**Lab 8. Applied Cryptography**

**1. Yêu cầu**

Telnet & SSH: Cấu hình truy cập từ xa cho router qua Telnet và SSH.

HTTPS:

* Tạo CA server để cấp Certificate cho Web Server.
* Cấu hình Web Server để truy cập Website qua giao thức HTTPS.

**2. Kịch bản**

Telnet & SSH:

* Cấu hình IP cho router.
* Cấu hình Telnet và SSH để đăng nhập vào router từ xa.

HTTPS:

* Máy chủ CA cấp chứng chỉ SSL cho Web Server.
* Web Server sử dụng chứng chỉ để truy cập website qua giao thức HTTPS an toàn.

**3. Công cụ/Mô hình**



Thiết bị mạng: Router.

Máy chủ:

* Máy CA Server (Domain Controller).
* Máy Web Server (chạy IIS).

Phần mềm:

* Windows Server (Cài đặt Active Directory Certificate Services).
* Trình duyệt web để truy cập HTTP/HTTPS.
* Công cụ dòng lệnh (cmd, ssh).

**4. Cài đặt**

**Telnet:**

Cấu hình IP Address.

Cấu hình Telnet trên Router:

R(config)# line vty 0 4

R(config-line)# password 123456

R(config-line)# login

Cấu hình Enable password:

R(config)# enable password 111111

(hoặc dùng enable secret).

**SSH:**

Cấu hình hostname và domain-name:

R(config)# hostname R1

R(config)# ip domain-name hcmute.edu.vn

Thiết lập console và enable password.

Tạo khóa RSA:

R(config)# crypto key generate rsa

Cấu hình VTY để chỉ cho phép SSH:

R(config)# line vty 0 4

R(config-line)# transport input ssh

R(config-line)# login local

Tạo user đăng nhập:

R(config)# username admin password 111111

Kiểm tra kết nối SSH từ máy tính:

C:\> ssh -l <username> <IP>

**HTTPS:**

**CA Server:**

Cài đặt Domain Controller với domain XYZ.COM.

IP: 192.168.12.254 / Subnet: 255.255.255.0 / DNS: 192.168.12.254.

Cài dịch vụ Active Directory Certificate Services.

Promote server thành Domain Controller.

**Web Server:**

IP: 192.168.12.200 / DNS: 192.168.12.254.

Cài dịch vụ Web Server (IIS).

Tạo Certificate Request trên IIS.

Gửi yêu cầu ký chứng chỉ tới CA Server tại http://192.168.12.254/certsrv.

CA Server duyệt yêu cầu và cấp chứng chỉ.

Tải chứng chỉ về, cài đặt vào Web Server.

Cấu hình IIS yêu cầu HTTPS và SSL.

**5. Các bước thực hiện**

**Telnet:**

1. Cấu hình IP cho router.
2. Thiết lập Telnet password.
3. Cấu hình enable password hoặc enable secret.

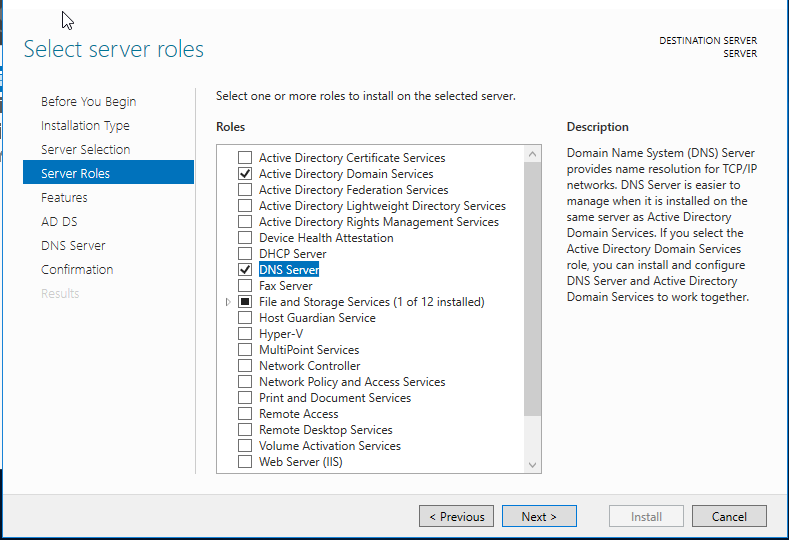
**SSH:**

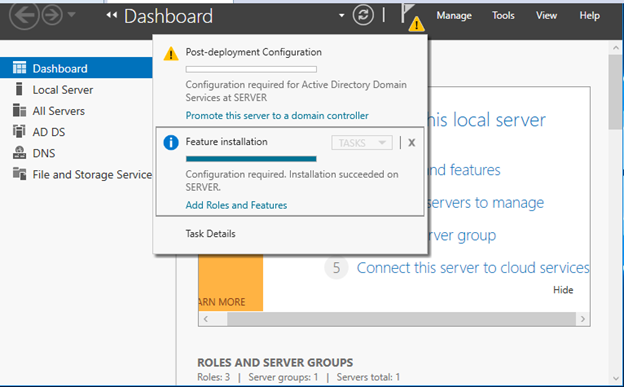
1. Cấu hình hostname và domain-name.
2. Thiết lập console password và enable password.
3. Tạo khóa RSA.
4. Giới hạn VTY chỉ nhận SSH.
5. Tạo user đăng nhập SSH.
6. Kiểm tra SSH bằng lệnh.

**HTTPS:**

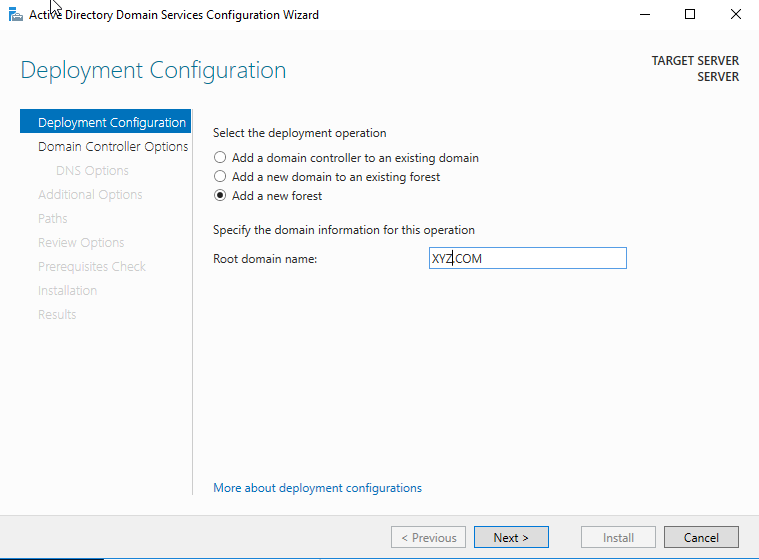
1. Trên CA Server:

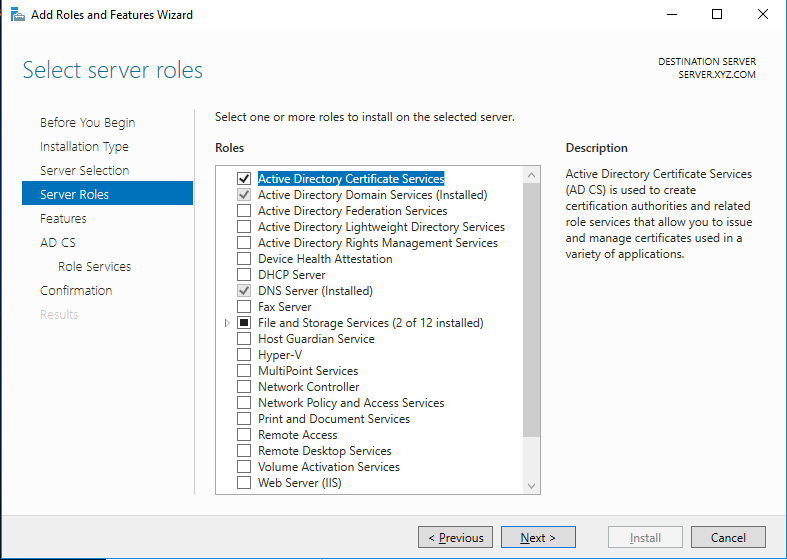
Cài Active Directory Certificate Services.

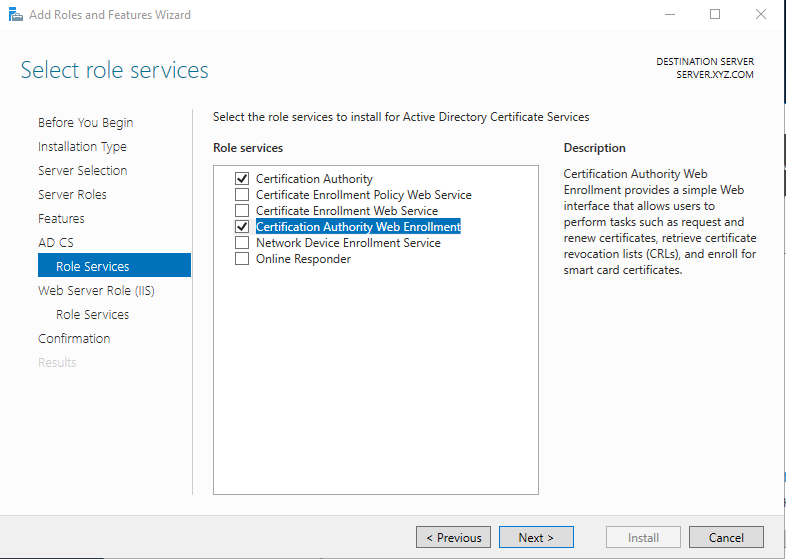


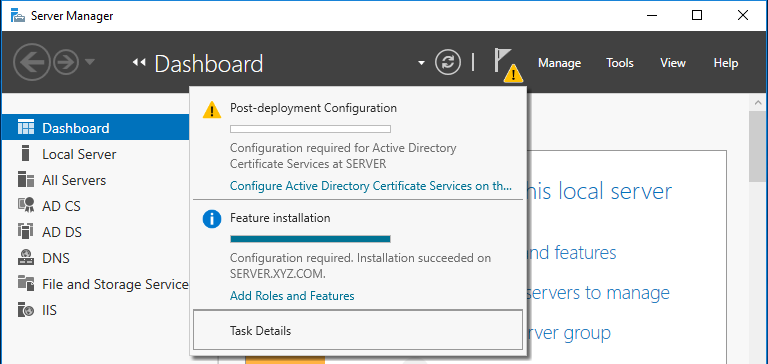


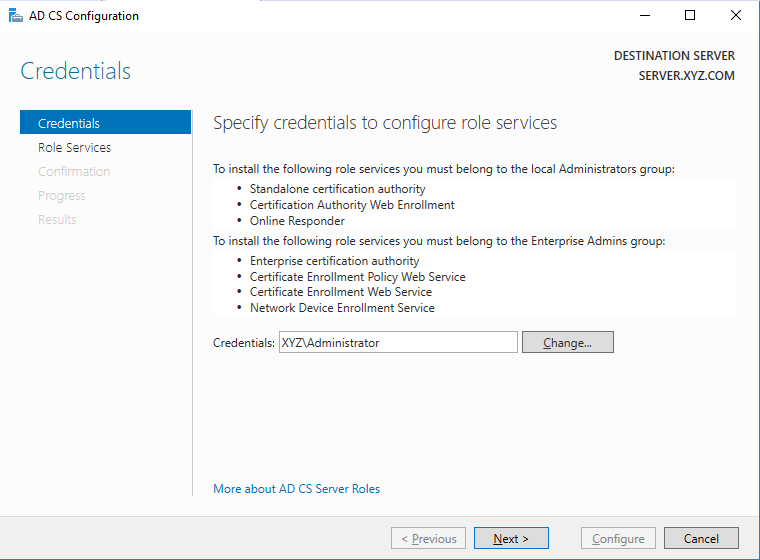
Promote thành Domain Controller.

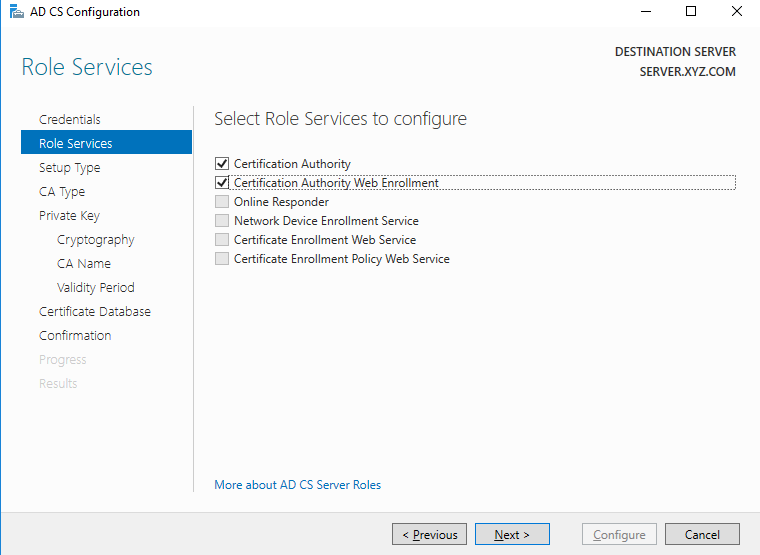


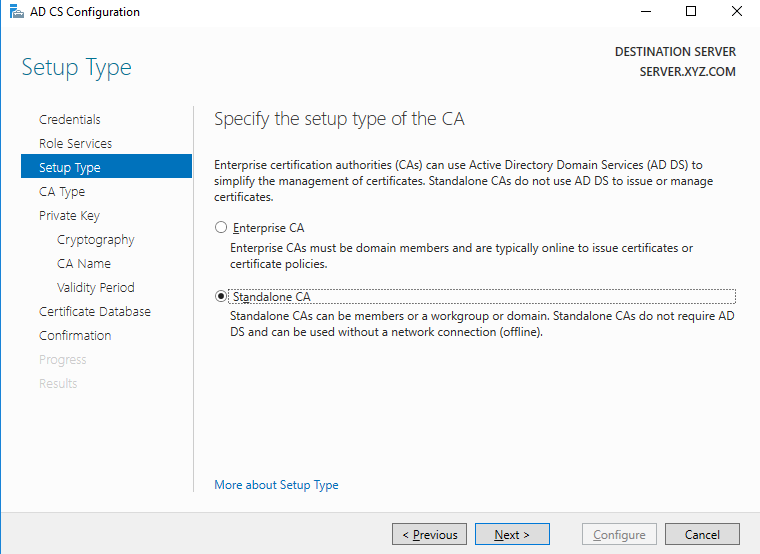


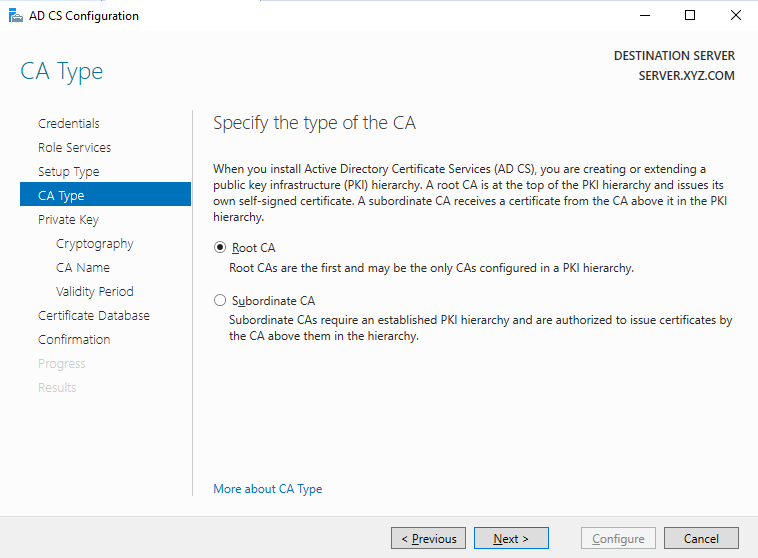


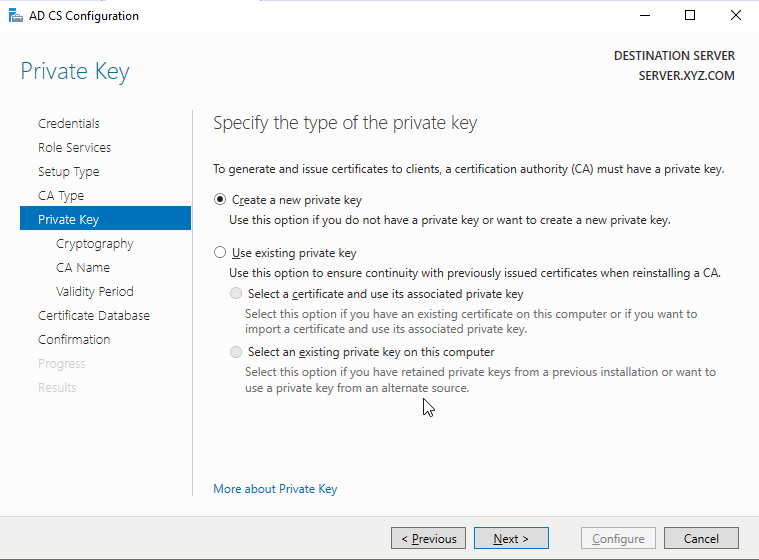


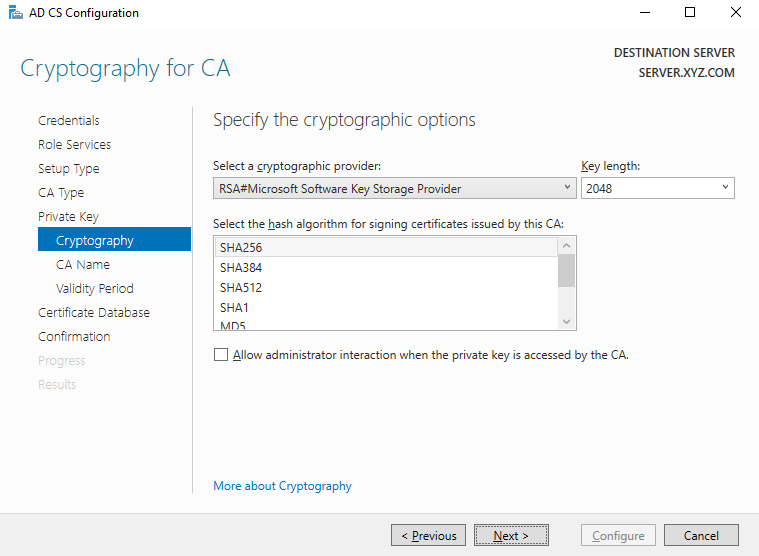


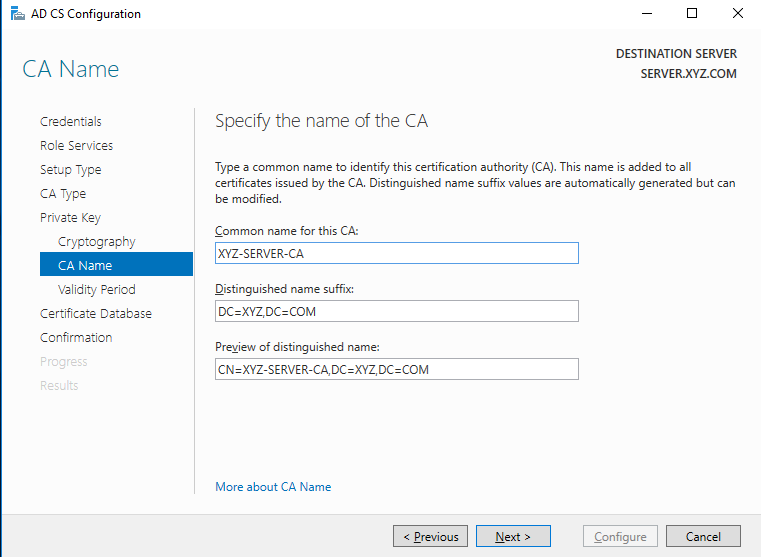


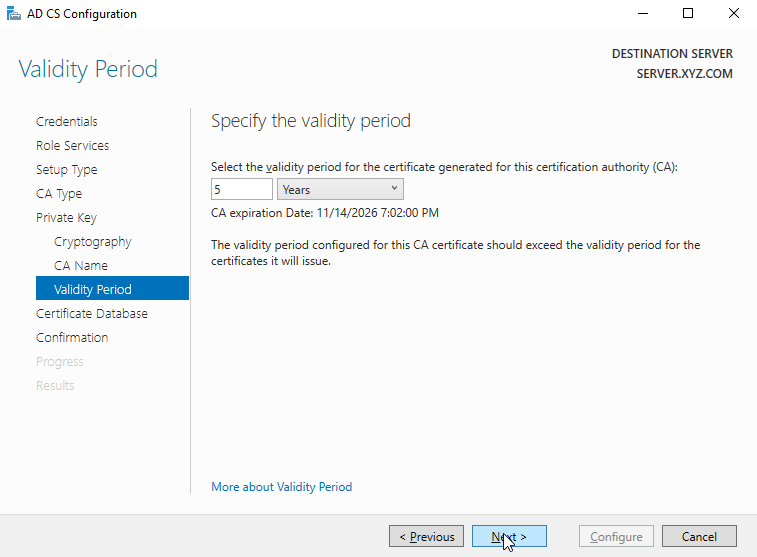


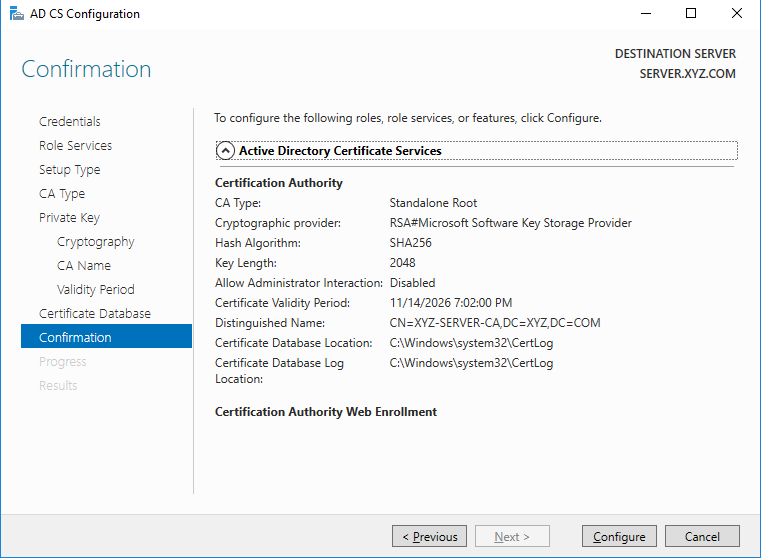


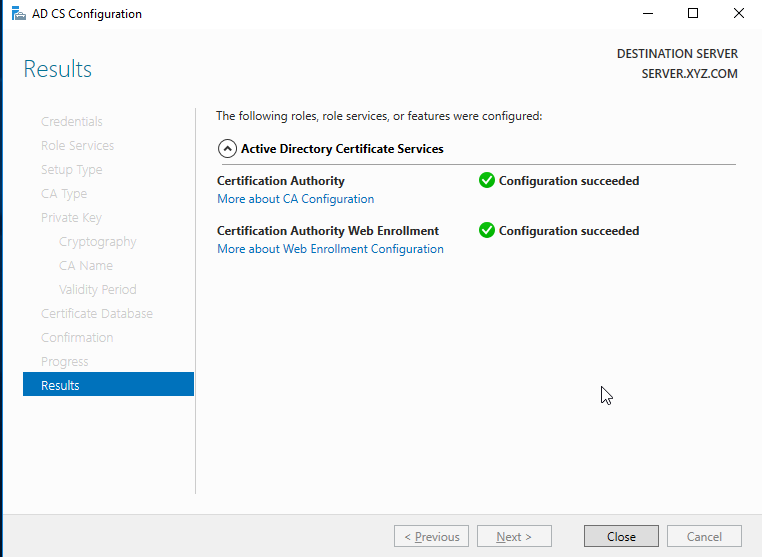




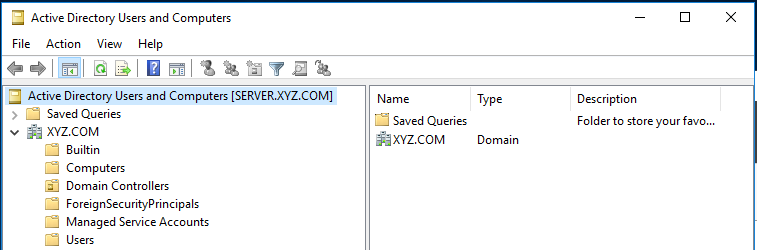


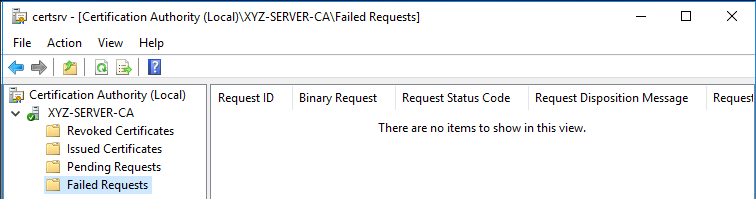






**Kết quả:**





1. Trên Web Server:

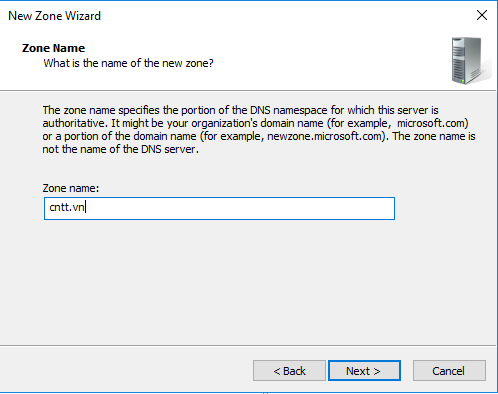
Tạo Certificate Request.

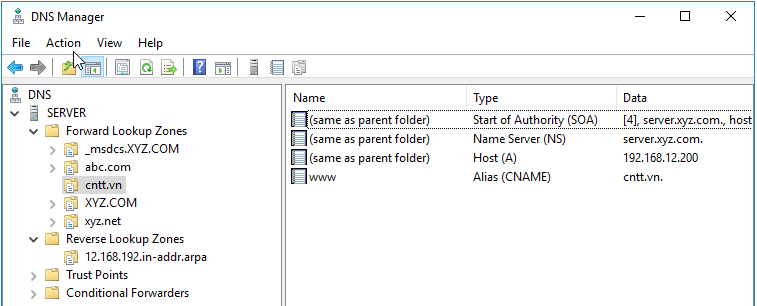
Gửi yêu cầu tới CA Server.

CA Server duyệt và cấp chứng chỉ.

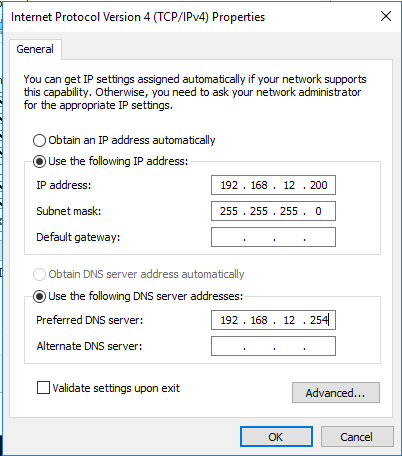
Tải chứng chỉ về và import vào Web Server.

Cấu hình SSL trên IIS (Require SSL, Edit Bindings).

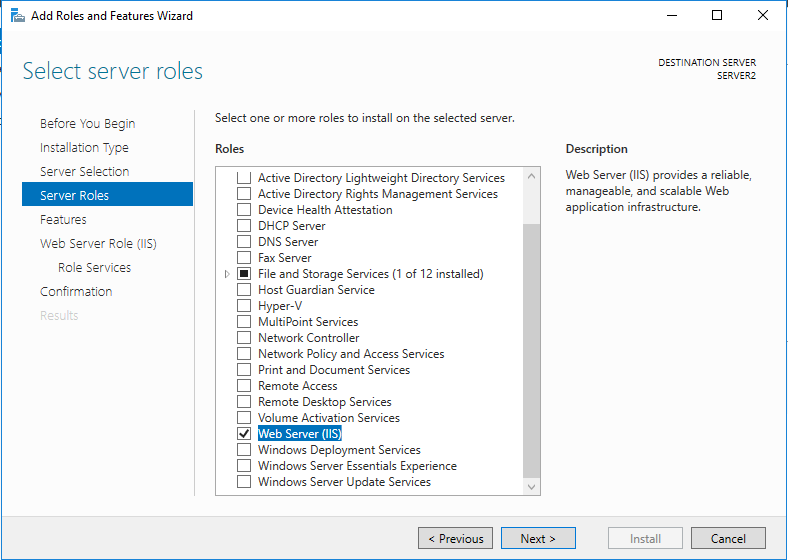


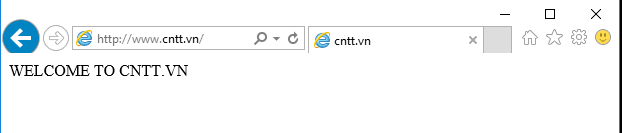


**Máy Web server**

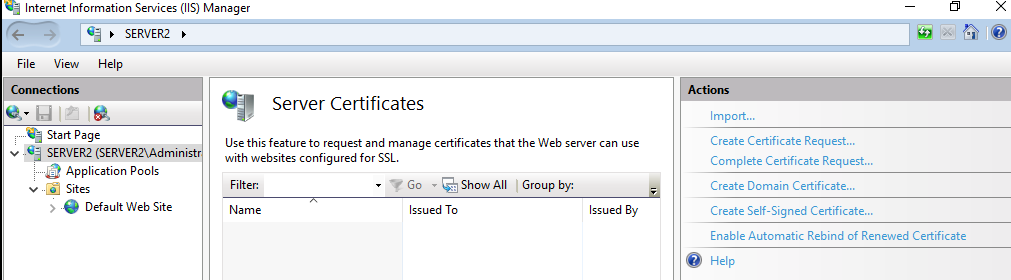


Cài dịch vụ Web server

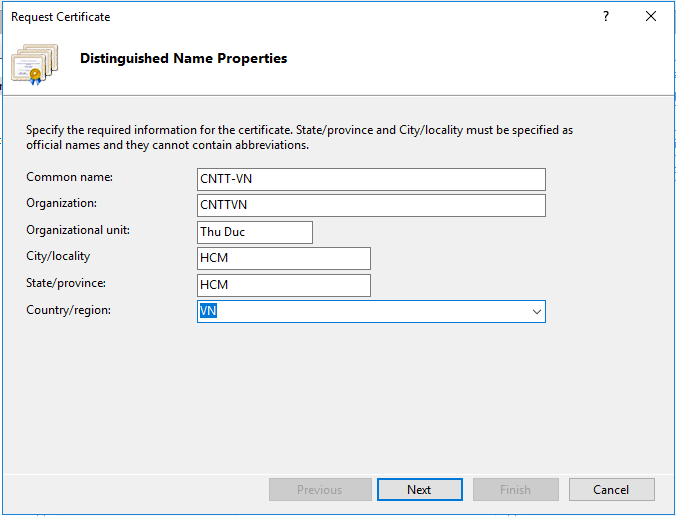


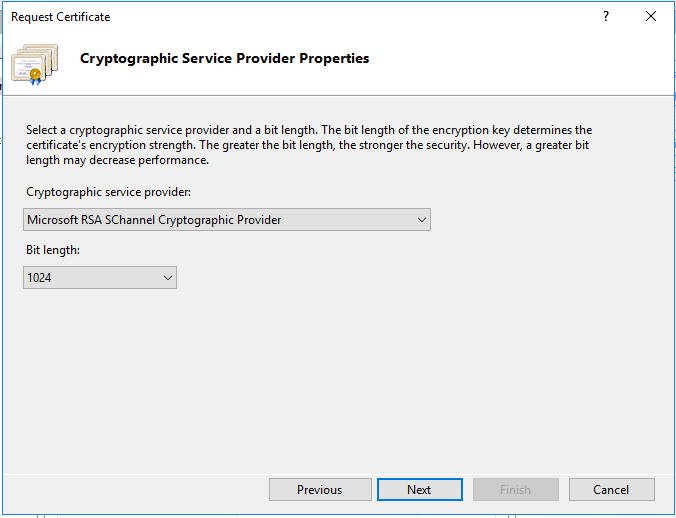


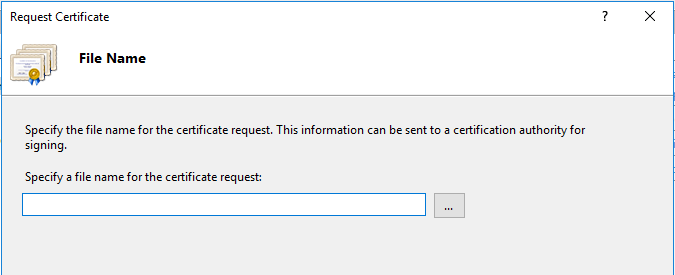
Cấu hình SSL



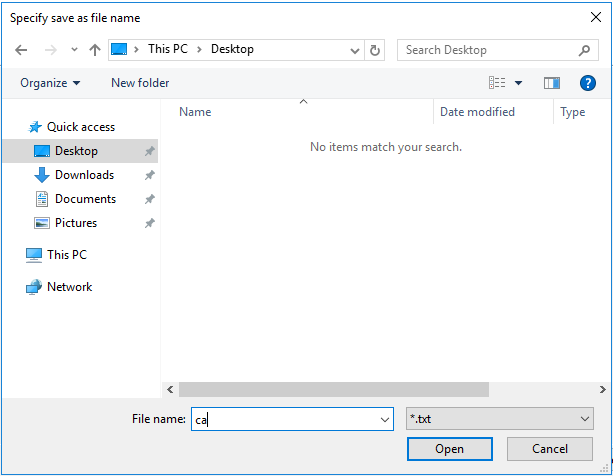
Click Create Certificate Request

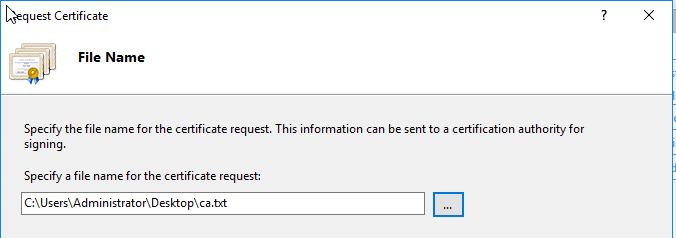




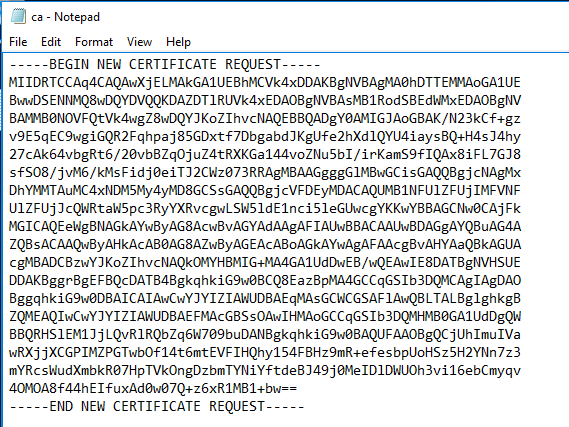


Click vào dấu …

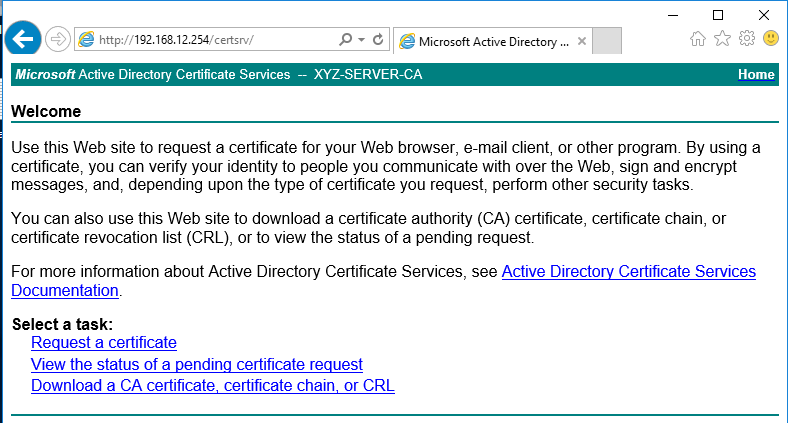




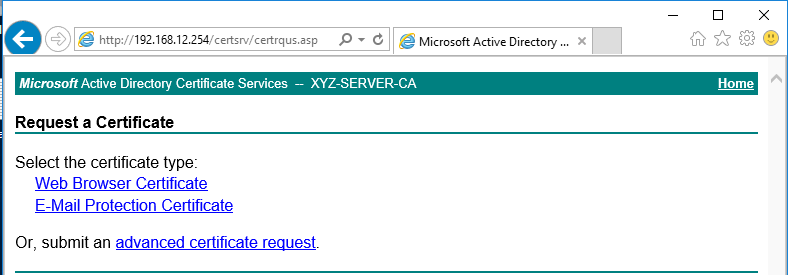
File ca.txt



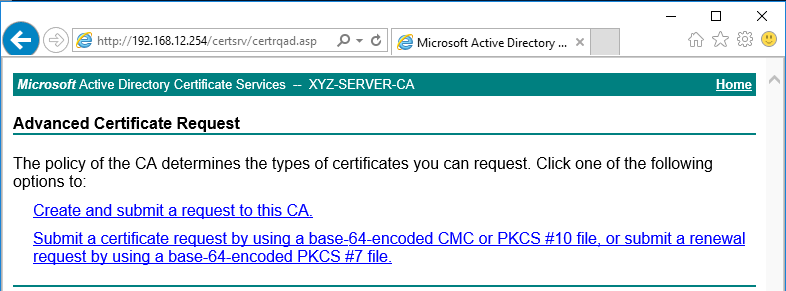
Truy cầp vào CA server: <http://192.168.12.254/certsrv>



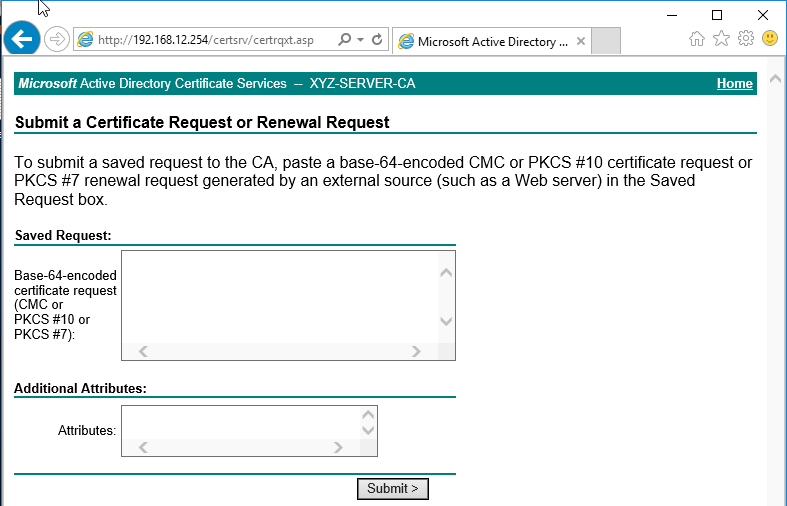
Chọn Request a certificate



Chọn advanced certificate request

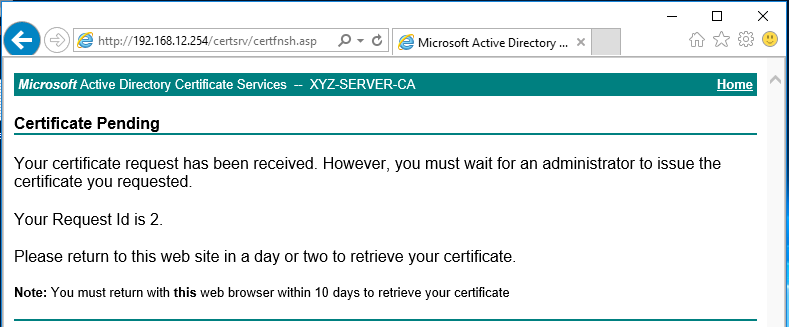


Chọn Submit a certificate by using …

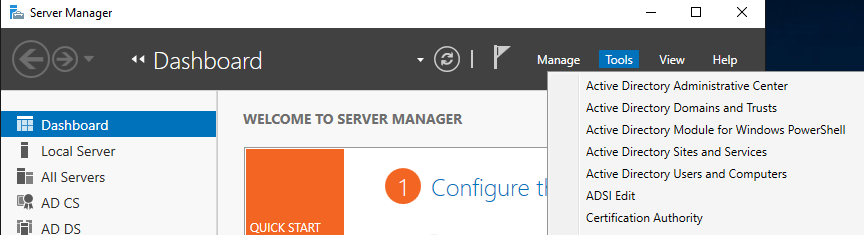


Mở và copy nội dung trong file ca.txt bỏ vào mục Base-64….

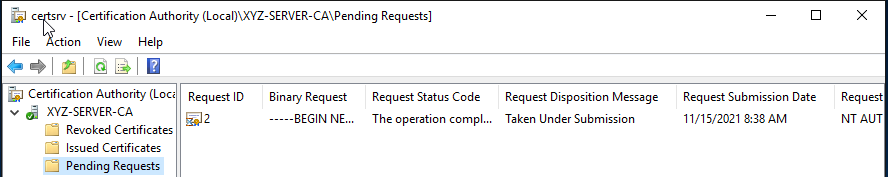
Click Submit



Step . Trên máy CA Server

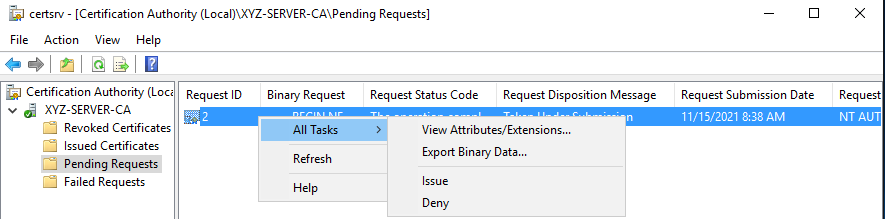


Mục Certification Authority

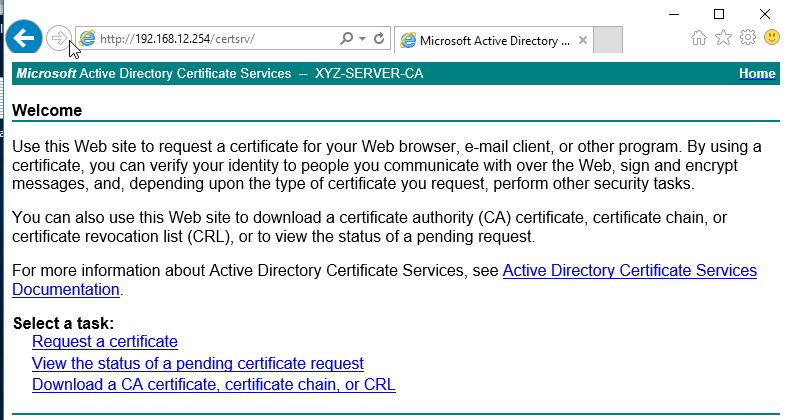


Mục Pending Requests

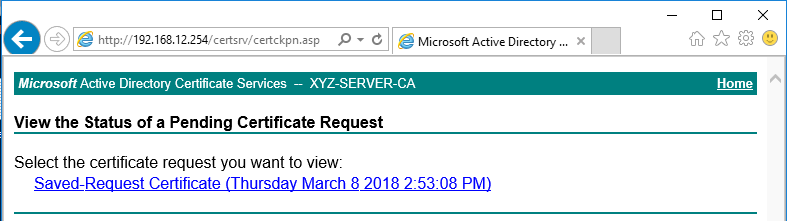
Right click 🡪 All tasks/Issue



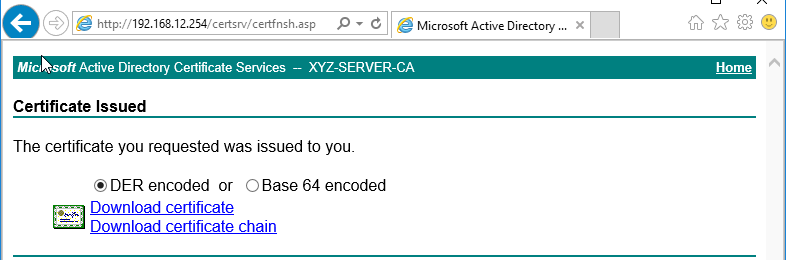
Step. Về lại máy Web server 🡪 download chứng chỉ về máy



Click View the status of a pending certificate request

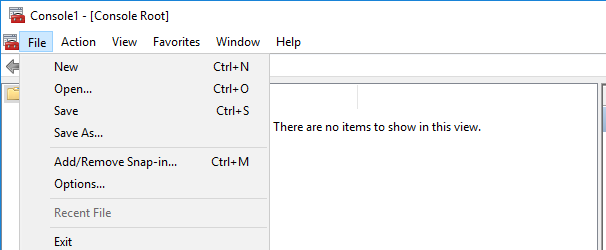


Click Save

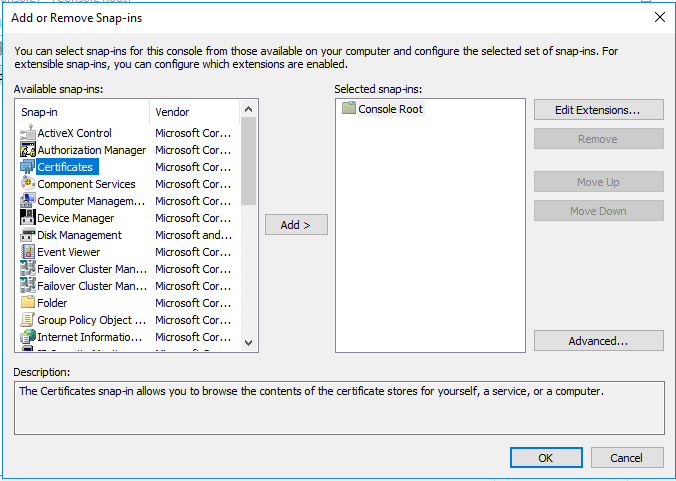


Download cả 2 về máy

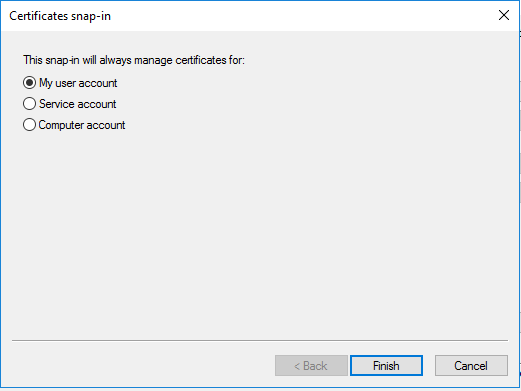
Vào Run 🡪 mmc



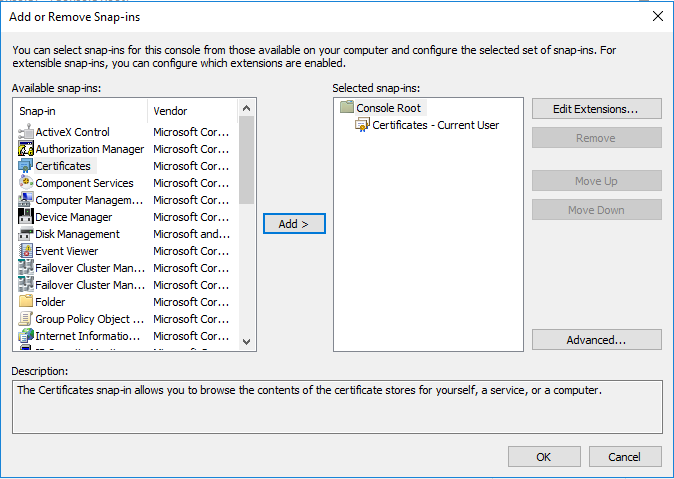
File 🡪 Add/Remove Snap-in…



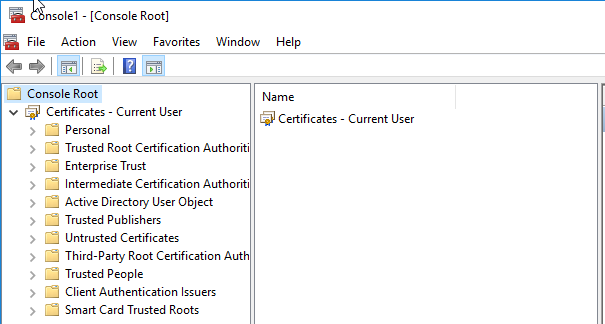
Chọn Certificate 🡪 Add



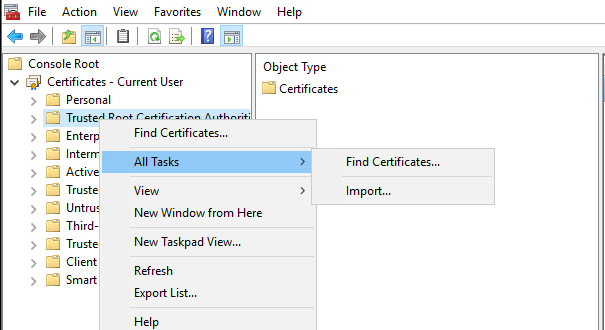
Chọn My user account



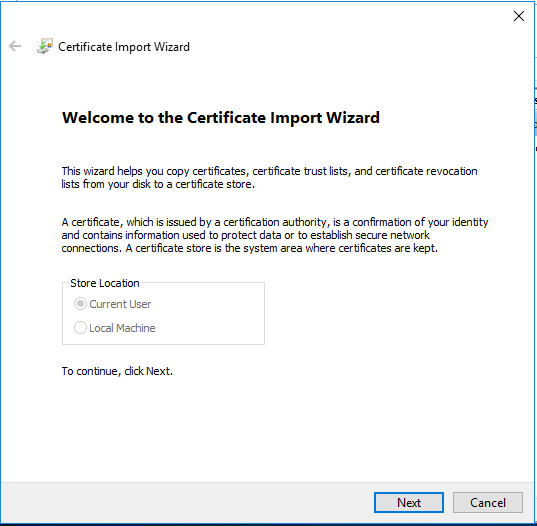
* OK

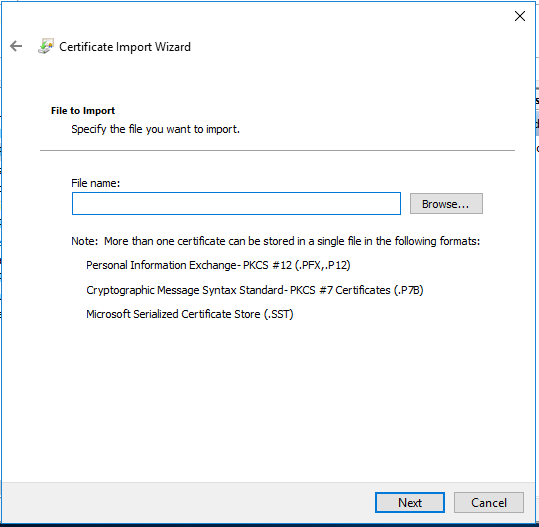


Chọn Trust Root Certificate Authority….

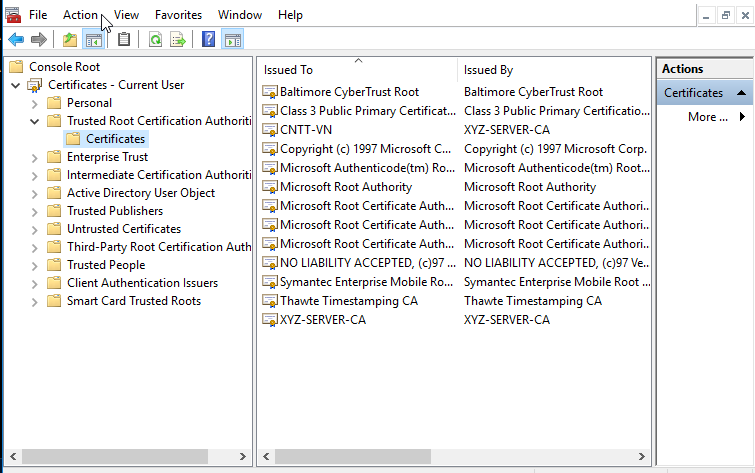


Import

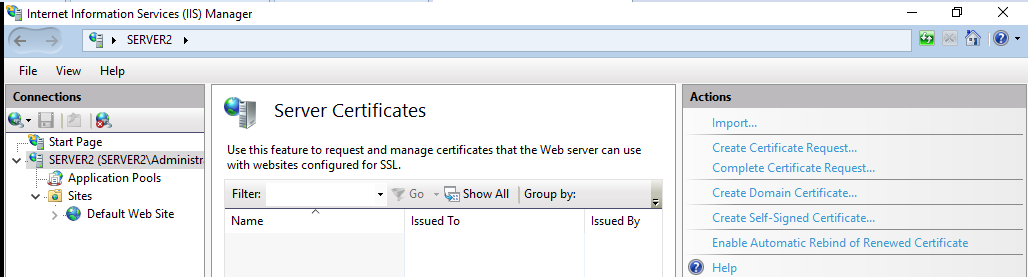




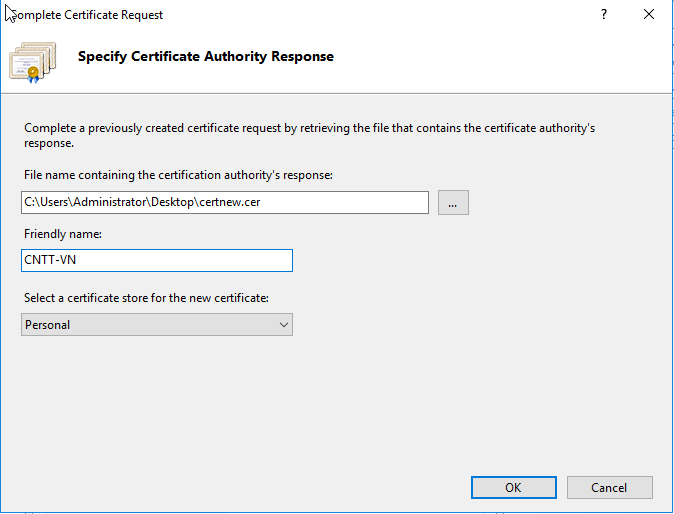
Chọn Browser… lần lượt import 2 file đã tải về lúc trước.



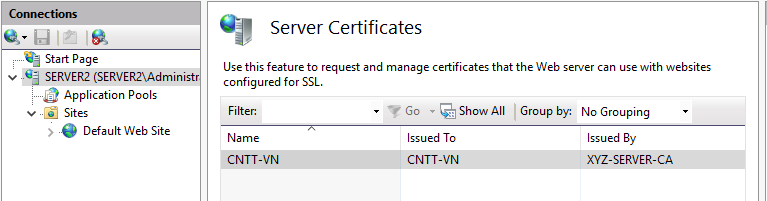
Mở lại cửa sổ IIS



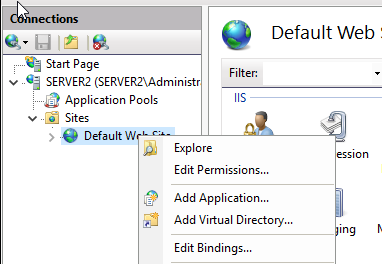
clickComplete Certificate Request



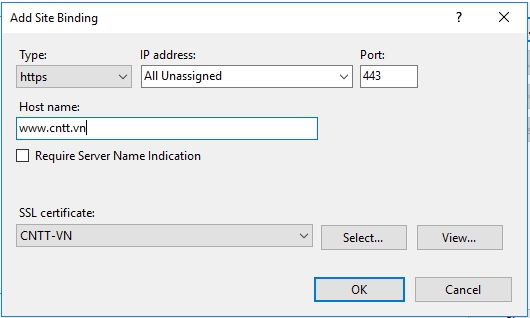
Browser tới file .cer và điền Friendly name:

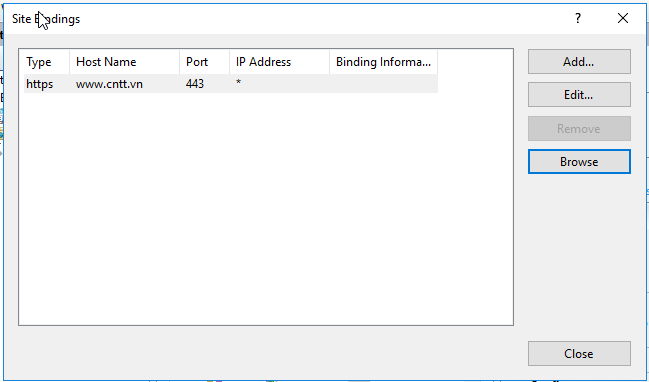


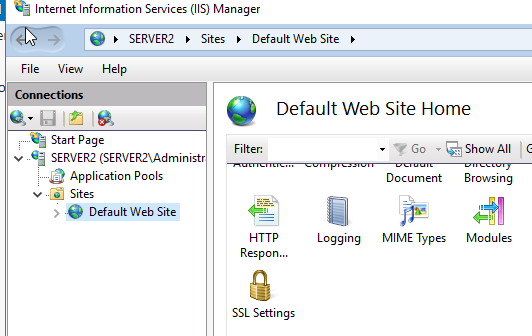
Cấu hình Web server sử dụng SSL



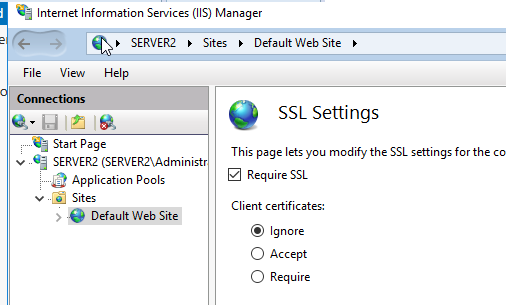
Chọn Edit bindings…





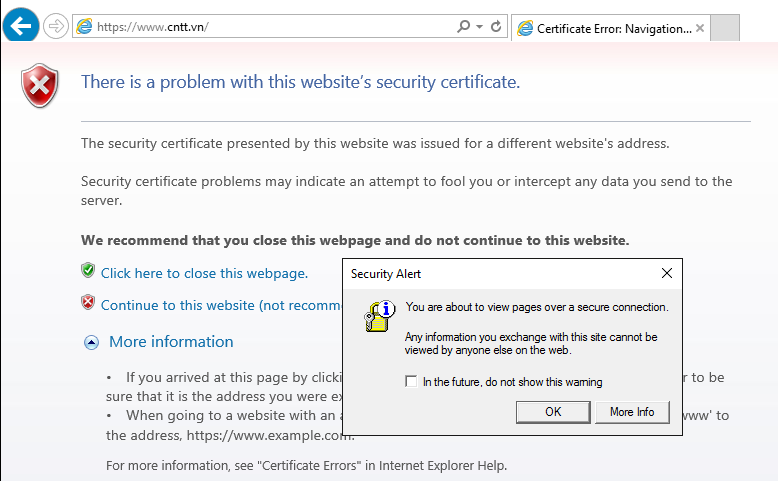


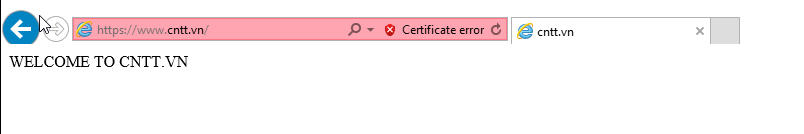
Chọn SSL Settings

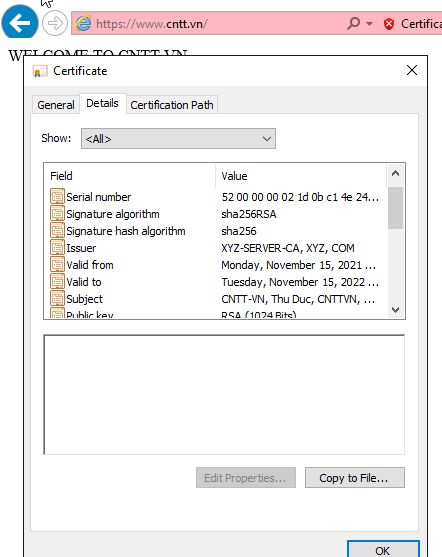


Check vào mục Require SSL

Test https







1. Kiểm tra truy cập HTTPS.

**6. Kết quả**

Telnet & SSH:

* Có thể đăng nhập vào Router từ xa thông qua Telnet và SSH.

HTTPS:

* Web server truy cập thành công thông qua giao thức HTTPS với chứng chỉ hợp lệ.
* Trình duyệt hiển thị kết nối bảo mật (HTTPS xanh).

**7. Đánh giá/Nhận xét**

Ưu điểm:

* Quy trình bảo mật được đảm bảo từ bước đăng nhập từ xa đến truy cập website.
* CA Server và Web Server cấu hình đúng chuẩn, tạo môi trường an toàn cho truyền thông tin.

Hạn chế:

* Cần kiểm soát quyền truy cập trên CA Server chặt chẽ để tránh bị lạm dụng.
* Phải đảm bảo DNS hoạt động chính xác giữa Web Server và CA Server.

Bài học kinh nghiệm:

* Hiểu rõ quy trình cấp phát, xác thực chứng chỉ SSL.
* Biết cách cấu hình router để tăng tính bảo mật khi truy cập từ xa.
* Biết triển khai và quản lý CA trong hệ thống nội bộ.