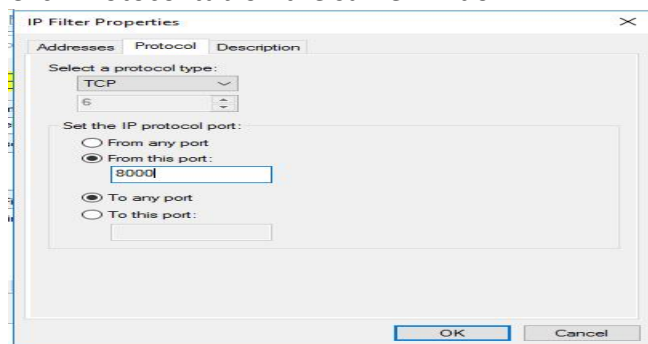


Click Add button. Following window opens. Here we need to identify the traffic that will be encrypted by the applied IPsec policy. In this lab we are going to apply IPsec policy for the traffic between web server TCP port 8000 to any client port.

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.

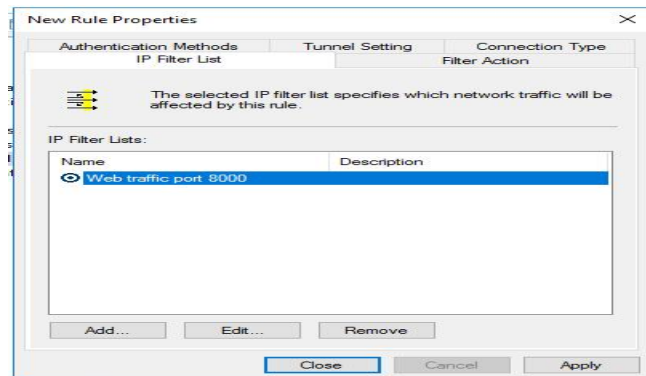


On this tab in the Protocol type select TCP.

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.



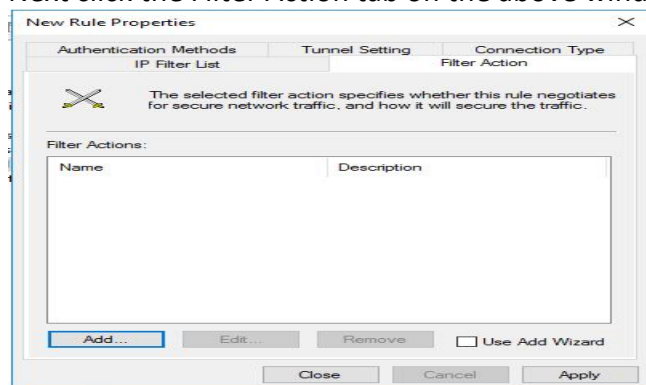
Click OK to close the window.

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.

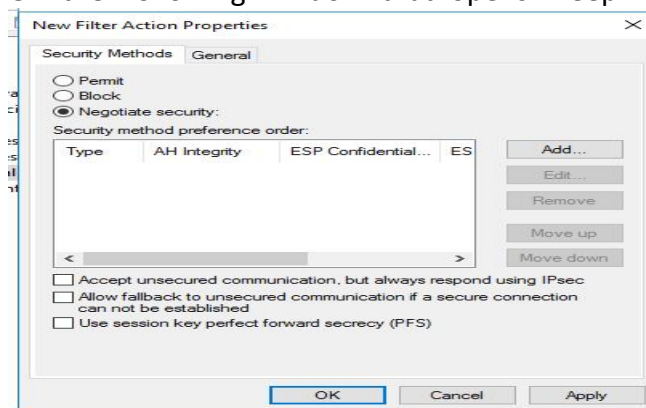
Next click the Filter Action tab on the above window.



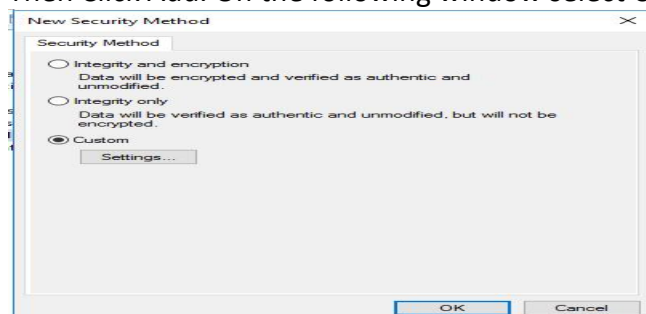
On the Filter Action tab, first remove the tick from the check box of **Use Add Wizard**.

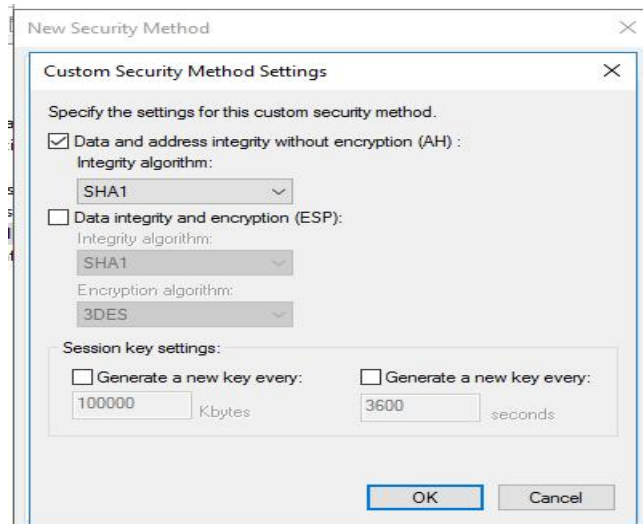
Then Click Add.

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



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





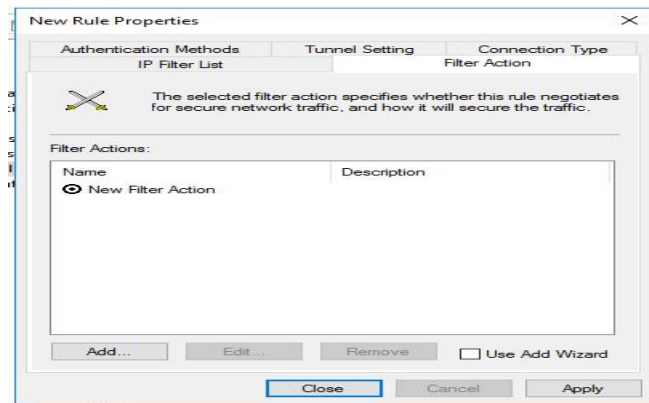
On this Screen Select Data and address integrity without encryption check box.

Select SHA1 from the drop down list.

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

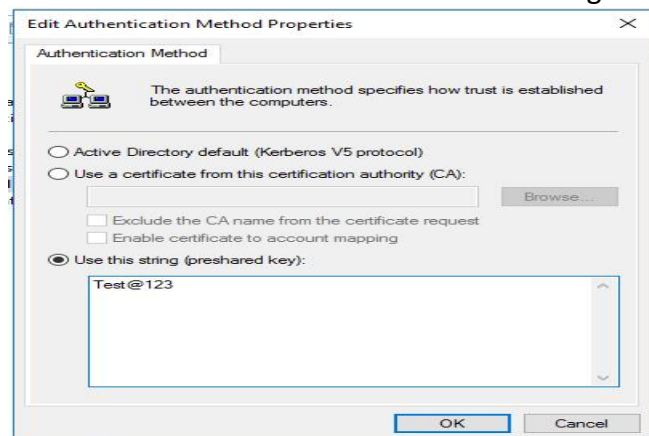
Click OK.

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.

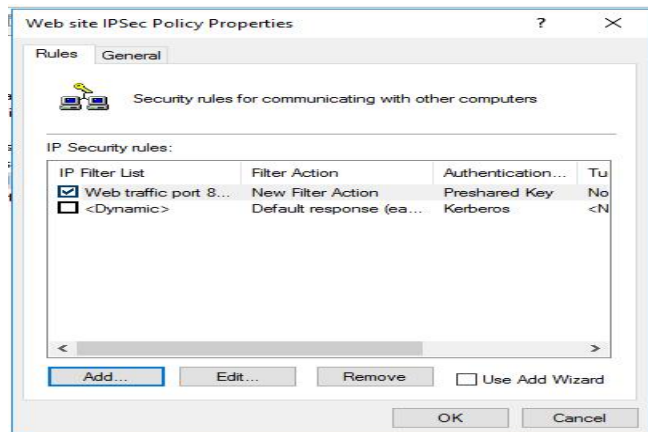


Click **Authentication Methods** tab in the above window. Click Edit button. Following window is displayed.

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.

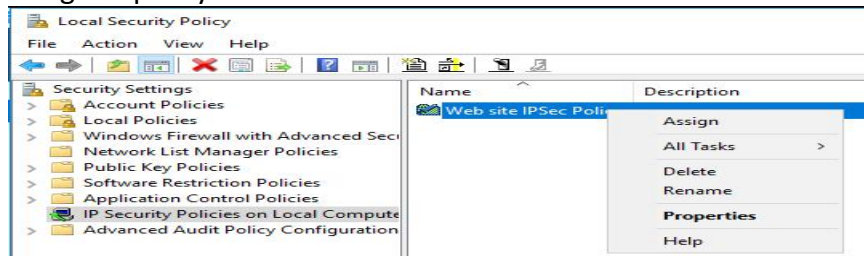


Click OK. Then Click Apply. Again Click OK on the window. Finally following window is displayed.



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.

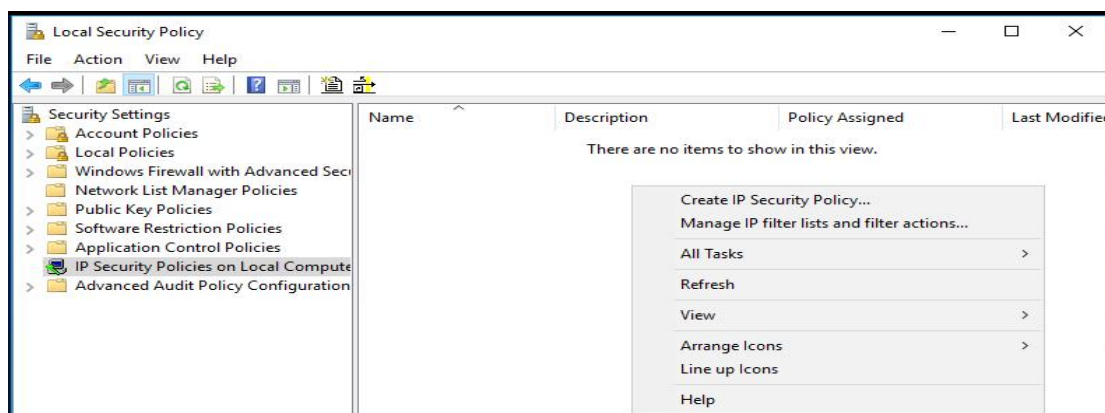


4. Configure IPsec policy on the client.

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 server is active and requires the client also to perform IPsec.

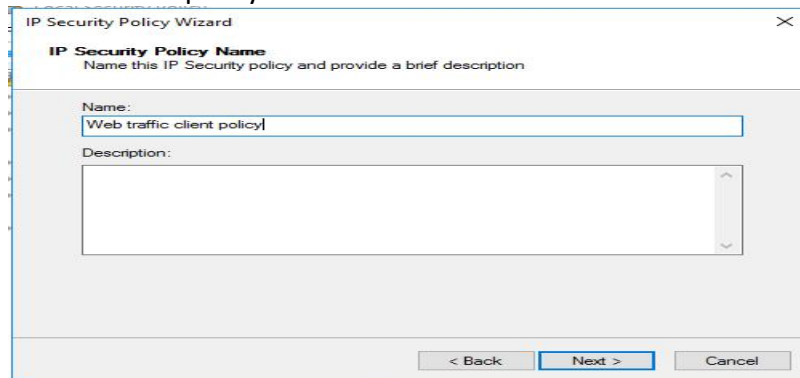
Now we will create the IPsec policy on the client.

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



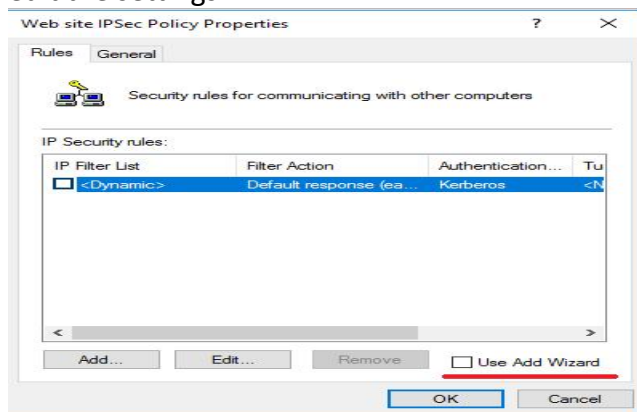
Select IP Security Policies on Local Computer. Right click and select Create IP Security Policy.

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



The screenshot shows the 'IP Security Policy Wizard' window, specifically the 'IP Security Policy Name' step. The title bar reads 'IP Security Policy Wizard'. Below the title, it says 'IP Security Policy Name' and 'Name this IP Security policy and provide a brief description'. There are two input fields: 'Name:' with the text 'Web traffic client policy' and 'Description:' which is empty. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

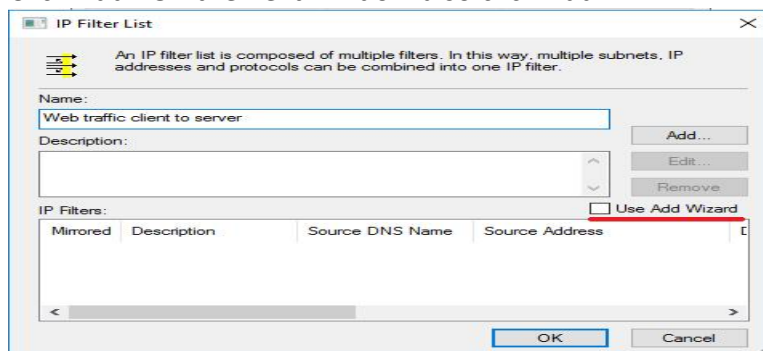
Click Next. Click Next on next window. Finally click Finish to create the policy and edit the settings.



The screenshot shows the 'Web site IPsec Policy Properties' window, 'Rules' tab. The title bar reads 'Web site IPsec Policy Properties'. Below the title, it says 'Security rules for communicating with other computers'. There is a table with columns: 'IP Filter List', 'Filter Action', 'Authentication...', and 'T...'. The first row has a checkbox, '<Dynamic>', 'Default response (ea...', and 'Kerberos'. Below the table are buttons: 'Add...', 'Edit...', 'Remove', and a checkbox 'Use Add Wizard' which is unchecked. At the bottom are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue border.

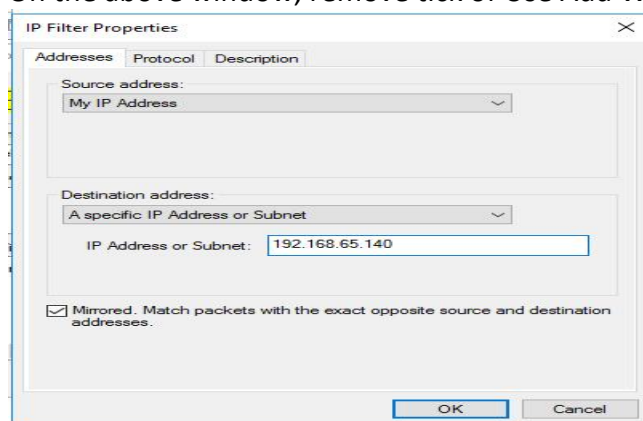
Remove Use Add Wizard tick.

Click Add. On the next window also click Add.



The screenshot shows the 'IP Filter List' window. The title bar reads 'IP Filter List'. Below the title, it says 'An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.' There are input fields for 'Name:' with the text 'Web traffic client to server' and 'Description:' which is empty. Below these are buttons: 'Add...', 'Edit...', and 'Remove'. There is also a checkbox 'Use Add Wizard' which is unchecked. At the bottom are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue border.

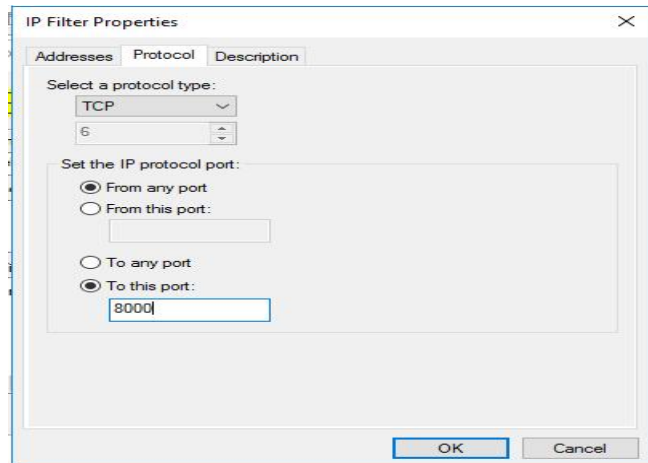
On the above window, remove tick of Use Add Wizard. Provide a name. Click Add.



The screenshot shows the 'IP Filter Properties' window, 'Addresses' tab. The title bar reads 'IP Filter Properties'. Below the title, there are tabs: 'Addresses', 'Protocol', and 'Description'. Under 'Addresses', there are two sections: 'Source address:' with a dropdown menu showing 'My IP Address' and 'Destination address:' with a dropdown menu showing 'A specific IP Address or Subnet'. Below the 'Destination address' dropdown is an input field for 'IP Address or Subnet:' with the text '192.168.65.140'. There is a checkbox 'Mirrored. Match packets with the exact opposite source and destination addresses.' which is checked. At the bottom are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue border.

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.

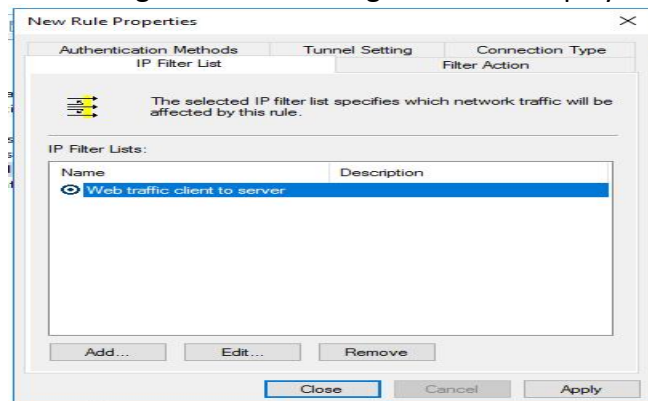


As we are identifying the traffic from client to Web server, select protocol as TCP.

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.

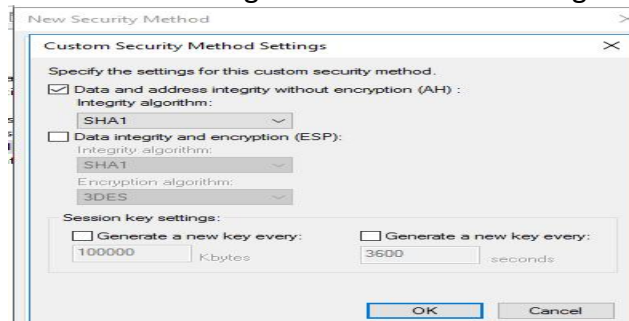
Then Click Add.

On the New window that opens select Negotiate Security. Click Add.

On the next Window select Custom and Click Settings tab.

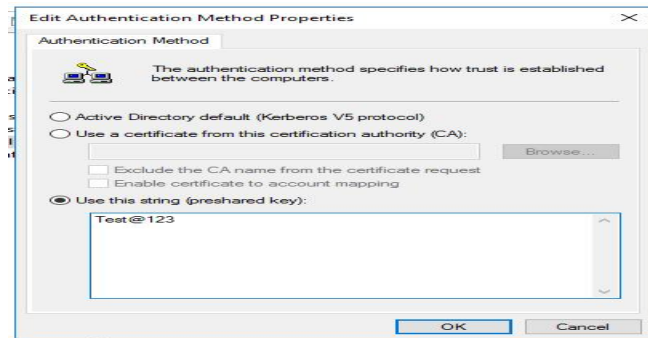
(These steps are same as the IPSec configuration on the web server. Thus you can refer to those screen shots or steps.)**

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. Type the 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 policy is created and applied.

Now both server and client could be able to create an IPSec tunnel.

5. Checking if IPSec is working.

Open 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.

No.	Time	Source	Destination	Protocol	Length	Info
8	16.626393	192.168.65.136	192.168.65.140	HTTP	323	GET / HTTP/1.1
10	16.727751	192.168.65.140	192.168.65.136	HTTP	346	HTTP/1.1 200 OK (text/html)
16	16.889565	192.168.65.136	192.168.65.140	HTTP	285	GET /favicon.ico HTTP/1.1
17	16.894761	192.168.65.140	192.168.65.136	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
77	19.199502	192.168.65.136	23.221.53.191	HTTP	478	GET /fwlink/?LinkId=403856&language=en-US&scale=100&contrast=gra...
79	19.555540	23.221.53.191	192.168.65.136	HTTP	467	HTTP/1.1 302 Moved Temporarily
330	53.629132	192.168.65.136	192.168.65.140	HTTP	352	GET / HTTP/1.1
332	53.710681	192.168.65.140	192.168.65.136	HTTP	364	HTTP/1.1 200 OK (text/html)
337	53.767541	192.168.65.136	192.168.65.140	HTTP	314	GET /favicon.ico HTTP/1.1
338	53.769620	192.168.65.140	192.168.65.136	HTTP	1461	HTTP/1.1 404 Not Found (text/html)
340	53.770536	23.221.53.191	192.168.65.136	HTTP	468	HTTP/1.0 408 Request Time-out (text/html)

Frame 10: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bit				0040	30 30 20 4f 4b 0d 0a 43	6f 6e 74 65 6e 74 2d 54	00 00	C ont
Ethernet II, Src: VMware_35:10:35 (00:0c:29:35:10:35), Dst: VMware_93				0050	79 70 65 3a 20 74 65 78	74 2f 68 74 6d 6c 0d 0a	00 00	ype: tex t/h
Internet Protocol Version 4, Src: 192.168.65.140, Dst: 192.168.65.136				0060	4c 61 73 74 2d 4d 6f 64	69 66 69 65 64 3a 20 53	00 00	Last-Mod ifi
Transmission Control Protocol, Src Port: 80, Dst Port: 62813, Seq: 1,				0070	61 74 2c 20 31 39 20 4e	6f 76 20 32 30 32 32 20	00 00	at, 19 N ov
Hypertext Transfer Protocol				0080	31 32 3a 34 32 3a 30 35	20 47 4d 54 0d 0a 41 63	00 00	12:42:05 GM
Line-based text data: text/html (1 lines)				0090	63 65 70 74 2d 52 61 6e	67 65 73 3a 20 62 79 74	00 00	cept-Ran ges
This web site is running on port 80. It is not encrypted using IPSec.				00a0	65 73 0d 0a 45 54 61 67	3a 20 22 37 34 64 37 66	00 00	es: ETag: "
				00b0	35 34 31 34 66 63 64 38	31 3a 30 22 0d 0a 53 65	00 00	5414fcd8 110
				00c0	72 76 65 72 3a 20 4d 69	63 72 6f 73 6f 66 74 2d	00 00	rver: Mi cro
				00d0	49 49 53 2f 31 30 2e 30	0d 0a 44 61 74 65 3a 20	00 00	IIS/10.0
				00e0	53 75 6e 2c 20 32 30 20	4e 6f 76 20 32 30 32 32	00 00	Sun. 20 Nov

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

No.	Time	Source	Destination	Protocol	Length	Info
8	16.626393	192.168.65.136	192.168.65.140	HTTP	323	GET / HTTP/1.1
10	16.727751	192.168.65.140	192.168.65.136	HTTP	346	HTTP/1.1 200 OK (text/html)
16	16.889565	192.168.65.136	192.168.65.140	HTTP	285	GET /favicon.ico HTTP/1.1
17	16.894761	192.168.65.140	192.168.65.136	HTTP	1437	HTTP/1.1 404 Not Found (text/html)
77	19.199502	192.168.65.136	23.221.53.191	HTTP	478	GET /fwlink/?LinkId=403856&language=en-US&scale=100&contrast=gra...
79	19.555540	23.221.53.191	192.168.65.136	HTTP	467	HTTP/1.1 302 Moved Temporarily
330	53.629132	192.168.65.136	192.168.65.140	HTTP	352	GET / HTTP/1.1
332	53.710681	192.168.65.140	192.168.65.136	HTTP	364	HTTP/1.1 200 OK (text/html)
337	53.767541	192.168.65.136	192.168.65.140	HTTP	314	GET /favicon.ico HTTP/1.1
338	53.769620	192.168.65.140	192.168.65.136	HTTP	1461	HTTP/1.1 404 Not Found (text/html)
340	53.770536	23.221.53.191	192.168.65.136	HTTP	468	HTTP/1.0 408 Request Time-out (text/html)

Frame 332: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bi				0000	00 0c 29 93 79 1c 00 0c	29 35 10 35 08 00 45 02	00 00	y...)S ^
Ethernet II, Src: VMware_35:10:35 (00:0c:29:35:10:35), Dst: VMware_93				0010	81 5e 55 c8 40 00 00 33	9f 3f c0 a0 42 8c c0 a0	00 00	^U @ 3 2
Internet Protocol Version 4, Src: 192.168.65.140, Dst: 192.168.65.136				0020	41 88 06 04 00 00 63 8c	b3 b0 00 00 00 03 e8 5f	00 00	A... C... ..
Authentication Header				0030	63 fe 44 3d a5 b6 58 82	77 36 1f 40 f5 6c 5b 99	00 00	C De: X: w0
Next header: TCP (6)				0040	43 5c b9 7b 9a 42 58 18	08 18 05 43 00 00 45 54	00 00	C\ { BP ...
Length: 4 (24 bytes)				0050	54 50 2f 31 2e 31 20 32	30 30 20 4f 4b 0d 0a 43	00 00	TP/1.1 2 00
Reserved: 0000				0060	6f 6e 74 65 6e 74 2d 54	79 70 65 3a 20 74 65 78	00 00	content-T ype
AH SPI: 0x638cb30e				0070	74 2f 68 74 6d 6c 0d 0a	4c 61 73 74 2d 4d 6f 64	00 00	t/html: Las
AH Sequence: 3				0080	69 66 69 65 64 3a 20 53	61 74 2c 20 31 39 20 4e	00 00	ified: S at,
AH ICV: e85f63fe443da5b658827736				0090	6f 76 20 32 30 32 32 20	31 32 3a 34 36 3a 35 36	00 00	ov 2022 12:
Transmission Control Protocol, Src Port: 8000, Dst Port: 62828, Seq:				00a0	20 47 4d 54 0d 0a 41 63	63 65 70 74 2d 52 61 6e	00 00	GMT: Ac cpe
Hypertext Transfer Protocol				00b0	3a 20 22 36 34 39 31 34	32 32 31 35 66 63 64 38	00 00	ges: byt es
Line-based text data: text/html (1 lines)				00c0	72 76 65 72 3a 20 4d 69	63 72 6f 73 6f 66 74 2d	00 00	10" Se rve
This site is running on port 8000. It is encrypted using IPSec.				00d0	63 72 6f 73 6f 66 74 2d	49 49 53 2f 31 30 2e 30	00 00	crosoft- IIS
				00e0	0d 0a 44 61 74 65 3a 20	53 75 6e 2c 20 32 30 20	00 00	-Date: Sun
				00f0	4e 6f 76 20 32 30 32 32	20 30 38 3a 33 39 3a 34	00 00	Nov 2022 00
				0100	36 20 47 4d 54 0d 0a 43	6f 6e 74 65 6e 74 2d 4c	00 00	6 GMT: C ont
				0110	65 6e 67 74 68 3a 20 30	33 0d 0a 0d 0a 54 00 69	00 00	length: 6 3

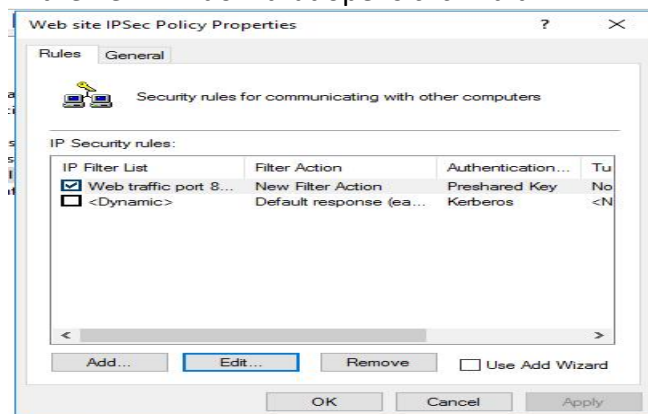
You are able to see the contents of the web page. Thus AH protocol of IPsec is not encrypting the data. It is just calculating hash and attaching it. Thus it provides authentication and integrity.

6. Changing from AH to ESP in IPsec.

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

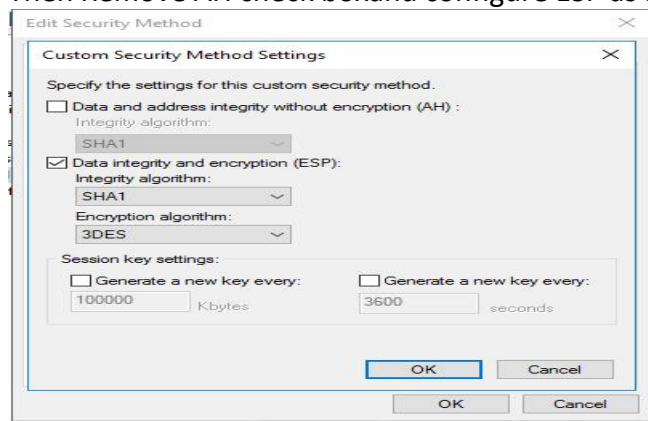
On the Web Server go to secpol.msc. Select IP Security policy. Double click the policy name that we created earlier.

In the new window that opens click Edit.



Then click the **Filter Action** tab. Click Edit. Again Click Edit. Then Below Customs option click Settings tab.

Then Remove AH check box and configure ESP as below.



Click OK. Click OK if any message is displayed. Click Apply and then Click OK.

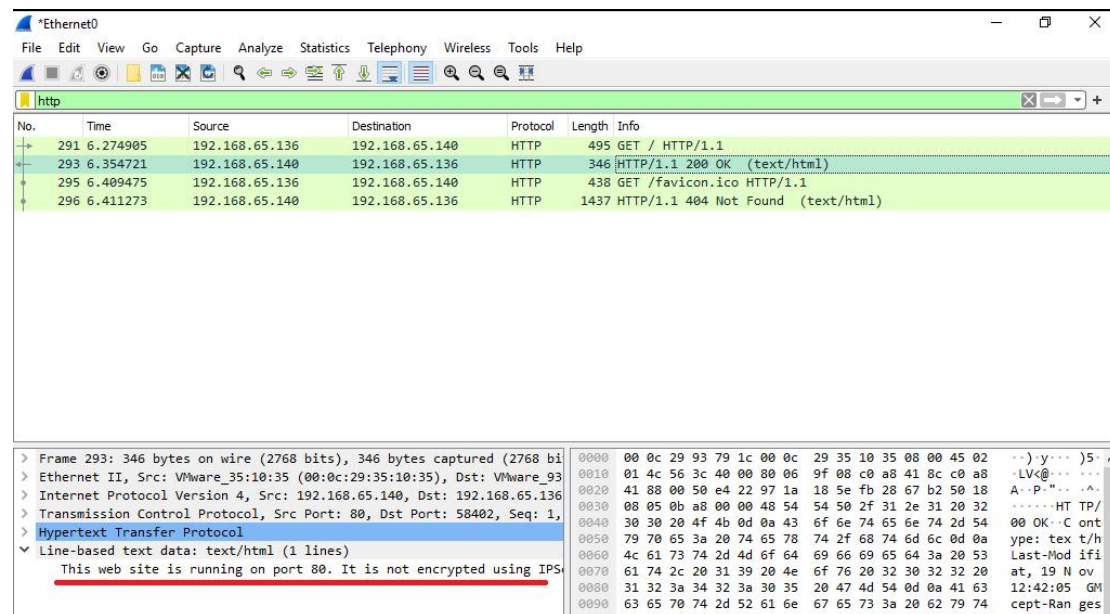
Then click close. On the final window click Apply and close.

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

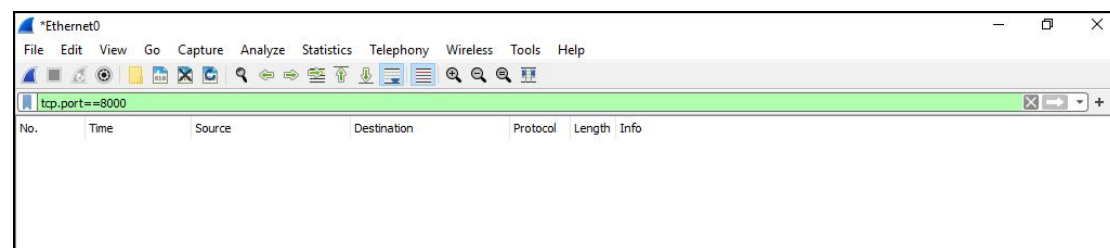
7. Test ESP Configuration.

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.



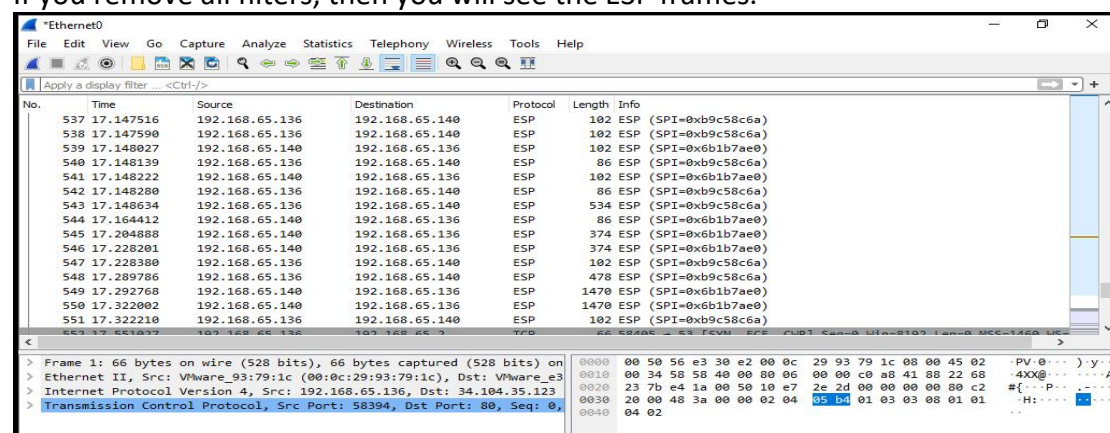
But you can see that now there are no http frames for port 8000 web site traffic. Try applying a filter for TCP port 8000. (tcp.port==8000)



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 sure you delete IPSec policy from both the servers.