



Technical Documentation about RPC over HTTP implementation for Exchange 2003 Rev.1.1



Prepared BY:
Mahmoud magdy
Reda sherif

Date:3-10-2005

Technical over view:

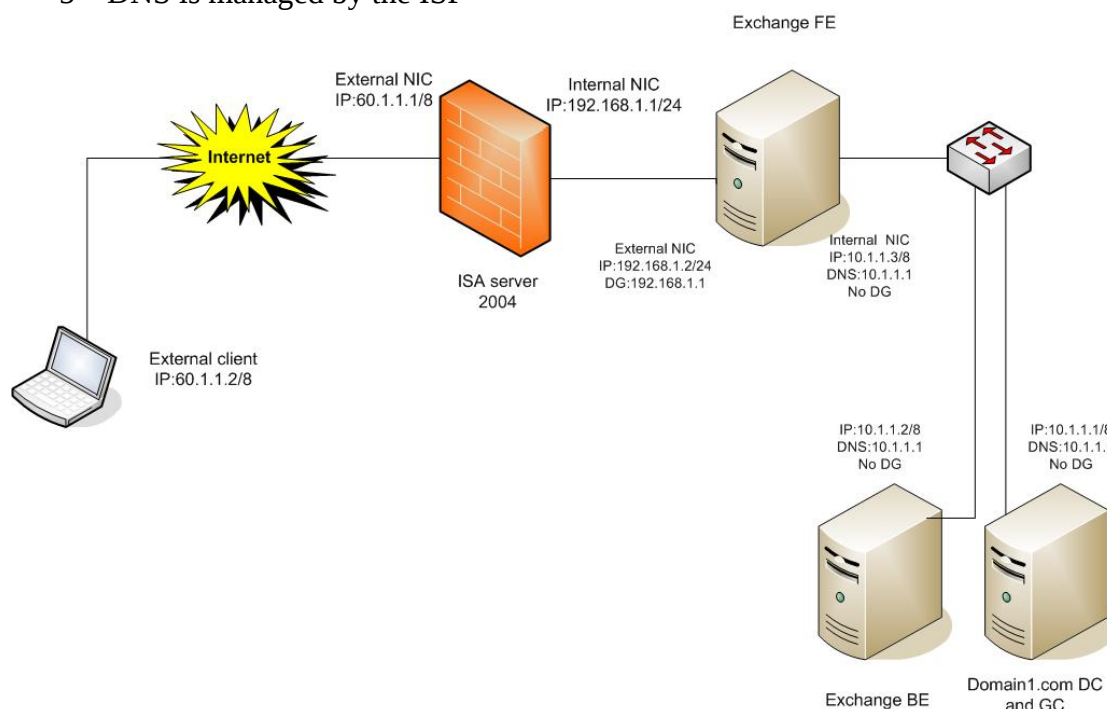
[RPC over HTTP general over view](#)

[PRC over HTTP for Exchange over view Technet webcast](#)

Implementation Plan:

In the following figure we have assumed the following plan:

- 1- a company that have registered a domain with the name domain1.com and have also a local domain with the name domain1.com
- 2- a separate server for each server role: server for DC and GC, server for Exchange BE, server for exchange FE
- 3- An isa server in front of the FE and split DNS is running around
- 4- Isa implement Hosts file instead of DNS you can implement it if you want to host your DNS
- 5- DNS is managed by the ISP

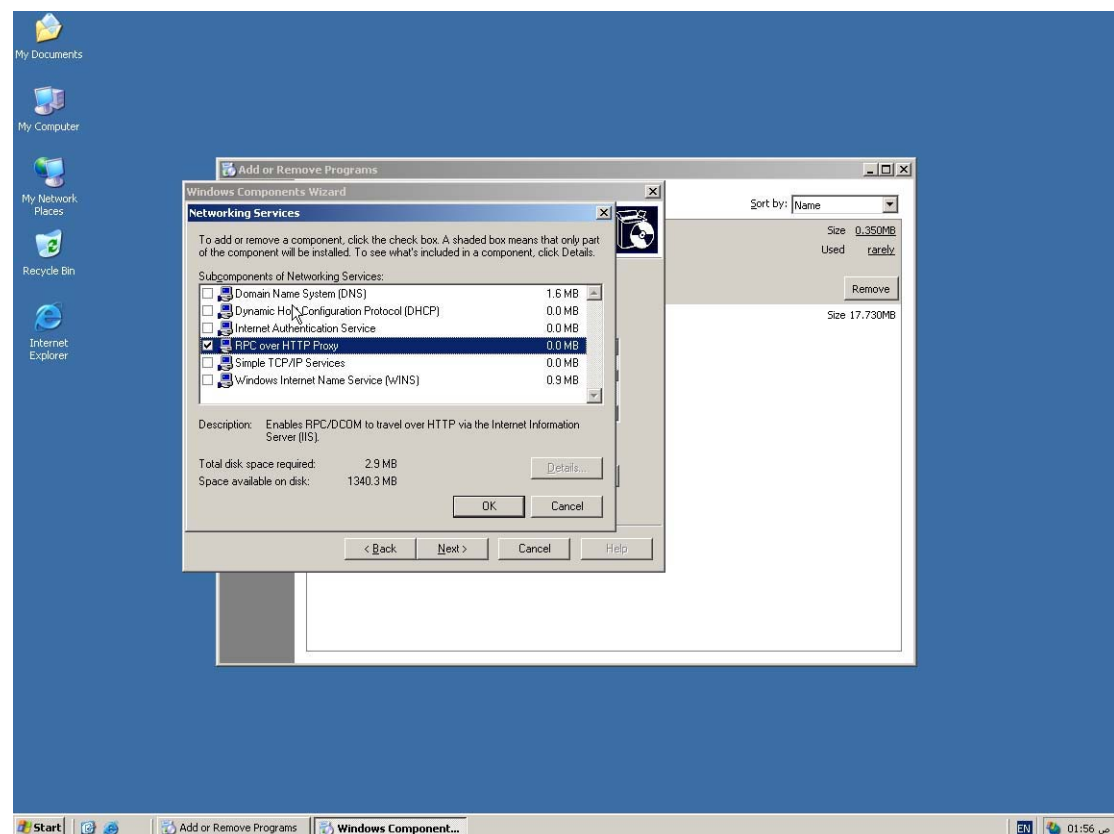
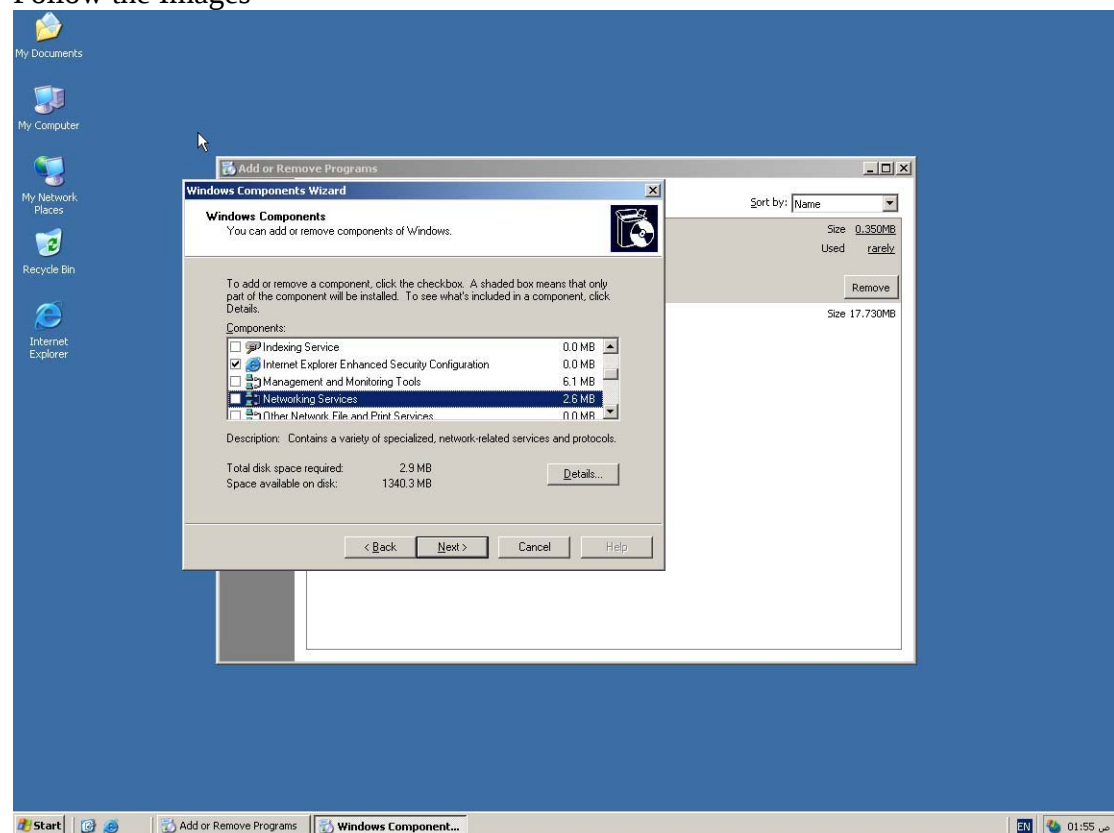


We have assumed that the installation of the domain and exchange with is done, also installation of the certificate authority service is done on the DC as enterprise root CA and that every thing is set in place

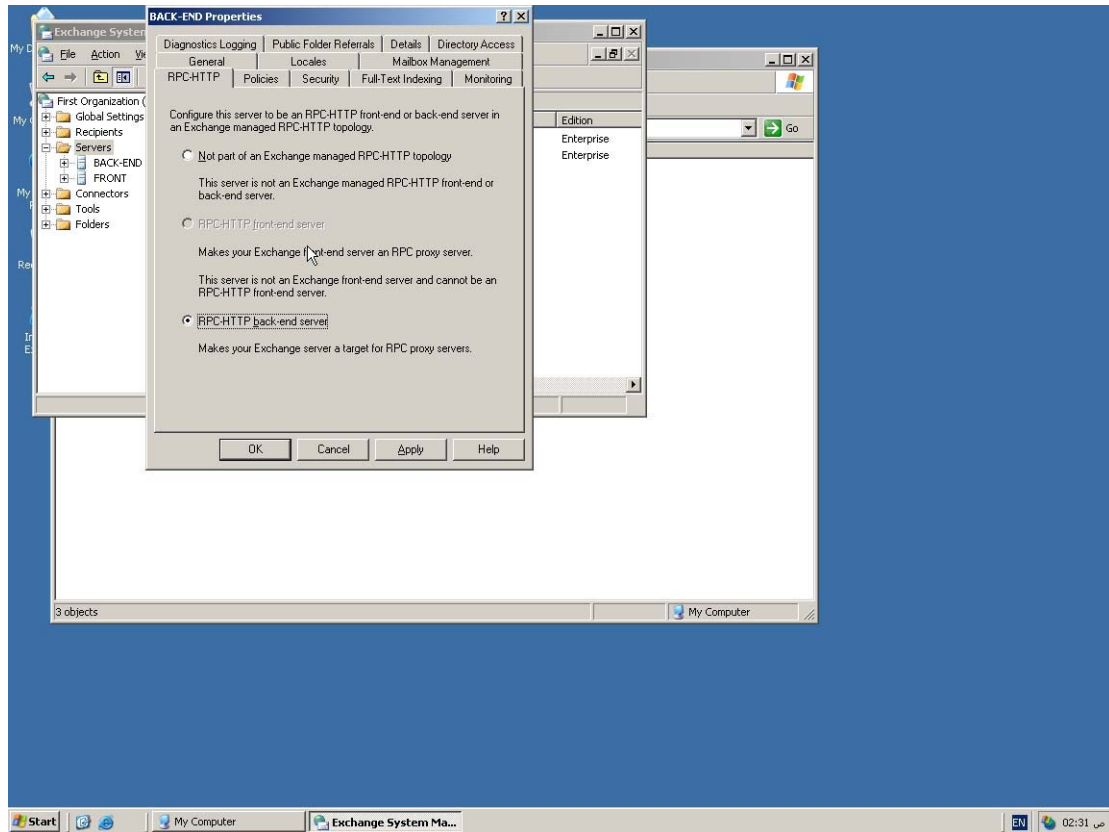
Stage 1: configure RPC over HTTP on the FE and BE:

You will need to install the RPC over HTTP component from windows networking component

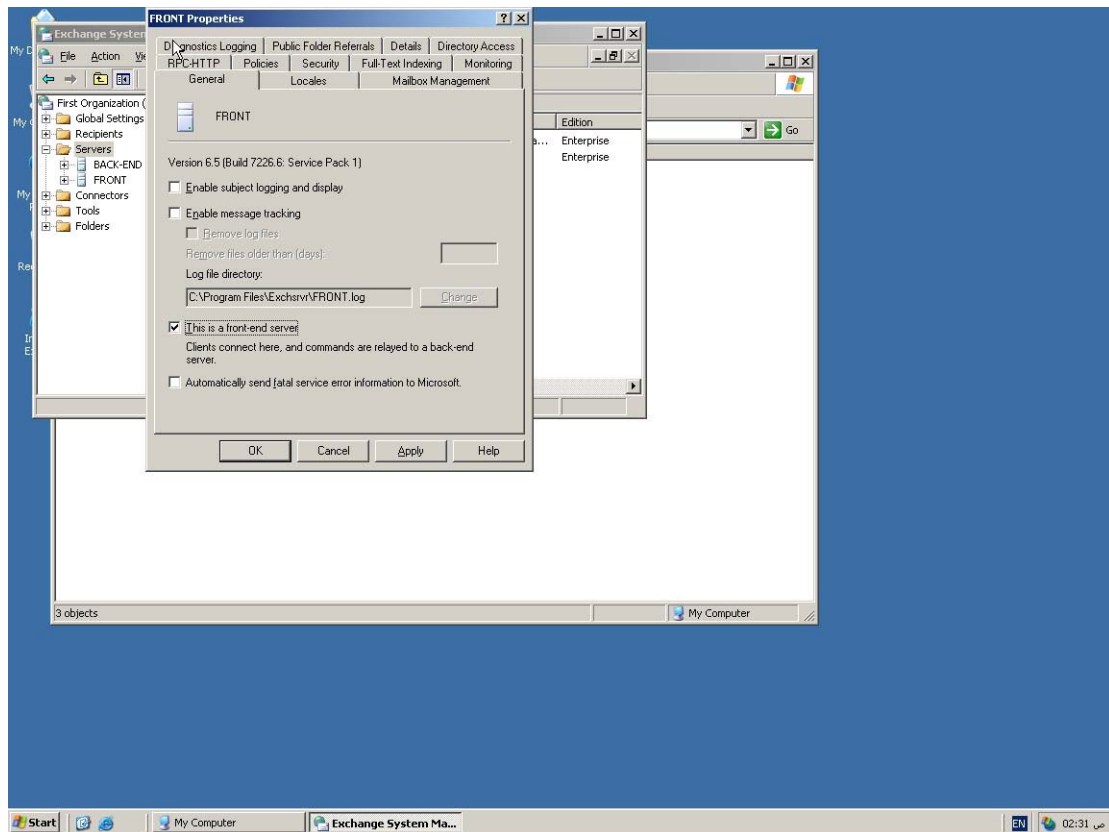
Go to the control panel
Add remove program
Add windows component
Follow the Images



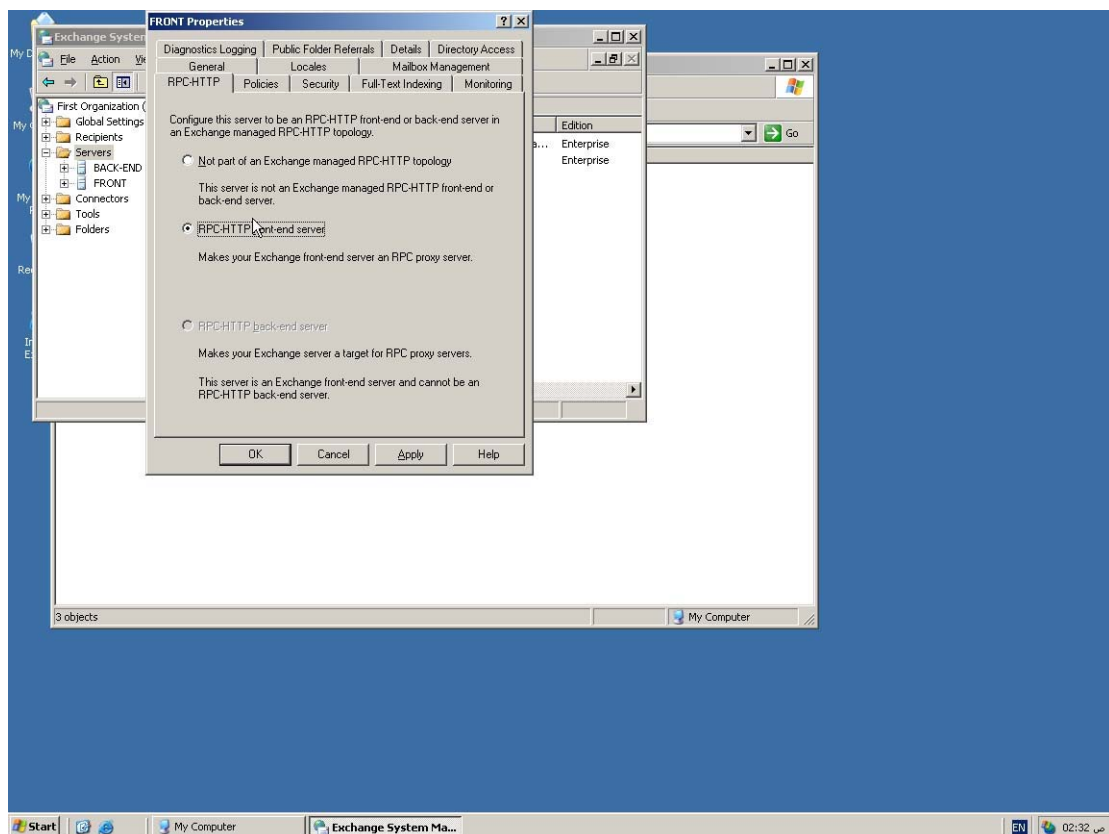
Then you will need to configure the BE and FE role for rpc
Open system manager
Click on the BE properties
Click the RPC-HTTP tab
Choose it as a BE rpc as in the Image



Then configure the FE role
Click on it in the system manager
Choose properties
Configure it as a FE



Then RPC-HTTP tab
Configure it as in the Image



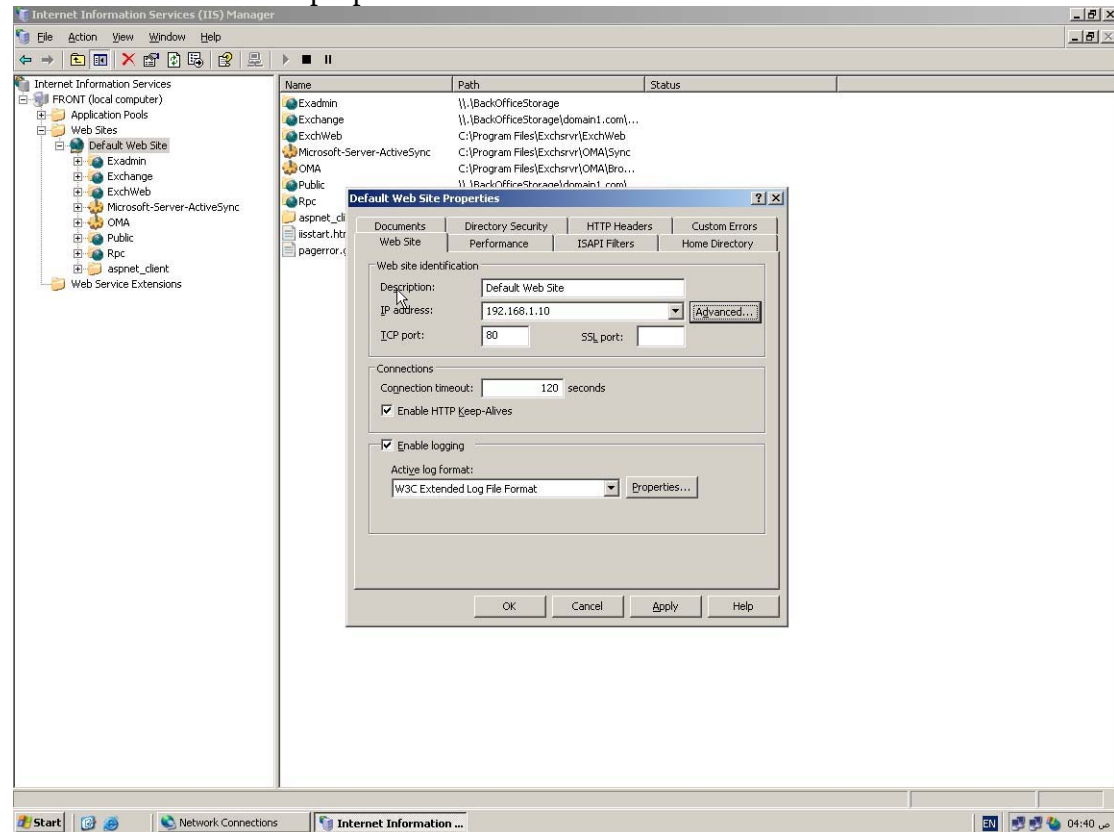
Stage 2: configure the IIS on the FE and:

All the IIS work will be on the front end server no work is needed on the BE ,We will configure the http header on the front end to be mail.domain1.com because this is the name that the users will type in the IE to login(they will type from external network mail.domain1.com/exchange)

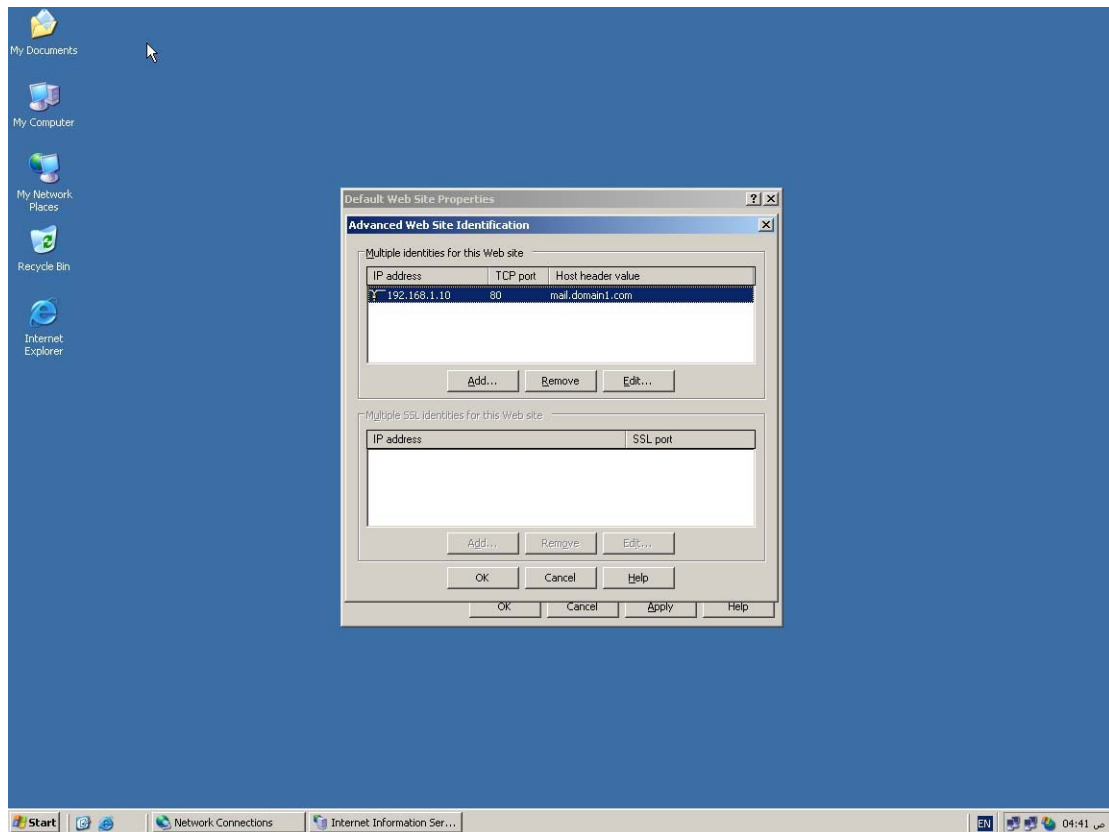
Open the IIS mmc

Expand web sites

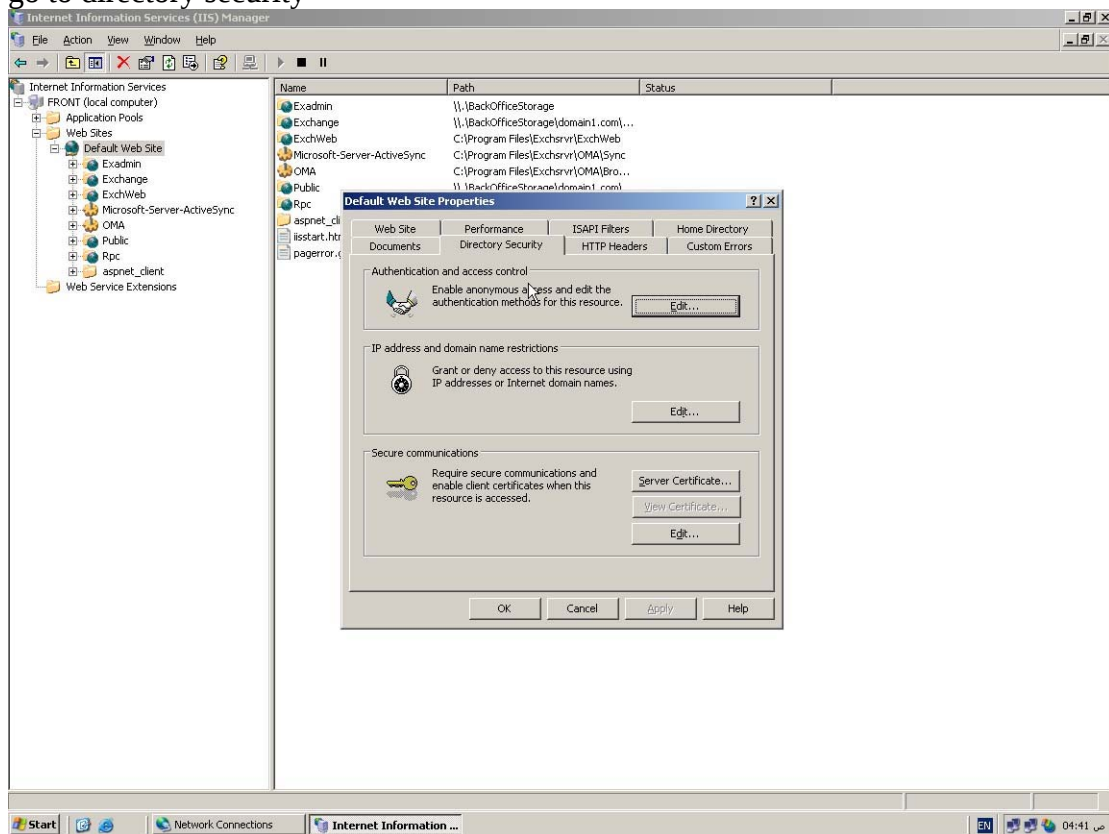
Go the default website properties



Click advanced click edit and add the host header

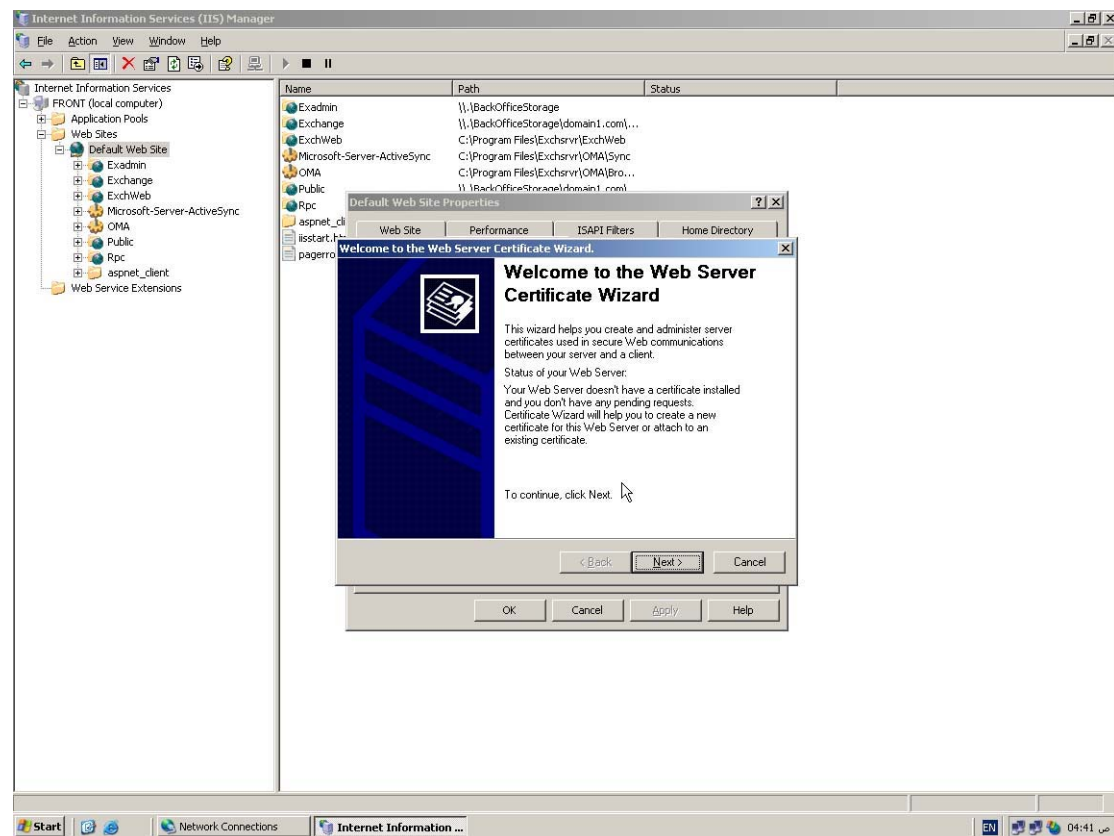


Now we will request the certificate that the FE will use for HTTPS
go to directory security

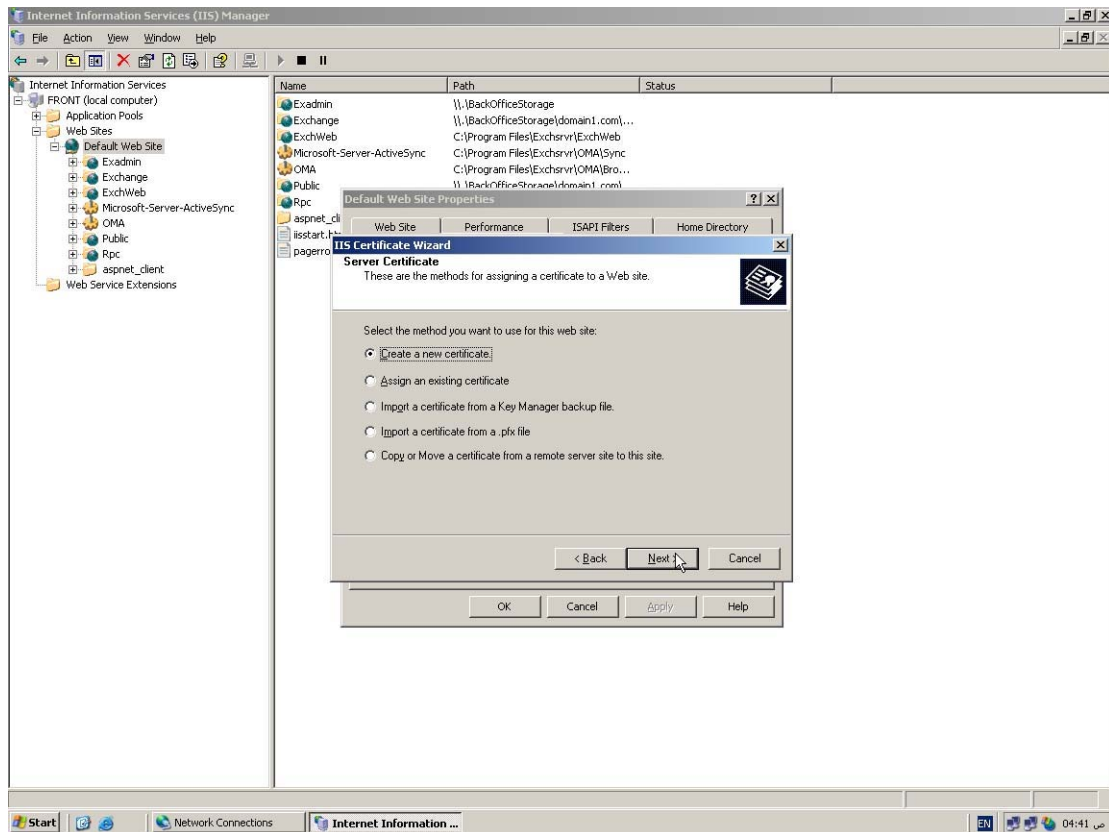


Click on server certificate

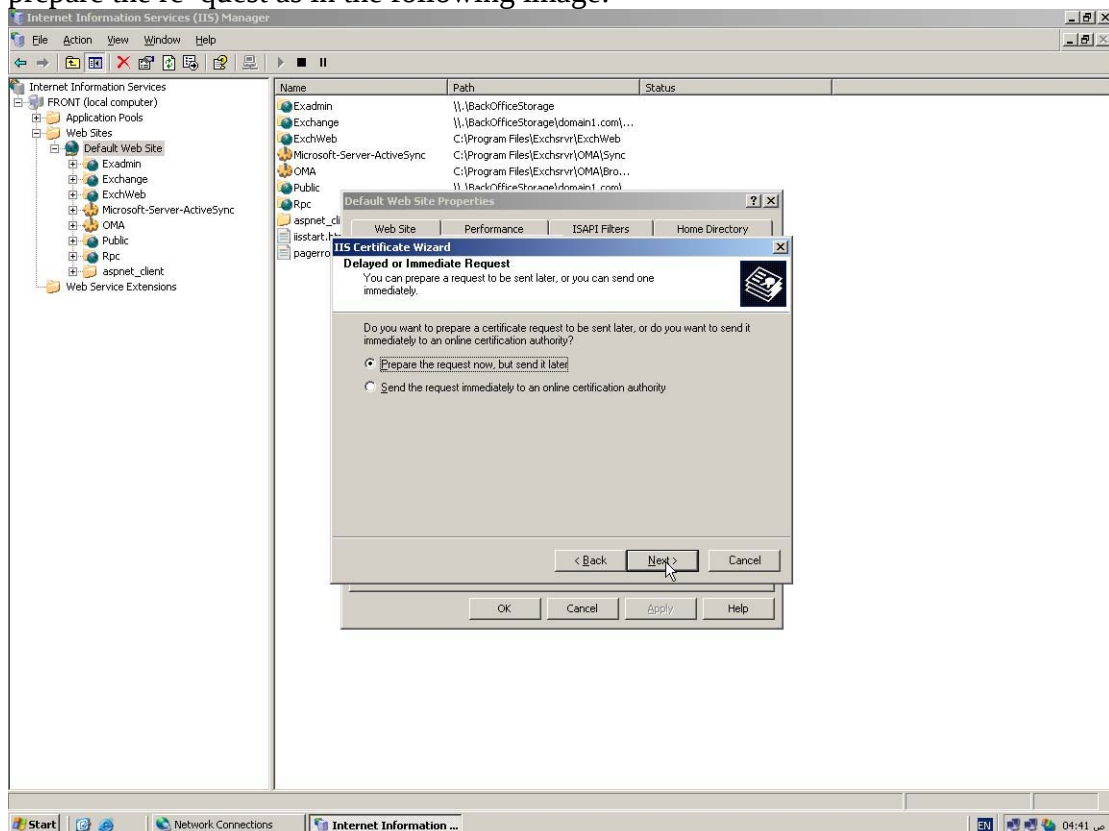
You will be prompted with this welcome screen, click next



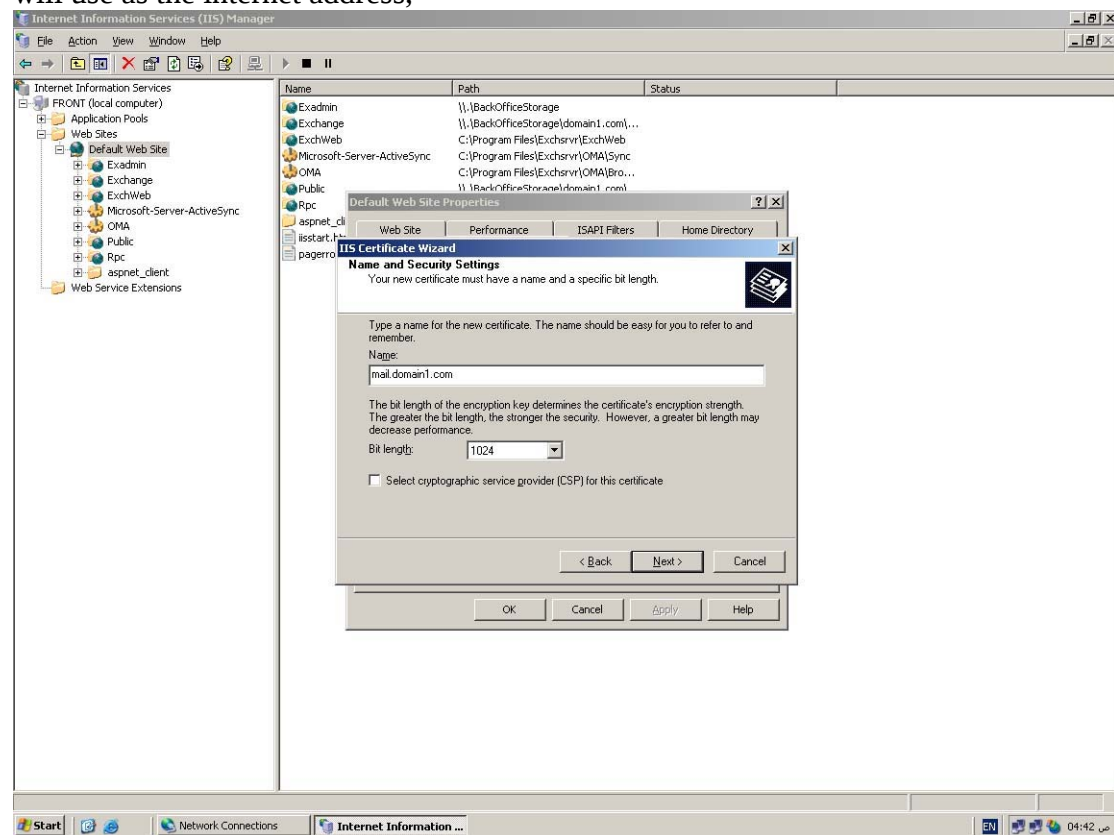
You will have the following screen with the multi choose option you will choose create new certificate
Then next



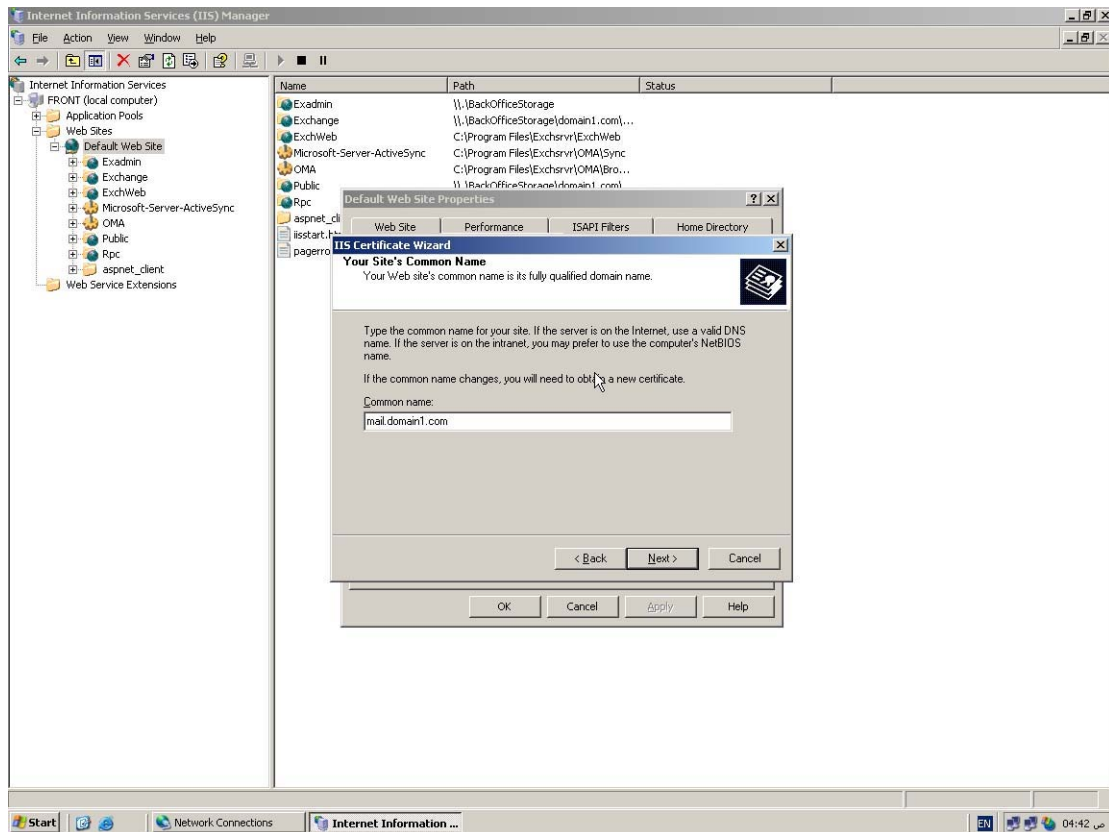
You will use your own certificate which you have installed on the DC, so choose prepare the request as in the following image:



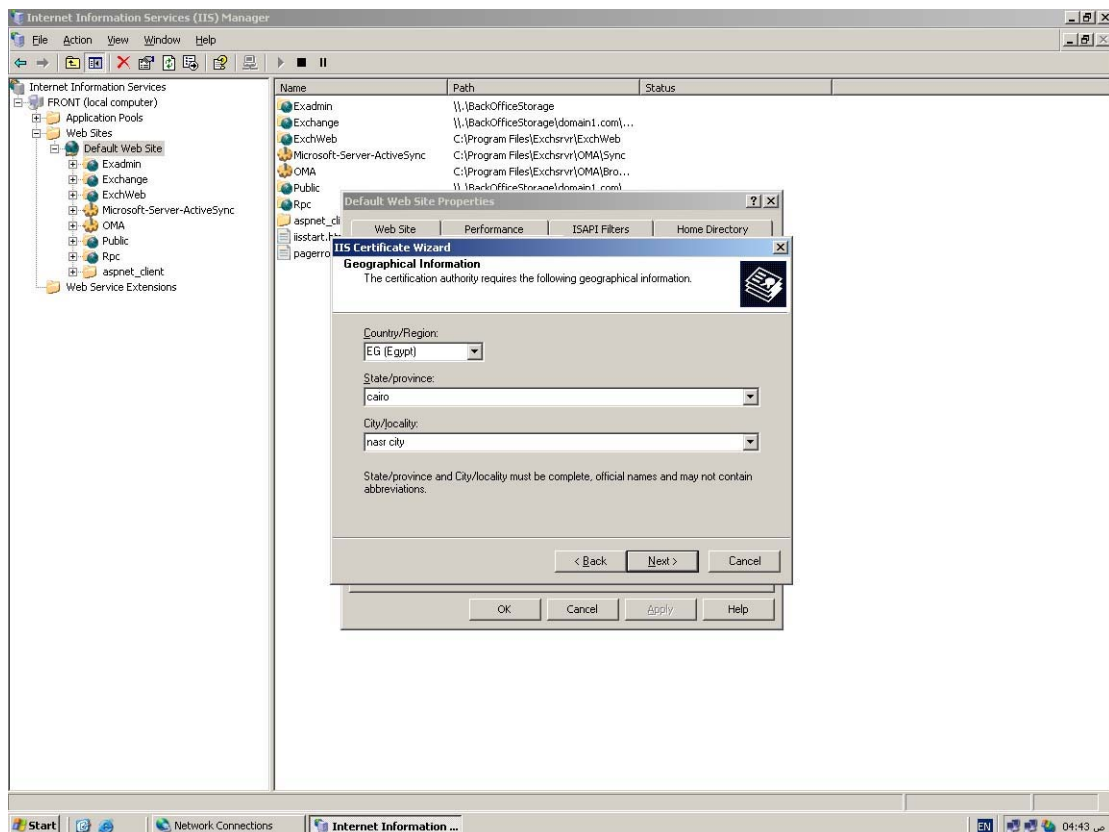
In the name type a name that you will recognize the certificate with it in the certificate store, MS documentation indicate that this name is not important and you can name it as you wish but I have tested it should be the exact name as the name that the user will use as the internet address,



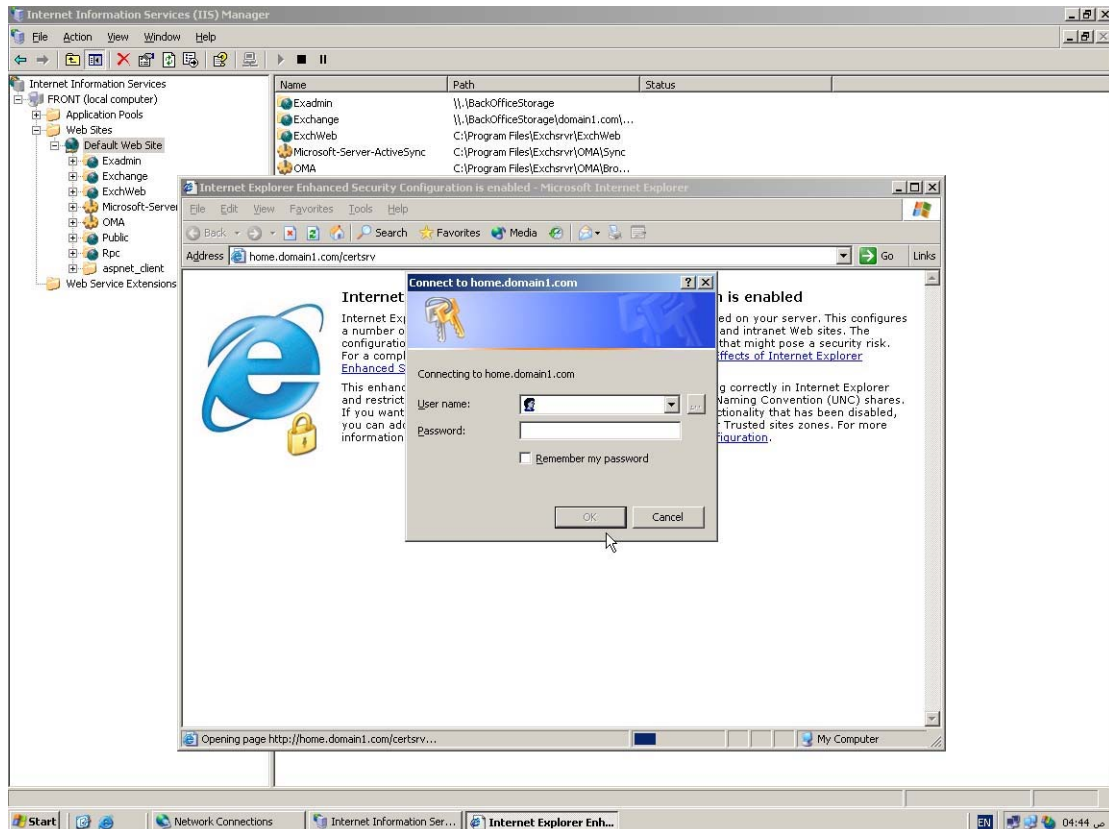
In the organization and OU type any thing that you want



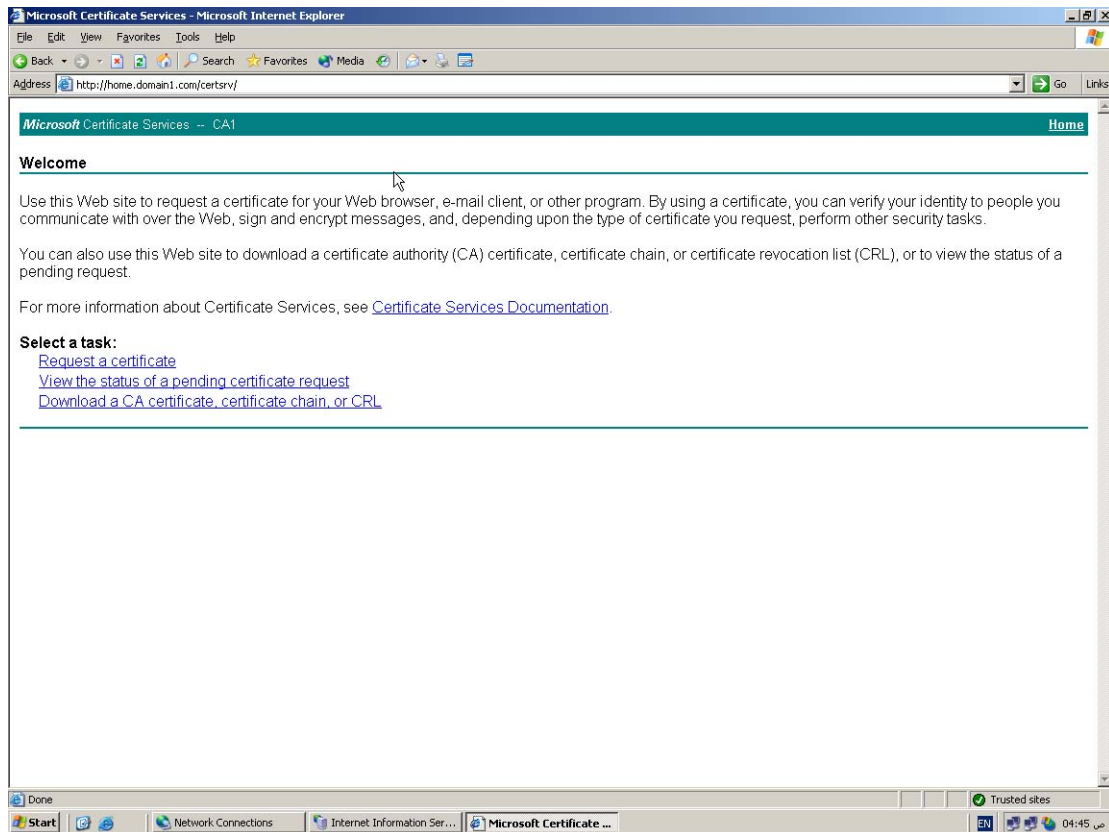
In the common name be sure for hundreds times that this is the exact name that users will type in the browser for the web site, the users will type mail.domain1.com so type mail.domain1.com



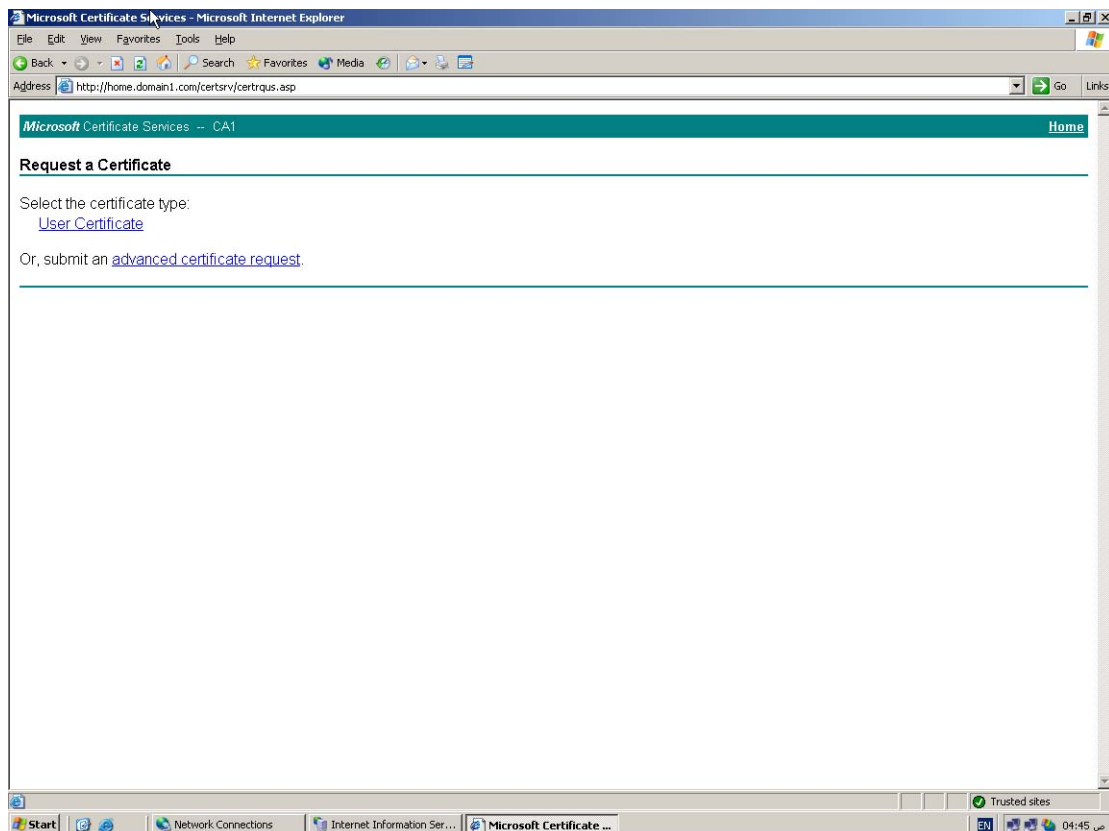
In the country and city choose the country and city
Now you will be prompted to save the request file save it on the hard disk
Now you are ready to submit it to the local CA:
Open the internet explorer, choose tools → option → security then reset the security setting for trusted sites to low or medium low
Add the <http://dc.domain1.com> to the trusted sites
Now in the address bar type: `http://dc.domain1.com/certsrv`
You will be prompted with the username and password type the user name and password for administrator or a user with the rights to submit and request a certificate



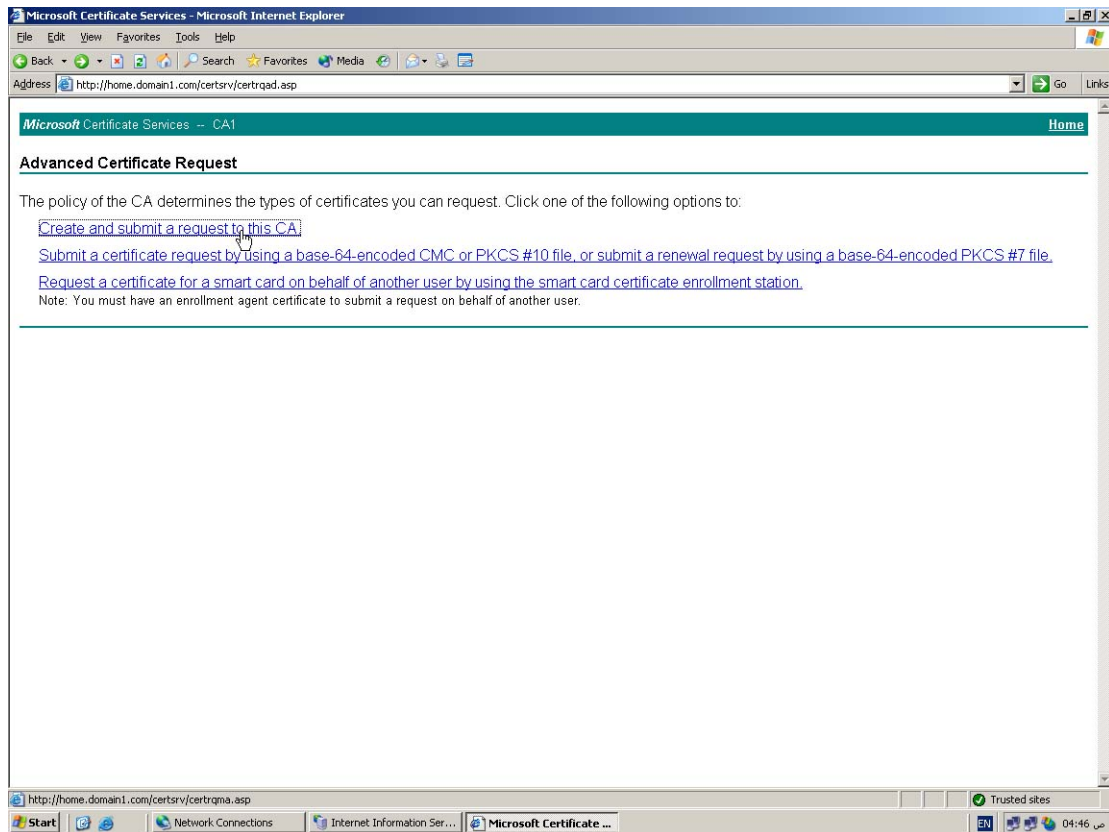
When you logged in choose request a certificate



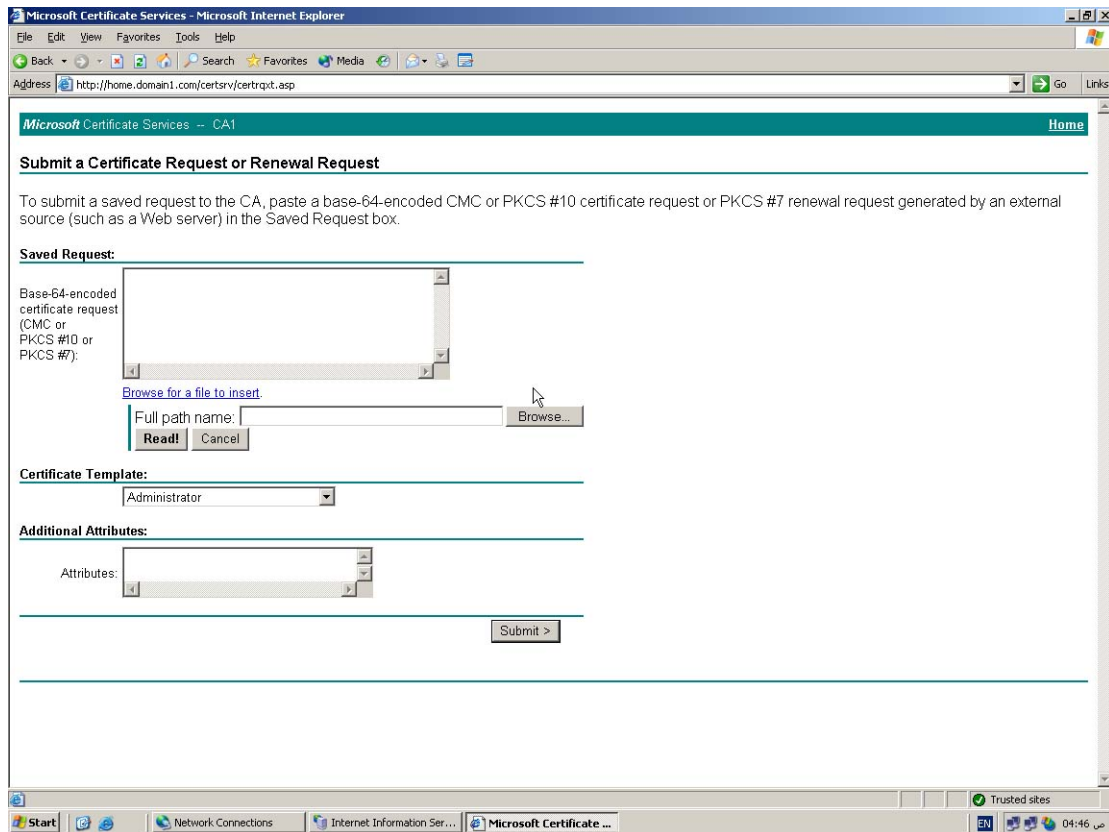
Choose advanced certificates



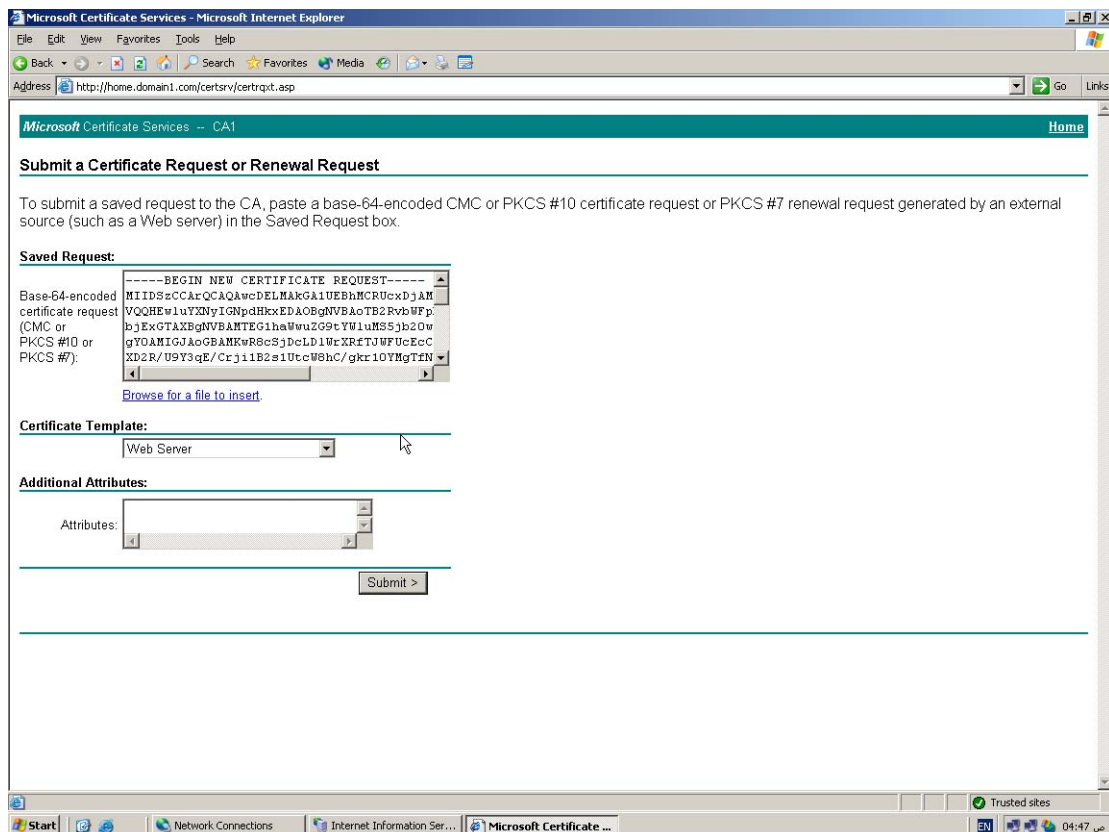
Choose submit a certificate request by using base 64-encoded



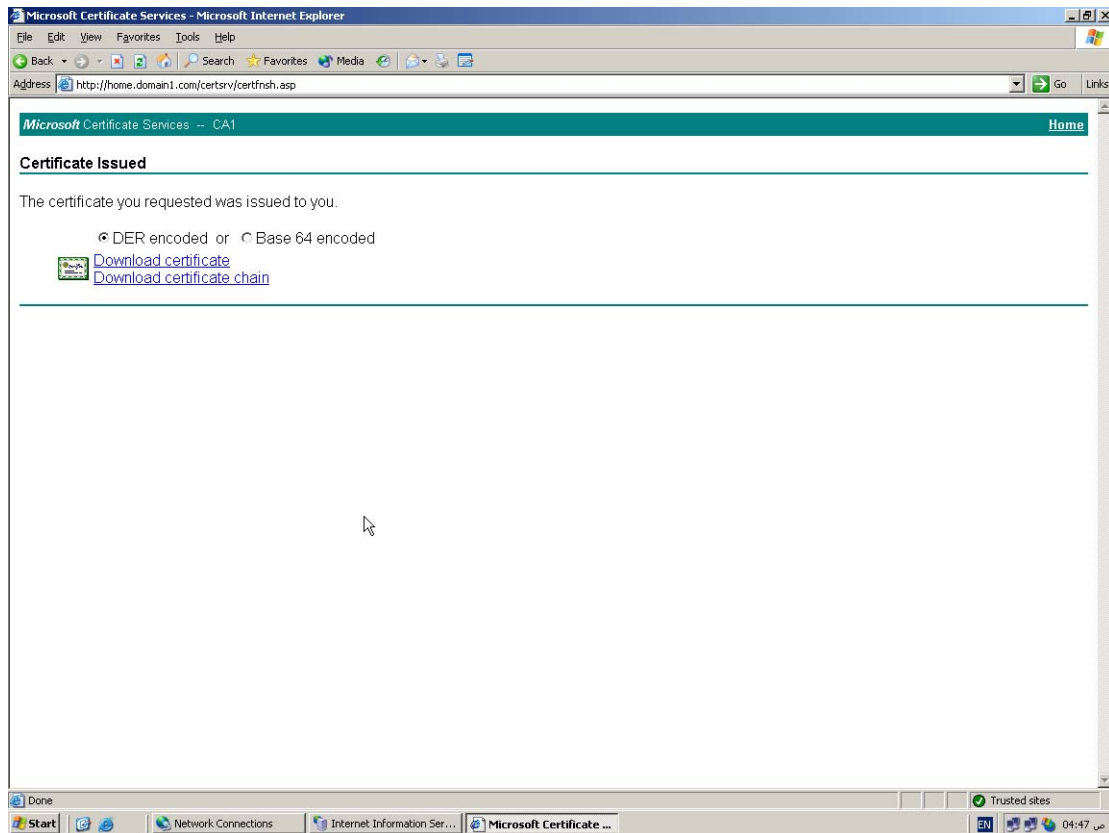
In the page click on browse for a file you will be warned for active x warning click yes
And then open the file that contains the certificate request that you have saved before



Click on read
Change the certificate template to web server
Then submit



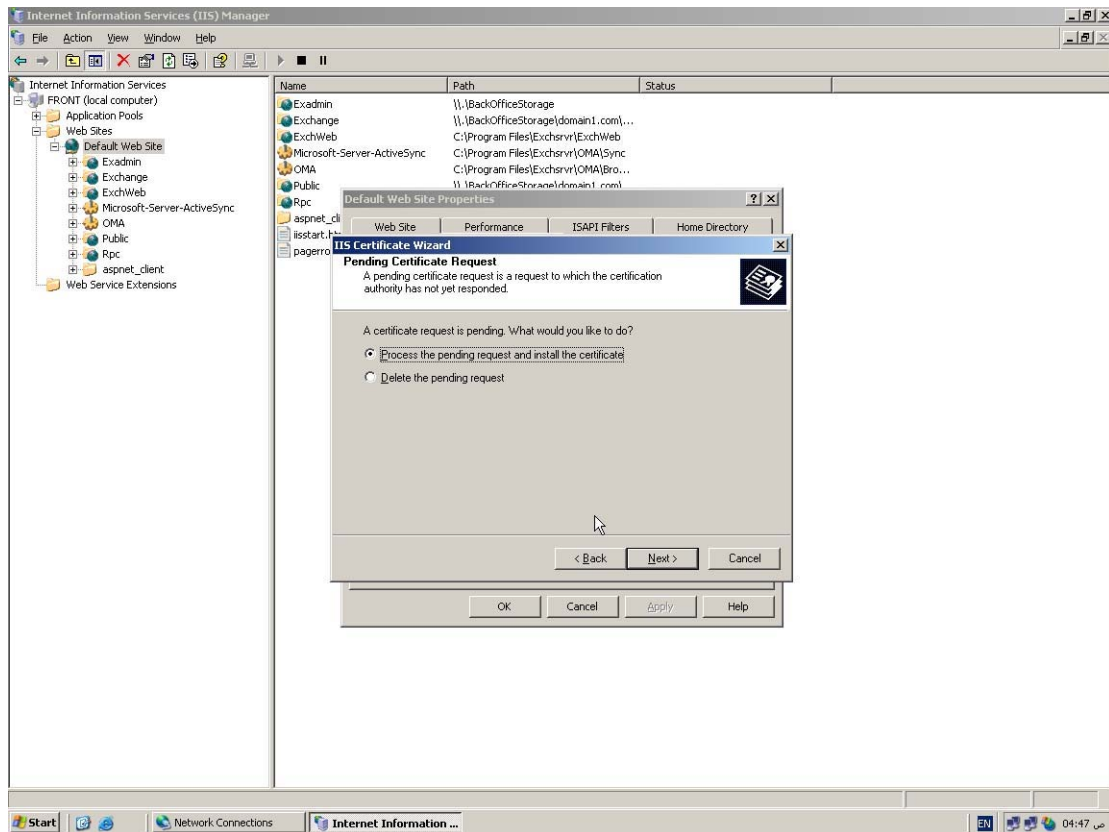
In the next page after the certificate has been issued choose to download it:



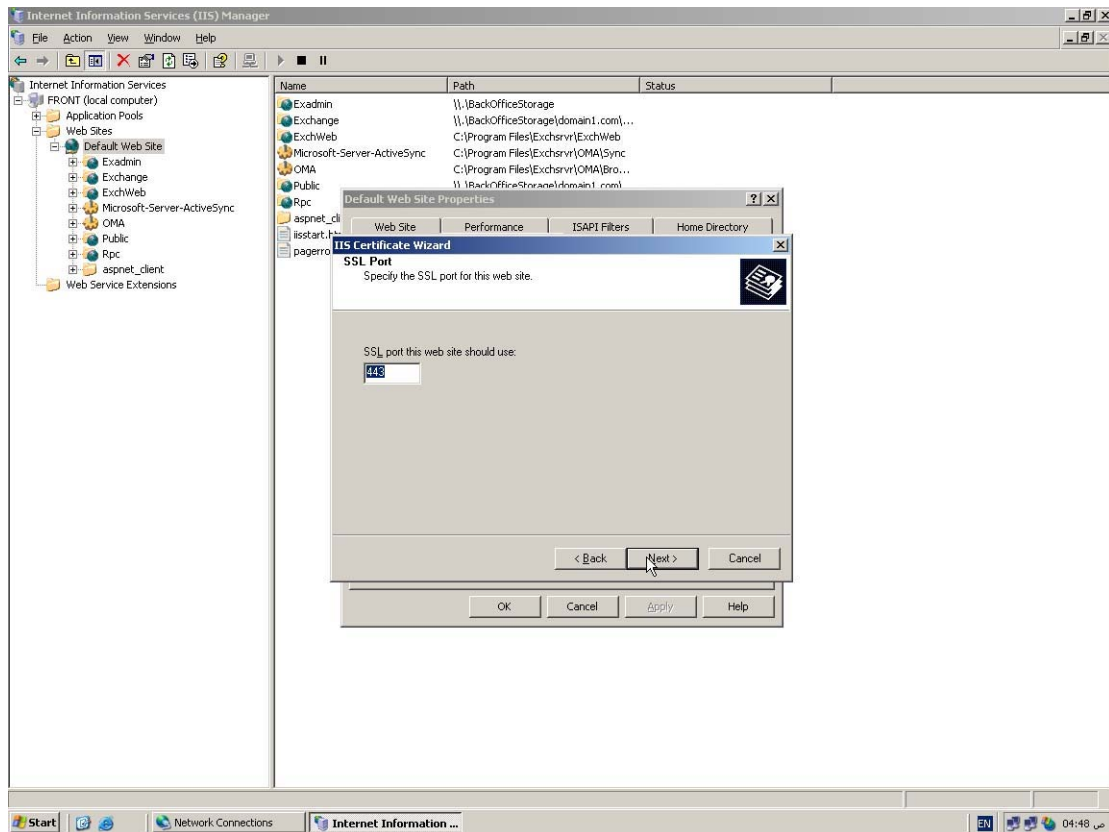
And save it on the FE

Now switch back to the IIS mmc

Open the server certificate you will be prompted with the following screen: choose process the pending request.



Open the certificate that you have saved
When you click and if the certificate is right you will have the following screen to
choose the SSL port
Accept the defaults

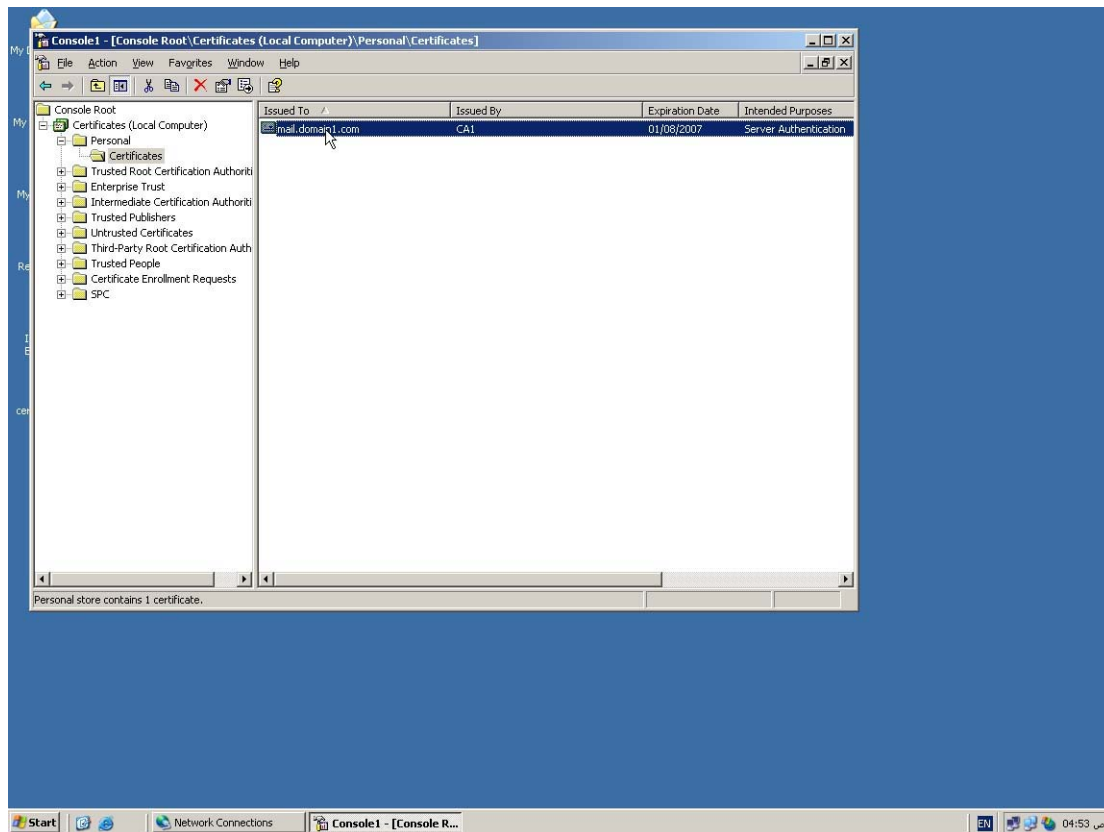


Click next then finish

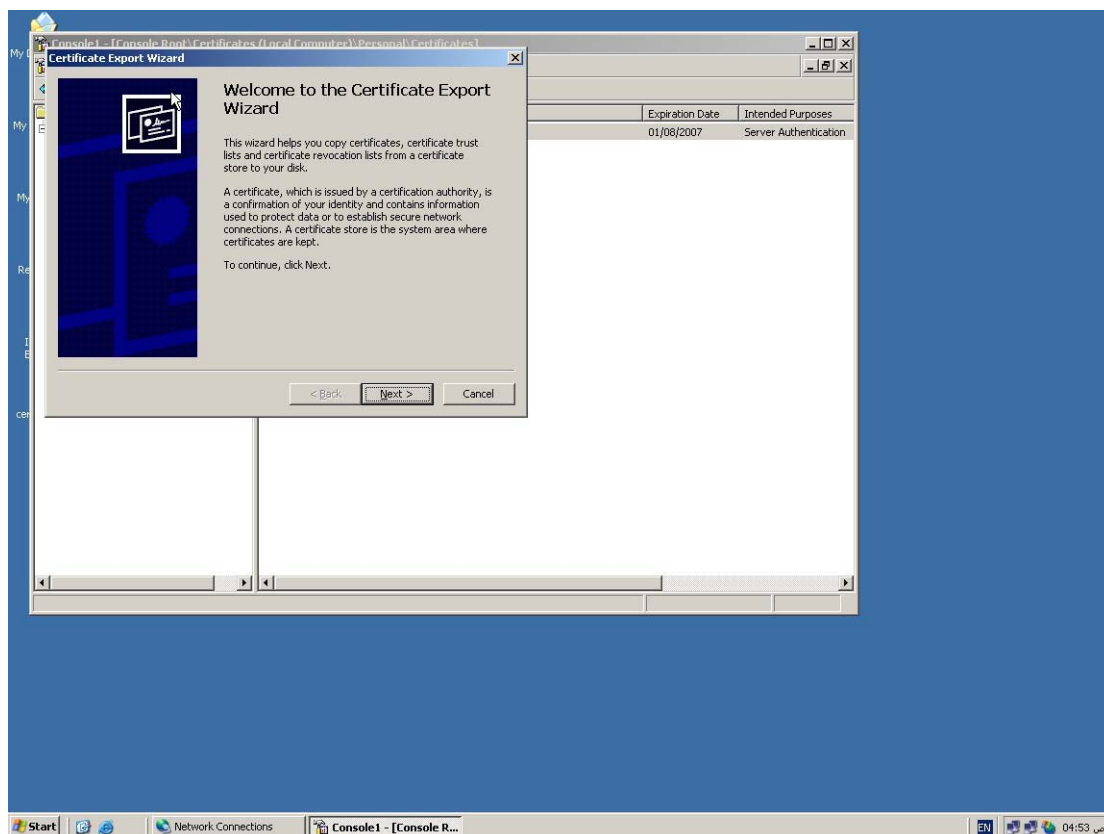
Now we need to export this certificate as the ISA server will use it to publish the HTTPS, so go to start → run → mmc → ctrl + m → alt+d then add certificate and choose computer account

In the personal container open the certificates

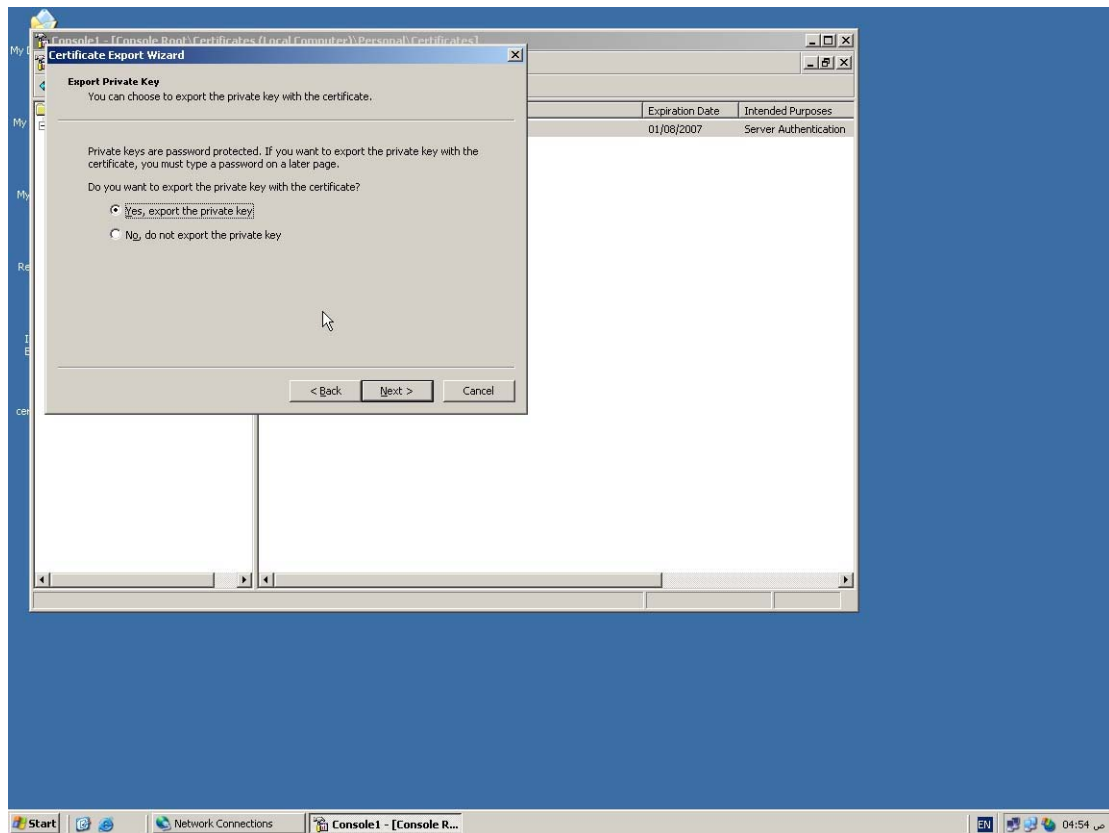
You will find the mail.domain1.com certificate as in the image



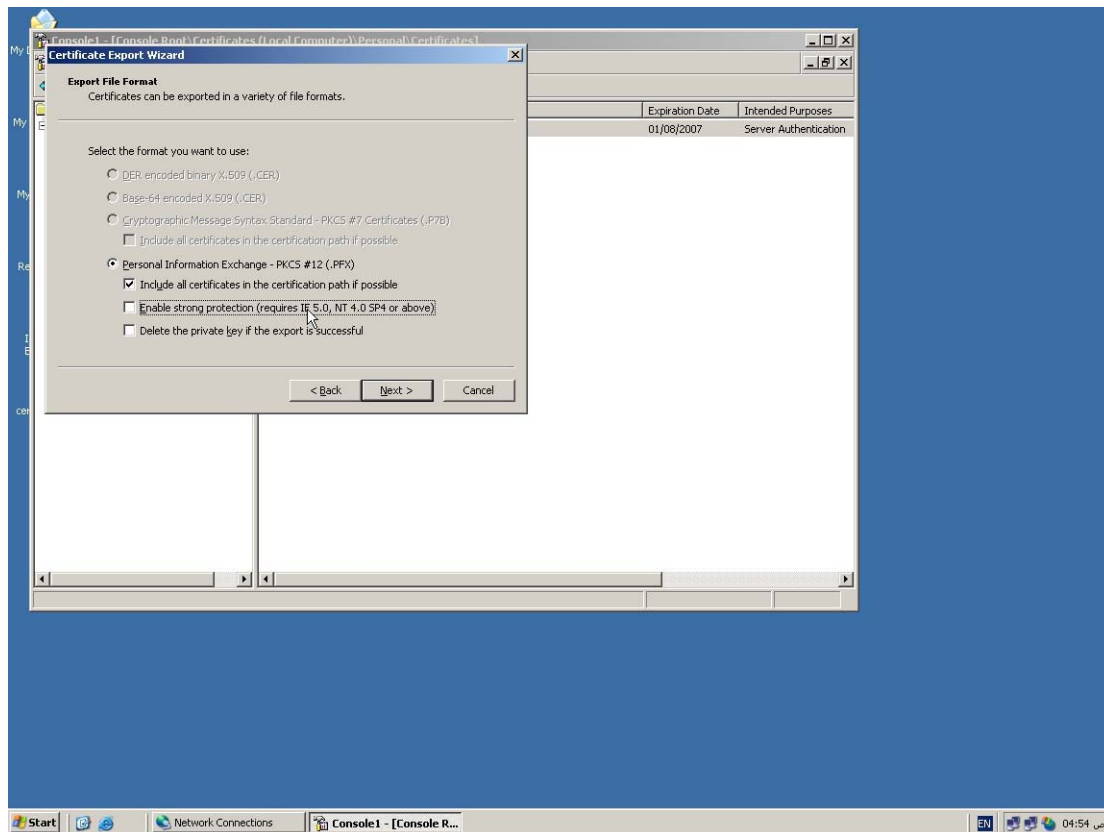
Right click on it and on all tasks choose export
You will be faced with the export wizard click next



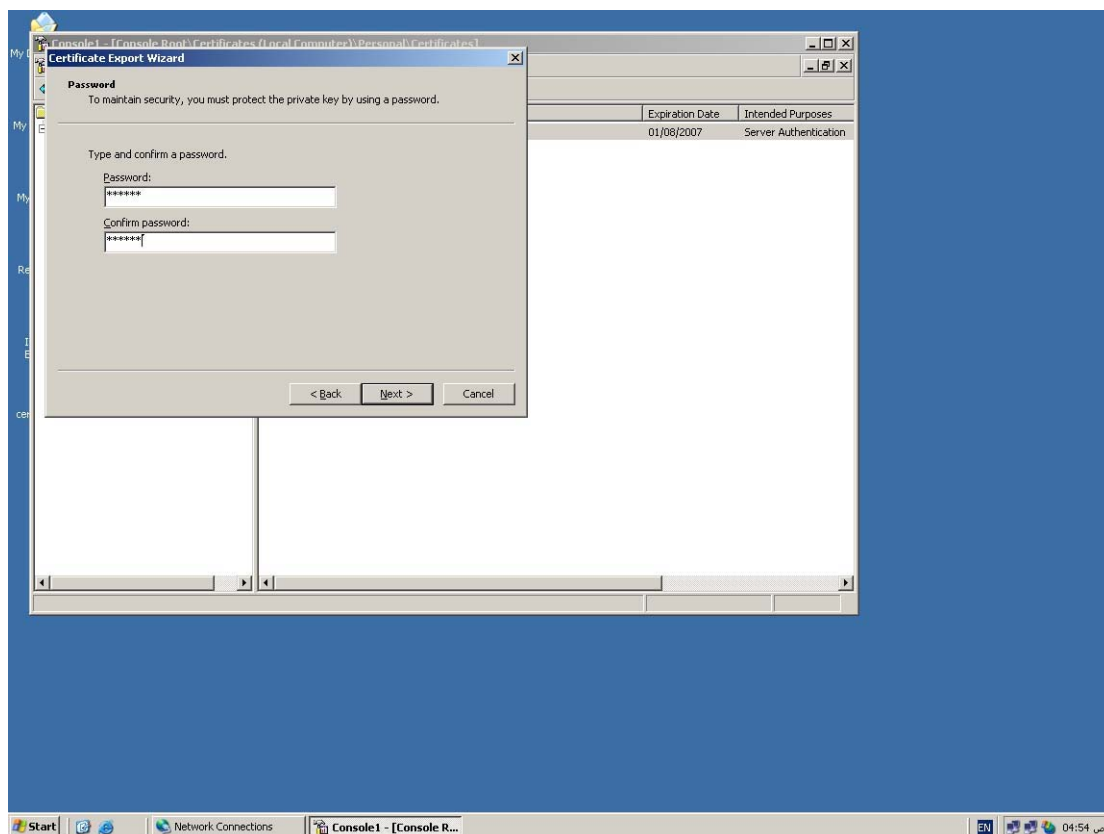
Choose to export the private key (it is very important to export the private key or your users will be prompted with http error 500)



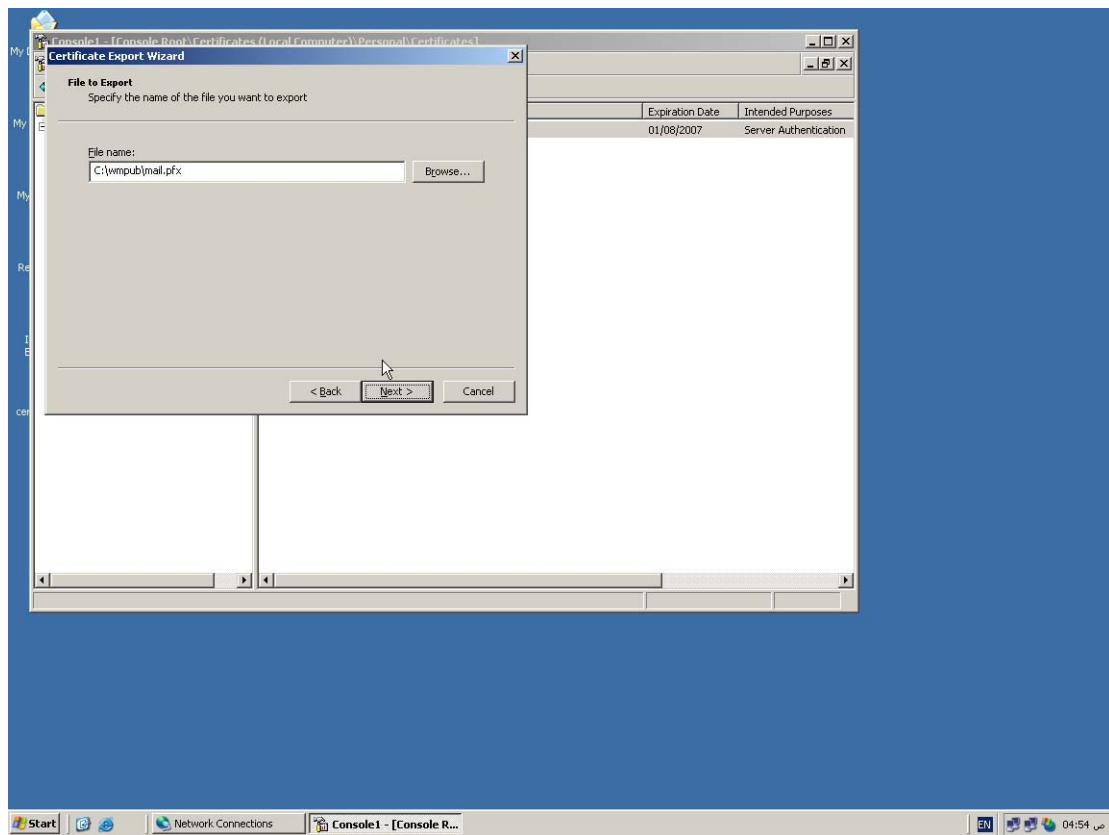
In the export file format choose to export all related certificates (it is also very important so we can export the root CA certificate)



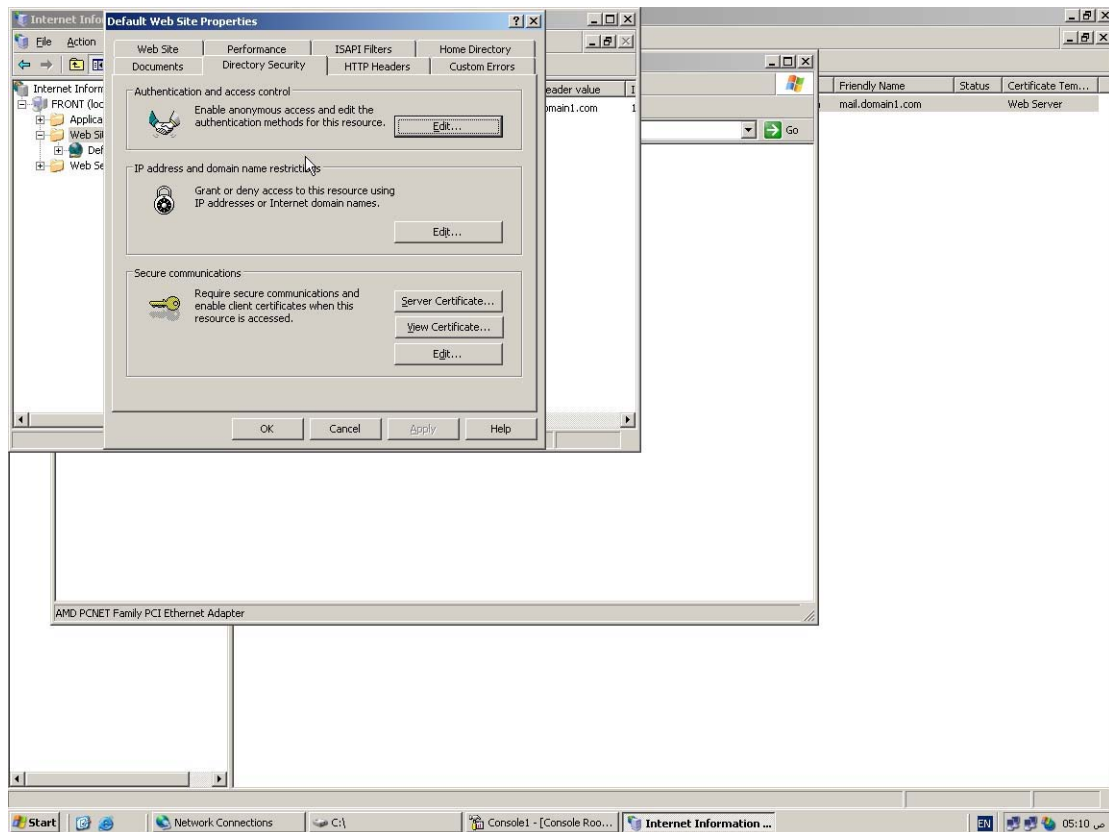
Type a password to protect the private key (you will be prompted for it when you import it on the ISA server.



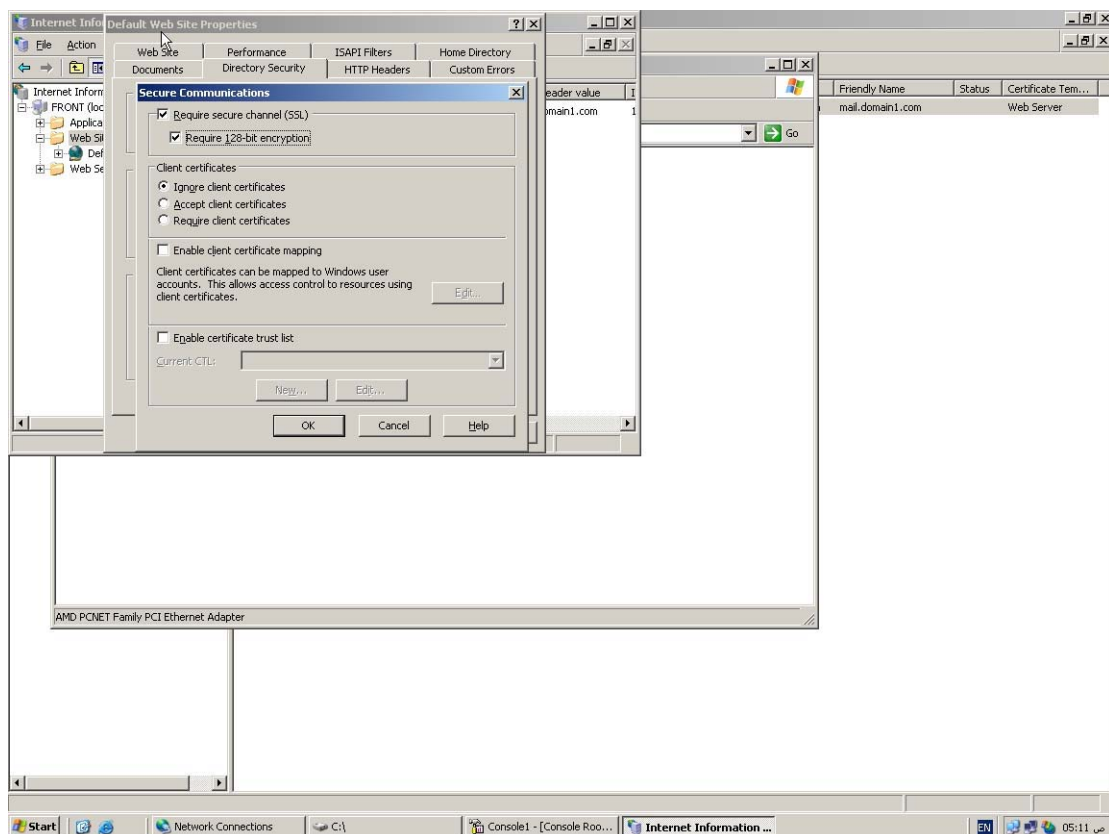
Save the file in a shared folder that is accessible for the ISA, you will use this file later on in the Play with ISA section...



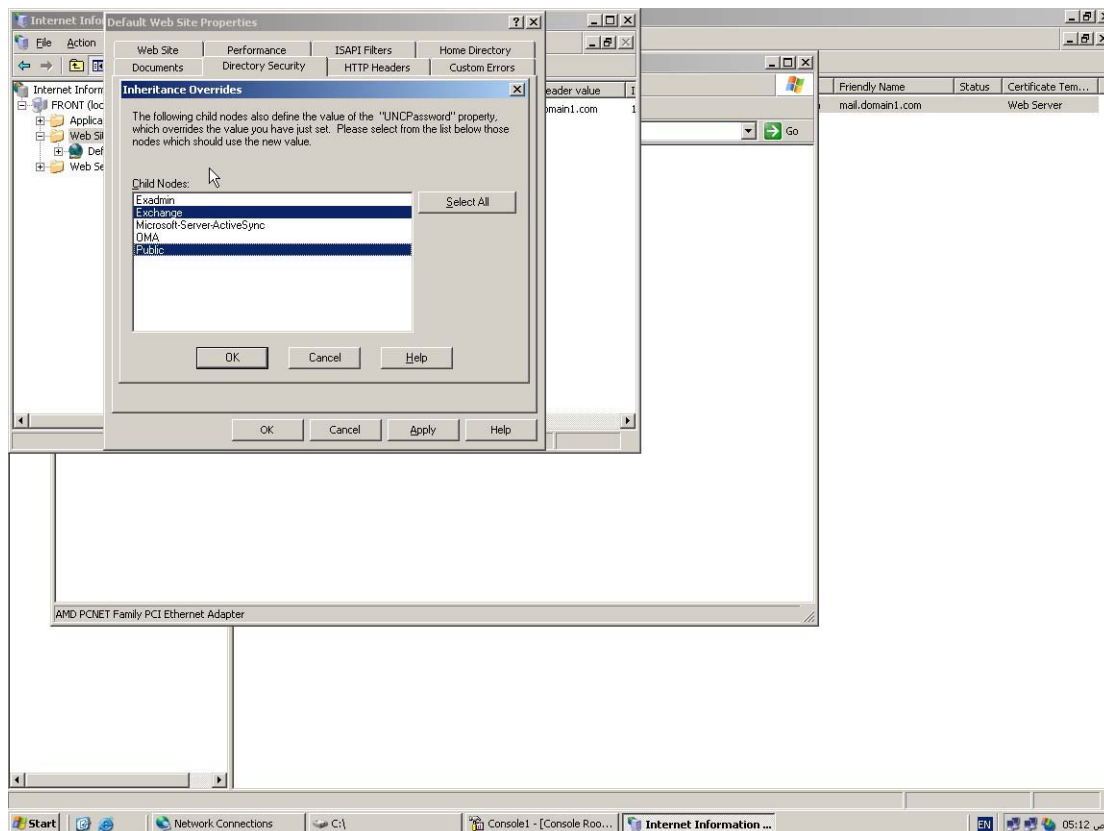
Now to require the users to connect over https on the FE open the IIS mmc choose properties and in the directory security chose edit



Check the box to require the SSL and also check the box to enable require 128 encryption



Choose apply, you will be prompted that the subfolders setup is different than the configuration that you chose so choose to apply these settings for the public and exchange folders

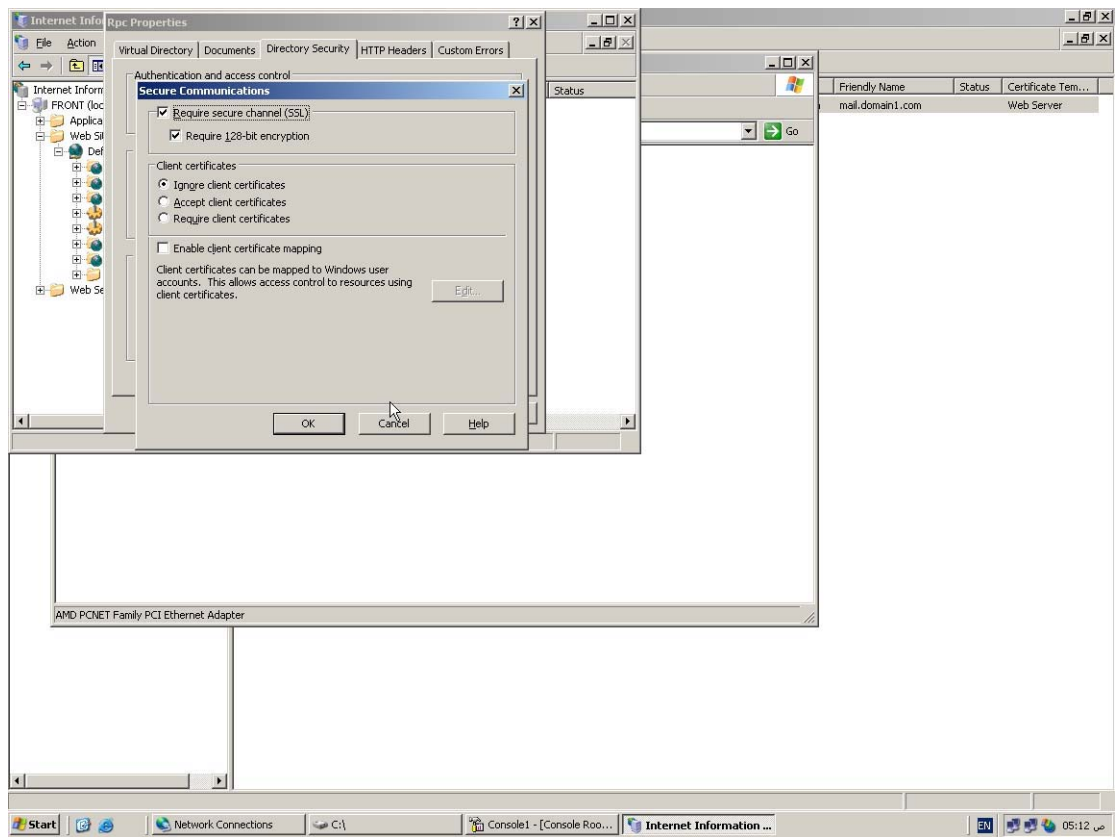
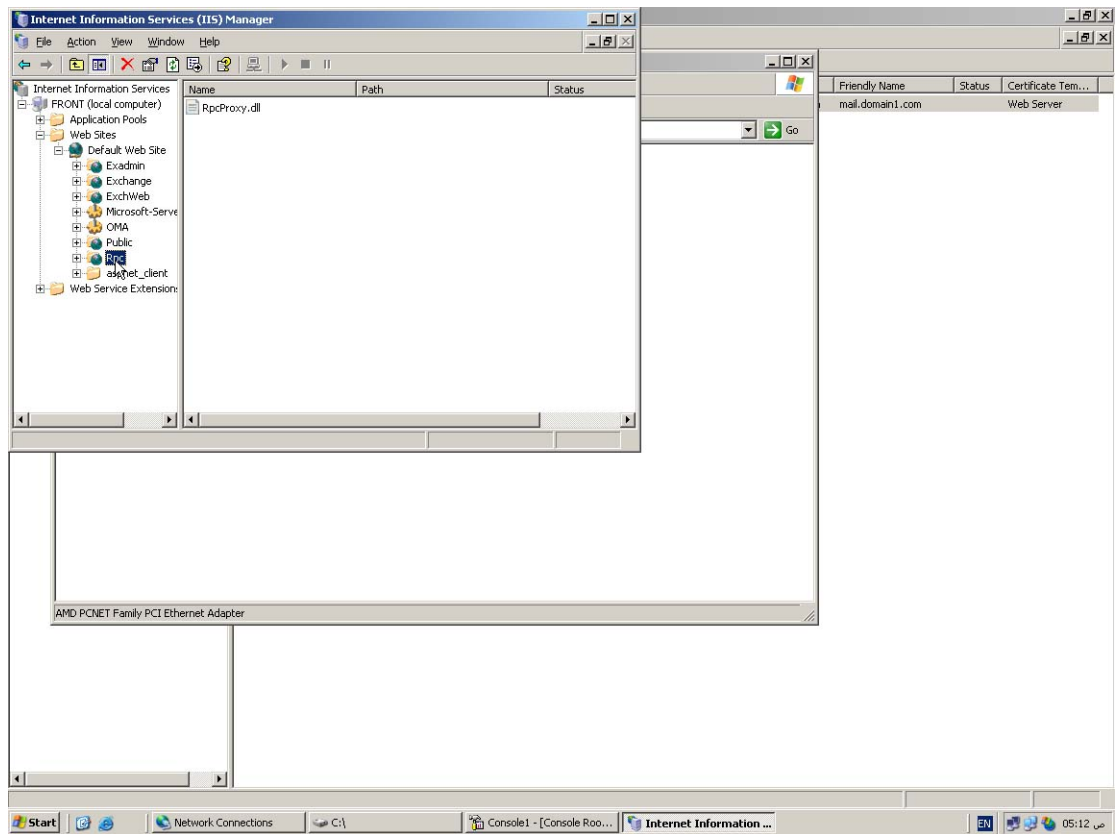


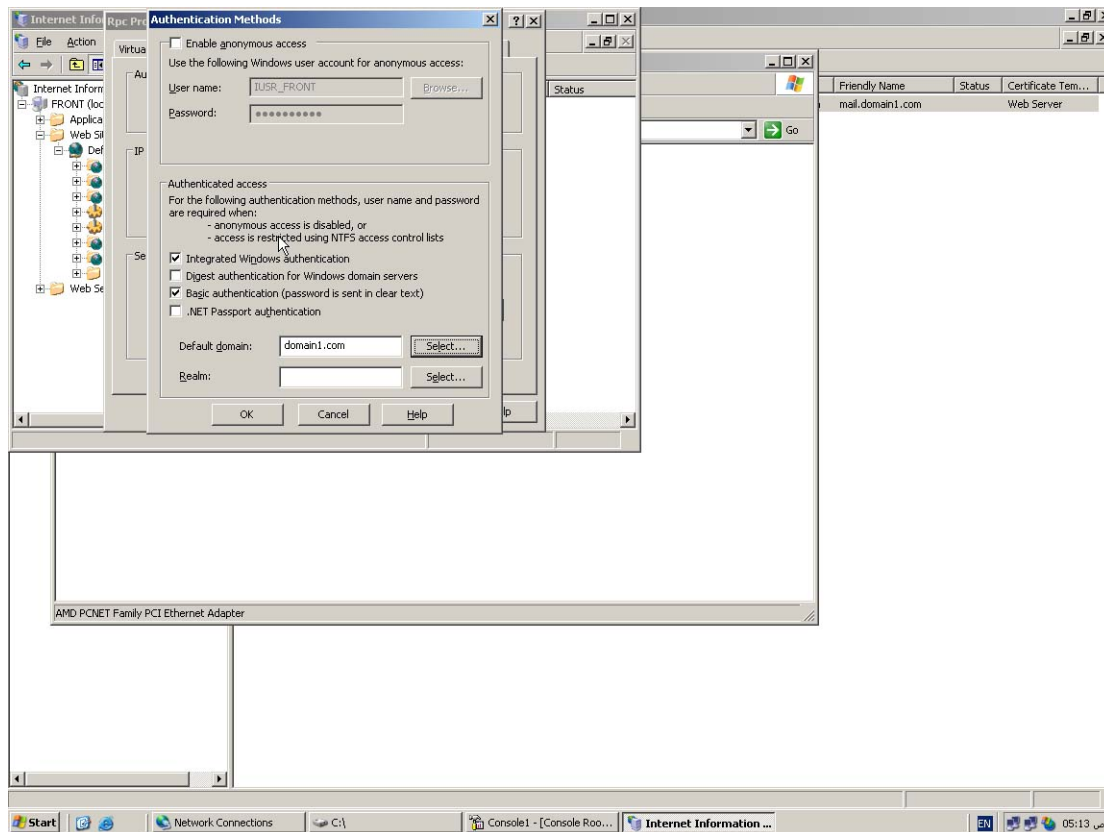
User over the RPC will connect using basic authentication, in the basic authentication user name and password are sent in plain text, but you don't have to worry about it because you secured it using the HTTPS

Also users can use NTLM authentication but this is not preferable, To insure that basic authentication is used and no anonymous login over the rpc is used

go to the RPC directory Choose properties, then directory security then edit and ensure that you require SSL and 128 encryption on it, this is a very important stage because this will require the outlook 2003 users to connect over the rpc using https

in the authentication and access control choose edit and remove the check box on the anonymous access, and remove the check box on the integrated windows authentication (this will remove the NTLM authentication method) and choose basic authentication and choose the domain to be domain1.com





Stage 3 : work around with the ISA:

The access to the OWA will be over HTTPS and also the rpc will access the backend using HTTPS so we will use one rule to grant the users the access for both OWA and RPC over HTTP, and we will use the OWA publishing using mail publishing rule. First we need to import the certificate because we will implement SSL bridging.

SSL bridging Overview:

SSL Bridging is a ISA firewall feature that allows the ISA firewall to perform stateful application layer inspection on SSL connections made to Web published Web servers on an ISA firewall Protected Network. This unique feature allows the ISA firewall to provide a level of stateful application layer inspection that no other firewall in its class can perform today.

SSL bridging prevents intruders from hiding exploits within an encrypted SSL tunnel. Conventional stateful filtering firewalls (such as most 'hardware' firewalls on the market today) cannot perform stateful application layer inspection on SSL connections moving through them. These hardware stateful filtering firewalls see that an incoming SSL connection, check the firewall's Access Control List, and if there is an ACL instructing the stateful packet filter based firewall to forward the connection to a server on the corporate network, then the connection is forwarded to the published server without any inspection for potential application layer exploits.

The ISA firewall supports two methods of SSL bridging:

- SSL to SSL bridging

- SSL to HTTP bridging

SSL to SSL bridging provides a secure SSL connection from end to end. SSL to HTTP bridging ensures a secure connection between the Web client and the ISA firewall and then allows a clear text connection between the ISA firewall and the published Web server.

In order to appreciate how the ISA firewall works with SSL in protecting your Web server, let's look at the life cycle of a communication between the Web client on the Internet and the Web site on the ISA firewall protected network:

1. The OWA client on the Internet sends a request to the ISA firewall's external interface.
2. An SSL session is negotiated between the Web client on the Internet and the ISA firewall's external interface
3. *After* the SSL session is established, the Web client sends the username and password to the ISA firewall. The SSL tunnel that has already been established between the Web client and ISA firewall and protects these credentials.
4. The request is decrypted *before* the request is forwarded by the ISA firewall to the published Web server. The decrypted packets received from the Web client are examined by the ISA firewall and subjected stateful application layer inspection via the ISA firewall's HTTP security filter and any other application layer inspection filters you've installed on the ISA firewall. If the ISA firewall finds a problem with the request, it is dropped.
5. If the request is acceptable, the ISA Server firewall re-encrypts the communication and sends it over a *second* SSL connection established between the ISA firewall and the published Web site on the ISA firewall Protected Network.
6. The published Web server decrypts the packet and replies to the ISA firewall. The Web server encrypts its response and before sends it to the ISA firewall.
7. The ISA firewall decrypts the response received from the published Web server. It evaluates the response in the same way it did in step 4. If something is wrong with the response, the ISA firewall drops it. If the response passes stateful application layer inspection, the ISA firewall re-encrypts the communication and forwards the response to the Web client on the Internet via the SSL session the Internet Web client already established with the ISA firewall.

SSL 'Tunneling' versus SSL 'Bridging'

The ISA firewall actually participates in *two* different SSL sessions when SSL-to-SSL bridging is used:

- An SSL session between the Web client and the external interface of the ISA firewall
- A second SSL session between an internal interface of the ISA firewall and the published Web server

The typical stateful packet-filter firewall only performs forwards connections for published SSL sites. This is sometimes referred to as 'SSL tunneling.' The conventional stateful filtering firewall accepts SSL communications on its external interface and forwards them to the published SSL server. Application-layer information in the communication is completely hidden inside the SSL tunnel because the packet filter-based firewall has no mechanism to decrypt, inspect, and re-encrypt the data stream. Because traditional stateful filtering firewalls are unable to make allow and deny decisions based on knowledge of the contents of the encrypted tunnel, it passes viruses, worms, buffer overflows and other exploits from the Web client to the published Web site.

The ISA firewall can also perform SSL-to-HTTP bridging. In the SSL-to-HTTP bridging scenario, the connection between the Web client and the external interface of the ISA firewall is protected in the SSL tunnel. The connection between the ISA firewall's internal interface and the published Web server on the corporate network is sent 'in the clear' and not encrypted. This helps performance because avoids the processor overhead incurred for the second SSL link.

However, you have to consider the implications of SSL-to-HTTP bridging. Steve Riley (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/askus/auaswho.asp>), a Program Manager on the ISA Server team at Microsoft, has mentioned that the external user connecting to the published Web site using SSL has an implicit agreement and expectation that the entire transaction is protected. We agree with this assessment. The external Web client enters into what can arguably be considered a 'social contract' with the published Web server, and part of that contract is that communications are protected from 'end to end.'

SSL-to-SSL bridging protects the data with SSL and the ISA Server firewall services from end to end. SSL-to-HTTP bridging protects the data from the OWA client and while it's on the ISA Server firewall, but it is not safe once it's forwarded from the ISA Server firewall and the OWA site on the internal network.

Step 1 Import the certificate from the FE website:

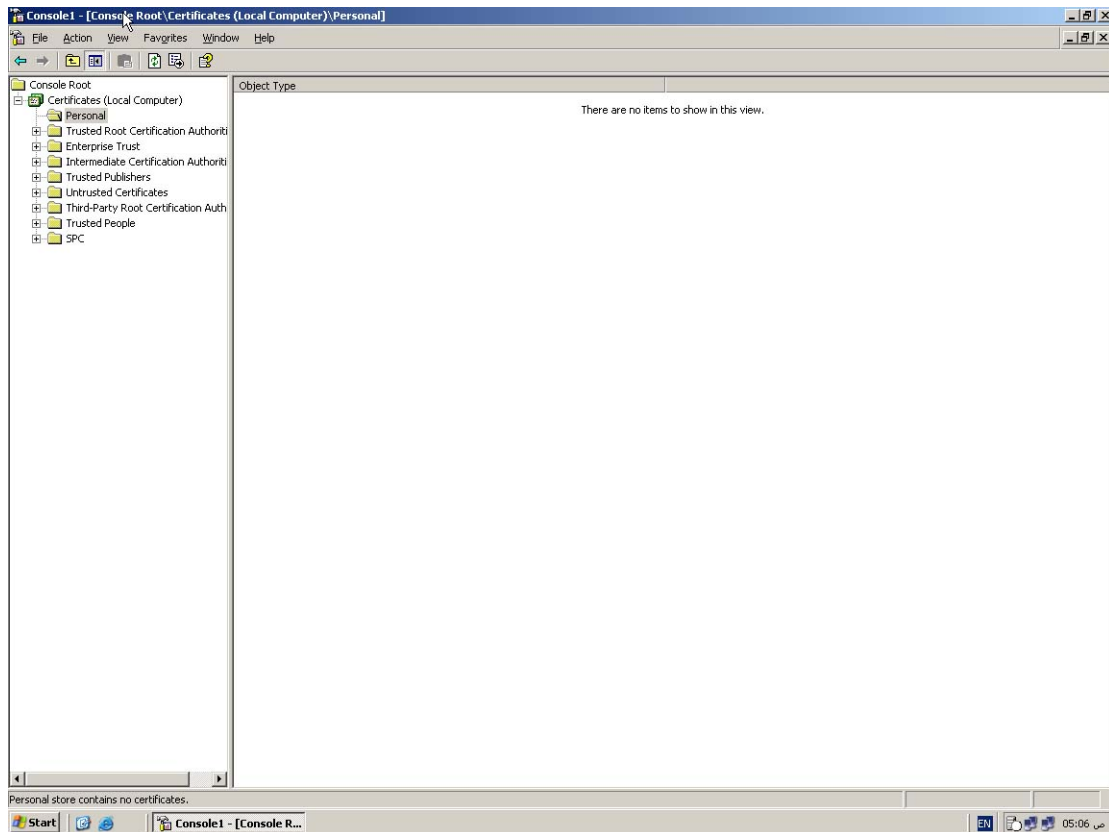
Do you remember that we have exported the certificate the FE use to implement SSL for the OWA access now we will import this certificate on the ISA

Create a simple rule that allows all traffic from localhost(ISA) to the internal network or for more security to the FE only but create a computer set first.

Then share the folder that contains the file that has been exported before and copy that file to the ISA it self

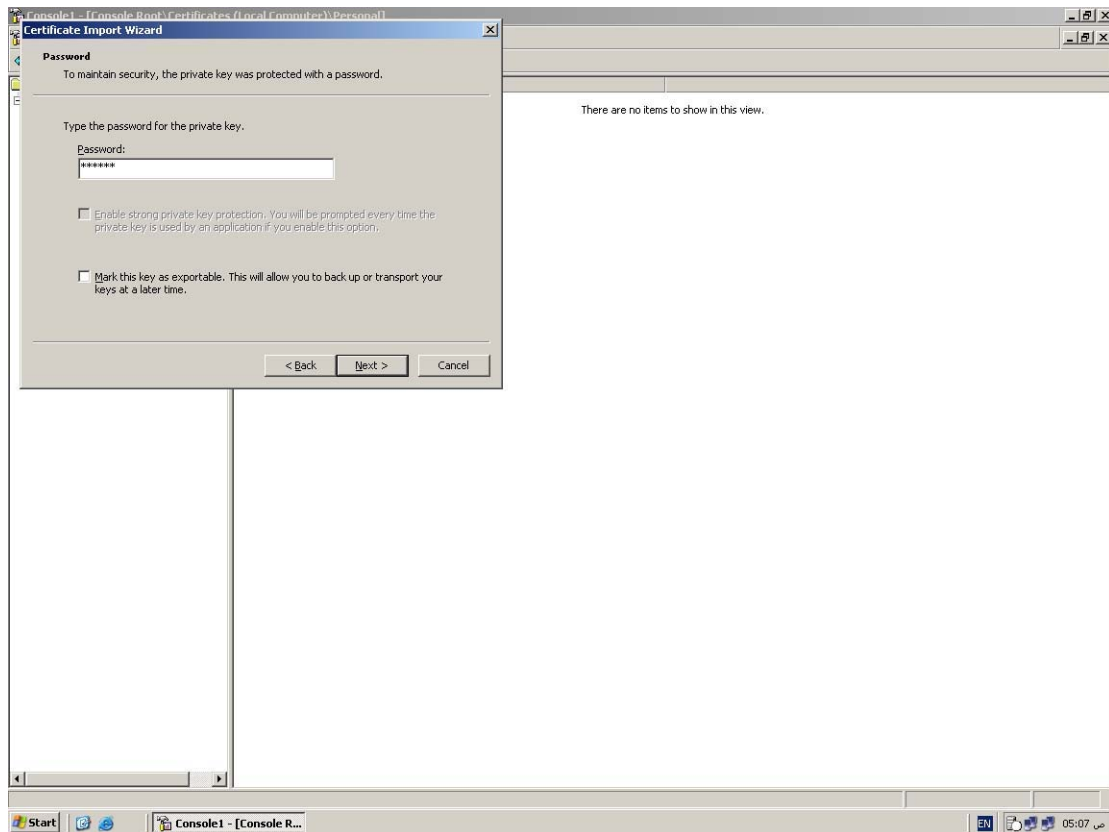
Open Start → run → mmc → ctrl+m → alt+d → add certificate → add computer account → then local computer

You should be at this image:

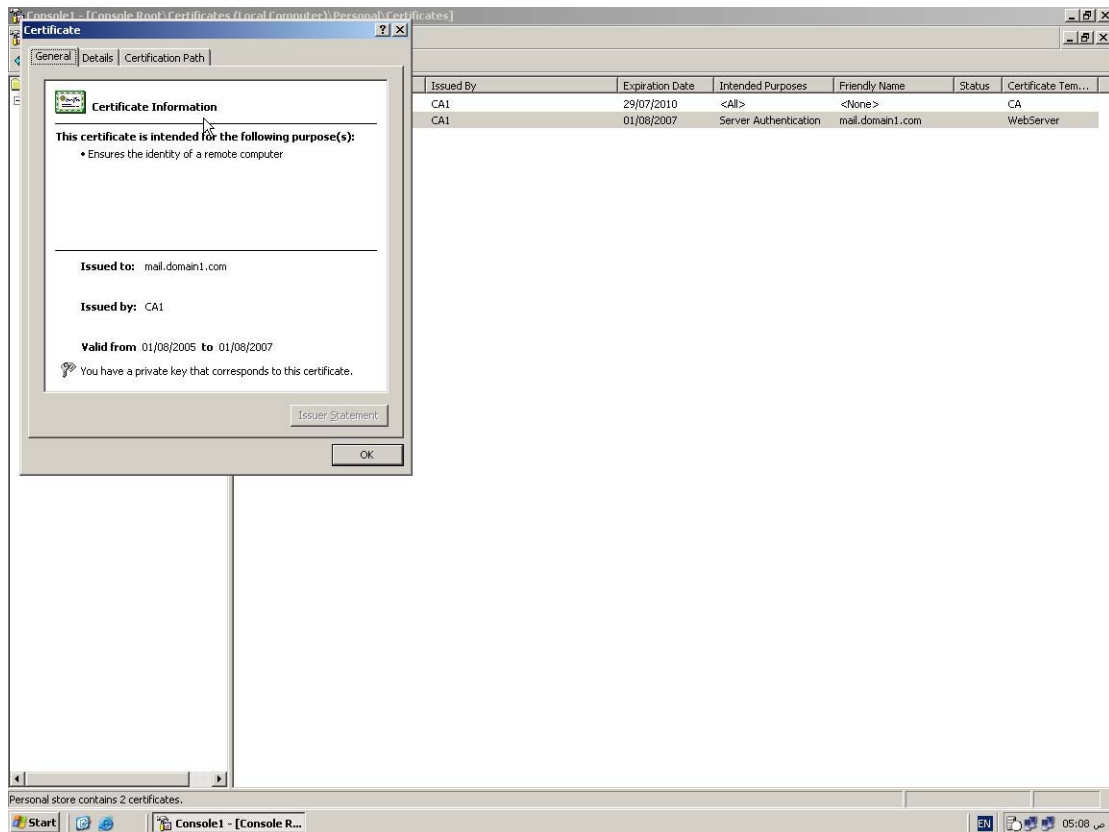


Expand personal the right click then import

You will prompted with the import wizard select the exported certificate when you click next you will be faced with the password that you have chose to protect the private Key (that is why I have told you to save it) type the password and click next then finish



If you double click on the mail.domain1.com certificate you will find that it is marked with a red rose because the isa is not a member in the domain and have no idea about the CA that issued the certificate so to make the ISA trust the CA in the certificate container in the personal folder you will find actually 2 certificates one for mail.domain1.com and the other is for CA(which is the name of my CA it will be a name according to your setup) so copy the CA certificate the paste it in the trusted root authority folder and double click again on the mail,.domain1.com certificate it should be like this

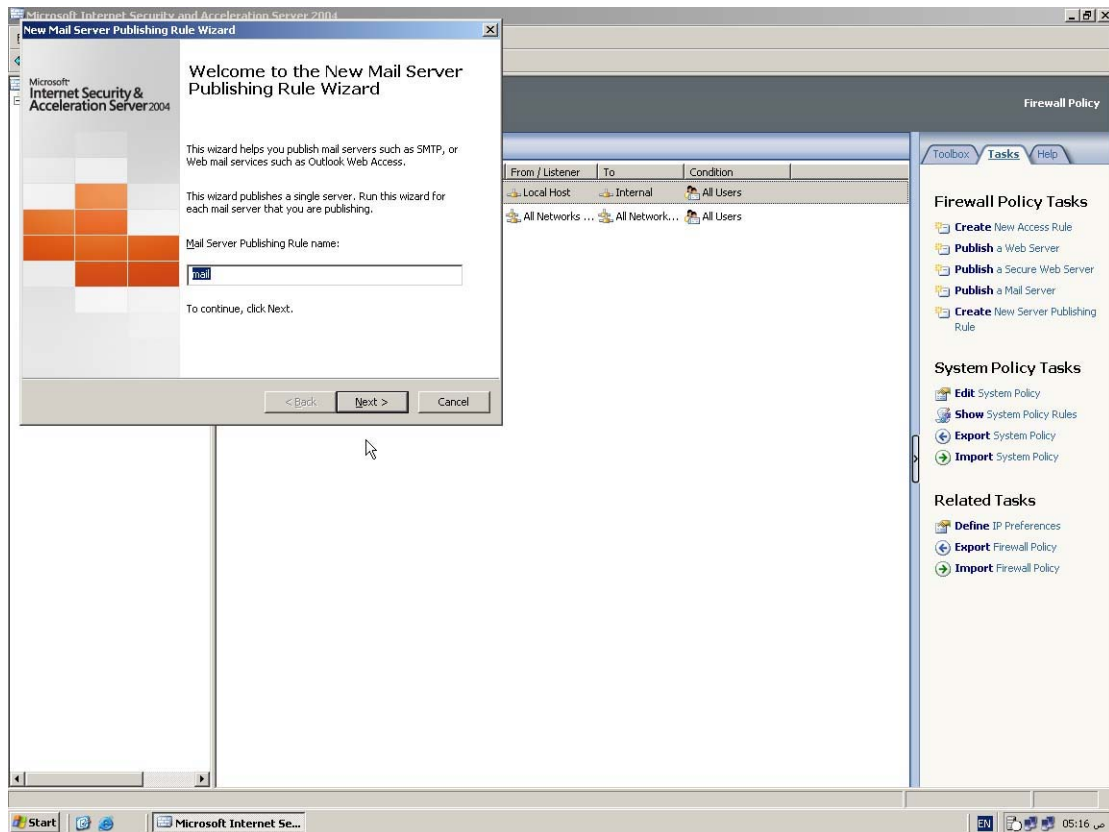


Step 2 publish the OWA and allow the RPC:

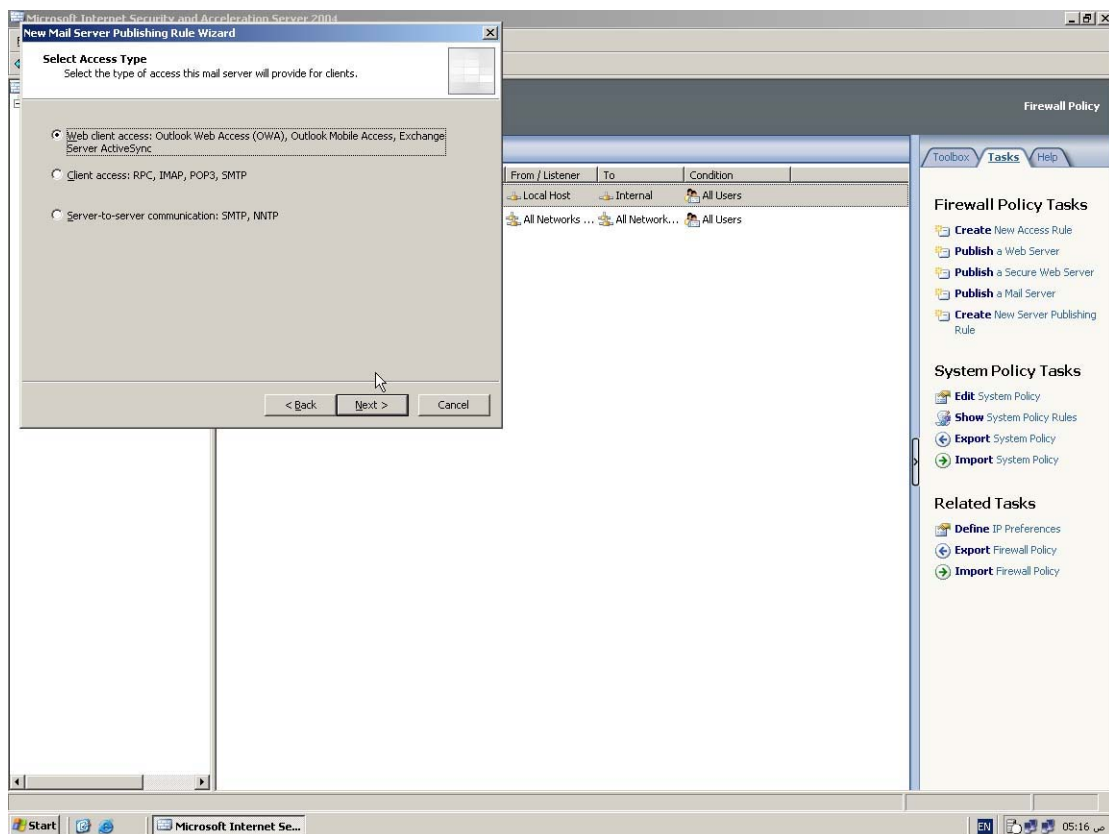
Now you are ready to use this certificate to publish the OWA throw the SSL

On the ISA server go to firewall policy right click new policy and then mail publishing rule

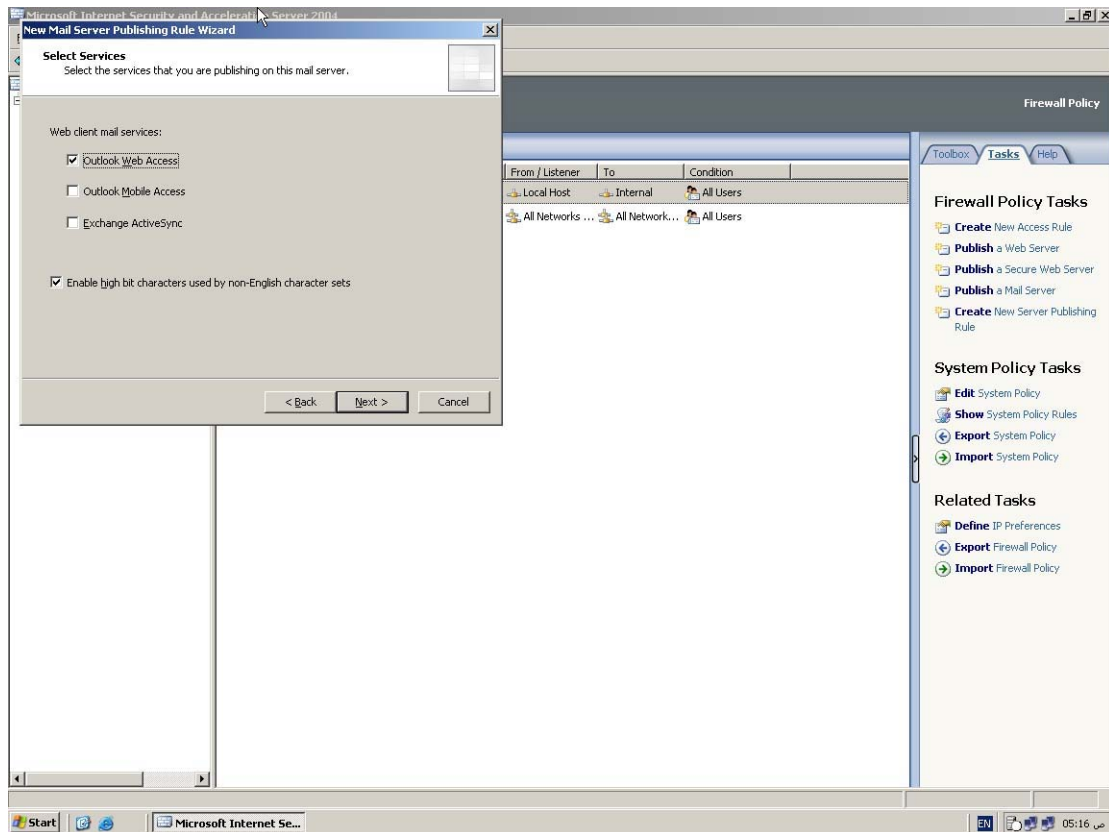
Name the rule any name



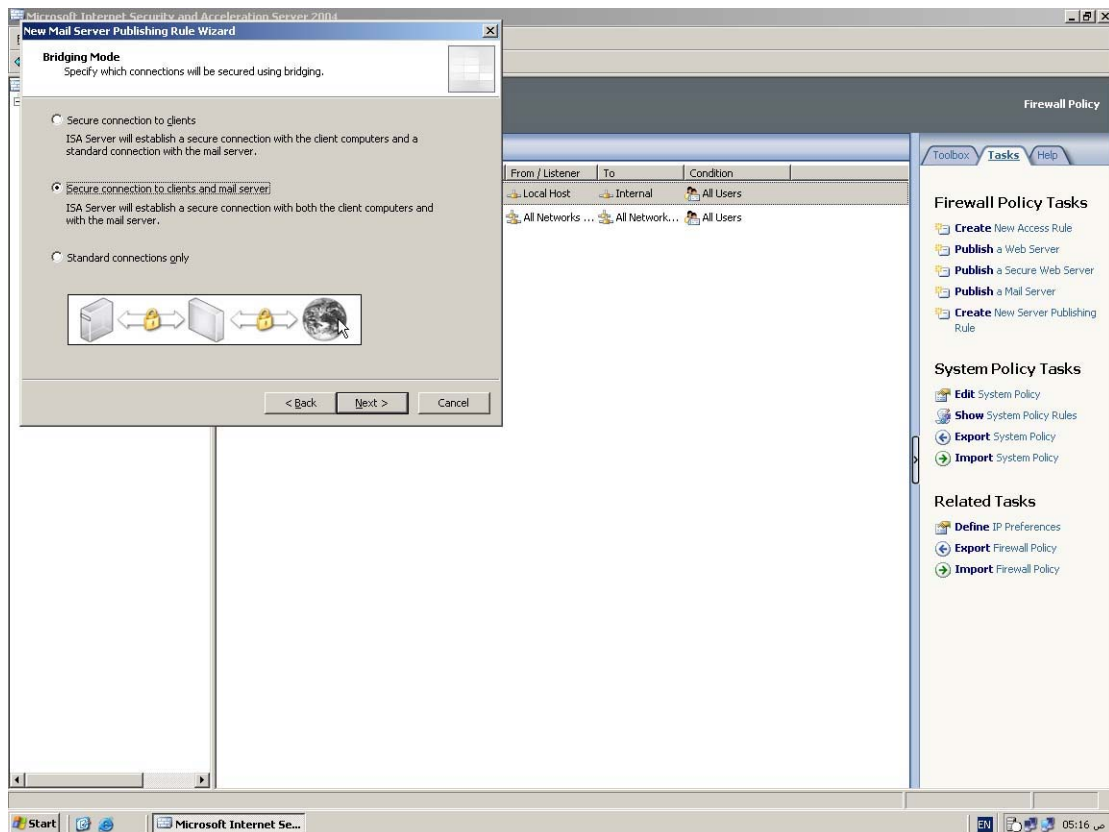
Select web client access



Select outlook web access and if you use active sync and OMA select them also

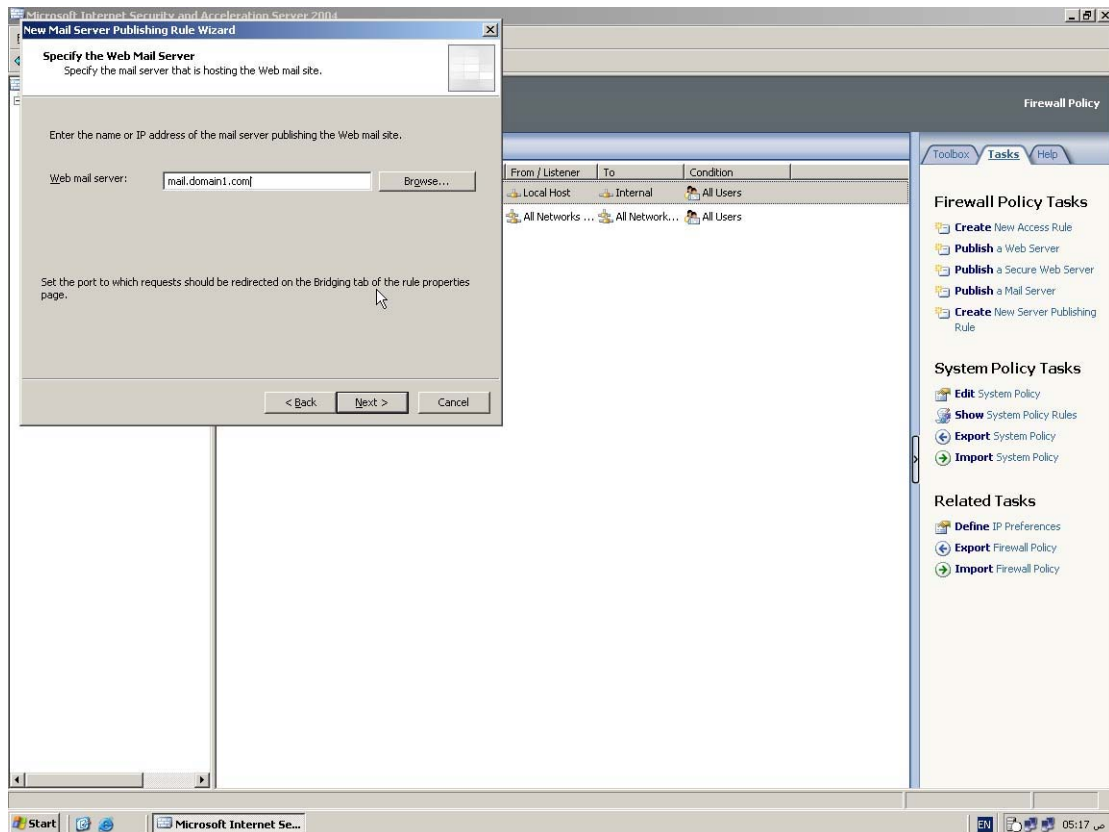


In the bridging mode select secure connection between the client and mail server



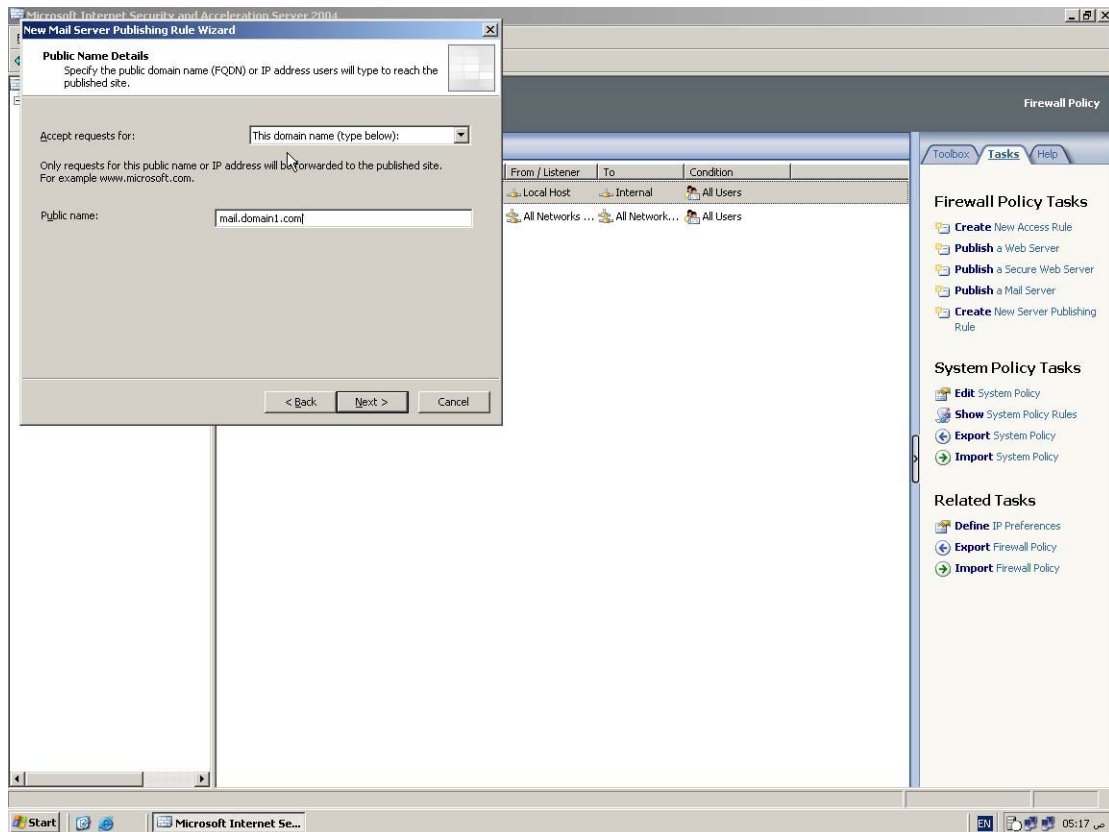
In the web mail server (please please please) I spent 3 hours trying to troubleshoot the OWA access because it wasn't working because of this because the mail server name should be the name that used in the common name in the certificate while you was requesting out also it should be the exact name as the header name that you set it up on the FE using the IIS mmc

So put here mail.domain1.com



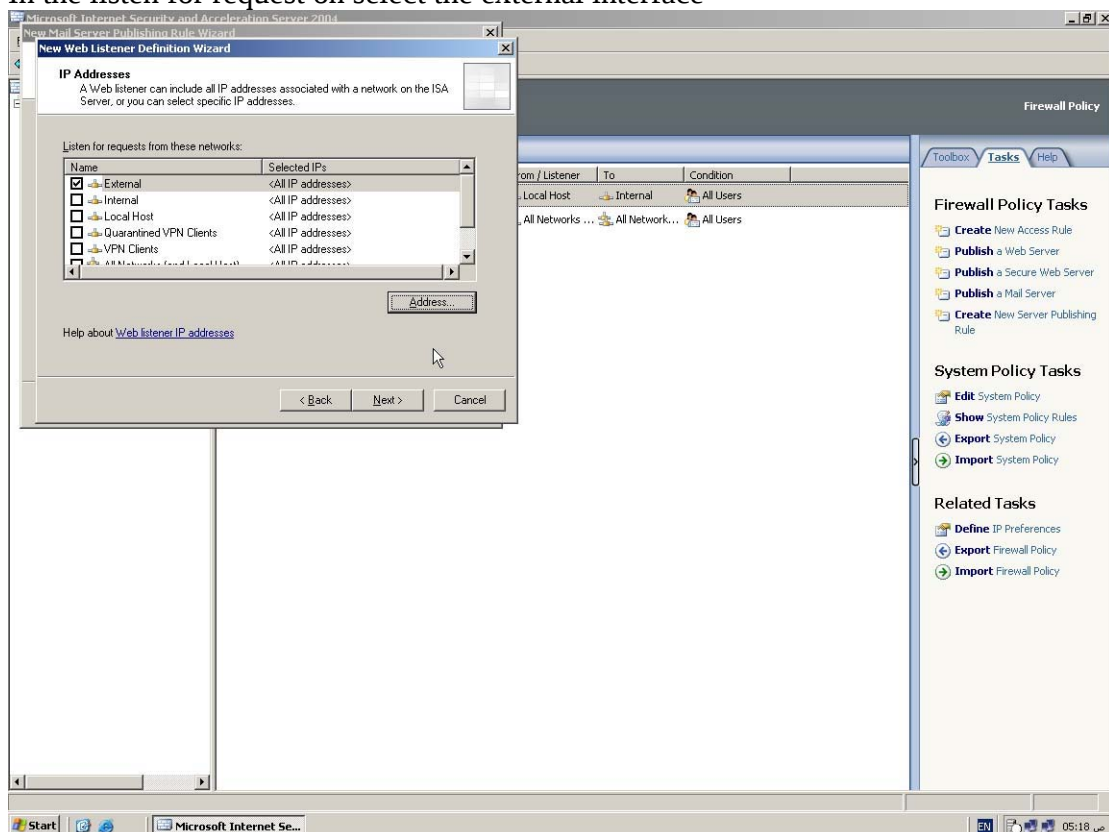
In the public name type mail.domain1.com

This is will be the public name that users will use to access the mail server

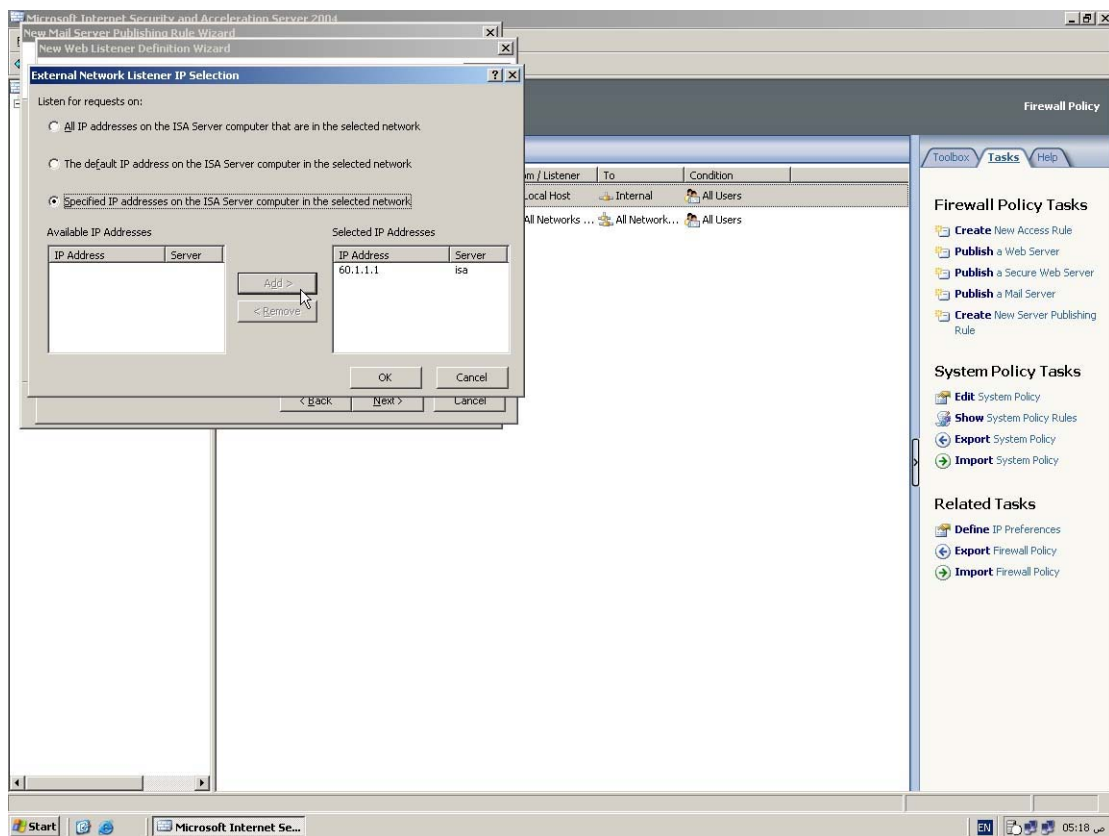


When you click next you will be prompted to choose a listener so we don't have one yet so choose new

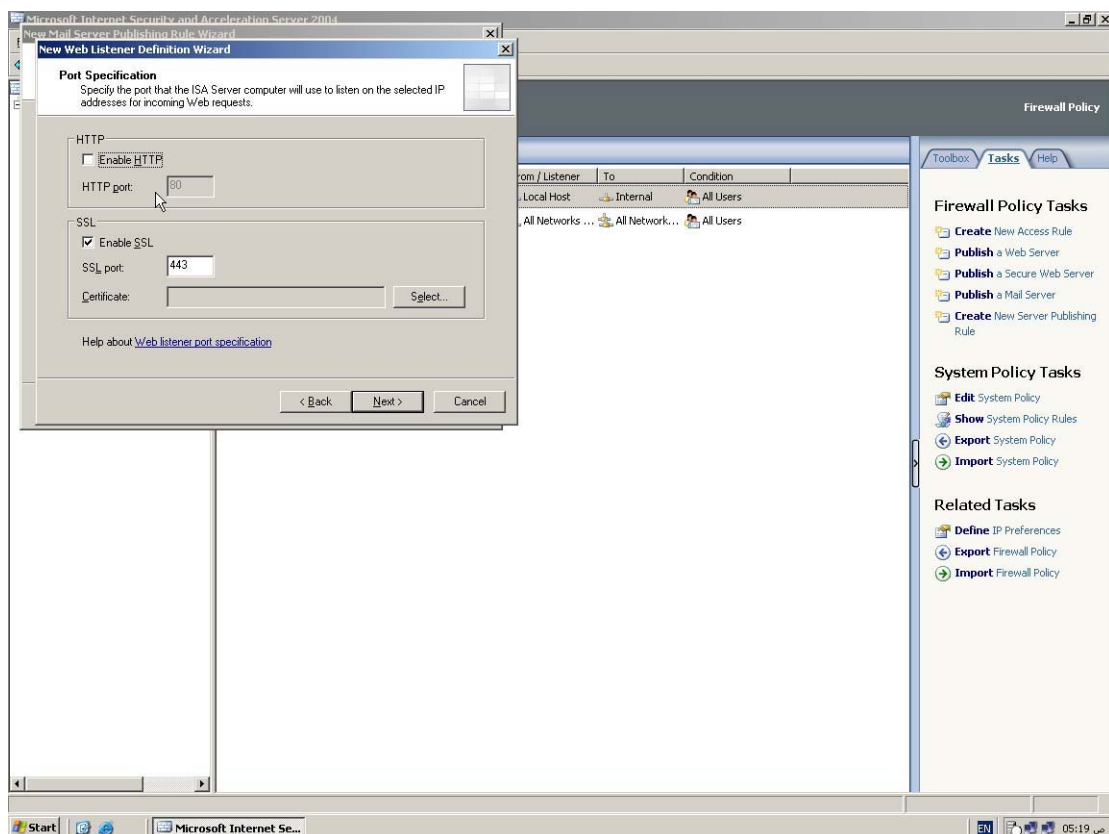
In the listen for request on select the external interface



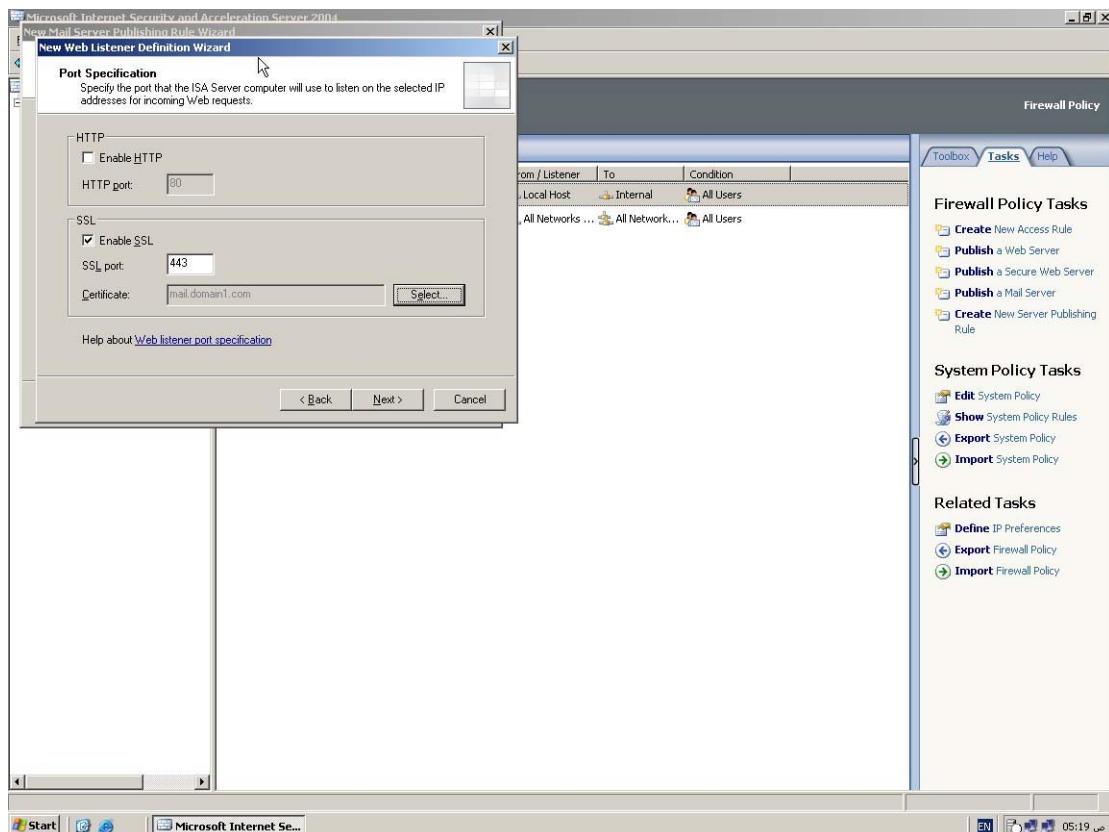
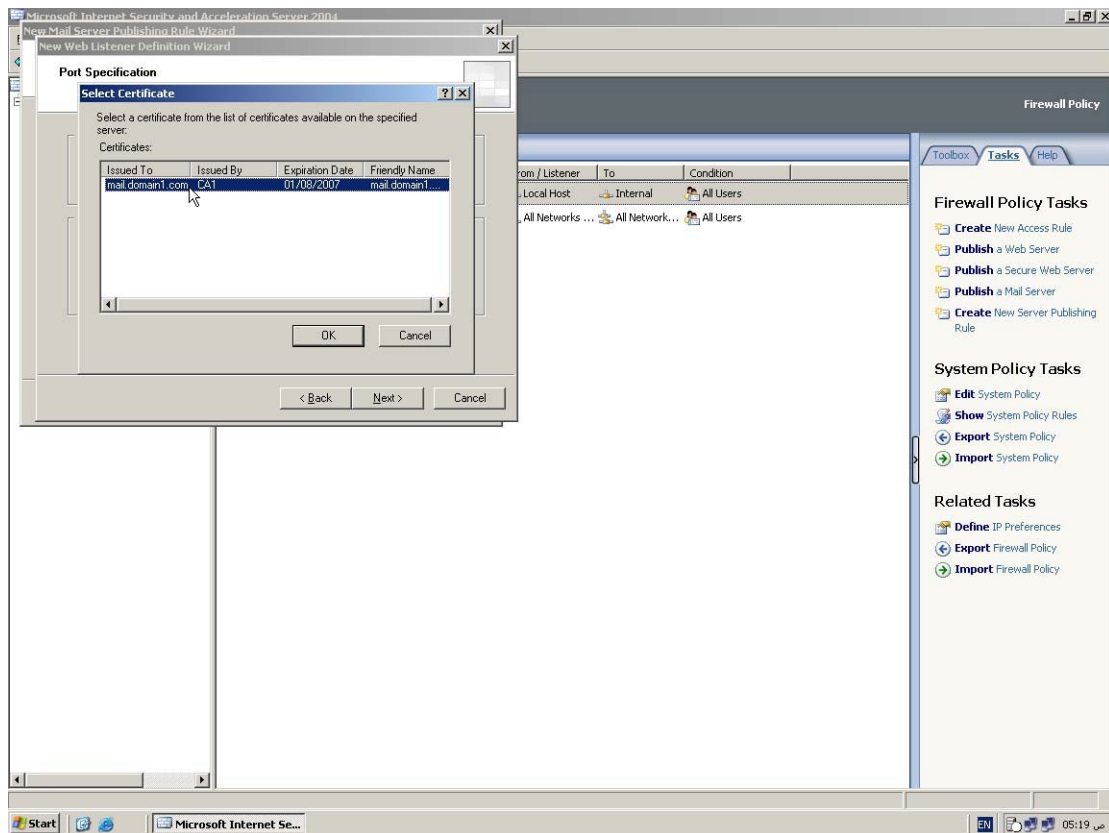
In the ip specify one ip to listen on (this is also to prevent socket pooling on isa)



In the port deselect the http and enable only ssl



You will have to choose a certificate before you click next so click on select and you will be prompted with a list of certificates that isa can use so select the mail.domain1.com



Then next then finish

There is last step, ISA now don't now where is mail.domain1.com so you can choose to install DNS service and use it or use the hosts file I used it, in the hosts file add the internal IP of the FE which in this scenario 192.168.1.2 and it should be mapped to mail.domain1.com FQDN

Now from a laptop which represents the external client add the mail.domain1.com in the hosts file and it should map to the external interface's IP that ISA listen on which is 60.1.1.1 to map to mail.domain1.com

In the IE type <http://mail.doamin1.com/exchange> you should be required to use ssl
Now type <https://mail.domain1.com/exchange> you should be prompted with a warn for the certificate click use and you will prompted to enter the username and password enter them you should have the access to the OWA

To setup RPC over http in outlook 2003 clients:

[How to configure RPC over http for Outlook2003](#)

General notes:

- 1- you might experience very slow connection from outlook while connecting rpc over http this is because outlook2003 fallback to rpc over tcp and wait for a response then connect using rpc over Http to force RPC over HTTP :create the following value:
Value Name: DisableRpcTcpFallback
Data: 1
Path: HKLM\Software\Microsoft\Office\11.0\Outlook also review this [MS KB](#)
- 2- review this [KB](#)
- 3- [PKI design](#)
- 4- [troubleshoot certificates using certutil](#)
- 5- [Troubleshoot certificates in ISA2004](#) very important article
- 6- You can use the FE as a Bridge head this is the preferred methode and use the ISA or use the FE as smart host and forward the email from the BE
- 7- To allow outbound email messages you will have to allow SMTP traffic I didn't add this step but it is mandatory to allow internal and external users to send email for an external recipient.

Any notes or question are welcome on mmagdy@synergyps.org or rshereif@synergyps.org

Thanks a lot

Mahmoud magdy

Rēda shereif

