GENERAL INFORMATION ABOUT THE PRACTICE

Practice name: Deploying vpn remote access service using ssl protocol

Number of students working together: 01

Score: 02 point

Practice location: Computer room

Request:

- Hardware requirements:

+ Each student is provided with 01 computer with minimum configuration: CPU 2.0 GHz, RAM 8GB, HDD 50GB

- Software requirements on the computer:

+ Windows Server 2012 R2, Windows 7

+ VMware Workstation 9.0 or later

- Practice tools:

+ VMware virtual machine: Windows 7 SP1, Windows Server 2012. Each virtual machine has at least 02 hard drive partitions. In which partition C: contains the operating system, partition D: has at least 10 GB of free space.

- LAN connection required: no

- Internet connection required: no

- Other requirements: projector, whiteboard, pen/chalk

- Tools provided with this document: no

PREPARATION FOR PRACTICE

For instructors

Before the lesson, the lecturer (practice instructor) needs to check the suitability of the actual conditions of the practice room with the requirements of the practice lesson.

No other requirements.

For students

Before starting the practice, it is necessary to create copies of the virtual machines for use. Also specify the storage location for the tools specified in the requirements section.

DEPLOYING VPN REMOTE ACCESS SERVICE USING SSL AND RADIUS PROTOCOLS

1.1. Description

When users have a request to remotely connect to the internal network system to access data, it is necessary to ensure the security of data transmitted over the network to avoid attackers from intercepting, eavesdropping, or stealing data content.

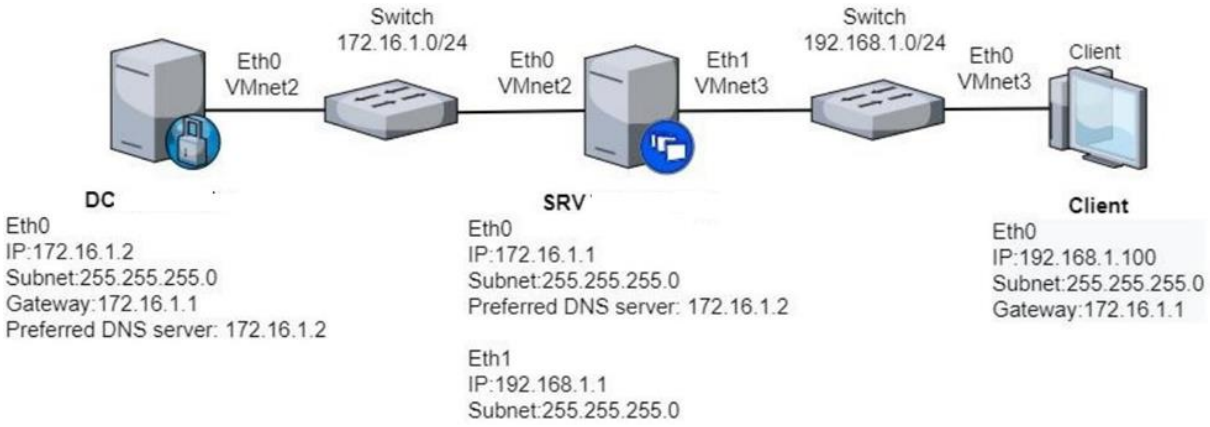
Deploy VPN technology on Windows Server 2012 using SSL/TLS security protocol combined with RADIUS authentication protocol. With this protocol, only users with accounts in the Active Directory server can access.

1.2. Preparation

- Virtual machine running Windows 7 operating system connected to Lan Segment (VMware Virtual Switch) has been set up.

- Virtual machine running Windows Server 2012 operating system connected to Lan Segment with Windows 7.

1.3. Deployment model



1.4. Implementation steps

1.4.1. Execute on DC server:

- Upgrade DC server

- Create users to allow remote access

- Install and configure Network Policy Service as Radius Server

- Install CA authentication center

- Issue digital certificate with secret key to SRV server as VPN

1.4.2. Execute on SRV server:

- Install Routing and Remote Access service ÿ Configure authentication using Radius Client to connect to DC.

- Install digital certificate issued from DC.

1.4.3. Execute on Windows 7 workstation:

- Access DC via SRV to request CA digital certificate.

- Create VPN network connection

- Configure using SSTP

- Connect to the account created on DC

- Check the result

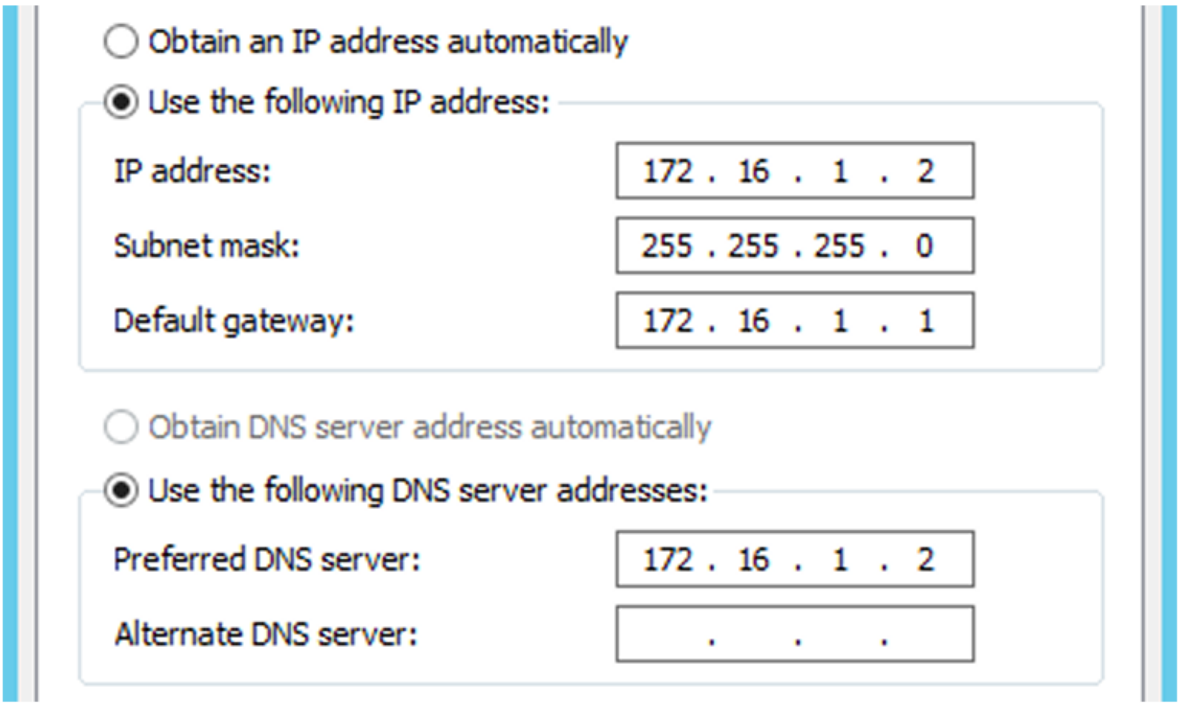
1.5. Set up IP addresses for the machines

1.5.1. On DC

- Rename the machine to DC

- Set password for user Administrator

- Set up static IP address according to deployment model

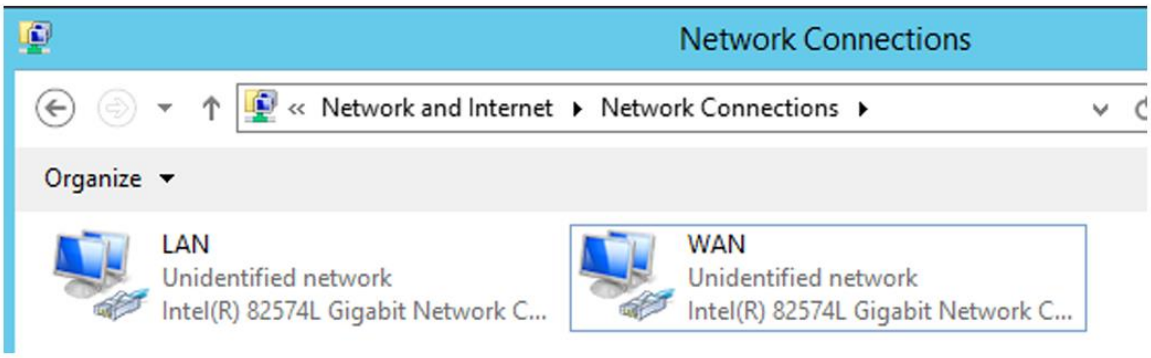


1.5.2. On SRV

- Rename the machine to SRV

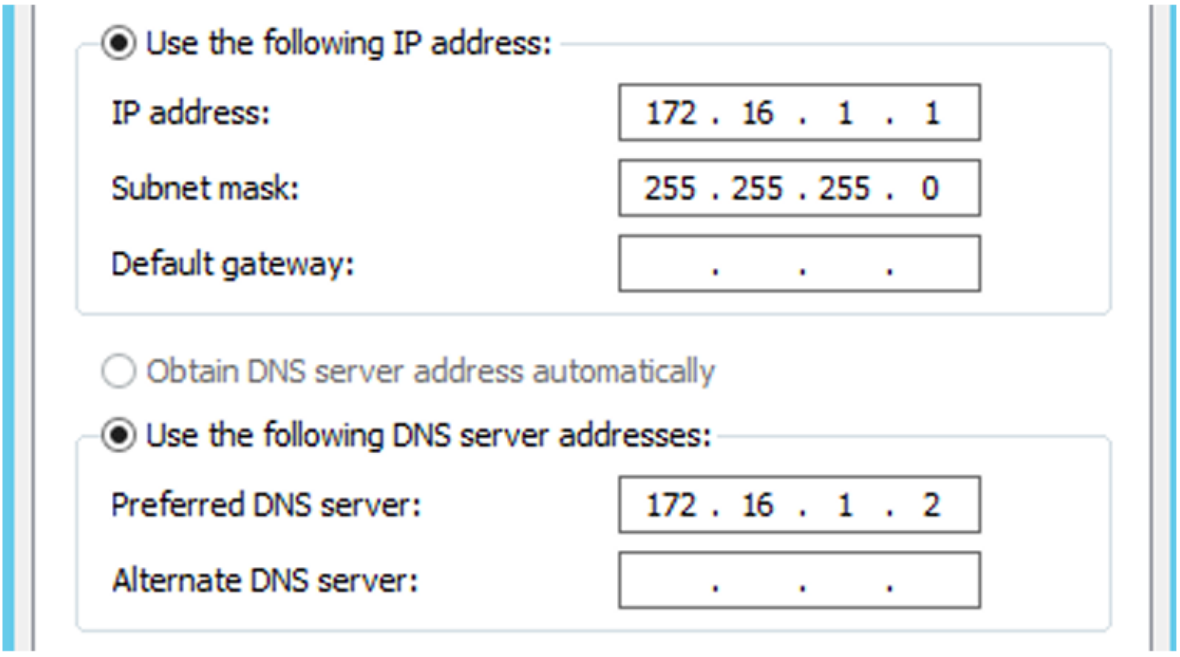
- Set password for user Administrator

- Rename card Eth0 to LAN and Eth1 to WAN

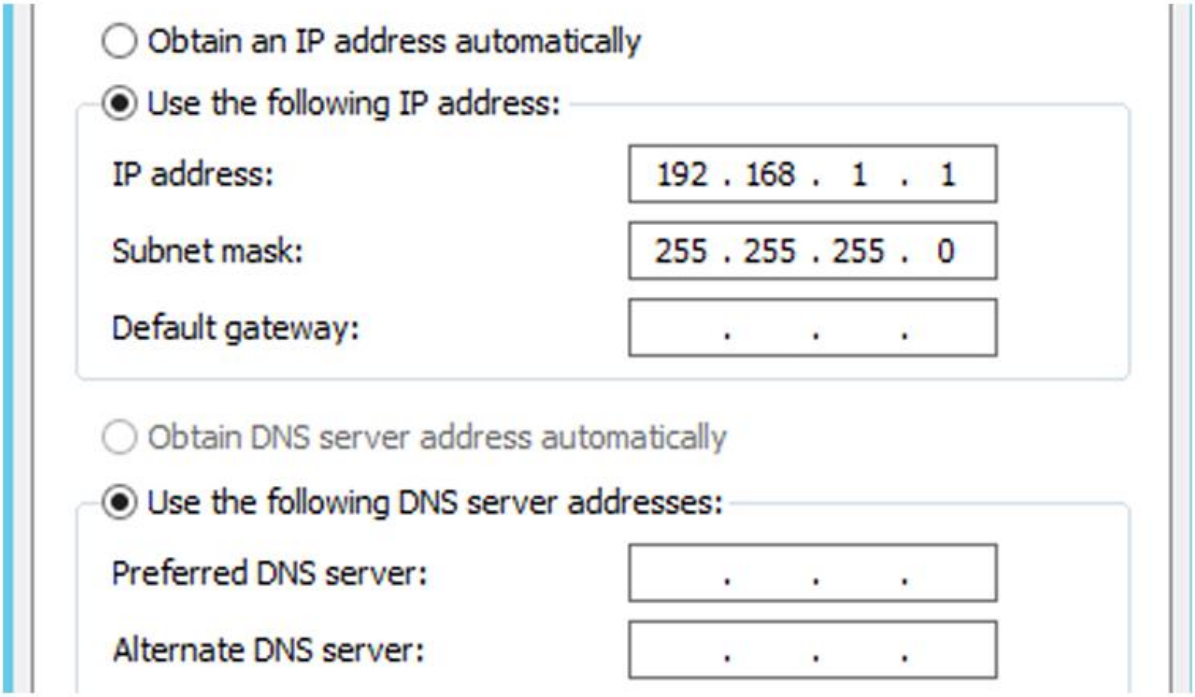


- Set up static IP address according to deployment model

- IP of LAN card



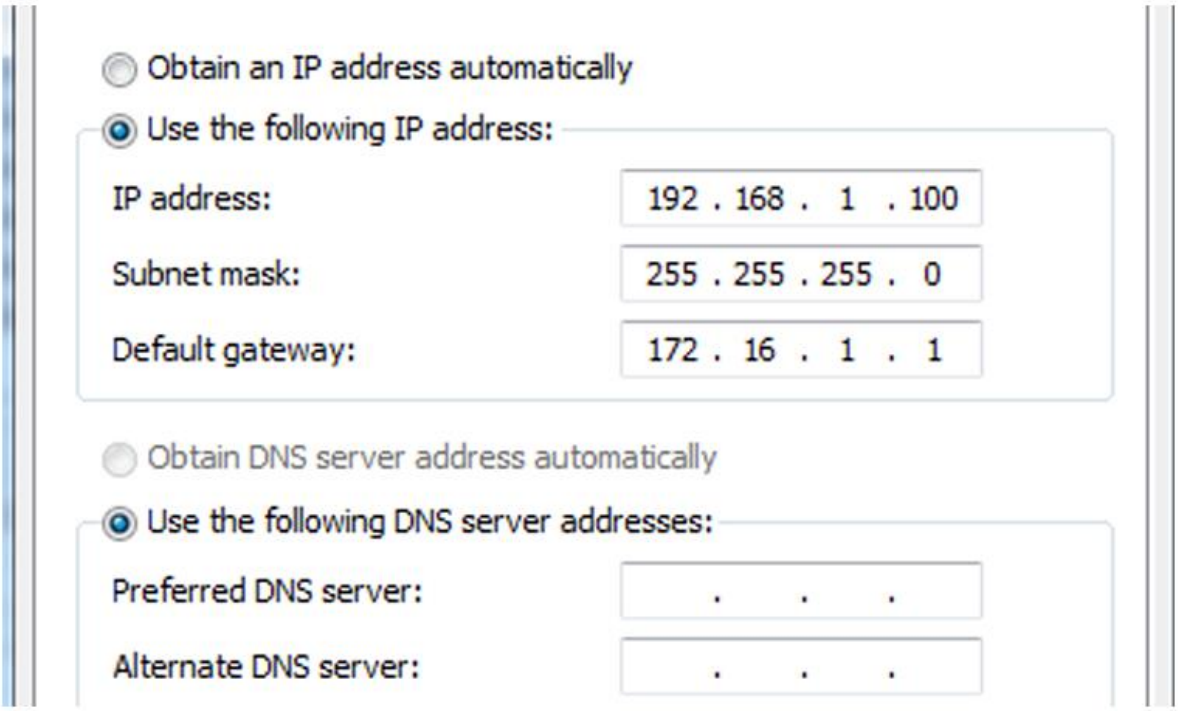
- IP of WAN card



1.5.3. On Client

- Rename the machine to Client

- Set up static IP address according to deployment model



1.5.4. Testing

- To make it easier to do the lab, we should turn off the firewall on all 3 machines DC, SRV, Client.

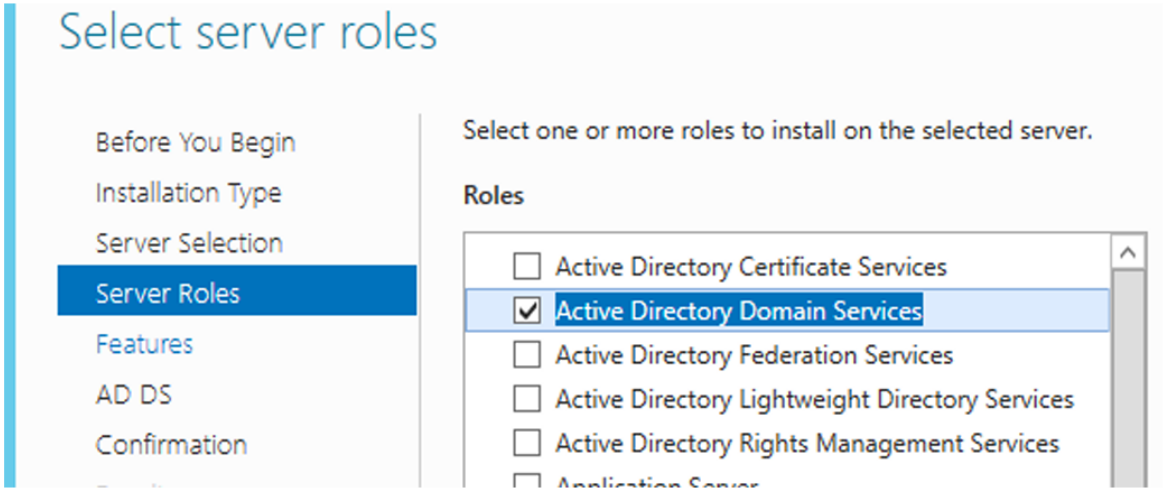
- Make sure that ping is possible between SRV – DC and from SRV – Client

1.6. Execute on DC server

1.6.1. Upgrade Win 2012 to Domain Controller (DC)

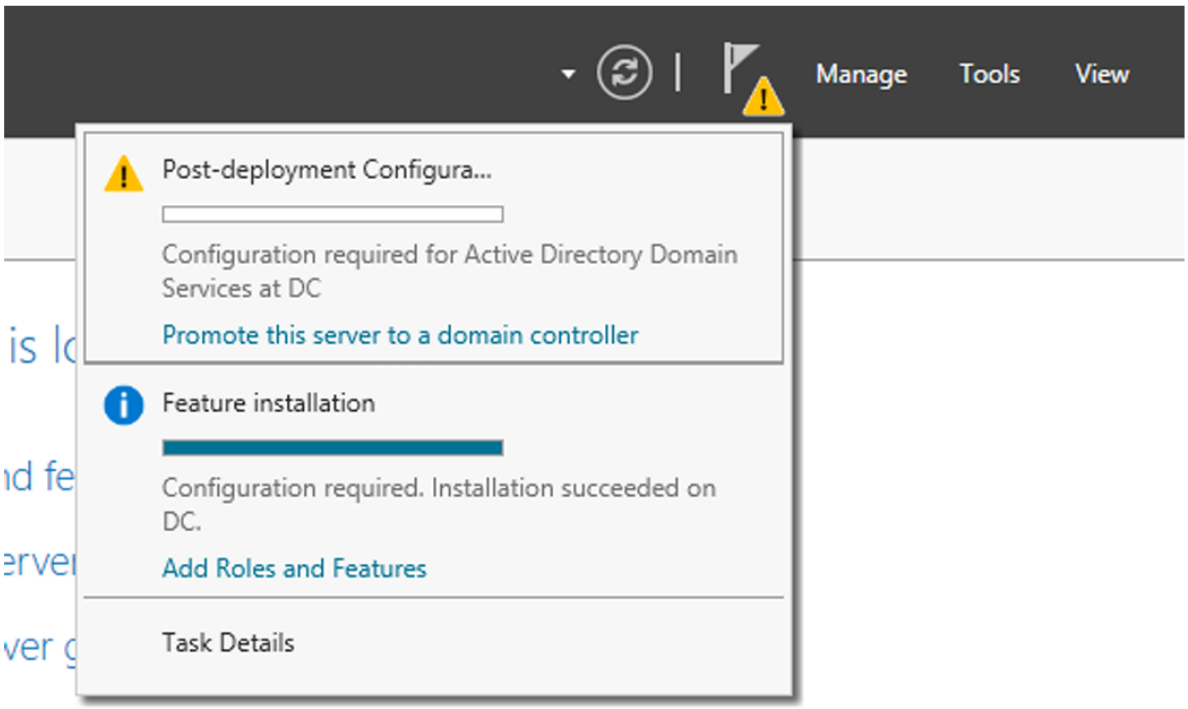
- Access by following the path: Server Manager → Manage → Add Roles and Feature.

- Select Next by default to the Server Roles window, select Active Directory Domain Services



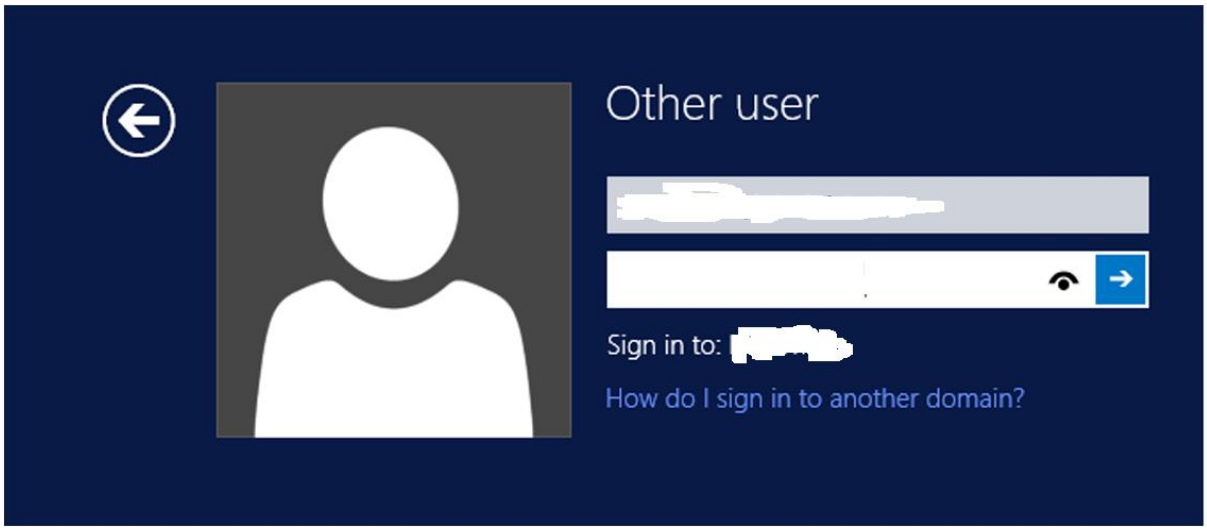
- Continue Next by default and select Install to install.

- After the installation process is complete, select Promote this server to a domain controller



- Select Add a new forest. In the Root domain name section, enter the domain name.

- Continue to select Next by default and Install to upgrade to DC. The DC server will automatically restart after the upgrade is complete. The login account will now be in the form DOMAIN\user as shown below.

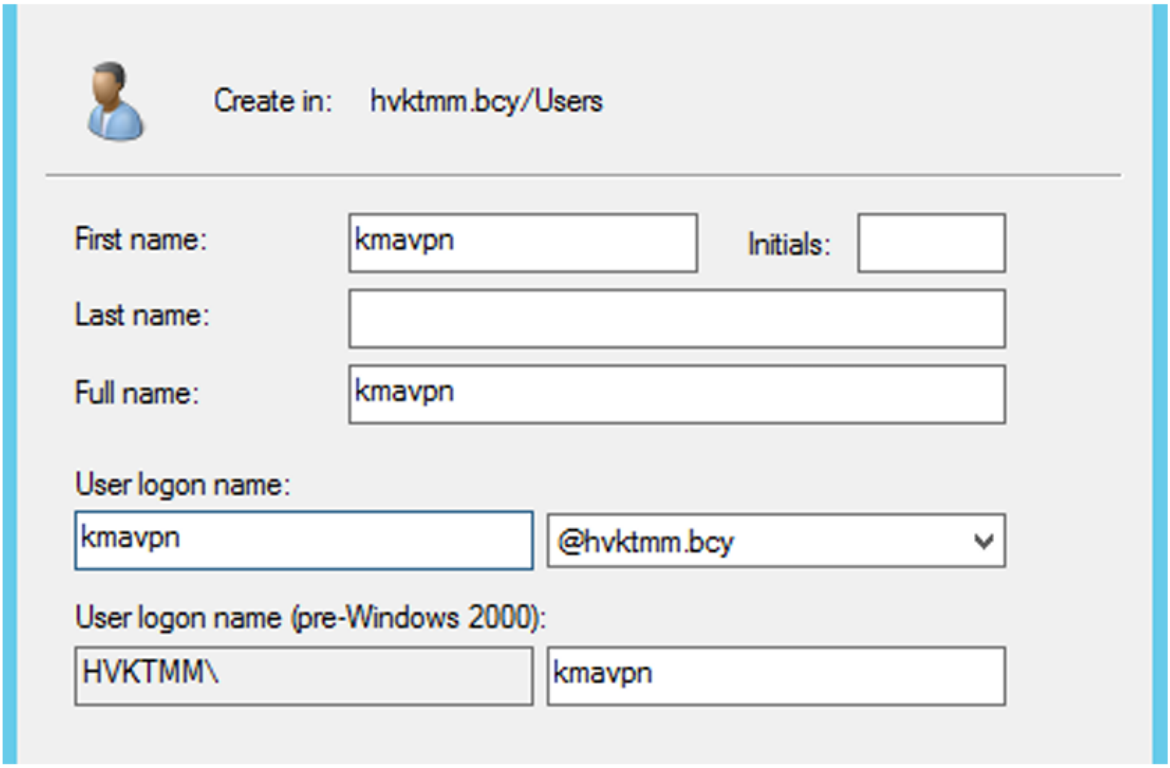


1.6.2. Create a user that allows remote access via VPN

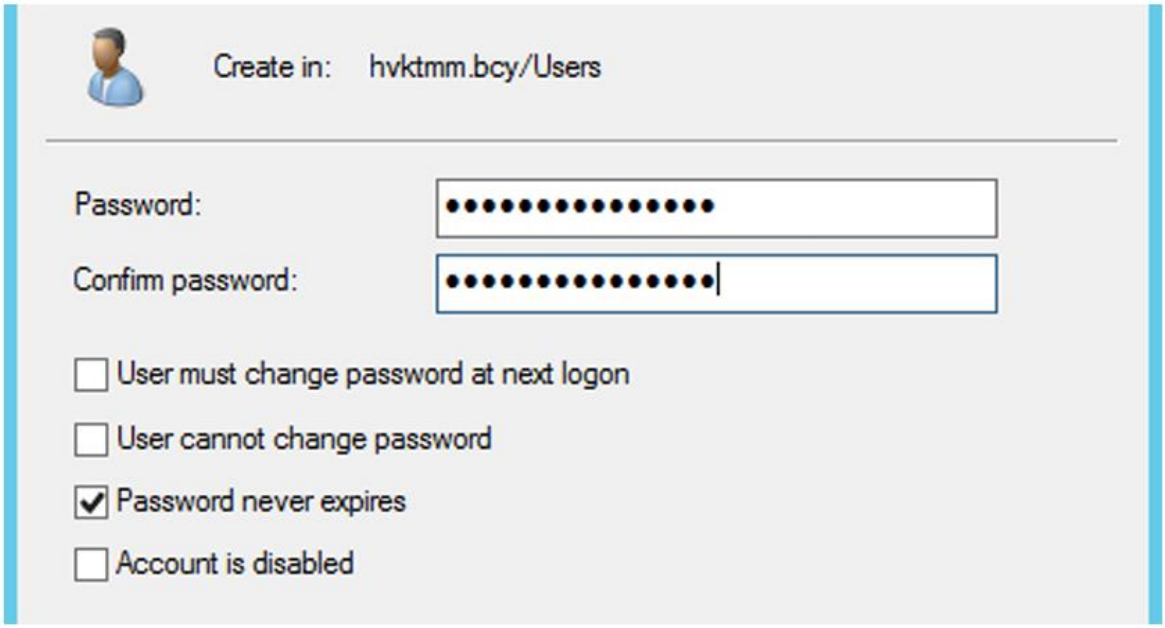
- Access the path: Server Manager → Tools → Active Directory User and Computer.

- Right click on the Users → New → User.

- Set the username for remote access as: vpn



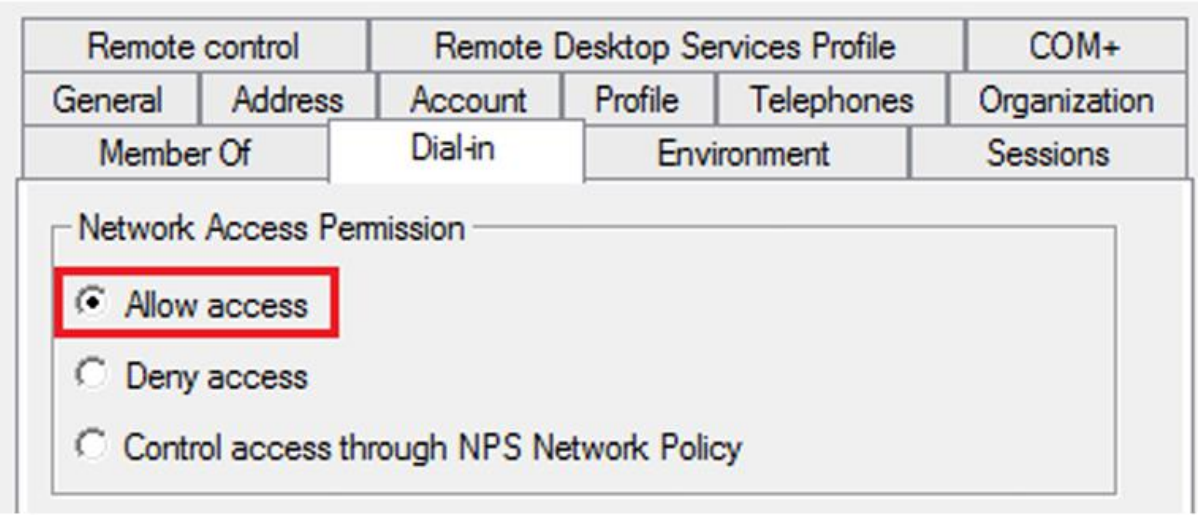
- The next interface sets the password for the user. Note that the password here must be complex



- Click Next and Finish to complete the user creation process.

- The next step is to configure this user to be allowed access from distant.

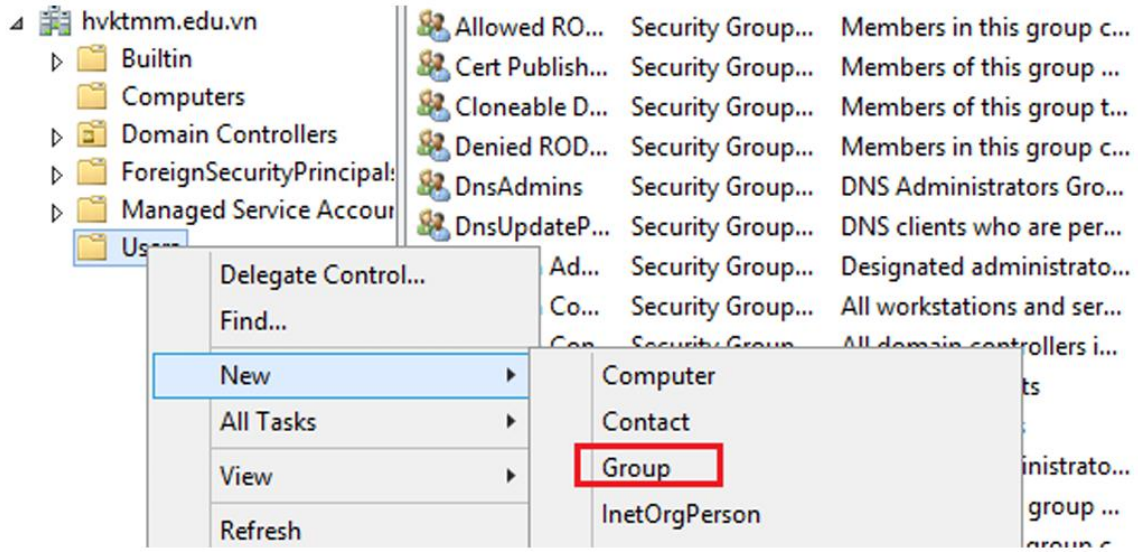
- Right click on the user, select Properties, select the Tab Dial-in →



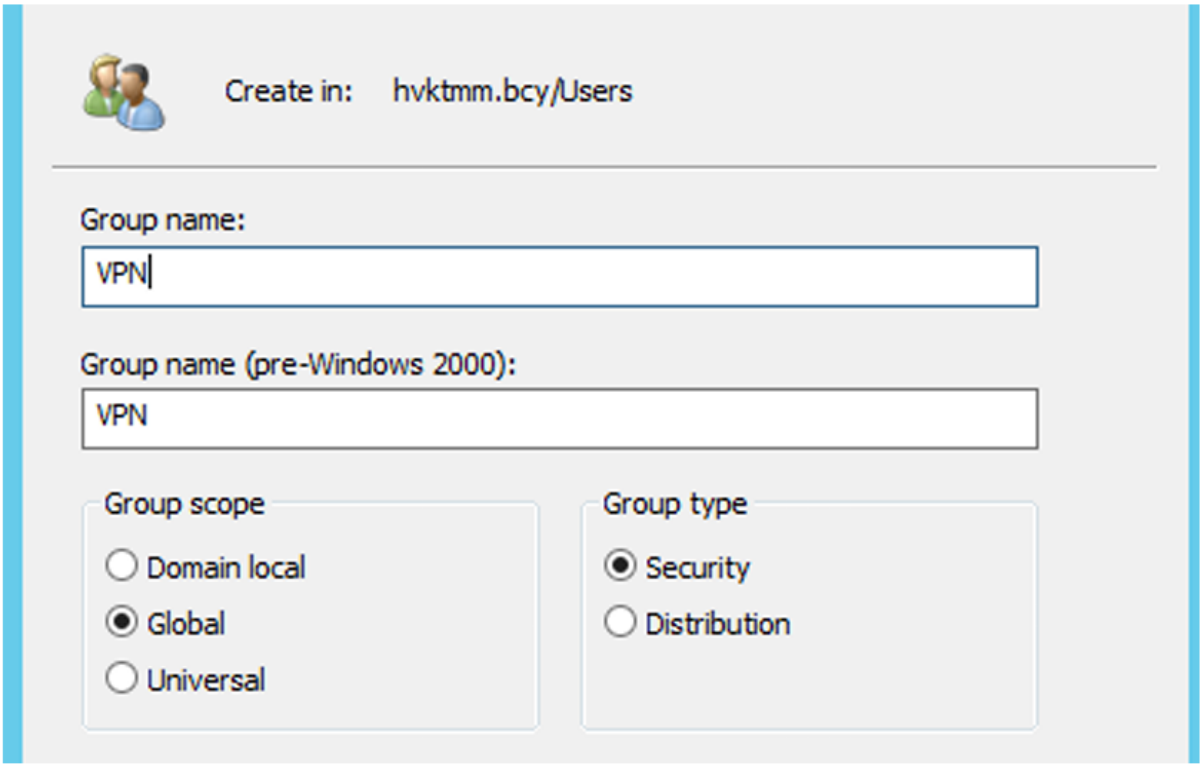
Allow access.

- Click Apply → OK to finish.

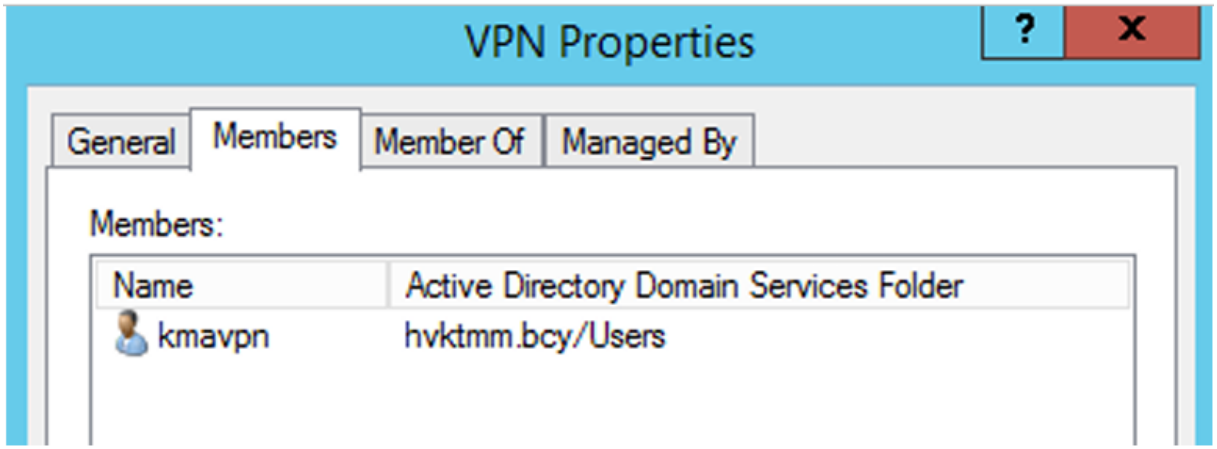
- Create a VPN group and add this user to the group.



- Name the group is VPN



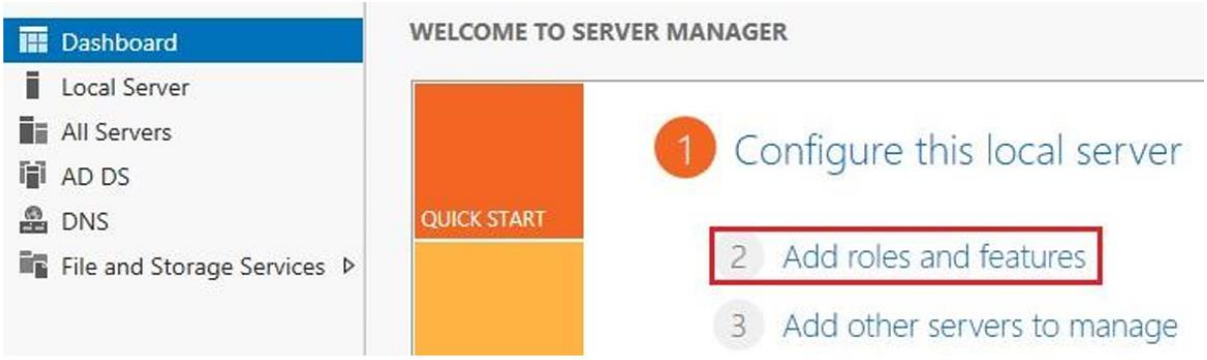
- Add user to VPN group



- Finish the step of creating remote access user.

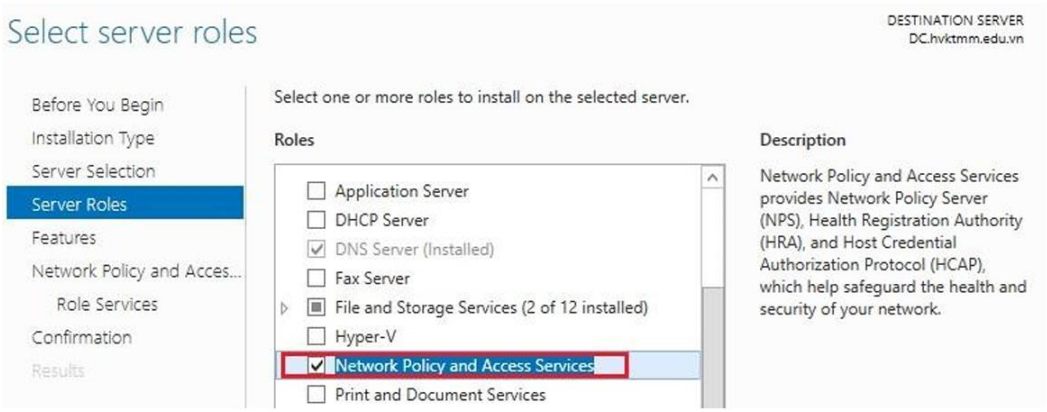
1.6.3. Install Network Policy Server service

- Access the path: Server Manager → Dashboard → Add roles and features



- Leave the three first steps as default and select Next.

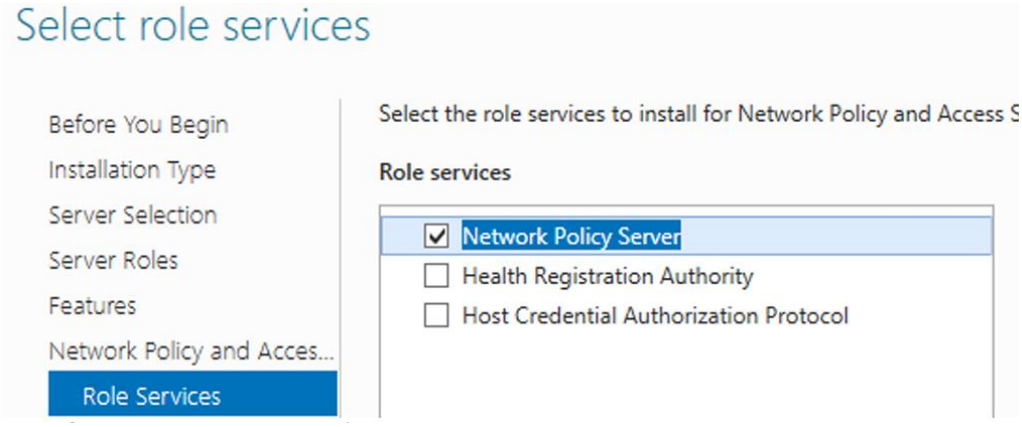
- At the role selection step (Select server roles): Select Network Policy and Access Services:



- Select Next to continue.

- Leave the next options as default.

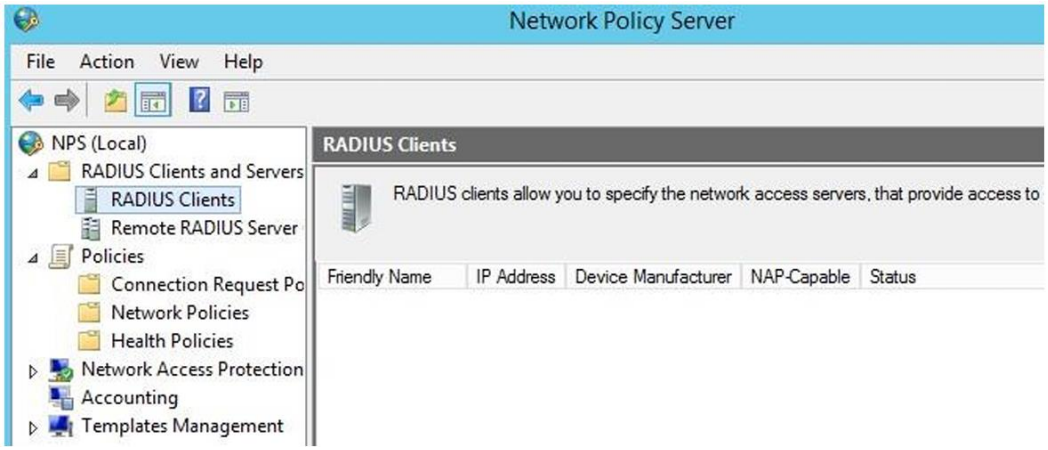
- Service selection interface select: Network Policy Server.



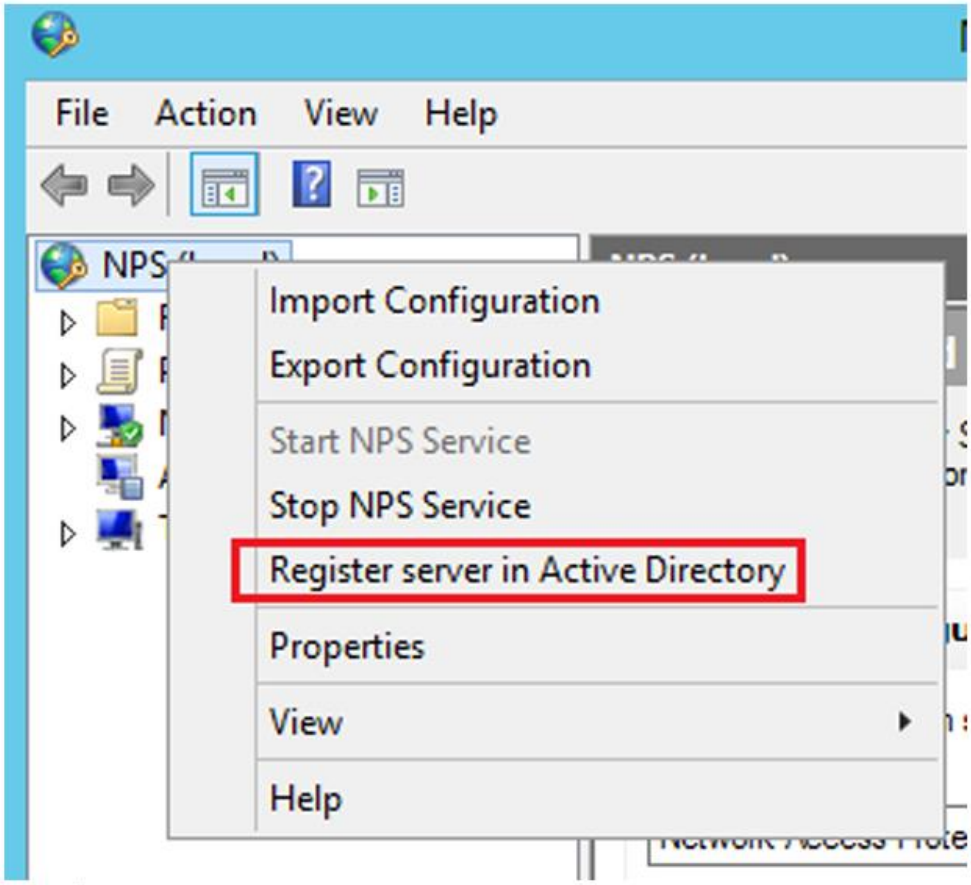
- Click Next and Install to install the service.

1.6.4. Configure Radius Server in Network Policy Server

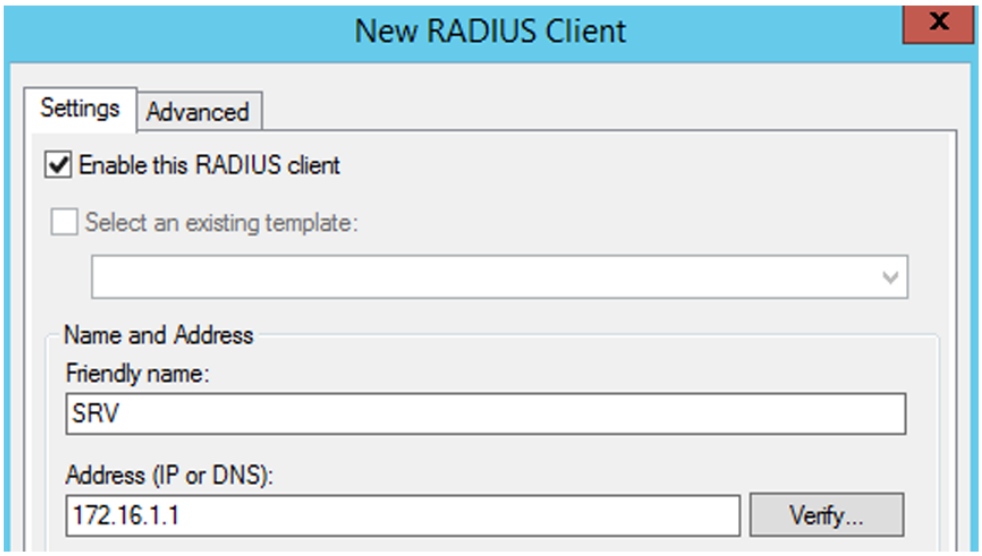
- Access Network Policy Server via the path: Server Manager → Tools → Network Policy Server



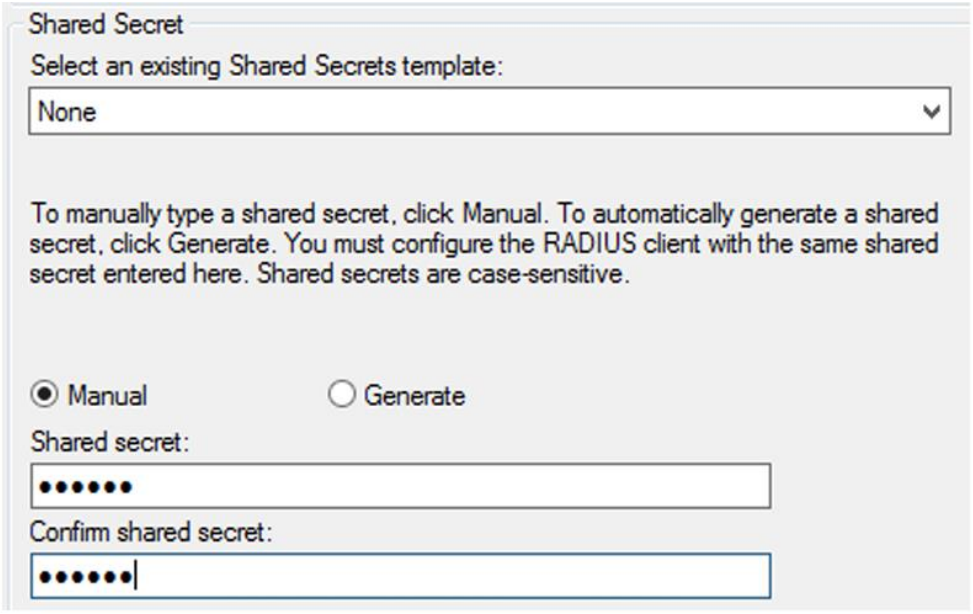
- Register the service in Active Directory:



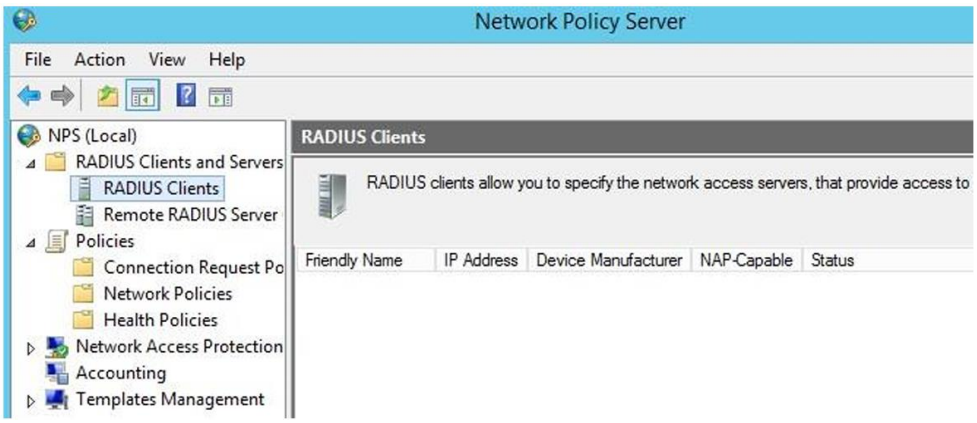
- Configure the Radius Client machine definition as the SRV machine.



- Shared Secret section: Secret key shared between 2 machines. Secret key This 2 machines must enter the same.

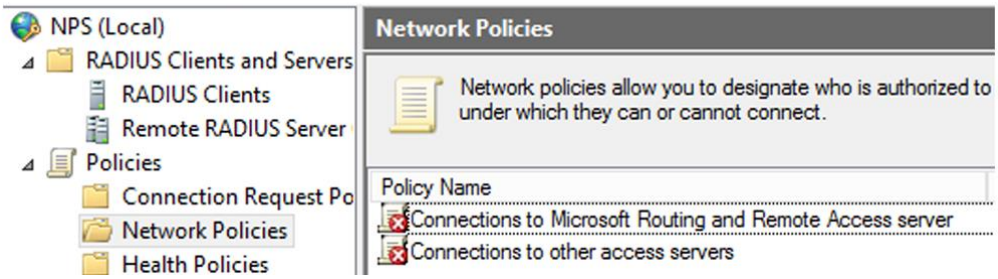


- Select OK to finish.



- Next we need to define the authentication policy.

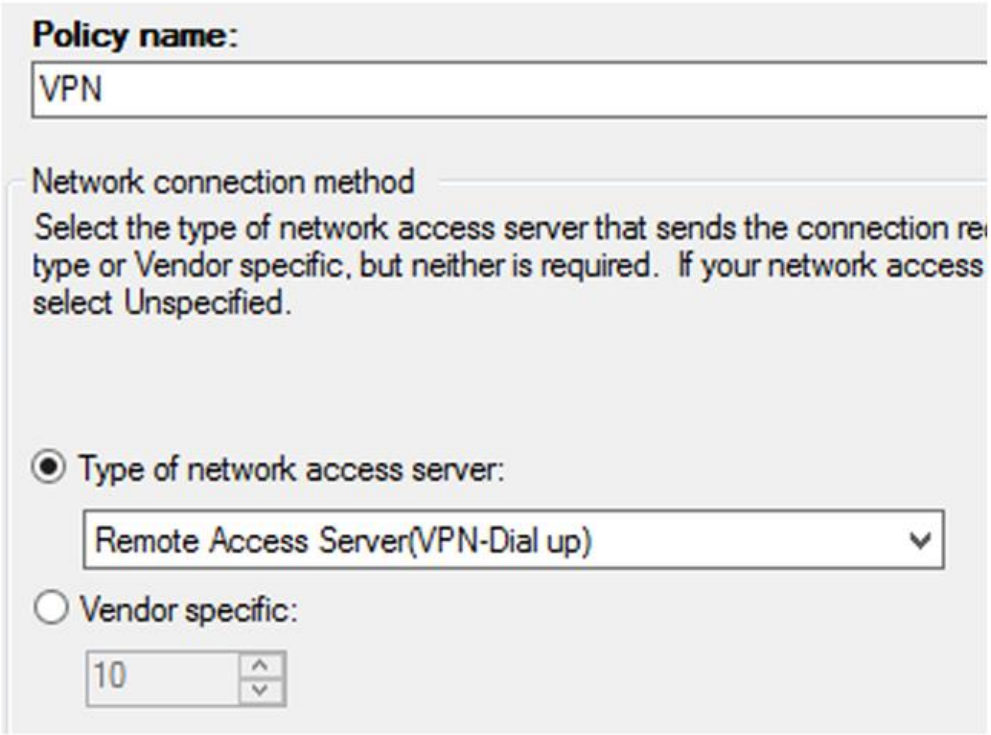
- Go to Policies → Network Policies. The interface is as follows:



- Delete the 2 existing default policies. And create a new policy.

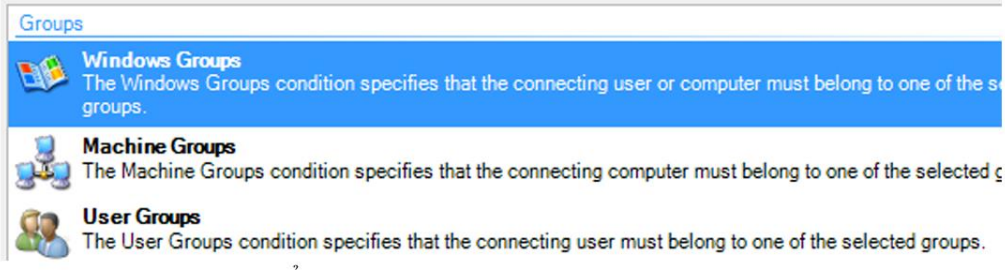
- The Policy name item is named VPN.

- Type of network access server: select Remote Access Server



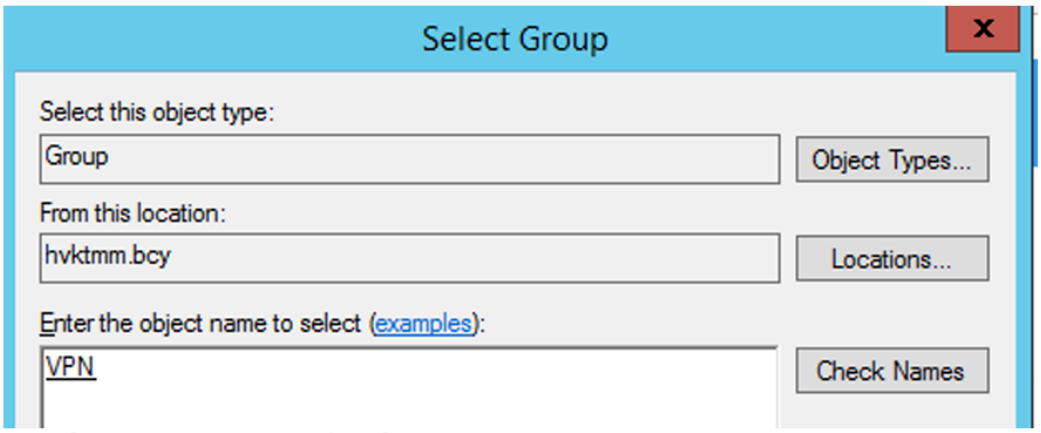
- Select Next to continue.

- Conditions section: Select Add to add: Export interface Now select Windows Groups:

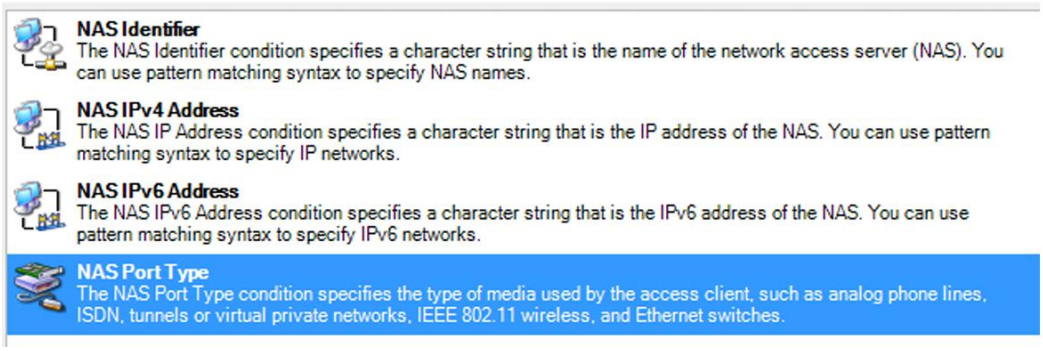


- Select Add Group to add a group:

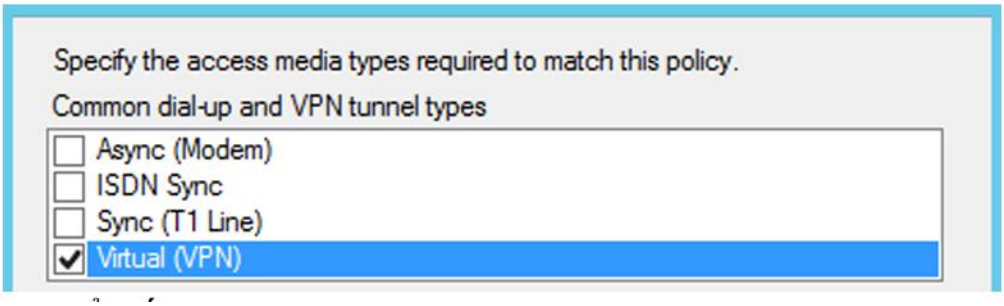
- Point the VPN group created in the step above:



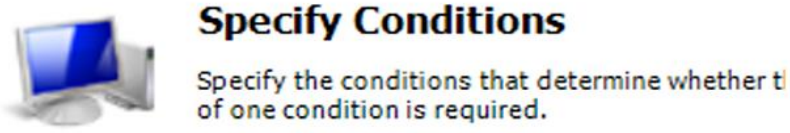
- Still in the Conditions interface, continue to select Add to add another condition. The select condition interface appears, find and select NAS PortType:

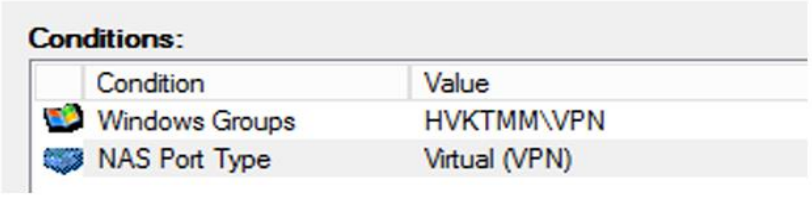


- Add VPN

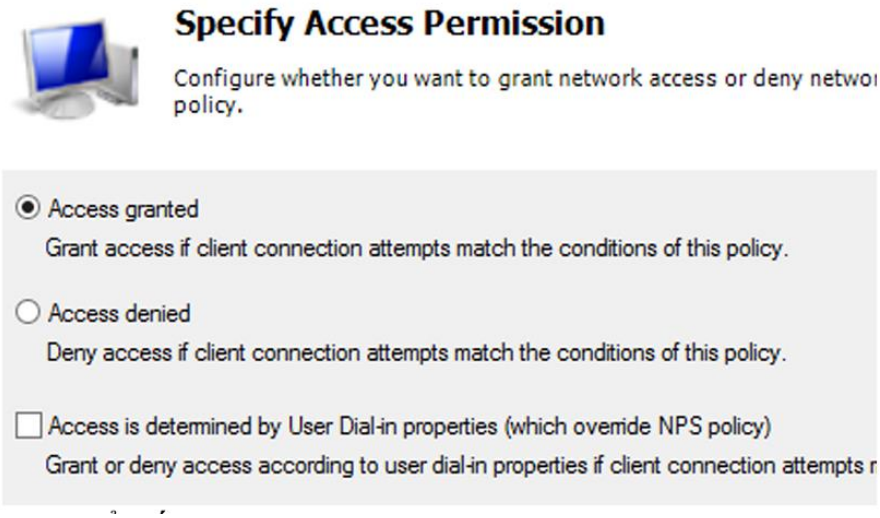


- Now the main interface will have 2 conditions defined.



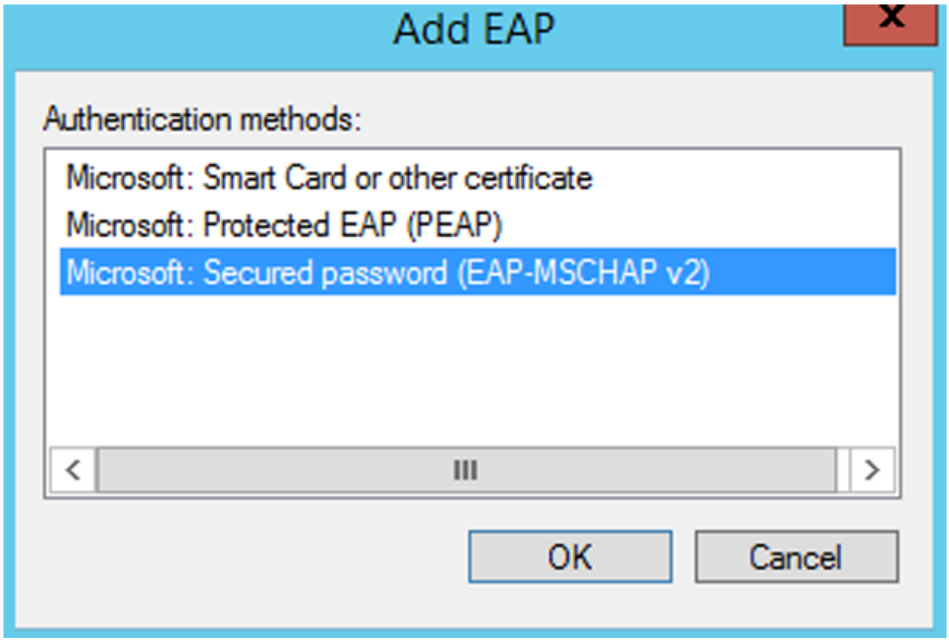


- Next interface select access rights: select Access granted

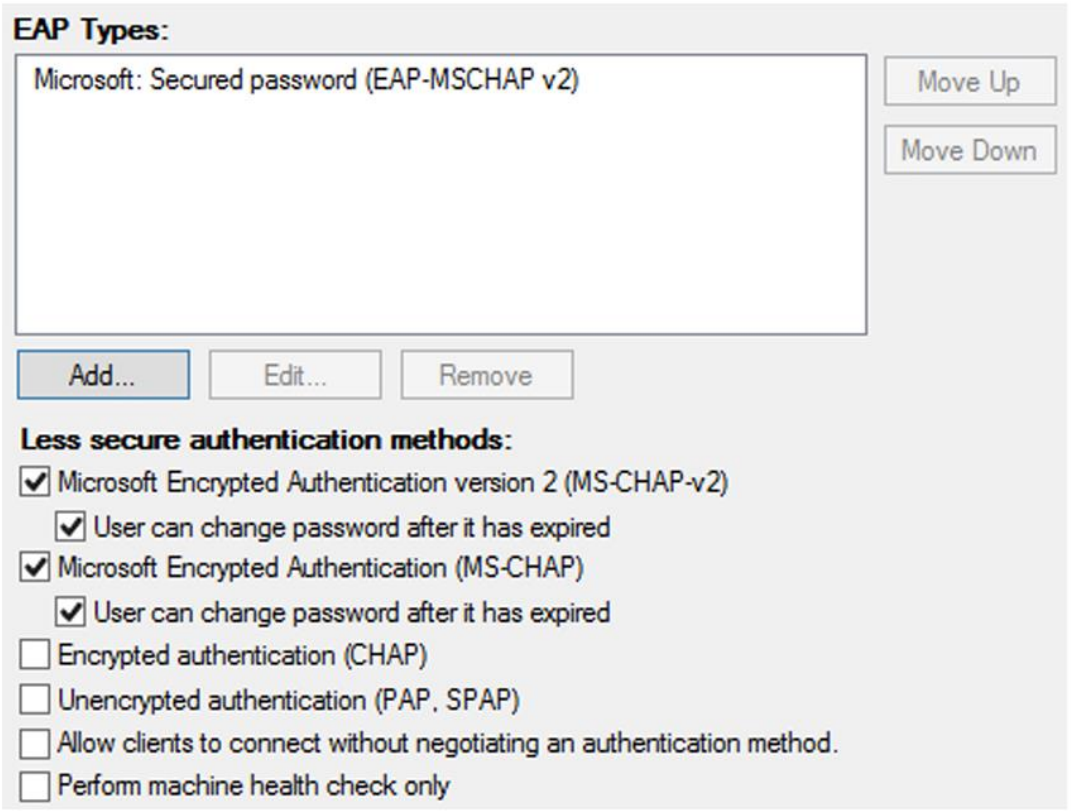


- Next interface select authentication protocol.

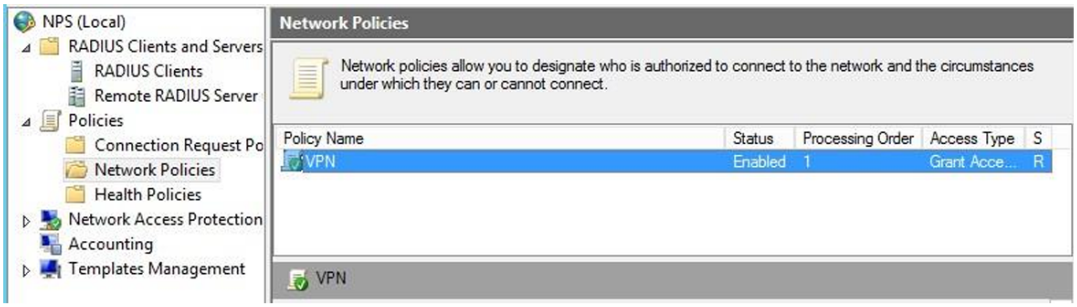
- In the EAP type section, select Add: The interface appears, select Secured password:



- Interface after configuration.

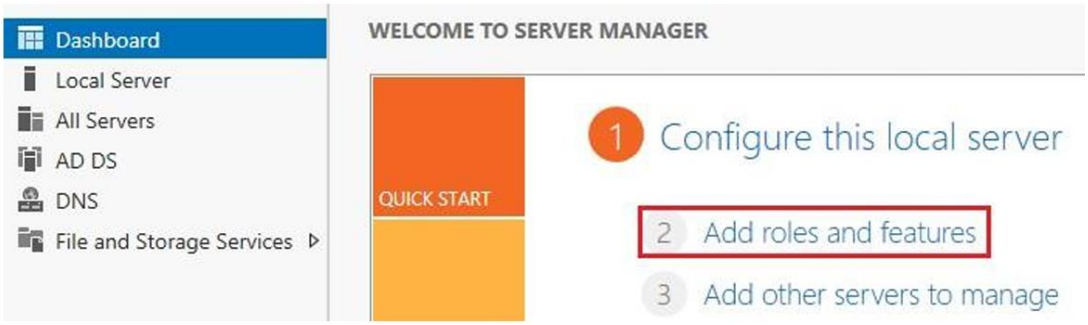


- Leave the interfaces as default. Select Finish to finish.



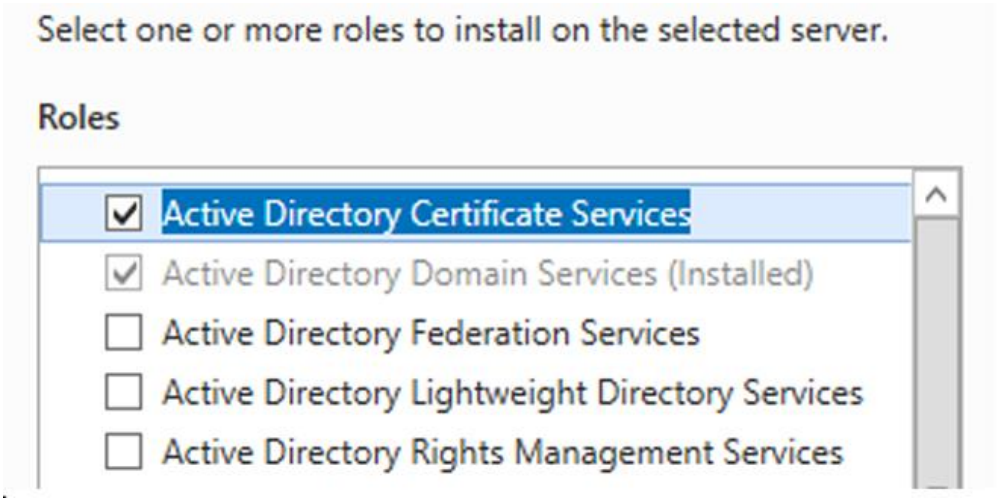
1.6.5. Install CA authentication center service.

- Access by following the path: Server Manager → Dashboard → Add roles and features



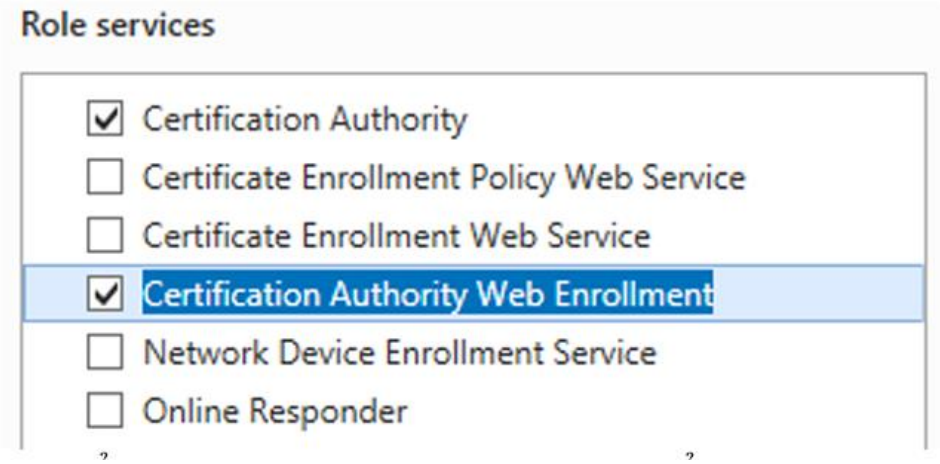
- Leave the three first steps as default and select Next.

- At the role selection step (Select server roles): Select Active Directory Certificate Services.



- Next steps select Next.

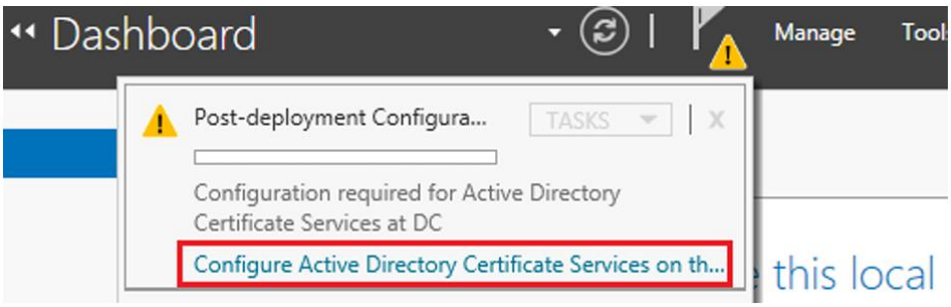
- Go to Select roles services interface: Check 2 options as shown below.



Next steps leave default and select Install to install.

1.6.6. Configure CA to issue digital certificates for SRV server

- After installing the service in the Dashboard interface. In the upper corner next to the flag there is a warning section. In this warning section the system requires CA configuration:

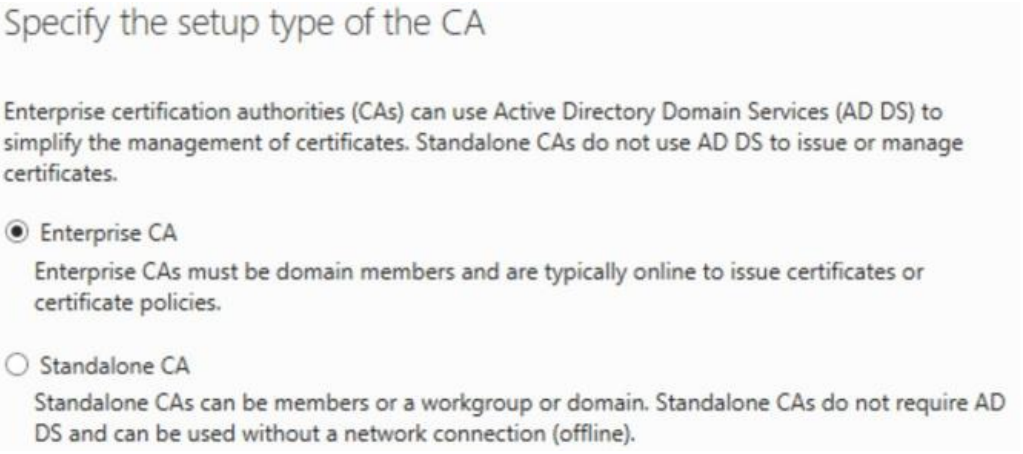


- The CA configuration interface appears

- Select Next to continue.

- Next interface select 2 options as shown below:

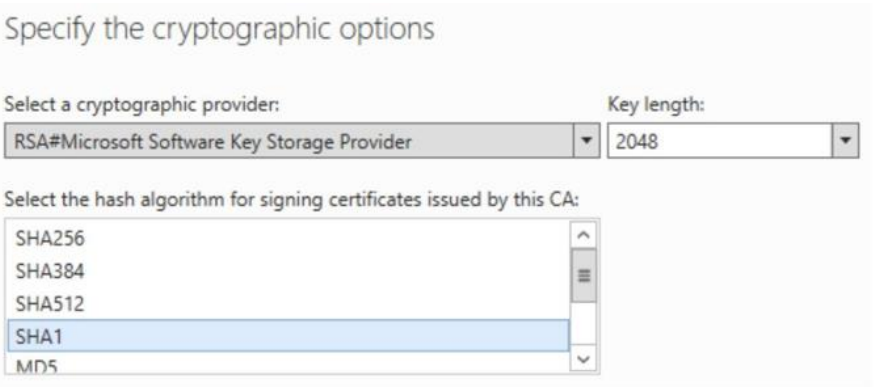
- Next interface select Enterprise CA:



- Select Next to continue:

- Select CA Type: Root CA

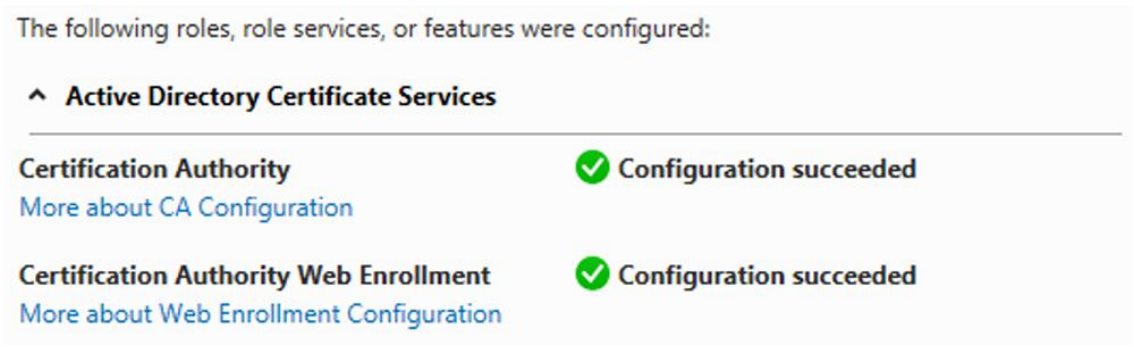
- Private key section: Select Create a new private key Select.



- The next interface names the CA:

- Default time is 5 years.

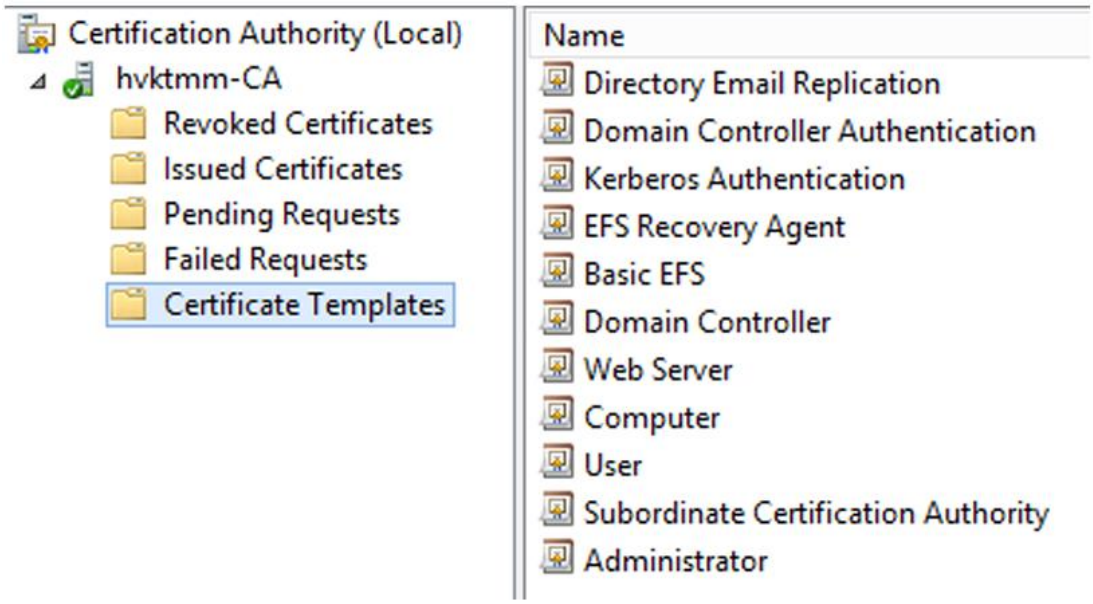
- Leave the next interfaces as default, select Configure to configure CA. Configuration complete:



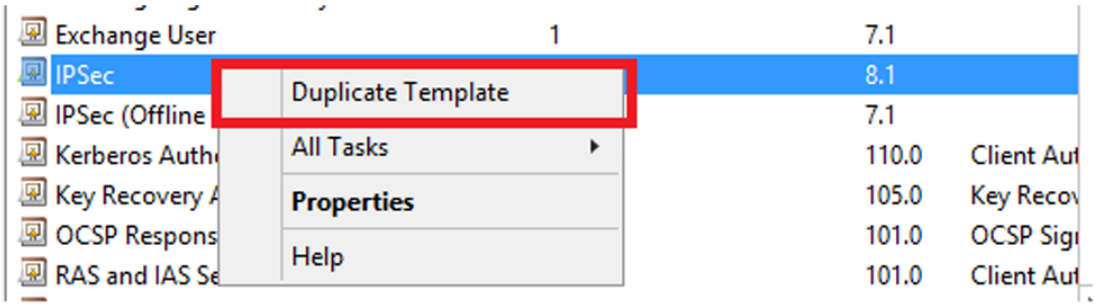
- Click Close to close the configuration completion window

1.6.7. Create Templates

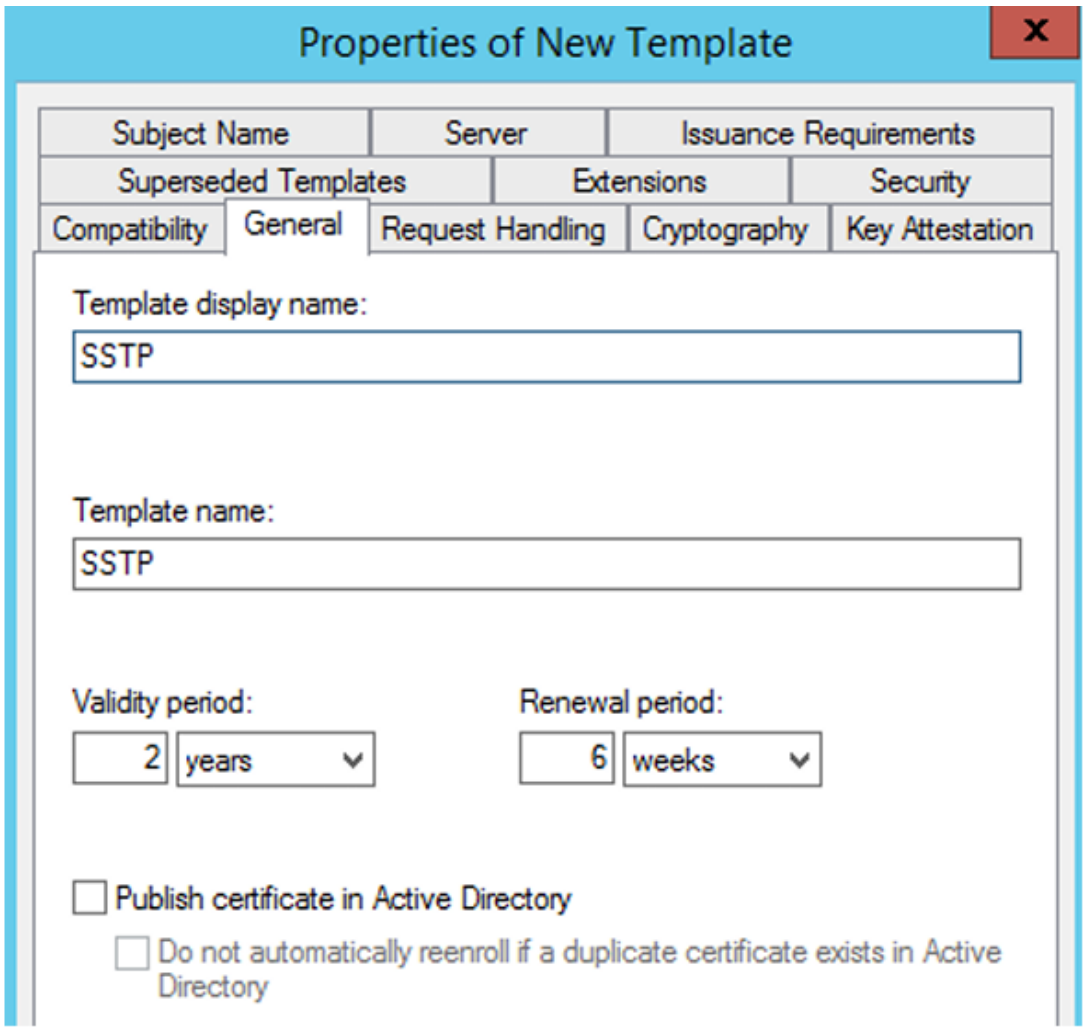
- Access the path to open the CA management interface: Server Manager → Tools → Certification Authority → Certificate Templates



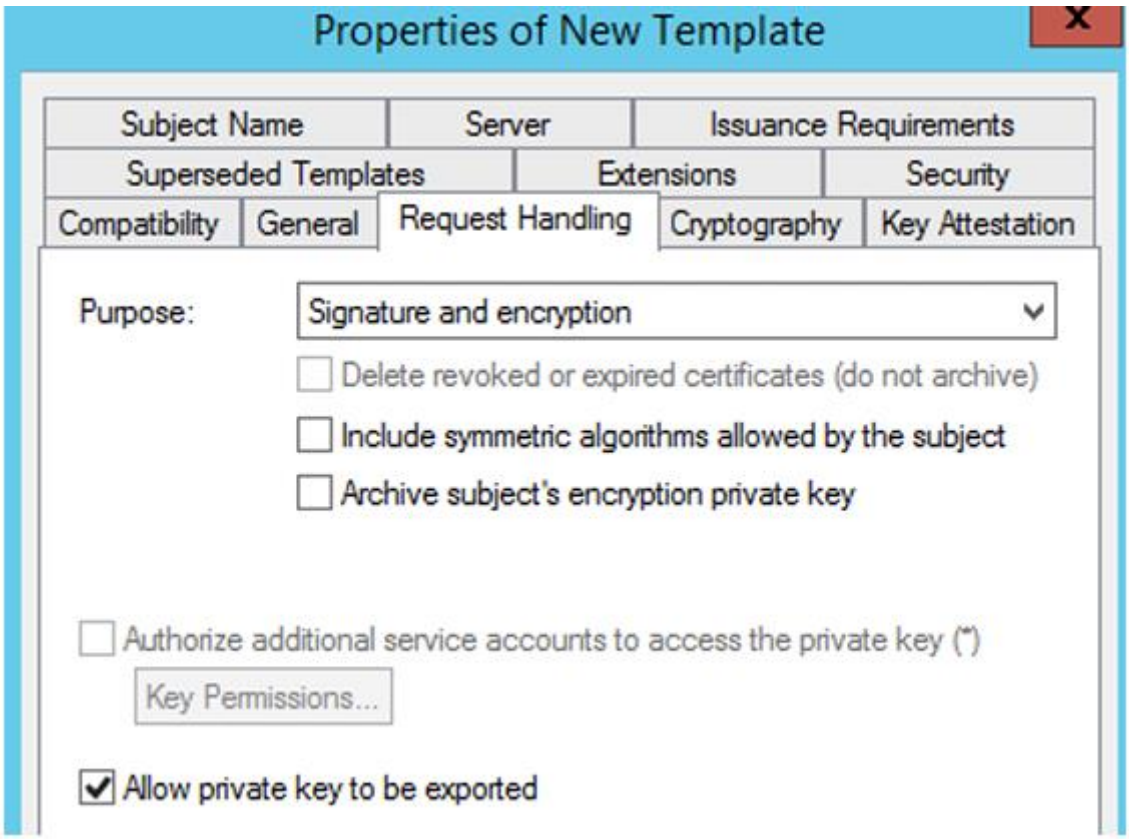
- Right click on Certificate Templates → Manage. Go to template for IPSec. Right click and select Duplicate Template



- In the new window that appears, select the General tab. In the Template display name section, change it to SSTP:

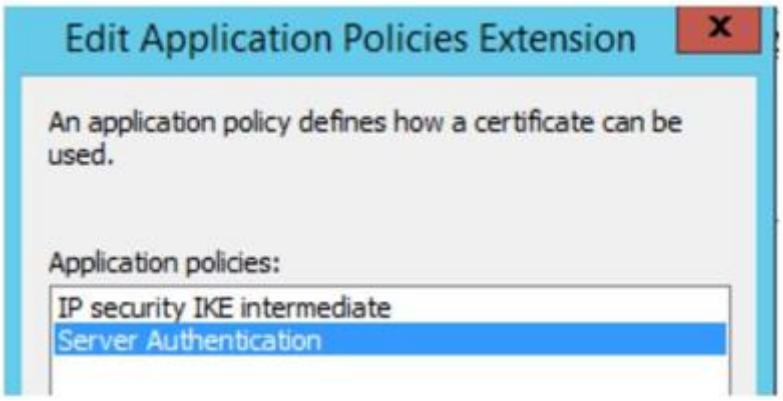


- In the Request Handling tab select Allow private key to be exported:



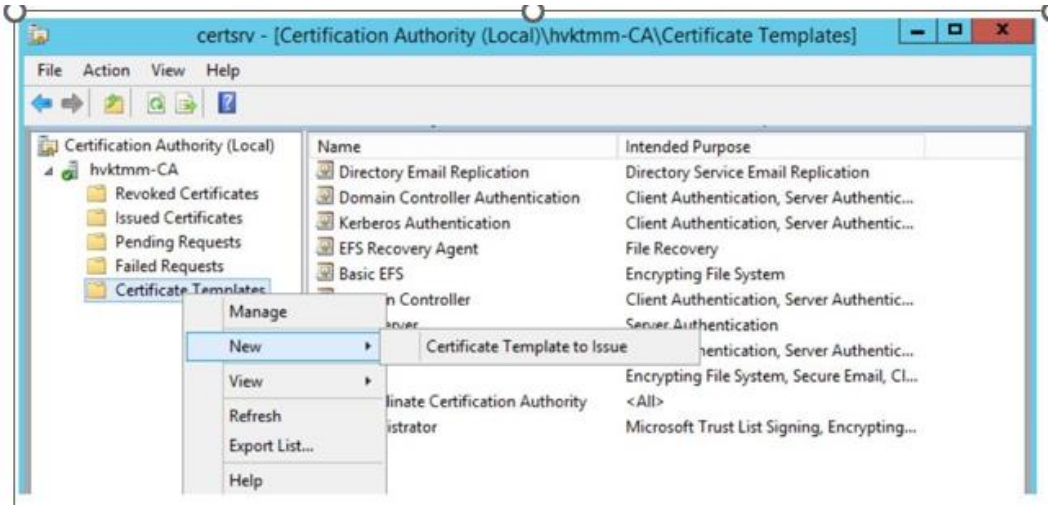
- Subject Name tab select Supply in the request

- Tab Extensions select Edit → Add then select Server Authentication



- Then Apply → OK to complete the process of creating new Templates

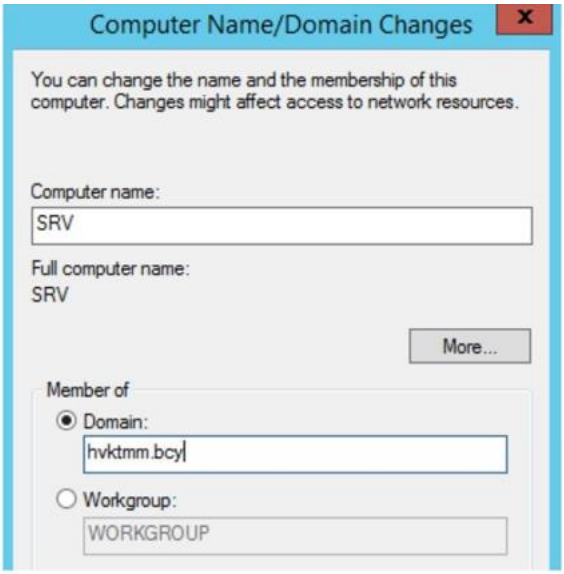
- Then, right click on Certificate Templates → New → Certificate Template to Issue:



1.7. Execute on SRV server

1.7.1. Join SRV server to DC

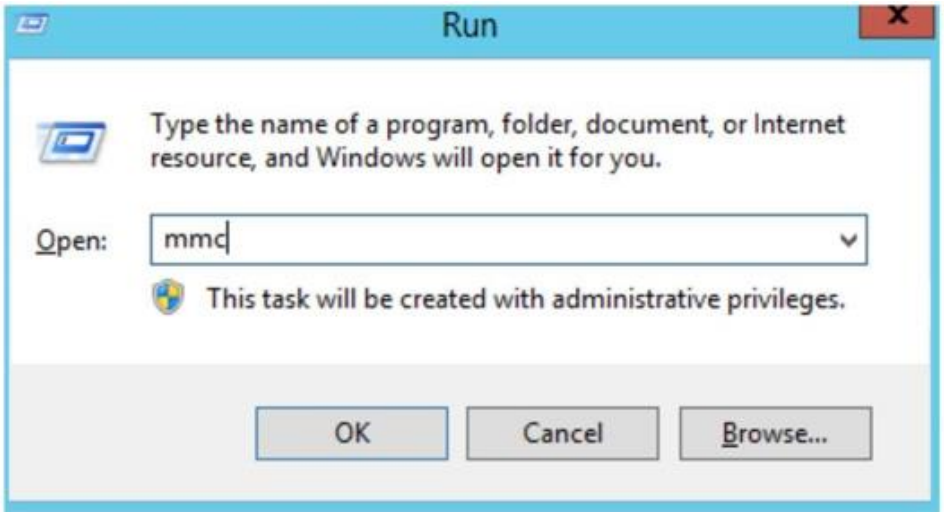
- Perform SRV join to DC:



- After successfully joining, the SRV machine will automatically restart and the login screen will be similar to the DC side.

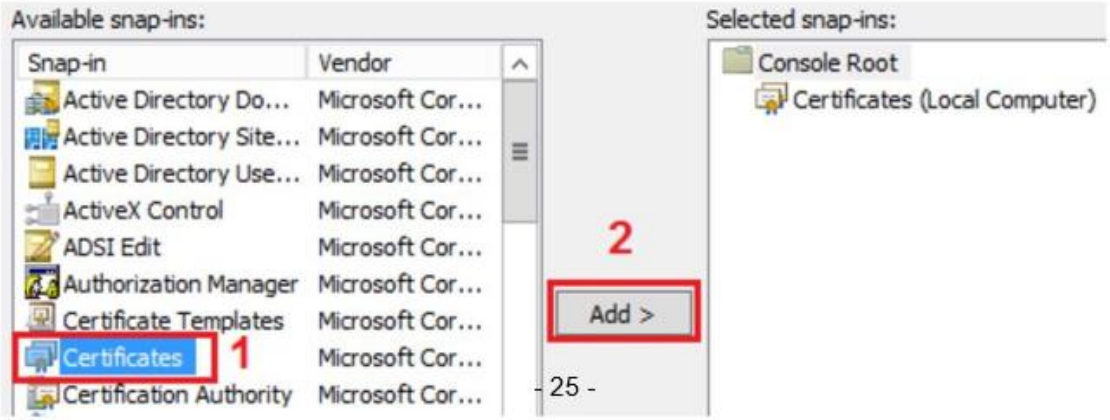
1.7.2. Request for digital certificate issuance

- Turn on the MMC program from Run:

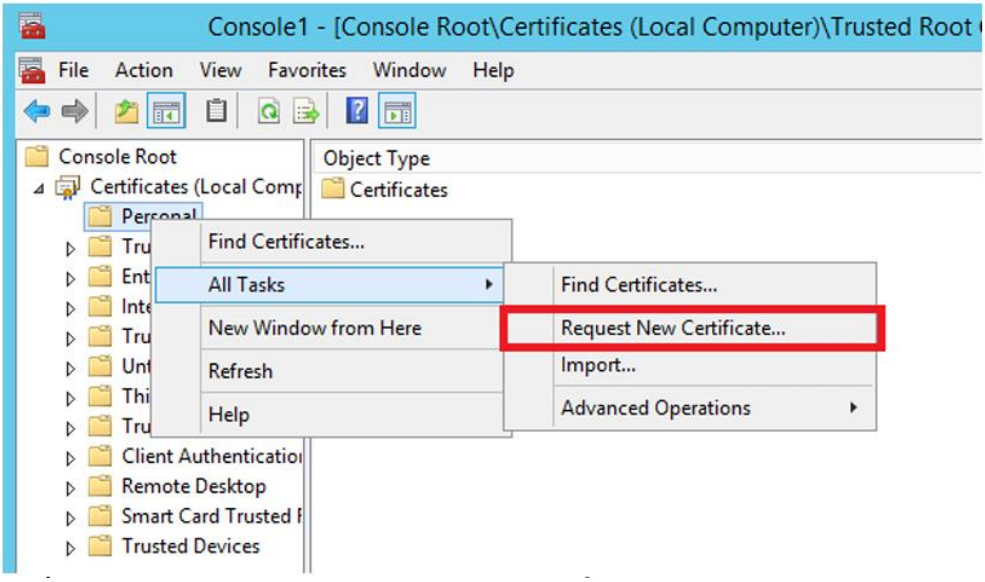


- In the window that appears to select File → Add or Remove snap-in

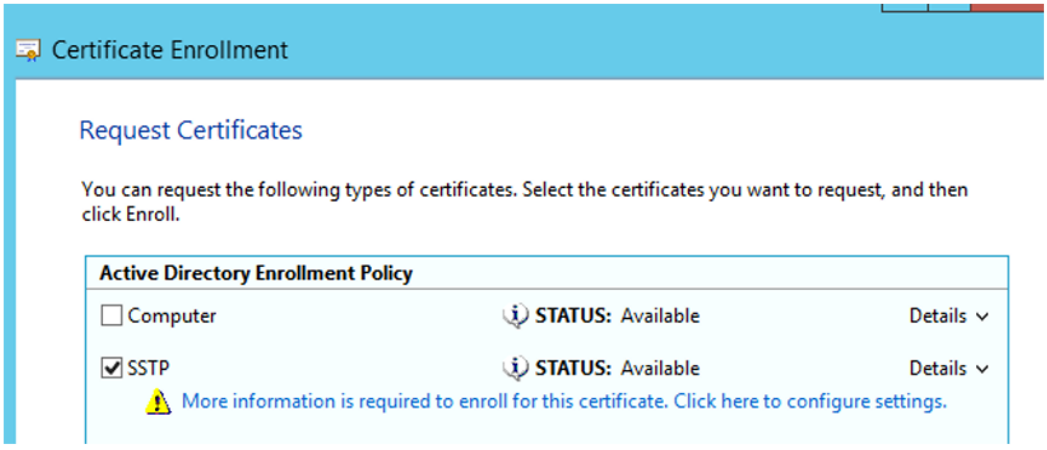
- In the window appears, select as shown below:



- In the digital certificate format selection window, select Personal →All Tasks → Request New Certificate:

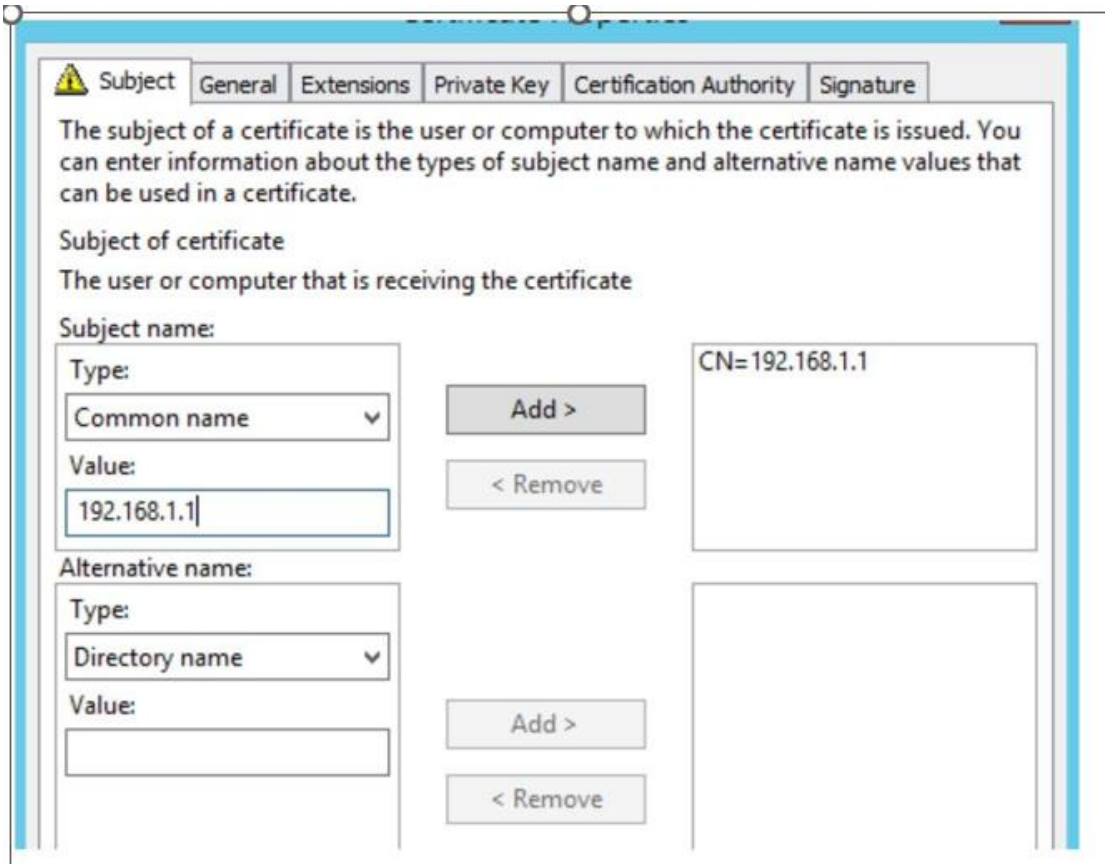


- Continue to select Next by default, in the Request Certificates window select SSTP and click on the yellow warning icon.

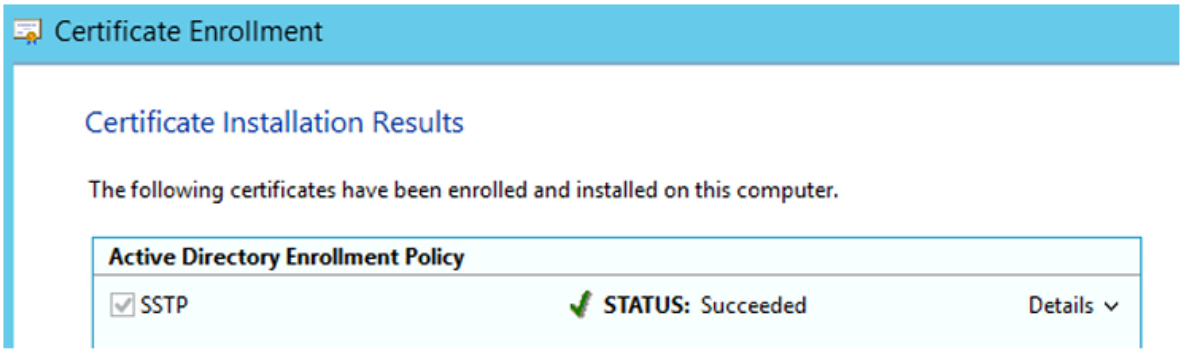


- Select Common name in the Type section

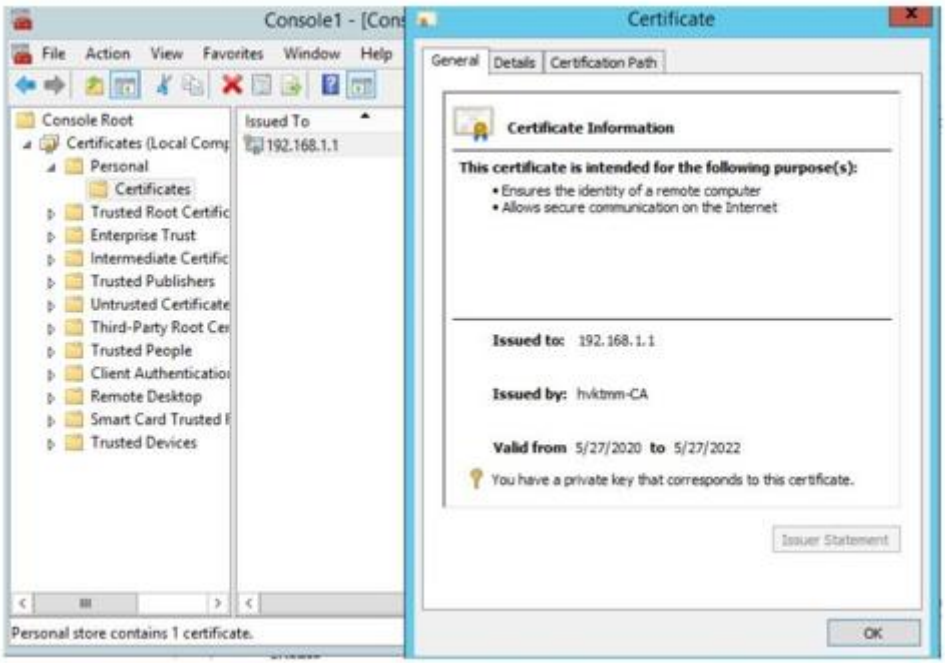
- In the Value field, enter the IP as the external interface of the SRV server. Select Add to agree.



- Select Apply → OK. Select Enroll to request a digital certificate. Select Finish to complete the process.



- Check the newly issued digital certificate



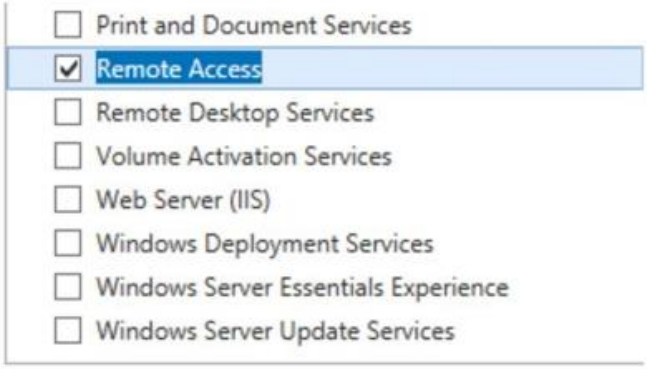
1.7.3. Install Routing and Remote Access application

- On the first SRV server, the Routing and Remote access management application must be installed.

- Access by following the path: Server Manager → Dashboard → Add roles and features.

- Leave the first three steps as default and select Next.

- Go to Select server roles interface: Select Remote Access

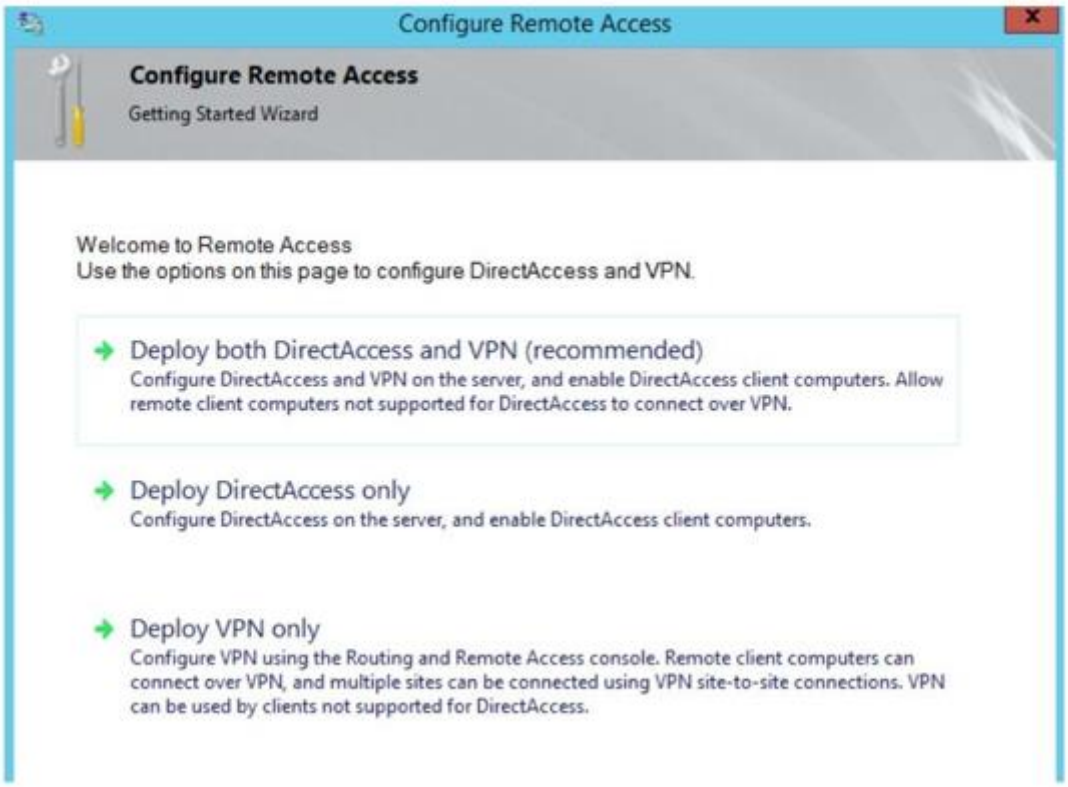


- Select role service interface: Select 2 options as shown below:

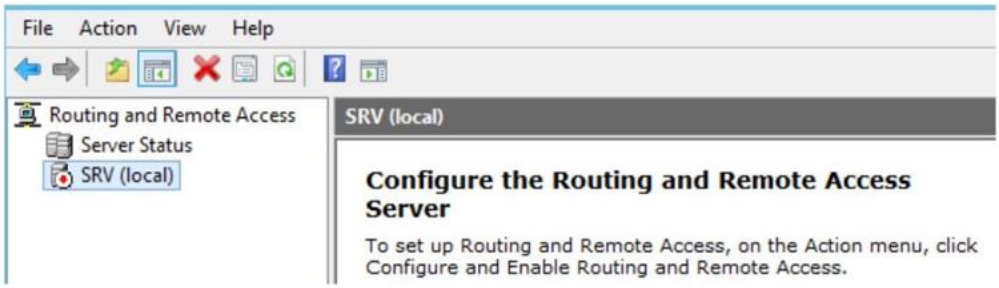
- Next steps select Next and Install to install

1.7.4. Configuring Routing and Remote Access services

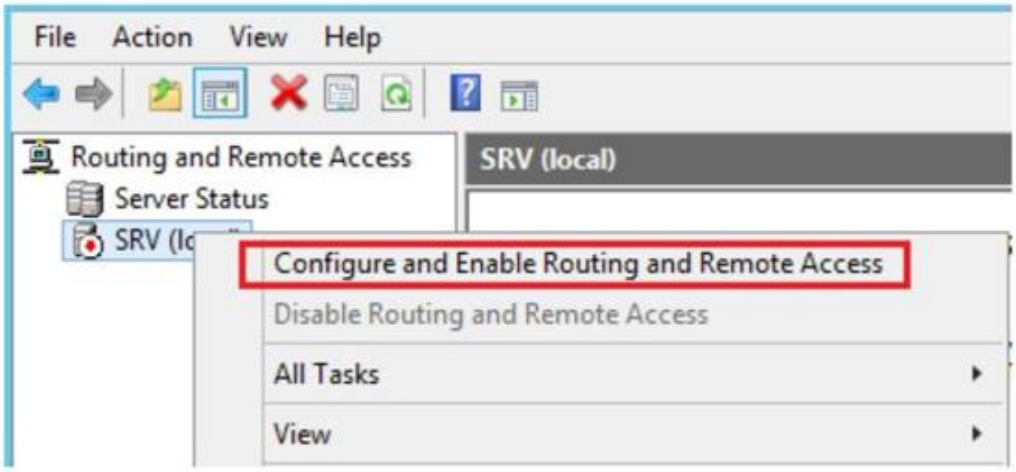
- Access by following the path: Server Manager → Tools → Routing and Remote Access. Select Deploy VPN only.



- The configuration window appears:

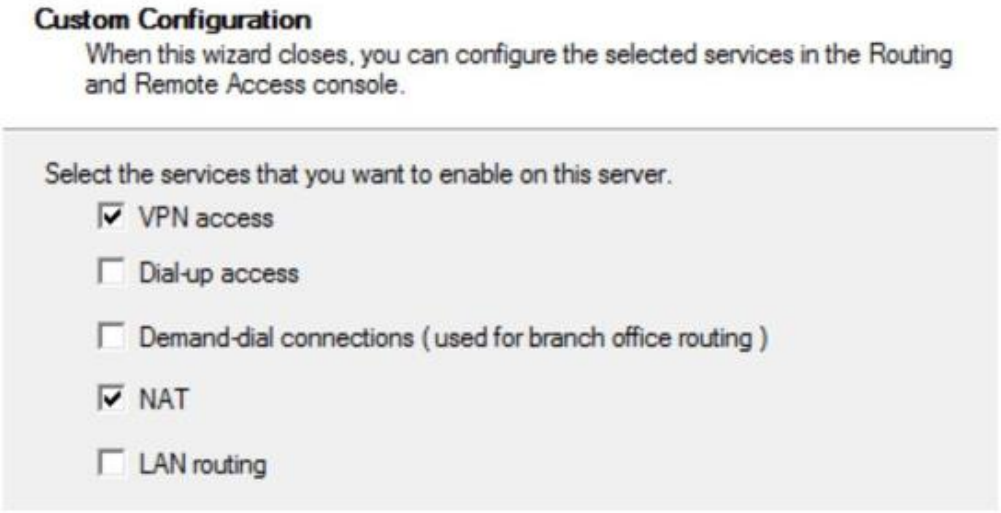


- Right click on SRV Server and select Configure and Enable Routing:

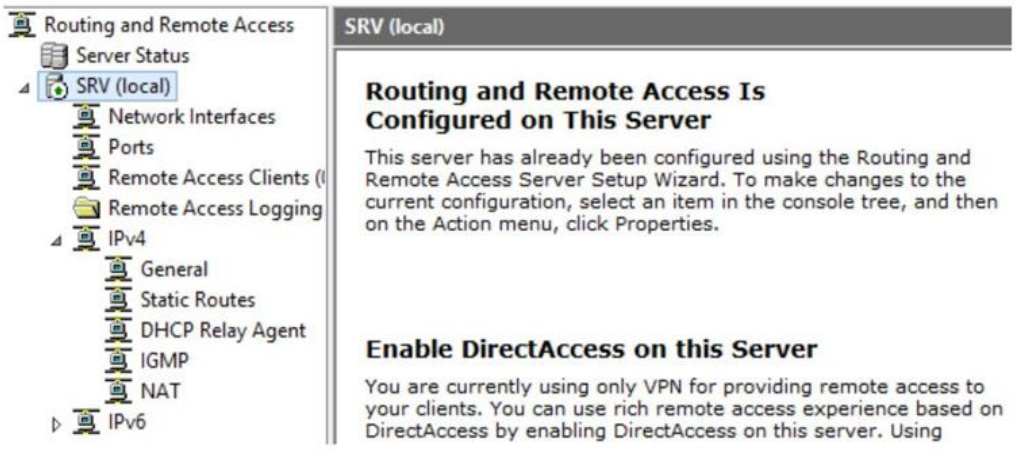


- The interface appears, select Next.

- Next interface select usage method: select Custom Configure Next interface check 2 options as shown below select VPN and NAT functions.

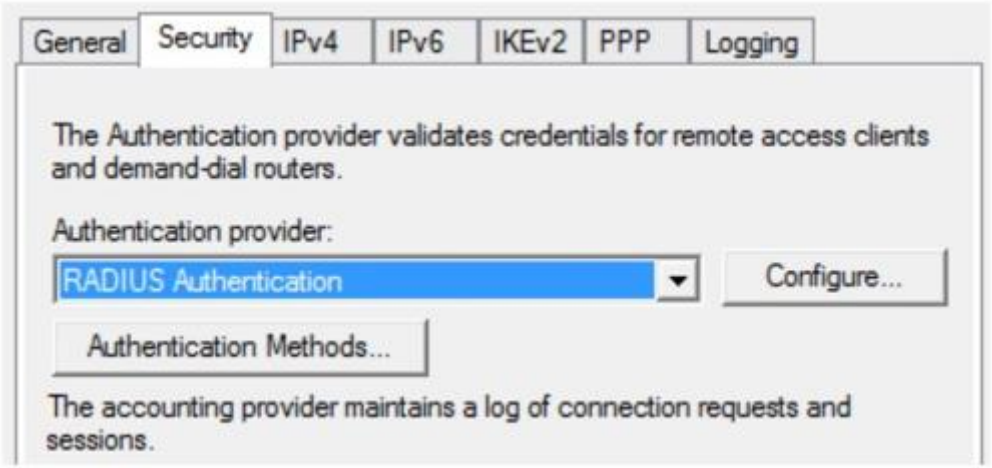


- Select Next and Finish to finish. Interface after installation.



- Right click on the SRV server name and select Properties.

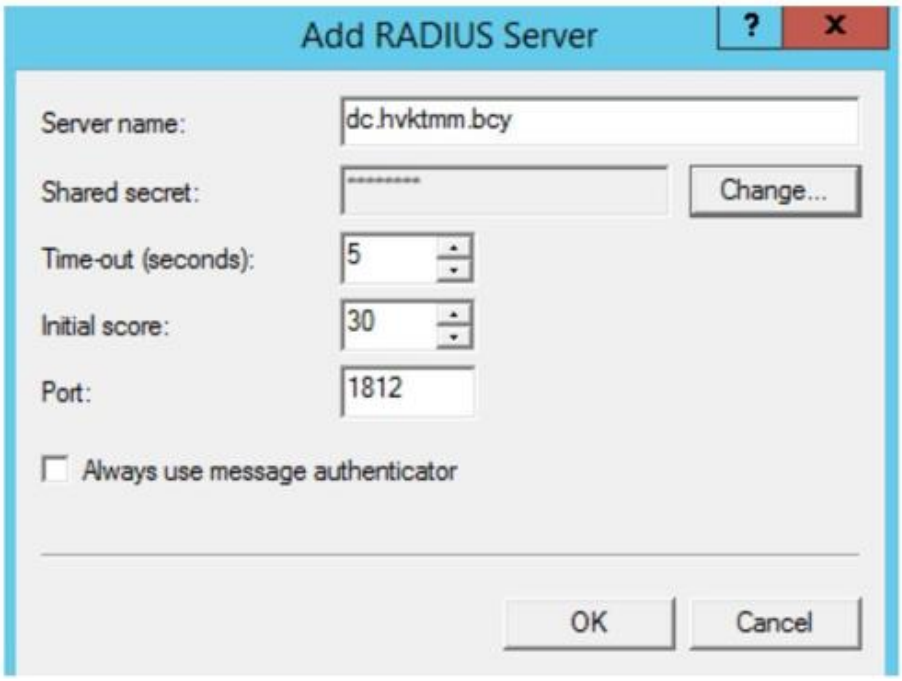
- In the Security tab, select RADIUS authentication method. Next, select Configure.



- The window appears, select Add.

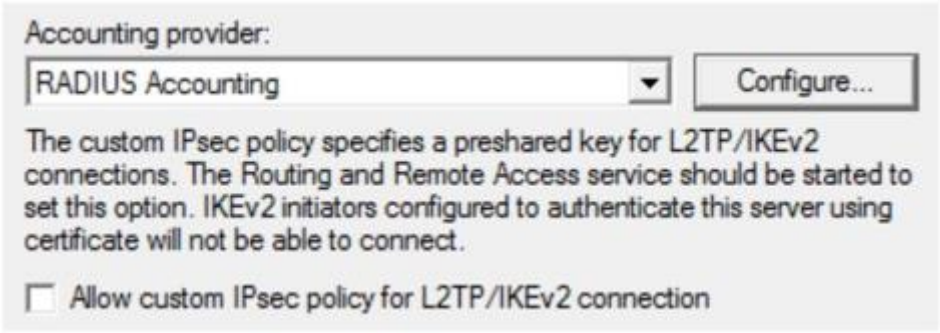
- Server name: enter the name and domain of the DC server.

- Shared secret: Enter the shared key set up in Radius DC.



- Click OK to close the window.

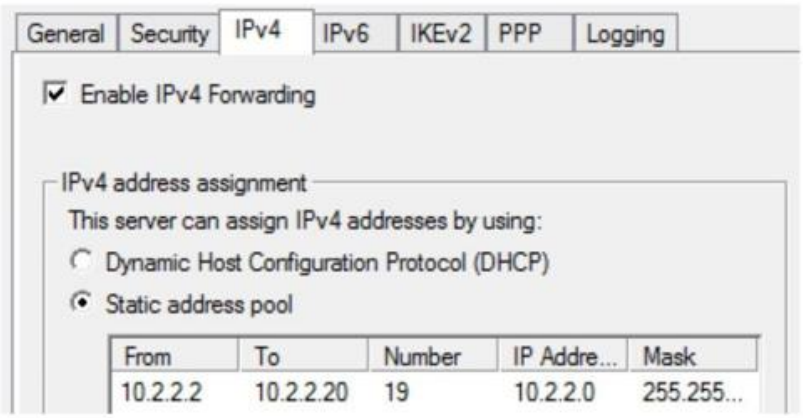
- Similar settings for Accounting provider:



- In the SSL Binding section: select the digital certificate just installed:

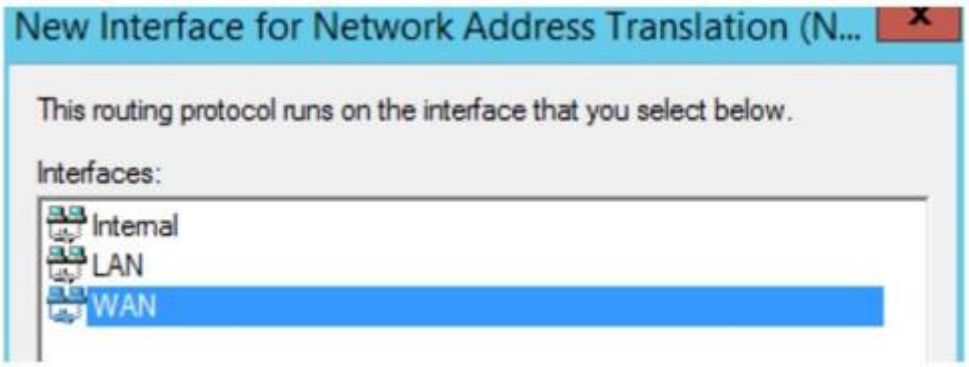
- Switch to IPv4 Tab

- Select Static address and enter the IP range that will be assigned to the workstation when connecting to VPN.



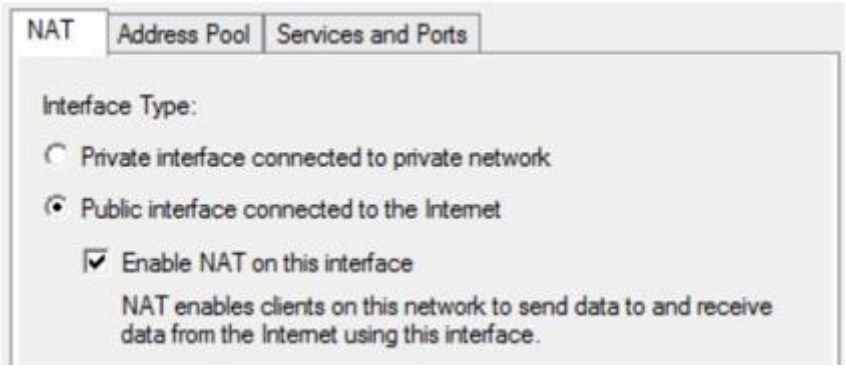
- Continue configuring NAT to allow workstations to access into the webserer in the DC server.

- Right click on NAT, select New Interface. The interface appears. Select External WAN Interface.



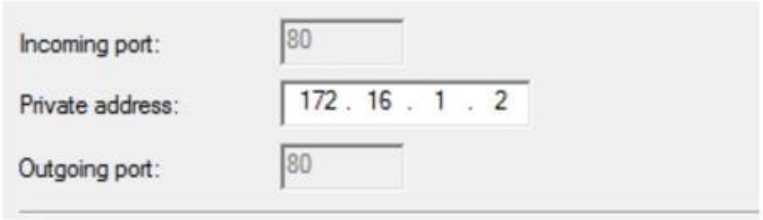
- Click OK and the configuration window will appear.

- In the NAT tab, select Public interface, check Enable NAT.



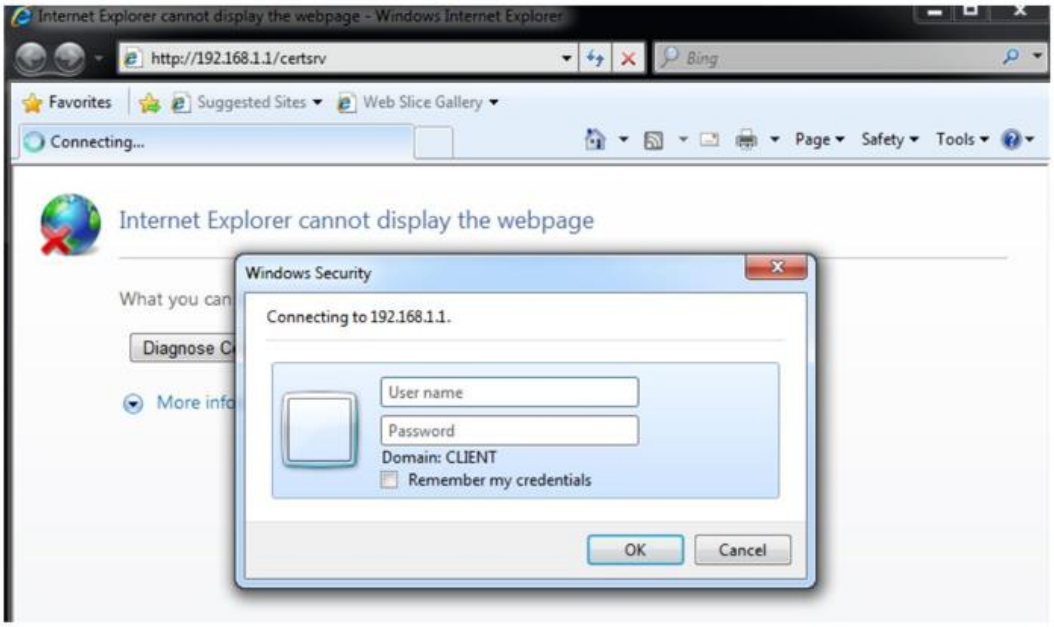
- In the Services and Ports Tab: Select Web Server (HTTP):

- The window that appears requires setting the IP address of the DC:

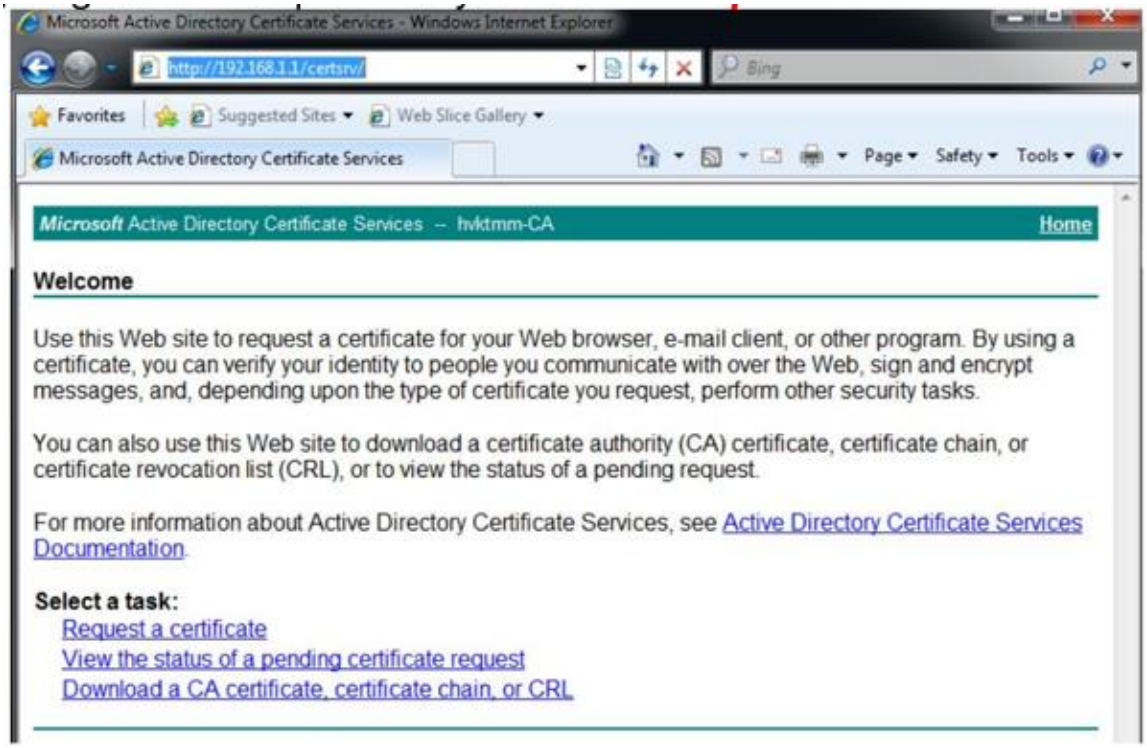


1.8. Perform on Windows 7 machine

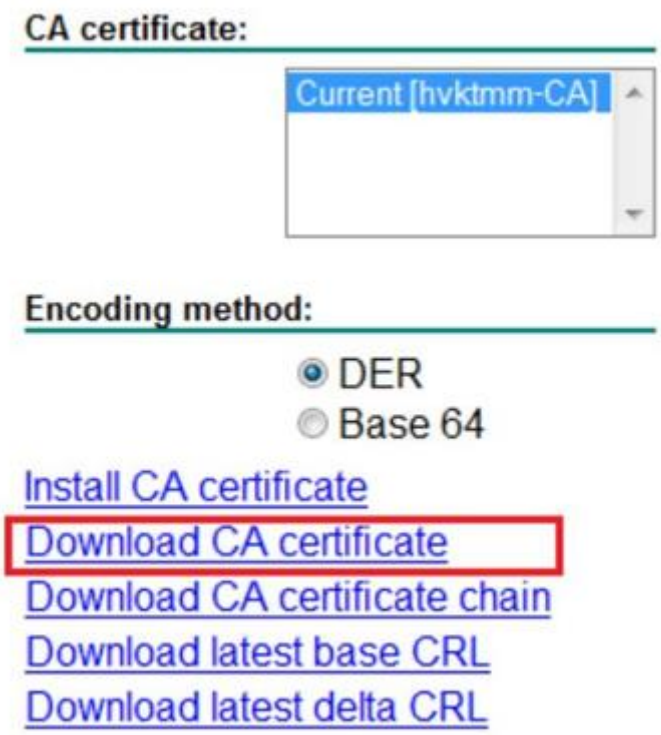
- Access to digital certificate issuance service in DC server via web browser at http:// 192.168.1.1/ certsrv



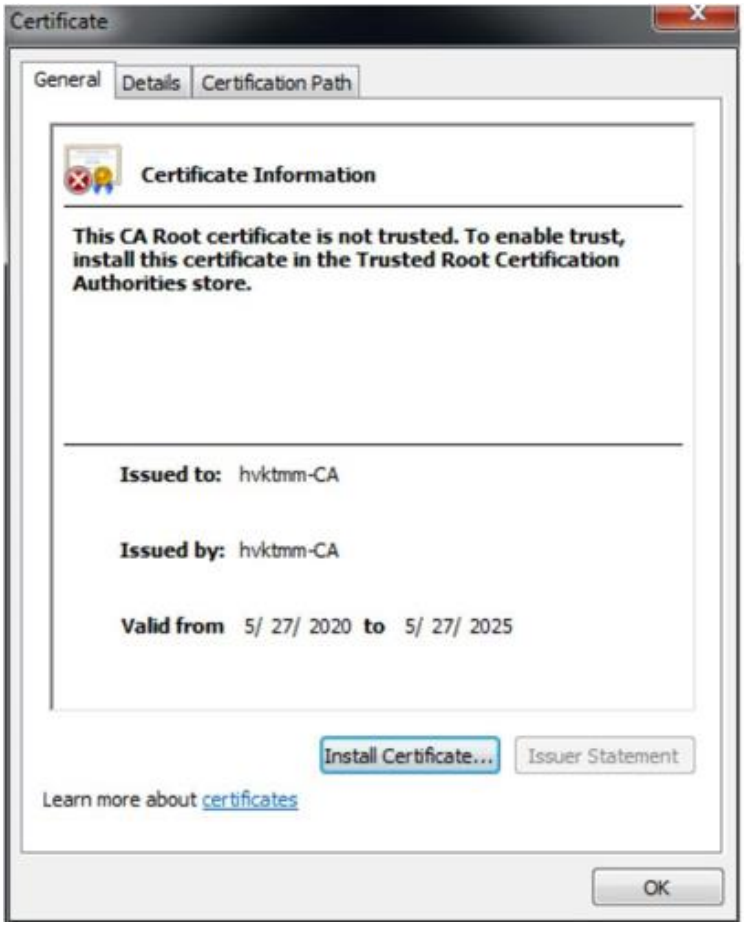
- Log in with the previously created account.



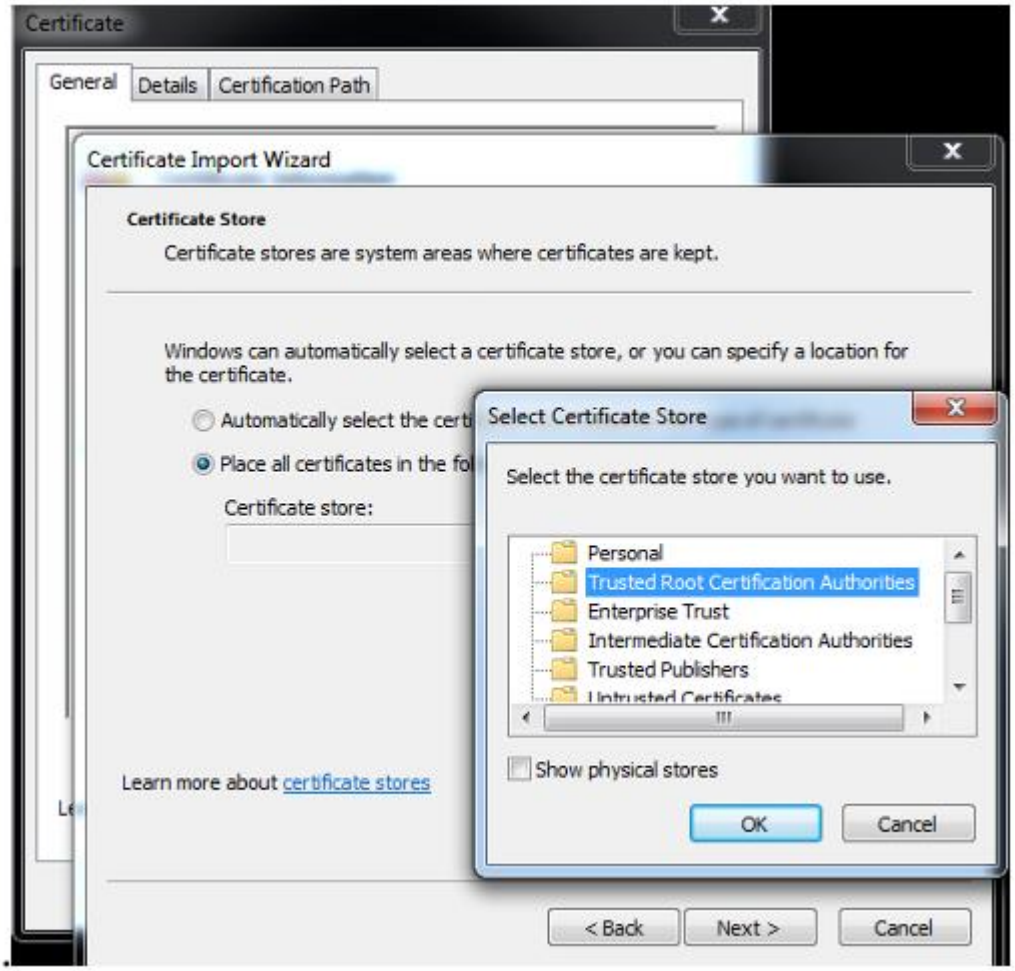
- Check the Download a CA certificate option. Continue to select Download CA certificate:



- Select where to save the CA digital certificate. Open the downloaded digital certificate and select Install Certificate

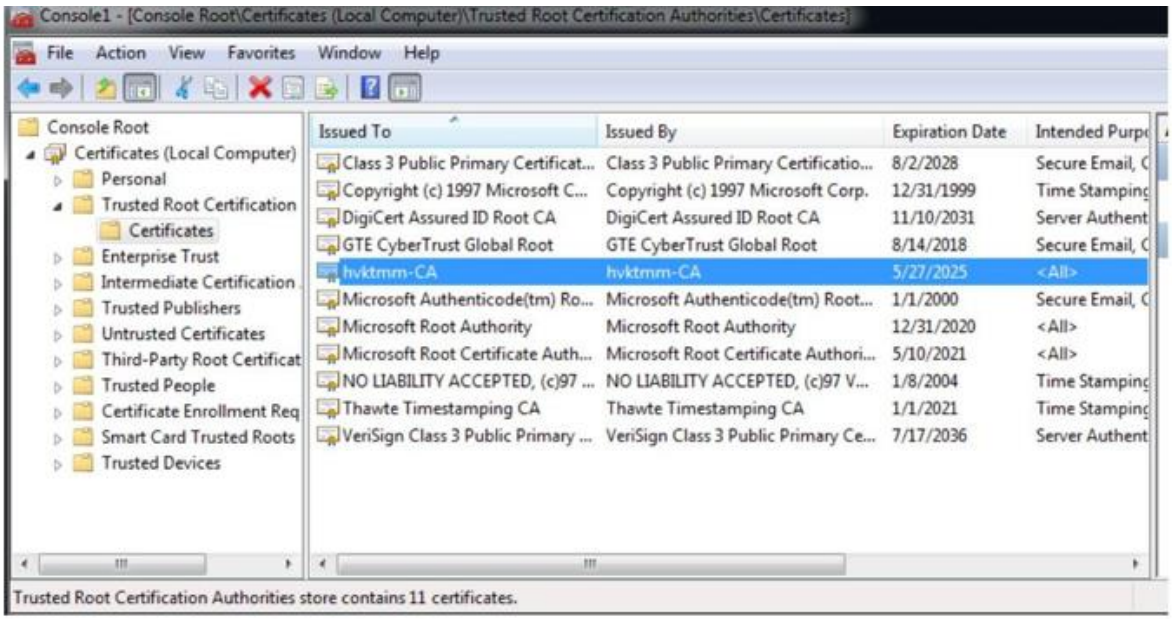


- In the Certificate Import Wizard window, select Certificate store → Trusted Root Certification Authorities → OK → Next →Finish.



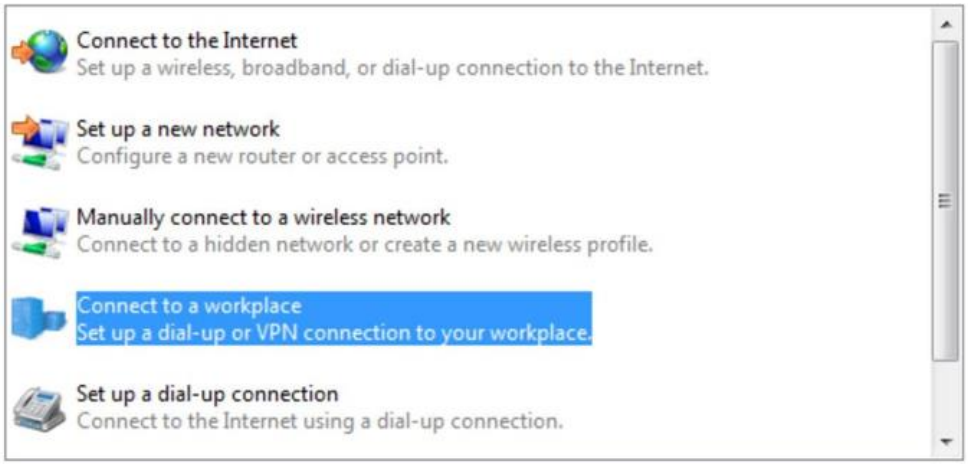
- If a warning dialog box appears asking if you want to install this Certificate, select Yes.

- Perform a check and see that the digital certificate has been installed on the machine.



- The next step is to install and configure the VPN connection. Access the path: Control Panel → Network and Sharing Center → Set up a new connection or network or network.

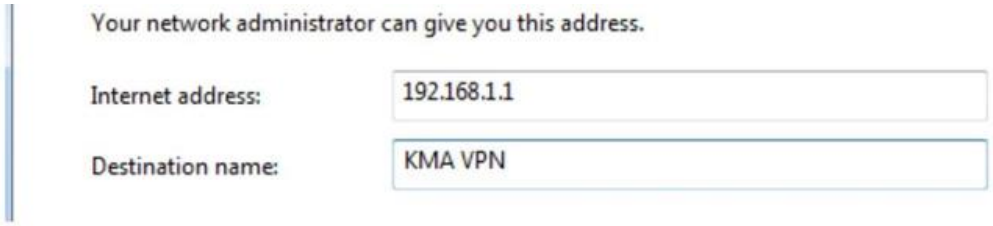
- Next interface select Connect to a workplace.



- Next interface select connection via VPN:

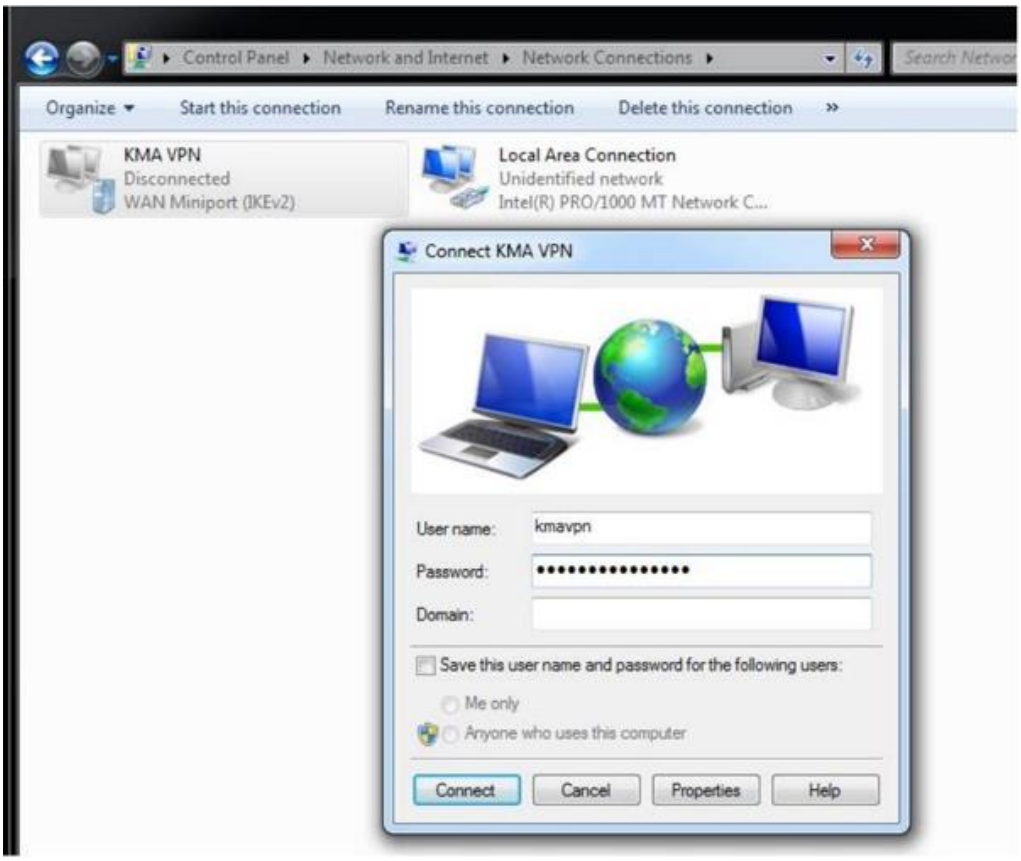
- Select I'll set up an Internet connection later.

- The next interface enters the external IP address of the SRV (connect to Windows 7). Name the connection is:

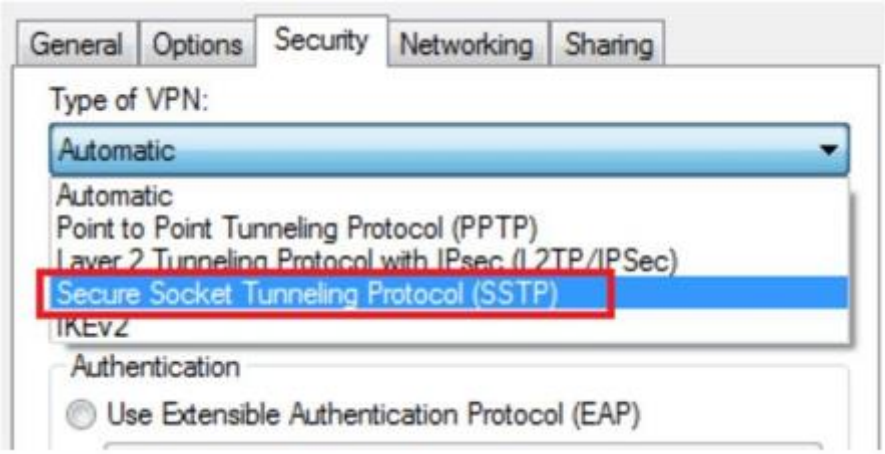


- Next step is to enter the account created on the DC server. Select Create to create the connection.

- Access the path Control Panel\Network and Internet\Network Connections.



- Select Properties to configure using SSTP protocol. Security tab select SSTP connection.

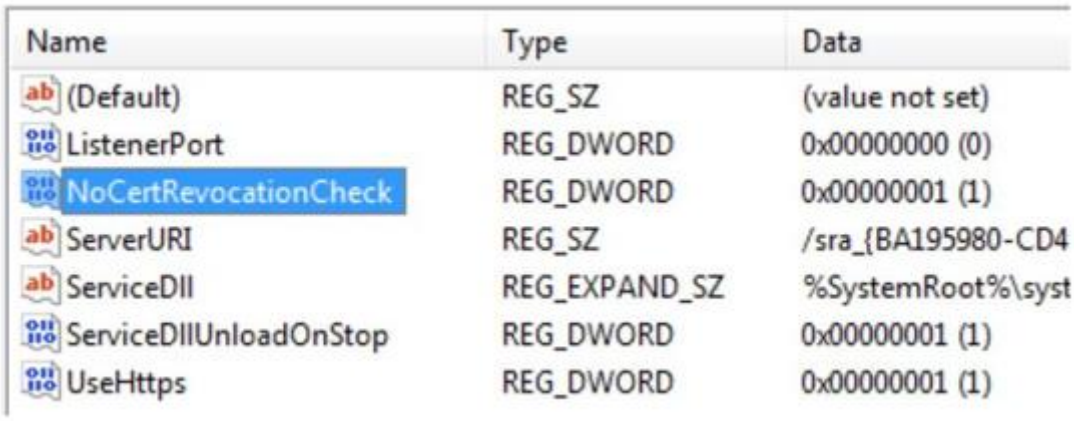


- Leave other parameters as default. Select OK to save and close the window. Access the Registry via Run. (type regedit).

- Access the path: HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Services → SstpSvc.

- Right click on Parameters → New → DWORD

- Name this DWORD: NoCertRevocationCheck with value 1.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ListenerPort	REG_DWORD	0x00000000 (0)
NoCertRevocationCheck	REG_DWORD	0x00000001 (1)
ServerURI	REG_SZ	/sra_{BA195980-CD4
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\syst
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
UseHttps	REG_DWORD	0x00000001 (1)

- Finish and close the Registry window.

- Return to the connection login window. Re-enter the username and password of the kmavpn user. Click Connect to connect.

- Successful

1.9. Check the results

- On Windows 7 machine, perform Ping to DC server. Success.

- Access shared resources on the DC server

- Check packets sent on the transmission line. Install the WireShark packet capture and analysis tool.