

HỌC VIỆN KỸ THUẬT MẬT MÃ  
**KHOA AN TOÀN THÔNG TIN**  
-----

MODULE THỰC HÀNH  
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 05.2

**TRIỂN KHAI DỊCH VỤ TRUY CẬP TỪ XA  
VPN SSTP TRÊN WINDOWS SERVER  
2012 R2**

Người xây dựng bài thực hành:

**ThS. Cao Minh Tuấn**

HÀ NỘI, 2015

## MỤC LỤC

<b>Mục lục .....</b>	<b>2</b>
<b>Thông tin chung về bài thực hành .....</b>	<b>3</b>
<b>Chuẩn bị bài thực hành .....</b>	<b>4</b>
Đối với giảng viên .....	4
Đối với sinh viên .....	4
<b>TRIỂN KHAI dịch vụ truy cập từ xa vpn sử dụng giao thức ssl và radius .....</b>	<b>5</b>
1.1. Chuẩn bị .....	5
1.2. Mô hình triển khai .....	5
1.3. Các bước thực hiện .....	5
1.4. Thực hiện trên máy chủ DC .....	6
1.4.1. Tạo người dùng cho phép truy cập từ xa thông qua VPN .....	6
1.4.2. Cài đặt dịch vụ Network Policy Server .....	8
1.4.3. Cấu hình Radius Server trong Network Policy Server .....	9
1.4.4. Cài đặt dịch vụ trung tâm chứng thực CA .....	15
1.4.5. Cấu hình CA để cấp phát chứng thư số cho máy chủ SRV .....	16
1.4.6. Cấp phát chứng thư số .....	18
1.5. Thực hiện trên máy chủ SRV .....	25
1.5.1. Cài đặt ứng dụng Routing and Remote Access .....	25
1.5.2. Cấu hình dịch vụ Routing and Remote Access .....	26
1.6. Thực hiện trên máy Windows 7 .....	32
1.7. Kiểm tra kết quả .....	36
<b>Phụ lục .....</b>	<b>38</b>

## **THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH**

**Tên bài thực hành:** Triển khai dịch vụ truy cập từ xa VPN

**Module:** Quản trị an toàn hệ thống

**Số lượng sinh viên cùng thực hiện:** 01

**Địa điểm thực hành:** Phòng máy

**Yêu cầu:**

- Yêu cầu phần cứng:
  - + Mỗi sinh viên được bố trí 01 máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 8GB, HDD 50GB
- Yêu cầu phần mềm trên máy:
  - + Hệ điều hành Windows 7. Server 2012
  - + VMware Workstation 9.0 trở lên
- Công cụ thực hành:
  - + Máy ảo VMware: Windows 7 SP1, Windows Server 2012. Trên mỗi máy ảo có ít nhất 02 phân vùng ổ cứng. Trong đó phân vùng C: chứa hệ điều hành, phân vùng D: có ít nhất 10 GB còn trống.
- Yêu cầu kết nối mạng LAN: không
- Yêu cầu kết nối mạng Internet: không
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

**Công cụ được cung cấp cùng tài liệu này:**

- 
-

## **CHUẨN BỊ BÀI THỰC HÀNH**

### **Đối với giảng viên**

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

### **Đối với sinh viên**

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

# TRIỂN KHAI DỊCH VỤ TRUY CẬP TỪ XA VPN SỬ DỤNG GIAO THỨC SSL VÀ RADIUS

## 1.1. Mô tả

Khi người dùng có yêu cầu kết nối từ xa tới hệ thống mạng nội bộ bên trong để truy cập dữ liệu thì cần phải đảm bảo an toàn dữ liệu truyền trên mạng tránh kẻ tấn công có thể chặn bắt, nghe lén, độc trộm nội dung dữ liệu.

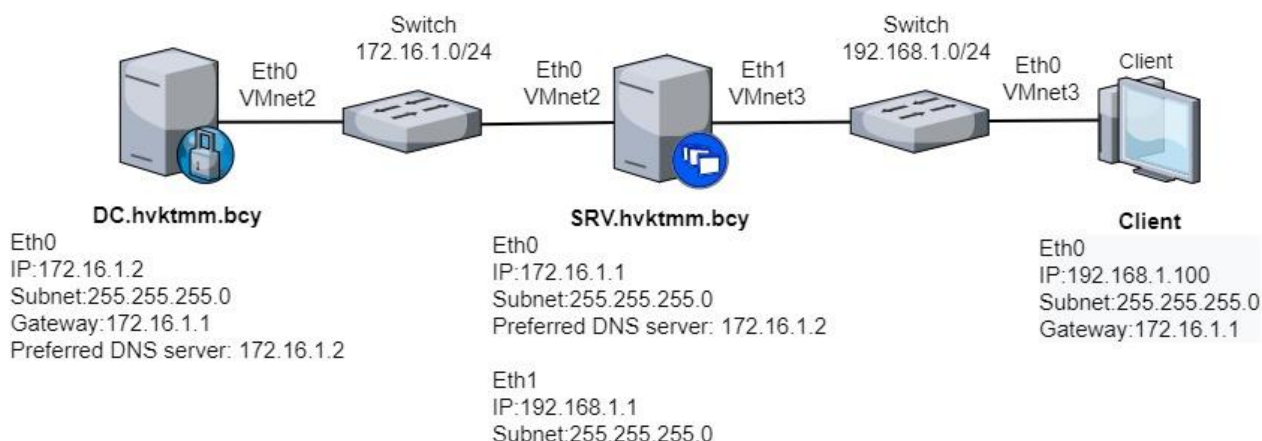
Triển khai công nghệ mạng riêng ảo VPN trên máy chủ Windows Server 2012 sử dụng giao thức bảo mật SSL/TLS kết hợp với giao thức xác thực RADIUS. Với giao thức này chỉ người dùng có tài khoản trong máy chủ Active Directory mới truy cập được.

## 1.2. Chuẩn bị

– Máy ảo chạy hệ điều hành Windows 7 có kết nối vào Lan Segment (Switch ảo của VMware) đã thiết lập.

– Máy ảo chạy hệ điều hành Windows Server 2012 kết nối cùng với Lan Segment với Windows 7.

## 1.3. Mô hình triển khai



## 1.4. Các bước thực hiện

### 1.4.1. Thực hiện trên máy chủ DC:

- Nâng cấp máy chủ DC
- Tạo người dùng cho phép truy cập từ xa
- Cài đặt, cấu hình Network Policy Service làm Radius Server
- Cài đặt trung tâm chứng thực CA
- Cấp phát chứng thư số có khóa bí mật cho máy chủ SRV làm VPN

### 1.4.2. Thực hiện trên máy chủ SRV:

- Cài đặt dịch vụ Routing and Remote Access
- Cấu hình xác thực sử dụng Radius Client kết nối với DC.
- Cài đặt chứng thư số được cấp phát từ DC.

#### 1.4.3. Thực hiện trên máy trạm Windows 7:

- Truy cập vào DC thông qua SRV để xin chứng thư số của CA.
- Tạo kết nối mạng VPN
- Cấu hình sử dụng SSTP
- Kết nối với tài khoản đã tạo trên DC
- Kiểm tra kết quả

### 1.5. Thiết lập địa chỉ IP cho các máy

#### 1.5.1. Trên DC

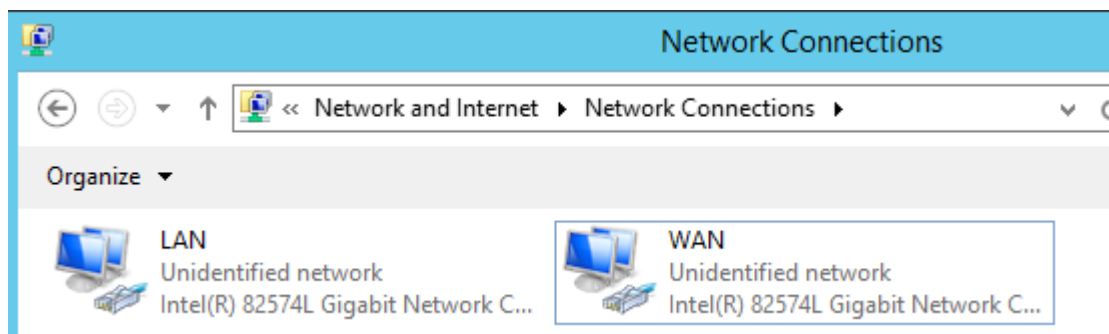
- Đổi tên máy thành DC
- Thiết lập mật khẩu cho user Administrator
- Thiết lập địa chỉ IP tĩnh theo mô hình triển khai

The screenshot shows the 'Network Settings' window for a static IP configuration. The 'Use the following IP address' option is selected. The IP address is set to 172.16.1.2, the Subnet mask is 255.255.255.0, and the Default gateway is 172.16.1.1. The 'Use the following DNS server addresses' option is also selected. The Preferred DNS server is 172.16.1.2, and the Alternate DNS server is left blank.

Obtain an IP address automatically	<input type="radio"/>
Use the following IP address:	<input checked="" type="radio"/>
IP address:	172 . 16 . 1 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	172 . 16 . 1 . 1
Obtain DNS server address automatically	<input type="radio"/>
Use the following DNS server addresses:	<input checked="" type="radio"/>
Preferred DNS server:	172 . 16 . 1 . 2
Alternate DNS server:	. . .

#### 1.5.2. Trên SRV

- Đổi tên máy thành SRV
- Thiết lập mật khẩu cho user Administrator
- Đổi tên card Eth0 thành LAN và Eth1 thành WAN



- Thiết lập địa chỉ IP tĩnh theo mô hình triển khai
- IP của card LAN

☒ Use the following IP address:

IP address: 172 . 16 . 1 . 1  
 Subnet mask: 255 . 255 . 255 . 0  
 Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 1 . 2  
 Alternate DNS server: . . .

- IP của card WAN

☐ 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. Trên Client

- Đổi tên máy thành Client
- Thiết lập địa chỉ IP tĩnh theo mô hình triển khai

☐ 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. Kiểm tra

- Để dễ dàng hơn trong việc thực hiện bài lab, chúng ta nên tắt tường

lừa trên cả 3 máy DC, SRV, Client.

- Đảm bảo rằng có thể ping được giữa SRV – DC và từ SRV – Client

```
C:\Users\Administrator>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time=1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 192.168.1.100

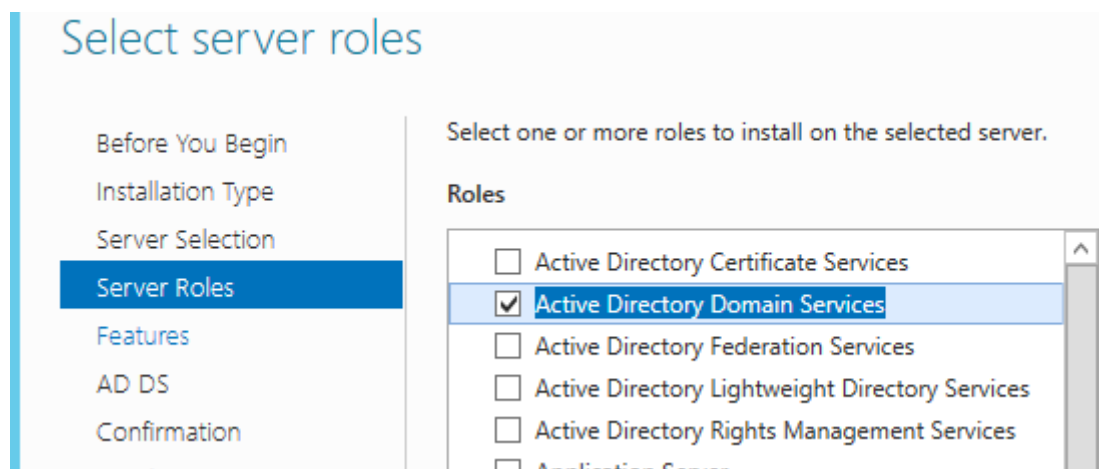
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## 1.6. Thực hiện trên máy chủ DC

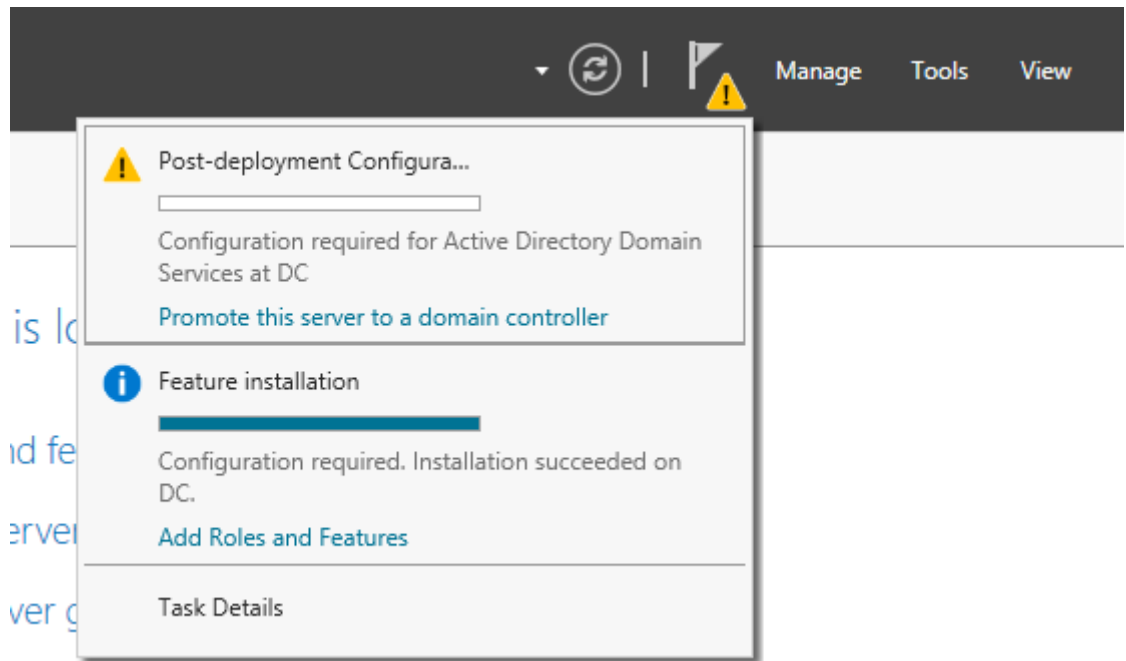
### 1.6.1. Nâng cấp Win 2012 lên Domain Controller (DC)

- Truy cập theo đường dẫn: Server Manager → Manage → Add Roles and Feature.
- Chọn Next theo mặc định tới cửa sổ Server Roles tích chọn Active Directory Domain Services

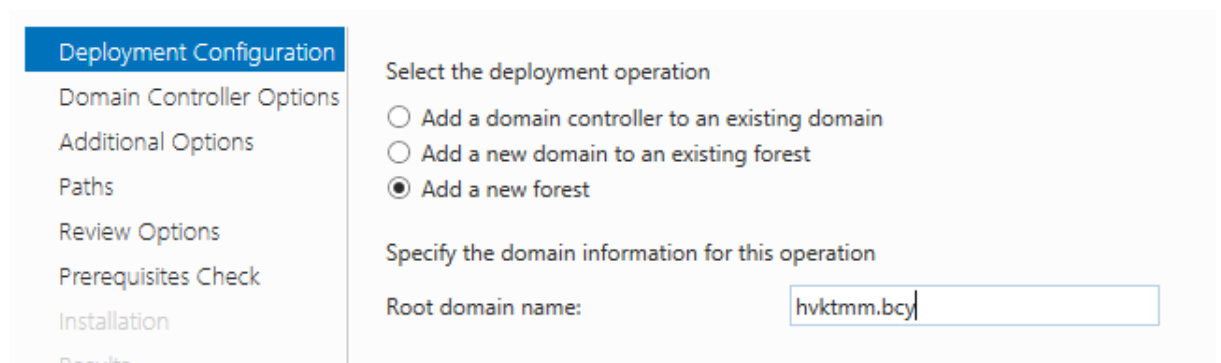


- Tiếp tục Next theo mặc định và chọn Install để cài đặt.
- Sau khi quá trình cài đặt hoàn tất, chọn Promote this server to a domain controller.

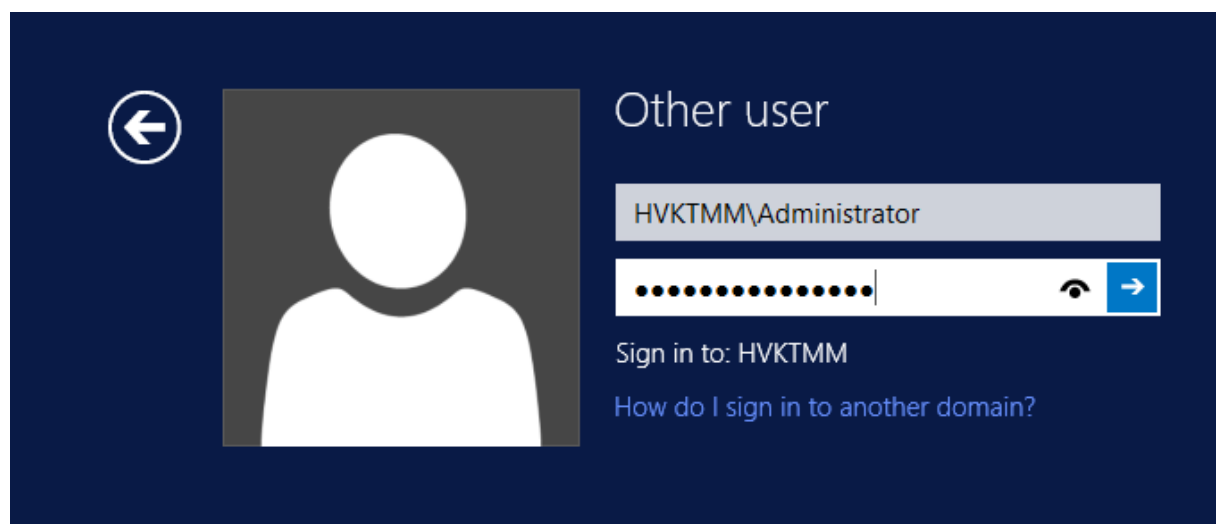




– Chọn Add a new forest. Tại mục Root domain name đặt tên domain name



– Tiếp tục chọn Next theo mặc định và Install để nâng cấp lên thành DC. Máy chủ DC sẽ tự khởi động lại sau khi nâng cấp hoàn tất. Tài khoản đăng nhập bây giờ sẽ có dạng DOMAIN\user như hình dưới.



#### 1.6.2. Tạo người dùng cho phép truy cập từ xa thông qua VPN

- Truy cập theo đường dẫn: Server Manager → Tools → Active Directory User and Computer.
- Phải chuột vào thư mục Users → New → User.
- Đặt tên người dùng cho phép truy cập từ xa là: **kmavpn**

Create in: hvktmm.bcy/Users

First name: kmavpn Initials:

Last name:

Full name: kmavpn

User logon name: kmavpn @hvktmm.bcy

User logon name (pre-Windows 2000): HVKTMM\ kmavpn

- Giao diện tiếp theo đặt mật khẩu cho người dùng. Chú ý mật khẩu ở đây phải đạt mức phức tạp.

Create in: hvktmm.bcy/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

- Nhấn Next và Finish để kết thúc quá trình tạo người dùng.
- Bước tiếp theo cấu hình để người dùng này được phép truy cập từ xa.
- Chuột phải vào người dùng chọn Properties, chọn Tab Dial-in →

Remote control		Remote Desktop Services Profile		COM+	
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Network Access Permission

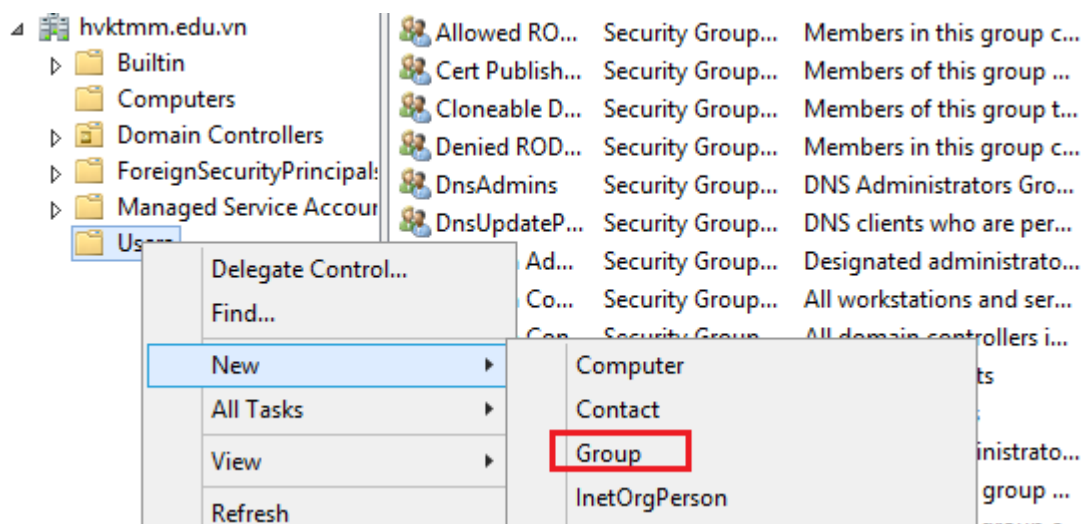
☒ Allow access

☐ Deny access

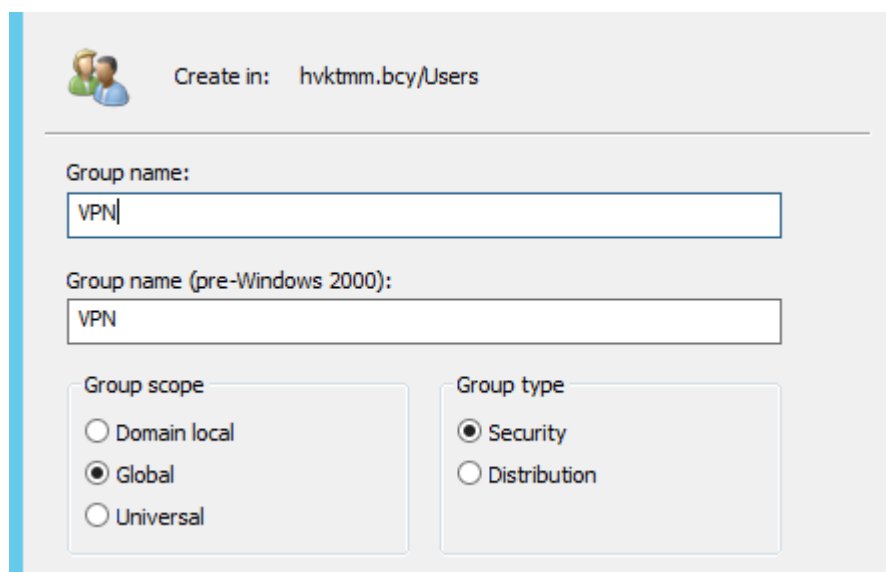
☐ Control access through NPS Network Policy

Allow access.

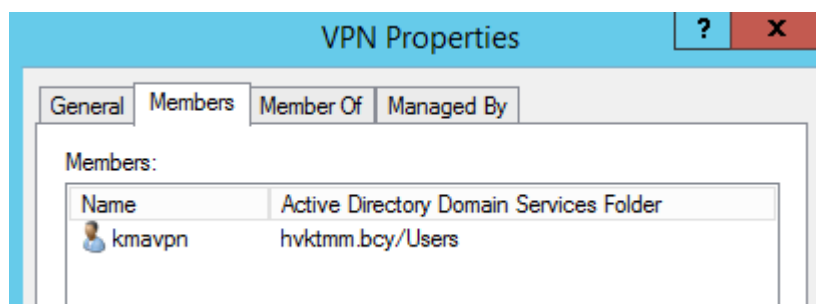
- Nhấn Apply → OK để kết thúc.
- Tạo nhóm **VPN** và thêm người dùng này vào nhóm.



- Đặt tên nhóm là **VPN**



- Thêm người dùng vào nhóm VPN:

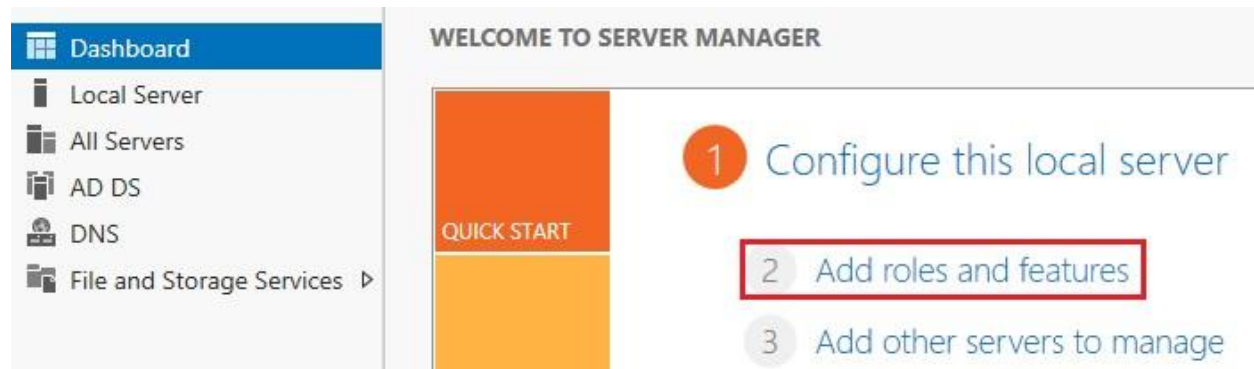


- Kết thúc bước tạo người dùng truy cập từ xa.

### 1.6.3. Cài đặt dịch vụ Network Policy Server

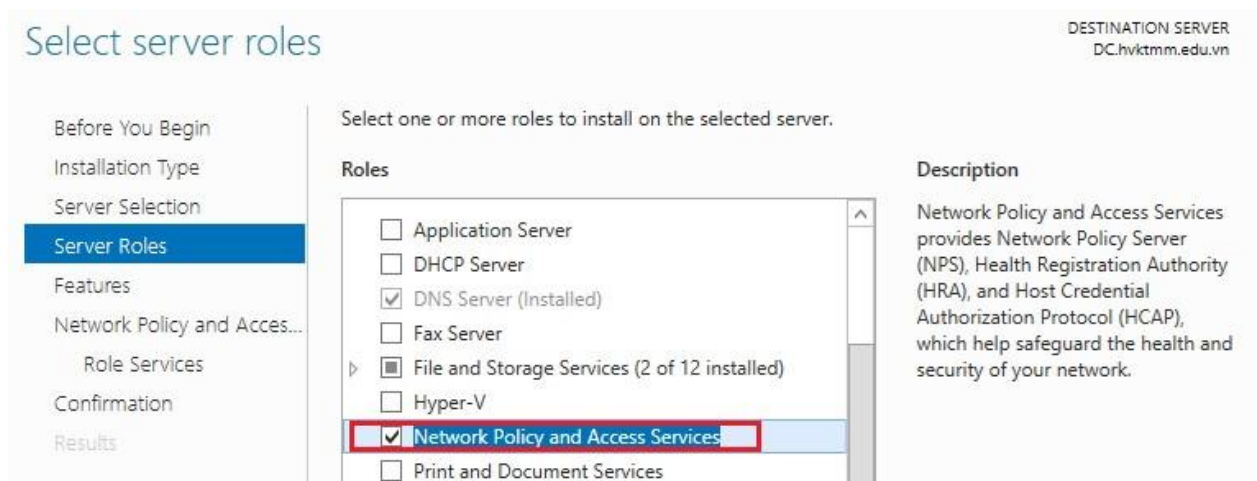
- Truy cập theo đường dẫn:

- Server Manager → Dashboard → Add roles and features

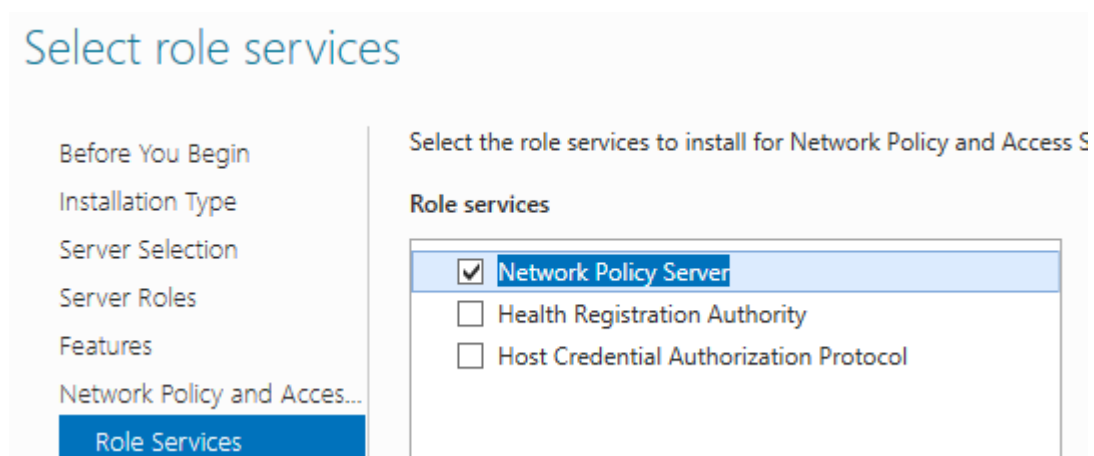


- Ba bước đầu tiên để mặc định và chọn Next.

- Tại bước lựa chọn vai trò (Select server roles): Chọn Network Policy and Access Services:



- Chọn Next để tiếp tục.
- Các lựa chọn tiếp theo để mặc định.
- Giao diện lựa chọn dịch vụ chọn: Network Policy Server.

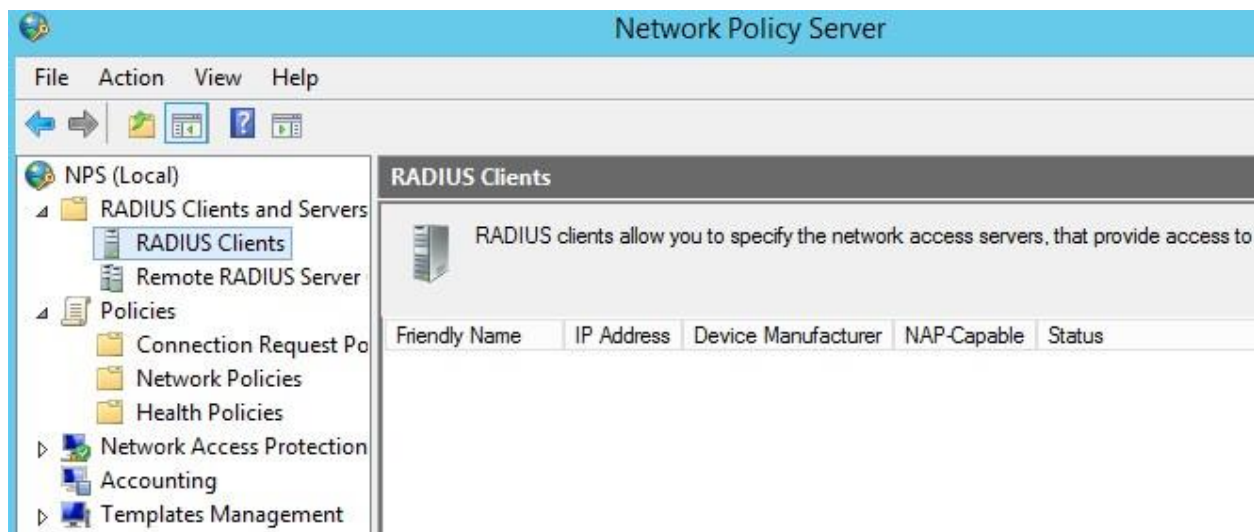


- Nhấn Next và Install để cài đặt dịch vụ.

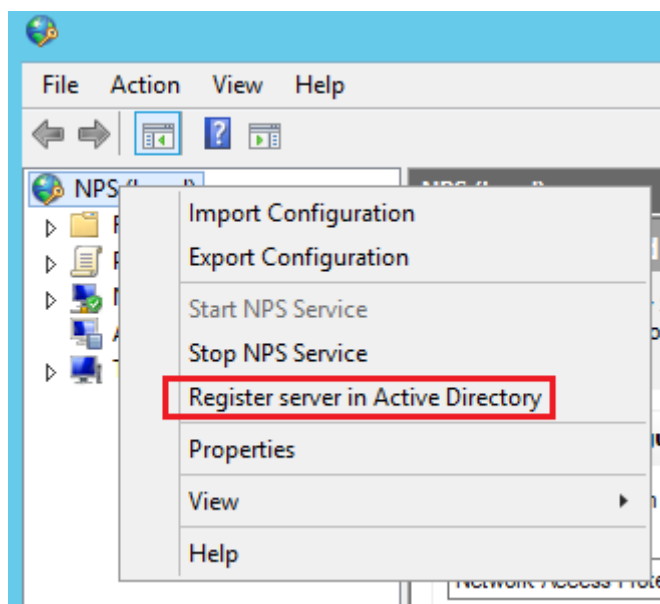
#### 1.6.4. Cấu hình Radius Server trong Network Policy Server

- Truy cập Network Policy Server theo đường dẫn: Server Manager

→ Tools → Network Policy Server: Giao diện như sau:

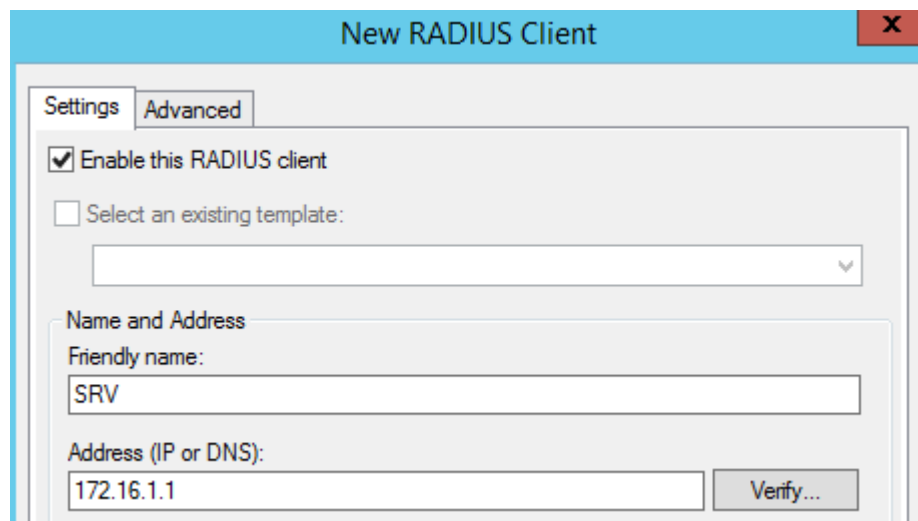


– Chuột phải vào NPS để đăng ký dịch vụ trong Active Directory:

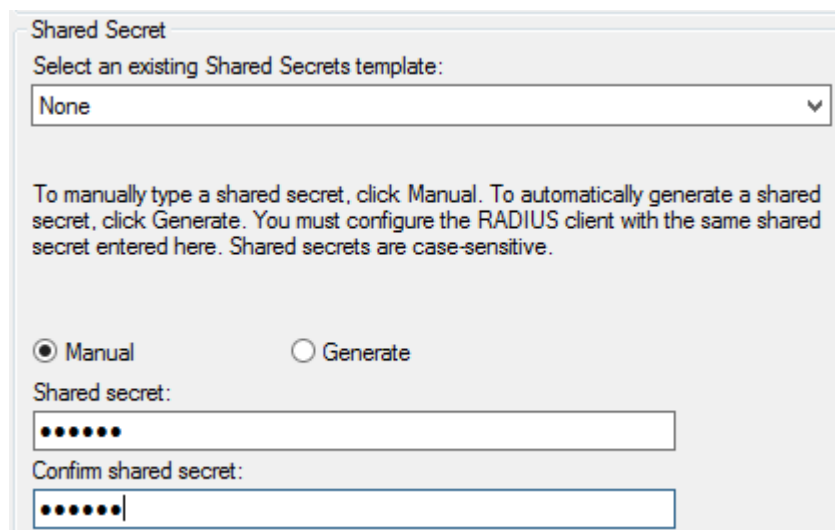


– Đầu tiên phải cấu hình định nghĩa máy Radius Client chính là máy SRV. Chuột phải vào mục Radius Clients chọn New:

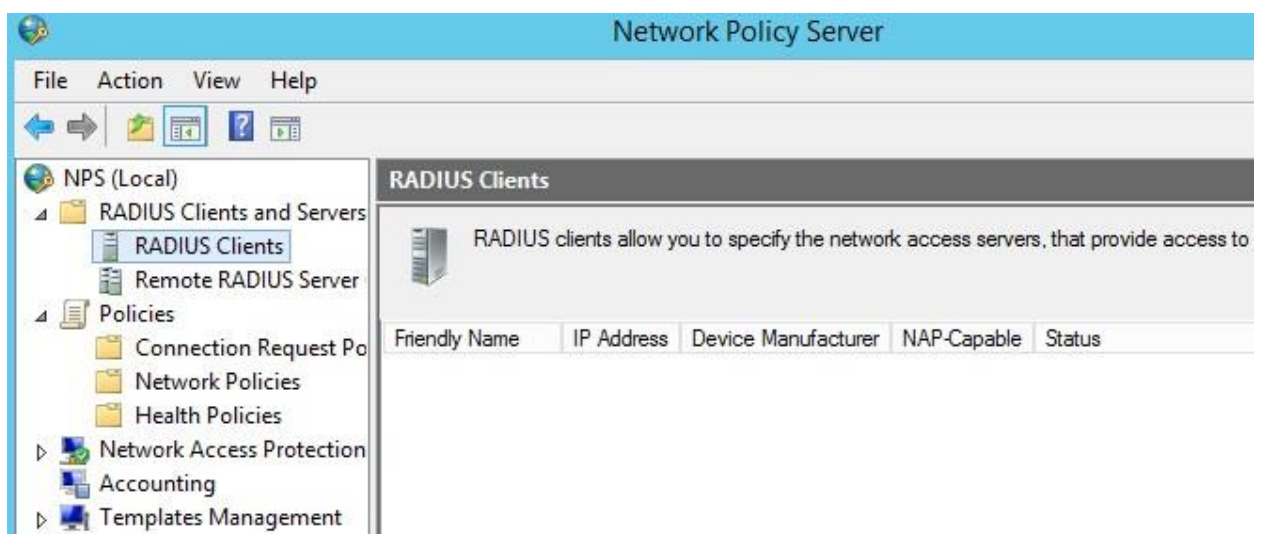
– Giao diện xuất hiện nhập thông tin của máy chủ SRV:



- Nhập tên và địa chỉ IP của máy SRV.
- Phần Shared Secret: Khóa bí mật chia sẻ giữa 2 máy. Khóa bí mật này 2 máy phải nhập giống nhau.

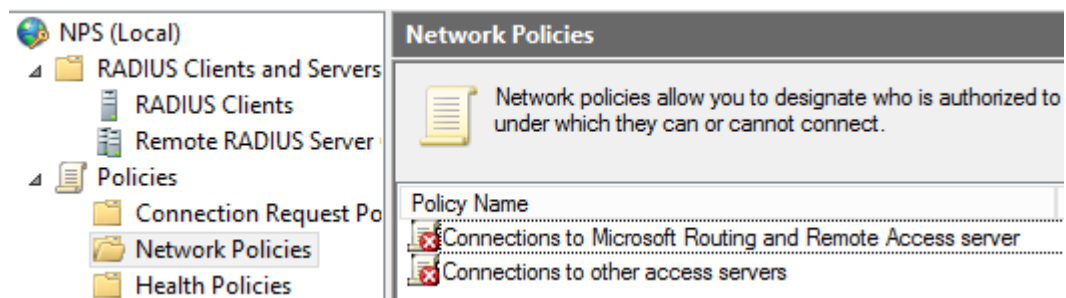


- Chọn OK để kết thúc.



- Tiếp theo cần phải định nghĩa chính sách xác thực.

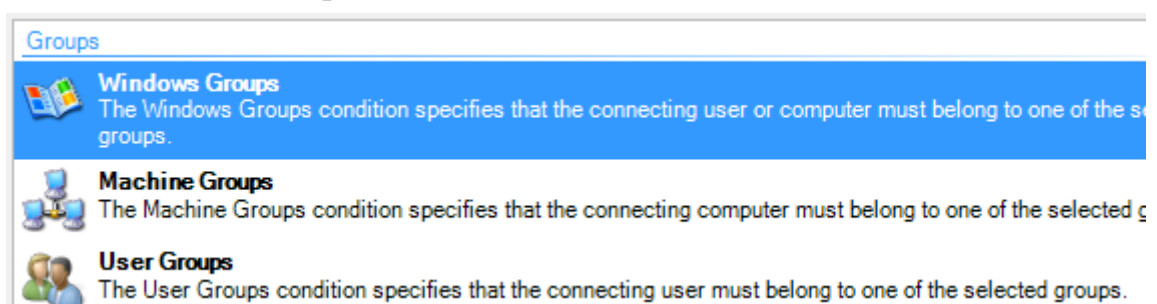
- Truy cập vào mục Policies → Network Policies. Giao diện như sau:



- Xóa 2 chính sách mặc định đã có. Và tạo chính sách mới. Chuột phải vào Network Policies → New

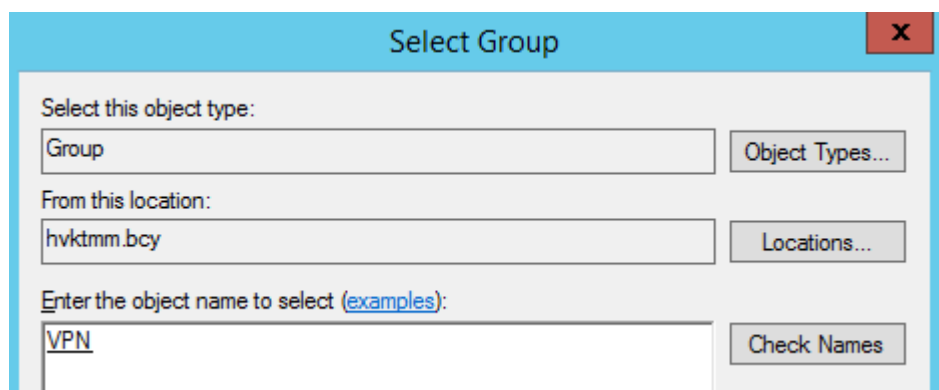
- Mục Policy name đặt tên là VPN.
- Mục Type of network access server: chọn Remote Access Server

- Chọn Next để tiếp tục.
- Mục điều kiện (Conditions): Chọn Add để thêm: Giao diện xuất hiện chọn Windows Groups:



- Chọn Add Group để thêm nhóm:
- Trở tới nhóm VPN đã tạo ở bước trên:





Select Group

Select this object type:

Group

Object Types...

From this location:

hvkttmm.bcy

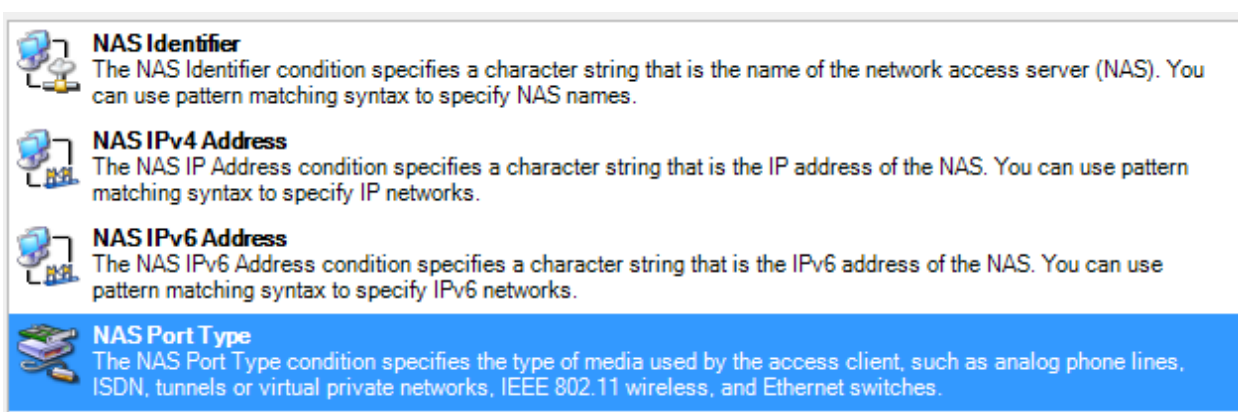
Locations...

Enter the object name to select (examples):

VPN

Check Names

- Nhấn OK → OK để tiếp tục.
- Vẫn trong giao diện Conditions tiếp tục chọn Add để thêm điều kiện khác. Giao diện select condition xuất hiện tìm đến và chọn NAS PortType:



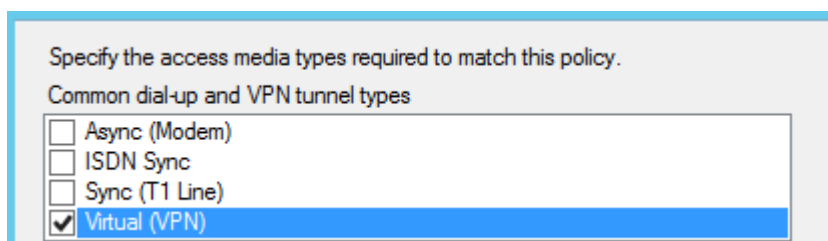
**NAS Identifier**  
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

**NAS IPv4 Address**  
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

**NAS IPv6 Address**  
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.

**NAS Port Type**  
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

- Chọn Add để xuất hiện bảng lựa chọn dịch vụ. Tích chọn Virtual (VPN)



Specify the access media types required to match this policy.

Common dial-up and VPN tunnel types

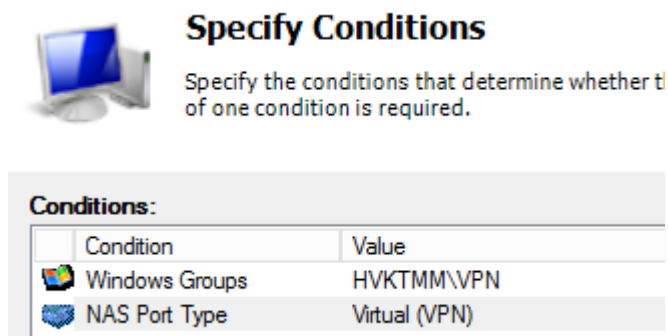
☐ Async (Modem)

☐ ISDN Sync

☐ Sync (T1 Line)

☒ Virtual (VPN)

- Chọn OK để kết thúc.
- Lúc này giao diện chính sẽ có 2 điều kiện đã được định nghĩa.



**Specify Conditions**

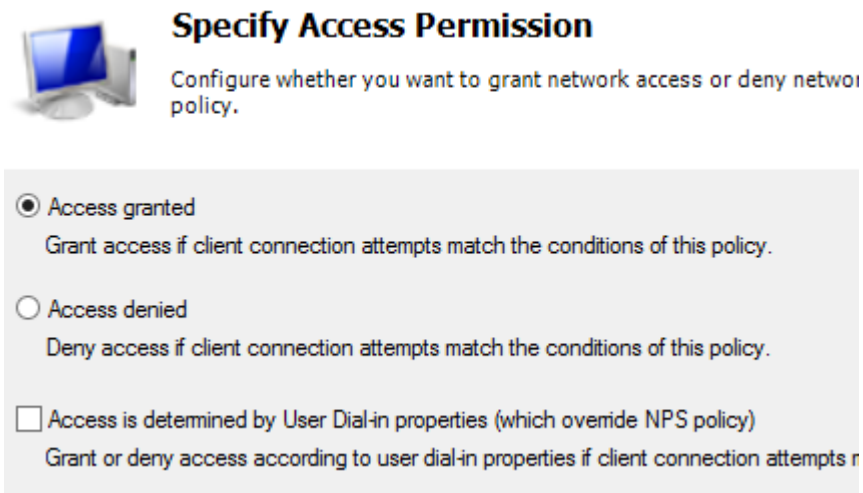
Specify the conditions that determine whether the policy is required.

**Conditions:**

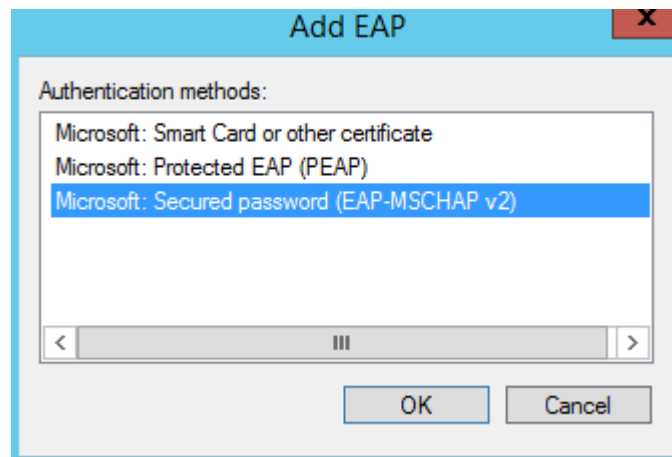
Condition	Value
Windows Groups	HVKTMM\VPN
NAS Port Type	Virtual (VPN)



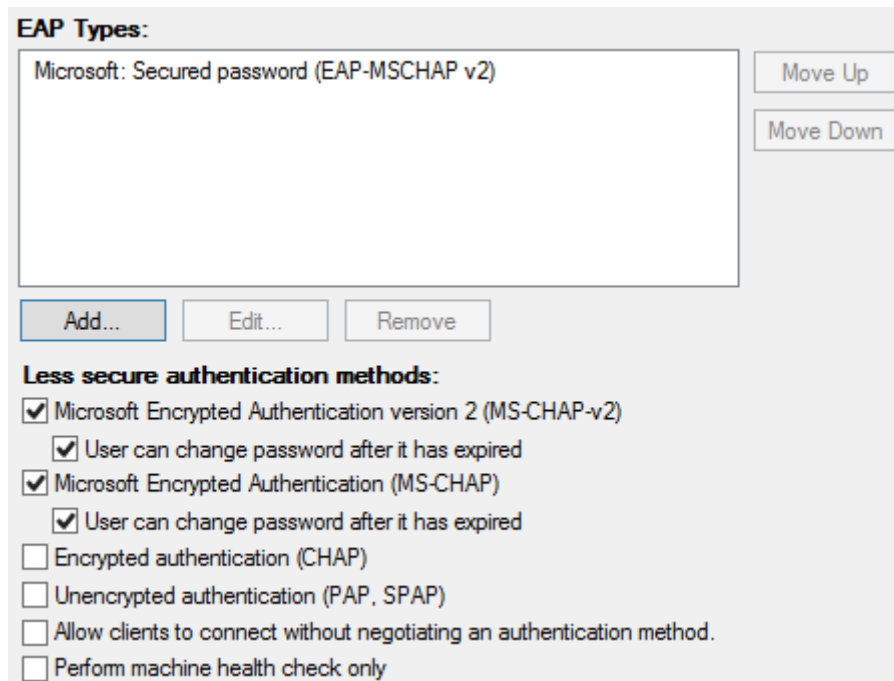
- Chọn Next để tiếp tục.
- Giao diện tiếp theo chọn quyền truy cập: chọn Access granted



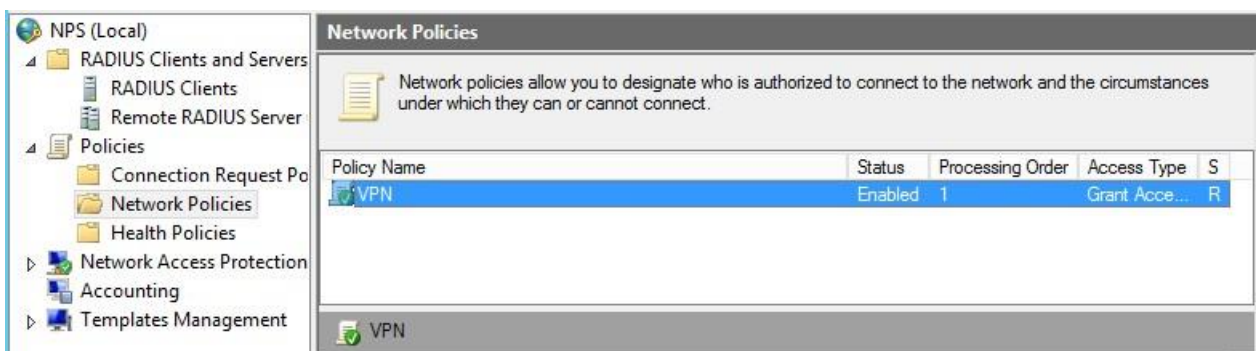
- Chọn Next để tiếp tục.
- Giao diện tiếp theo chọn giao thức xác thực.
- Trong mục EAP type chọn Add: Giao diện xuất hiện chọn Secured password



- Chọn OK để tiếp tục.
- Giao diện sau khi cấu hình.

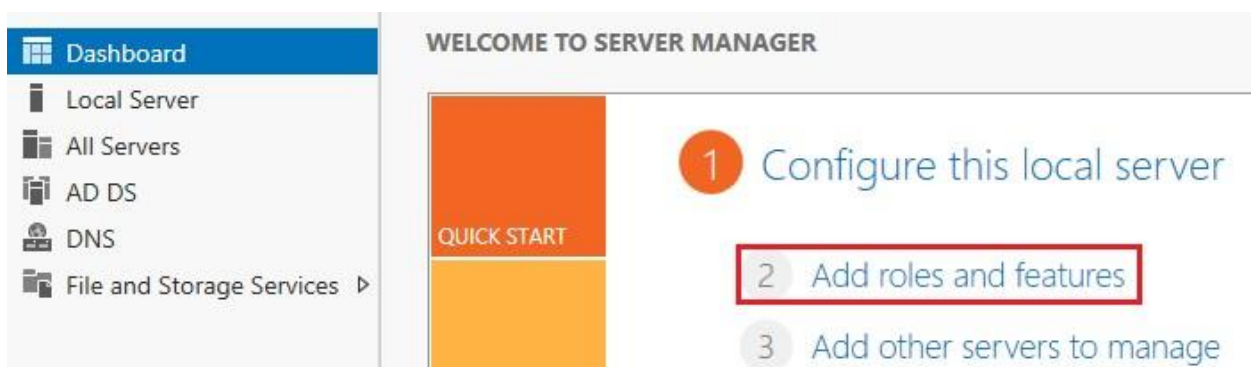


- Các giao diện tiếp thể để mặc định. Chọn Finish để kết thúc.

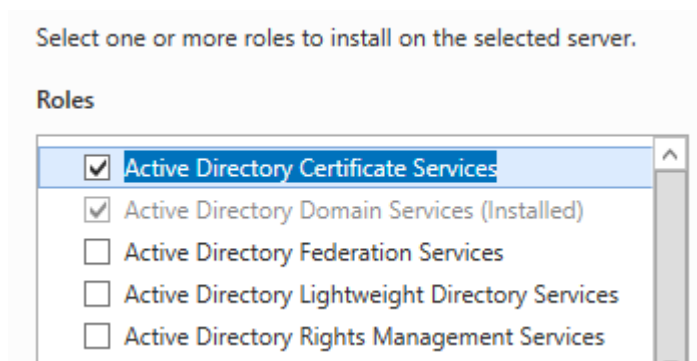


#### 1.6.5. Cài đặt dịch vụ trung tâm chứng thực CA.

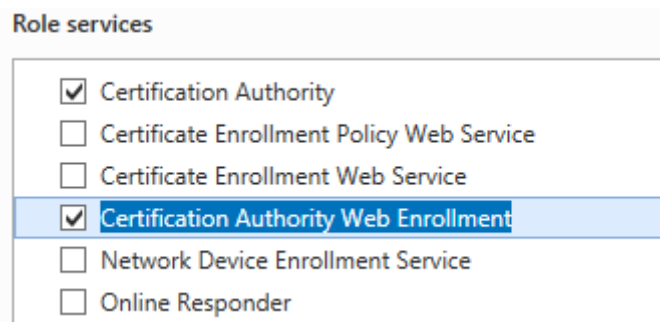
- Truy cập theo đường dẫn:
- Server Manager → Dashboard → Add roles and features



- Ba bước đầu tiên để mặc định và chọn Next.
- Tại bước lựa chọn vai trò (Select server roles): Chọn Active Directory Certificate Services.



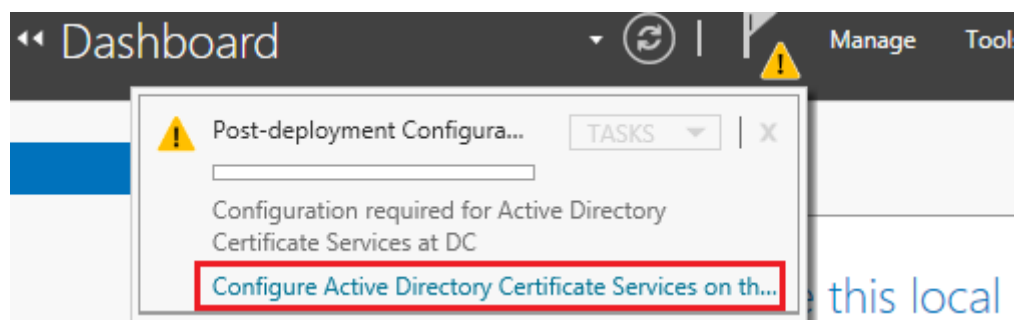
- Các bước tiếp theo chọn Next.
- Đến giao diện Select roles services: Tích 2 tùy chọn như hình sau.



Các bước tiếp theo để mặc định và chọn Install để cài đặt.

#### 1.6.6. Cấu hình CA để cấp phát chứng thư số cho máy chủ SRV

- Sau khi cài đặt dịch vụ trong giao diện Dashboard. Góc trên bên cạnh lá cờ có mục cảnh báo. Trong mục cảnh báo này hệ thống yêu cầu



cấu hình CA.

- Giao diện cấu hình CA xuất hiện

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...

- Chọn Next để tiếp tục.
- Giao diện tiếp theo chọn 2 tùy chọn như hình sau:

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

- Giao diện tiếp theo chọn 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 or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

- Chọn Next để tiếp tục:
- Mục CA Type chọn: Root CA
- Mục khóa bí mật Private key: Chọn Create a new private key Chọn hệ mật và độ dài khóa.

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

– Giao diện tiếp theo đặt tên cho 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


– Thời gian để mặc định 5 năm.


– Các giao diện tiếp theo để mặc định, chọn Configure để cấu hình CA. Cấu hình hoàn tất:

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

^ **Active Directory Certificate Services**

---

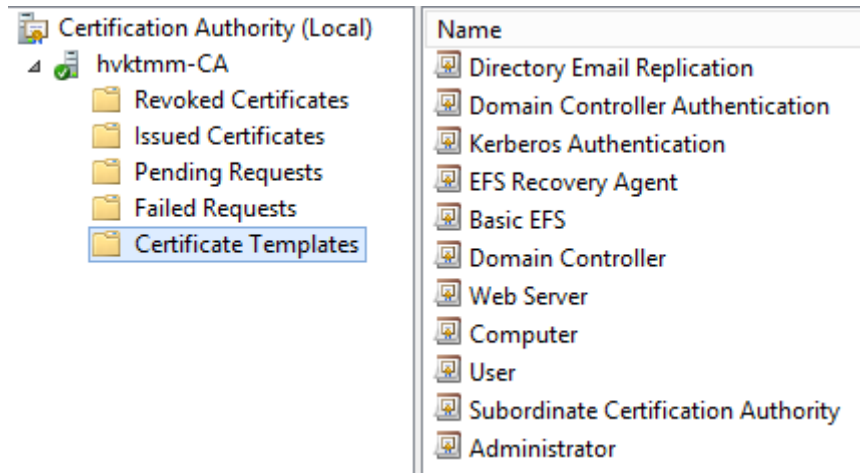
**Certification Authority**       **Configuration succeeded**  
[More about CA Configuration](#)

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

– Nhấn Close để đóng cửa sổ hoàn tất cấu hình.

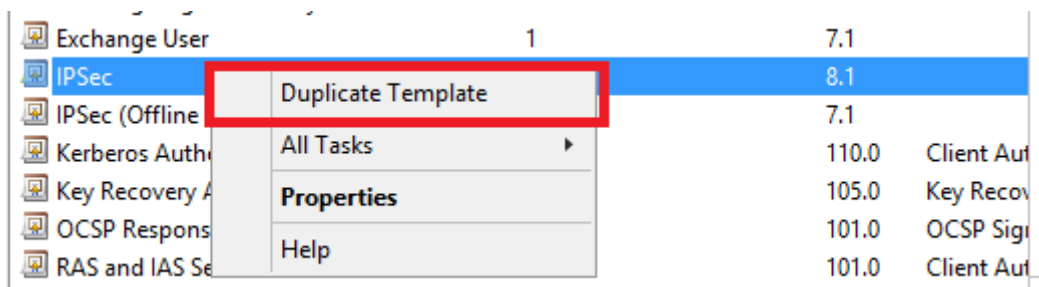
### 1.6.7. Tạo Templates

- Truy cập theo đường dẫn để mở giao diện quản lý CA: Server Manager → Tools → Certification Authority → Certificate

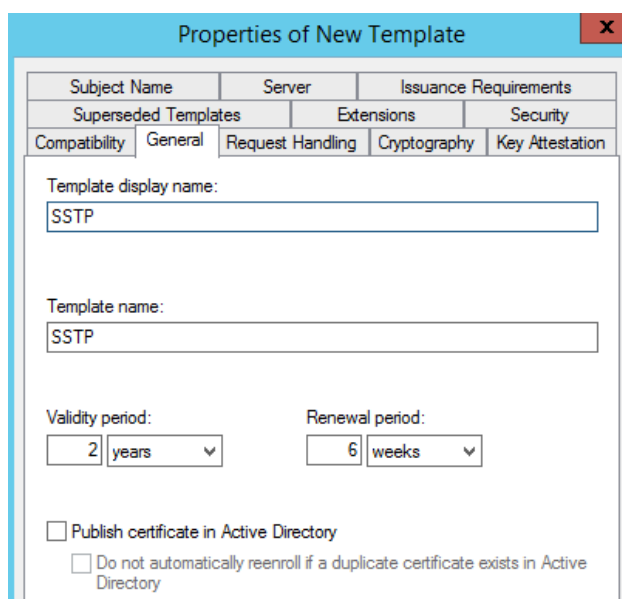


Templates.

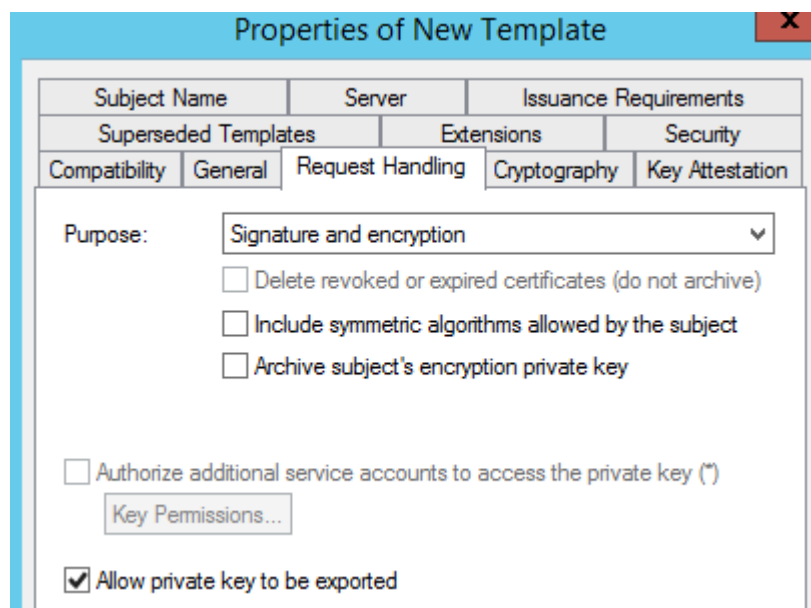
- Chuột phải vào mục Certificate Templates → Manage. Tìm đến template cho IPsec. Nháy chuột phải vào chọn Duplicate Template.



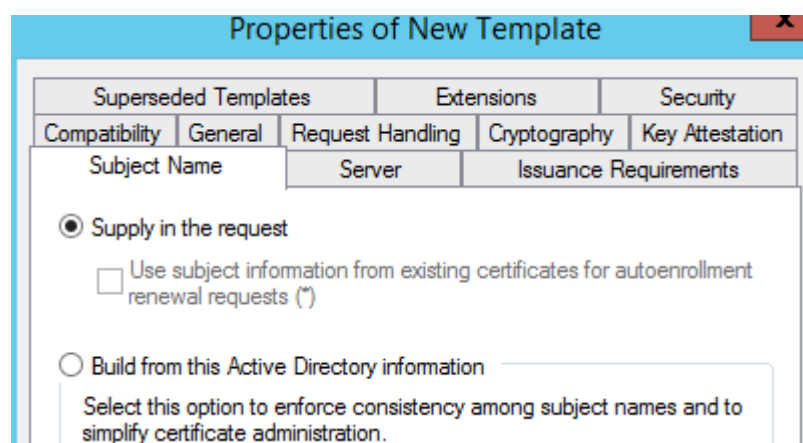
- Trong cửa sổ mới xuất hiện chọn tab General. Tại mục Template display name sửa thành SSTP



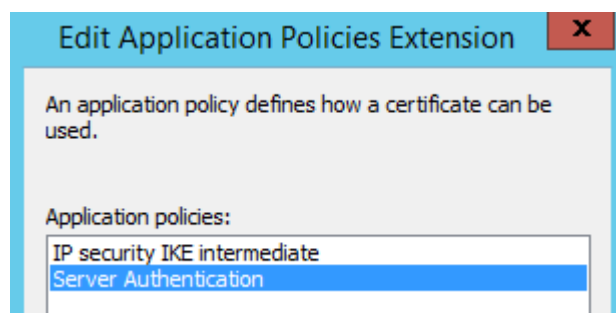
- Tab Request Handling chọn Allow private key to be exported



– Tab Subject Name chọn Supply in the request

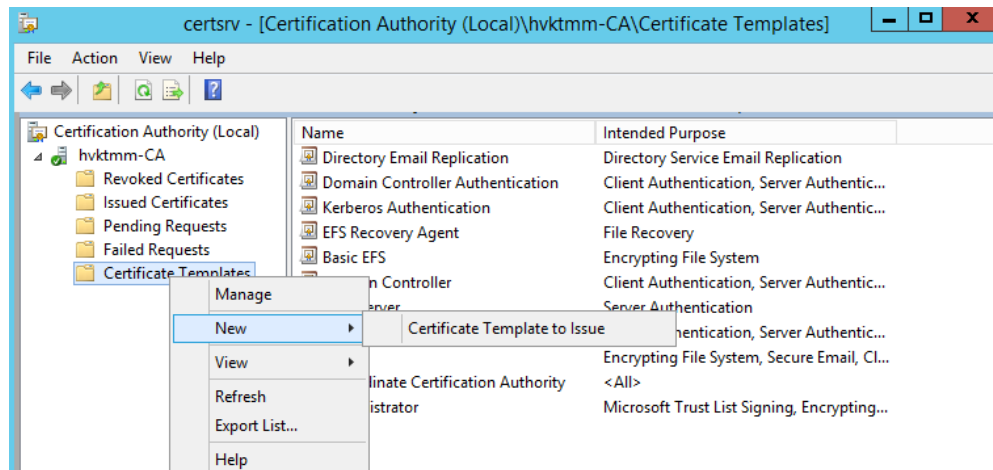


– Tab Extensions chọn Edit → Add rồi chọn Server Authentication



– Sau đó Apply → OK để hoàn tất quá trình tạo ra Templates mới.

– Sau đó, chuột phải vào Certificate Templates → New → Certificate Template to Issue như hình.

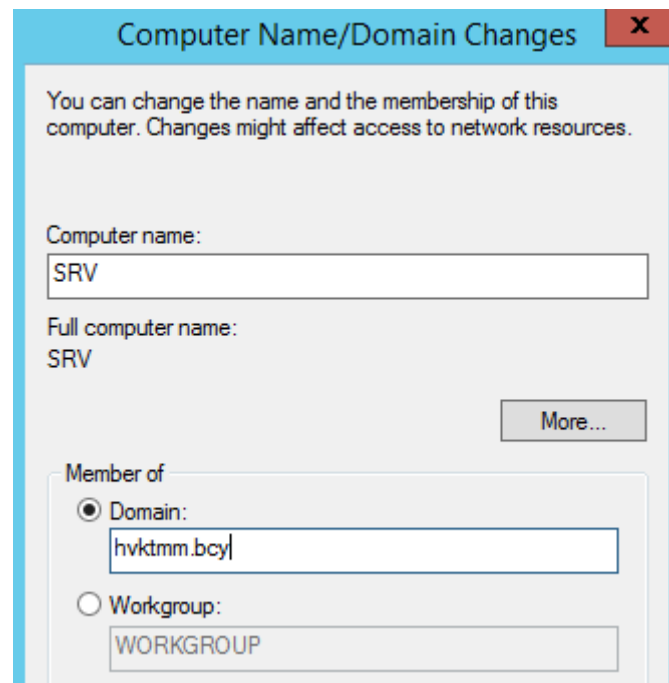


– Chọn tới Template SSTP vừa tạo rồi OK.

## 1.7. Thực hiện trên máy chủ SRV

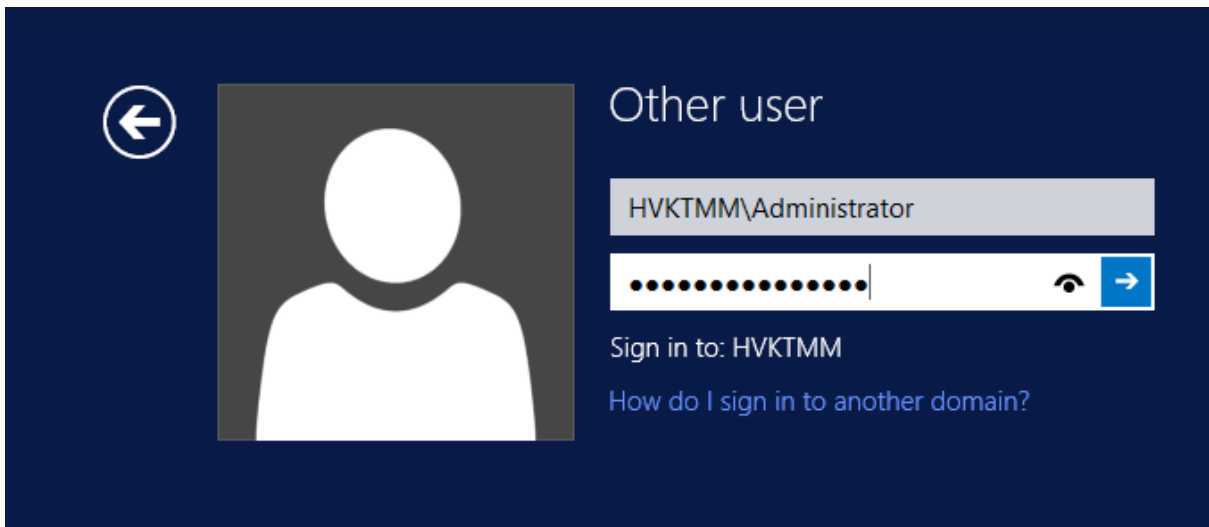
### 1.7.1. Join máy chủ SRV vào DC

– Thực hiện gia nhập SRV vào DC



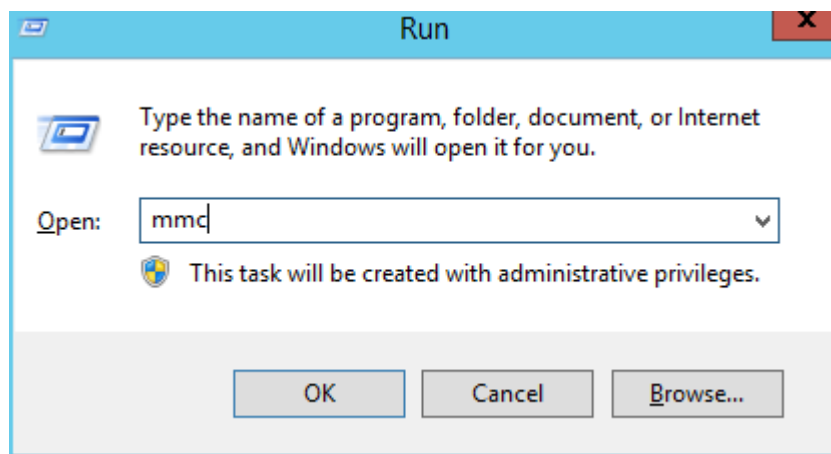
– Sau khi gia nhập thành công, máy SRV sẽ tự khởi động lại và màn hình đăng nhập sau đó cũng có dạng tương tự như bên DC.



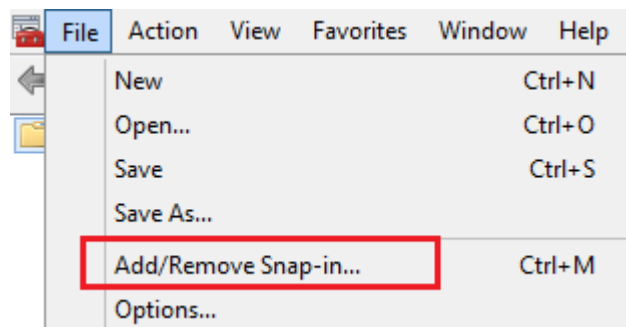


### 1.7.2. Xin cấp phát chứng thư số

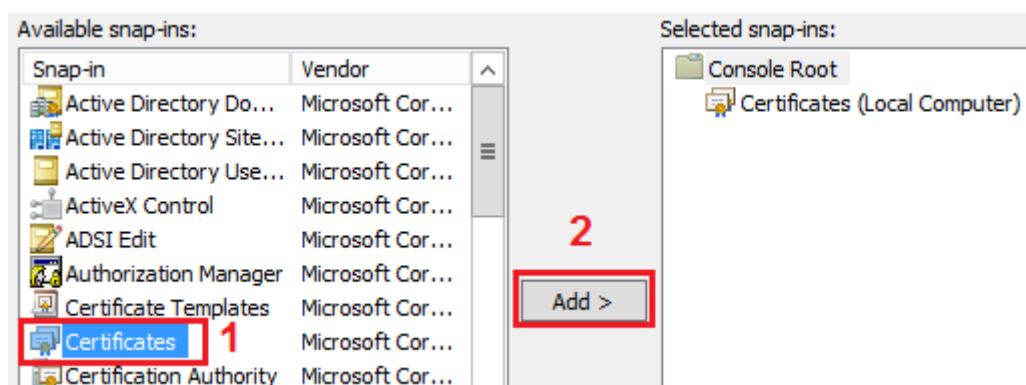
- Bật chương trình MMC từ Run:



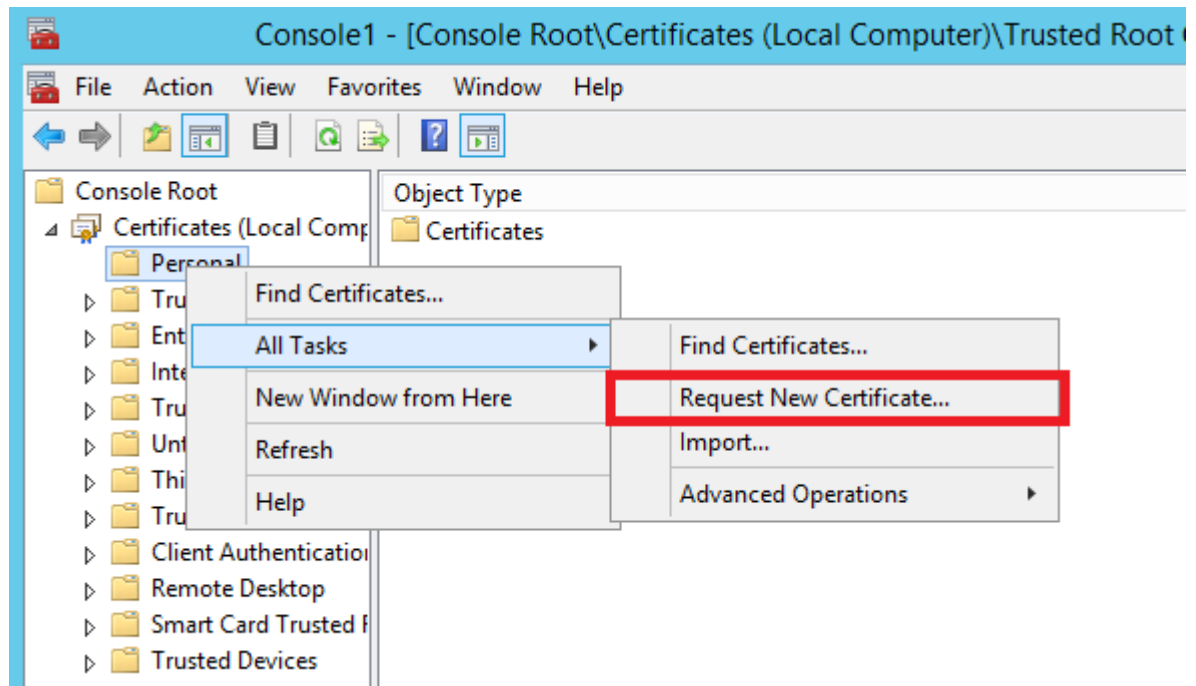
- Cửa sổ hiện lên chọn File → Add or Remove snap-in



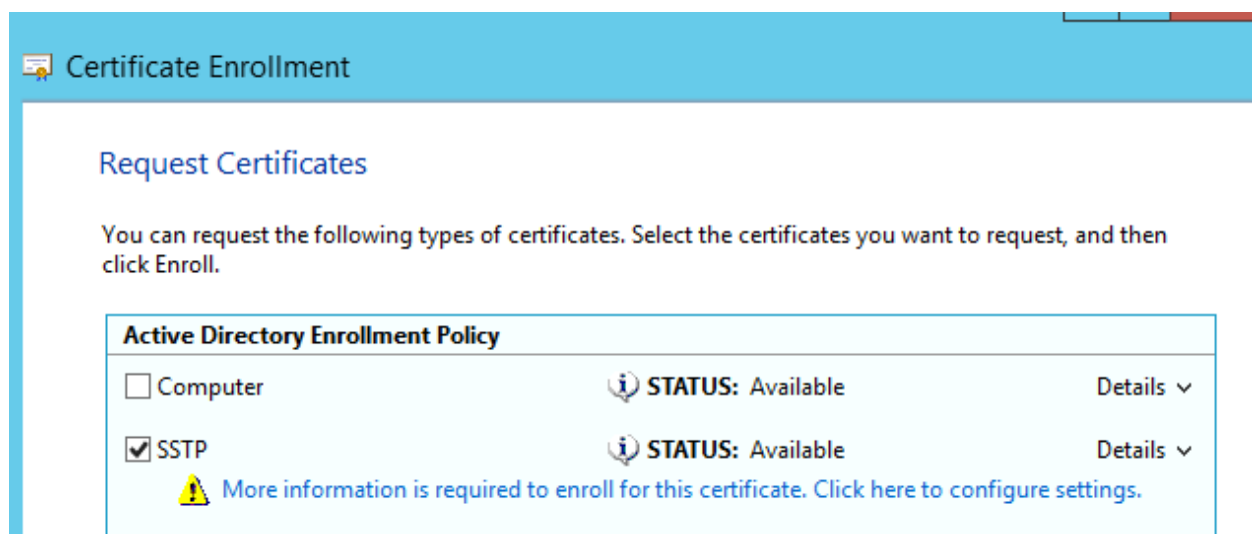
- Cửa sổ xuất hiện chọn như hình sau:



- Cửa sổ lựa chọn định dạng chứng thư số chọn Computer account → Finish.
- Tại cửa sổ quản lý chứng thư, chuột phải Personal → All Tasks → Request New Certificate



- Tiếp tục chọn Next theo mặc định, tại cửa sổ Request Certificates chọn SSTP và click vào biểu tượng cảnh báo màu vàng.



- Mục Type chọn Common name
- Mục Value nhập IP là giao diện bên ngoài của máy chủ SRV. Chọn Add để đồng ý.

**Subject** | General | Extensions | Private Key | Certification Authority | Signature

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

**Subject of certificate**  
The user or computer that is receiving the certificate

**Subject name:**

Type: Common name ▼

Value: 192.168.1.1

Add >

< Remove

**Alternative name:**

Type: Directory name ▼

Value:

Add >

< Remove

CN=192.168.1.1

- Chọn Apply → OK. Chọn Enroll để yêu cầu cấp chứng thư số. Chọn Finish để hoàn tất quá trình.

**Certificate Enrollment**

**Certificate Installation Results**

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy
<input checked="" type="checkbox"/> SSTP <span style="color: green; font-weight: bold;">✓ STATUS: Succeeded</span> <span style="float: right;">Details ▼</span>

- Kiểm tra chứng thư số vừa được cấp phát.

**Console1 - [Console Root]**

File | Action | View | Favorites | Window | Help

Console Root

- Certificates (Local Computer)
  - Personal
    - Certificates
      - 192.168.1.1

Personal store contains 1 certificate.

**Certificate**

General | Details | Certification Path

**Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Allows secure communication on the Internet

**Issued to:** 192.168.1.1

**Issued by:** hvktnm-CA

**Valid from:** 5/27/2020 to 5/27/2022

You have a private key that corresponds to this certificate.

Issuer Statement

OK

### 1.7.3. Cài đặt ứng dụng Routing and Remote Access

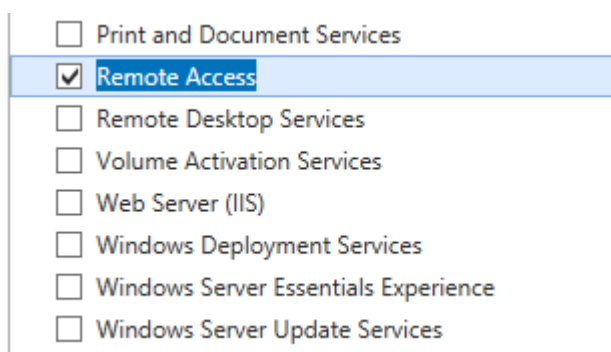
– Trên máy chủ SRV đầu tiên phải cài đặt ứng dụng quản lý truy cập từ xa Routing and Remote access.

– Truy cập theo đường dẫn: Server Manager → Dashboard → Add roles and features.

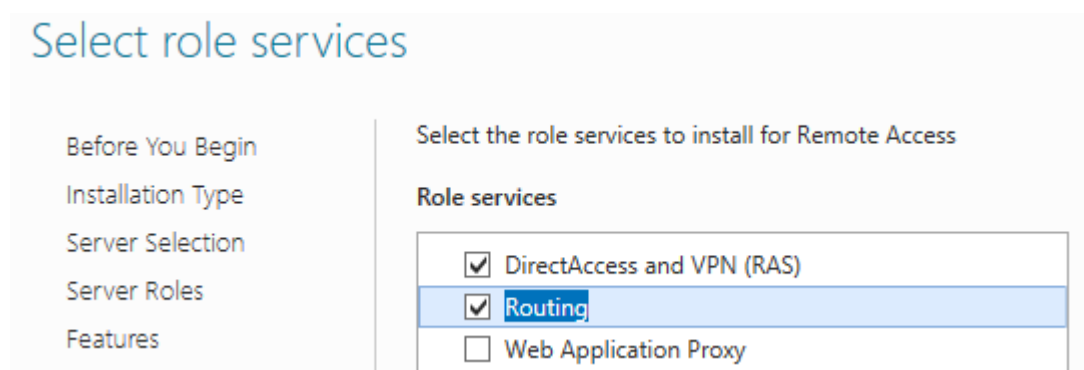


– Ba bước đầu tiên để mặc định và chọn Next.

– Đến giao diện Select server roles: Tích chọn Remote Access



– Giao diện Select role service: Tích chọn 2 tùy chọn như hình sau:

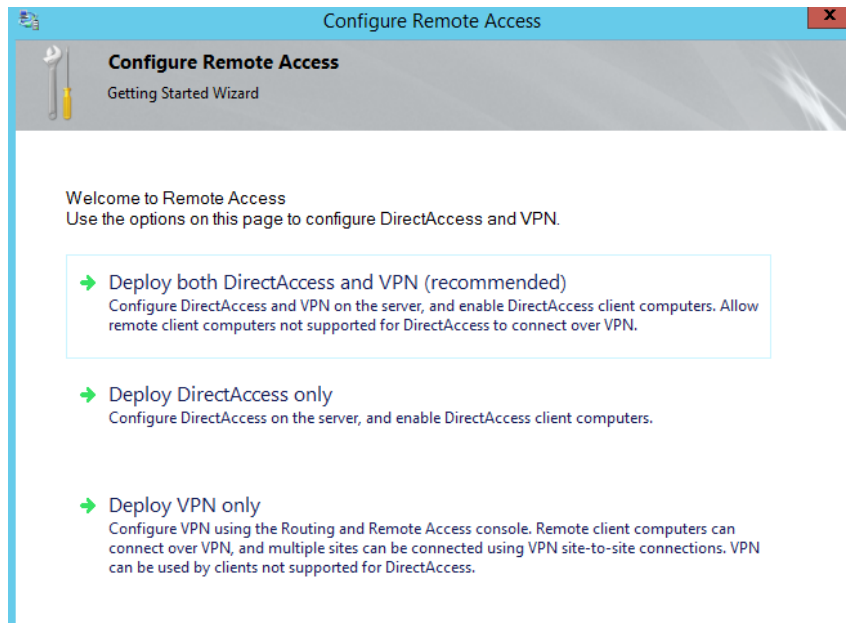


– Các bước tiếp theo chọn Next và Install để cài đặt.

#### 1.7.4. Cấu hình dịch vụ Routing and Remote Access

– Truy cập theo đường dẫn:

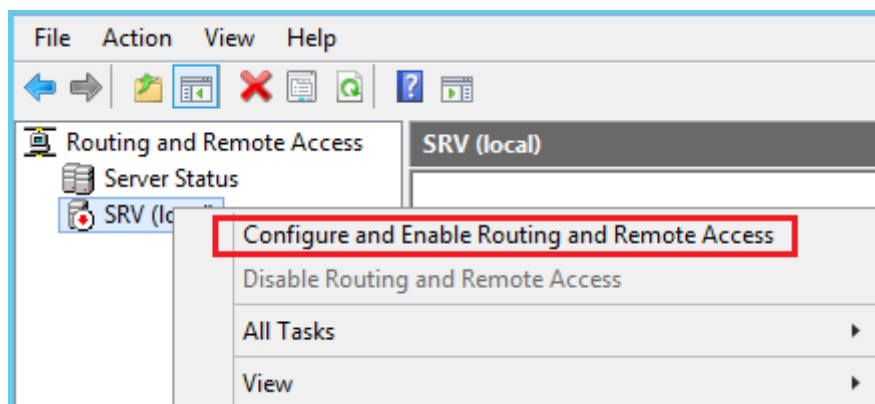
– Server Manager → Tools → Routing and Remote Access. Chọn Deploy VPN only



– Cửa sổ cấu hình xuất hiện.



– Chuột phải vào Server SRV chọn Configure and Enable Routing:



– Giao diện xuất hiện chọn Next.

– Giao diện tiếp theo lựa chọn phương thức sử dụng: chọn Custom  
Configure Giao diện tiếp theo tích vào 2 tùy chọn như hình dưới đây chọn chức năng VPN và NAT.

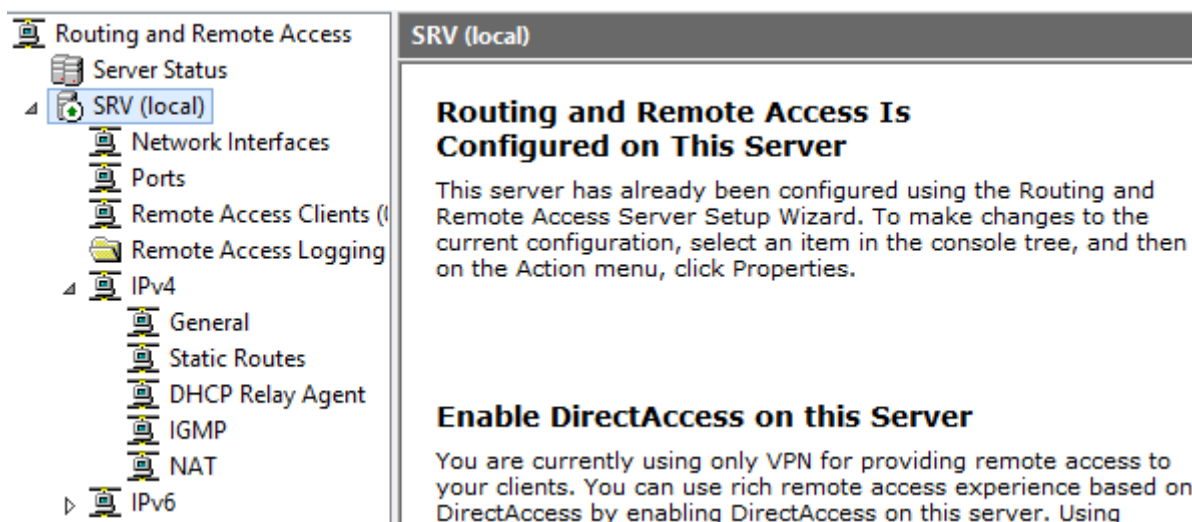
### Custom Configuration

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.

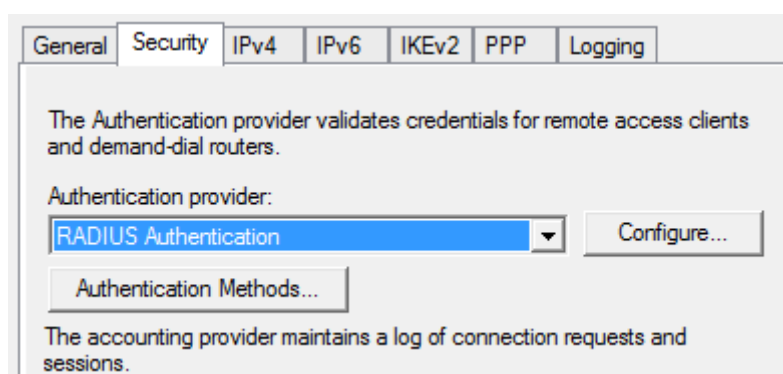
- ☒ VPN access
- ☐ Dial-up access
- ☐ Demand-dial connections ( used for branch office routing )
- ☒ NAT
- ☐ LAN routing

– Chọn Next và Finish để kết thúc. Giao diện sau khi cài đặt.



– Chuột phải vào tên máy chủ SRV chọn Properties.

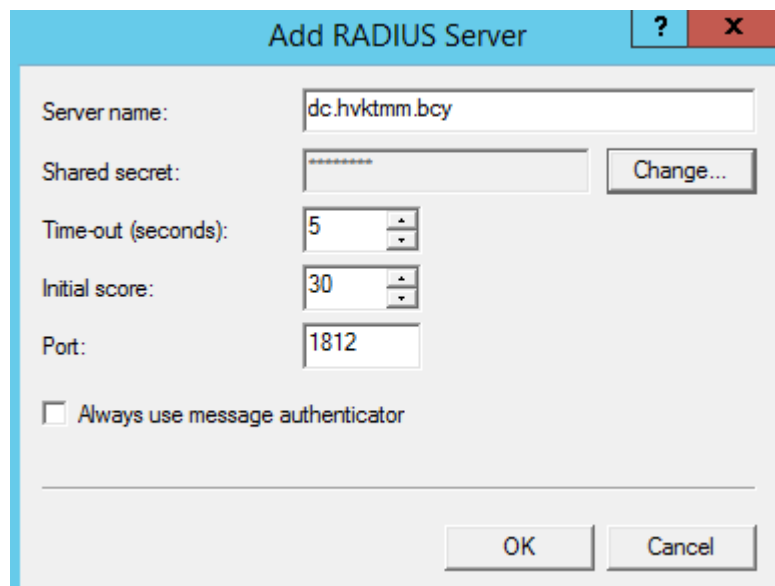
– Tab Security chọn phương thức xác thực là RADIUS. Tiếp chọn Configure.



– Cửa sổ xuất hiện chọn Add.

– Mục Server name: nhập tên và miền của máy chủ DC.

– Mục Shared secret: Nhập khóa chia sẻ đã thiết lập trong Radius DC.



**Add RADIUS Server**

Server name: dc.hvktmm.bcy

Shared secret: [masked] Change...

Time-out (seconds): 5

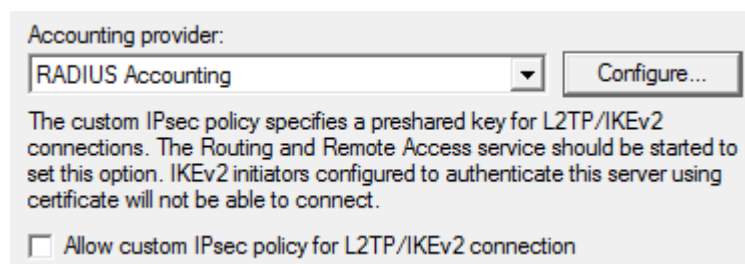
Initial score: 30

Port: 1812

☐ Always use message authenticator

OK Cancel

- Nhấn OK để đóng cửa sổ.
- Tương tự thiết lập cho mục Accounting provider:



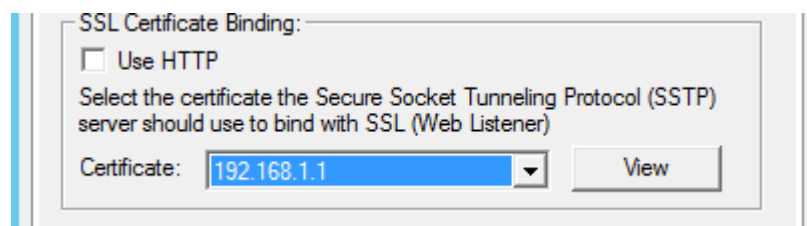
Accounting provider:

RADIUS Accounting Configure...

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☐ Allow custom IPsec policy for L2TP/IKEv2 connection

- Mục SSL Binding: chọn chứng thư số vừa cài đặt:



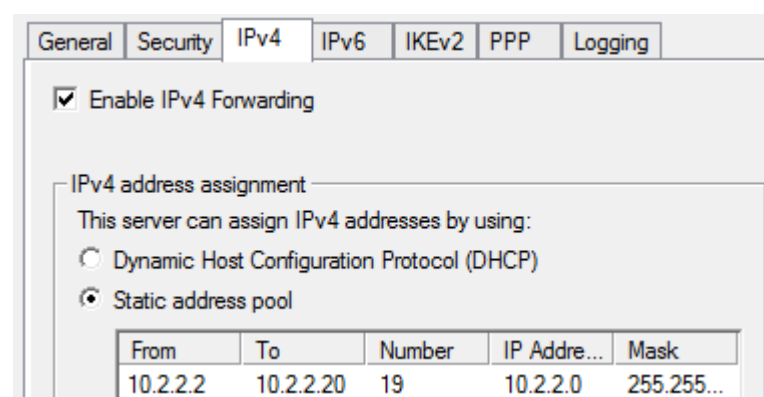
SSL Certificate Binding:

☐ Use HTTP

Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: 192.168.1.1 View

- Chuyển sang Tab IPv4.
- Chọn Static address và nhập dãy IP sẽ cấp phát cho máy trạm khi kết nối VPN



General Security **IPv4** IPv6 IKEv2 PPP Logging

☒ Enable IPv4 Forwarding

IPv4 address assignment

This server can assign IPv4 addresses by using:

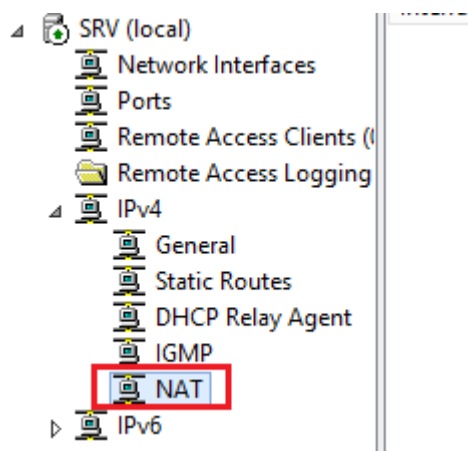
☐ Dynamic Host Configuration Protocol (DHCP)

☒ Static address pool

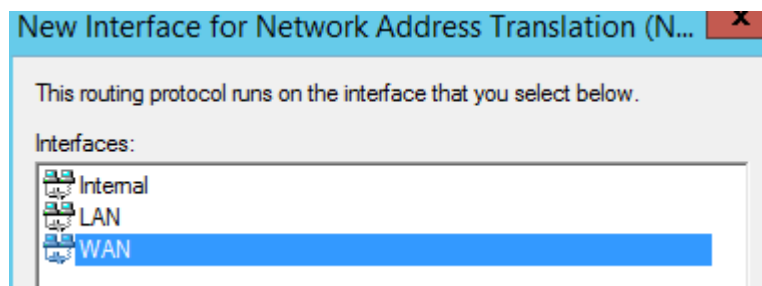
From	To	Number	IP Address	Mask
10.2.2.2	10.2.2.20	19	10.2.2.0	255.255...

- Nhấp Apply và OK để kết thúc.

– Tiếp tục cấu hình NAT để cho phép máy trạm có thể truy cập được vào webserver trong máy chủ DC.

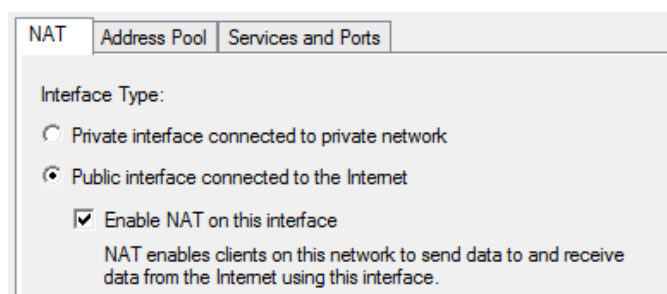


– Chuột phải vào NAT, chọn New Interface. Giao diện xuất hiện chọn Interface bên ngoài WAN.

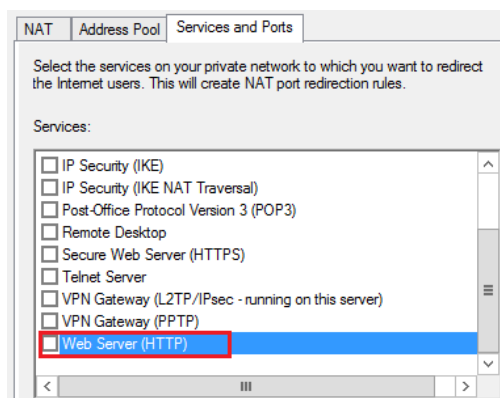


– Nhấn OK sẽ xuất hiện cửa sổ cấu hình.

– Tab NAT chọn Public interface, tích chọn Enable NAT.



– Tab Services and Ports: Chọn Web Server (HTTP)



– Cửa sổ xuất hiện cần thiết lập địa chỉ IP của DC:

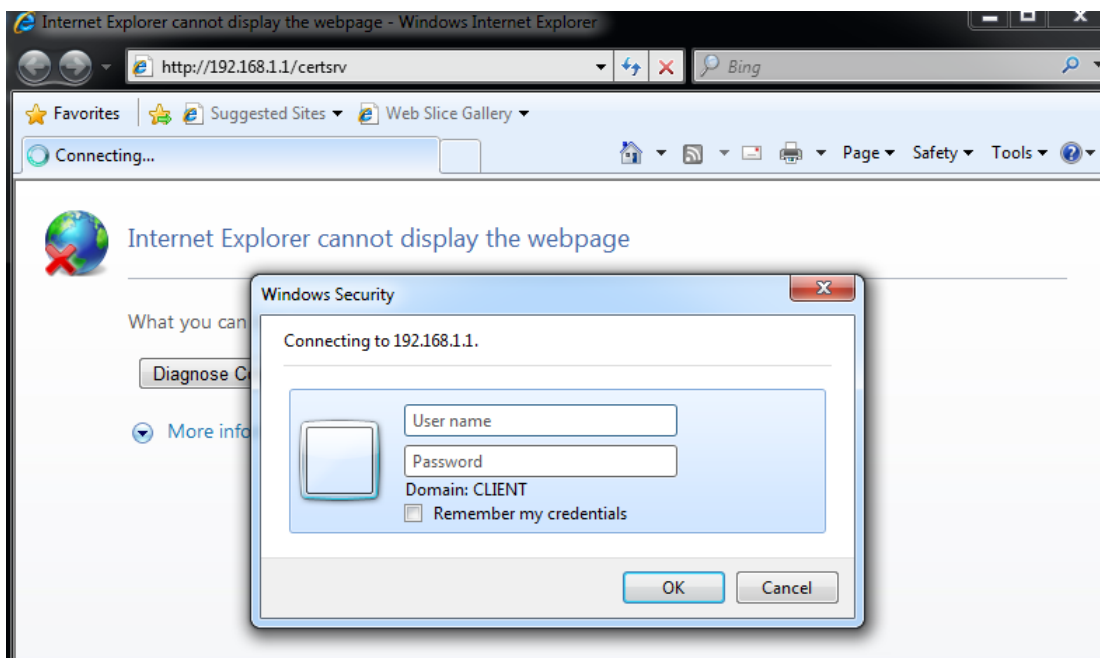


Incoming port:	<input type="text" value="80"/>
Private address:	<input type="text" value="172 . 16 . 1 . 2"/>
Outgoing port:	<input type="text" value="80"/>

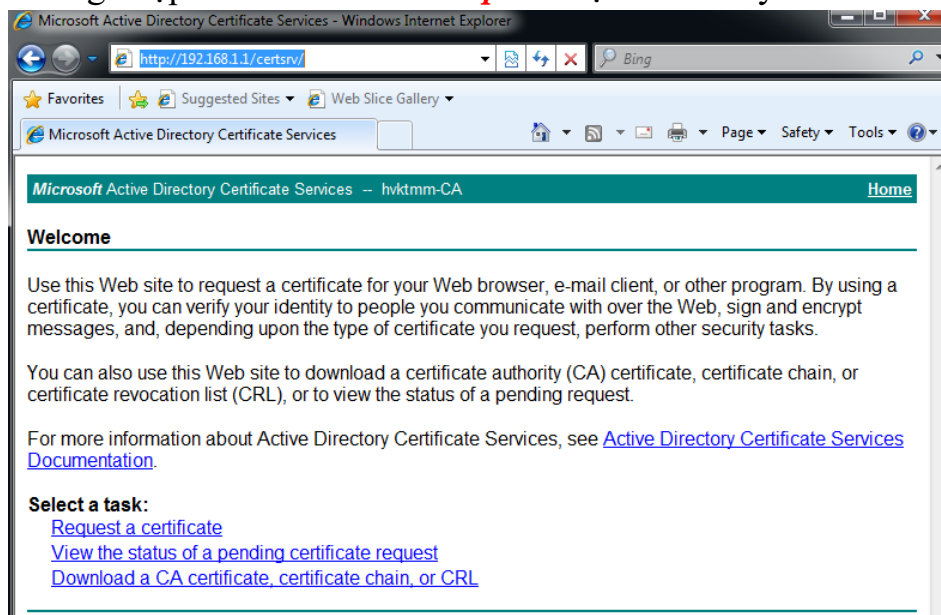
– Nhấn OK → Apply → OK để kết thúc cấu hình.

## 1.8. Thực hiện trên máy Windows 7

– Truy cập tới dịch vụ cấp phát chứng thư số trong máy chủ DC thông qua trình duyệt web theo đường dẫn *http://192.168.1.1/certsrv*.

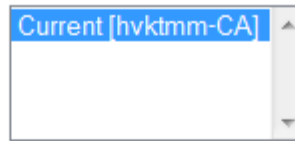


– Đăng nhập với tài khoản *kmavpn* đã tạo trước đây.



– Tích vào tùy chọn Download a CA certificate. Tiếp tục chọn Download CA certificate:

CA certificate:



Encoding method:

- ☒ DER  
☐ Base 64

[Install CA certificate](#)

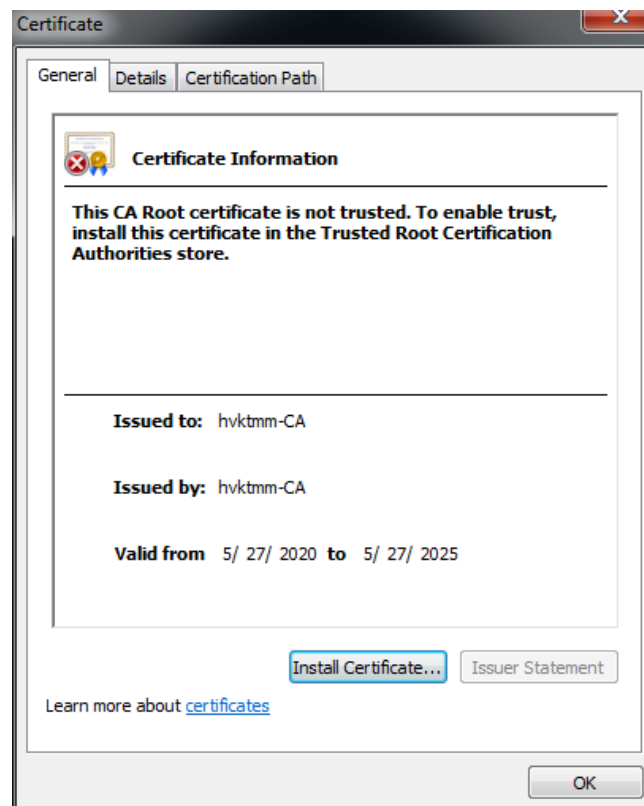
[Download CA certificate](#)

[Download CA certificate chain](#)

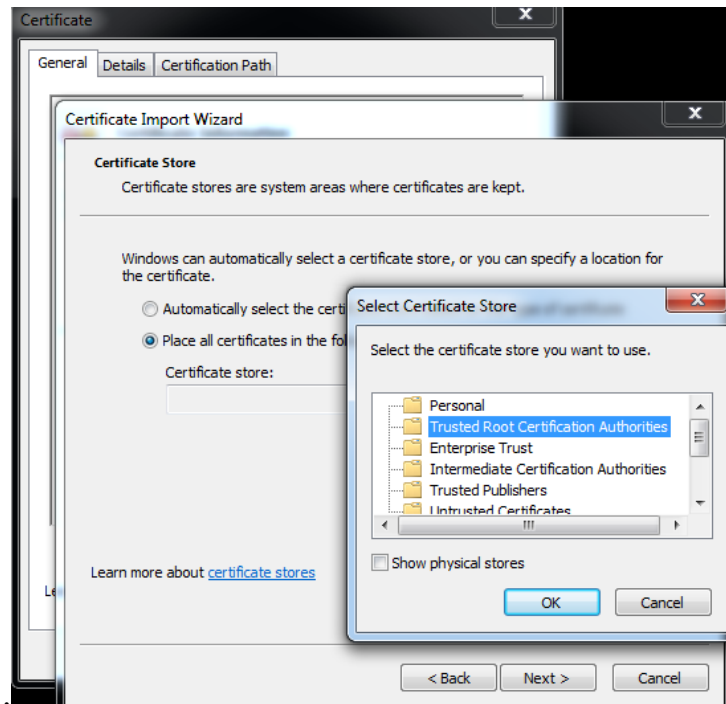
[Download latest base CRL](#)

[Download latest delta CRL](#)

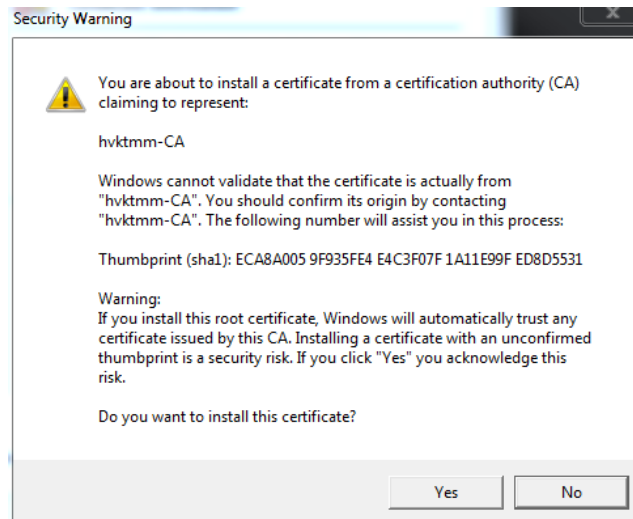
– Chọn nơi lưu chứng thư số của CA. Mở chứng thư số vừa tải về và chọn Install Certificate



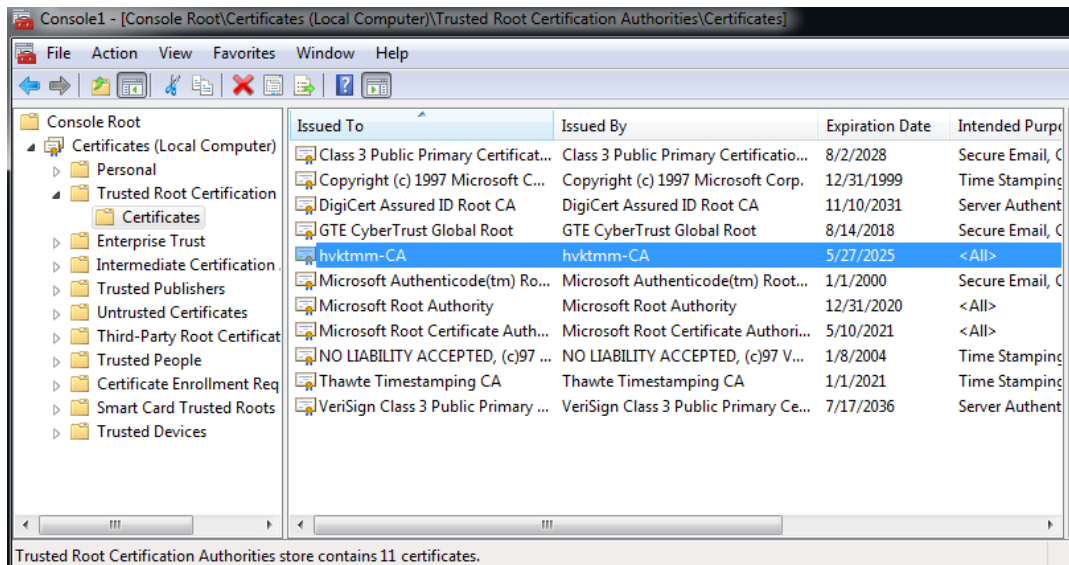
– Tại cửa sổ Certificate Import Wizard chọn Certificate store → Trusted Root Certification Authorities → OK → Next → Finish.



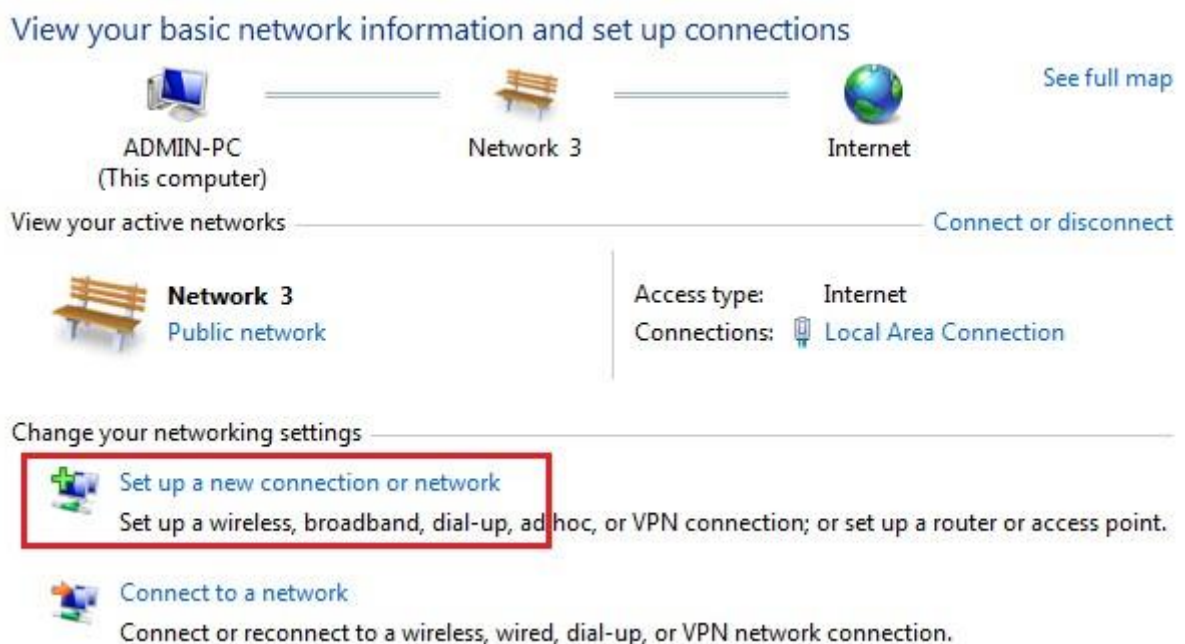
– Trường hợp xuất hiện hộp thoại cảnh báo có muốn cài Certificate này không ta chọn Yes.



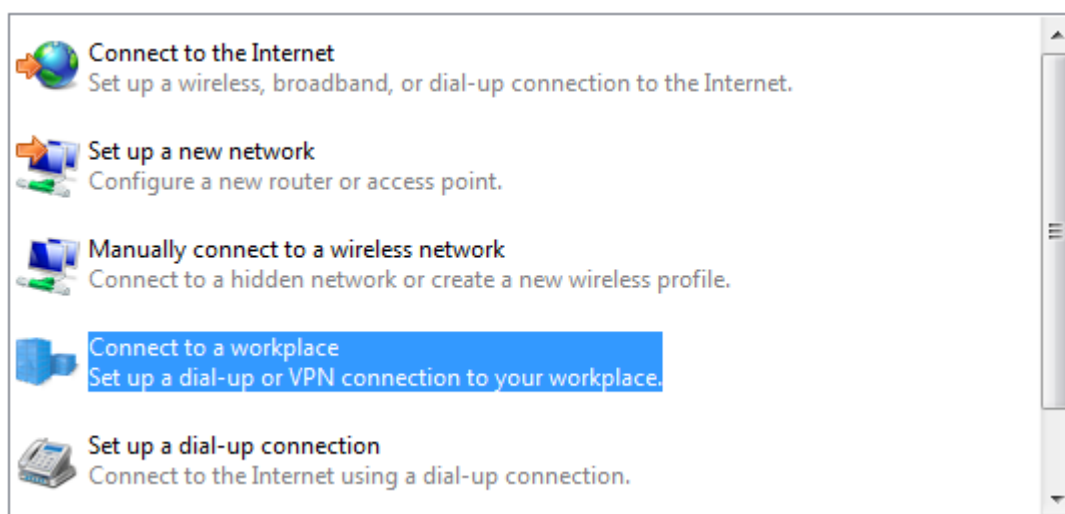
– Thực hiện kiểm tra và thấy chứng thư số đã được cài vào máy



– Bước tiếp theo cài đặt và cấu hình kết nối VPN. Truy cập theo đường dẫn: Control Panel → Network and Sharing Center → Set up a new connection or network or network.



– Giao diện tiếp theo chọn Connect to a workplace.



- Giao diện tiếp theo chọn kết nối thông qua VPN:



- Chọn I'll set up an Internet connection later.
- Giao diện tiếp theo nhập địa chỉ IP bên ngoài của SRV (kết nối với Windows 7). Đặt tên cho kết nối:

Your network administrator can give you this address.

Internet address:	<input type="text" value="192.168.1.1"/>
Destination name:	<input type="text" value="KMA VPN"/>

- Bước tiếp theo nhập tài khoản đã tạo trên máy chủ DC. Chọn Create để tạo kết nối.

Type your user name and password

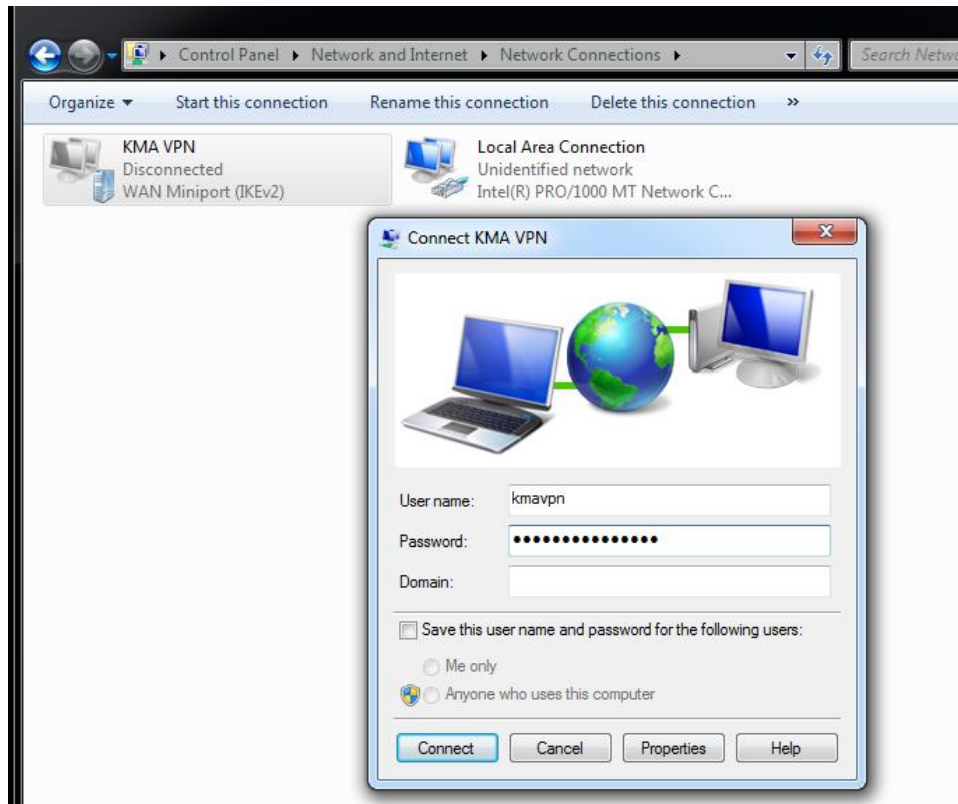
User name:

kmavpn

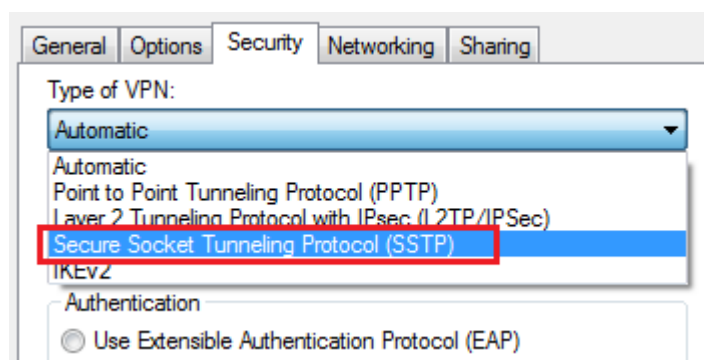
Password:

••••••••••

– Truy cập vào đường dẫn Control Panel\Network and Internet\Network Connections. Cửa sổ đăng nhập kết nối xuất hiện.



– Chọn Properties để cấu hình sử dụng giao thức SSTP. Tab Security chọn kết nối SSTP.



– Các thông số khác để mặc định. Chọn OK để lưu và đóng cửa sổ. Truy cập vào Registry thông qua Run. (gõ regedit)

– Truy cập theo đường dẫn: HKEY\_LOCAL\_MACHINE → SYSTEM → CurrentControlSet → Services → SstpSvc.

- Chuột phải vào mục Parameters → New → DWORD
- Đặt tên DWORD này là: NoCertRevocationCheck có giá trị là 1.

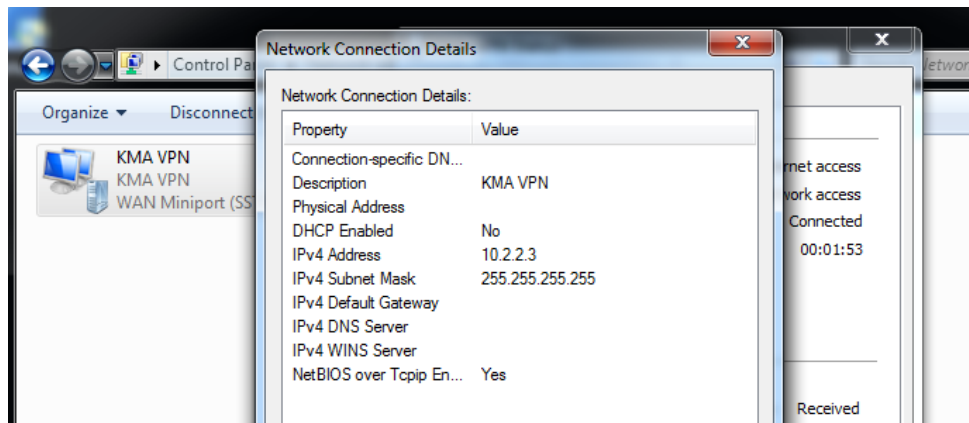
Name	Type	Data
(Default)	REG_SZ	(value not set)
ListenerPort	REG_DWORD	0x00000000 (0)
NoCertRevocationCheck	REG_DWORD	0x00000001 (1)
ServerURI	REG_SZ	/sra_{BA195980-CD4
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\syst
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
UseHttps	REG_DWORD	0x00000001 (1)

- Kết thúc và đóng cửa sổ Registry.
- Quay trở lại cửa sổ đăng nhập kết nối. Nhập lại tên và mật khẩu của người dùng kmavpn. Nhấn Connect để kết nối.



- Kết quả thành công.





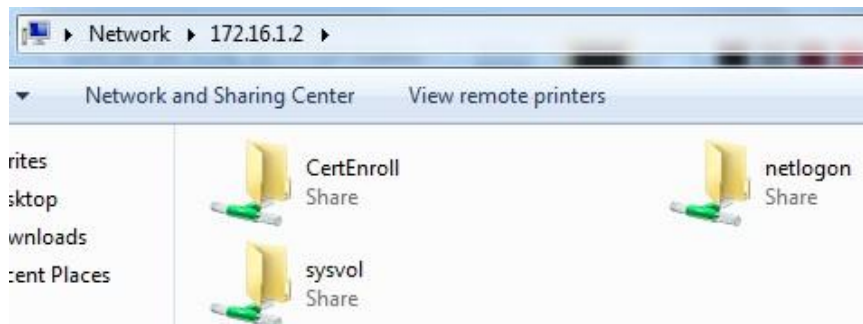
## 1.9. Kiểm tra kết quả

- Tại máy Windows 7 thực hiện Ping tới máy chủ DC. Thành công.

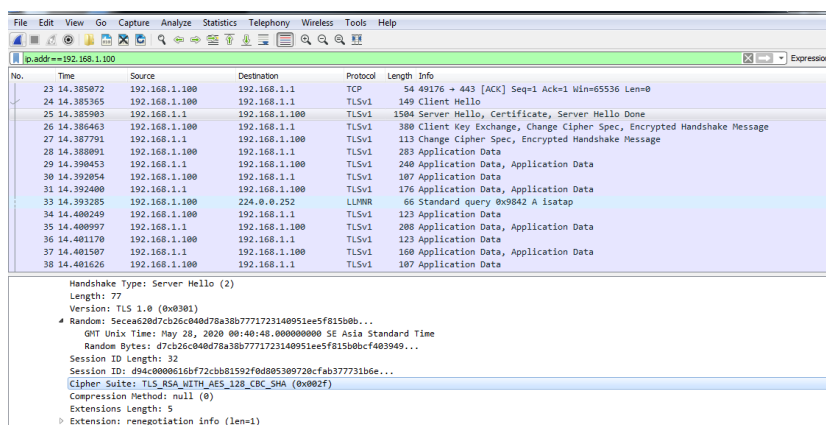
```
C:\Users\admin>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
```

- Truy cập vào tài nguyên chia sẻ trên máy chủ DC



- Kiểm tra gói tin gửi trên đường truyền. Thực hiện cài đặt công cụ chặn bắt và phân tích gói tin Wireshark.



- Các gói tin đã được mã hóa với giao thức TLSv1. Kết thúc bài thực hành./.