

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

Mục lục	2
Thông tin chung về bài thực hành	3
Chuẩn bị bài thực hành	4
Đối với giảng viên	4
Đối với sinh viên	4
TRIỂN KHAI dịch vụ truy cập từ xa vpn sử dụng giao thức ssl và radius	5
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
Phụ lục.....	38

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. 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



(Giải thích hình vẽ, vai trò của từng thiết bị)

1.4. Các bước thực hiện

Thực hiện trên 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

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.

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

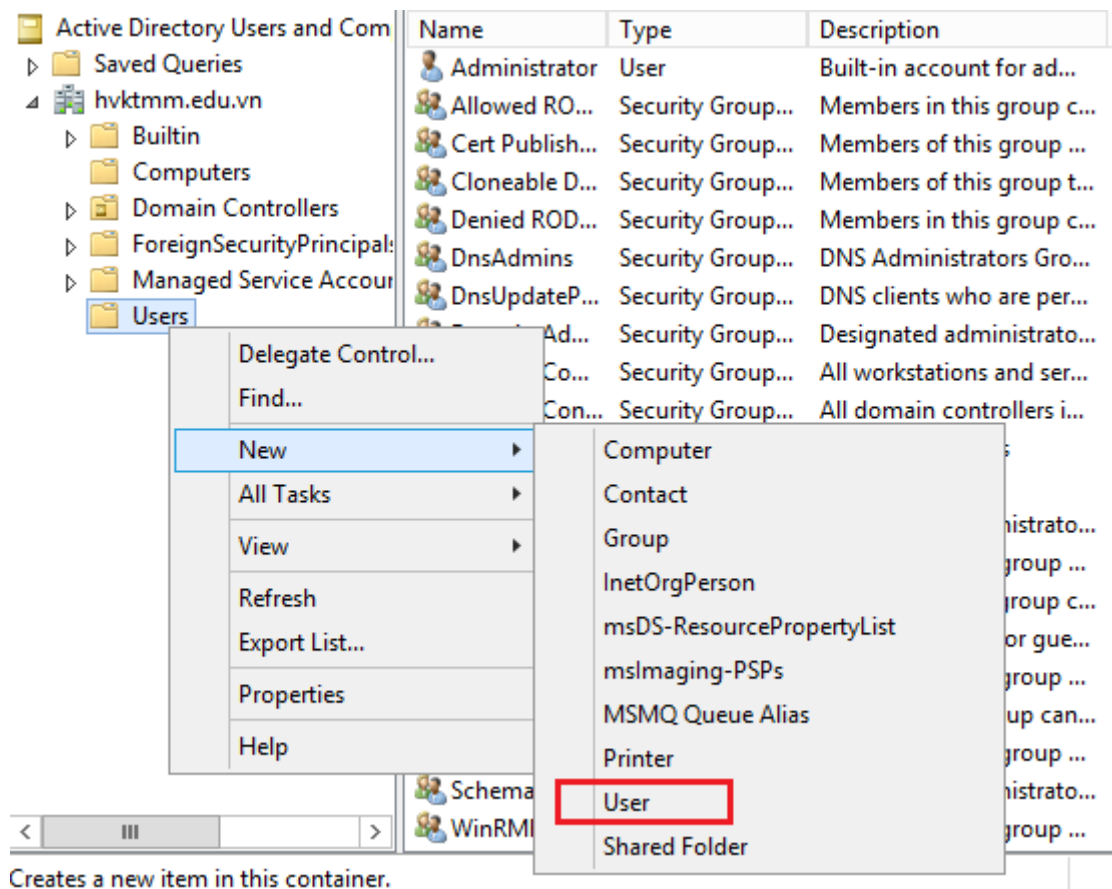
1.5. Thực hiện trên máy chủ DC

1.4.1. 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: user1

Create in: hvktmm.edu.vn/Users

First name: user1 Initials:

Last name:

Full name: user1

User logon name: user1 @hvktmm.edu.vn

User logon name (pre-Windows 2000): HVKTMM\ user1

< Back Next > Cancel

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

Create in: hvktmm.edu.vn/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 → Allow access.

Remote control Remote Desktop Services Profile COM+

General Address Account Profile Telephones Organization

Member Of Dial-in Environment Sessions

Network Access Permission

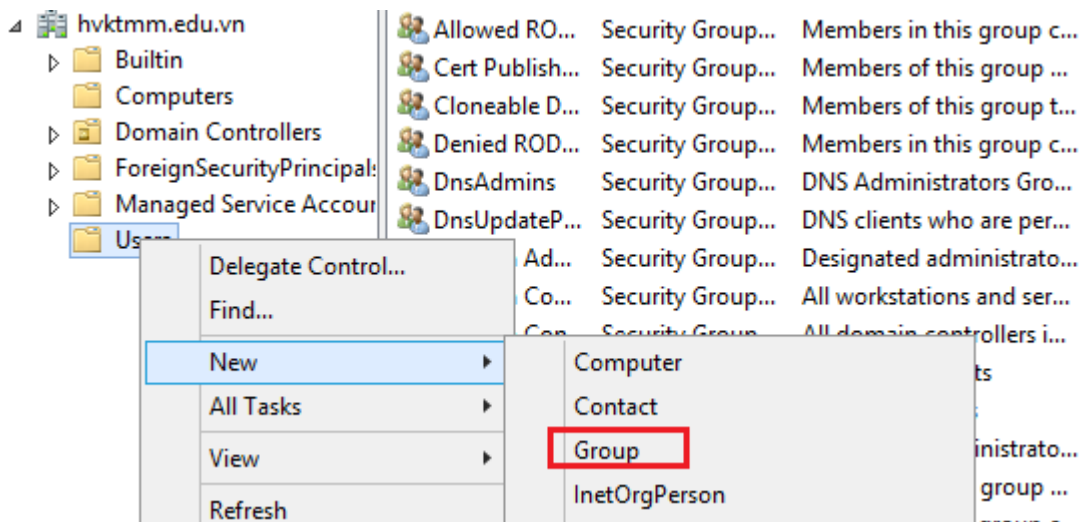
☒ Allow access

☐ Deny access

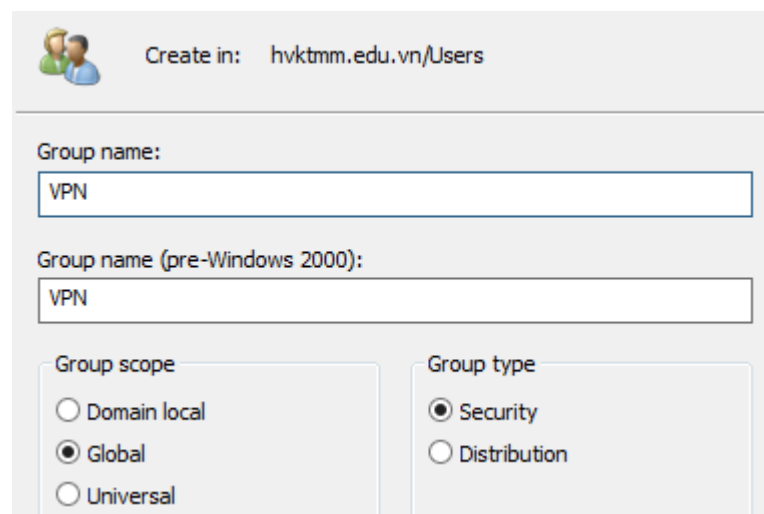
☐ Control access through NPS Network Policy

Nhấn Apply và OK để kết thúc.

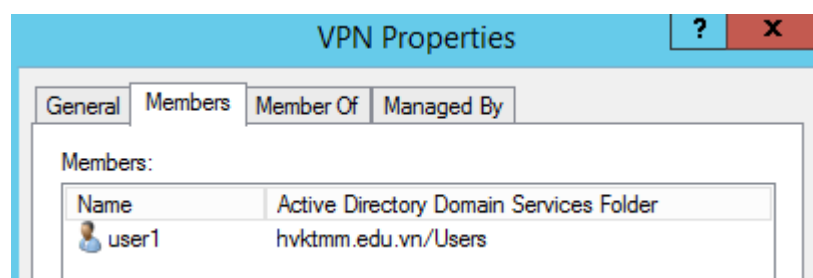
Tạo nhóm VPN và thêm người dùng này vào nhóm.



Đặt tên nhóm là VPN:



Thêm người dùng vào nhóm VPN:

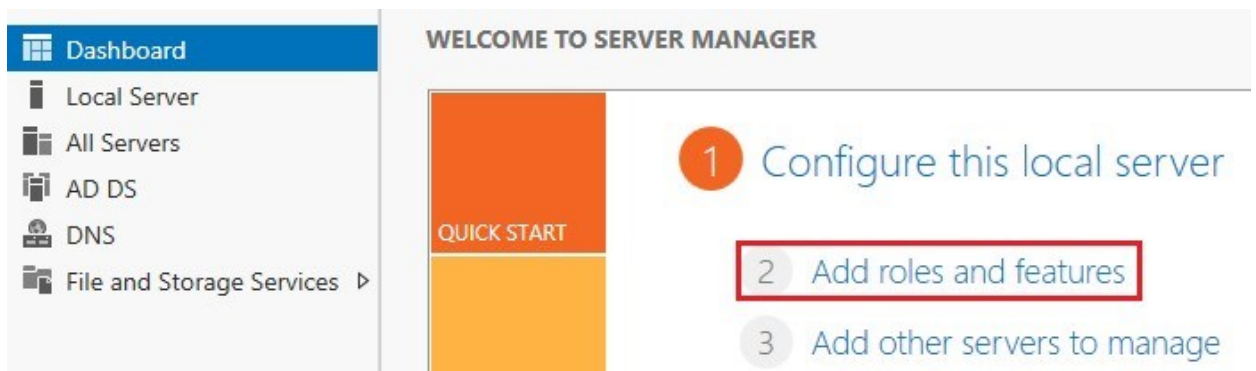


Kết thúc bước tạo người dùng truy cập từ xa.

1.4.2. Cài đặt dịch vụ Network Policy Server

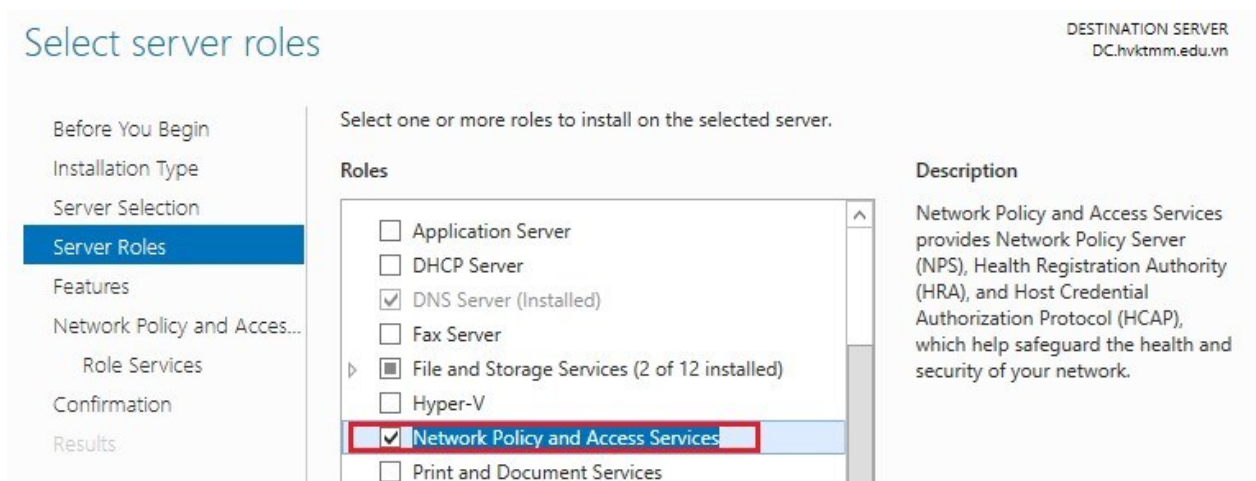
Truy cập theo đường dẫn:

Server Manager → Dashboard → Add roles and features:



Ba bước đầu tiên để mặc định và chọn Next.

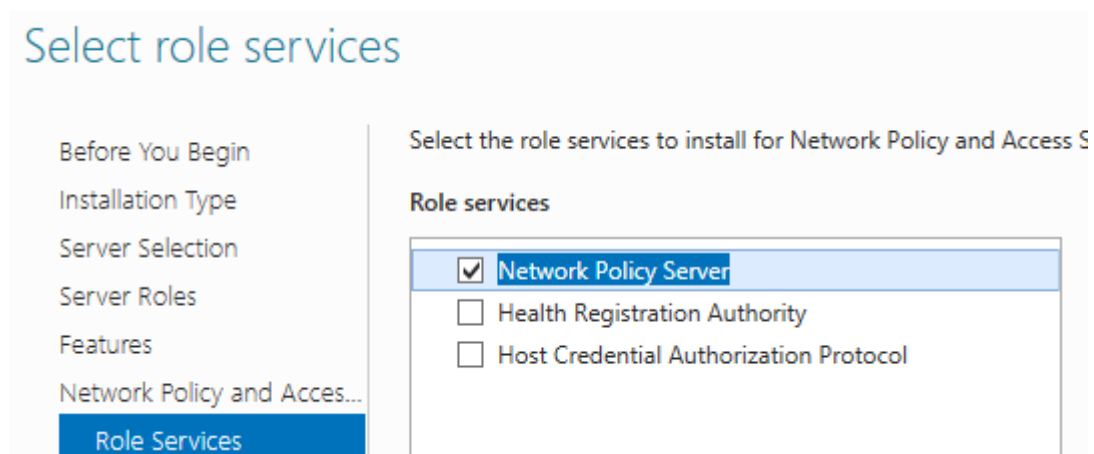
Tại bước lựa chọn vai trò (Select server roles): Chọn Network Policy and Access Services:



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.

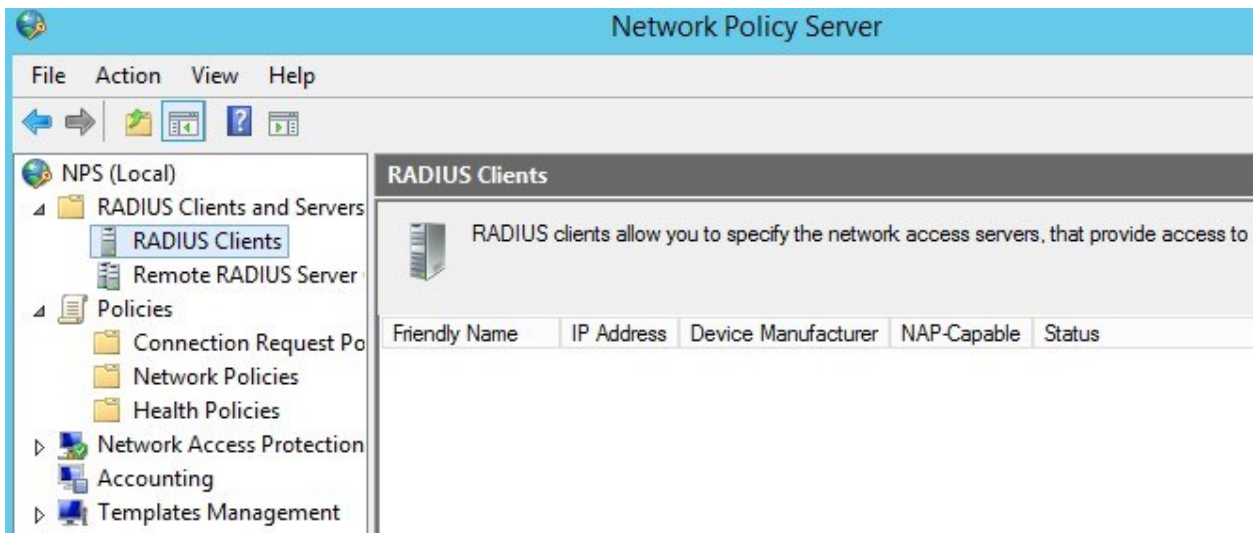
1.4.3. Cấu hình Radius Server trong Network Policy Server

(Nêu mục đích của bước thực hiện)

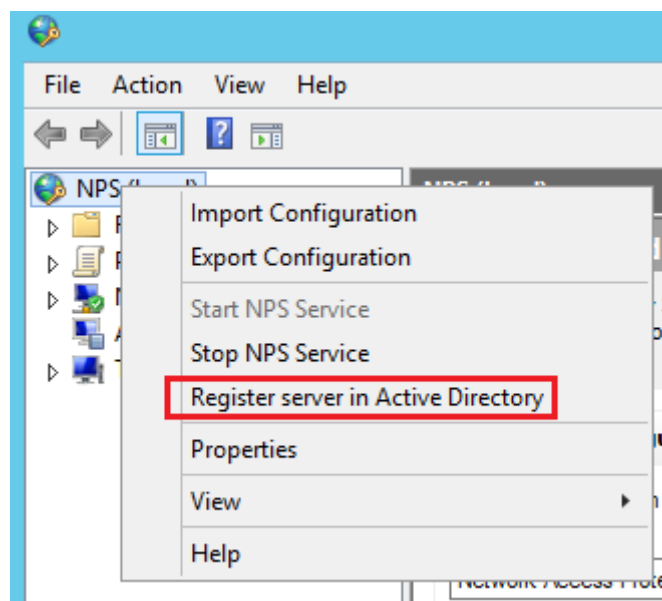
Truy cập Network Policy Server theo đường dẫn:

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:

New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
SRV

Address (IP or DNS):
172.16.1.1 Verify...

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.

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

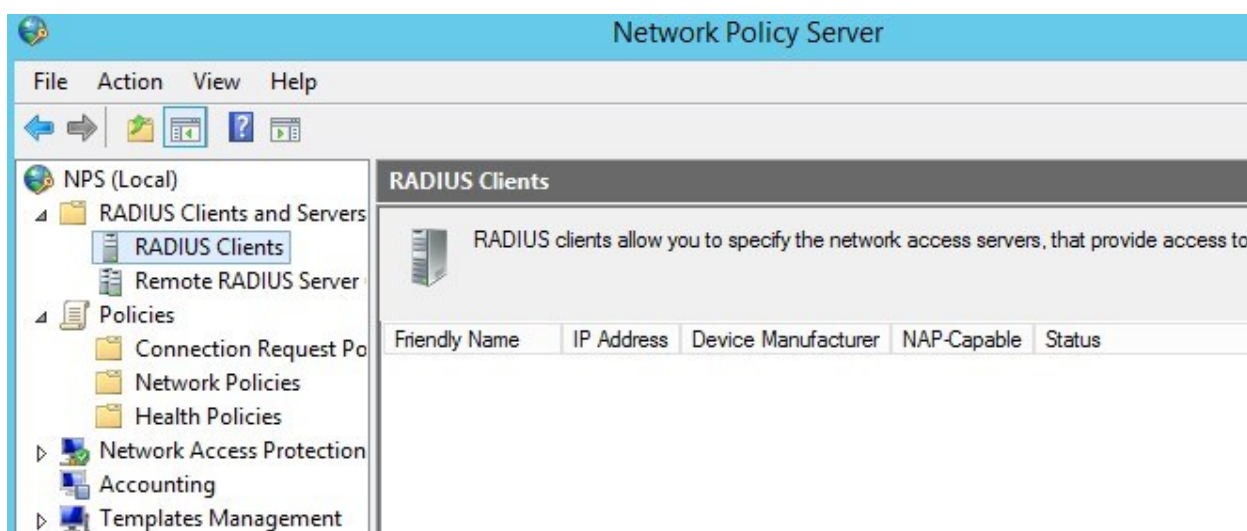
☒ Manual ☐ Generate

Shared secret:
.....

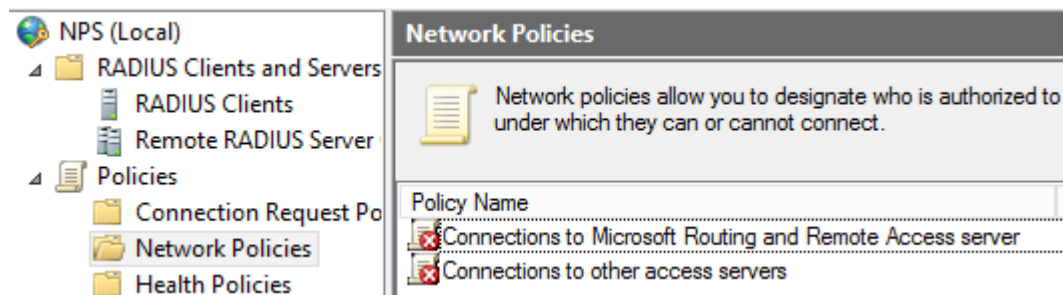
Confirm shared secret:
.....

Chọn OK để kết thúc.

Tiếp theo cần phải định nghĩa chính sách xác thực.



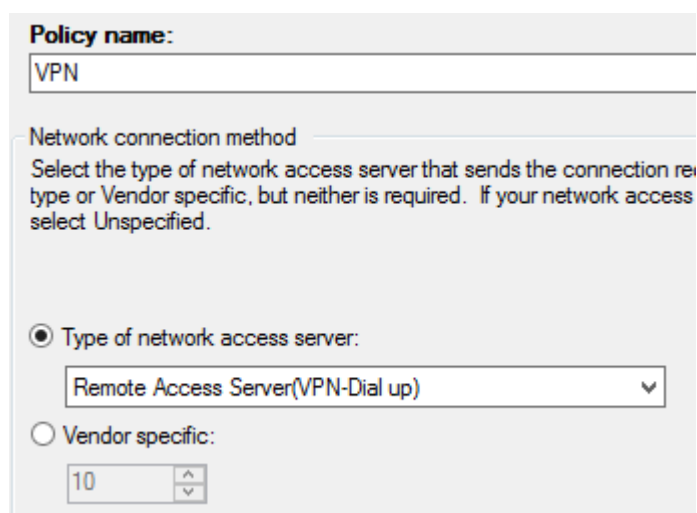
Truy cập vào mục Policies → Network Policies. Giao diện như sau:



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.

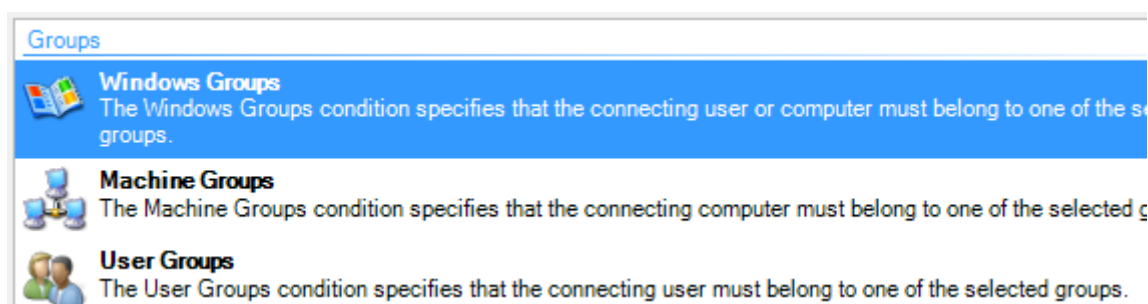
Mục Type of network access server: chọn Remote Access Server



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 this object type:

Group Object Types...

From this location:

hvktmm.edu.vn Locations...

Enter the object name to select (examples):

VPN Check Names

Advanced... OK Cancel

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 client connection attempts match the conditions of one condition 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



Specify Access Permission

Configure whether you want to grant network access or deny network access according to the policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

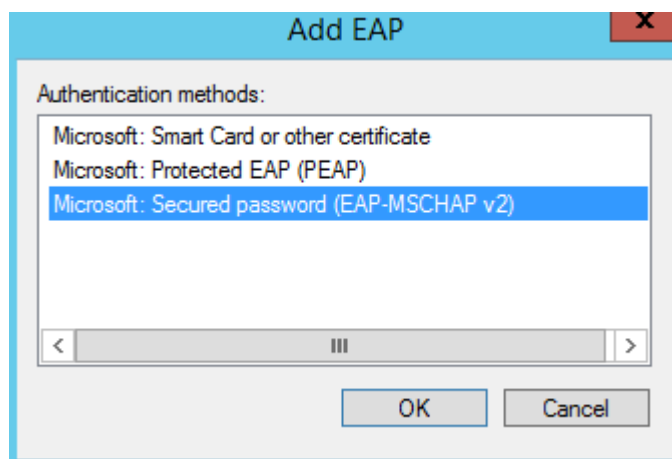
☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Chọn Next để tiếp tục.

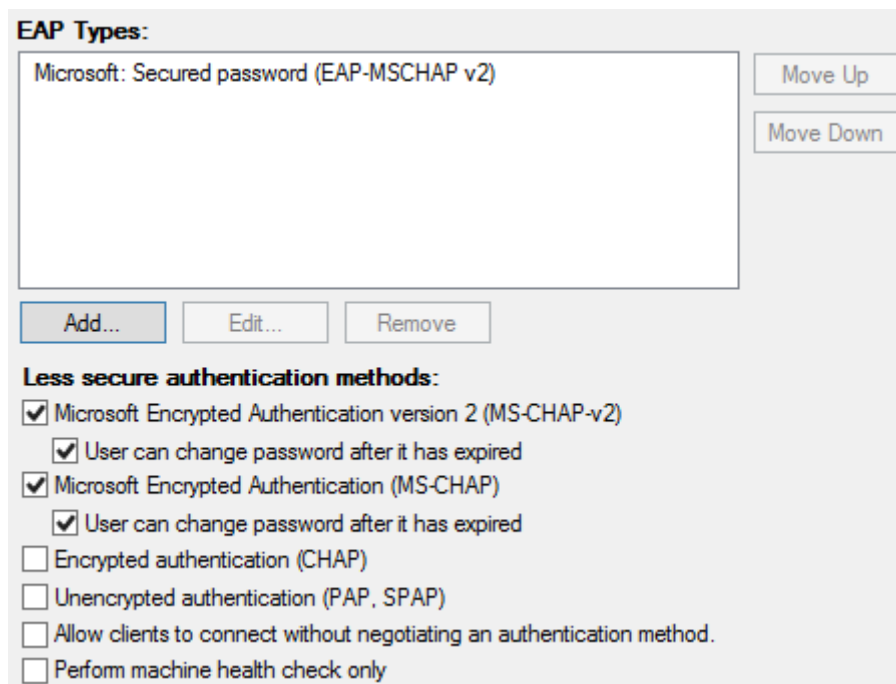
Giao diện tiếp theo chọn giao thức xác thực.

Trong mục EAP type chọn Add: Giao diện xuất hiện chọn Secured password

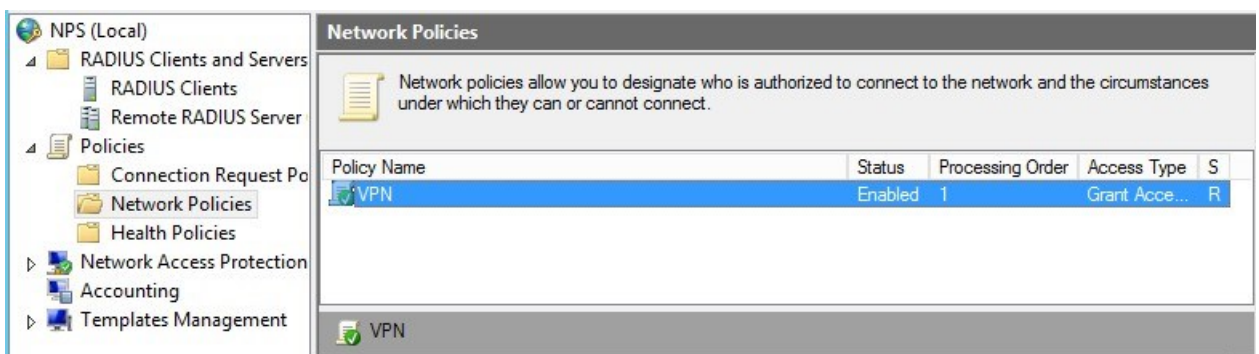


Chọn OK để tiếp tục.

Giao diện sau khi cấu hình:



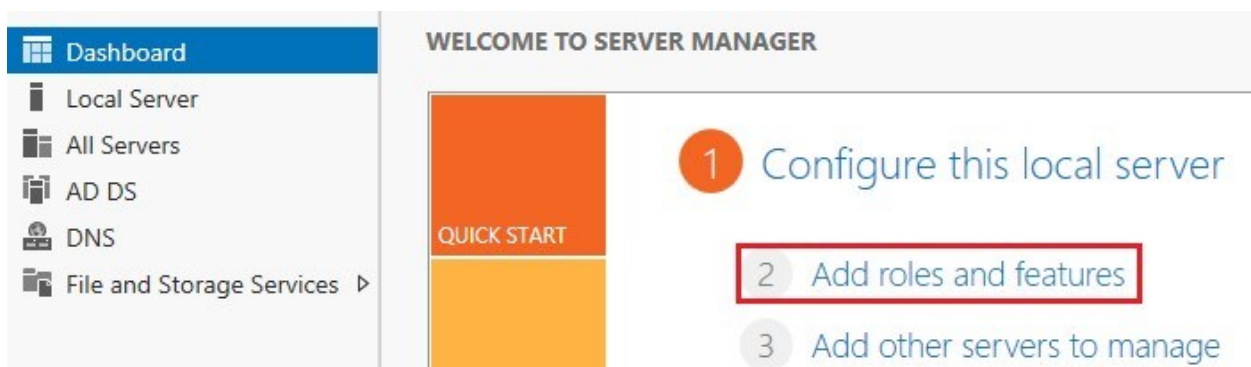
Các giao diện tiếp thế để mặc định. Chọn Finish để kết thúc.



1.4.4. Cài đặt dịch vụ trung tâm chứng thực CA.

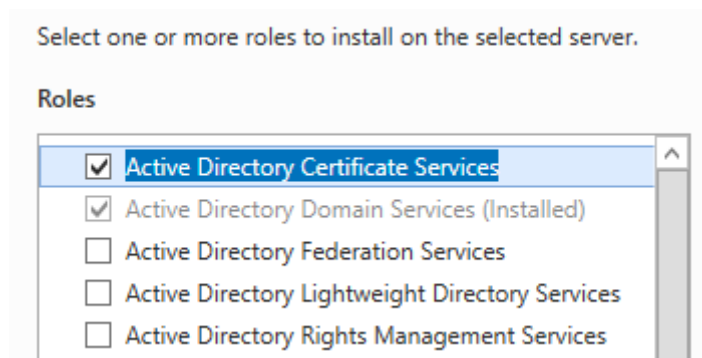
Truy cập theo đường dẫn:

Server Manager → Dashboard → Add roles and features:



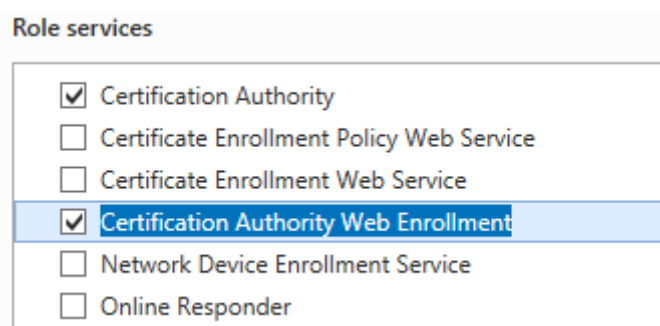
Ba bước đầu tiên để mặc định và chọn Next.

Tại bước lựa chọn vai trò (Select server roles): Chọn Active Directory Certificate Services:



Các bước tiếp theo chọn Next.

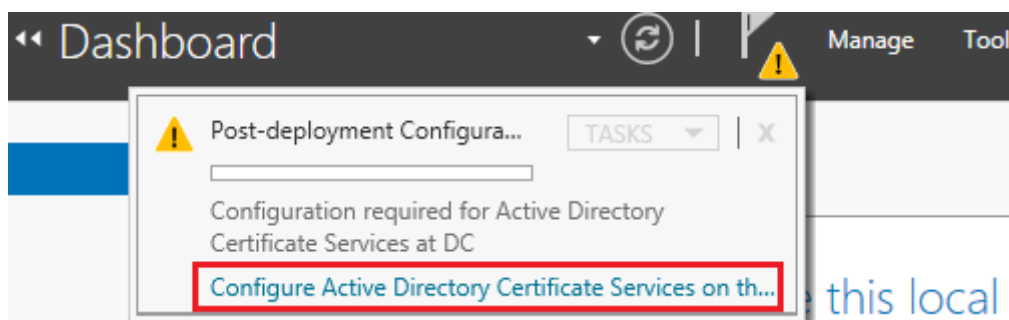
Đến giao diện Select roles services: Tích 2 tùy chọn như hình sau:



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

1.4.5. 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:

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: hvtmm-CA

Distinguished name suffix: DC=hvtmm,DC=edu,DC=vn

Preview of distinguished name: CN=hvtmm-CA,DC=hvtmm,DC=edu,DC=vn

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:

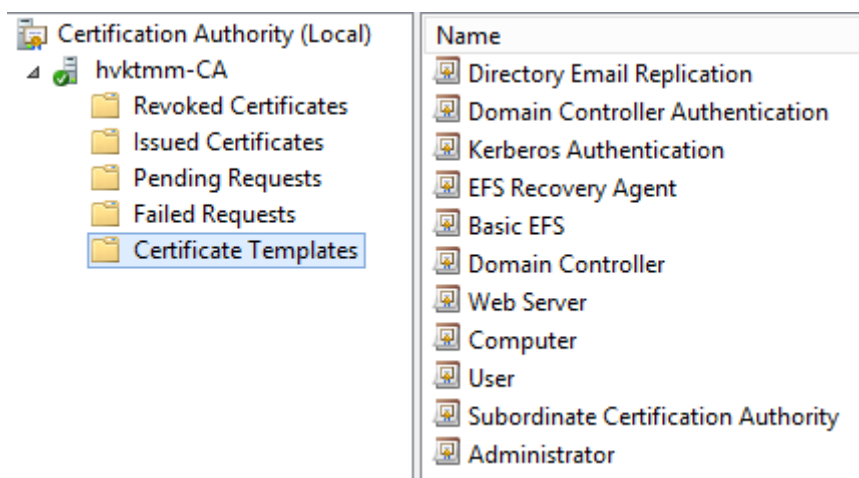
- Active Directory Certificate Services**
 - Certification Authority** ✓ Configuration succeeded
[More about CA Configuration](#)
 - Certification Authority Web Enrollment** ✓ Configuration succeeded
[More about Web Enrollment Configuration](#)

Nhấn Close để đóng cửa sổ hoàn tất cấu hình.

1.4.6. Cấp phát chứng thư số

Truy cập theo đường dẫn để mở giao diện quản lý CA:

Server Manager → Tools → Certification Authority → Certificate Templates.

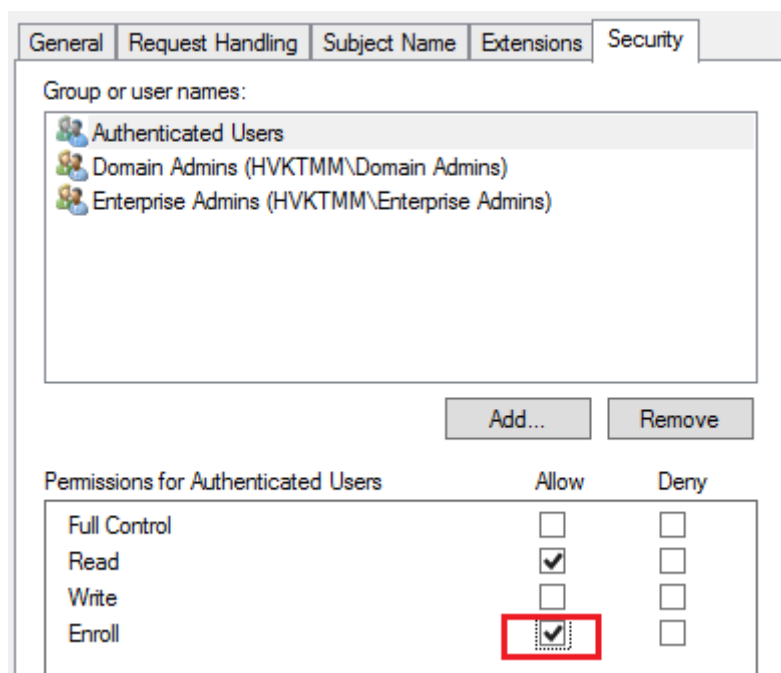


Chuột phải vào mục Certificate Templates → Manage. Tìm đến template cho Web Server.

Smartcard Logon	1	6.1
Smartcard User	1	11.1
Subordinate Certification Authority	1	5.1
Trust List Signing	1	3.1
User	1	3.1
User Signature Only	1	4.1
Web Server	1	4.1
Workstation Authentication	2	101.0

Chuột phải vào Web Server chọn Properties:

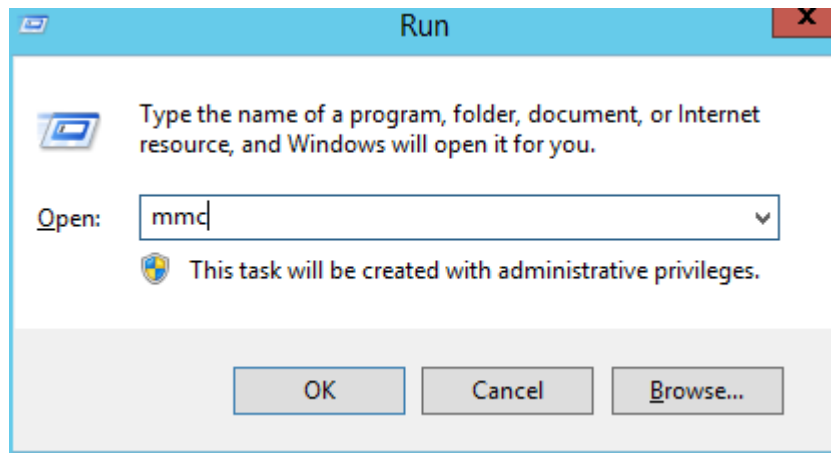
Tab Security, nhóm Authenticated Users: tích chọn Enroll:



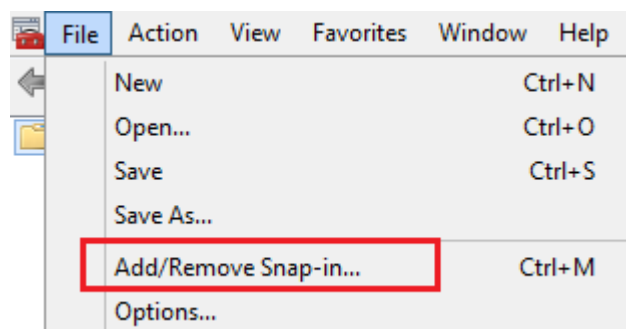
Chọn Apply -> OK.

Đóng cửa sổ quản lý CA.

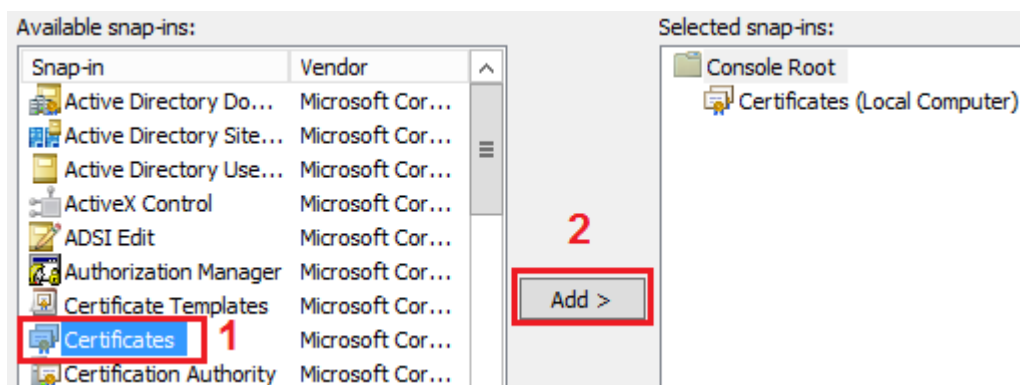
Bật chương trình MMC từ Run:



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

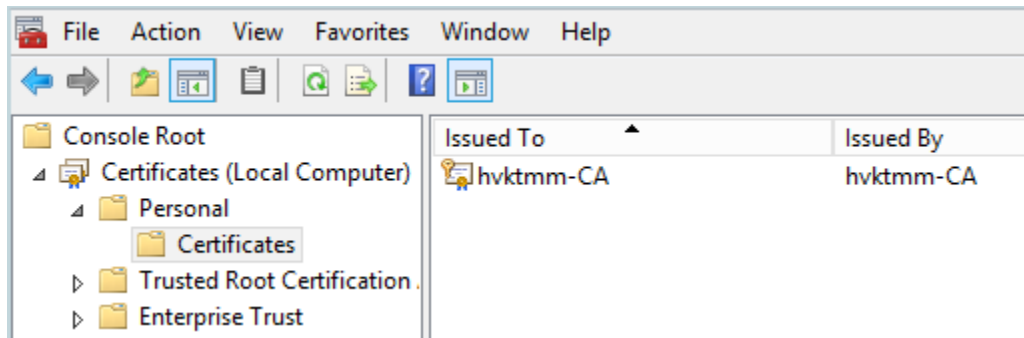


Cửa sổ xuất hiện chọn như hình sau:



Cửa sổ lựa chọn định dạng chứng thư số chọn Computer account → Finish.

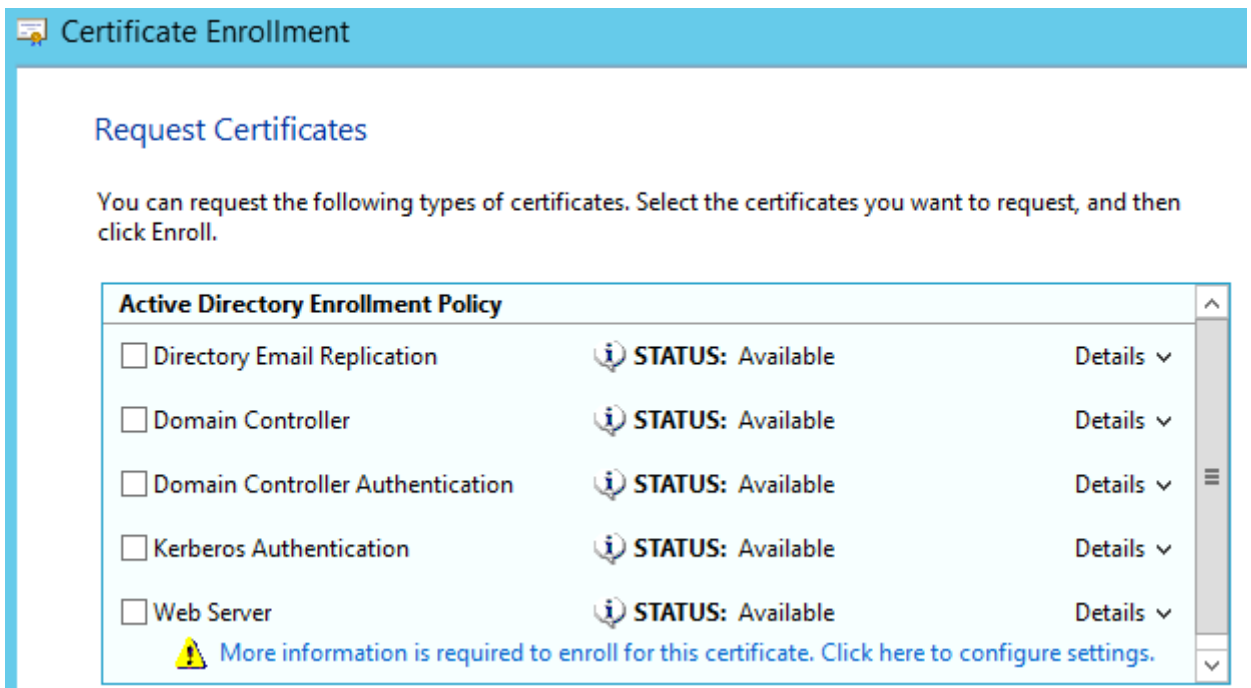
Tại giao diện quản lý chứng thư số:



Chuột phải vào Certificates → All task → Request new certificate

Cửa sổ xuất hiện chọn Next.

Giao diện quản lý chứng thư số mẫu:



Tích chọn dòng chữ màu xanh có cảnh báo màu vàng để cấu hình.

Cửa sổ Certificate Properties xuất hiện. Chọn tab Subject:

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

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 (dropdown)
Value: 192.168.3.150 (text box)

Buttons: Add >, < Remove

CN=192.168.3.150

Chuyển sang tab Private Key tích chọn vào mục Make private key exportable để xuất khóa bí mật.

Certificate Properties

Subject | General | Extensions | Private Key | Certification Authority

Cryptographic Service Provider

Key options
Set the key length and export options for the private key.

Key size: 2048 (dropdown)

☒ Make private key exportable

☐ Allow private key to be archived

☐ Strong private key protection

Chọn Apply -> OK, quay ra giao diện cấu hình ngoài.

Lúc này tích chọn vào ô Web Server:

Active Directory Enrollment Policy

<input type="checkbox"/> Directory Email Replication	<i>i</i> STATUS: Available	Details ▾
<input type="checkbox"/> Domain Controller	<i>i</i> STATUS: Available	Details ▾
<input type="checkbox"/> Domain Controller Authentication	<i>i</i> STATUS: Available	Details ▾
<input type="checkbox"/> Kerberos Authentication	<i>i</i> STATUS: Available	Details ▾
<input checked="" type="checkbox"/> Web Server	<i>i</i> STATUS: Available	Details ▾

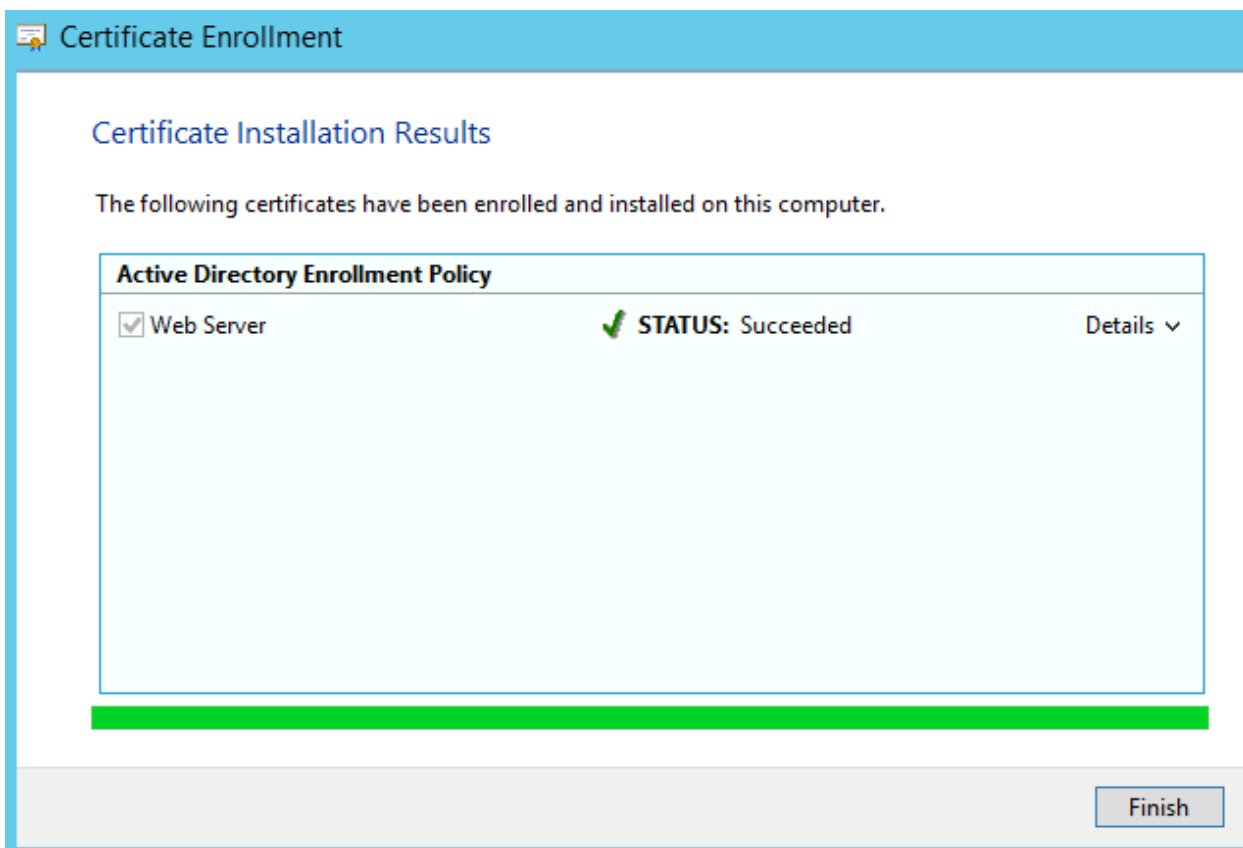
1

☐ Show all templates

2

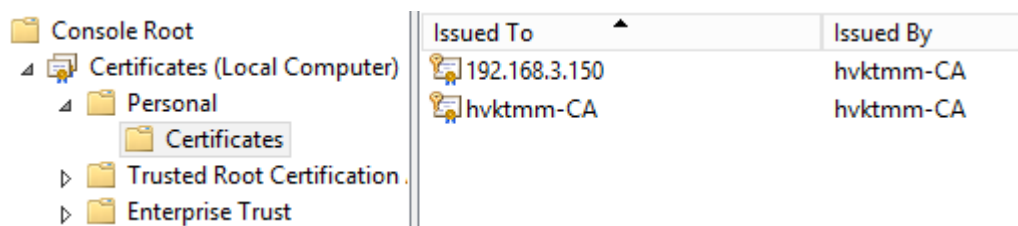
Enroll Cancel

Chọn Enroll để xuất chứng thư số.

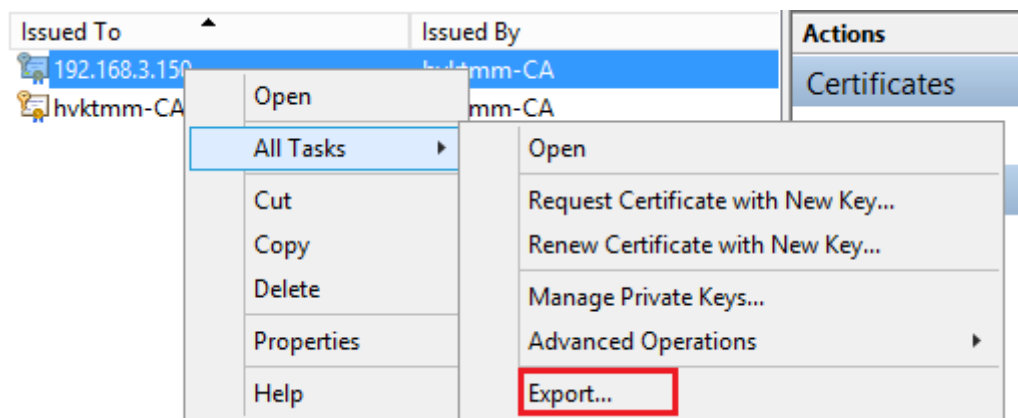


Nhấn Finish để kết thúc.

Lúc này trong mục chứng thư số cá nhân đã có chứng thư số của SRV.



Chuột phải vào chứng thư số của SRV → All Tasks → Export.



Export cả khóa bí mật.

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- ☒ Yes, export the private key
☐ No, do not export the private key

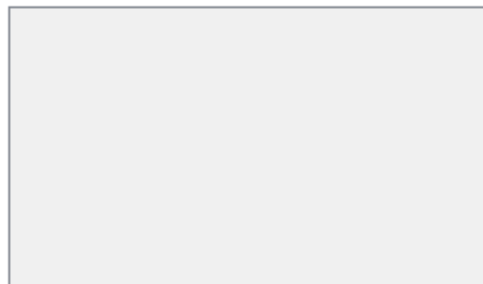
Các bước tiếp theo chọn Next.

Nhập mật khẩu bảo vệ chứng thư:

Security

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)



Add

Remove

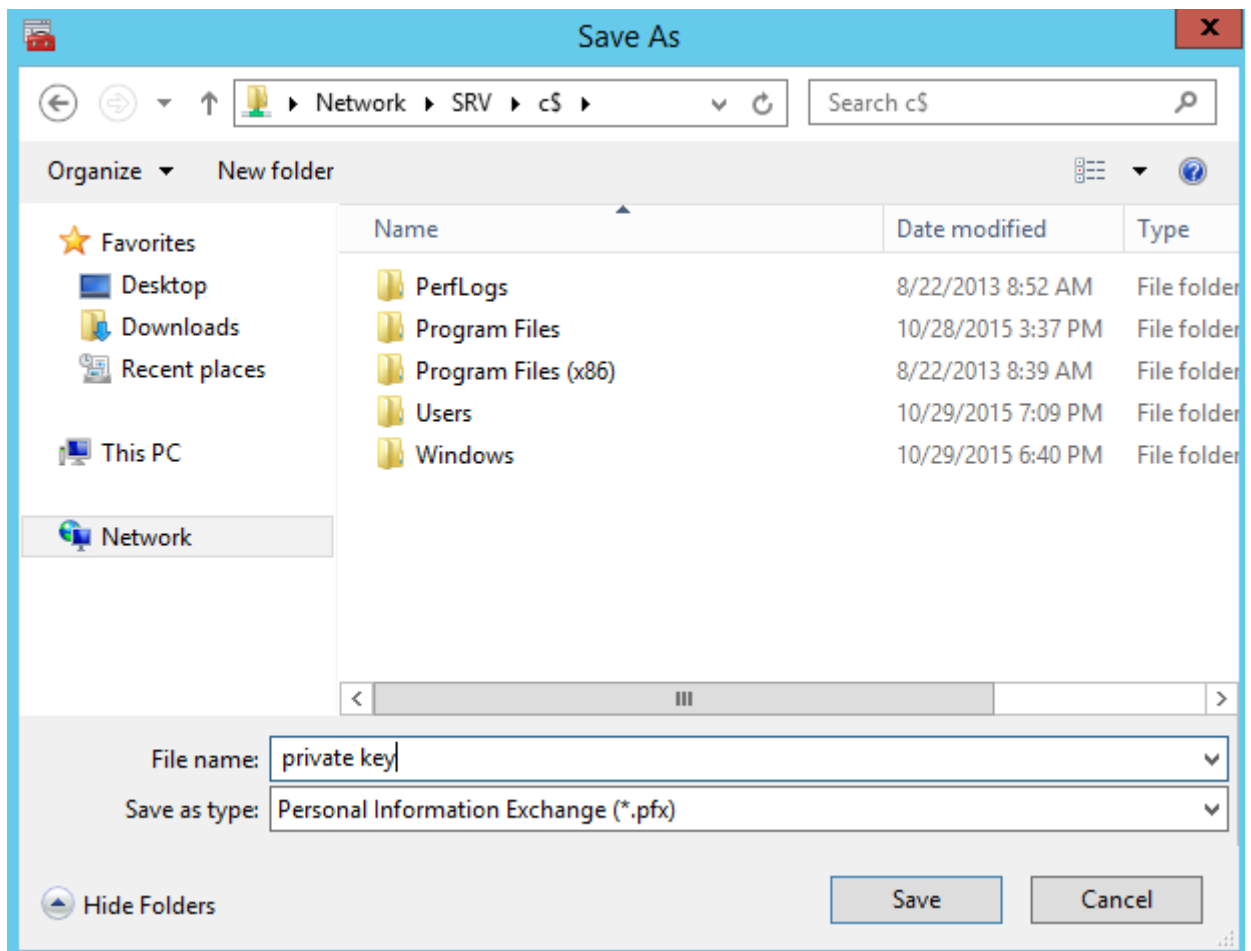
☒ Password:

••••••

Confirm password:

••••••

Giao diện tiếp theo nhập đường dẫn lưu chứng thư số.



Trong hình trên, nơi lưu chứng thư số ổ C của SRV.

Các bước tiếp theo chọn Next và Finish.

Kết thúc cấu hình trên máy chủ DC.

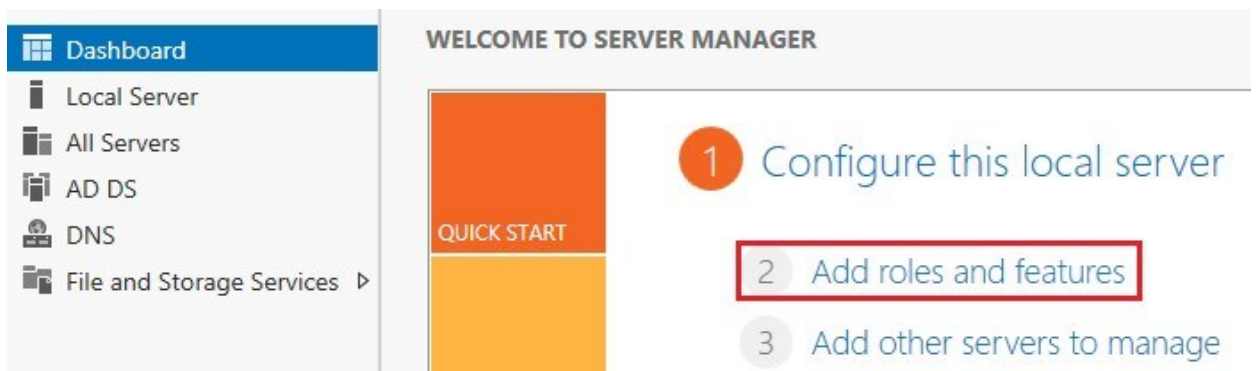
1.5. Thực hiện trên máy chủ SRV

1.5.1. 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.

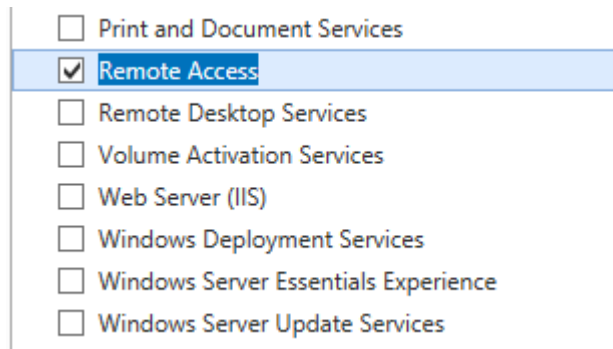
Truy cập theo đường dẫn:

Server Manager → Dashboard → Add roles and features:

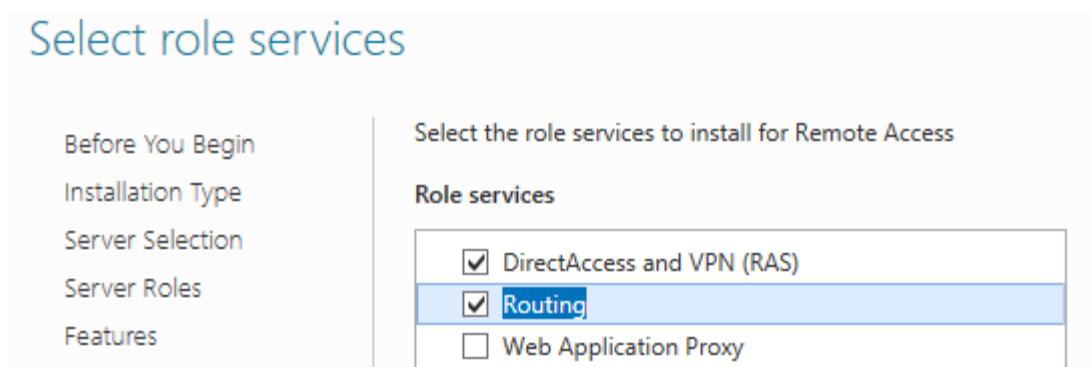


Ba bước đầu tiên để mặc định và chọn Next.

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.

1.5.2. Cấu hình dịch vụ Routing and Remote Access

Cài đặt chứng thư số đã cấp ở bước trước. Truy cập vào ổ C:\

inetpub	10/30/2015 12:44 ...	File folder	
PerfLogs	8/22/2013 8:52 AM	File folder	
Program Files	10/30/2015 12:44 ...	File folder	
Program Files (x86)	10/30/2015 12:44 ...	File folder	
Users	10/30/2015 12:45 ...	File folder	
Windows	10/30/2015 12:45 ...	File folder	
private key	10/30/2015 12:35 ...	Personal Informati...	4 KB

Chuột phải vào chứng thư chọn Install PFX

Giao diện xuất hiện chọn Local Machine.

Tiếp tục nhập mật khẩu đã thiết lập ở bước trên.

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

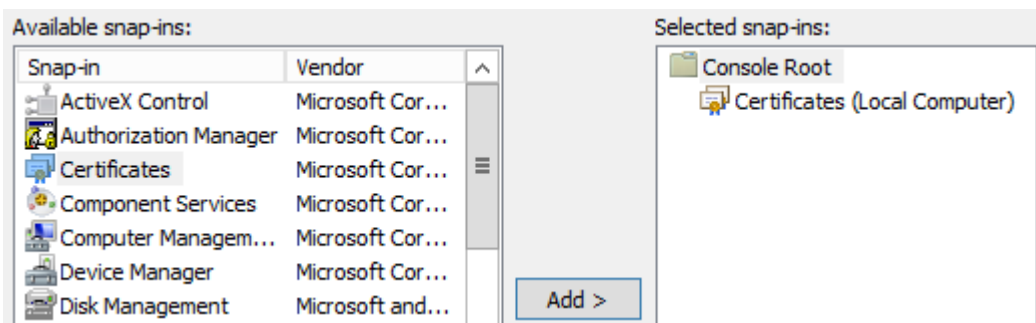
Password:

☐ Display Password

Các bước tiếp theo để mặc định và Install.

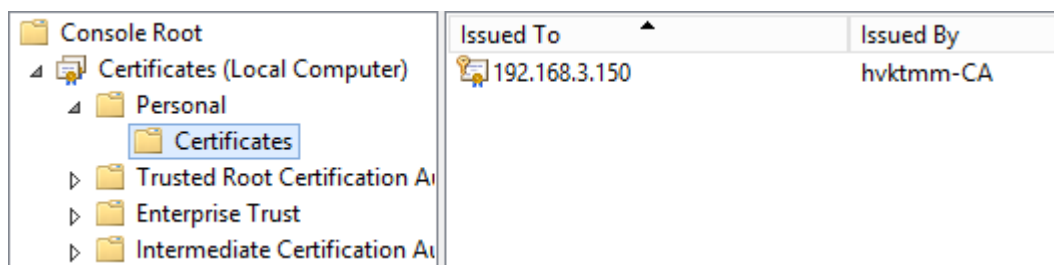
Kiểm tra chứng thư số đã cài. Vào Run gõ MMC → File → Add / Remove snap-in

Chọn Certificate → Add → Computer Account

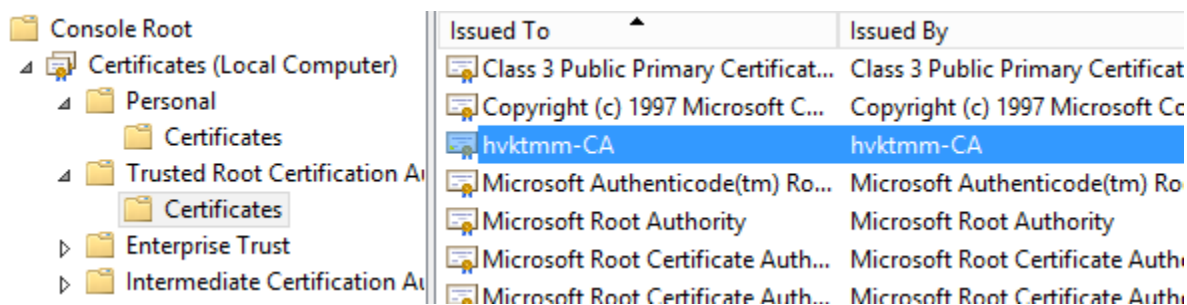


Chọn OK để đóng cửa sổ.

Tại cửa sổ quản lý chứng thư số. Truy cập vào Personal → Certificates. Giao diện bên phải đã thấy chứng thư số dành cho địa chỉ IP của chính máy SRV.



Truy cập vào Trusted Root Certification Authority. Thấy chứng thư số của máy chủ CA.



Thành công bước cài đặt chứng thư số.

Bước tiếp theo cài đặt và cấu hình dịch vụ Routing and Remote Access.

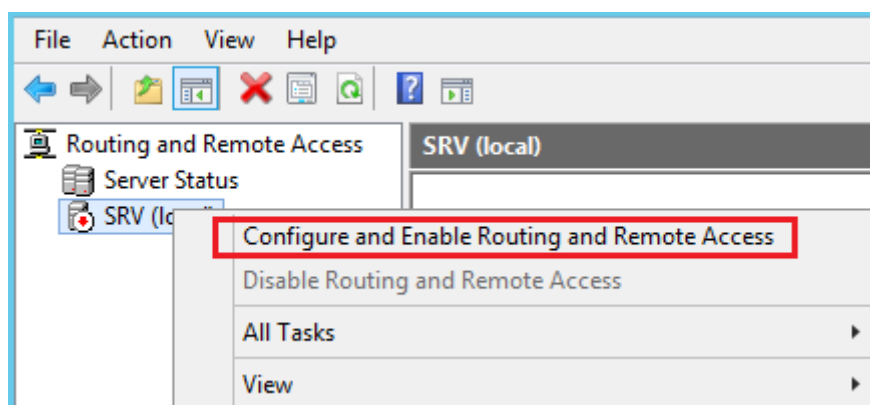
Truy cập theo đường dẫn:

Server Manager → Tools → Routing and Remote Access

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

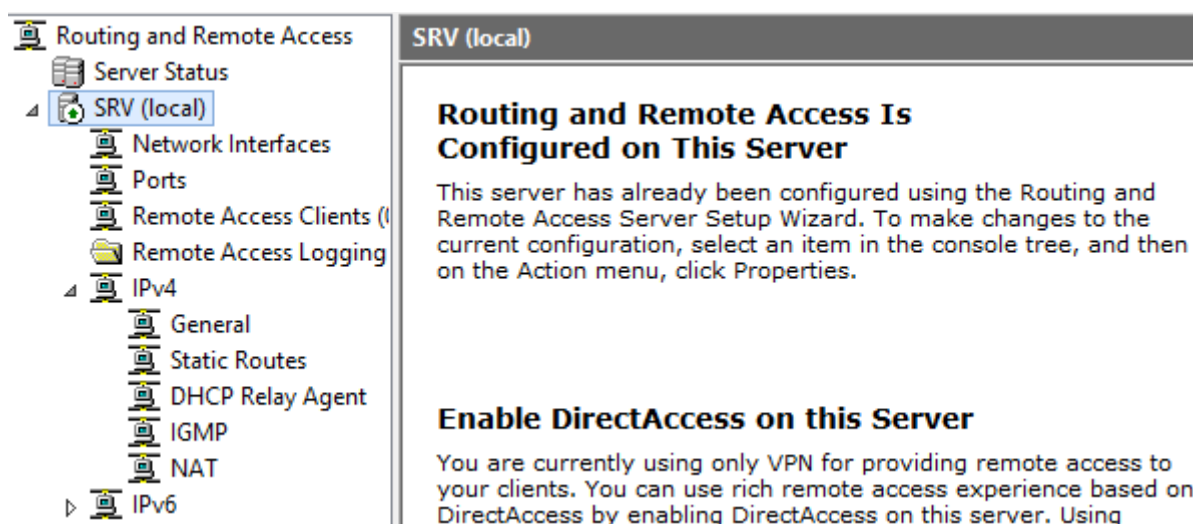
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

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

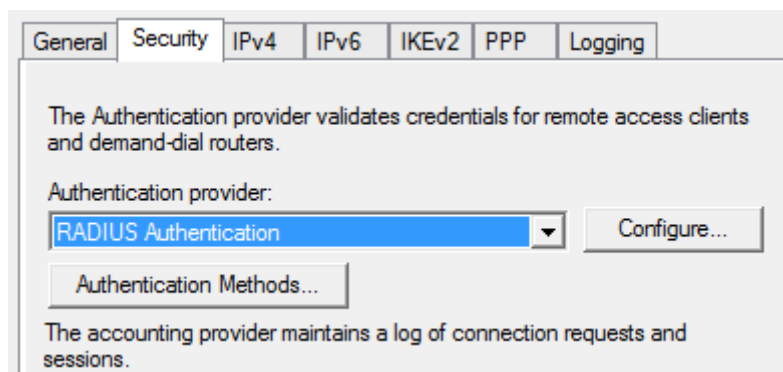
Chọn Next và Finish để kết thúc.

Giao diện sau khi cài đặt.



Chuột phải vào tên máy chủ SRV chọn Properties.

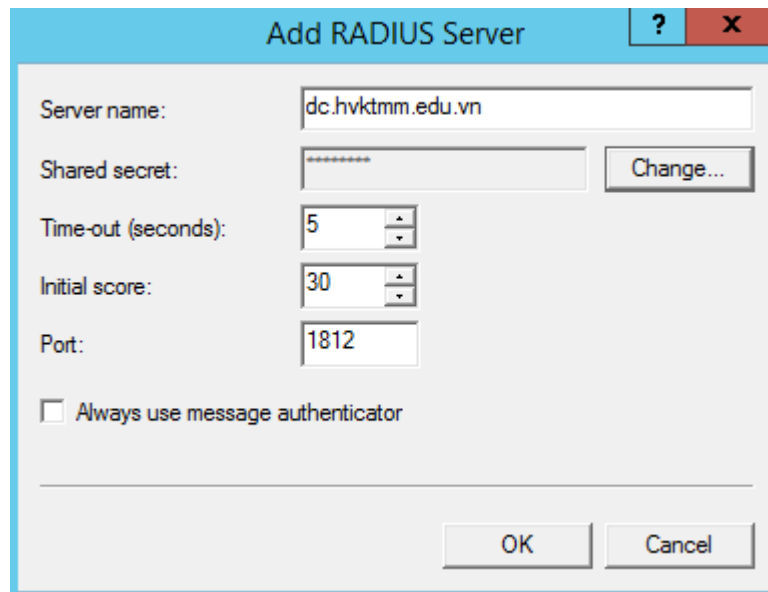
Tab Security chọn phương thức xác thực là RADIUS. Tiếp chọn Configure.



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.edu.vn

Shared secret: [masked] Change...

Time-out (seconds): 5

Initial score: 30

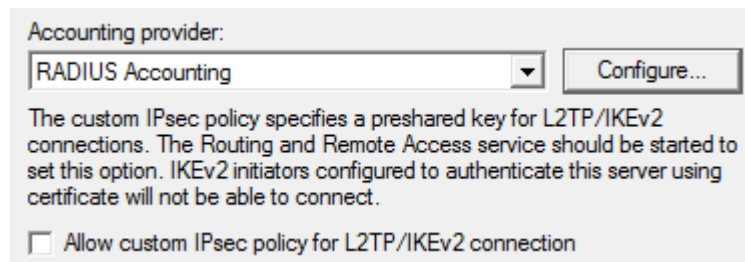
Port: 1812

☐ Always use message authenticator

OK Cancel

Nhấn OK để đóng cửa sổ.

Tương tự thiết lập cho mục Accounting provider:



Accounting provider:

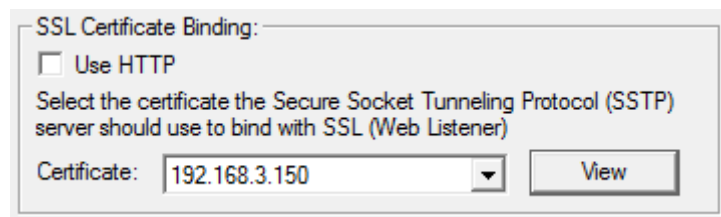
RADIUS Accounting Configure...

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:

VPN:



SSL Certificate Binding:

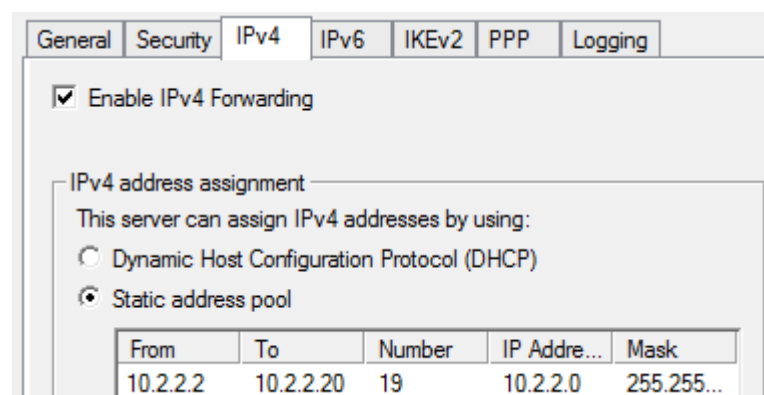
☐ Use HTTP

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

Certificate: 192.168.3.150 View

Chuyển sang Tab IPv4.

Chọn Static address và nhập dãy IP sẽ cấp phát cho máy trạm khi kết nối



General Security **IPv4** IPv6 IKEv2 PPP Logging

☒ Enable IPv4 Forwarding

IPv4 address assignment

This server can assign IPv4 addresses by using:

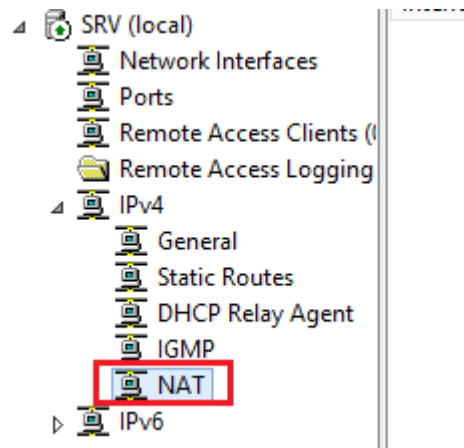
☐ Dynamic Host Configuration Protocol (DHCP)

☒ Static address pool

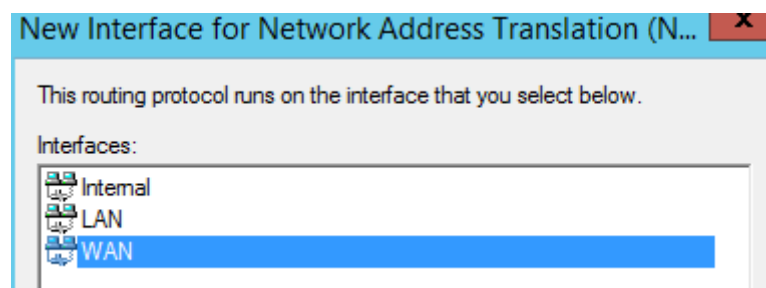
From	To	Number	IP Address	Mask
10.2.2.2	10.2.2.20	19	10.2.2.0	255.255...

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.

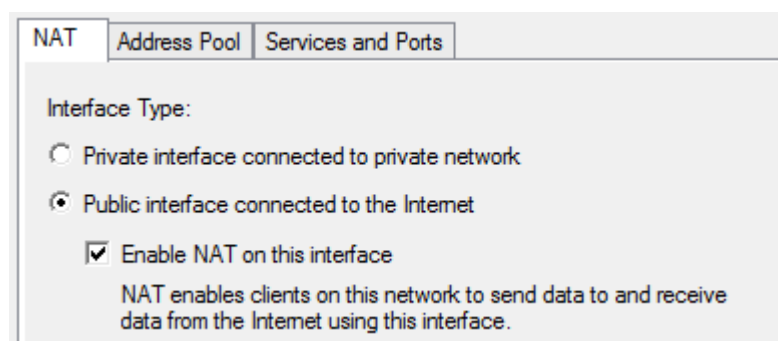


Chuột phải vào NAT, chọn New Interface. Giao diện xuất hiện chọn Interface bên ngoài WAN.



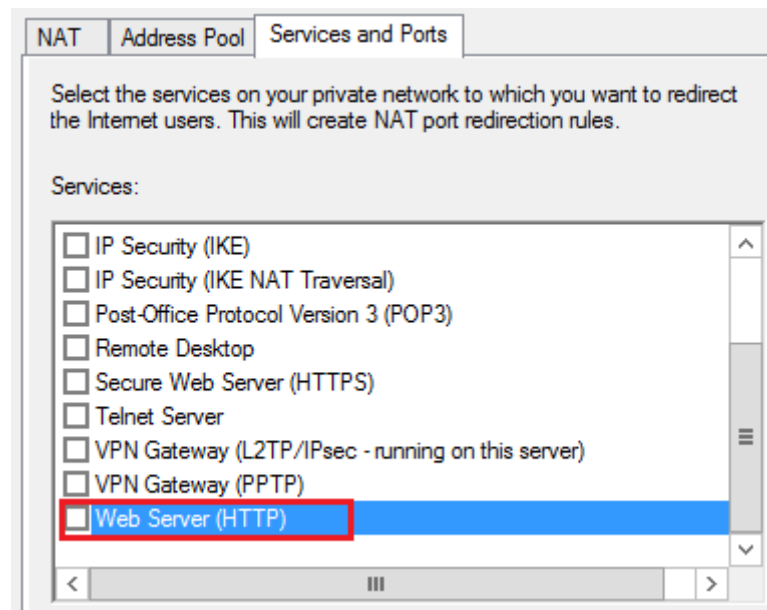
Nhấn OK sẽ xuất hiện cửa sổ cấu hình.

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:

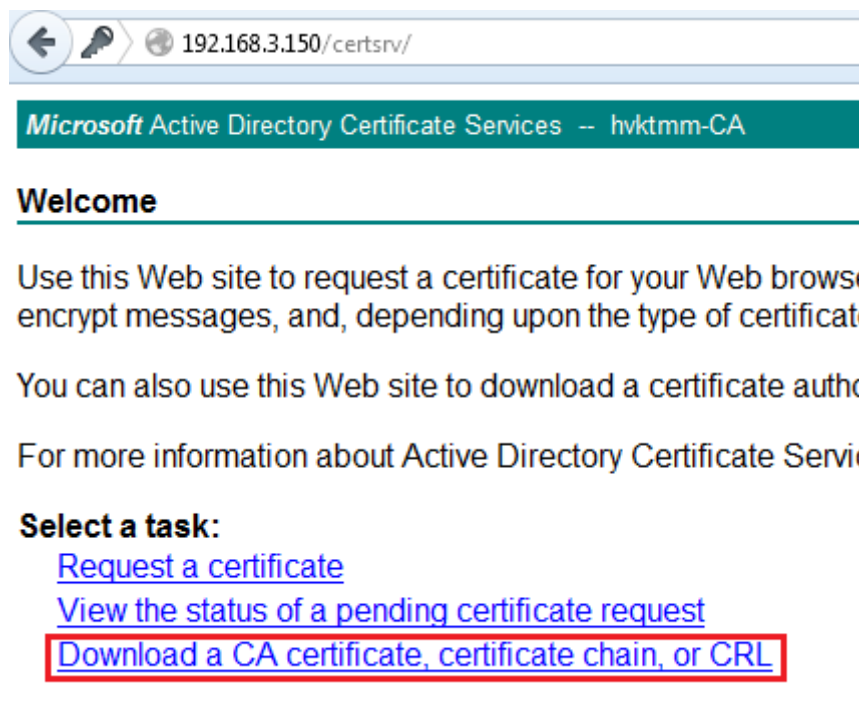
Private address:

Outgoing port:

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

1.6. Thực hiện trên máy Windows 7

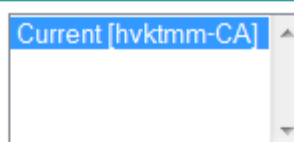
Truy cập tới dịch vụ cấp phát chứng thư số trong máy chủ DC thông qua trình duyệt web. Nhập IP bên ngoài của máy SRV.



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.

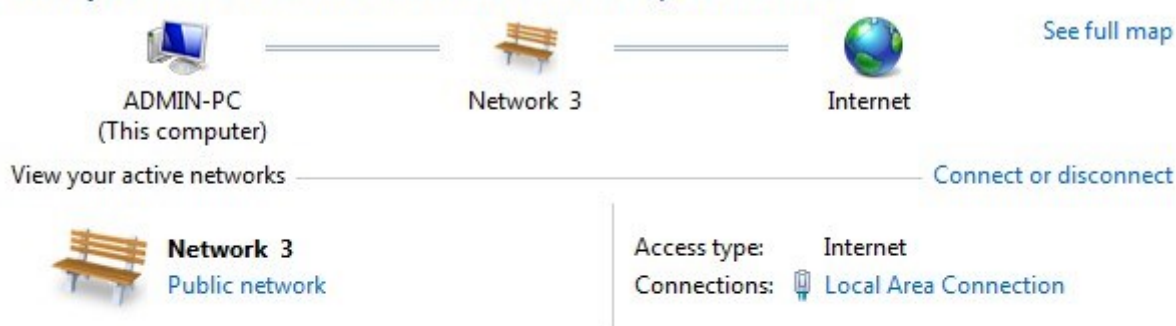
Tương tự như các bước trên bật Run gõ MMC. Chọn Certificate

Trong mục Trusted Root CA chọn Import chứng thư số của DC vừa mới tải về.



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:

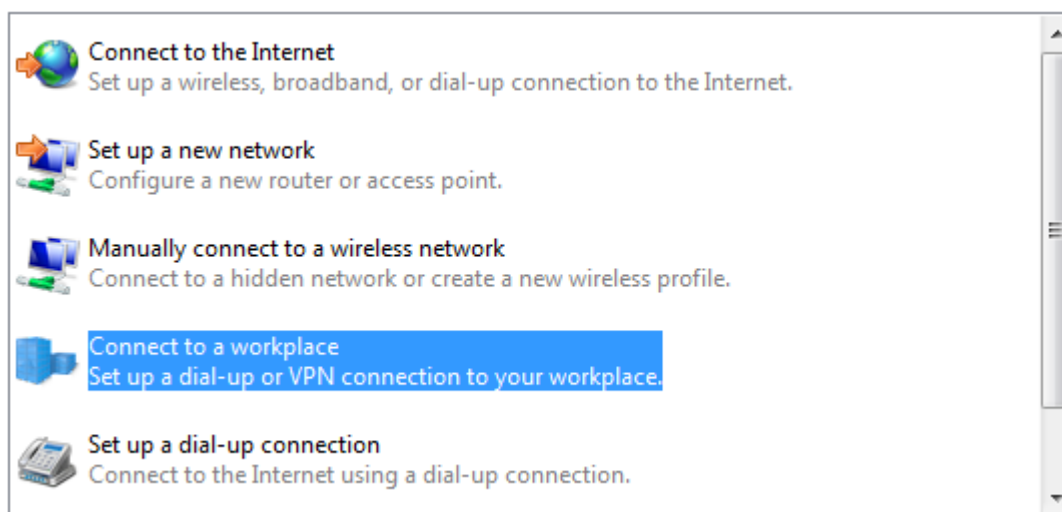
View your basic network information and set up connections



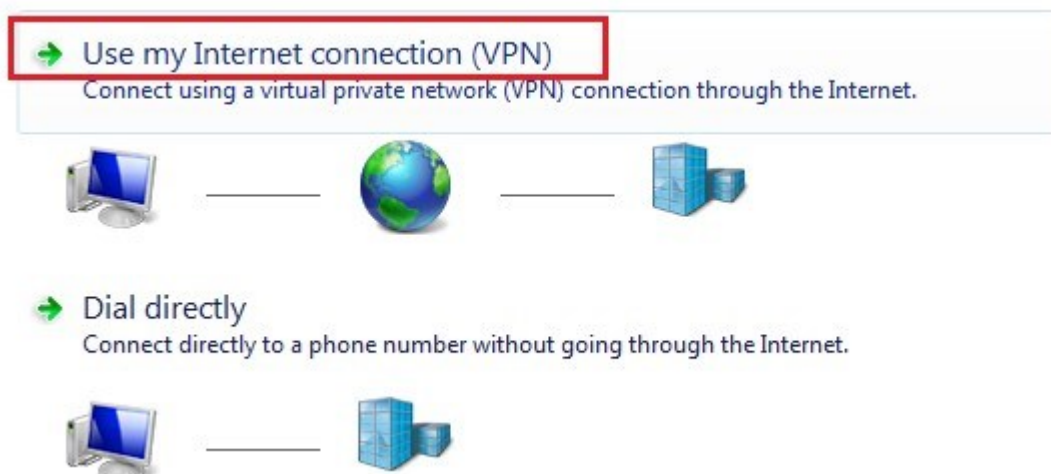
Change your networking settings

-  **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.

Giao diện tiếp theo chọn Connect to a workplace:



Giao diện tiếp theo chọn kết nối thông qua VPN:



Giao diện tiếp theo nhập địa chỉ IP bên ngoài của SRV (kết nối với Windows 7). Đặt tên cho kết nối:

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 192.168.3.150

Destination name: HVKTMM VPN

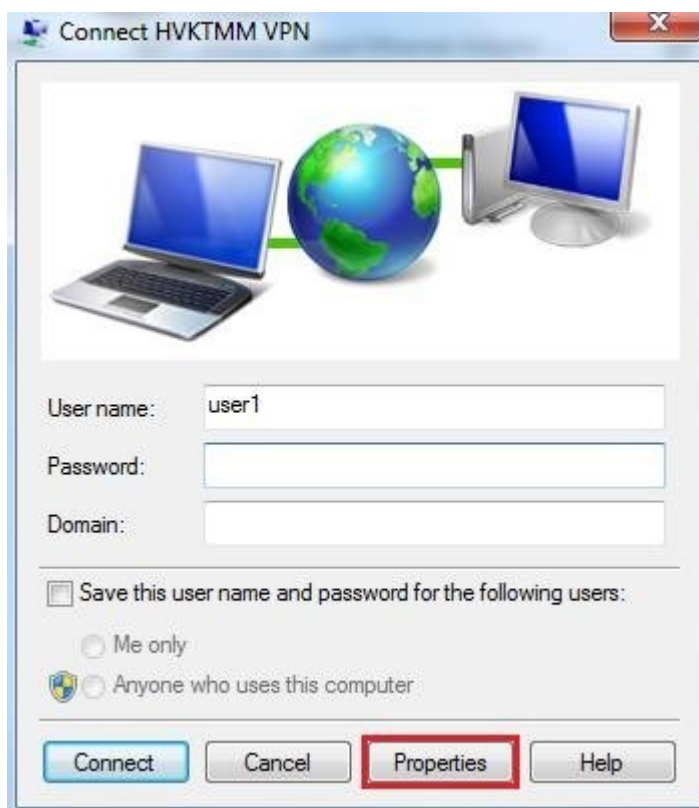
Bước kết tiếp nhập tài khoản đã tạo trên máy chủ DC.

Type your user name and password

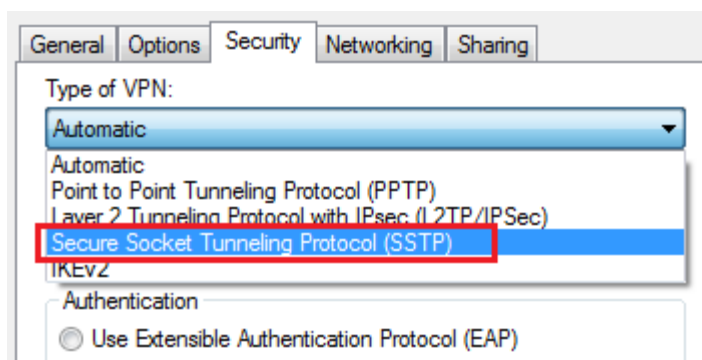
User name: user1

Password: ●●●●●●●●

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.

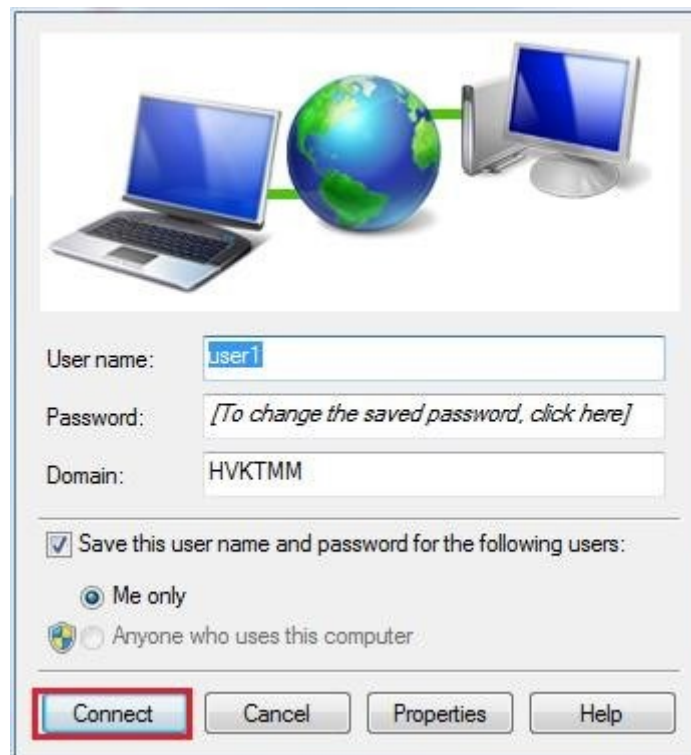
Chuột phải vào mục Parameters → New → DWORD

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.

Quy trở lại cửa sổ đăng nhập kết nối. Nhập lại tên và mật khẩu của người dùng user1. Nhấn Connect để kết nối.



Kết quả thành công.

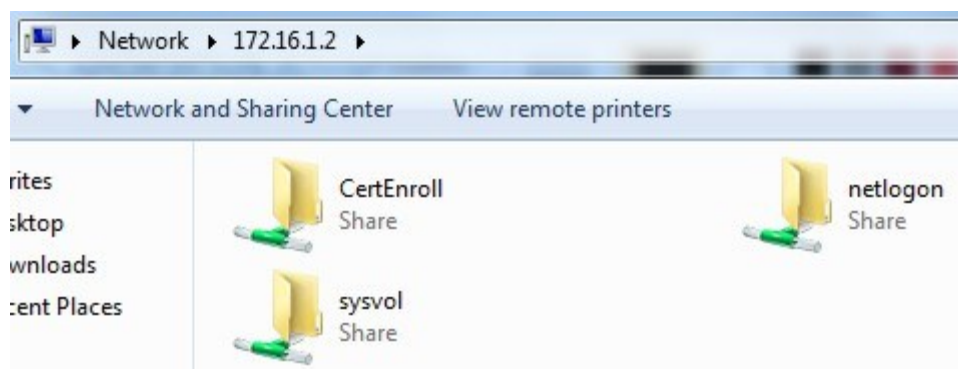
1.7. Kiểm tra kết quả

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:

Filter: ip.addr==192.168.3.150						
No.	Time	Source	Destination	Protocol	Length	Info
41	5.31622100	192.168.3.170	192.168.3.150	TLSv1	155	Application Data
42	5.31786400	192.168.3.150	192.168.3.170	TLSv1	192	Application Data, Appl
44	5.51585500	192.168.3.170	192.168.3.150	TCP	54	53678 > https [ACK] Se
47	6.31713500	192.168.3.170	192.168.3.150	TLSv1	155	Application Data
48	6.31860200	192.168.3.150	192.168.3.170	TLSv1	192	Application Data, Appl
51	6.51693600	192.168.3.170	192.168.3.150	TCP	54	53678 > https [ACK] Se
52	6.84017000	192.168.3.150	192.168.3.170	TLSv1	192	Application Data, Appl
56	7.03992900	192.168.3.170	192.168.3.150	TCP	54	53678 > https [ACK] se
57	7.04012700	192.168.3.170	192.168.3.150	TLSv1	139	Application Data
58	7.09141600	192.168.3.150	192.168.3.170	TCP	60	https > 53678 [ACK] se
60	7.31818200	192.168.3.170	192.168.3.150	TLSv1	155	Application Data
61	7.31954900	192.168.3.150	192.168.3.170	TLSv1	192	Application Data, Appl
63	7.51994000	192.168.3.170	192.168.3.150	TCP	54	53678 > https [ACK] se

Các gói tin đã được mã hóa với giao thức TLSv1.

Kết thúc bài thực hành./.

PHỤ LỤC