[**CẤU HÌNH VPN – SSTP (SECURE SOCKET TUNNELING PROTOCOL) TRÊN WINDOWS SERVER 2012**](http://mcthub.com/technologies/microsoft/windows-server/202-c%E1%BA%A5u-h%C3%ACnh-vpn-%E2%80%93-sstp-secure-socket-tunneling-protocol-tr%C3%AAn-windows-server-2012.html)

**I. GIỚI THIỆU:**

Trong các doanh nghiệp, đối với những người dùng có nhu cầu kết nối từ xa để truy cập mạng nội bộ, người quản trị thường cấu hình Virtual Private Network (VPN) cho phép người dung có thể kết nối vào mạng nội bộ từ một máy Client nào đó thông qua đường truyền Internet công cộng. Kỹ thuật VPN thông thường sử dụng Point to Point Tunneling Protocol (PPTP) hoặc Layer two Tunnneling Protocol (L2TP) kết hợp IPSEC. Tuy nhiên trong trường hợp người dùng ngồi trên 1 Client thuộc một mạng nội bộ khác truy cập Internet thông qua một Firewall, Firewall này không cho phép thiết lập kết nối PPTP hoặc L2TP thì người dùng sẽ không thể kết nối VPN vào mạng doanh nghiệp. Giải pháp trong tình huống này là sử dụng Secure Socket Tunneling Protocol (SSTP).

SSTP được giới thiệu từ Windows Server 2008 cho phép thiết lập kết nối VPN thông qua kênh mã hóa SSL của HTTPS, có nghĩa là kết nối sẽ chạy port 443, trong trường hợp này có thể thông qua các firewall cho phép truy cập Web.

Trong bài viết này tôi sẽ giới thiệu kỹ thuật kết nối VPN bằng SSTP trong môi trường Windows Server 2012

**II. CÁC BƯỚC TRIỂN KHAI:**

****

Mô hình bài lab bao gồm 3 máy:

+ *DC2012:*  *Domain Controller* chạy Windows Server 2012 (domain mcthub.local.

+ *Router:* Windows Server 2012 đã join domain.

+ *Client1:* Windows 8 chưa join domain

Cấu hình TCP/IP cho 3 máy như trong bảng sau:

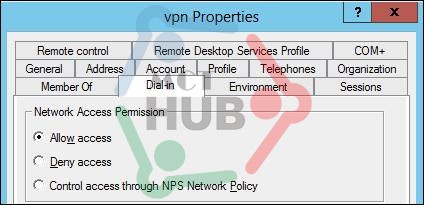
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Interface** | | **DC2012** | **Router** | **Client** |
| Internal | IP Address | 172.16.1.10 | 172.16.1.1 | Disable |
| Subnet Mask | 255.255.0.0 | 255.255.0.0 |
| Default Gateway | 172.16.1.1 |  |
| Preffered DNS | 172.16.1.10 | 172.16.1.10 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Interface** | | **DC2012** | **Router** | **Client** |
| External | IP Address | Disable | 123.1.1.1 | 123.1.1.100 |
| Subnet Mask | 255.0.0.0 | 255.0.0.0 |
| Default Gateway |  |  |
| Preffered DNS |  |  |

- Tạo OU VPN. Trong OU VPN, tạo user vpn.



- Cấp quyền ***Remote Access*** cho user ***vpn***.



**\* Quy trình thực hiện:**

1. Cài đặt Enterprise CA

2. Tạo Certificate Template và phát hành Certificate Template

3. Xin SSTP Certificate cho VPN Server

4. Cài đặt Remote Access

5. Cấu hình VPN Client-to-Gateway

6. Cấu hình NAT Inbound

7. Download CA Certificate

8. Cấu hình Trusted Root CA trên VPN Client

9. Tạo VPN Connection

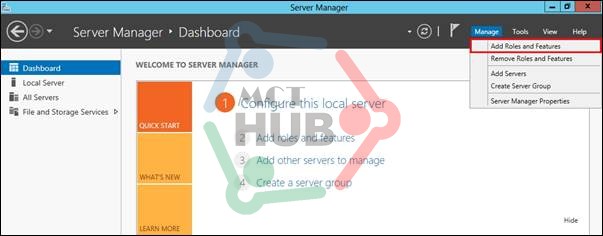
10. Kiểm tra kết nối VPN-SSTP

**III. TRIỂN KHAI CHI TIẾT:**

**1/ Cài đặt Enterprise CA**

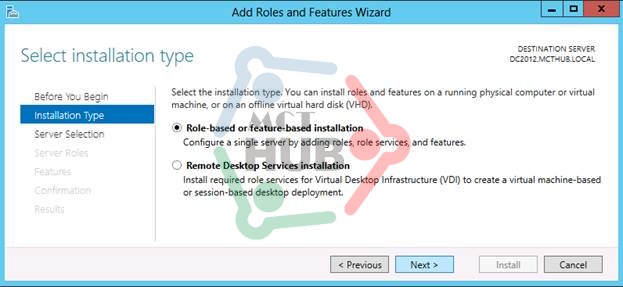
- Tại máy *DC2012*, logon *MCTHUB\Administrator*.

- Mở *Server Manager*, vào menu *Manage*, chọn *Add Roles and Features*.

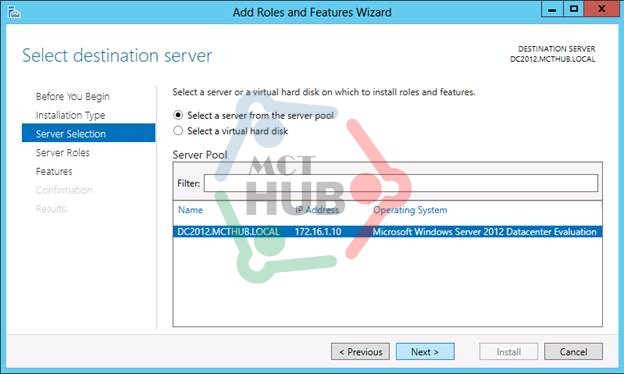


- Màn hình *Before You Begin*, nhấn Next.

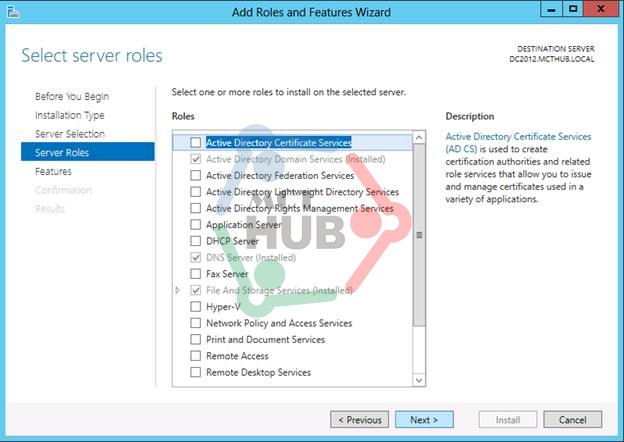
- Màn hình *Select installation type*, chọn *Role-based or feature-based installation*.



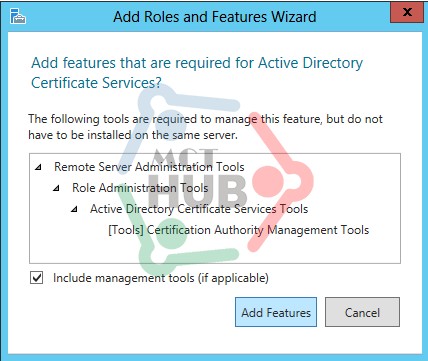
- Màn hình *Select destination server*, bạn chọn Server cần cài đặt là *DC2012.MCTHUB.LOCAL.*



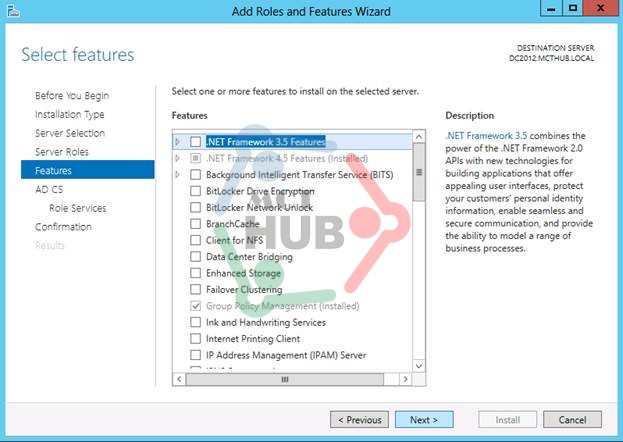
- Màn hình *Select server roles*, bạn đánh dấu chọn vào ô *Active Directory Certificate Services*, sau đó nhấn *Next*.



- Màn hình yêu cầu xác nhận cài thêm các Feature cần thiết, bạn nhấn *Add Features*.



- Màn hình *Select features*, nhấn Next.



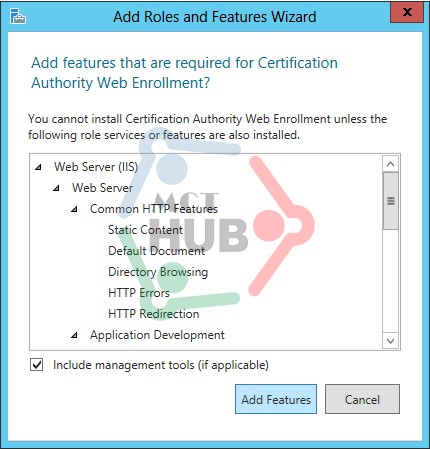
- Màn hình *Active Directory Certificate Services*, nhấn Next*.*



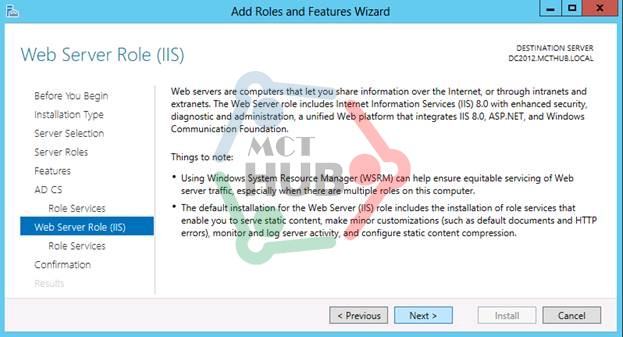
- Màn hình *Select roles services*, bạn đánh dấu chọn vào ô *Certification Authority* và *Certificate Authority Web Entrollment.*



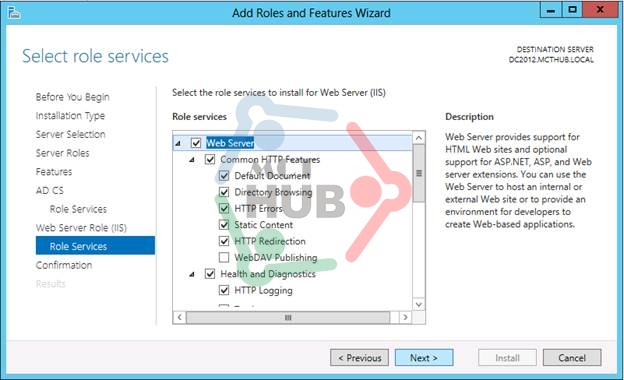
- Cửa  sổ *Add Roles and Features Wizard*, bạn nhấn *Add Features*.



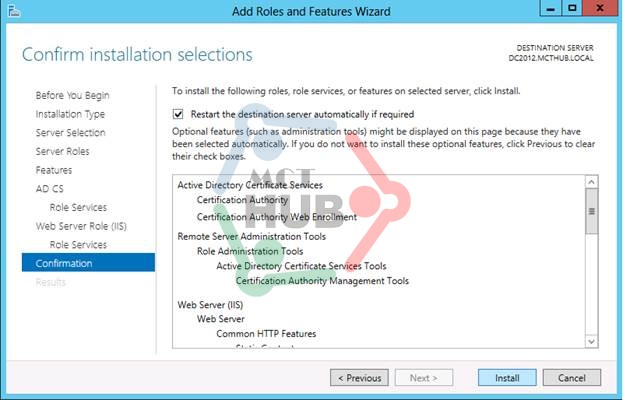
- Màn hình *Web Server Role (IIS)*, bạn nhấn *Next*.



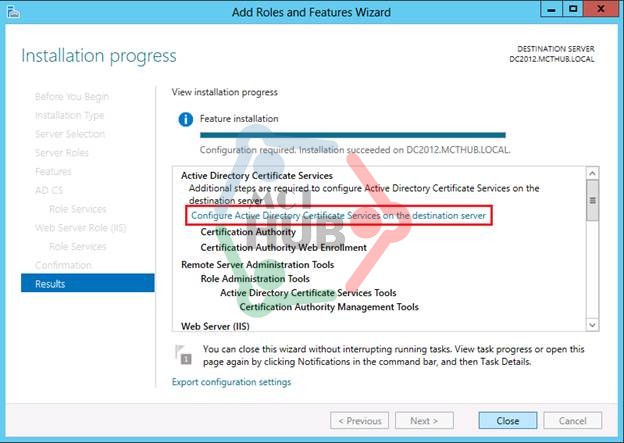
- Màn hình *Select role services*, do xin Certificate thông qua giao diện Web nên cài đặt thêm *Web Services*.



- Màn hình *Confirm installation selections*, bạn nhấn *Install* để tiến hành cài đặt.



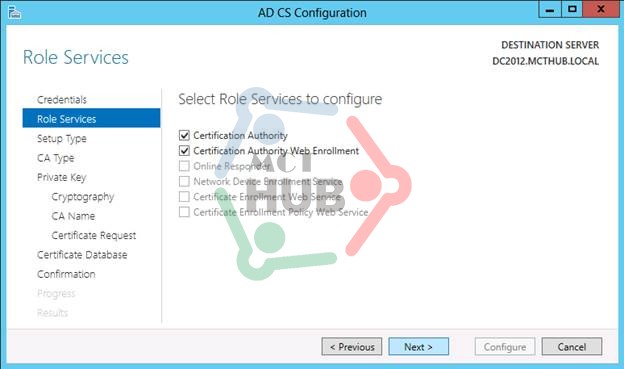
- Màn hình *Installation progress*, kiểm tra quá trình cài đặt thành công. Bạn nhấn vào mục *Configure Active Directory Certificate Services on the destination server*.



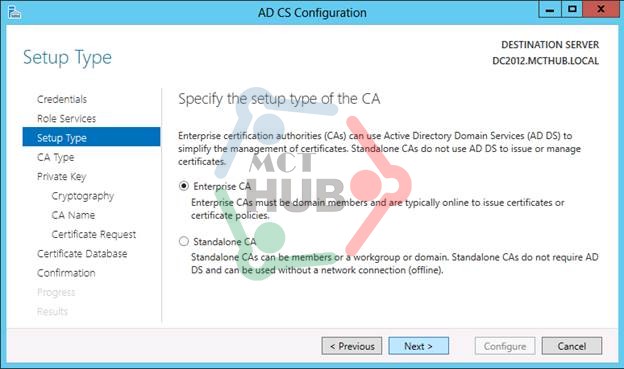
- Màn hình *Credentials*, chấp nhận User Account dùng để cấu hình là *MCTHUB/Administrator.*



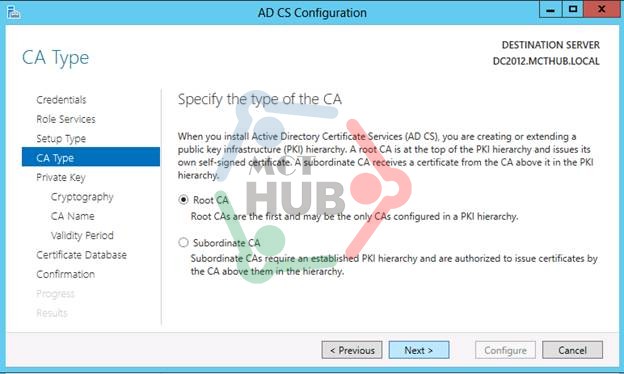
- Màn hình *Role Services*, bạn đánh dấu chọn vào ô *Certification Authority* và *Certification Authority Web Enrollment.*



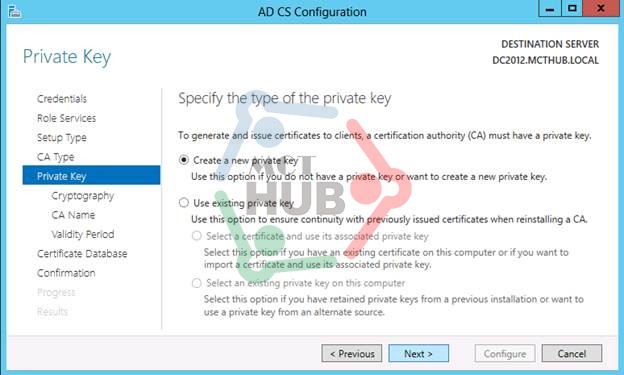
- Màn hình *Setup Type*, chọn loại CA là *Enterprise CA.*



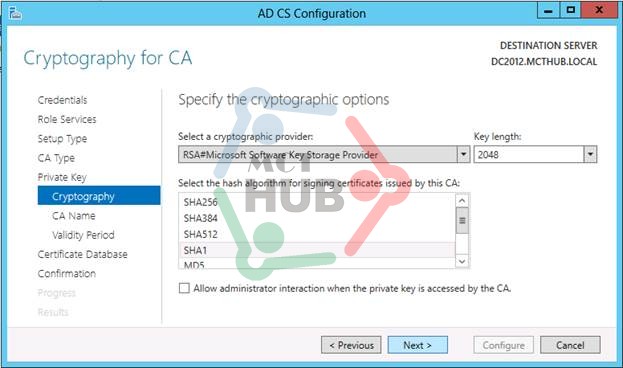
- Màn hình *CA Type*, do đây là CA Server đầu tiên và duy nhất trong hệ thống nên tôi chọn *Root CA.*



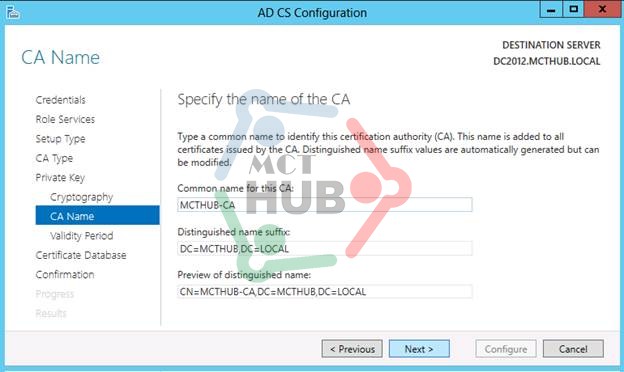
- Màn hình *Private Key*, bạn chọn ô *Create a new private key,* sau đó nhấn Next.



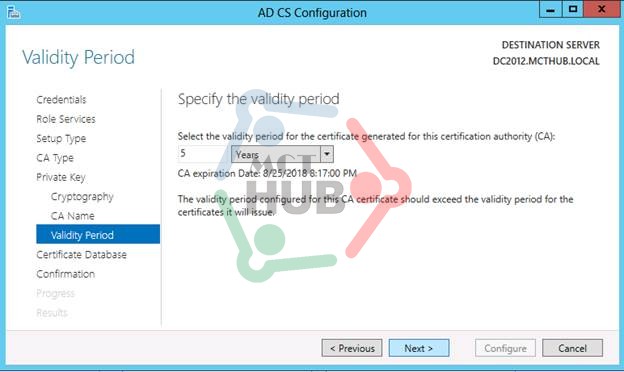
- Màn hình *Cryptography for CA*, bạn chấp nhận thuật toán mã hoá mặc định là *RSA*, sau đó nhấn Next.



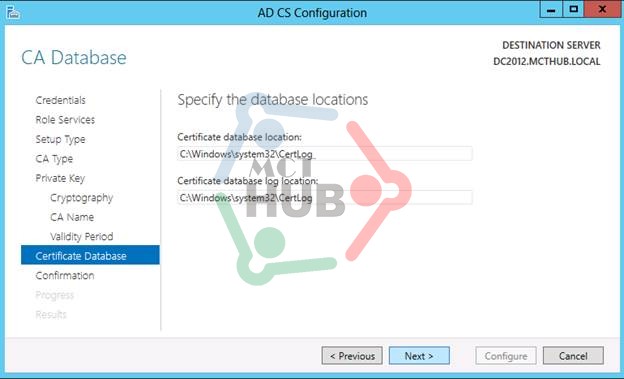
- Màn hình CA Name, đặt tên cho CA Server là: *MCTHUB-CA*, nhấn Next.



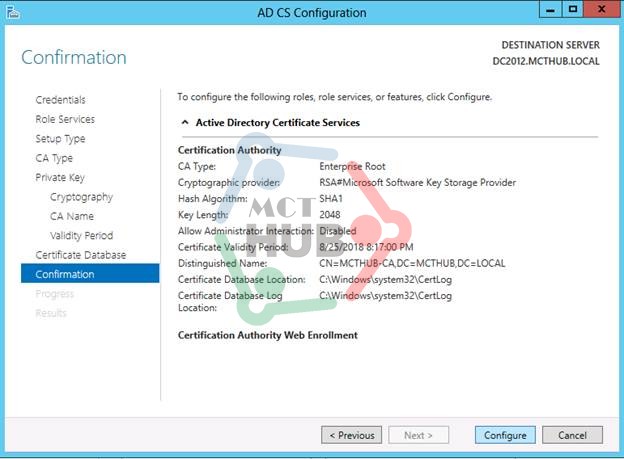
- Màn hình *Validity Period*, chấp nhận thời gian hoạt động của CA Server là 5 năm, nhấn *Next*.



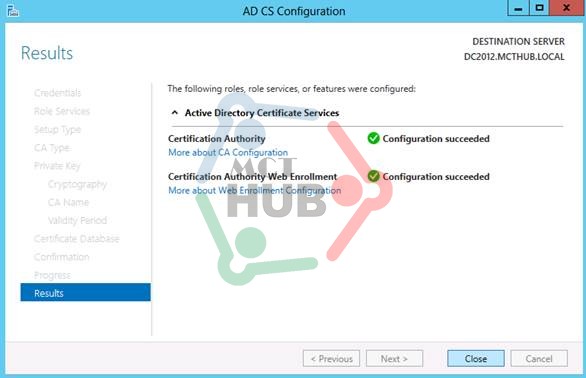
- Màn hình *CA Database*, nhấn *Next*.



- Màn hình *Confirmation*, bạn nhấn nút *Configure* để tiến hành cấu hình.



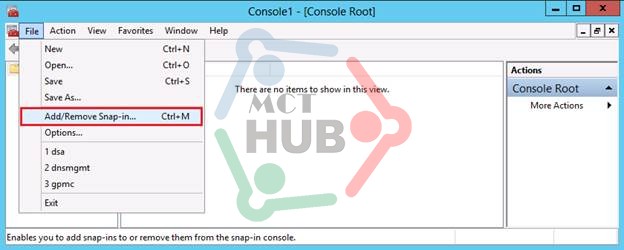
- Màn hình *Results*, nhấn nút *Close* khi hoàn tất.



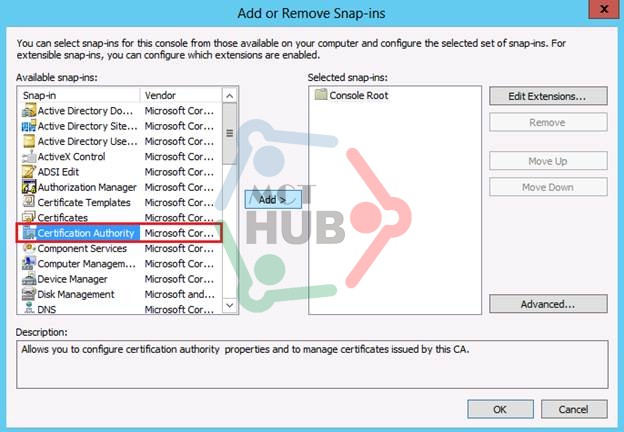
Sau khi cấu hình CA Server, bạn Restart máy ROUTER để máy này tự động Trust CA Server trên DC2012.

**2/ Tạo Certificate Template và phát hành Certificate Template**

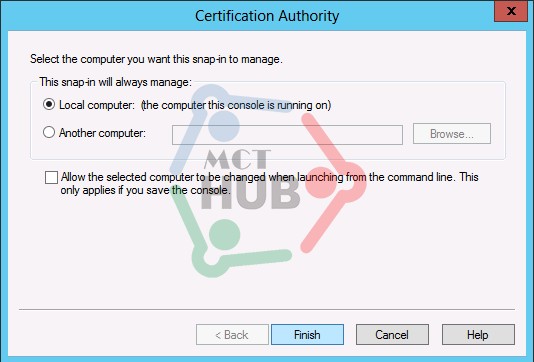
- Vào *Run*, gõ *MMC*. Tiếp theo bạn vào menu *File*, chọn *Add/Remove Snap-in…*



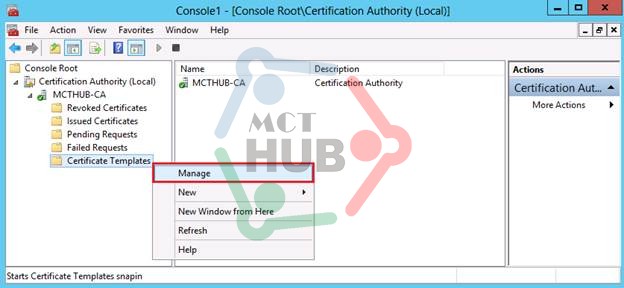
- Trong cửa sổ *Add or Remove Snap-in*, chọn công cụ *Certification Authority*, chọn *Add*.



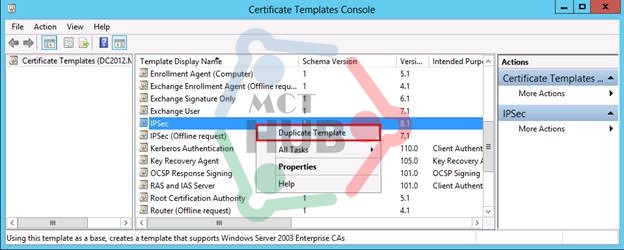
- Màn hình *Certification Authority*, chọn *Local Computer*. Sau đó bạn nhấn *Finish* và *OK*.



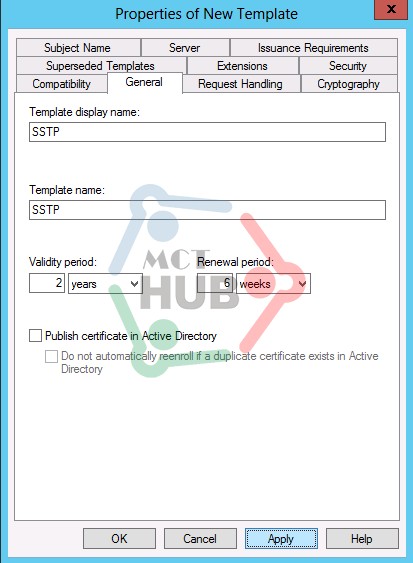
- Trong cửa sổ *Certification Authority*, chuột phải *Certificate Templates*, chọn *Manage*.



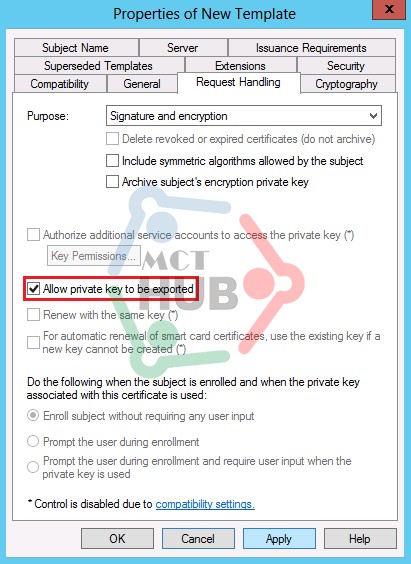
- Trong cửa sổ *Certificate Templates Console*, bạn sẽ sao chép Certificate Template này thành một Certificate Template mới. Chuột phải vào *IPSec*, chọn*Duplicate Template*.



- Tại tab *General*, ở mục Template Display Name, bạn đặt tên cho *Certificate Template* mới (ở đây tôi đặt là SSTP).



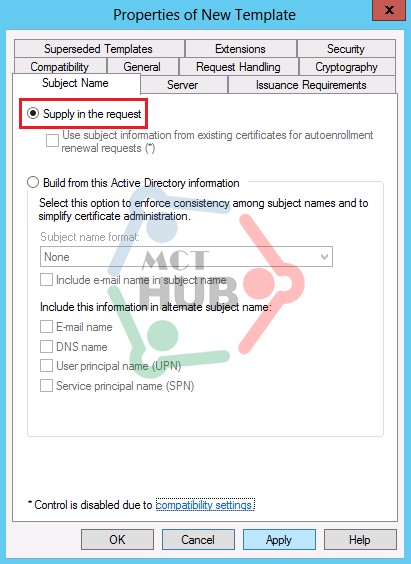
- Qua tab *Request Handling*, đánh dấu chọn vào ô *Allow private key to be exported* để có thể *Export Certificate* để phòng trường hợp bị mất Certificate.



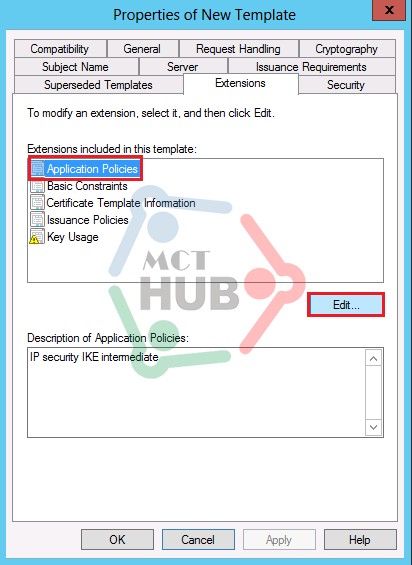
- Màn hình *Certificate Templates*, nhấn *OK*.



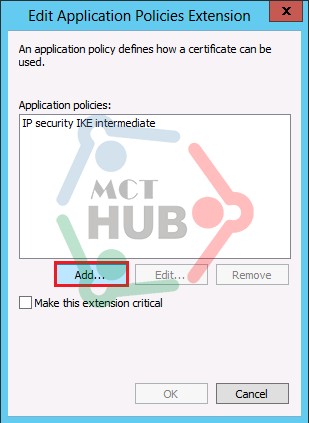
- Qua tab *Subject Name*, chọn *Supply in the request*  (cấp Certificate  cho Authenticated Users)



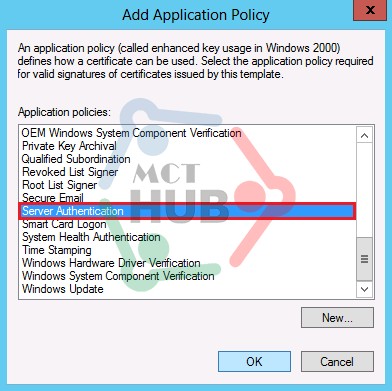
- Qua tab *Extensions*, chọn *Application Policies*, nhấn *Edit*.



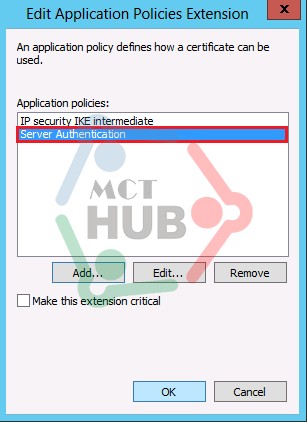
- Trong cửa sổ *Edit Application Policies Extension*, nhấn *Add*.



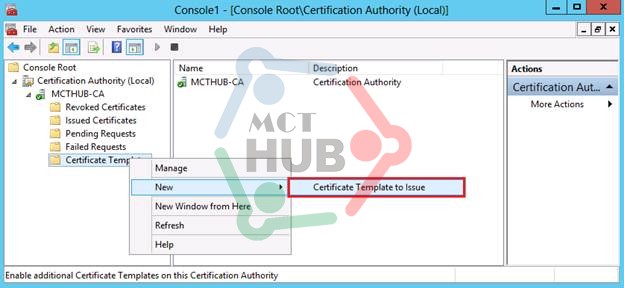
- Trong cửa sổ *Add Application Policy*, chọn *Server Authentication*, nhấn *OK*.



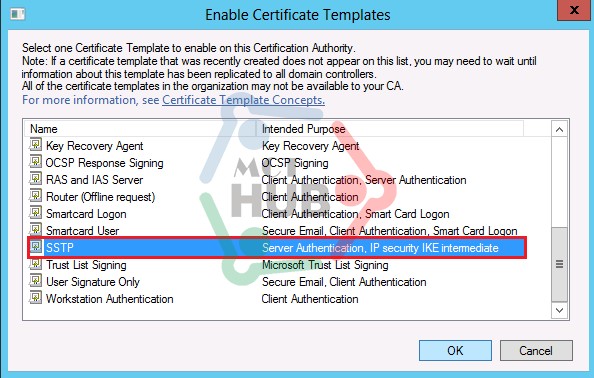
- Trong cửa sổ *Edit Application Policies Extension*, chọn *Server Authentication*, nhấn *OK*.



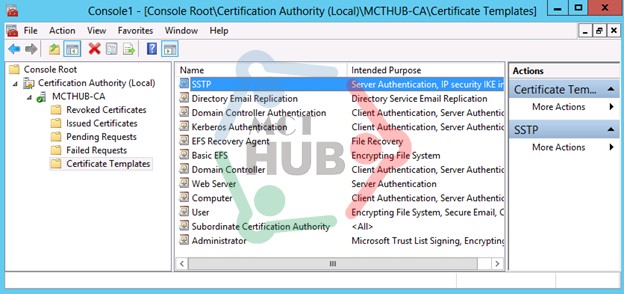
- Quay lại màn hình *Certification Authority*,tiến hành phát hành *Certificate*, chuột phải *Certificate Templates*, chọn *New,*sau đó chọn*Certificate Templates to Issue*.



- Cửa sổ *Enable Certificate Templates*, chọn *SSTP Templates*, nhấn *OK*.

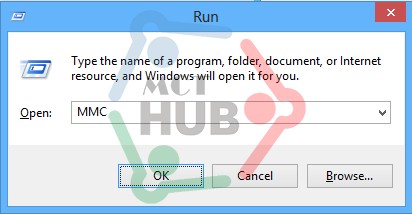


- Kiểm tra *SSTP Templates* đã được phát hành trong *Certification Authority*.

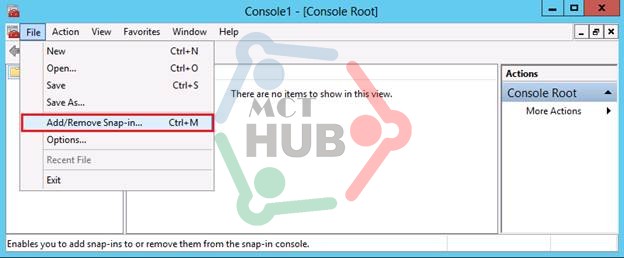


**3/ Xin SSTP Certificate cho VPN Server**

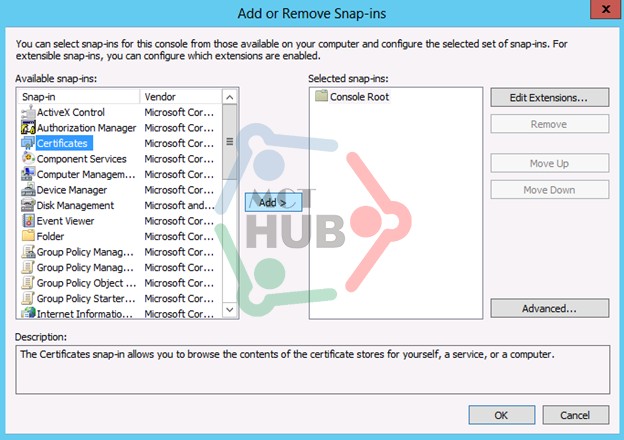
- Tại máy Router, vào *Run*, gõ: MMC, tạo một Console để quản lý Certificate cho *Local Computer*.



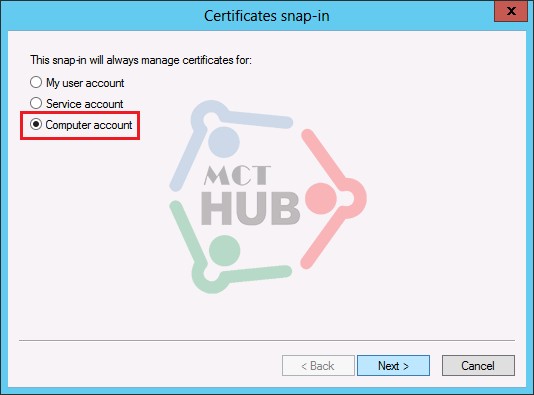
- Cửa sổ *Console1*, vào menu *File*, chọn *Add/Remove Snap-in*.



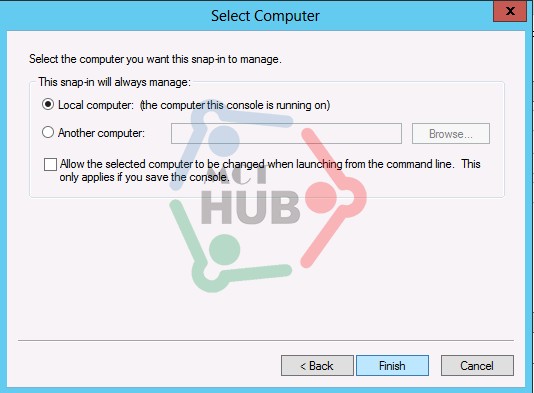
- Chọn *Certificates*, nhấn *Add*.



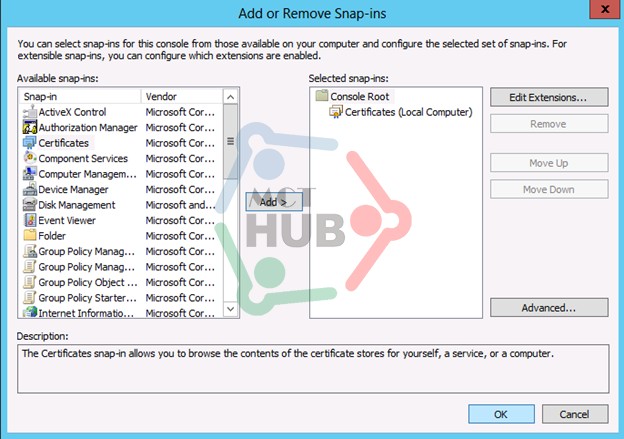
- Màn hình *Certificate Snap-in*, chọn *Computer Account*, nhấn *Next*.



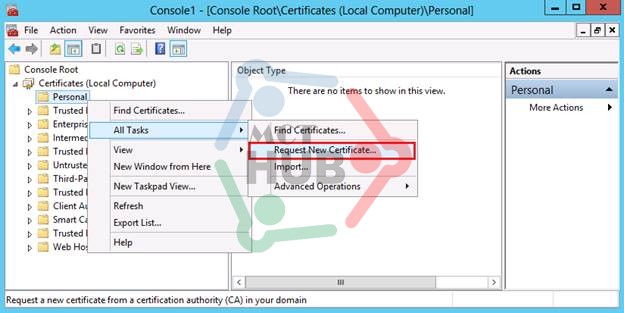
- Màn hình *Select Computer*, chọn *Local Computer*.



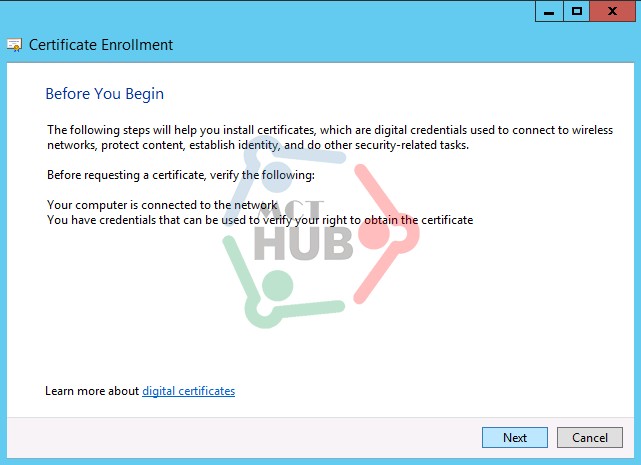
- Cuối cùng bạn nhấn *Finish* và *OK*.



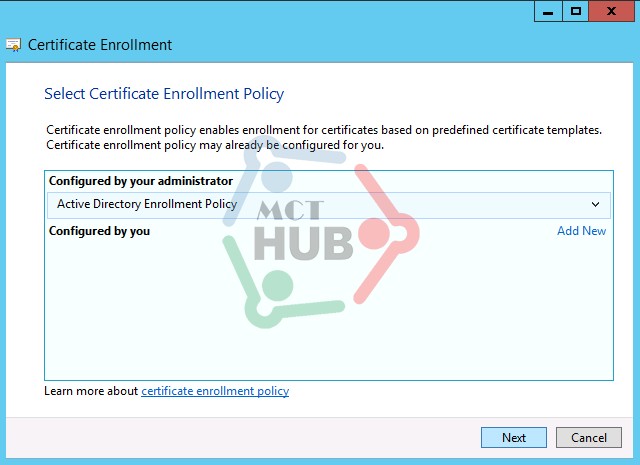
- Trong cửa sổ *Console*, chuột phải *Personal,* chọn *All Tasks*, chọn *Request New Certificate*.



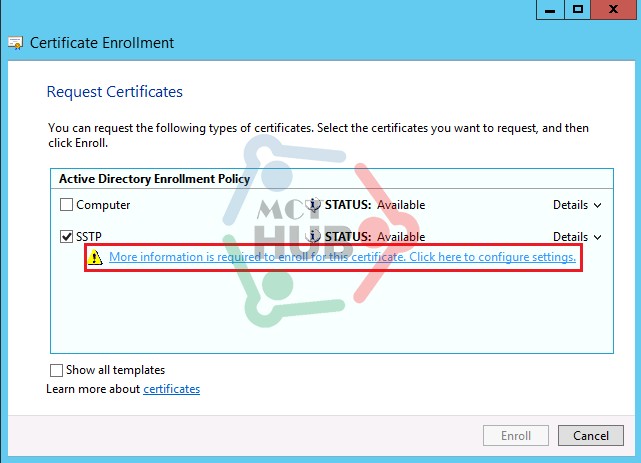
- Màn hình *Before You Begin*, nhấn *Next.*



- Màn hình *Select Certificate Enrollment Policy*, nhấn *Next*.



- Màn hình *Request Certificates*, đánh dấu chọn vào ô *SSTP*, chọn*“More information is required to enroll….”*



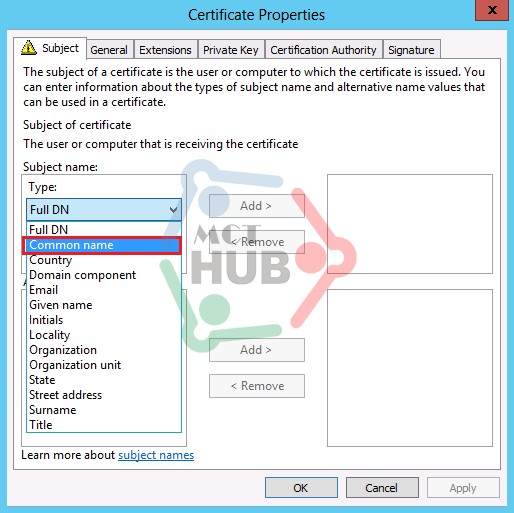
- Màn hình *Certificate Properties*, trong khung *Subject Name,*bạn chọn các thông số sau:

+ Type: Common Name

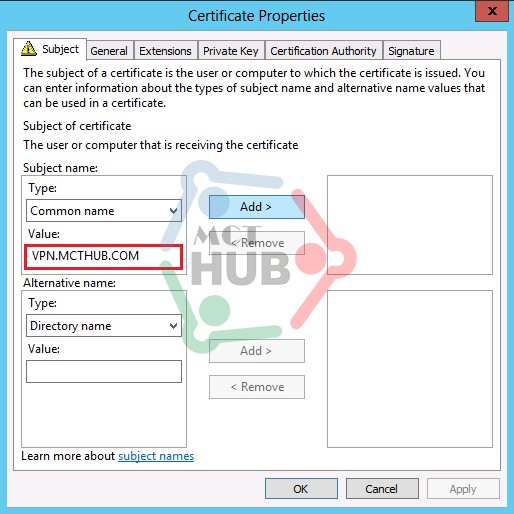
+ Value: *VPN.MCTHUB.COM* (Lưu ý trên thực tế bạn cần có một Internet Domain Name, ví dụ *MCTHUB.COM* và đã tạo Host tên tùy ý (ví dụ VPN) trỏ về IP Public của VPN Server.

- Sau đó nhấn *Add*, chọn *OK*.

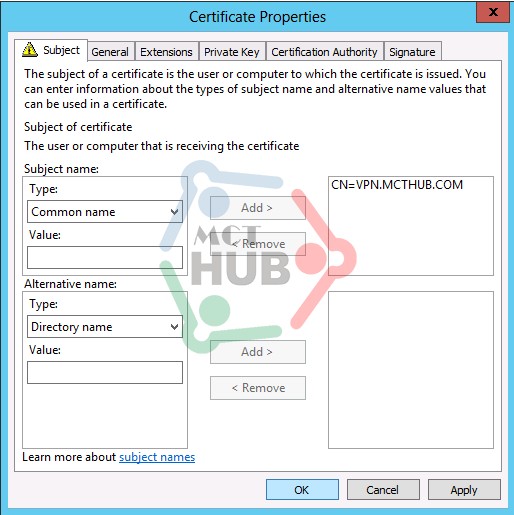
- Trong khung *Type*, chọn *Common Name*.



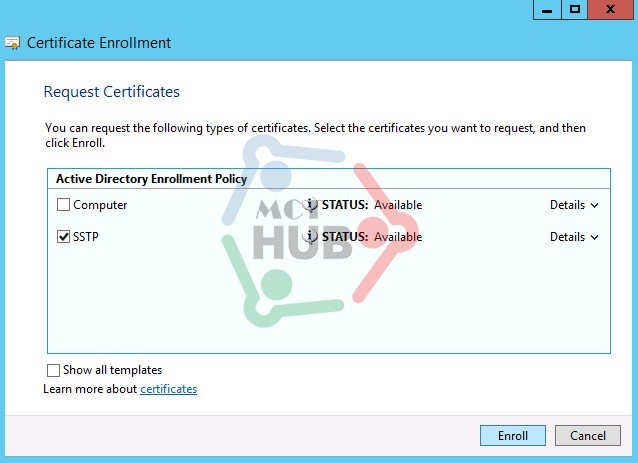
- Trong khung *Value* nhập tên *VPN.MCTHUB.COM* và nhấn nút *Add*.



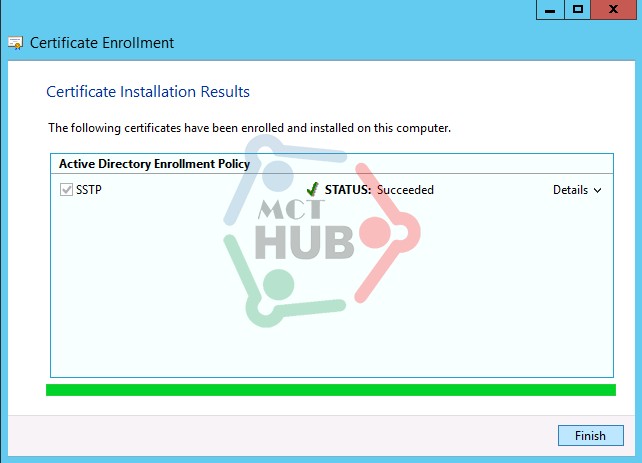
- Nhấn *OK* để xác nhận thông tin Certificate.



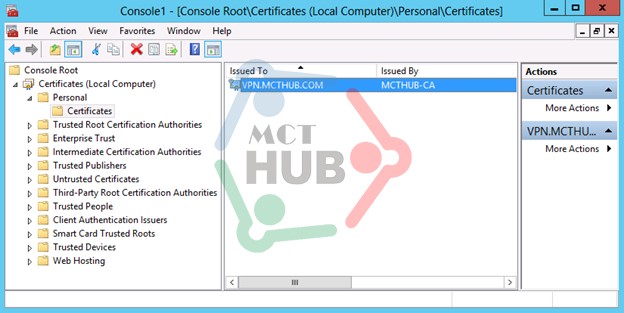
- Quay lại cửa sổ *Request Certificates*, bạn nhấn vào nút *Enroll.*



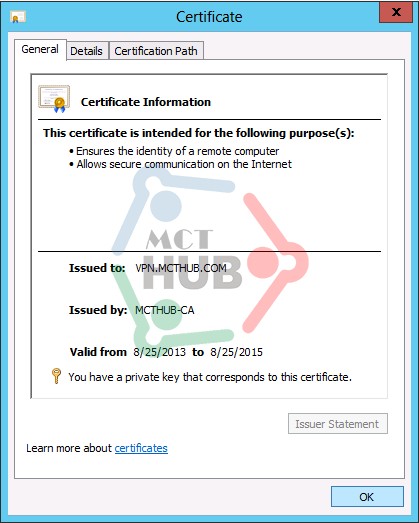
- Kiểm tra kết quả xin Certificate thành công và nhấn nút *Finish.*



- Trong cửa sổ Console1, vào *Personal*, chọn *Certificate*, double click *VPN.MCTHUB.COM.*



- Kiểm tra Certificate vừa xin cho VPN Server.

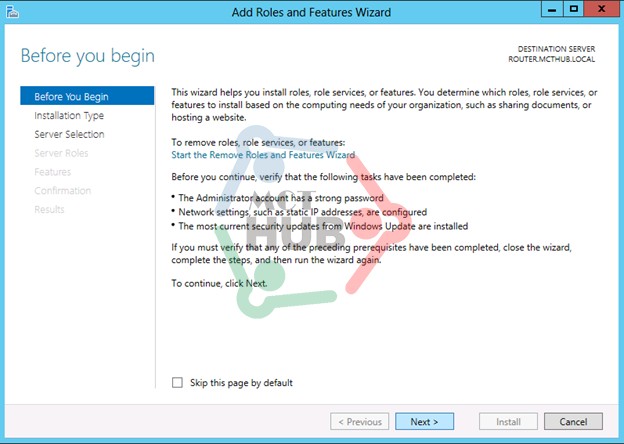


**4/ Cài đặt Remote Access.**

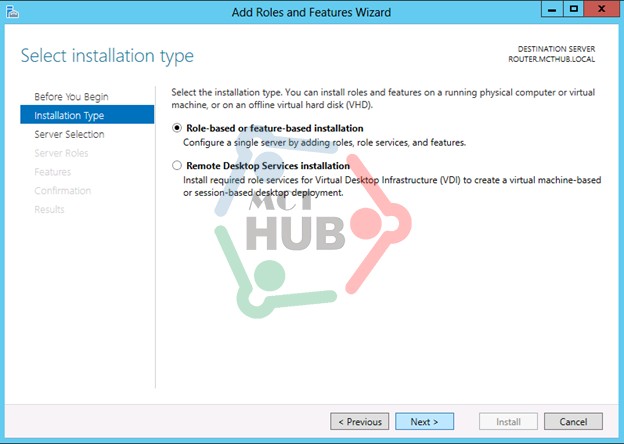
- Tại máy Router, mở *Server Manager*. Vào menu *Manage*, chọn *Add Roles and Features.*



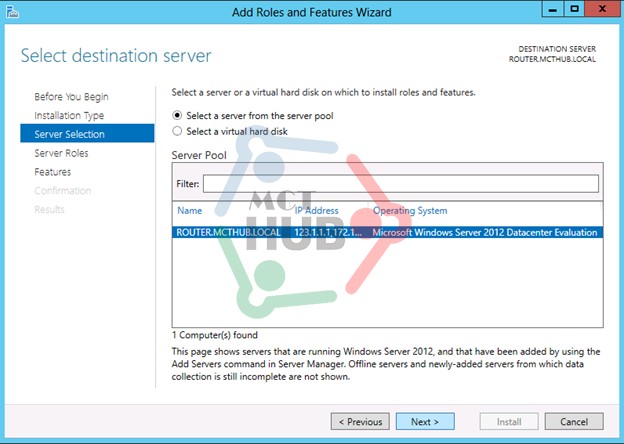
- Màn hình *Before You Begin*, nhấn *Next.*



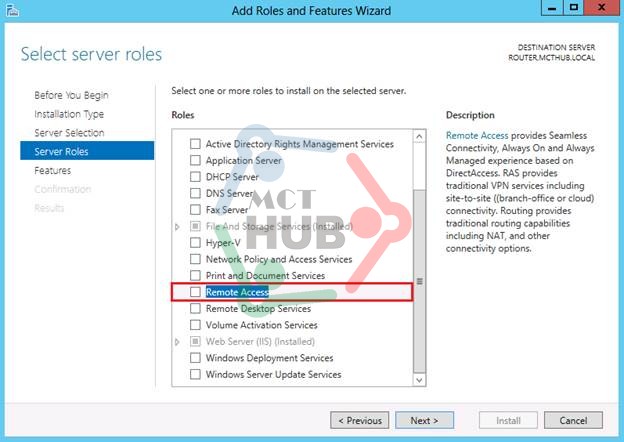
- Màn hình *Select installation type*, chọn *Role-based or feature-based installation*



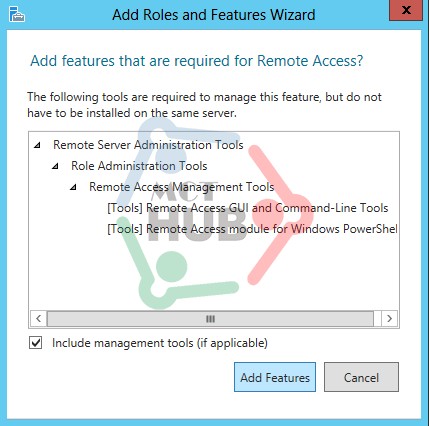
- Màn hình *Select destination server*, bạn chọn Server cần cài đặt là *DC2012.MCTHUB.LOCAL*



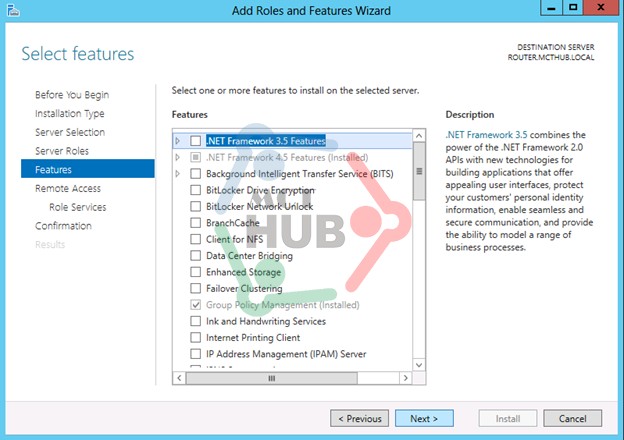
- Màn hình *Select server roles*, đánh dấu chọn vào ô *Remote Access*, nhấn *Next*.



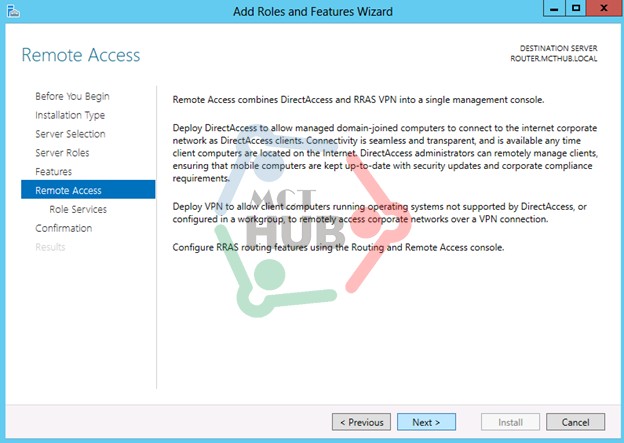
- Màn hình yêu cầu xác nhận cài thêm các Feature cần thiết, bạn nhấn *Add Features*.



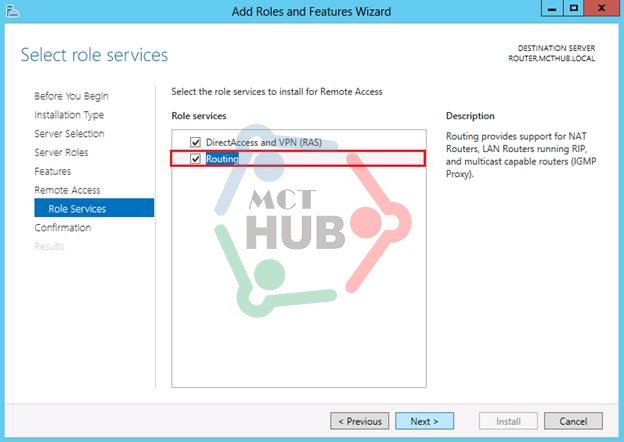
- Màn hình *Select features*, nhấn Next.



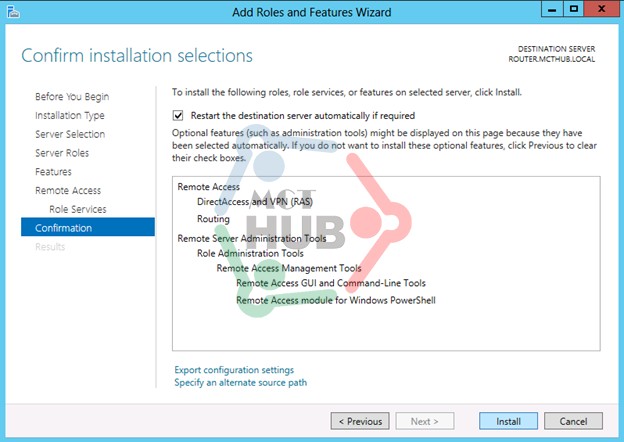
- Màn hình *Remote Access*, nhấn *Next*.



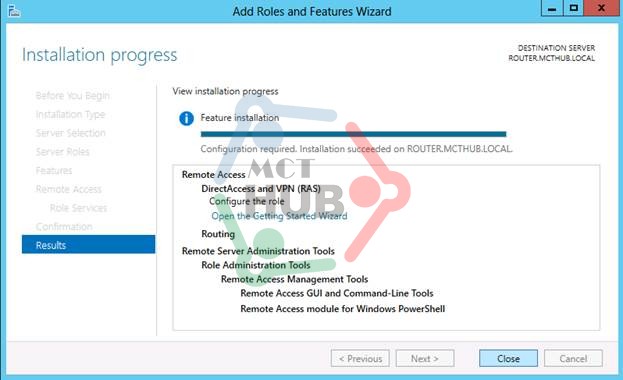
- Màn hình *Select role services*, đánh dấu chọn vào ô *Routing*, nhấn *Next*.



- Màn hình *Confirm installation selections*, đánh dấu chọn vào ô *Restart the destination server automaticcally*, sau đó bạn nhấn *Install*.

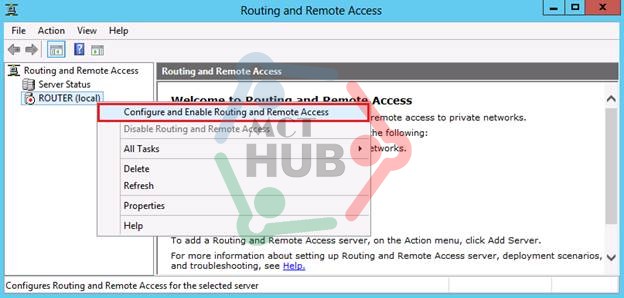


- Nhấn *Close* khi quá trình cài đặt hoàn tất.

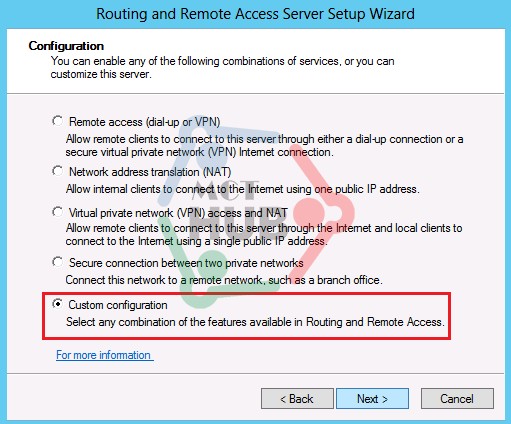


**5/ Cấu hình VPN Client-to-Gateway**

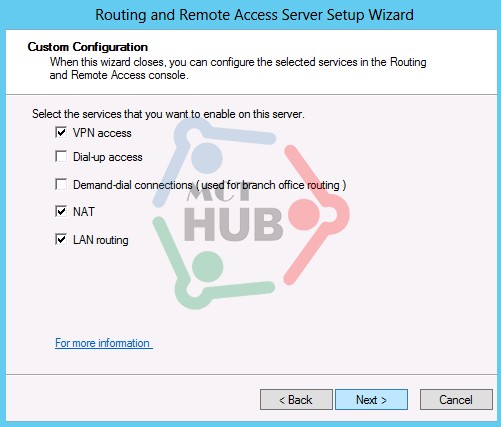
- Tại máy *Router*, mở *Routing and Remote Access* từ *Server Manager*, chuột phải *Router*, chọn *Configure and Enable Routing and Remote Access*.



- Màn hình *Configuration*, bạn chọn *Custom Configuration*.



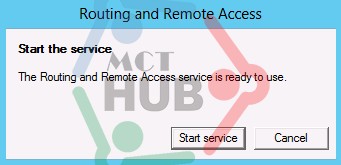
- Màn hình *Custom Configuration*, bạn đánh dấu chọn vào 3 ô: *VPN Server, NAT, Lan Routing*.



- Màn hình *Completing the Routing and Remote Access Server Setup Wizard*, bạn nhấn *Finish.*



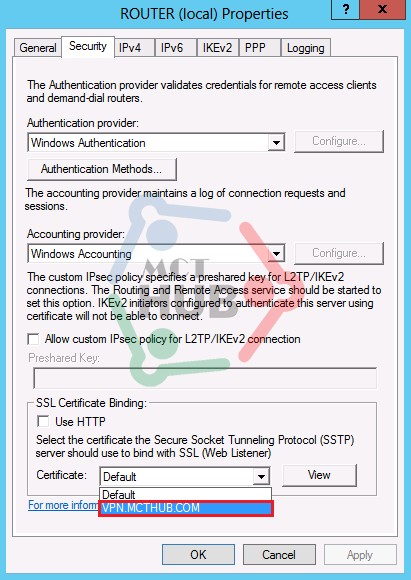
- Màn hình *Start the service*, bạn nhấn nút *Start service*.



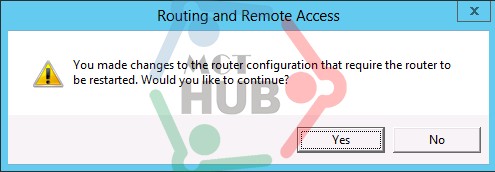
- Chuột phải *Router,* chọn *Properties*.



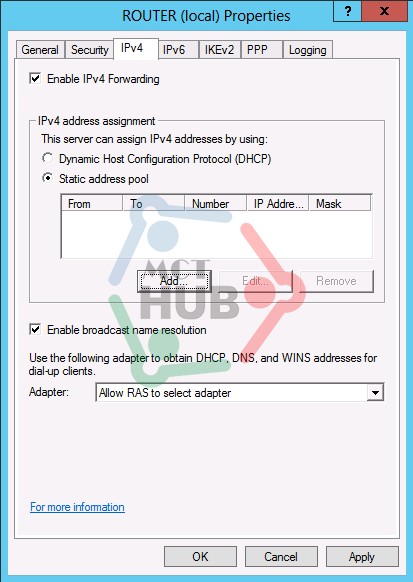
- Qua tab *Security*, mục *SSL Certificate Binding*, bung ra chọn *Certificate VPN.MCTHUB.COM*



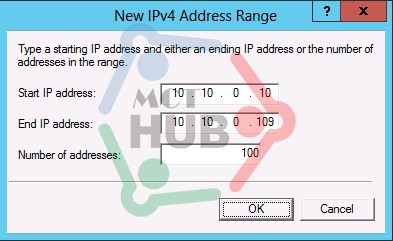
- Cửa sổ *Routing and Remote Access*, chọn *Yes*.



- Qua *tab IPv4,* chọn *Static Address Pool*, nhấn *Add.*



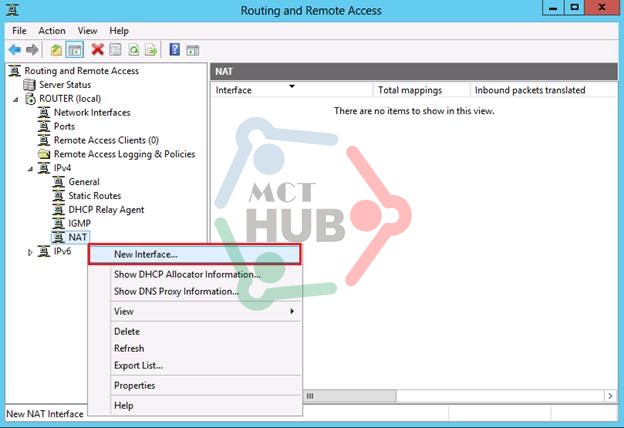
- Khai báo *Range IP* cấp cho *VPN Client*, nhấn *OK*.



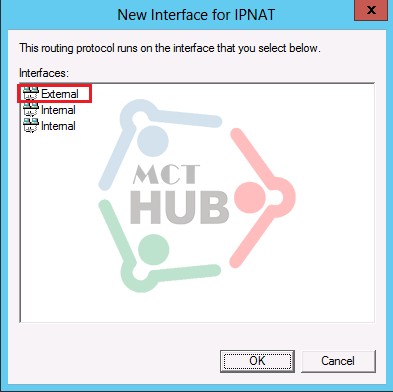
**6/ Cấu hình NAT Inbound**

Do Client muốn kết nối phải Trust CA Server, nếu Client thuộc mạng nội bộ có thể tự động Trust CA Server. Trong trường hợp Client  bên ngoài, muốn Trust CA Server cần tải Certificate của CA Server để Import vào Trusted Root Certification Authority. Để Client có thể truy cập vào CA Server để tải Certificate, bạn cần NAT Inbound port 80 vào CA Server.

- Tại máy *Router*, mở *Routing and Remote Access* từ *Server Manager*. Mở rộng mục *Router*, chọn *IPv4*, chuột phải *NAT*, chọn *New Interface…*



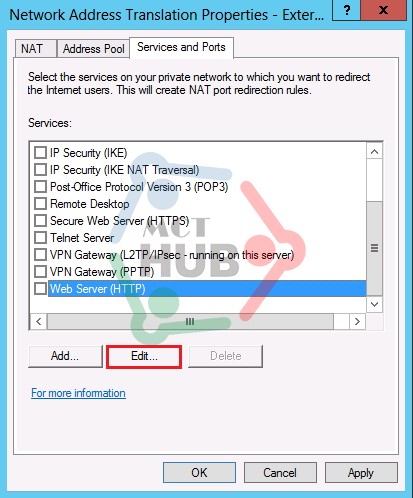
- Cửa sổ *New Interface for IPNAT*, chọn *Card External*, nhấn *OK*.



- Màn hình *Network Address Translation Properties*, tab *NAT*, chọn *Public interface connected to the Internet*, đánh dấu chọn vào ô *Enable NAT on this interface*.



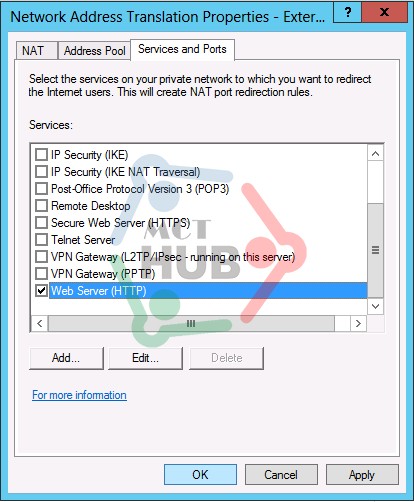
- Qua tab *Services and Ports*, bạn chọn vào ô *Web Server (HTTP)*. Sau đó nhấn nút *Edit*.



- Cửa sổ *Edit Services*, mục *Private addres*, bạn nhập vào IP*172.16.1.10*, sau đó nhấn *OK*.



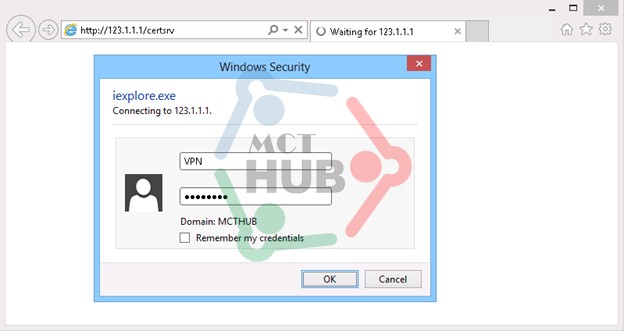
- Cuối cùng bạn nhấn *Apply* và *OK*.



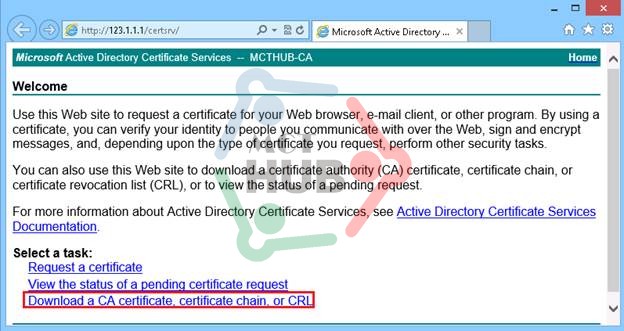
**7/ DownLoad CA Certificate**

- Tại máy Client1, mở Internet Explore, truy cập *http://10.10.0.1/certsrv.*

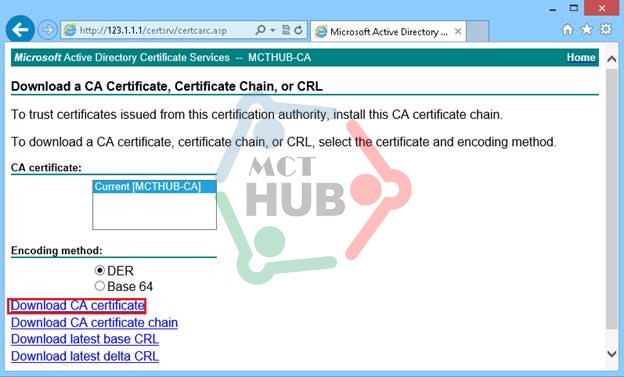
- Khai báo User/Pass bằng quyền user VPN, Add địa chỉ *http://10.10.0.1* vào *Trusted Site*.



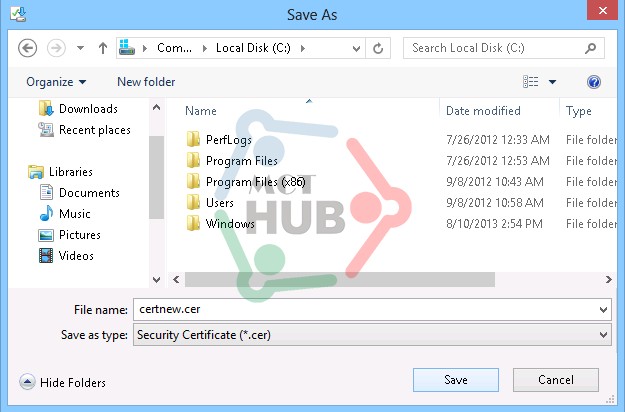
- Cửa sổ *Welcome*, chọn *Download a CA certificate, certificate chain, or CRL*.



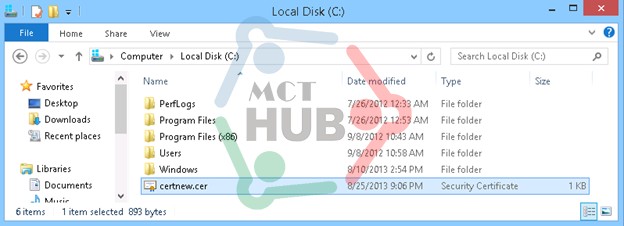
- Cửa sổ *Download a CA Certificate, Certificate Chain, or CRL,* chọn *Download CA Certificate*.



- Hộp thoại *Save As*, lưu file *certnew.cer* vào ổ đĩa *C:\,* chọn *Save*.

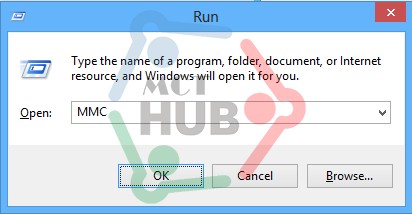


- Kiểm tra trong ổ C:\ có certificate vừa download.

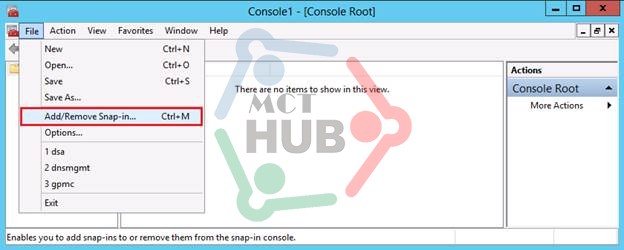


**8/ Cấu hình Trusted Root CA trên VPN Client**

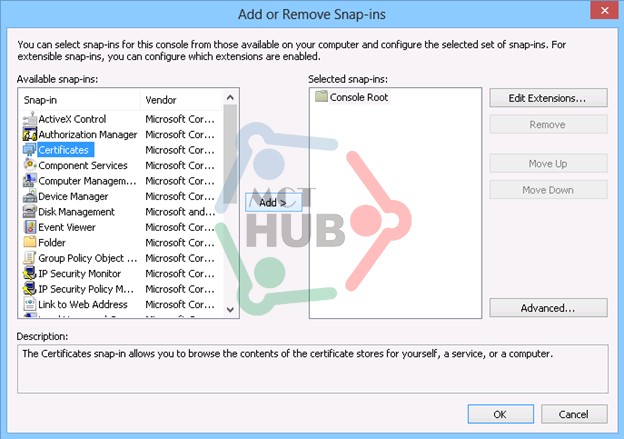
- Tại máy Client1, vào *Run*, gõ *MMC*.



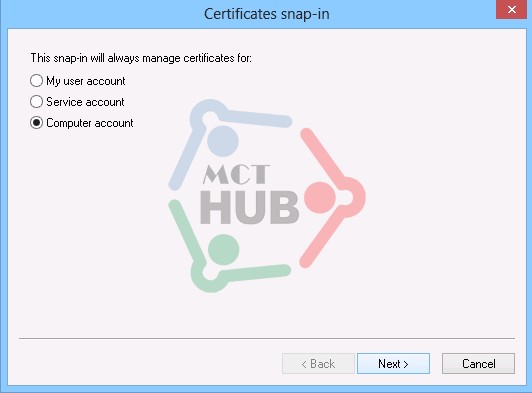
- Trong cửa sổ *Console1*, vào menu *File*, chọn *Add/Remove Snap-in*.



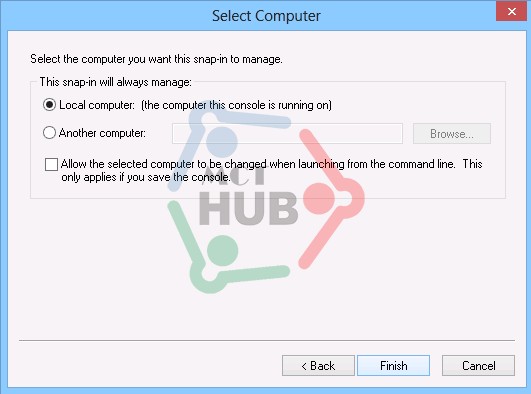
- Trong cửa sổ *Add or Remove Snap-in*, chọn *Certificates*, nhấn *Add,* chọn *OK*.



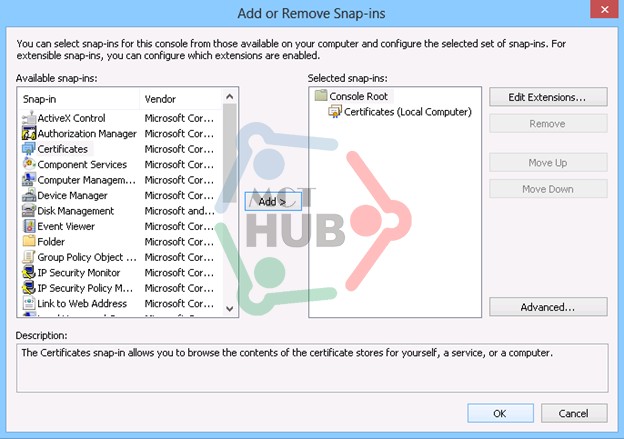
- Cửa sổ *Certificates Snap-in*, chọn *Computer Account*, nhấn *Next*.



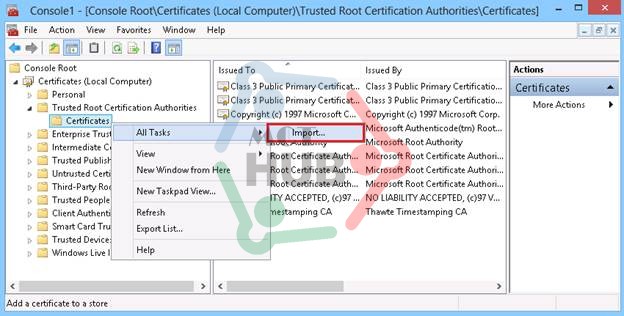
- Cửa sổ *Select Computer*, chọn *Local Computer*.



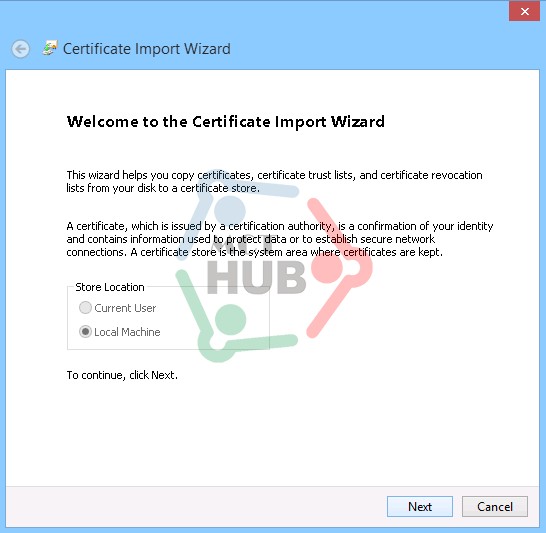
- Bạn nhấn OK.



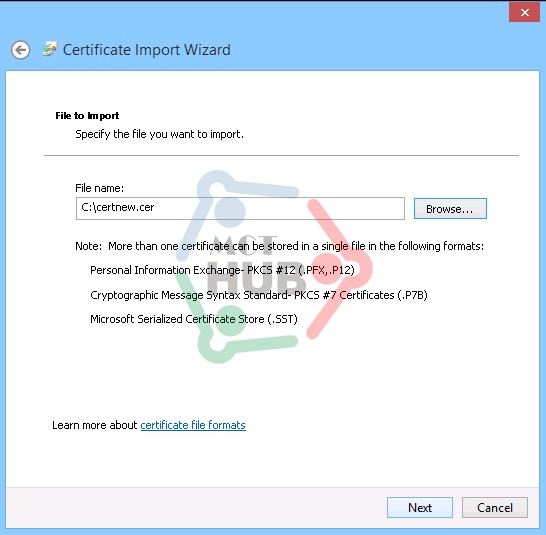
- Trong *cửa sổ Console1*, bung *Trusted Root Certificate Authority*, chuột phải *Certificates*, chọn *All Tasks*, chọn *Import*.



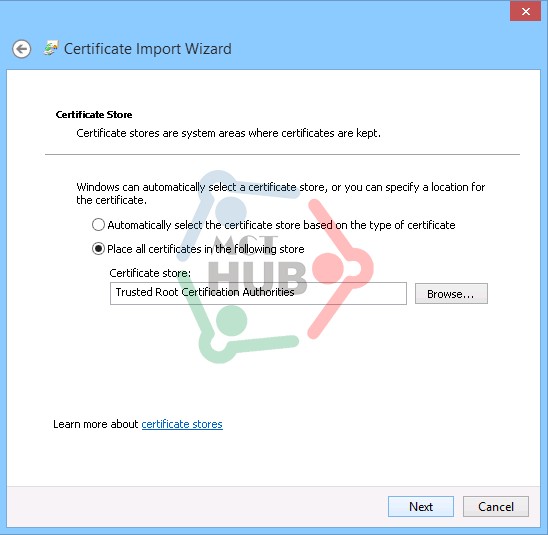
- Hộp thoại *Welcome to the Certificate Import Wizard*, nhấn *Next*.



- Hộp thoại *File to Import*, chọn *Browse*, trỏ đường dẫn đến *C:\certnew.cer*, nhấn *Next*.



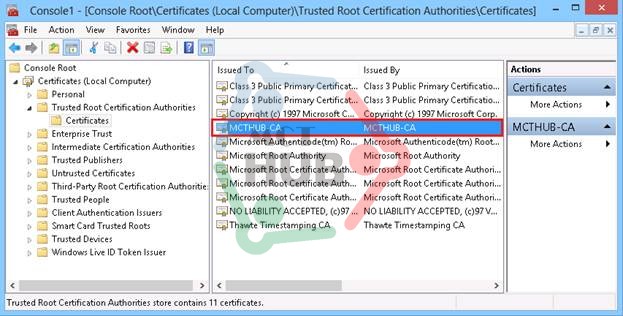
-  Hộp thoại *Certificate Store*, giữ nguyên cấu hình mặc định, nhấn Next.



- Hộp thoại *Completing the Certificate Import Wizard*, nhấn *Finish*.



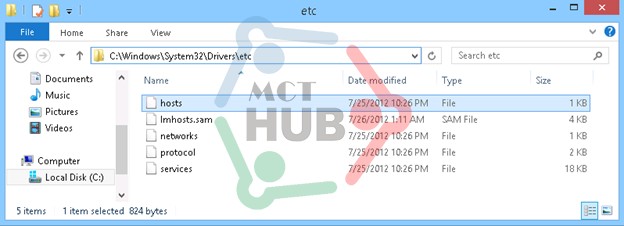
- Quan sát thấy certificate vừa được import.



**9/ Tạo VPN Connection**

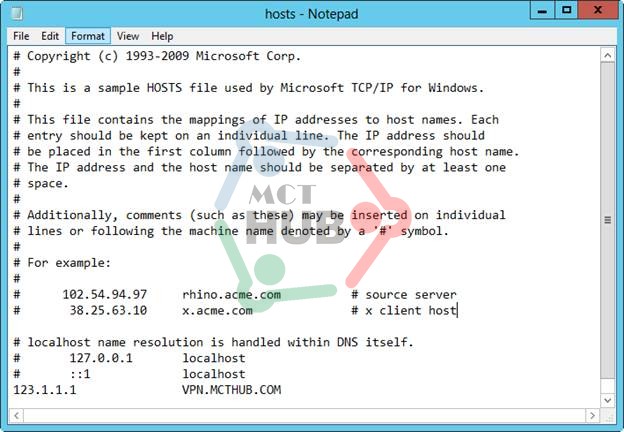
Trong môi trường thực tế, khi Client kết nối Internet sẽ phân giải được tên VPN.MCTHUB.COM ra IP Public của VPN Server. Để giả lập môi trường này, bạn cần khai báo file HOSTS để Client có thể phân giải tên *VPN.MCTHUB.COM*

- Tại máy Client1, mở *Windows Explore*, vào đường dẫn *C:\ Windows\System32\Driver\etc*, mở file Hosts



- Bạn nhập thêm nội dung sau:

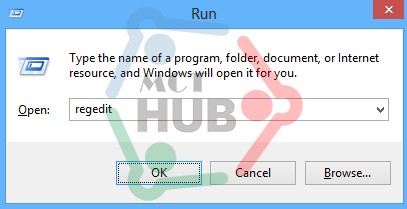
*123.1.1.1    VPN.MCTHUB.COM*



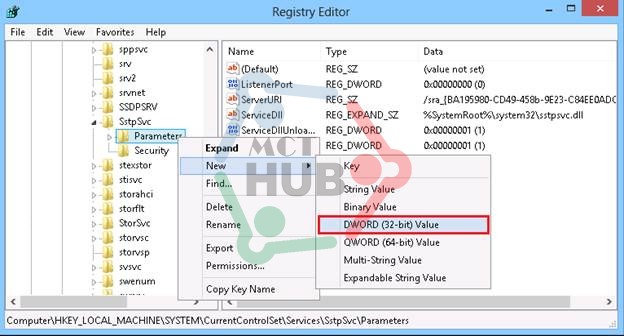
Tới bước này ta cần hiểu thêm về Certificate Revocation, mỗi một Certificate được tạo ra đều có một khoảng thời gian biệu lực (validity period) nhất định và thường từ 1 đến 2 năm. Khi vượt ra khỏi khoảng thời gian này thì nó sẽ hết hạn và không có giá trị nữa. Thông tin này được chứa trong bản thân Certificate gồm giá trị valid from và valid to, nên cần được kiểm tra trước khi quyết định có nên tiến hành giao dịch.

*Certificate Revocation List* là danh sách các Certificate bị thu hồi và không còn được tin dùng nữa. Trong quá trình giao dịch giữa Server và Client, thì Client sẽ tiến hành download Certificate Revocation List được publish trên Server và tiến hành import, ở đây tôi sẽ chỉnh Registry để Client không cần kiểm tra CRL khi thực hiện kết nối.

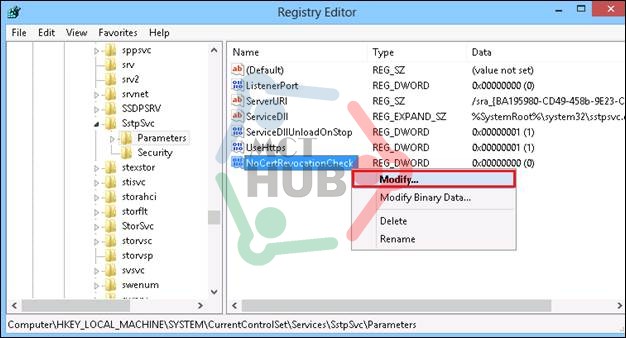
- Vào Run, gõ Regedit.



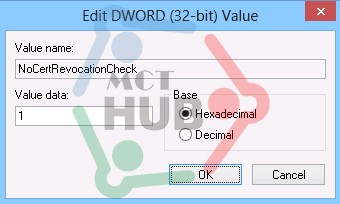
-  Trong cửa sổ Registry Editor, bạn tìm đến khóa sau *Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SSTPSVC\Parameters*. Chuột phải*Parameters,* chọn *New*, sau đó chọn *DWORD (32-bit) Value*.



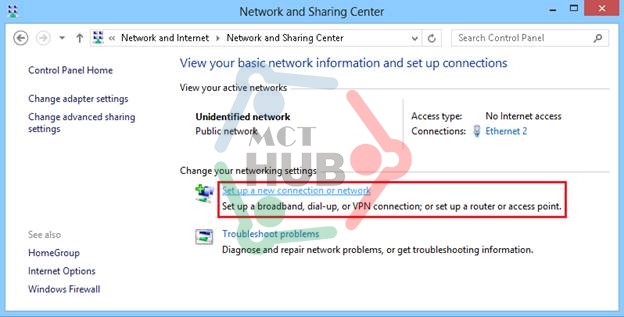
- Bạn đặt tên cho DWORD là *NoCertRevocationCheck,* chuột phải DWORD vừa tạo chọn *Modify.*



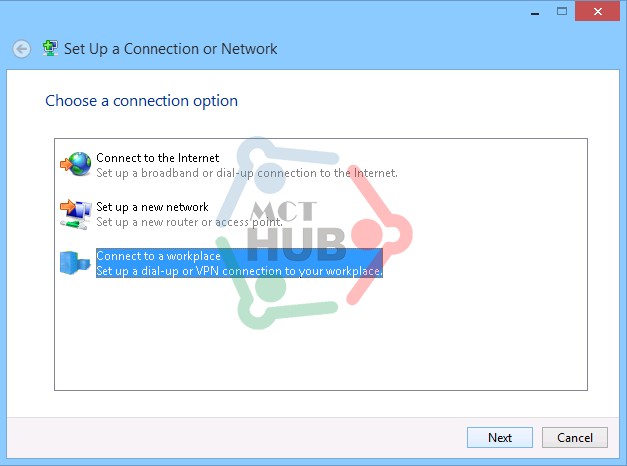
- Cửa sổ *Edit DWORD (32-bit) Value*, ở khung Value data, bạn sửa lại giá trị là1



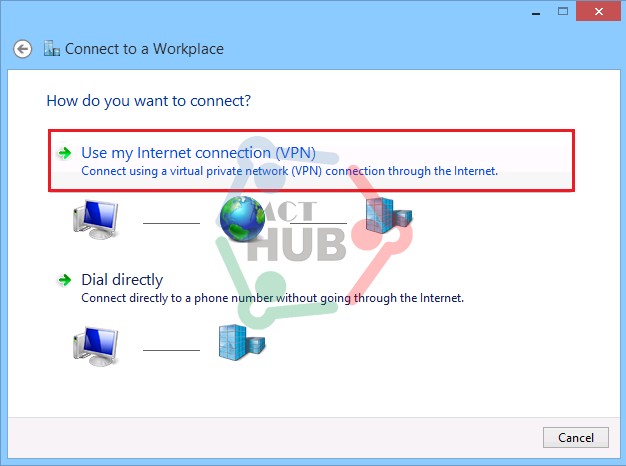
- Mở *Network and Sharing Center*, chọn *Setup a new connection or network*.



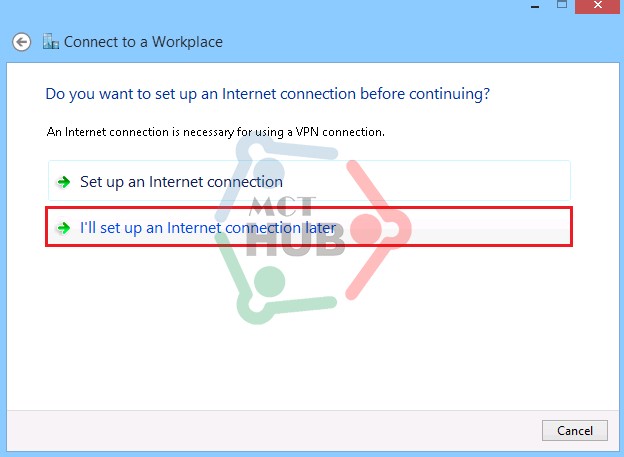
- Hộp thoại *Choose a connection options*, chọn *Connect to a workplace*, nhấn Next.



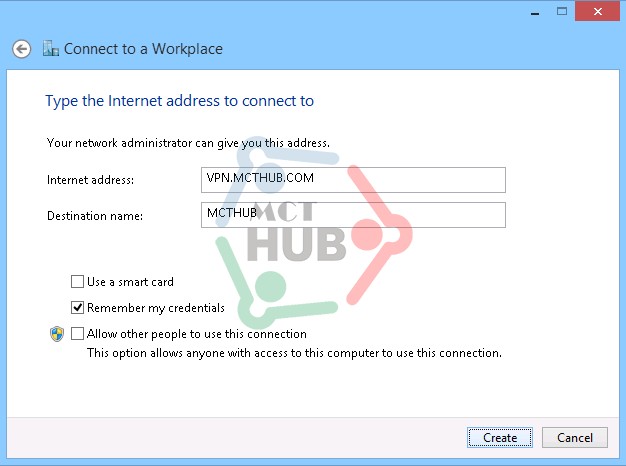
- Hộp thoại *How to you want to connect*, chọn *Use my Internet connection (VPN)*.



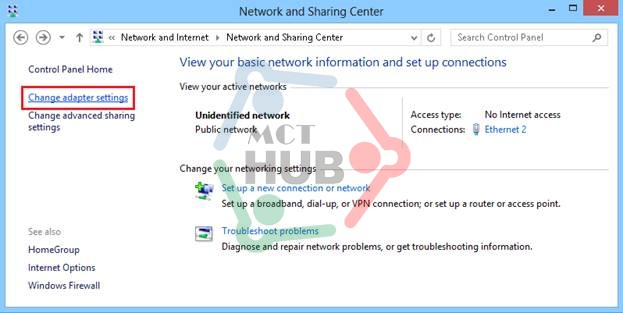
-  Hộp thoại *Do you want to setup an Internet connection before continuing*, chọn *I'll setup an Internet Connection later*.



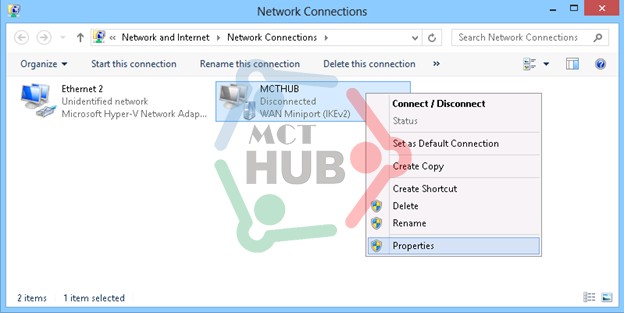
-  Hộp thoại *Type the internet address to connect to*, nhập *User Account* được phép kết nối (trong bài lab này là *VPN.MCTHUB.LOCAL*).



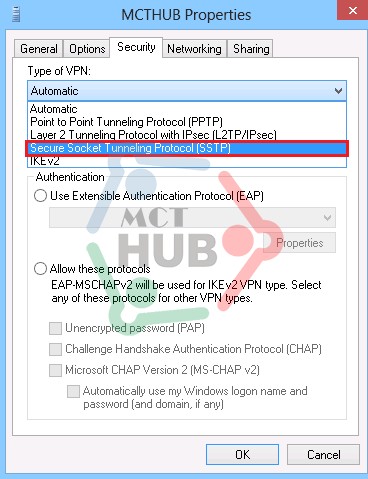
- Trong cửa sổ *Network Sharing Center*, bạn chọn *Change Adapter Settings*.



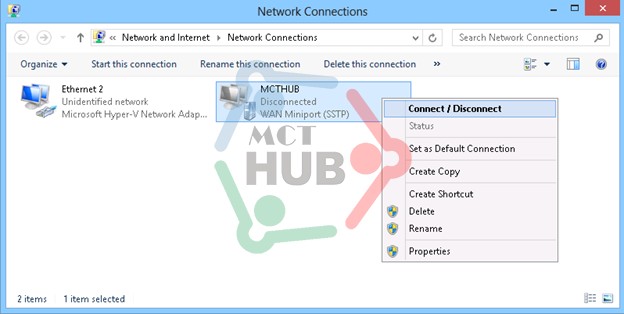
-  Cửa sổ *Network Connections*, chuột phải *VPN Connection*, chọn *Properties*.



-  Qua tab *Security*, type of *VPN: Serure Socket Tunneling Protocol (SSTP)*, kiểu kết nối *VPN SSTP* .



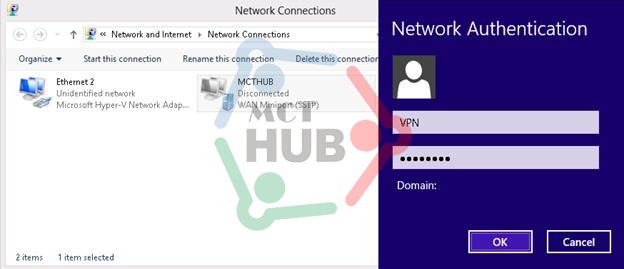
- Để kết nối *VPN*, bạn chuột phải lên *VPN Connections*, chọn *Connect / Disconnect*.



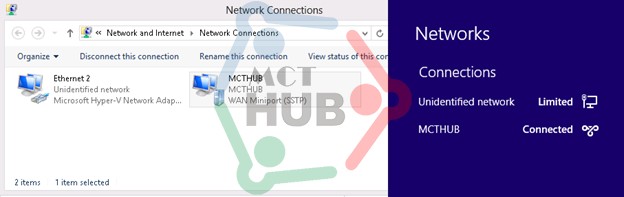
- Cửa sổ *Networks*, trong mục *MCTHUB* bạn chọn *Connect* để tiến hành kết nối.



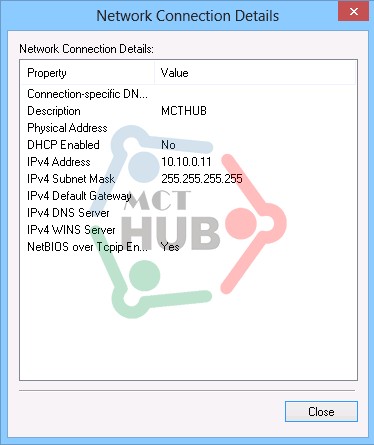
-  Trong cửa sổ *Network Authentication*, khai báo *Username và Password* chứng thực.

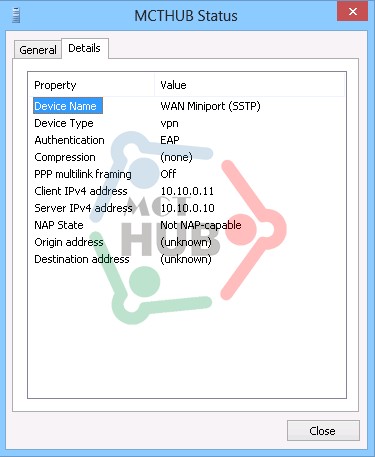


-  Kiểm tra *Connect VPN* thành công.

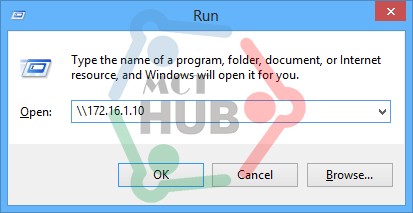


- Kiểm tra nhận được IP và sử dụng kết nối là Protocol SSTP do VPN Server cung cấp.





-  Truy cập địa chỉ [**\\172.16.1.10**](file:///\\172.16.1.10\).



- Kiểm tra truy cập thành công hệ thống mạng nội bộ bên trong.

