

## 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

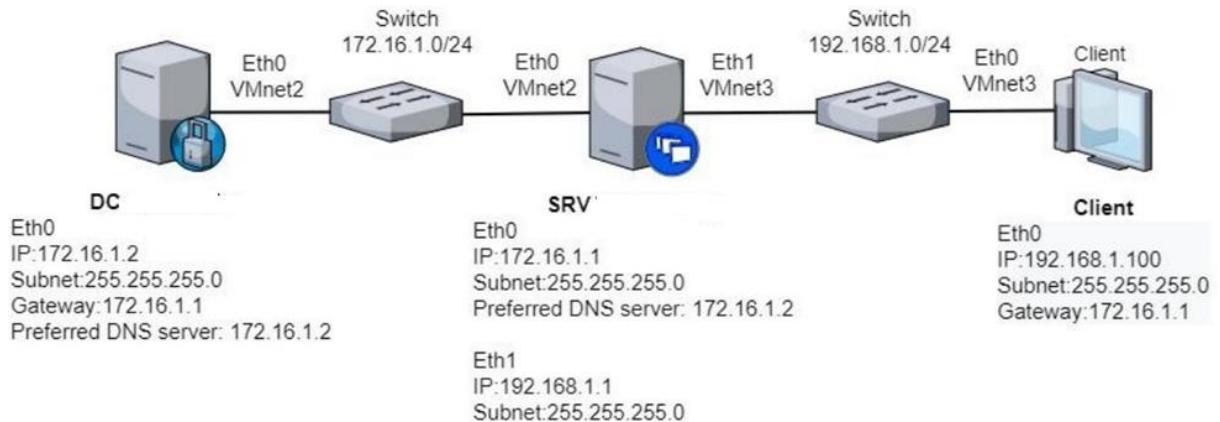
When users have a request to remotely connect to the internal network system to access data, it is necessary to ensure the security of data transmitted over the network to avoid attackers from intercepting, eavesdropping, or stealing data content.

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 ѿ 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

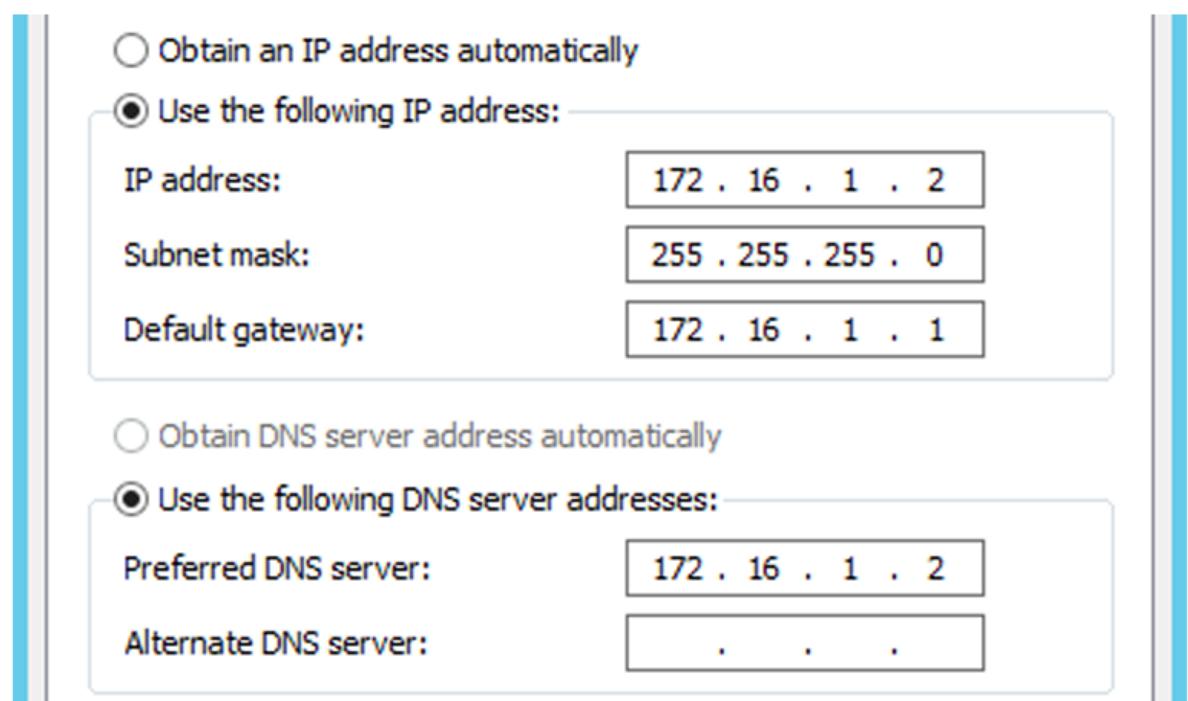
- Connect to the account created on DC

- Check the result

### **1.5. Set up IP addresses for the machines**

#### **1.5.1. On DC**

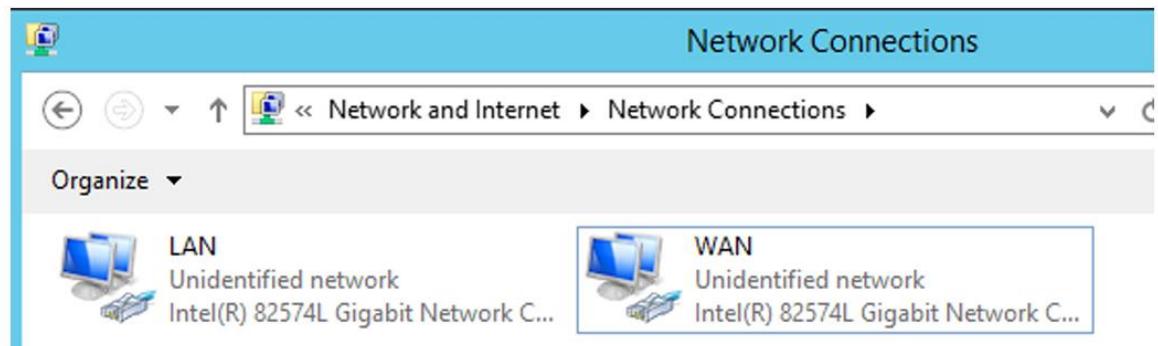
- Rename the machine to DC
- Set password for user Administrator
- Set up static IP address according to deployment model



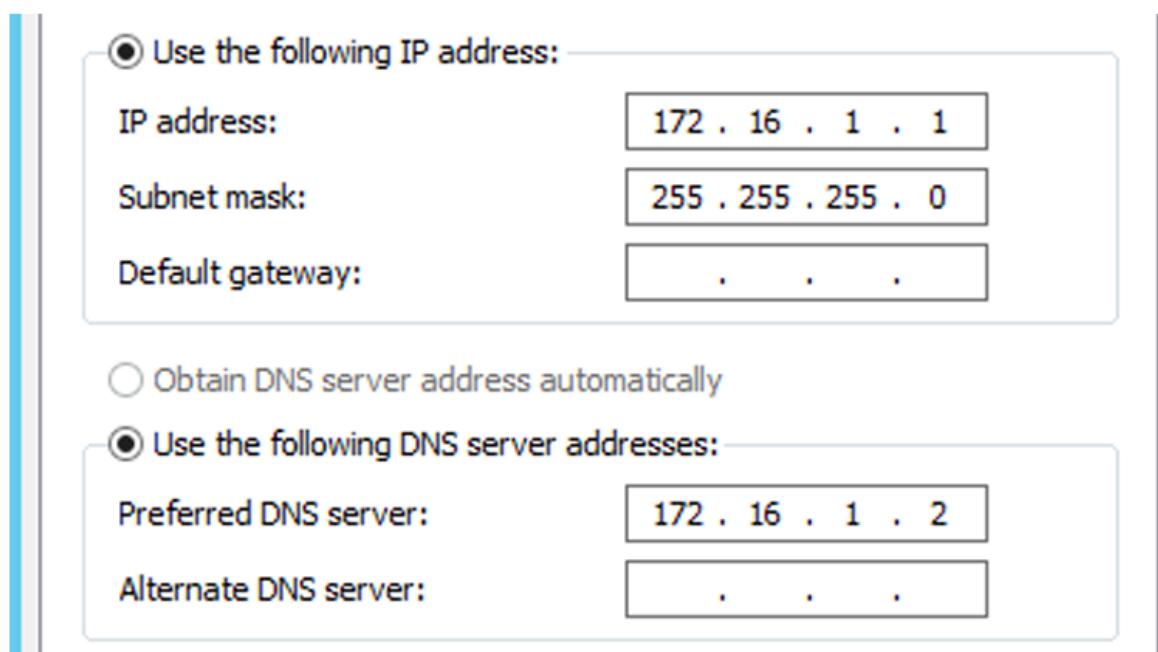
#### **1.5.2. On SRV**

- 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

Obtain an IP address automatically

Use the following IP address:

IP address:

192 . 168 . 1 . 1

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

· · ·

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

· · ·

Alternate DNS server:

· · ·

### 1.5.3. On Client

- Rename the machine to Client
- Set up static IP address according to deployment model

Obtain an IP address automatically

Use the following IP address:

IP address:

192 . 168 . 1 . 100

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

172 . 16 . 1 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

· · ·

Alternate DNS server:

· · ·

### 1.5.4. Testing

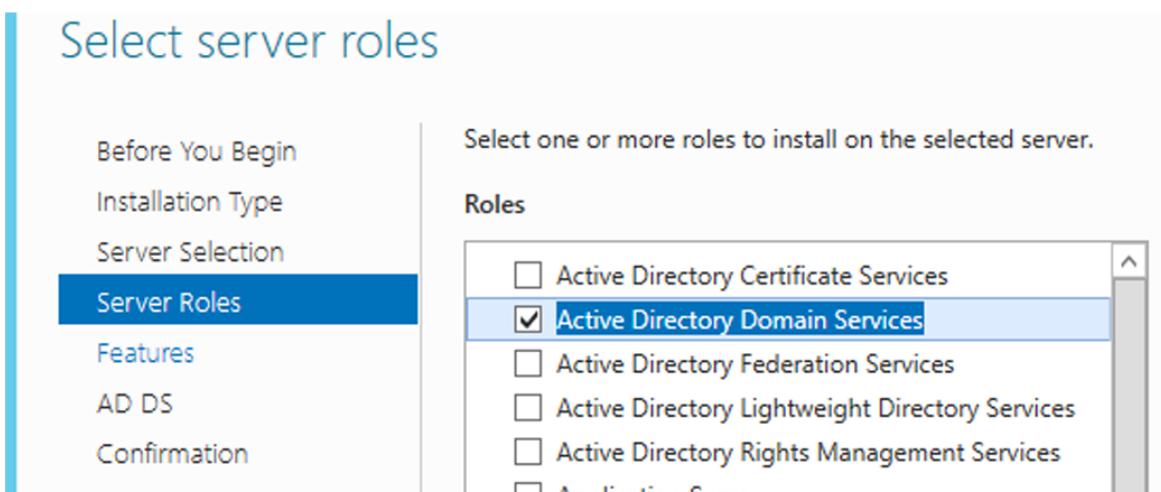
- To make it easier to do the lab, we should turn off the firewall on all 3 machines DC, SRV, Client.
- Make sure that ping is possible between SRV – DC and from SRV – Client

## 1.6. Execute on DC server

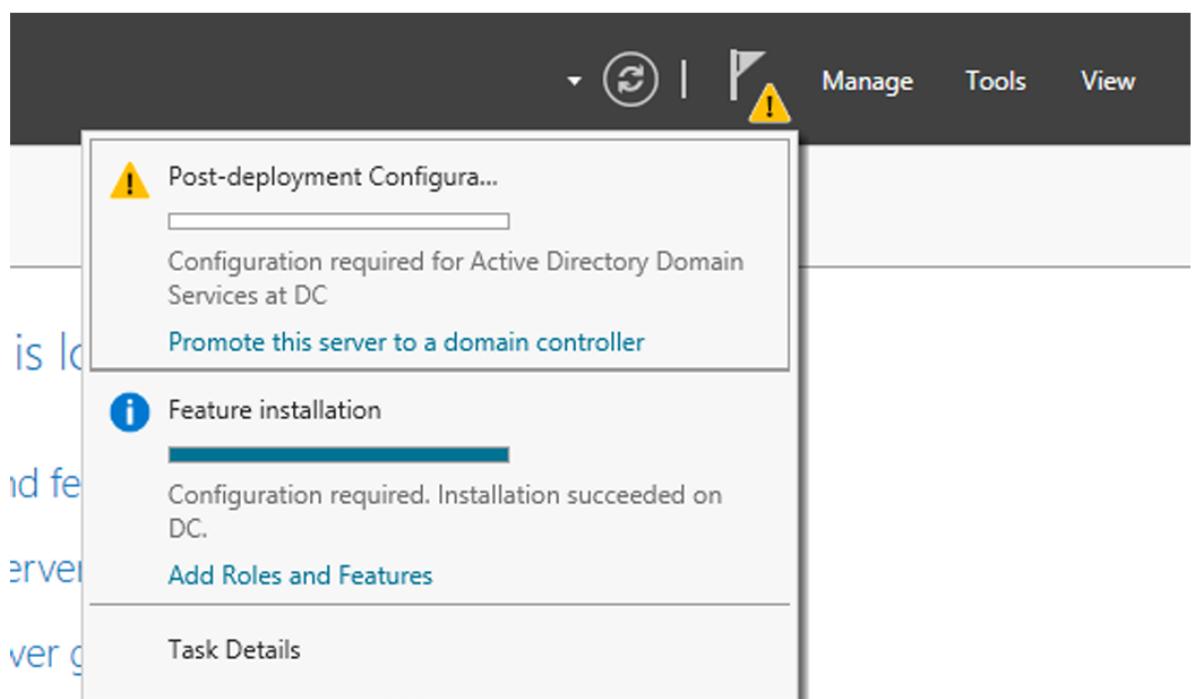
### 1.6.1. Upgrade Win 2012 to Domain Controller (DC)

- 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.

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

Add a domain controller to an existing domain

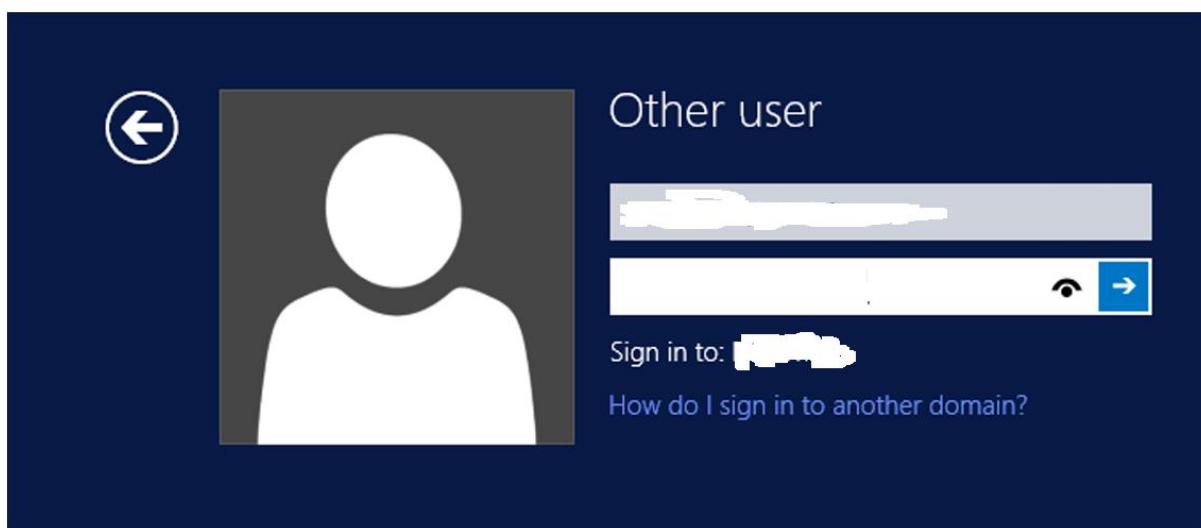
Add a new domain to an existing forest

Add a new forest

Specify the domain information for this operation

Root domain name: hvktmm.bcy

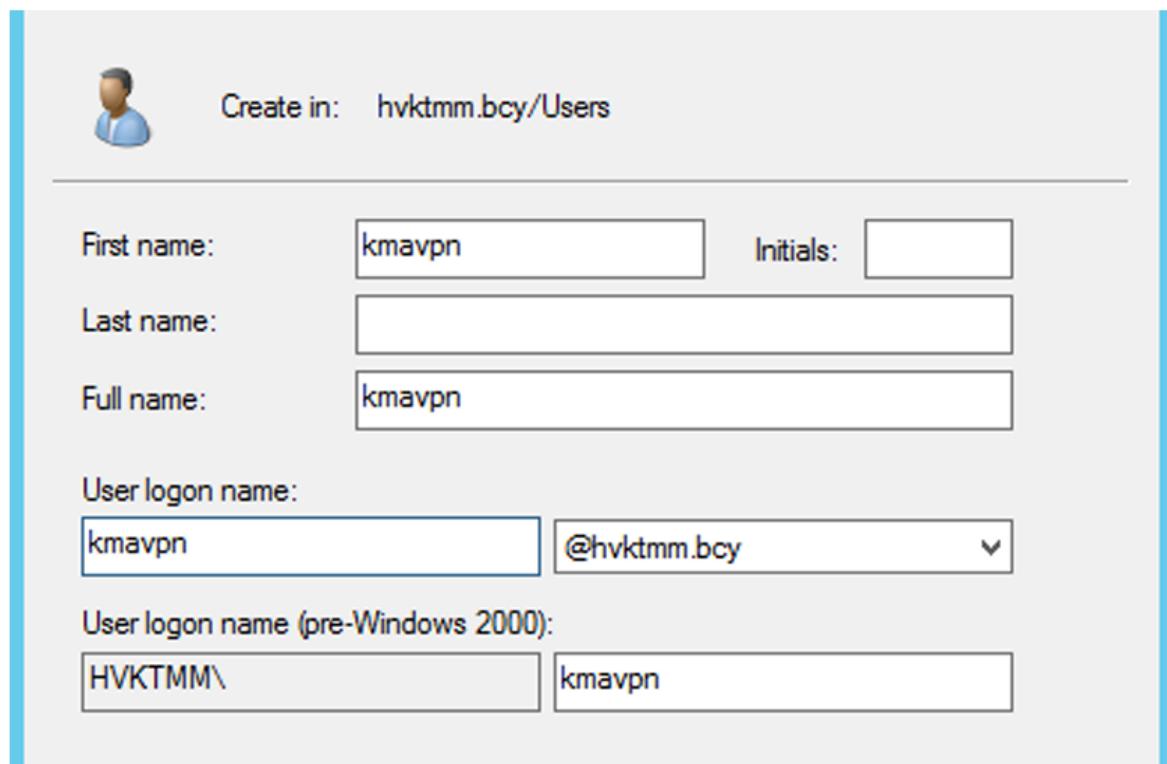
- Continue to select Next by default and Install to upgrade to DC. The DC server will automatically restart after the upgrade is complete. The login account will now be in the form DOMAIN\user as shown below.



### 1.6.2. Create a user that allows remote access via VPN

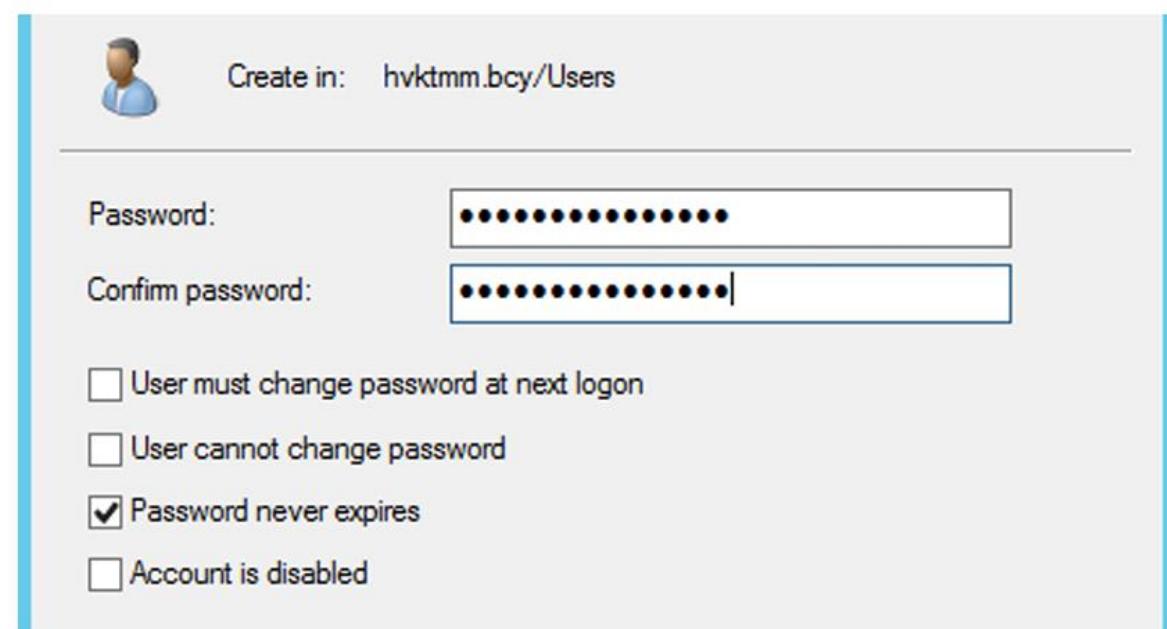
- Access the path: Server Manager → Tools → Active Directory User and Computer.

- Right click on the Users → New → User.
- Set the username for remote access as: vpn



A screenshot of a user creation interface. At the top, there is a small blue user icon. To its right, the text "Create in: hvktmm.bcy/Users" is displayed. Below this, there are several input fields: "First name" with the value "kmavpn", "Initials" (empty), "Last name" (empty), "Full name" with the value "kmavpn", "User logon name" with the value "kmavpn" and a dropdown menu showing "@hvktmm.bcy", and "User logon name (pre-Windows 2000)" with the value "HVKTMM\kmavpn".

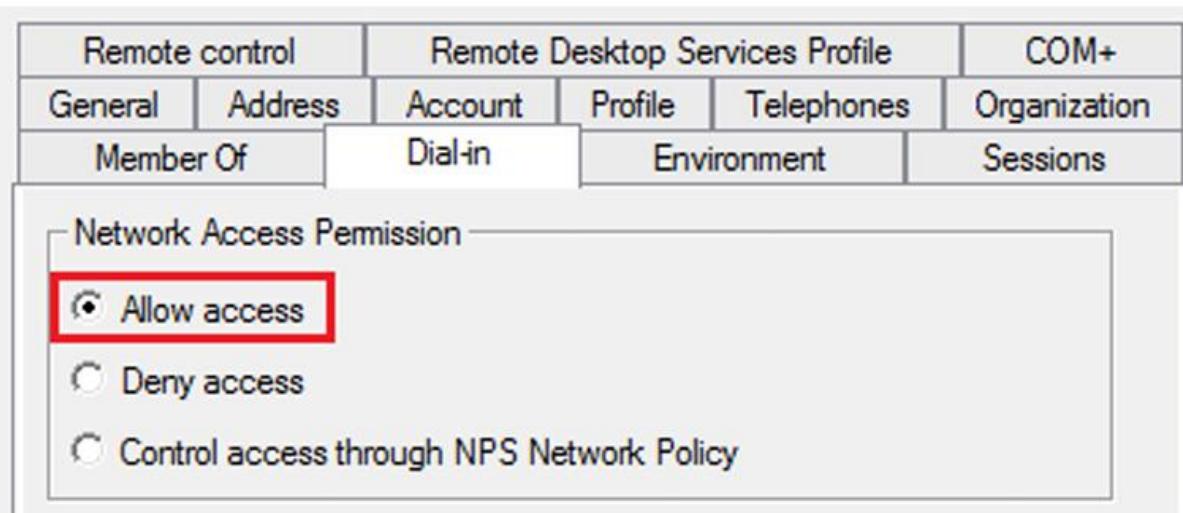
- The next interface sets the password for the user. Note that the password here must be complex



A screenshot of a password configuration interface. At the top, there is a small blue user icon. To its right, the text "Create in: hvktmm.bcy/Users" is displayed. Below this, there are two password fields: "Password" and "Confirm password", both containing a series of black dots representing a complex password. Below these fields is a group of checkboxes:

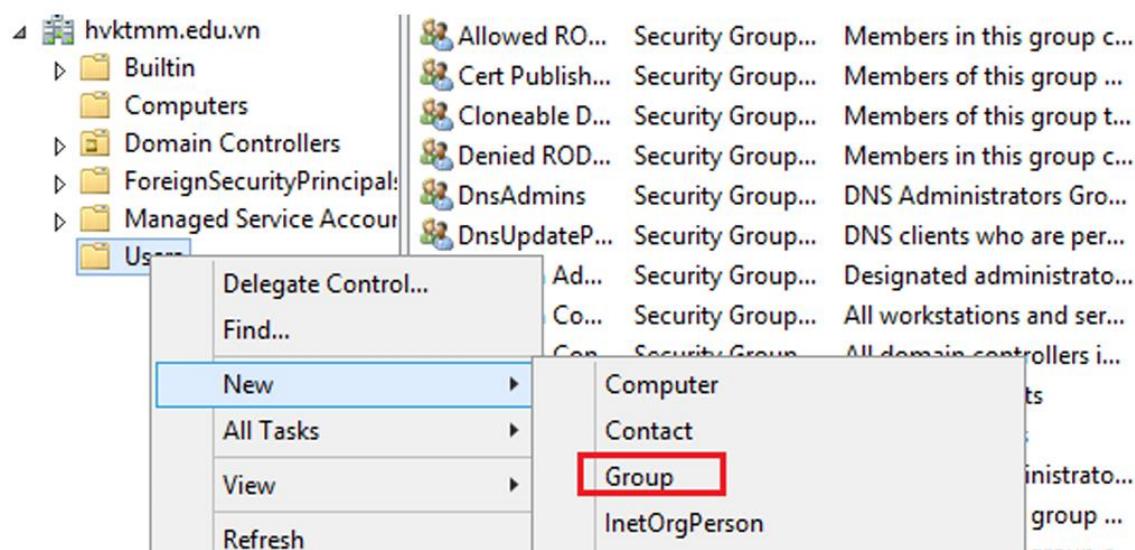
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

- 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

Create in: hvktmm.bcy/Users

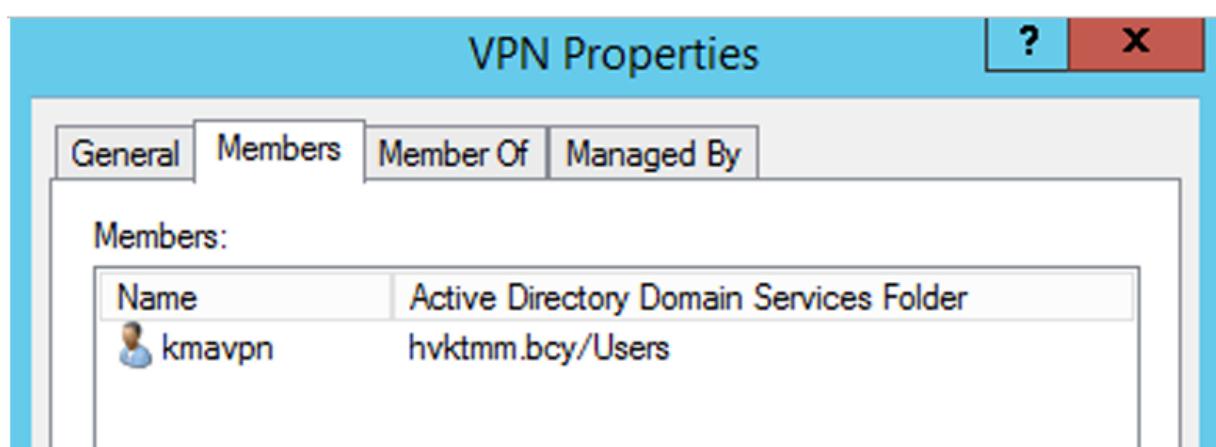
Group name:

Group name (pre-Windows 2000):

Group scope  Domain local  Global  Universal

Group type  Security  Distribution

- Add user to VPN group



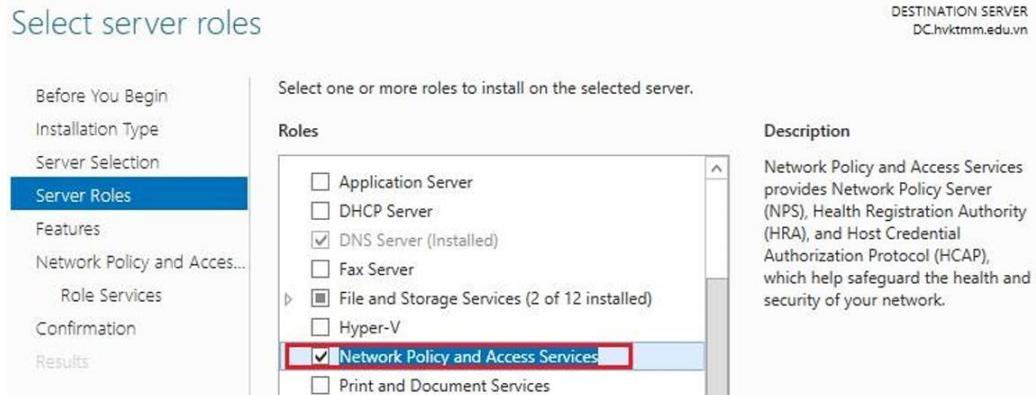
- Finish the step of creating remote access user.

### 1.6.3. Install Network Policy Server service

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

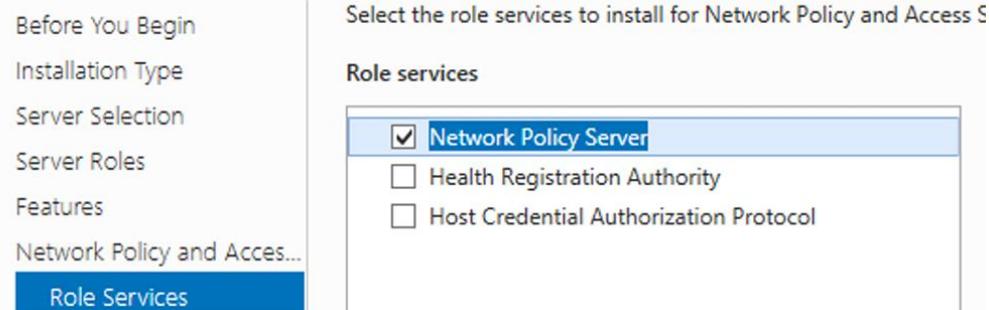


- Leave the three first steps as default and select Next.
- At the role selection step (Select server roles): Select Network Policy and Access Services:



- Select Next to continue.
- Leave the next options as default.
- Service selection interface select: Network Policy Server.

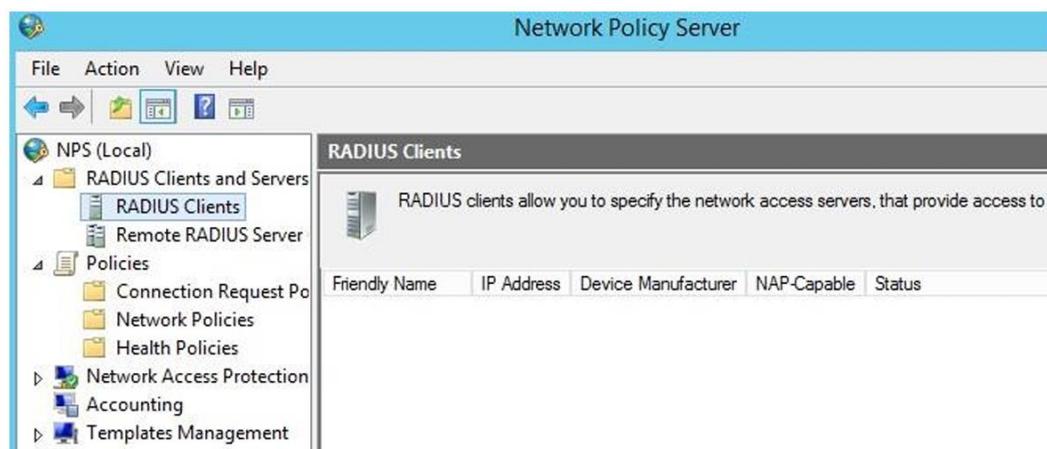
## Select role services



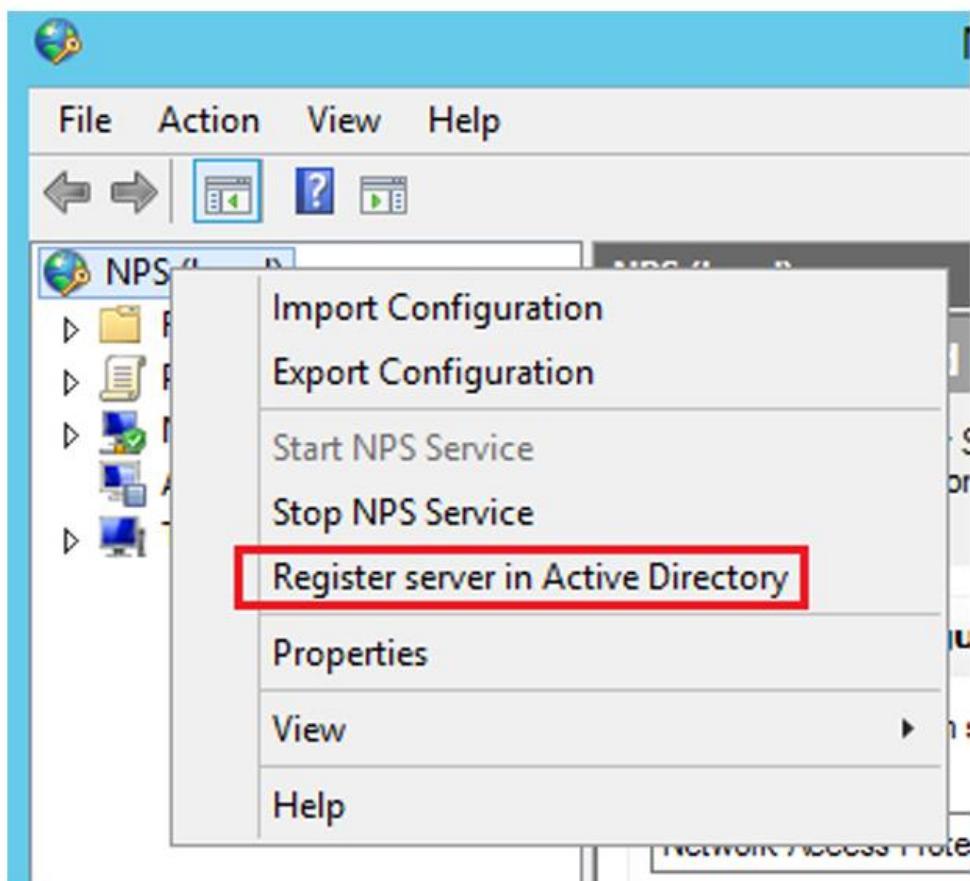
- Click Next and Install to install the service.

### 1.6.4. Configure Radius Server in Network Policy Server

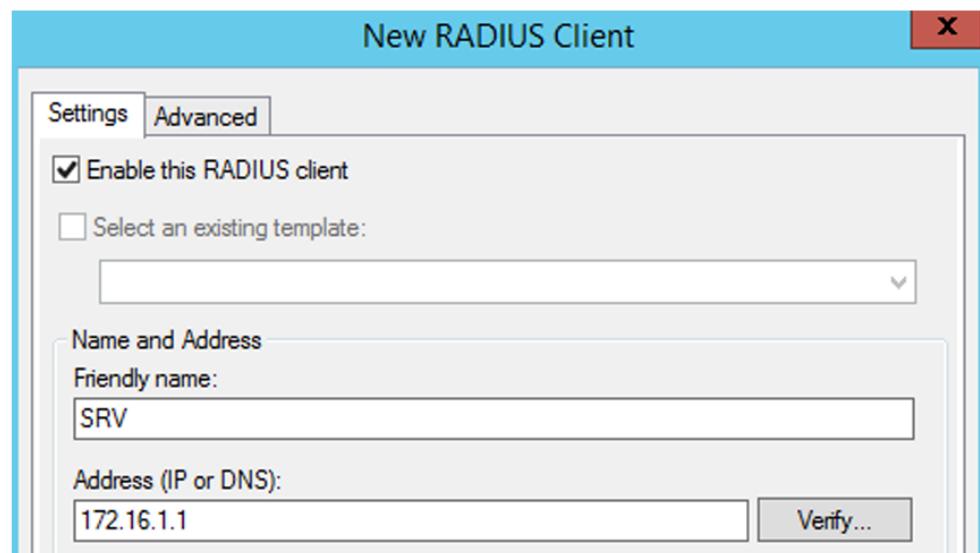
- Access Network Policy Server via the path: Server Manager → Tools → Network Policy Server



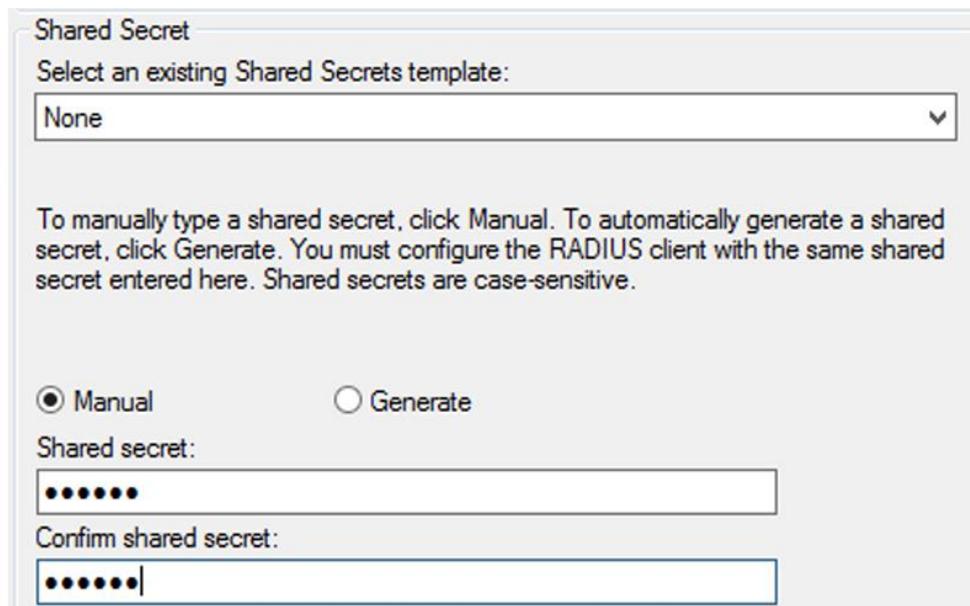
- Register the service in Active Directory:



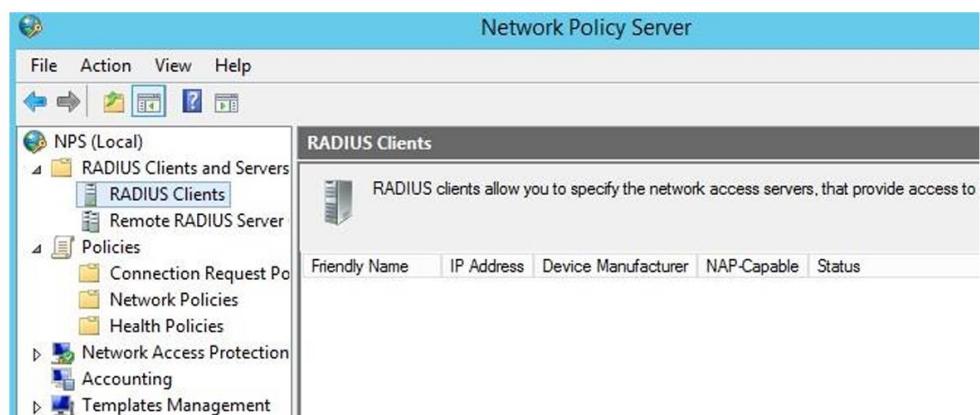
- Configure the Radius Client machine definition as the SRV machine.



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

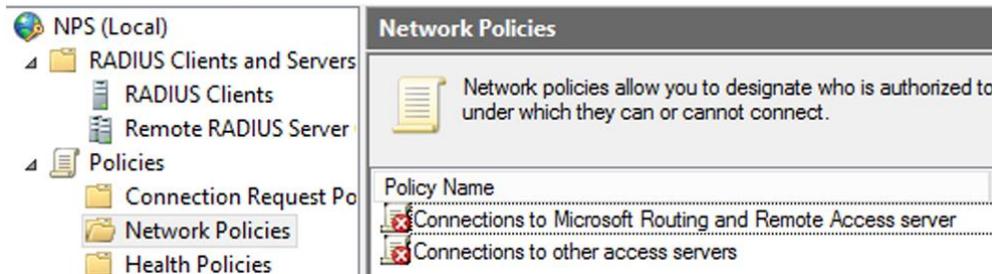


- Select OK to finish.

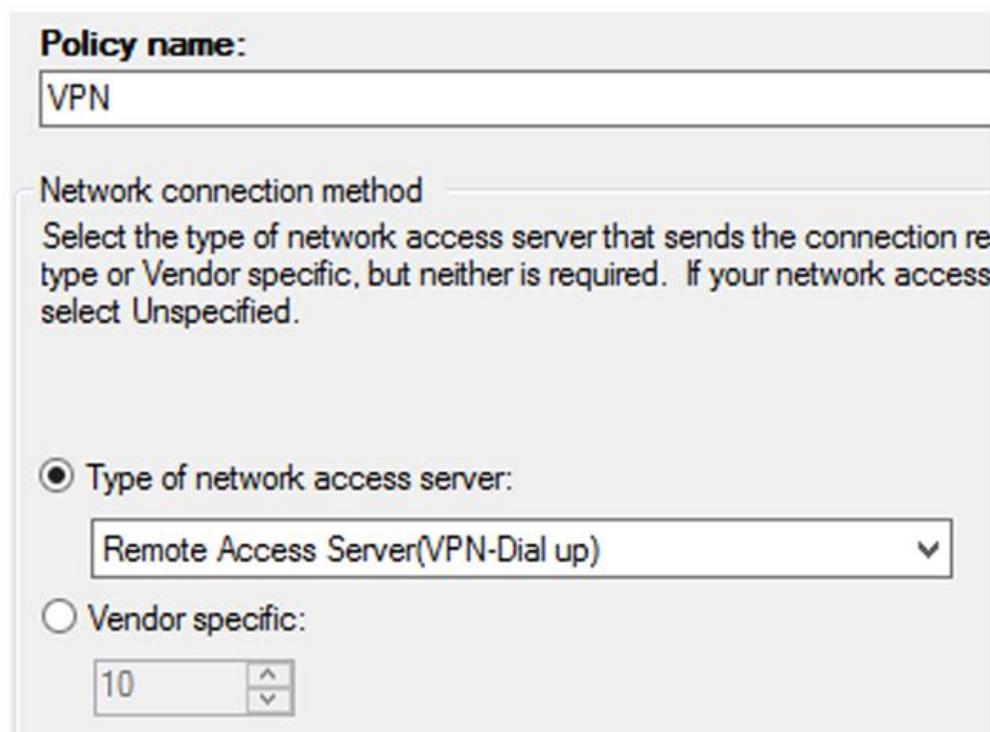


- Next we need to define the authentication policy.

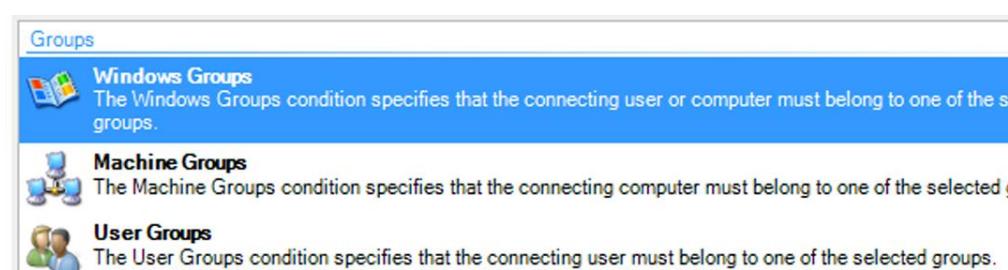
- Go to Policies → Network Policies. The interface is as follows:



- 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

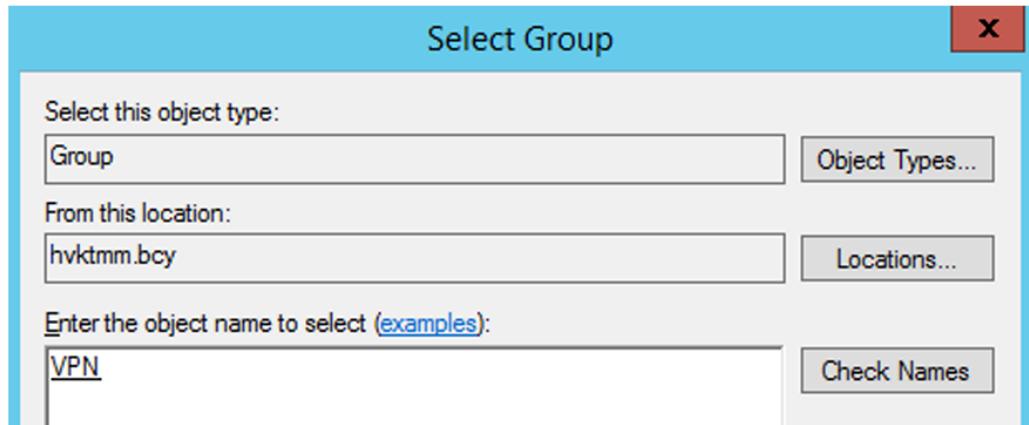


- Select Next to continue.
- Conditions section: Select Add to add: Export interface Now select Windows Groups:

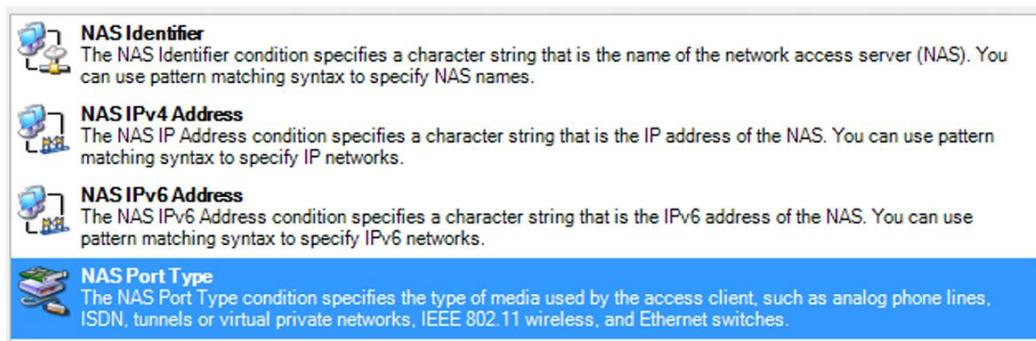


- Select Add Group to add a group:

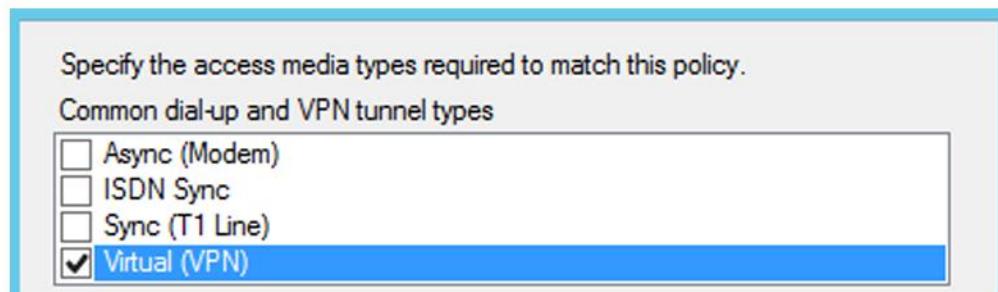
- Point the VPN group created in the step above:



- 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



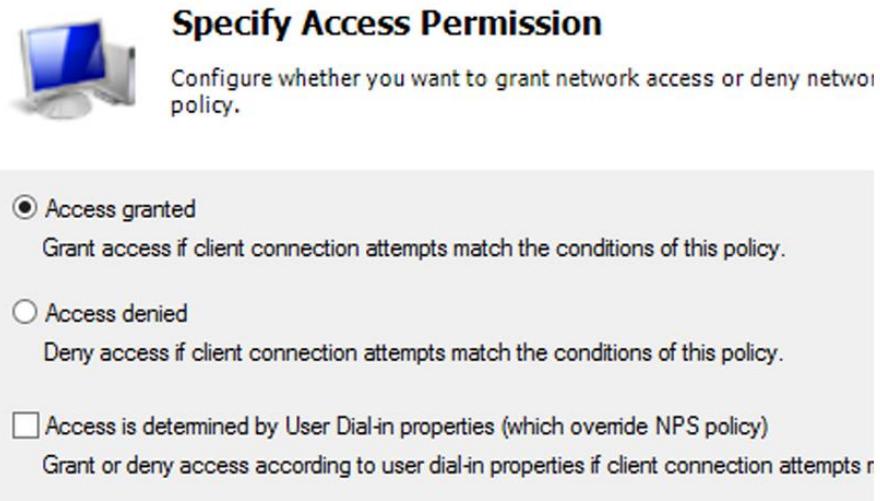
- Now the main interface will have 2 conditions defined.

**Specify Conditions**  
Specify the conditions that determine whether **one** condition is required.

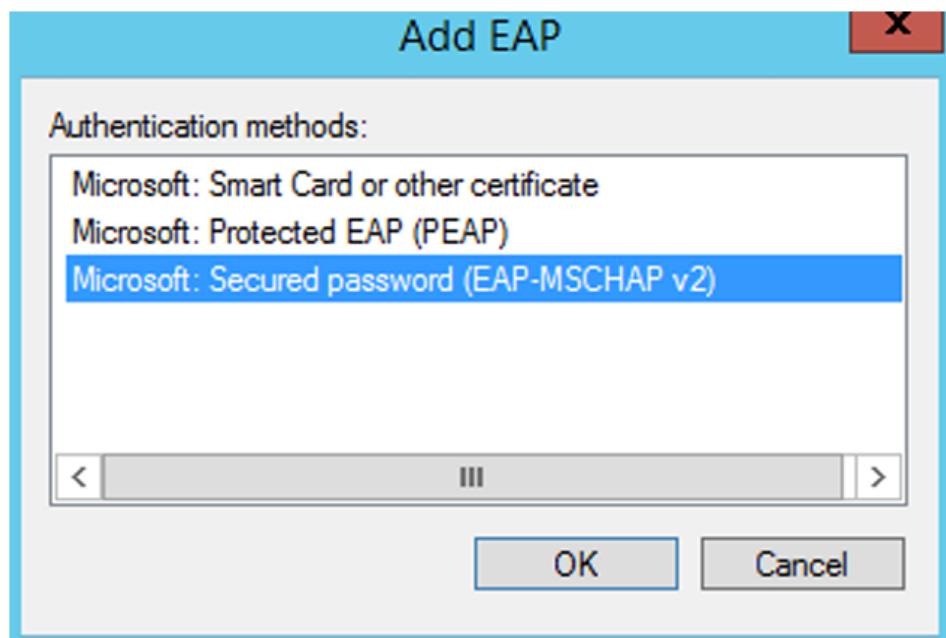
**Conditions:**

Condition	Value
Windows Groups	HVKTMM\VPN
NAS Port Type	Virtual (VPN)

- 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.

**EAP Types:**

Microsoft: Secured password (EAP-MSCHAP v2)	<b>Move Up</b>
	<b>Move Down</b>

**Add...** **Edit...** **Remove**

**Less secure authentication methods:**

<input checked="" type="checkbox"/> Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
<input checked="" type="checkbox"/> User can change password after it has expired
<input checked="" type="checkbox"/> Microsoft Encrypted Authentication (MS-CHAP)
<input checked="" type="checkbox"/> User can change password after it has expired
<input type="checkbox"/> Encrypted authentication (CHAP)
<input type="checkbox"/> Unencrypted authentication (PAP, SPAP)
<input type="checkbox"/> Allow clients to connect without negotiating an authentication method.
<input type="checkbox"/> Perform machine health check only

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

Policy Name	Status	Processing Order	Access Type	...
VPN	Enabled	1	Grant Access	R

### 1.6.5. Install CA authentication center service.

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

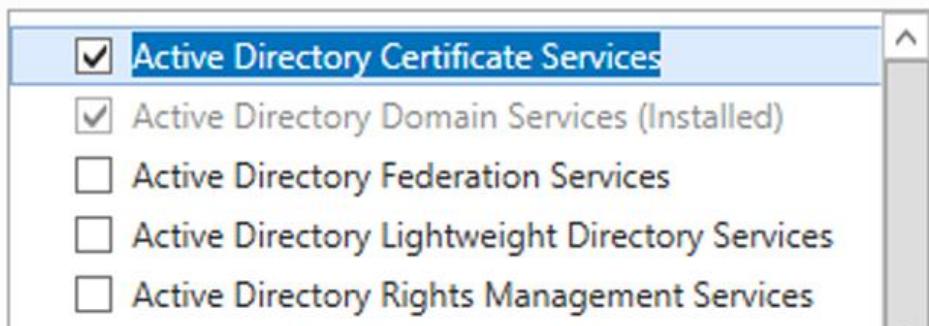
- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage

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

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

Select one or more roles to install on the selected server.

### Roles



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

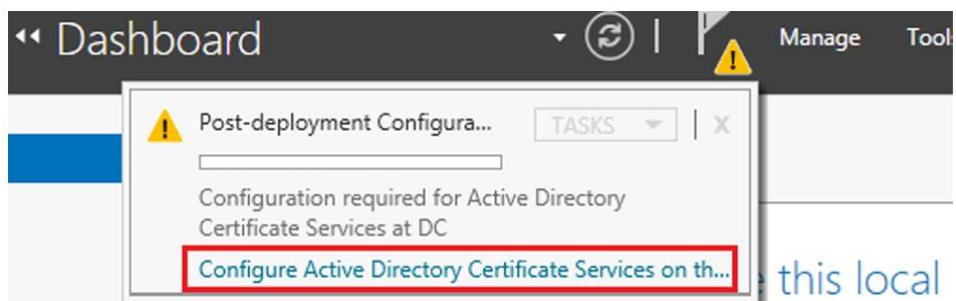
### Role services



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

## Credentials

DESTINATION SERVER  
DC.hvktmm.edu.vn

**Credentials**

Role Services  
Confirmation  
Progress  
Results

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: HVKTMM\Administrator Change...

- Select Next to continue.
- Next interface select 2 options as shown below:

### Select Role Services to configure

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

- Next interface select Enterprise CA:

#### Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

Standalone CA

Standalone CAs can be members of a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

- Select Next to continue:
- Select CA Type: Root CA
- Private key section: Select Create a new private key Select.

## Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1**
- MD5

- The next interface names the CA:

## Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

hvktmm-CA

Distinguished name suffix:

DC=hvktmm,DC=bcy

Preview of distinguished name:

CN=hvktmm-CA,DC=hvktmm,DC=bcy

- Default time is 5 years.
  - Leave the next interfaces as default, select Configure to configure CA.
- Configuration complete:

The following roles, role services, or features were configured:

### Active Directory Certificate Services

**Certification Authority**  
[More about CA Configuration](#)

 Configuration succeeded

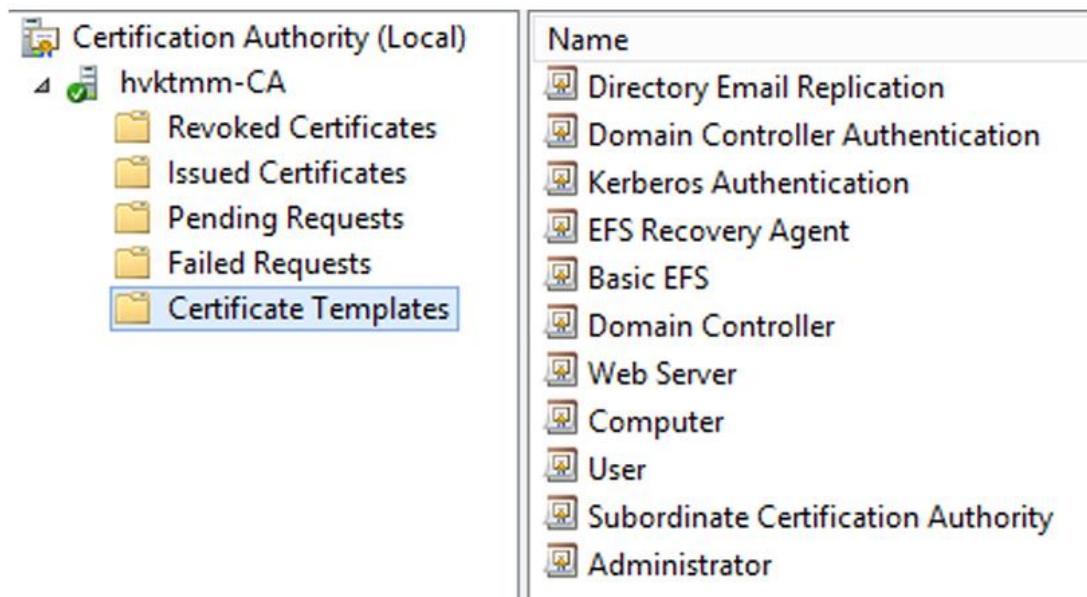
**Certification Authority Web Enrollment**  
[More about Web Enrollment Configuration](#)

 Configuration succeeded

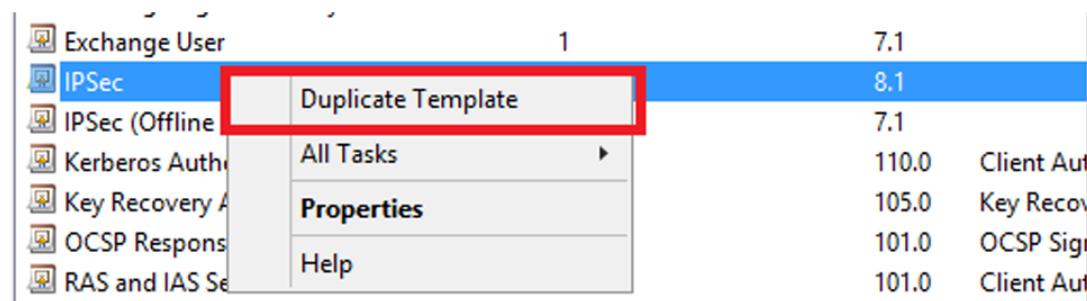
- Click Close to close the configuration completion window

### 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:

## Properties of New Template

X

Subject Name	Server	Issuance Requirements		
Superseded Templates	Extensions	Security		
Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

SSTP

Template name:

SSTP

Validity period:

2 years ▾

Renewal period:

6 weeks ▾

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

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

Properties of New Template X

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling Cryptography Key Attestation

Purpose: Signature and encryption ▼

Delete revoked or expired certificates (do not archive)

Include symmetric algorithms allowed by the subject

Archive subject's encryption private key

Authorize additional service accounts to access the private key (\*)

Key Permissions...

Allow private key to be exported

- Subject Name tab select Supply in the request

Properties of New Template X

Superseded Templates	Extensions	Security
Compatibility	General	Request Handling Cryptography Key Attestation
Subject Name	Server	Issuance Requirements

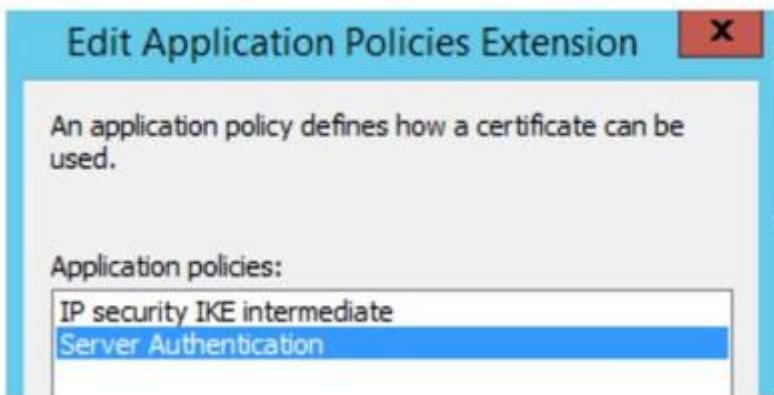
Supply in the request

Use subject information from existing certificates for autoenrollment renewal requests (\*)

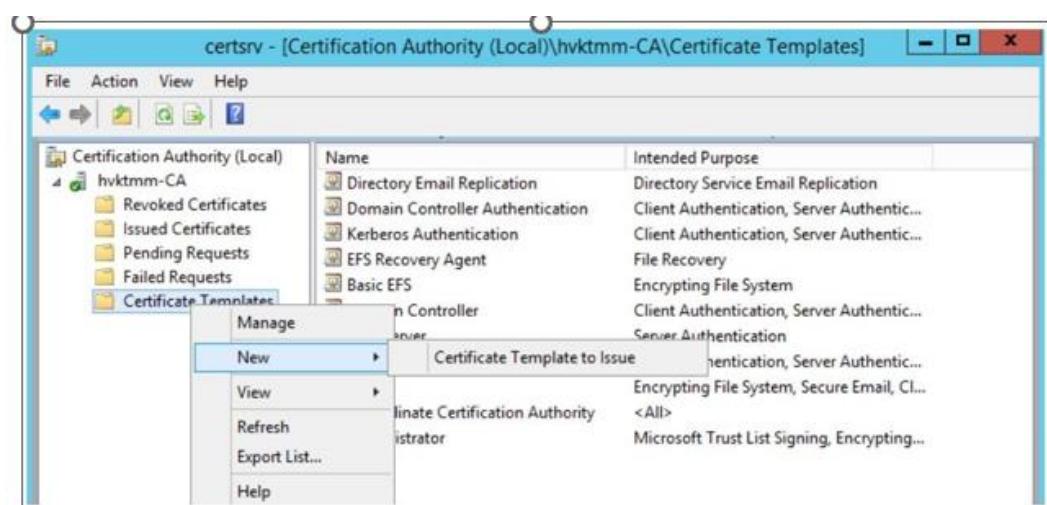
Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

- Tab Extensions select Edit → Add then select Server Authentication



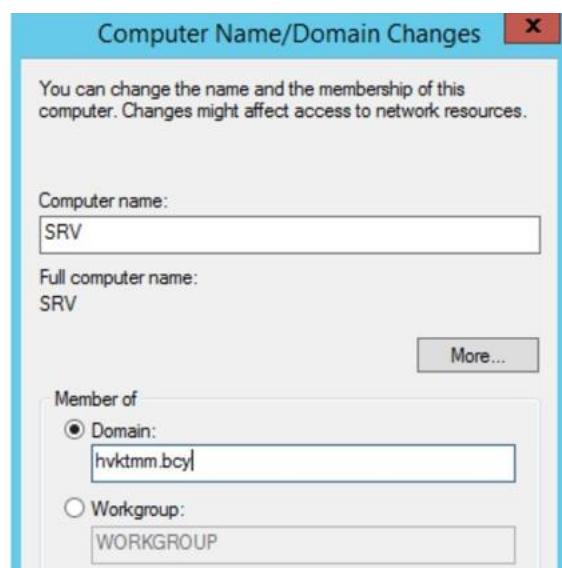
- Then Apply → OK to complete the process of creating new Templates
- Then, right click on Certificate Templates → New → Certificate Template to Issue:



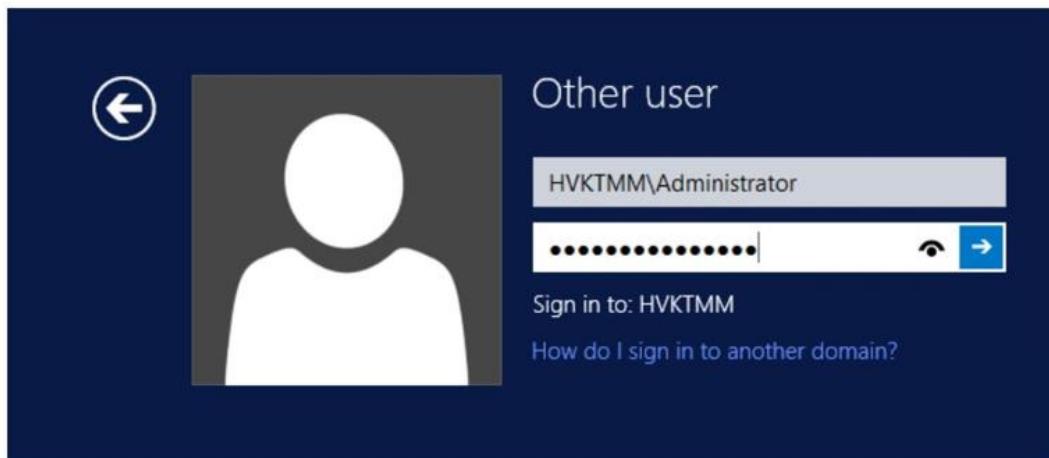
## 1.7. Execute on SRV server

### 1.7.1. Join SRV server to DC

- Perform SRV join to DC:

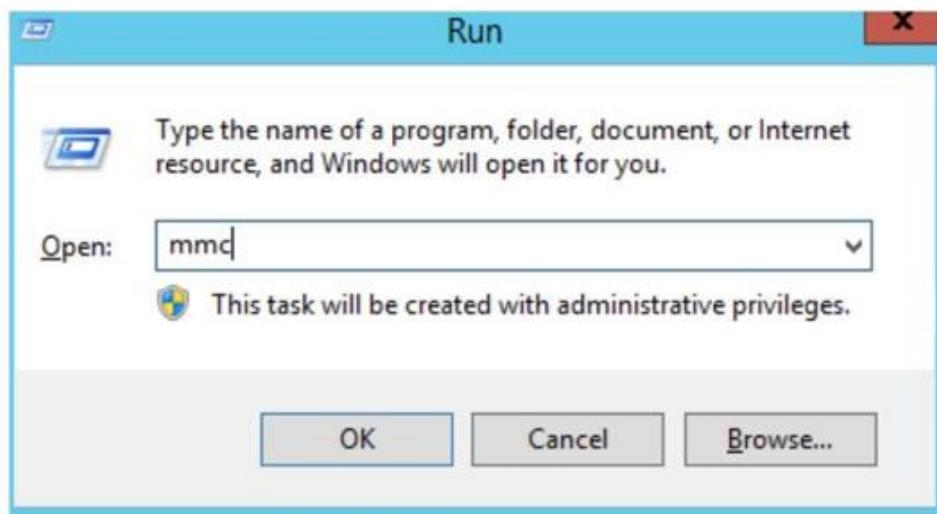


- After successfully joining, the SRV machine will automatically restart and the login screen will be similar to the DC side.



### 1.7.2. Request for digital certificate issuance

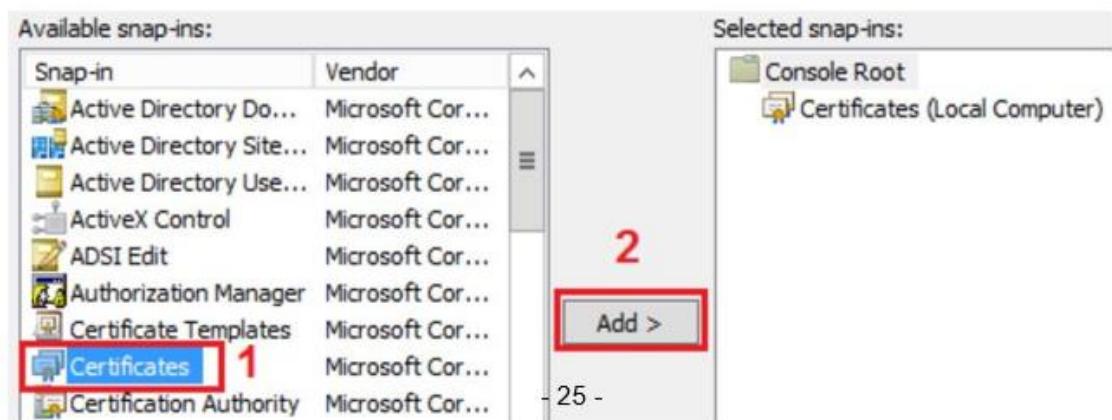
- Turn on the MMC program from Run:



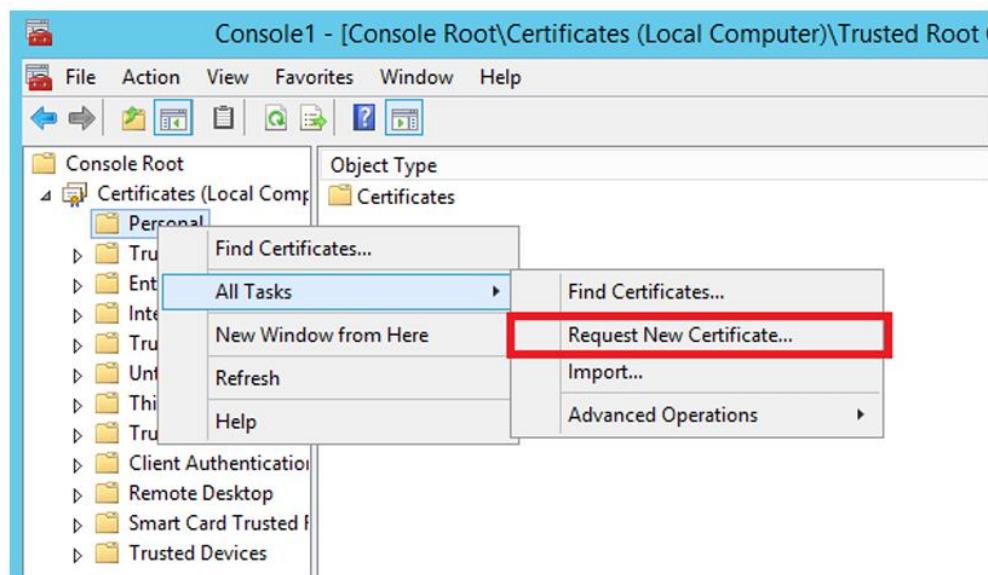
- In the window that appears to select File → Add or Remove snap-in



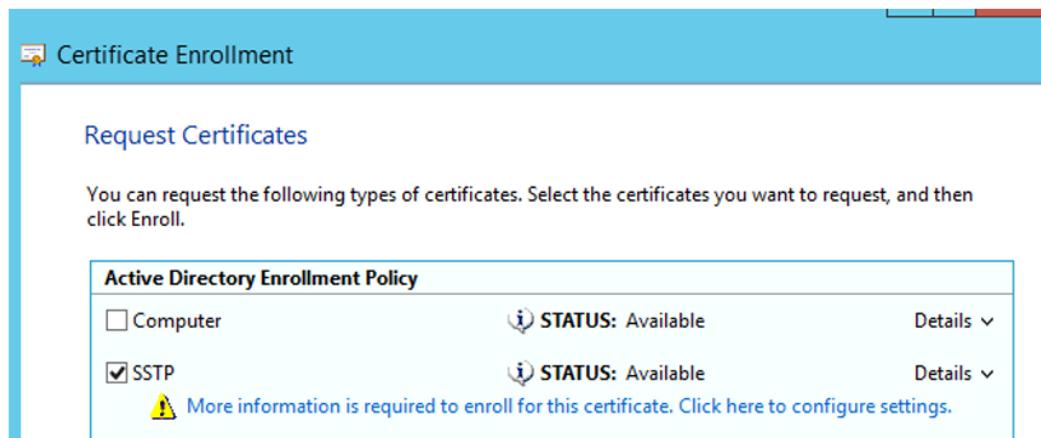
- In the window appears, select as shown below:



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

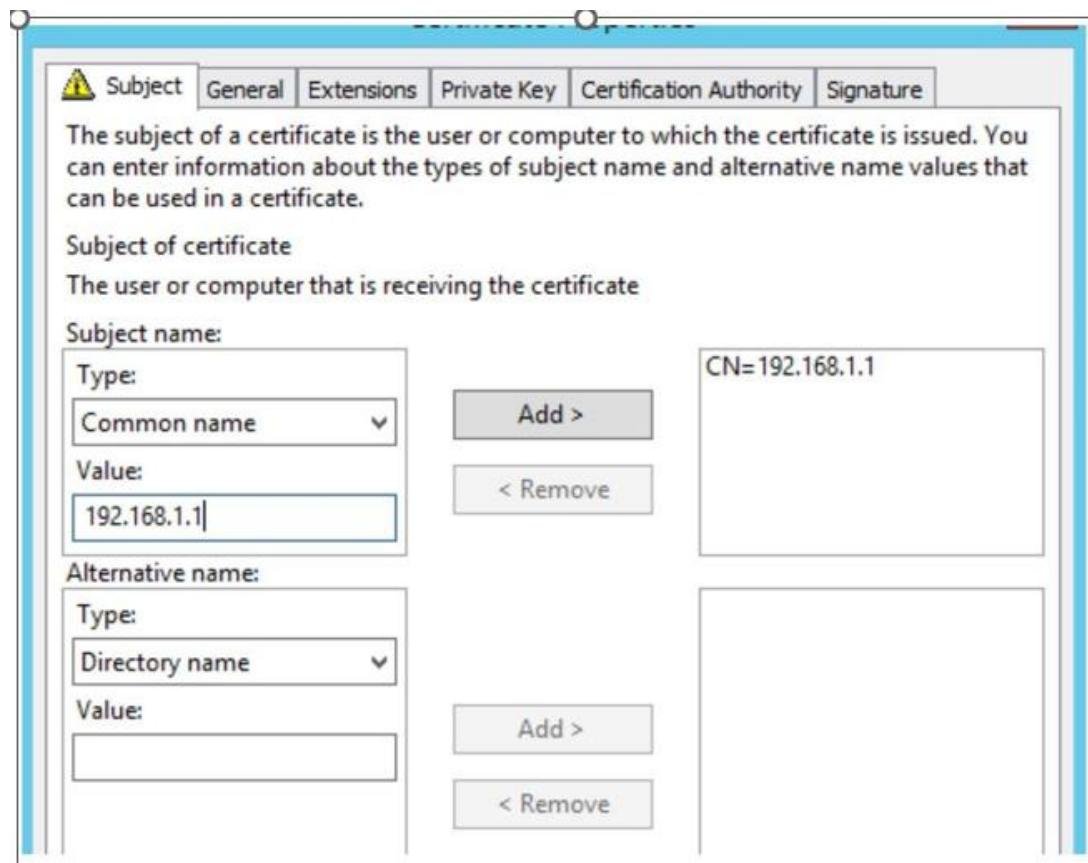


- Continue to select Next by default, in the Request Certificates window select SSTP and click on the yellow warning icon.

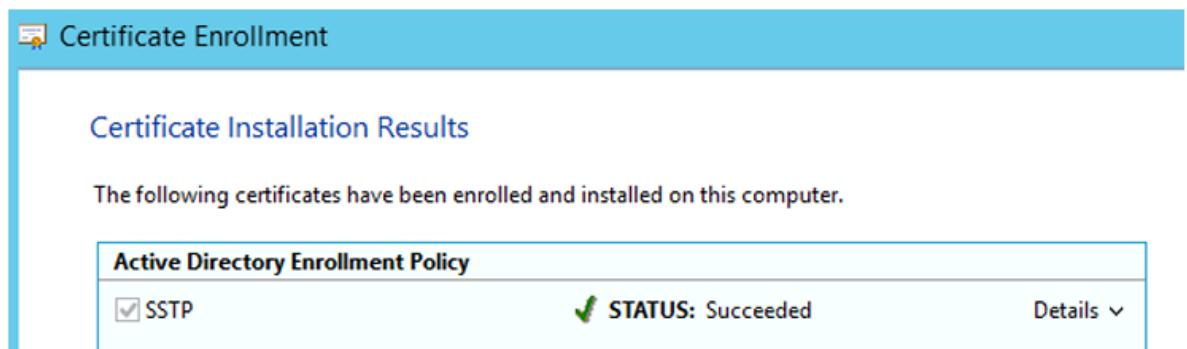


- Select Common name in the Type section

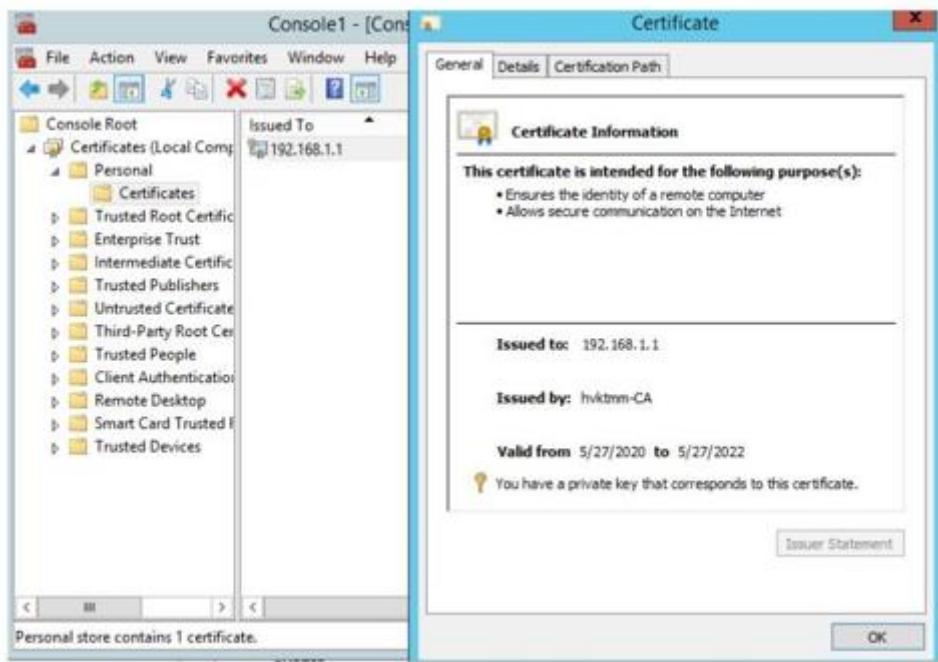
- In the Value field, enter the IP as the external interface of the SRV server. Select Add to agree.



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



- Check the newly issued digital certificate

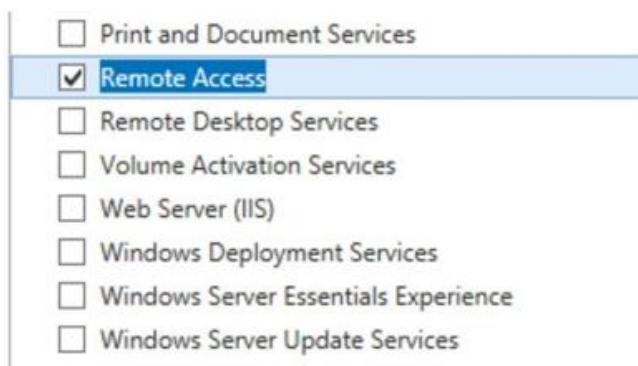


### 1.7.3. Install Routing and Remote Access application

- 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:

## Select role services

Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features

Select the role services to install for Remote Access

### Role services

- DirectAccess and VPN (RAS)
- Routing
- Web Application Proxy

- Next steps select Next and Install to install

### 1.7.4. Configuring Routing and Remote Access services

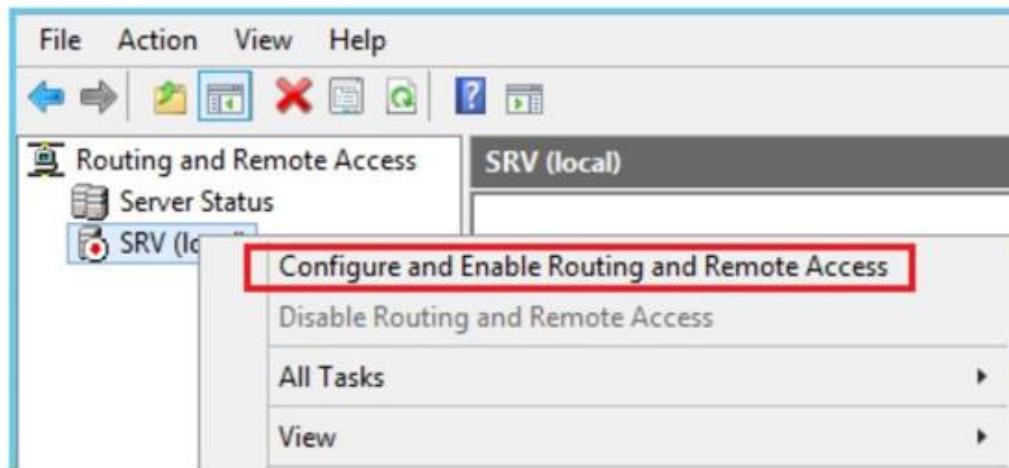
- Access by following the path: Server Manager → Tools → Routing and Remote Access. Select Deploy VPN only.



- 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.

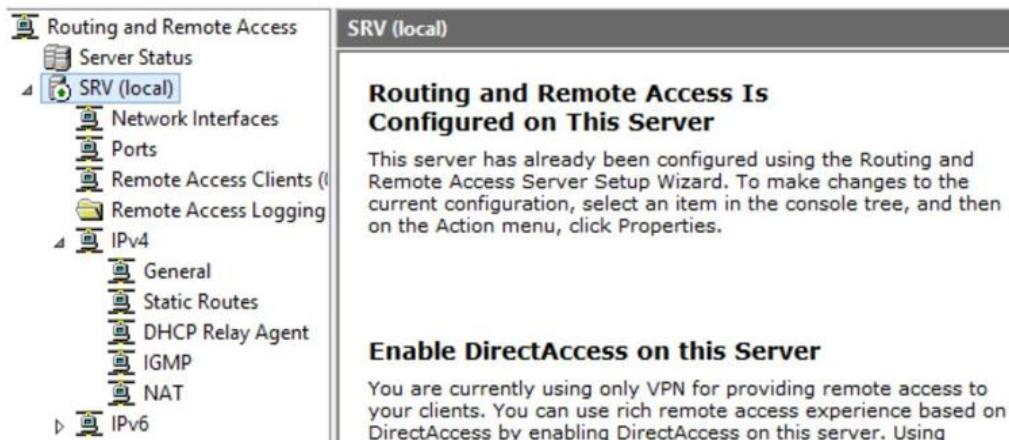
#### Custom Configuration

When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

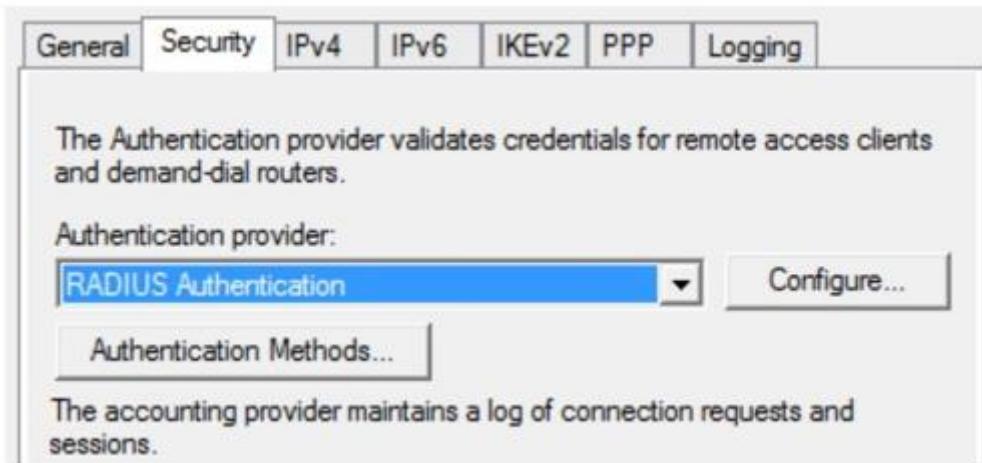
- VPN access
- Dial-up access
- Demand-dial connections ( used for branch office routing )
- NAT
- LAN routing

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

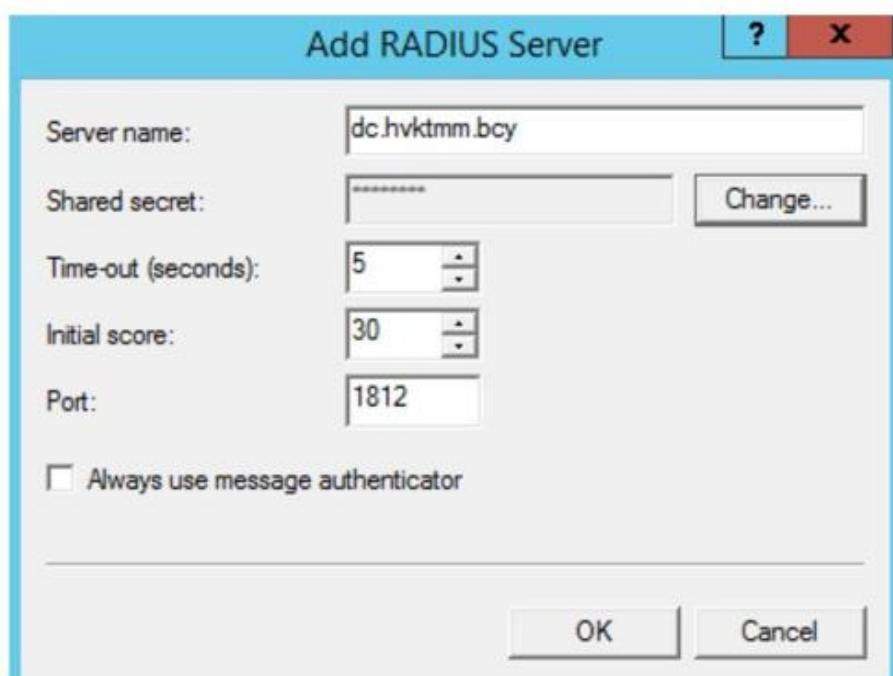


- Right click on the SRV server name and select Properties.

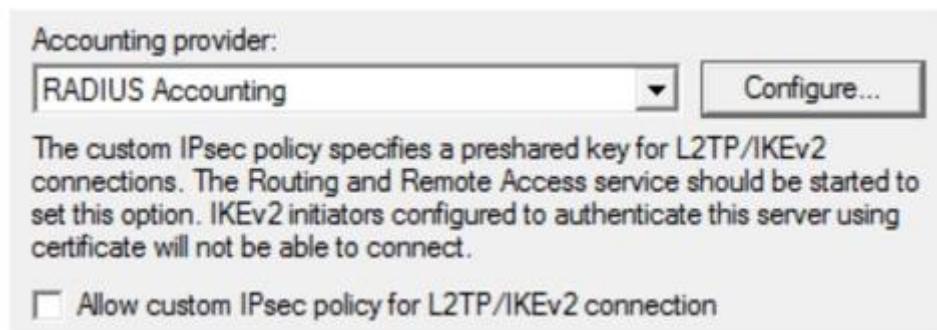
- In the Security tab, select RADIUS authentication method. Next, select Configure.



- 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.



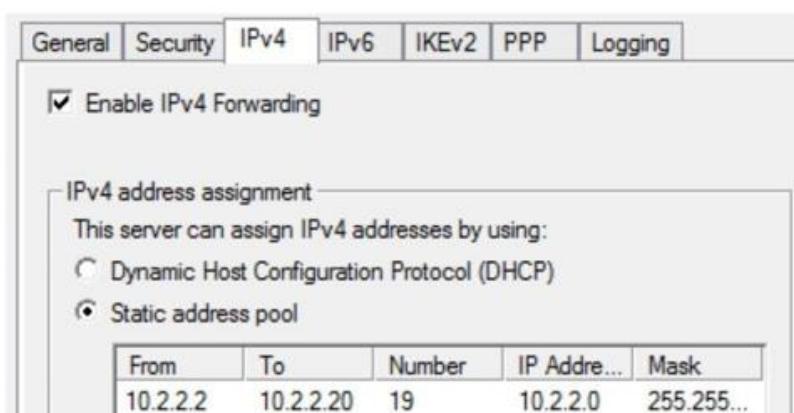
- Click OK to close the window.
- Similar settings for Accounting provider:



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



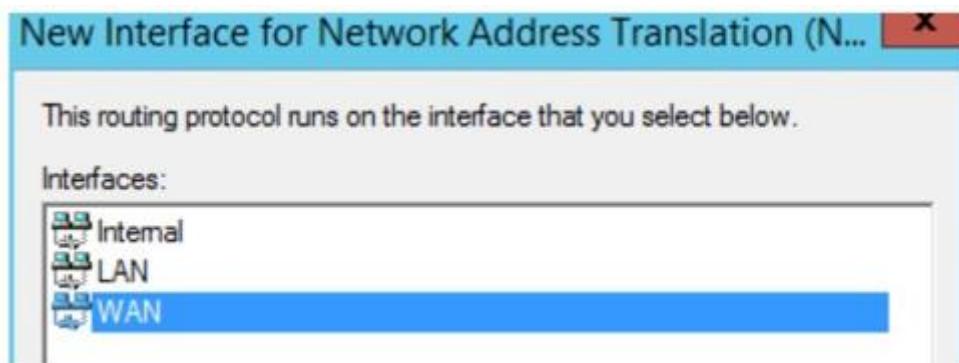
- Switch to IPv4 Tab
- Select Static address and enter the IP range that will be assigned to the workstation when connecting to VPN.



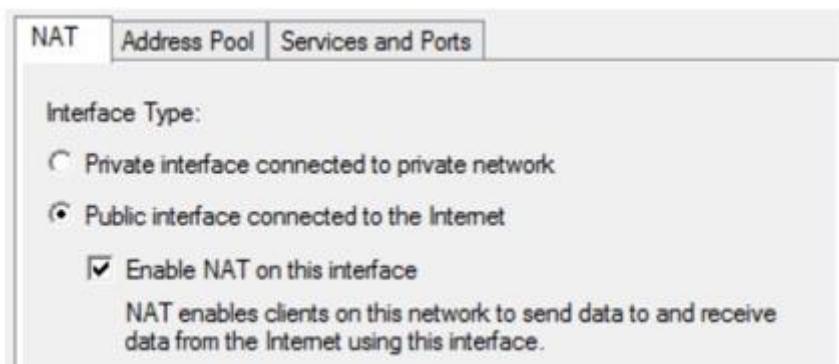
- Continue configuring NAT to allow workstations to access into the webserver in the DC server.



- 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):

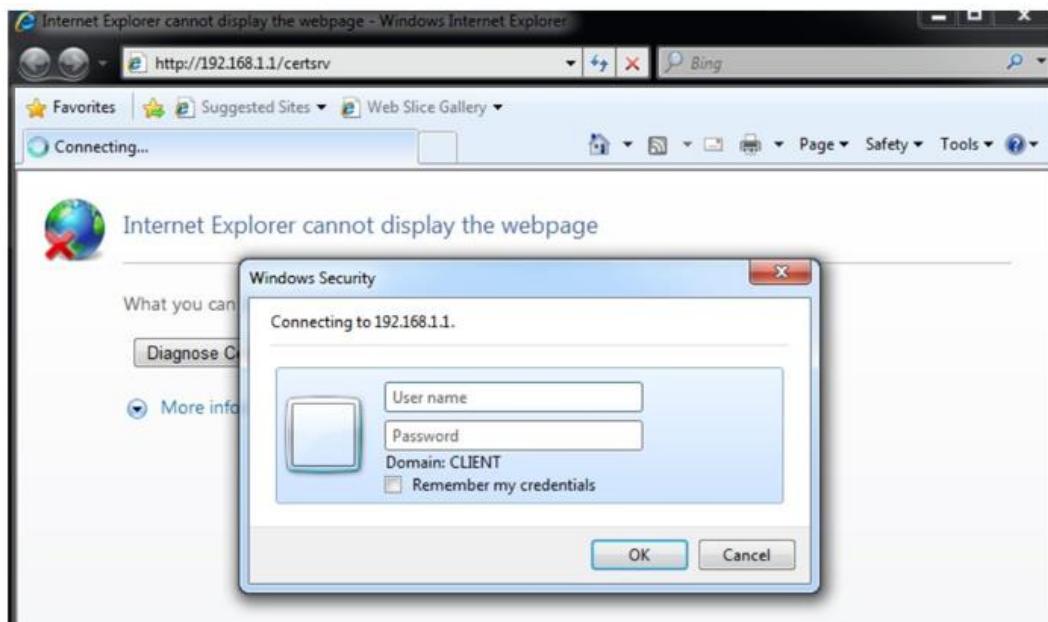


- The window that appears requires setting the IP address of the DC:

Incoming port:	<input type="text" value="80"/>
Private address:	<input type="text" value="172 . 16 . 1 . 2"/>
Outgoing port:	<input type="text" value="80"/>

## 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>

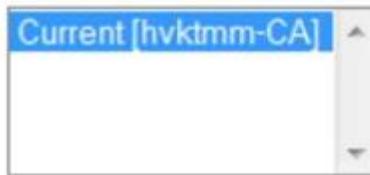


- Log in with the previously created account.

A screenshot of a Microsoft Active Directory Certificate Services page in Internet Explorer. The address bar shows "http://192.168.1.1/certsrv". The page title is "Microsoft Active Directory Certificate Services - hvktmm-CA". The main content area is titled "Welcome" and contains text about requesting certificates and managing certificate revocation lists. It includes a "Select a task:" section with links to "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

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

**CA certificate:**



**Encoding method:**

- DER  
 Base 64

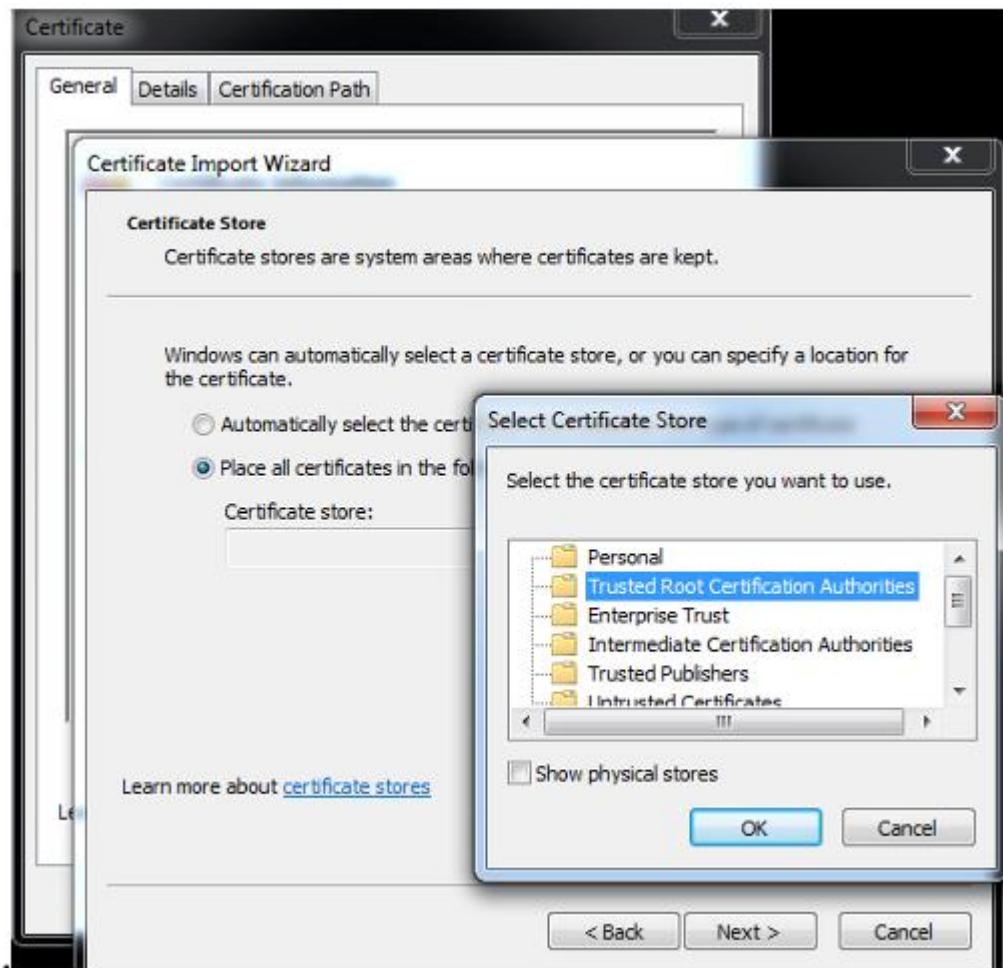
[Install CA certificate](#)

- [Download CA certificate](#)  
[Download CA certificate chain](#)  
[Download latest base CRL](#)  
[Download latest delta CRL](#)

- 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.

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]				
File	Action	View	Favorites	Window
Console Root				
Certificates (Local Computer)				
Personal				
Trusted Root Certification				
Certificates				
Enterprise Trust				
Intermediate Certification				
Trusted Publishers				
Untrusted Certificates				
Third-Party Root Certification				
Trusted People				
Certificate Enrollment Request				
Smart Card Trusted Roots				
Trusted Devices				
Issued To	Issued By	Expiration Date	Intended Purpose	
hvtm-CA	hvtm-CA	5/27/2025	<All>	
Class 3 Public Primary Certificate...	Class 3 Public Primary Certificate...	8/2/2028	Secure Email, C...	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Server Authent...	
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/14/2018	Secure Email, C...	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/1/2000	Secure Email, C...	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Author...	5/10/2021	<All>	
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/8/2004	Time Stamping	
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2021	Time Stamping	
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/17/2036	Server Authent...	

- 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.

View your basic network information and set up connections



ADMIN-PC  
(This computer)



Network 3



Internet

See full map

View your active networks



Network 3  
Public network

Access type: Internet  
Connections: Local Area Connection

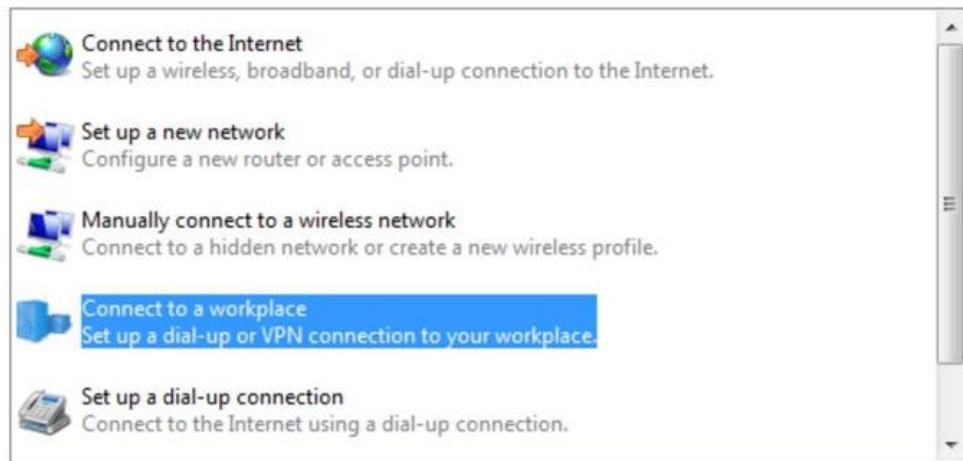
Connect or disconnect

Change your networking settings

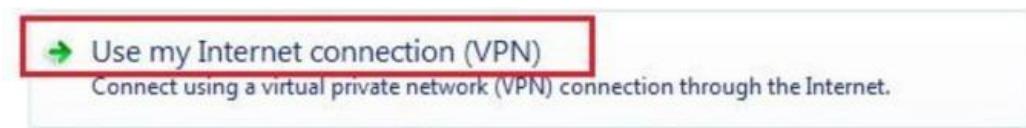
 Set up a new connection or network  
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

 Connect to a network  
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

- Next interface select Connect to a workplace.

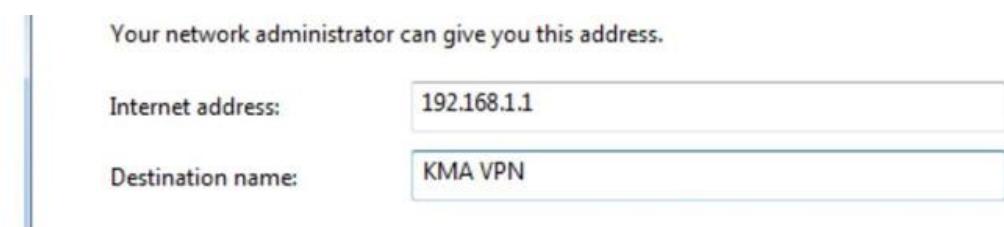


- Next interface select connection via VPN:

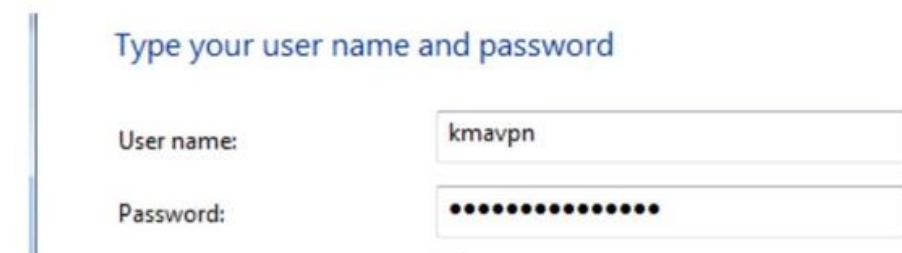


- Select I'll set up an Internet connection later.

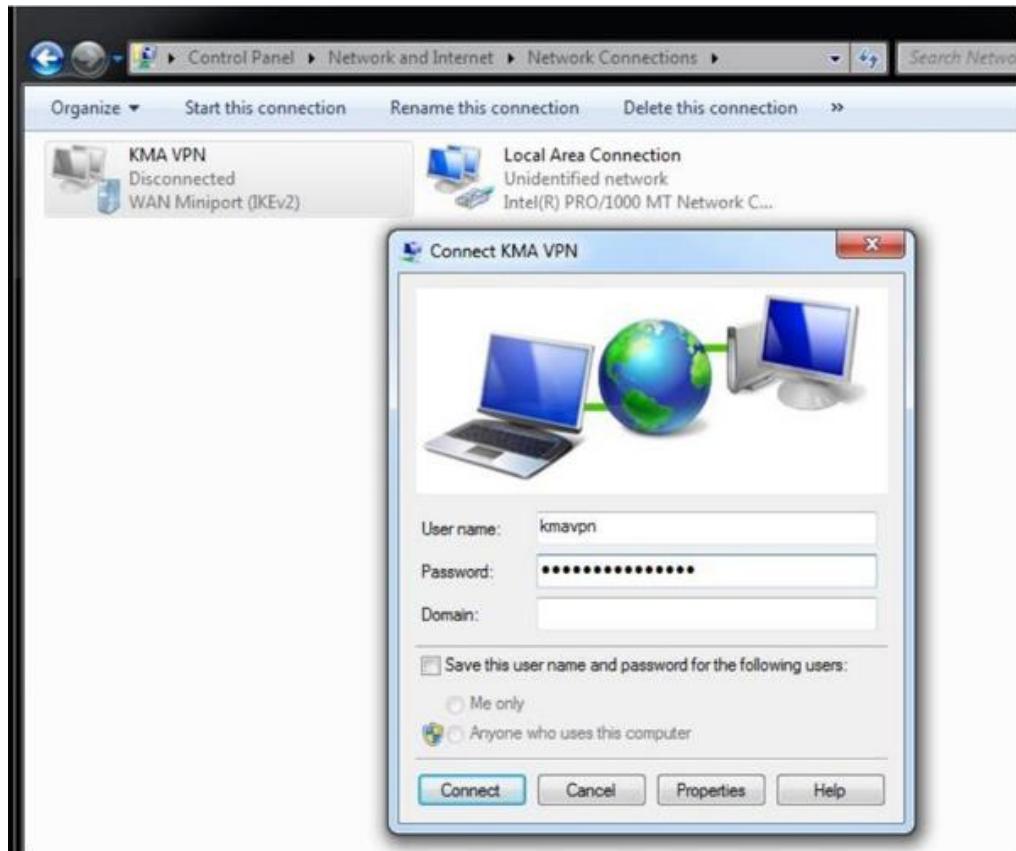
- The next interface enters the external IP address of the SRV (connect to Windows 7). Name the connection is:



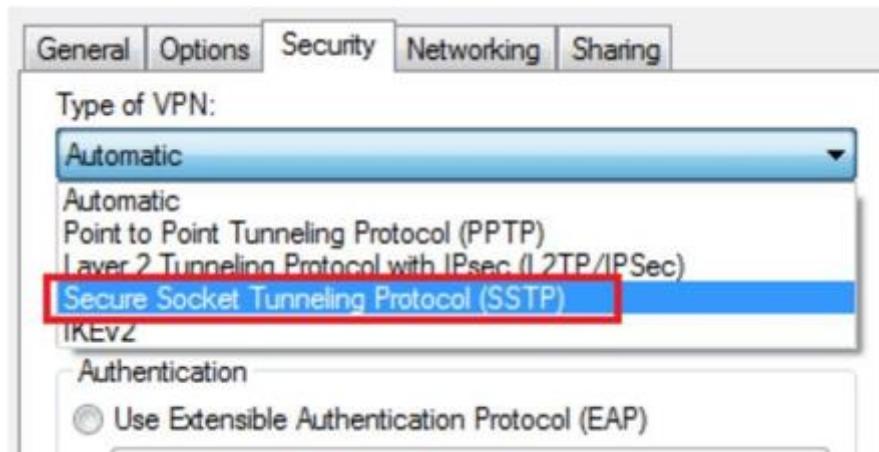
- Next step is to enter the account created on the DC server. Select Create to create the connection.



- 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
ab (Default)	REG_SZ	(value not set)
01 ListenerPort	REG_DWORD	0x00000000 (0)
01 NoCertRevocationCheck	REG_DWORD	0x00000001 (1)
ab ServerURI	REG_SZ	/sra_{BA195980-CD4
ab ServiceDLL	REG_EXPAND_SZ	%SystemRoot%\syst
01 ServiceDLLUnloadOnStop	REG_DWORD	0x00000001 (1)
01 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.