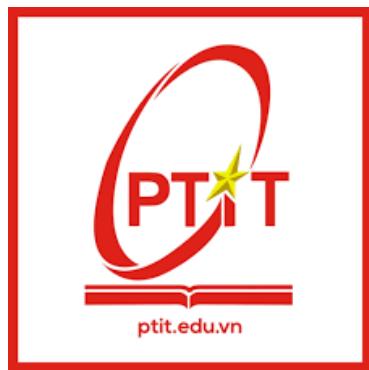


BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN 2



**Hệ Điều Hành Window, Linux
ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI
CÁC DỊCH VỤ TRÊN WINDOWS
(WINDOWS SERVER)**

Người thực hiện : Nguyễn Công Lực

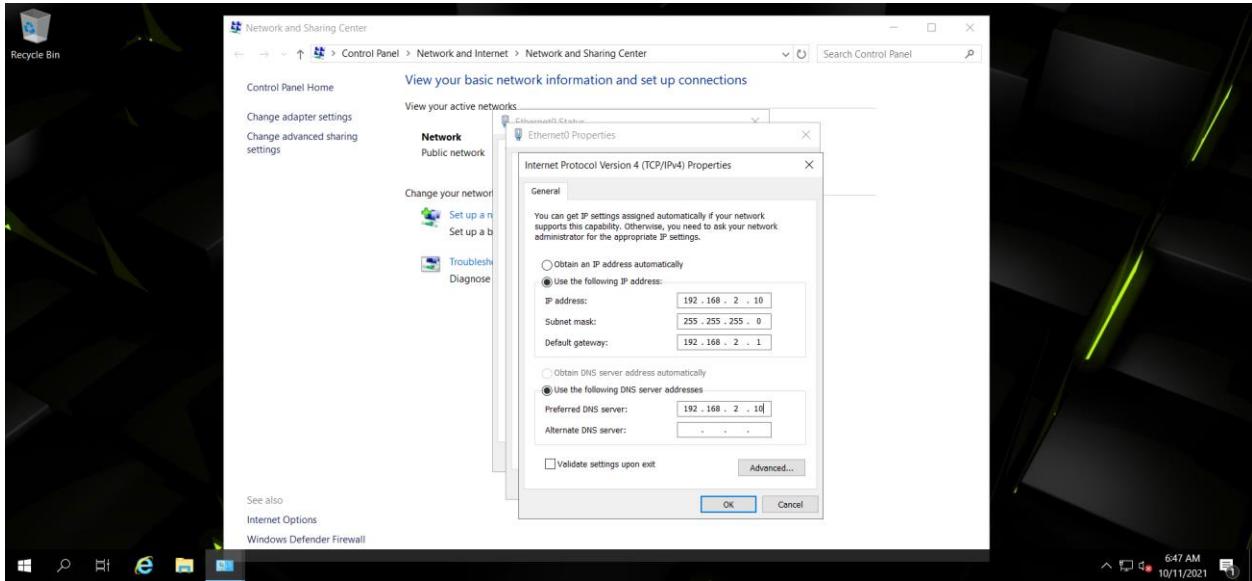
MỤC LỤC

- A. Cài đặt máy Domain Controller
 - 1. Cài đặt dịch vụ Active Directory Domain Services
 - 2. Nâng cấp thành Domain Controller
 - 3. Tạo Reverse Lookup Zones
 - 4. Cấu hình DNS Forwarder
 - 5. Cài đặt dịch vụ Remote Access
- B. Cài đặt VPN Server
 - 1 Cấp quyền Network Access Permission cho User
 - 2. Cài đặt NPS Network Policy
- C. Cài đặt Sophos Firewall và chính sách truy cập Internet
 - 1. Cài đặt cơ bản
 - 2. Cài đặt truy cập Internet cho nhân viên
 - 3. Thiết lập chính sách cho nhân viên
 - 4. Cài đặt chính sách Proxy Server cho máy nhân viên
- C. Cài đặt điều khiển Server từ xa cho quản trị viên
- D. Cấu hình DHCP sever

- A. Cài đặt máy Domain Controller

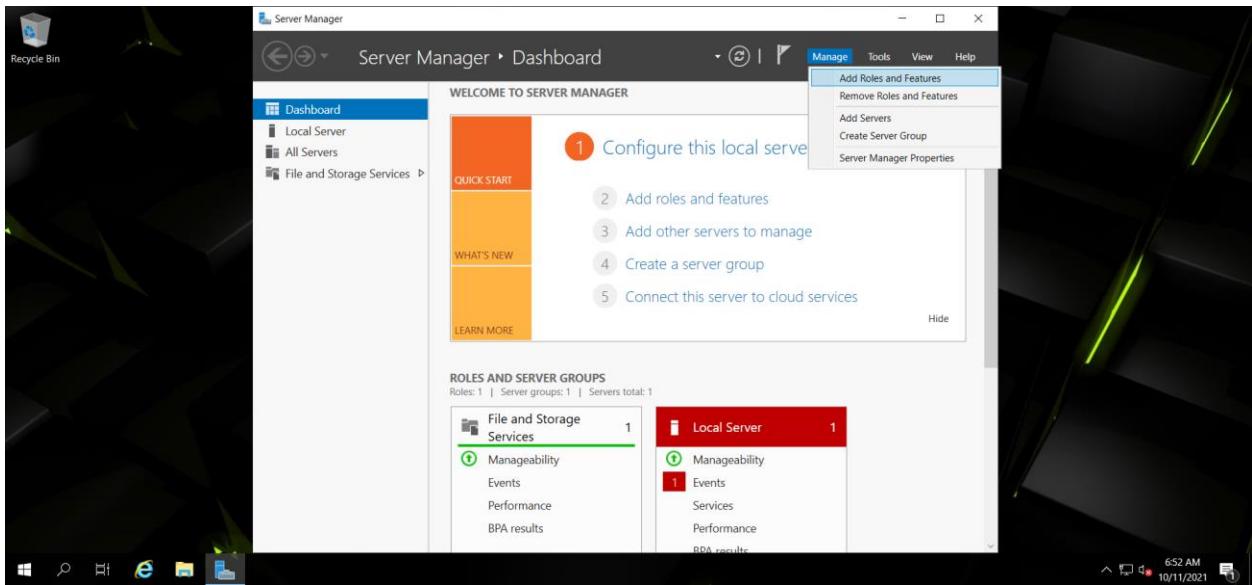
1. Cài đặt dịch vụ Active Directory Domain Services

Máy làm Domain Controller cài Windows Server 2019



Hình 1.1: Đặt IP cho máy Domain Controller

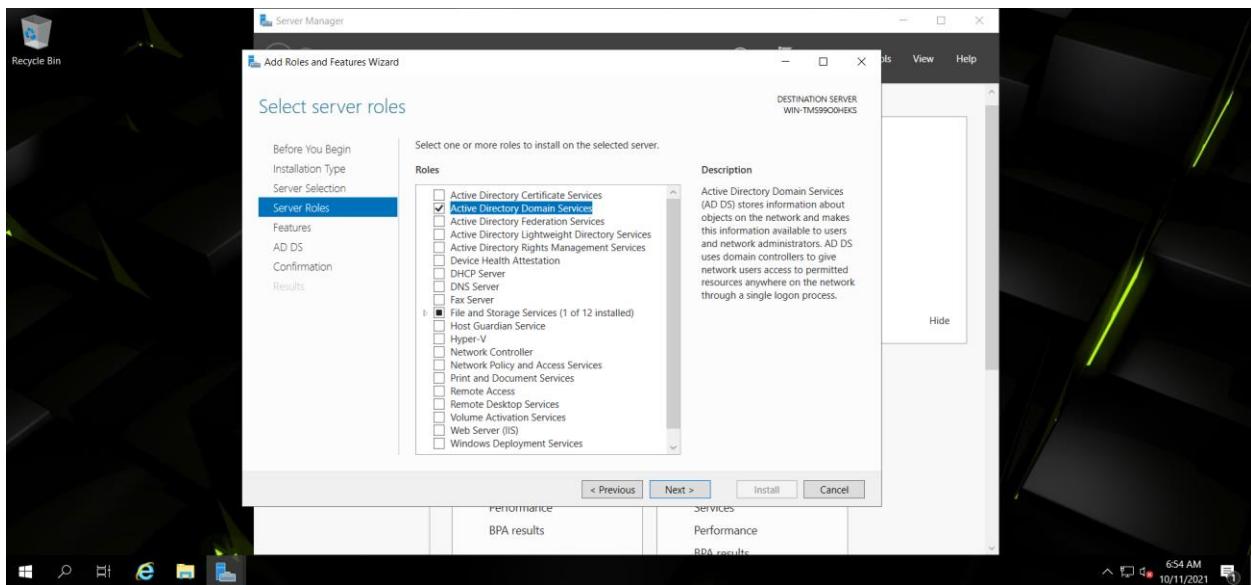
Vào Server Manager và chọn Add roles and feature



Hình 1.2 Server Manager

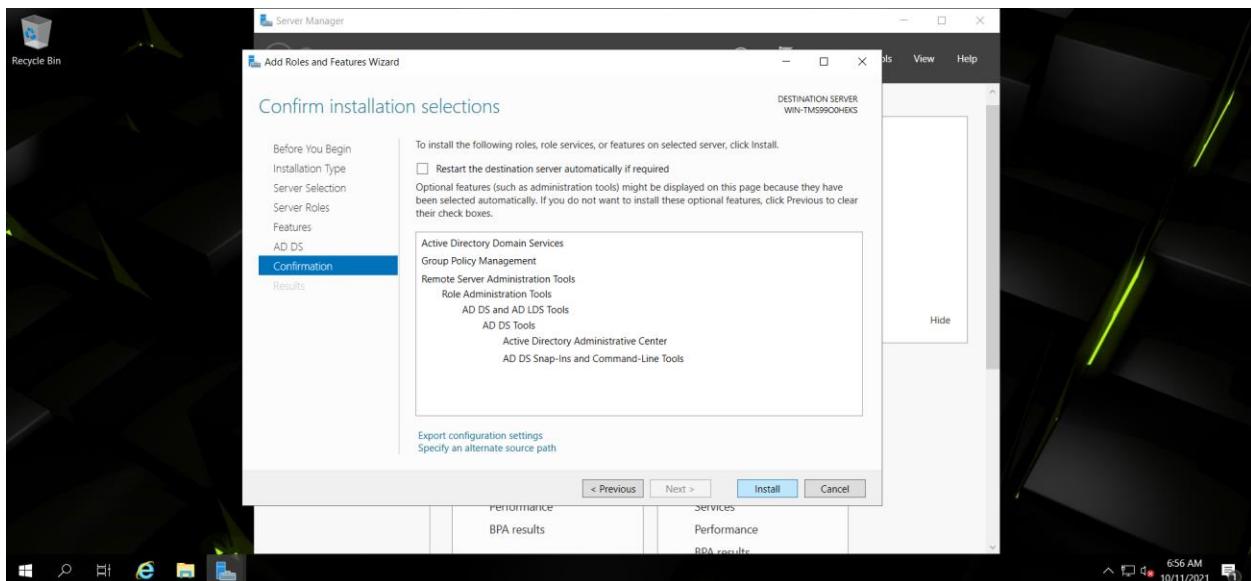
Thực hiện Next 3 lần

Tại Server Roles chọn vào Active Directory Domain Services rồi Add Features và tiếp tục Next 3 lần

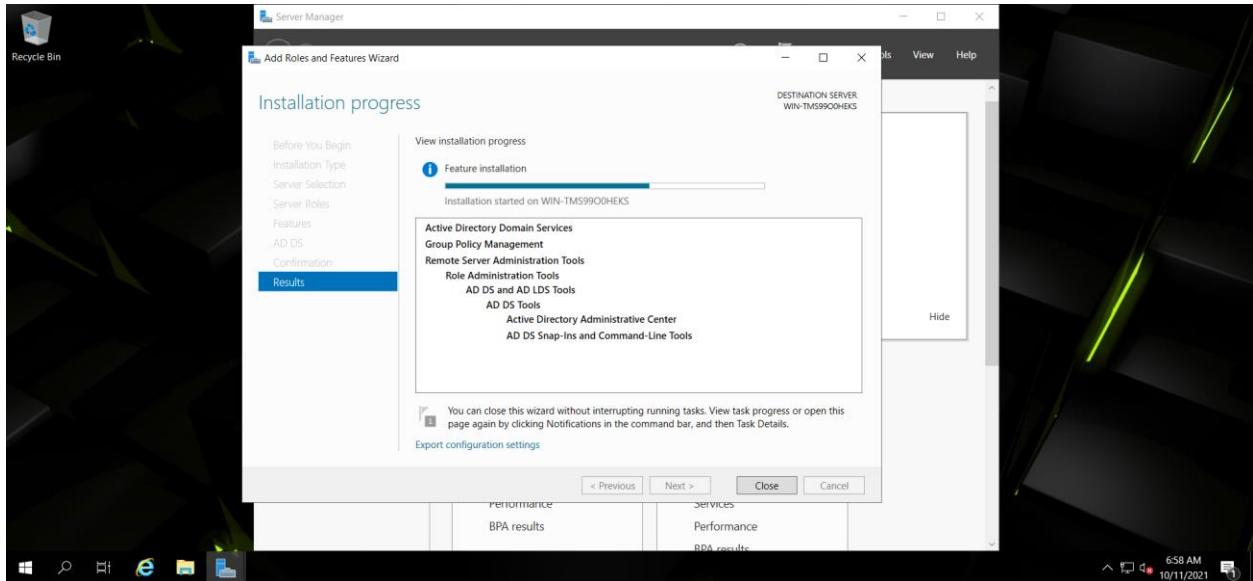


Hình 1.3 chọn Active Directory Domain Services

Kiểm tra lại các lựa chọn và nhấn Install

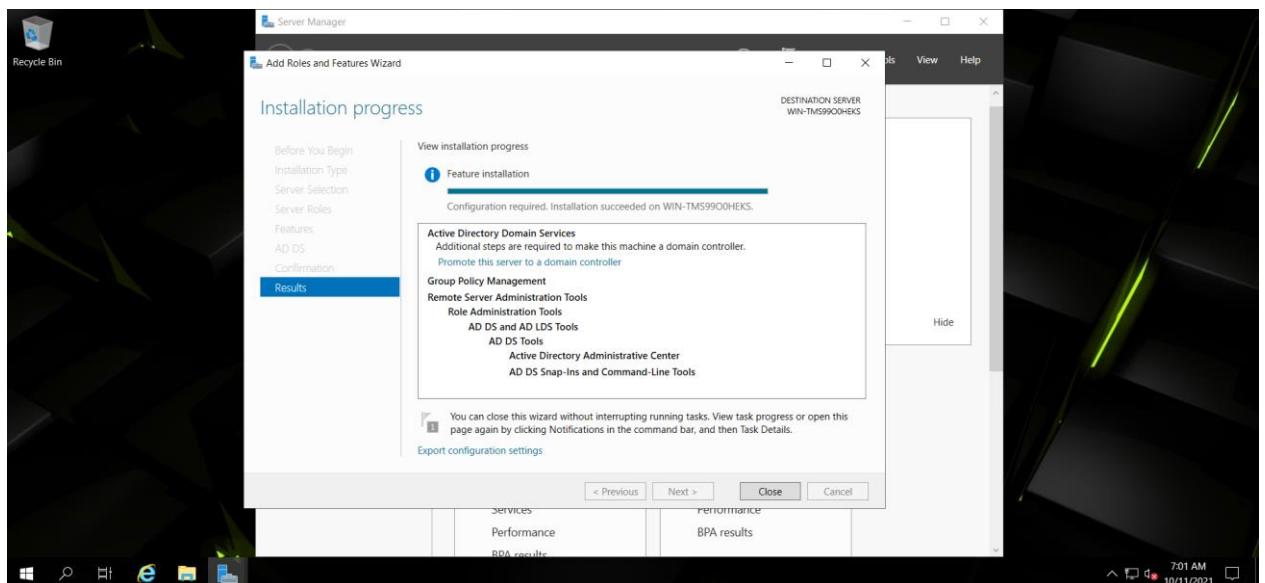


Hình 1.4: Quá trình xác nhận và cài đặt



Hình 1. 5: Quá trình cài đặt

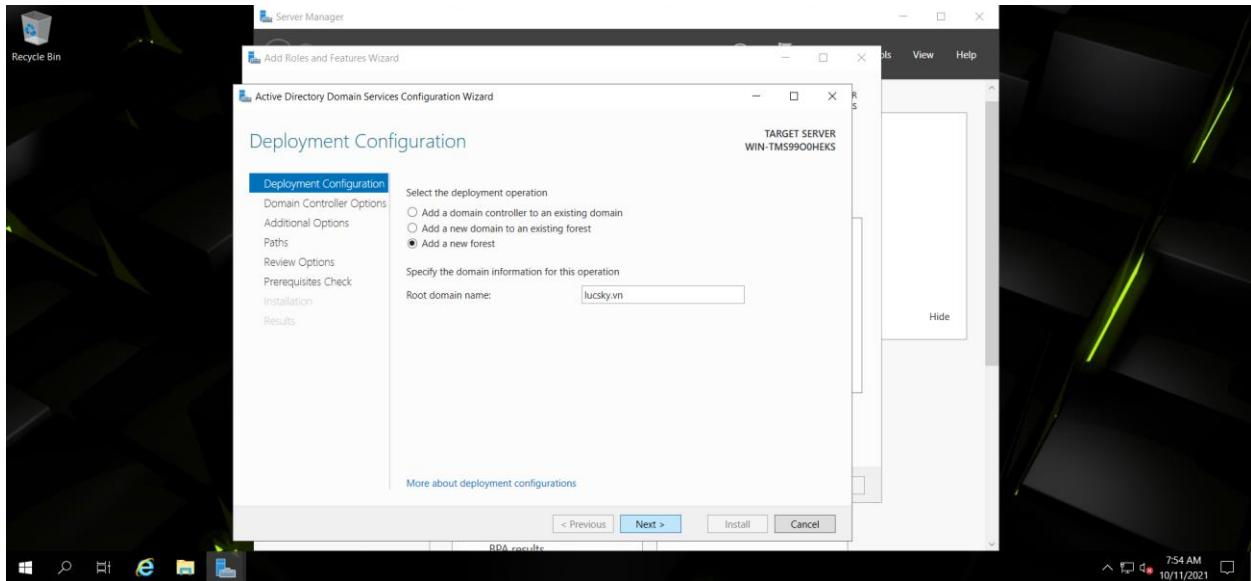
Nhấn vào Promote this server to a domain controller để thực hiện tiếp quá trình



Hình 1. 6: Cài đặt thành công

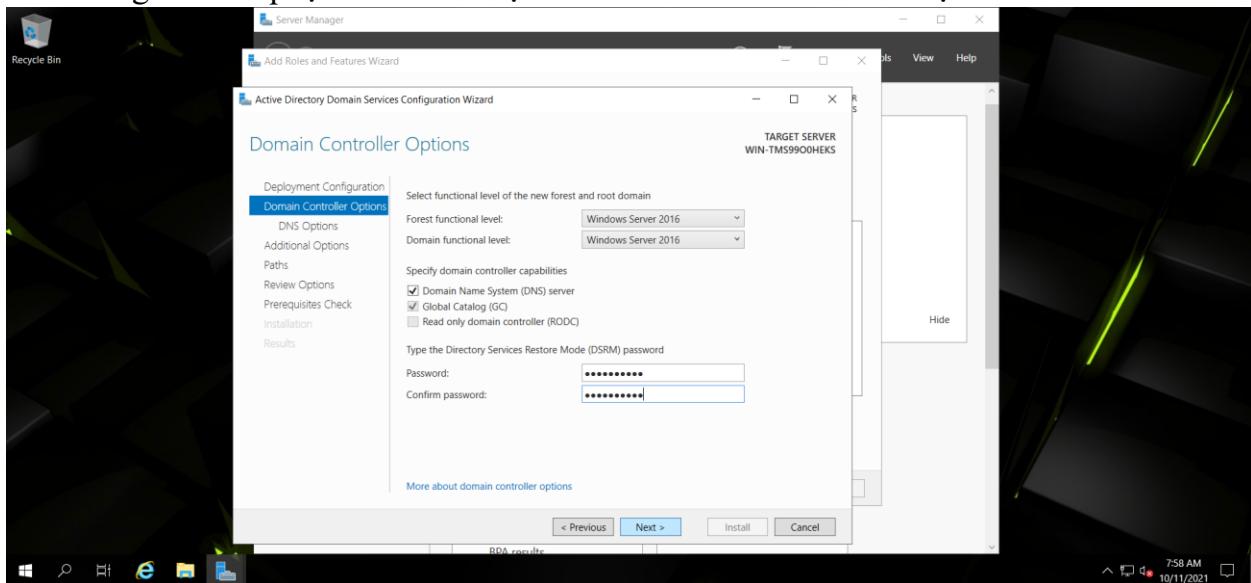
2. Nâng cấp thành Domain Controller

Ở đây thêm mới hoàn toàn một domain nên chọn vào Add a new forest và nhập domain name và chọn Next



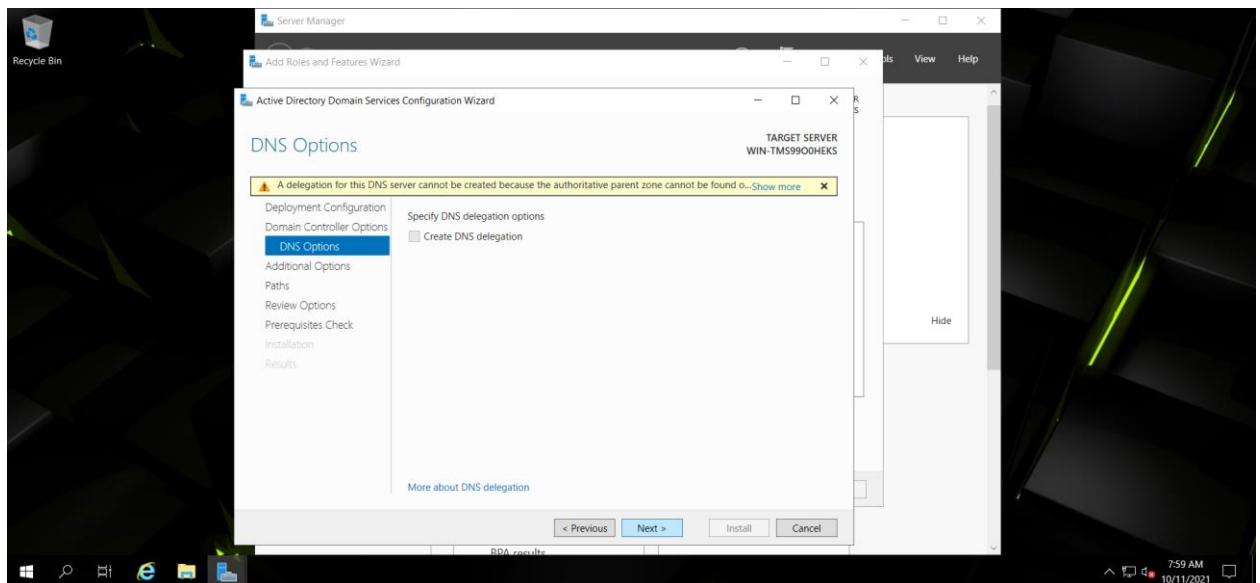
Hình 1.7: Thêm mới domain name

Thiết lập mật khẩu ở phần Type the Directory Services Restore Mode.
Dùng để khôi phục AD ở chế độ Restore Remote và sau đó chọn Next

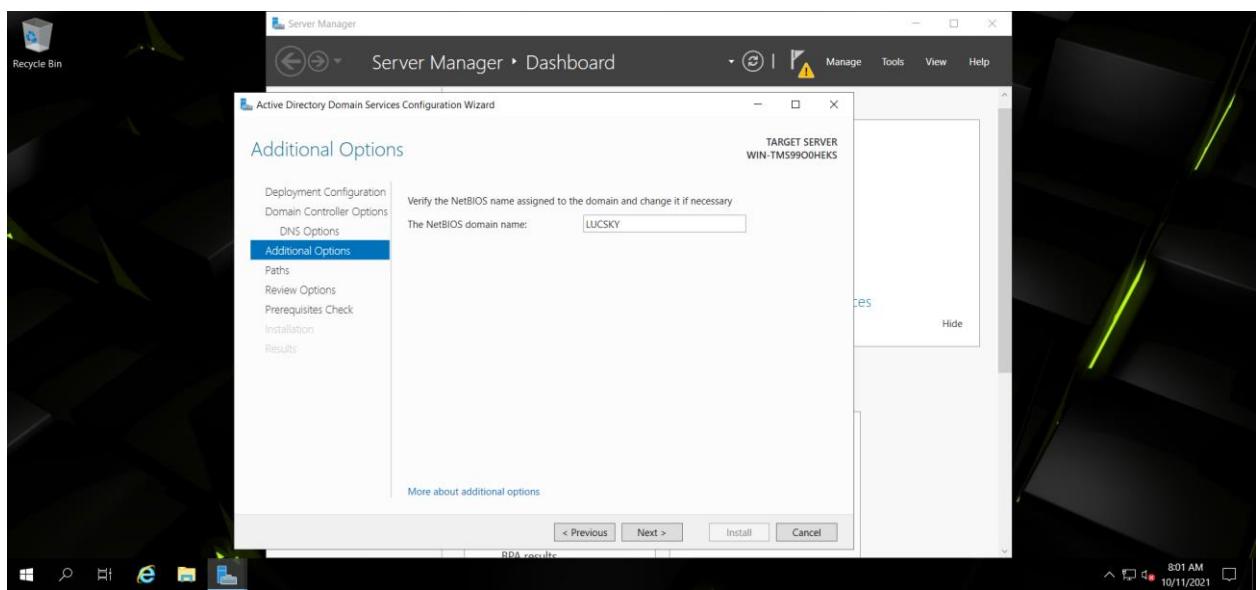


Hình 1.8: Thiết lập password Restore Mode

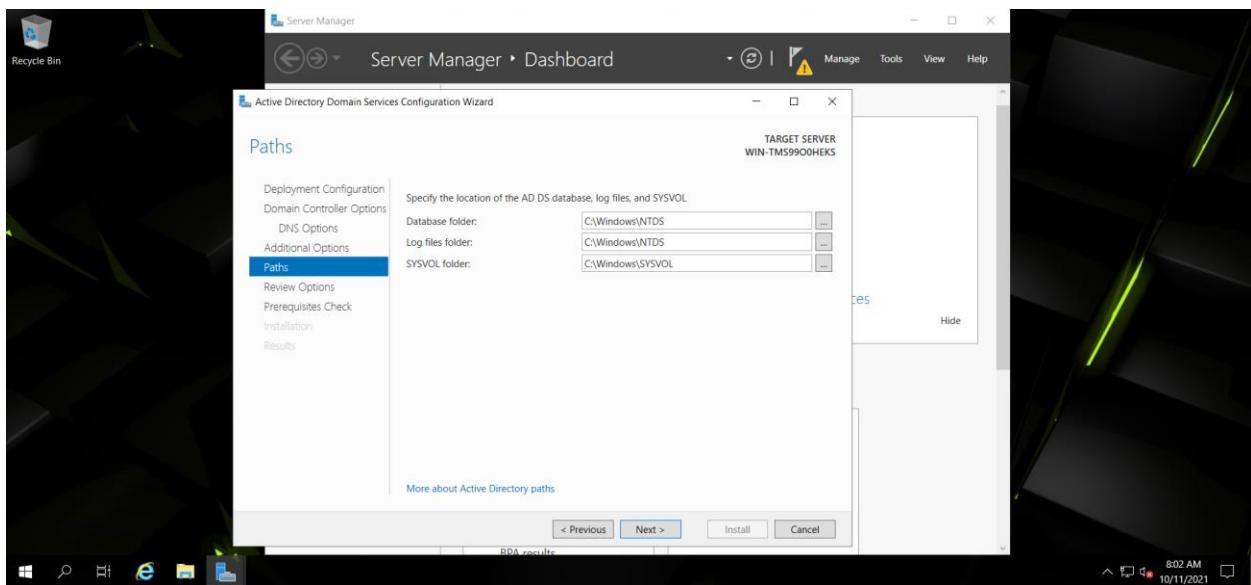
Các bước tiếp theo là Next theo hướng dẫn



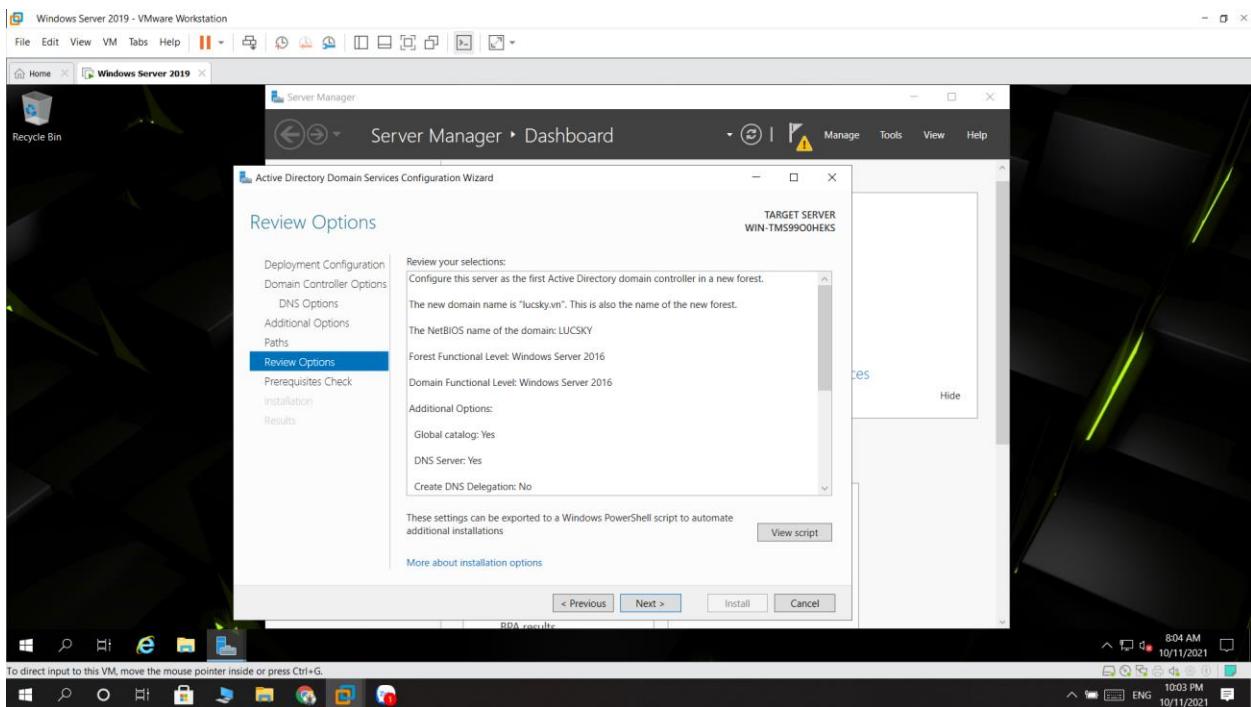
Hình 1. 9: DNS option



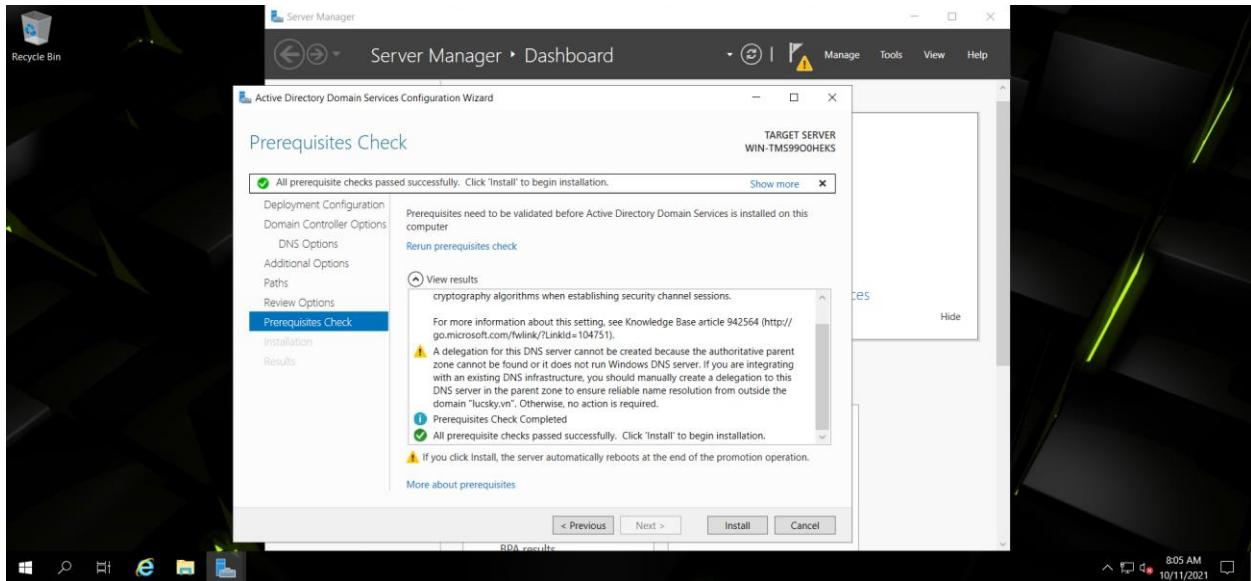
Hình 1. 10: NetBIOS domain name



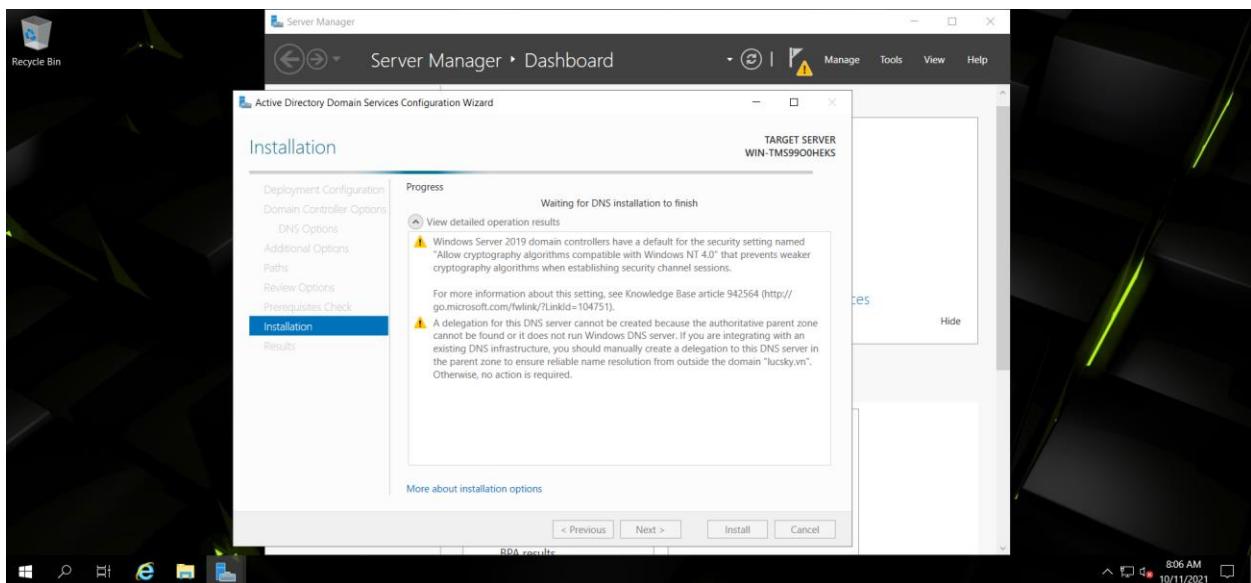
Hình 1. 11: Đường dẫn của database



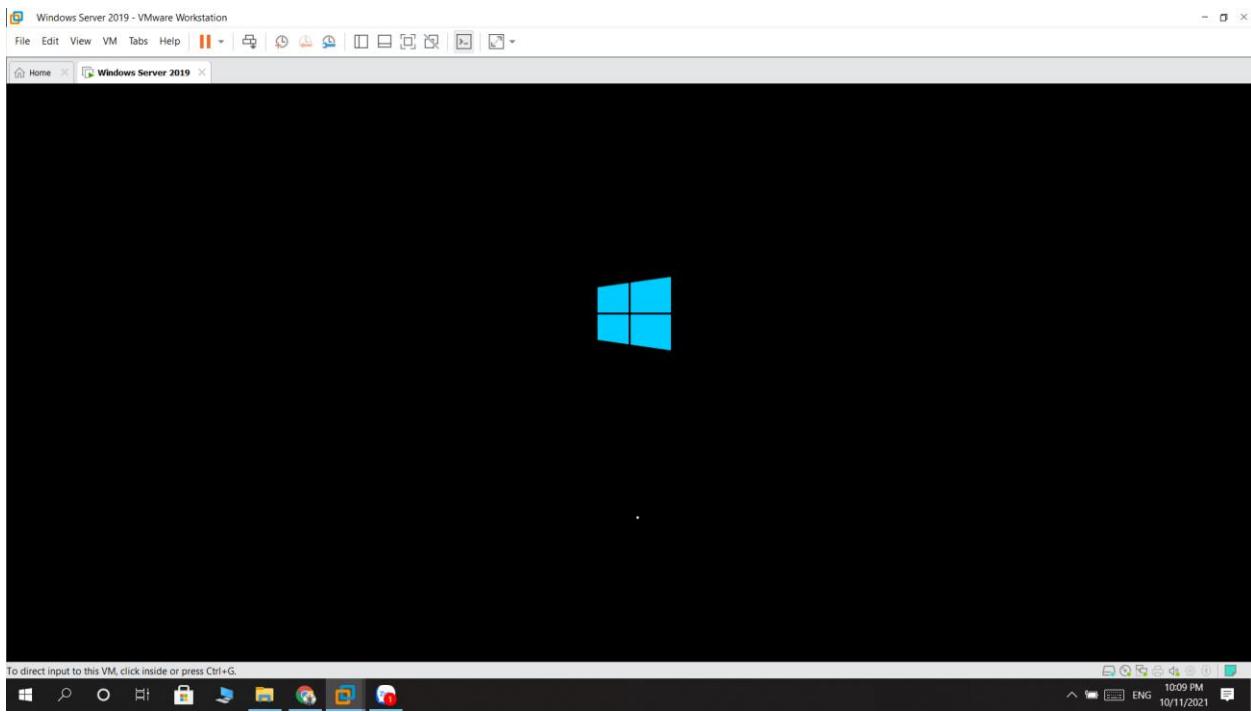
Hình 1. 12: Xem lại các lựa chọn



Hình 1. 13: Kiểm tra lại các yêu cầu trước



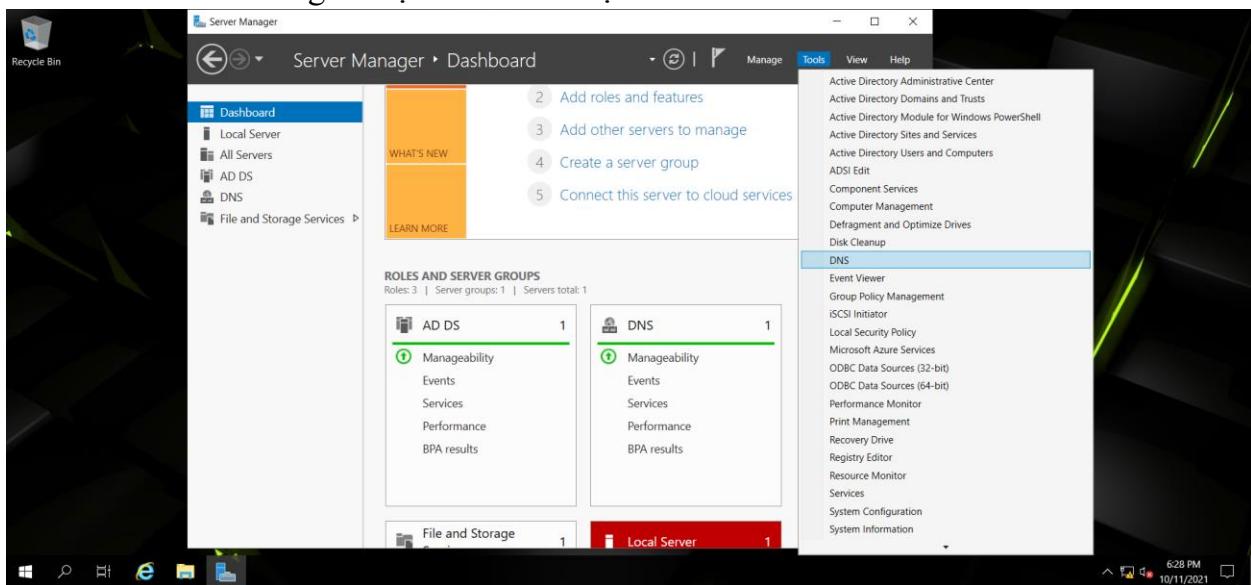
Hình 1. 14: Quá trình cài đặt



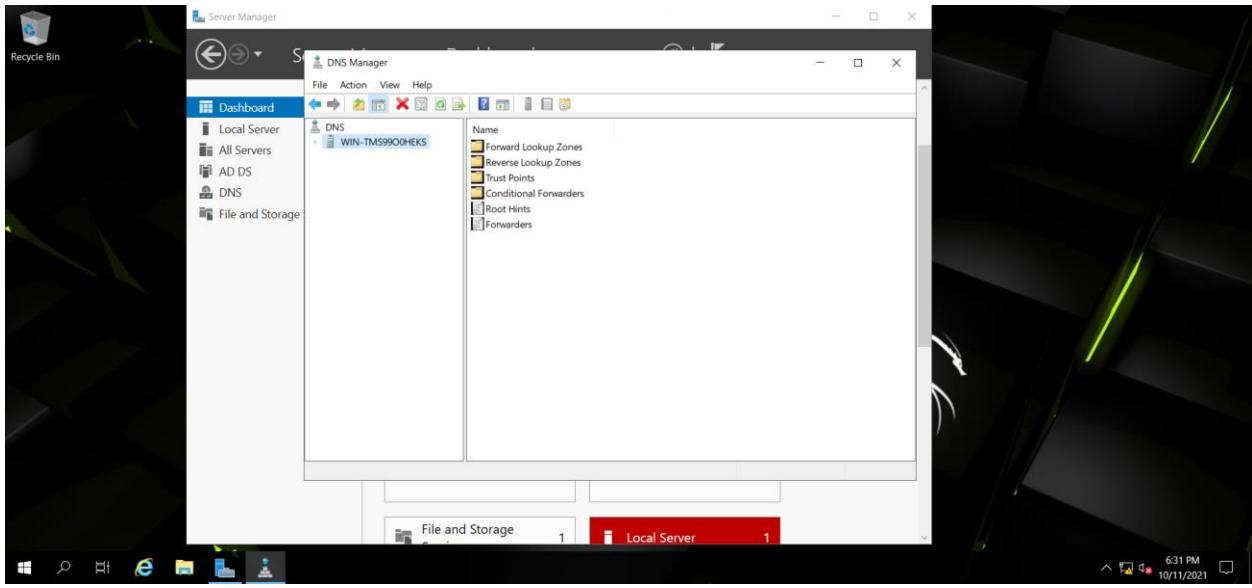
Hình 1. 15: Cài đặt đã thành công và khởi động lại

3. Tạo Reverse Lookup Zones

Mở Server Manager chọn Tools và chọn DNS

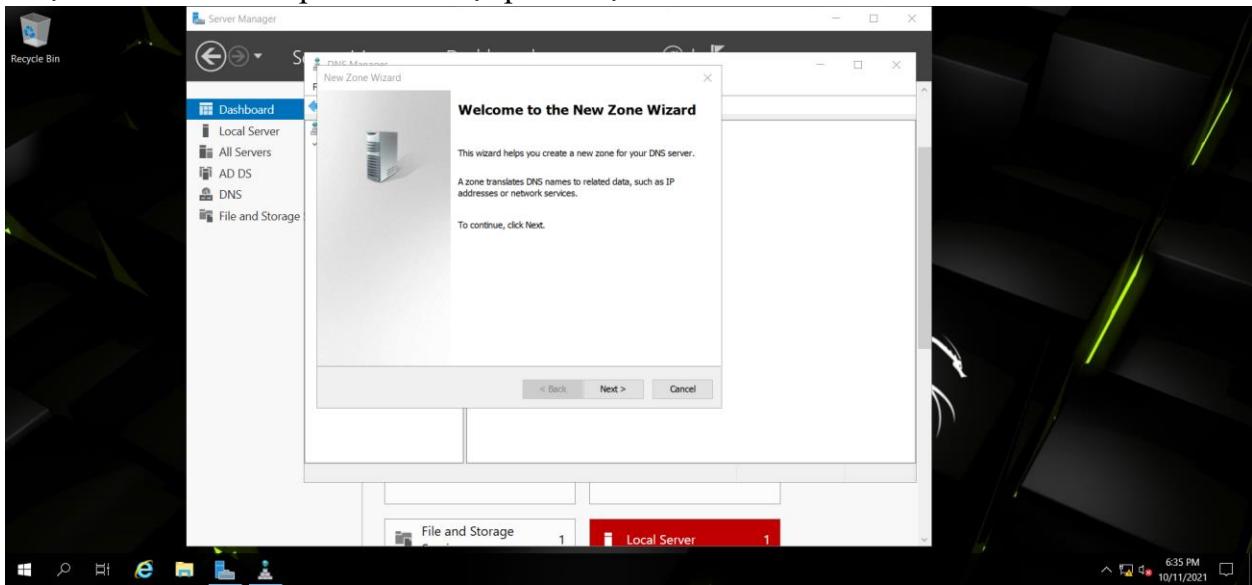


Hình 1. 16: Cửa sổ Server Manager



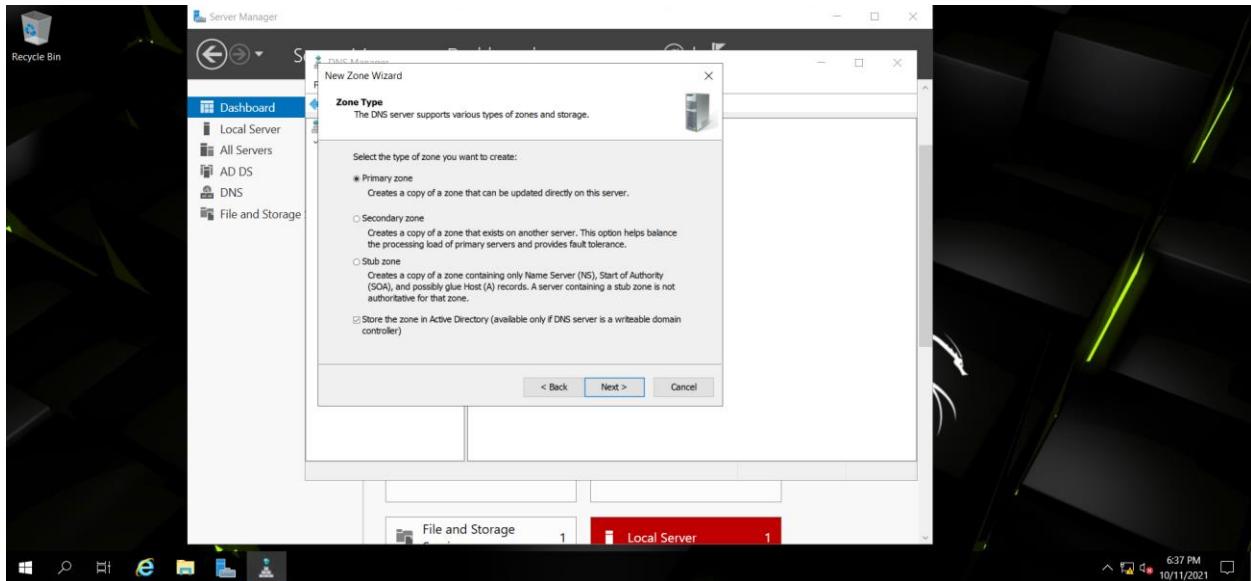
Hình 1. 17: DNS Manager

Chọn Reverse Lookup Zones chuột phải chọn new zone

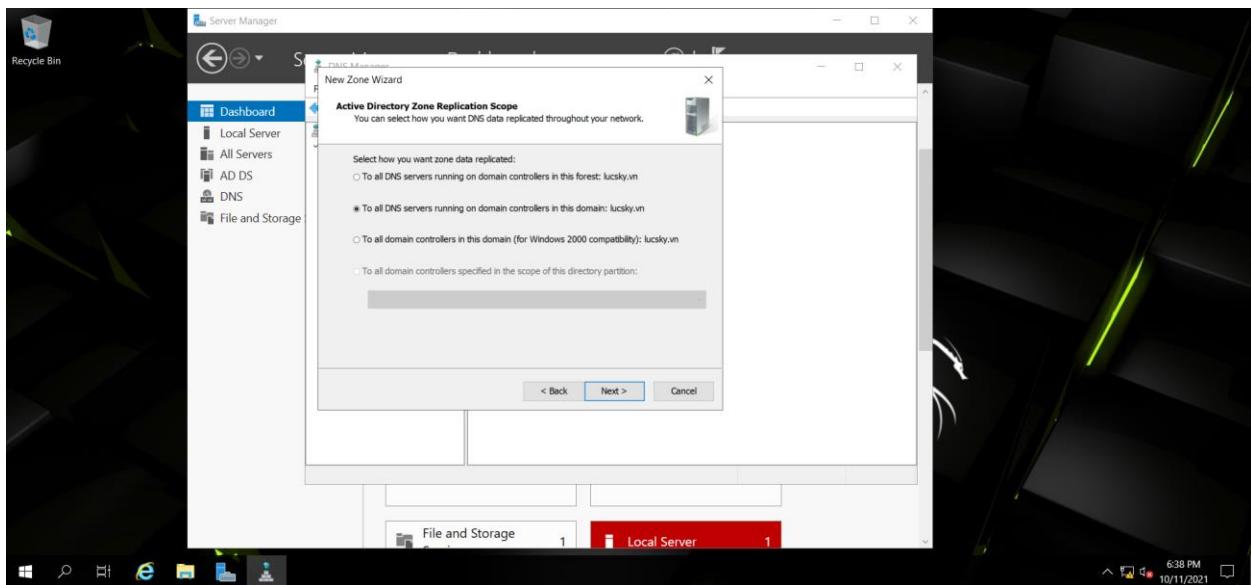


Hình 1. 18: Tạo new zone

Chọn Primary zone rồi chọn Next

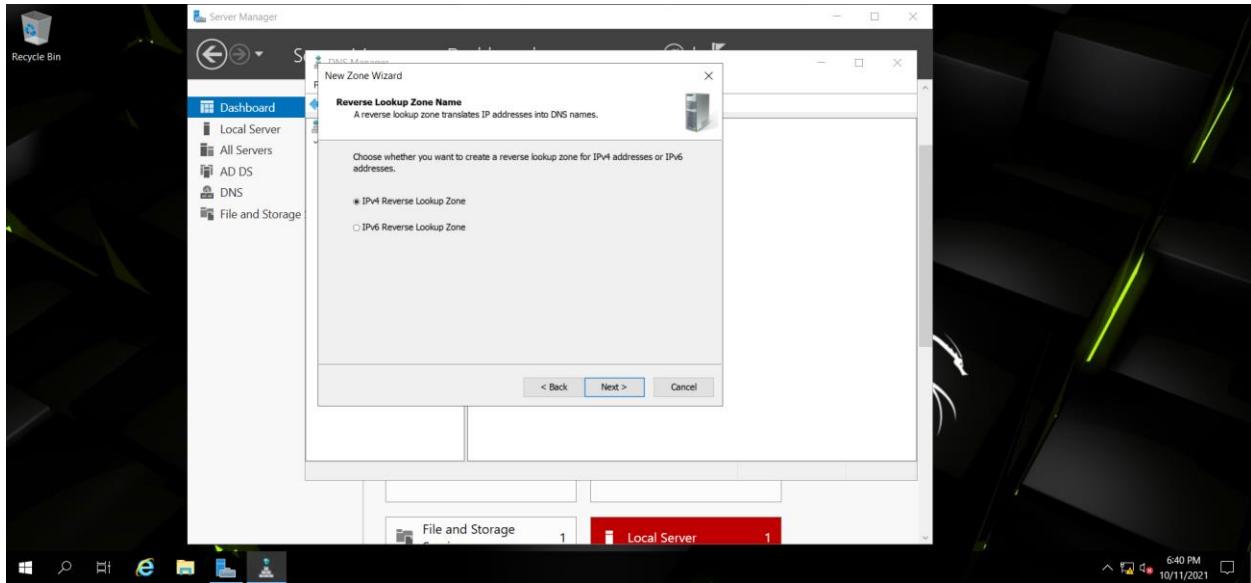


Hình 1. 19: Zone Type



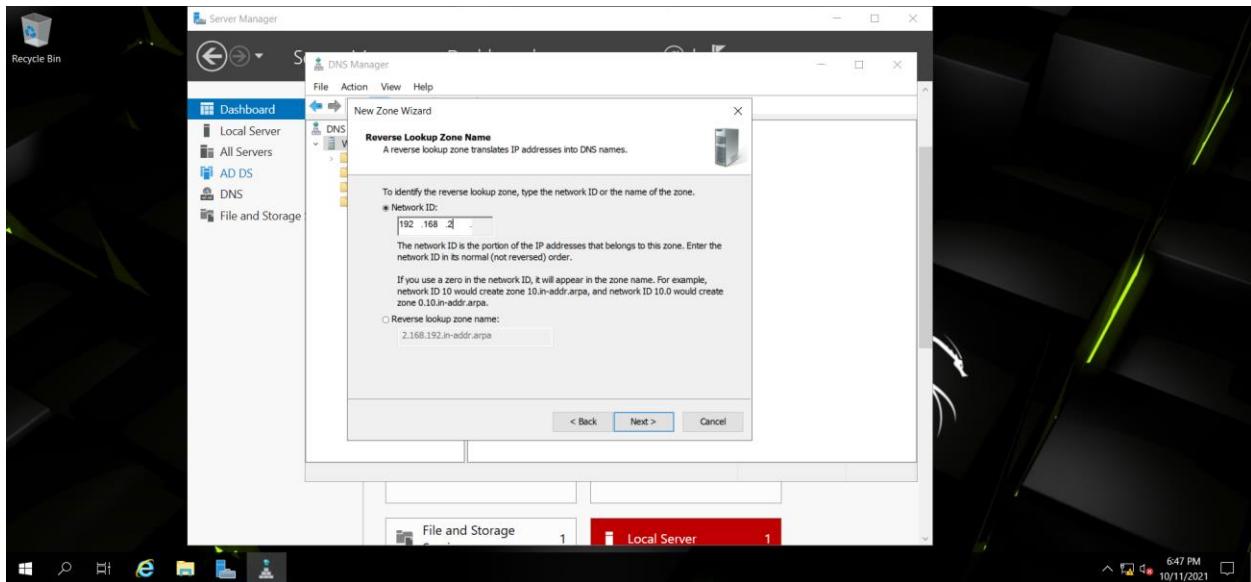
Hình 1. 20: Active Directory Zone

Chọn IPv4 Reverse Lookup Zone sau đó chọn Next

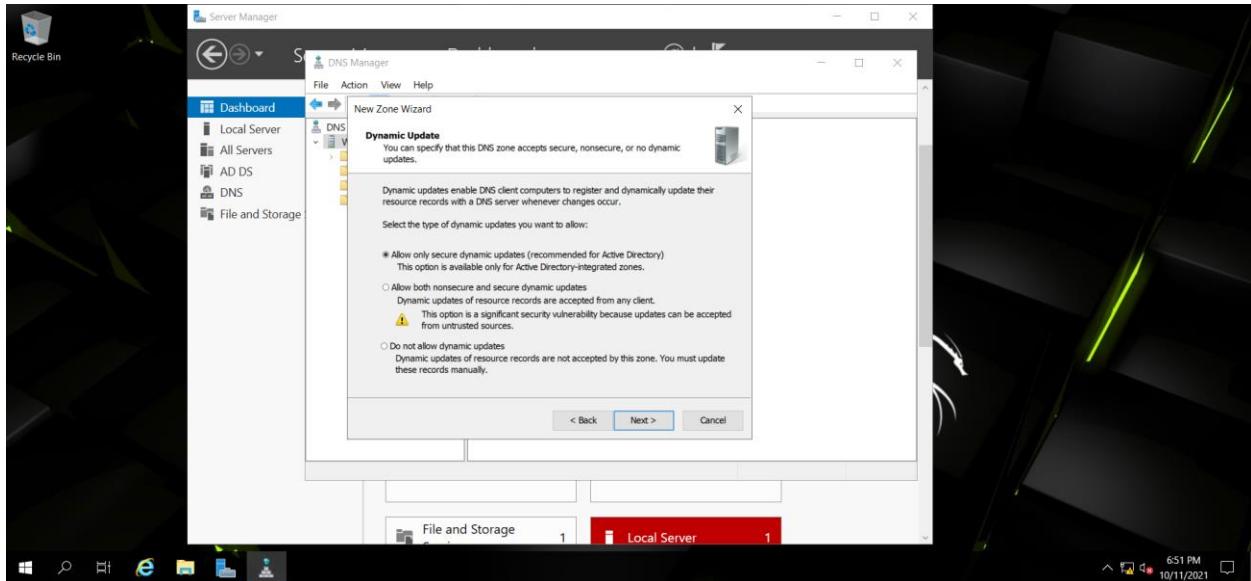


Hình 1. 21: IP Reverse Lookup Zone

Chỉ ra IP muốn tạo Reverse Lookup sau đó chọn Next



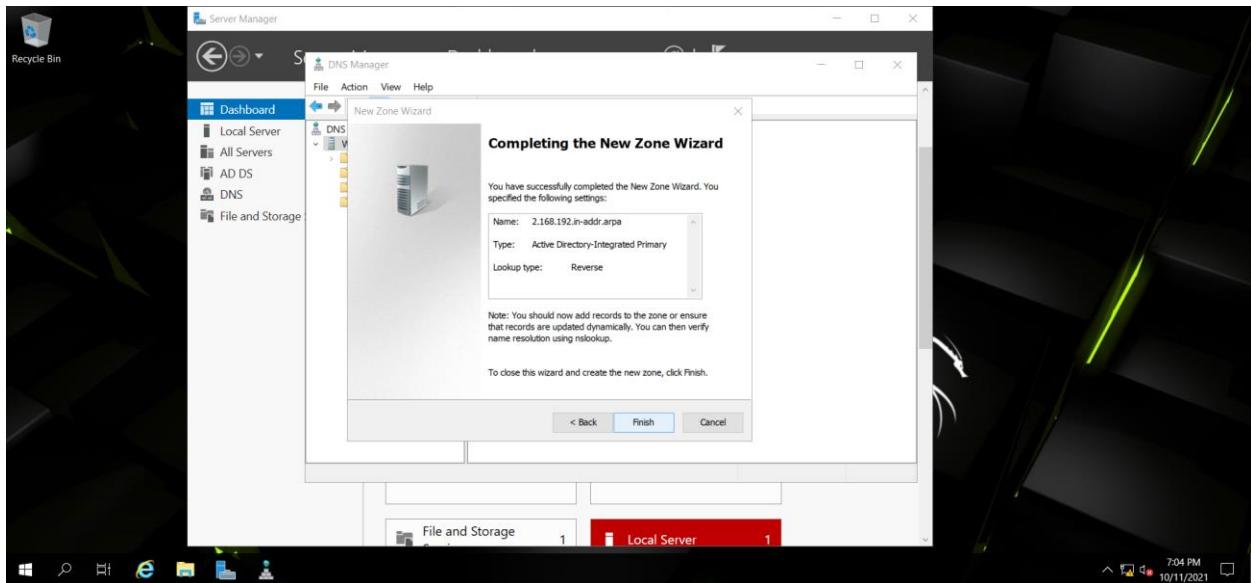
Hình 1. 22: Network ID



Hình 1. 23: Dynamic

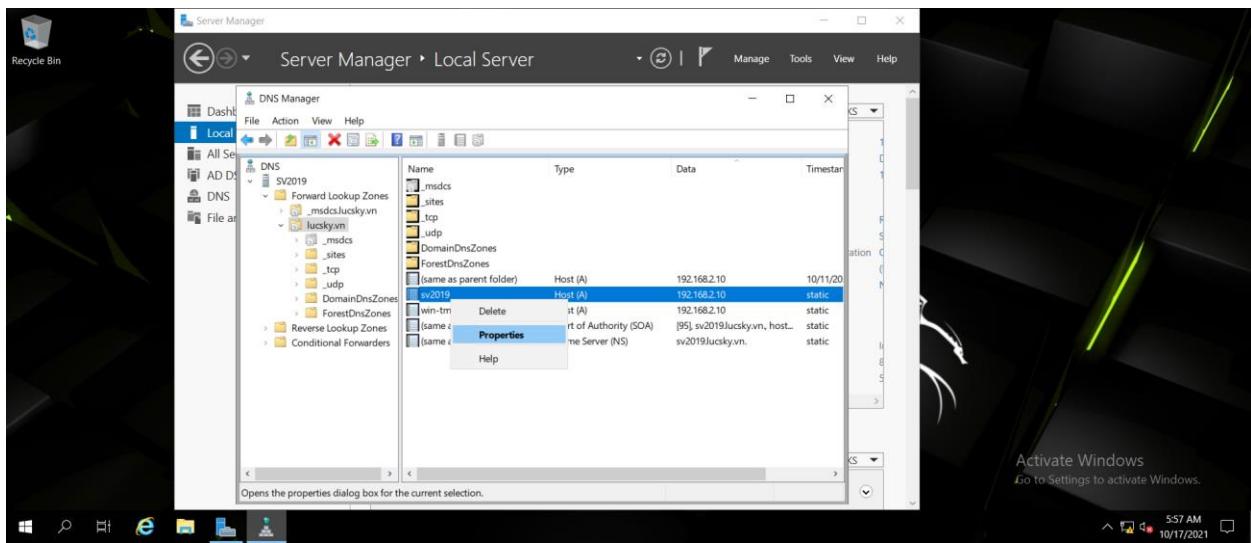
Update Kiểm tra lại thông tin đã chọn và chọn

finish

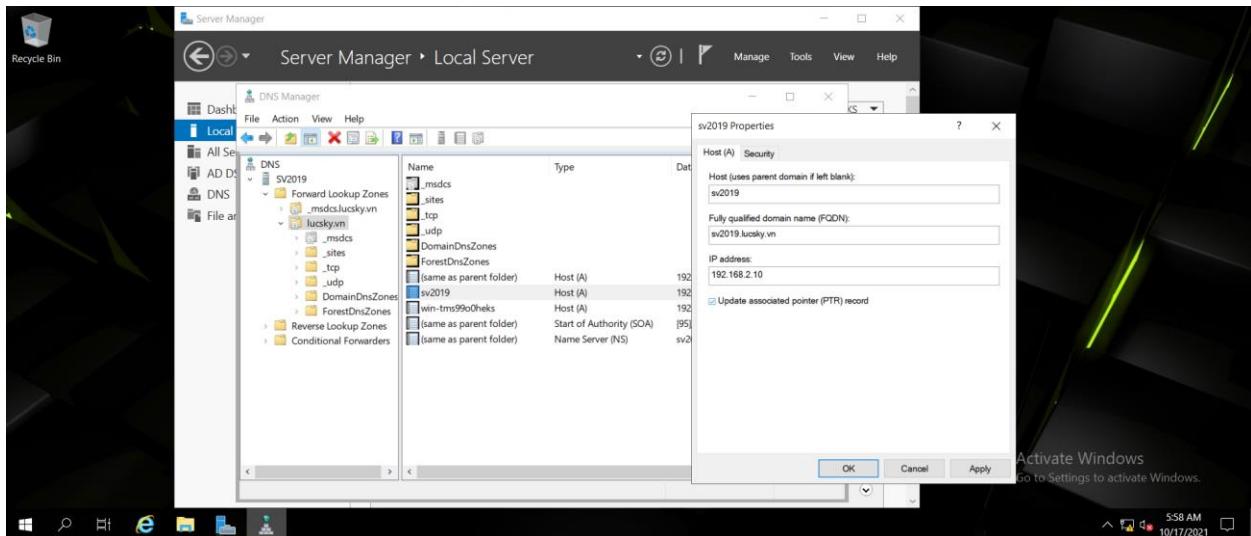


Hình 1. 24: Tạo new zone thành công

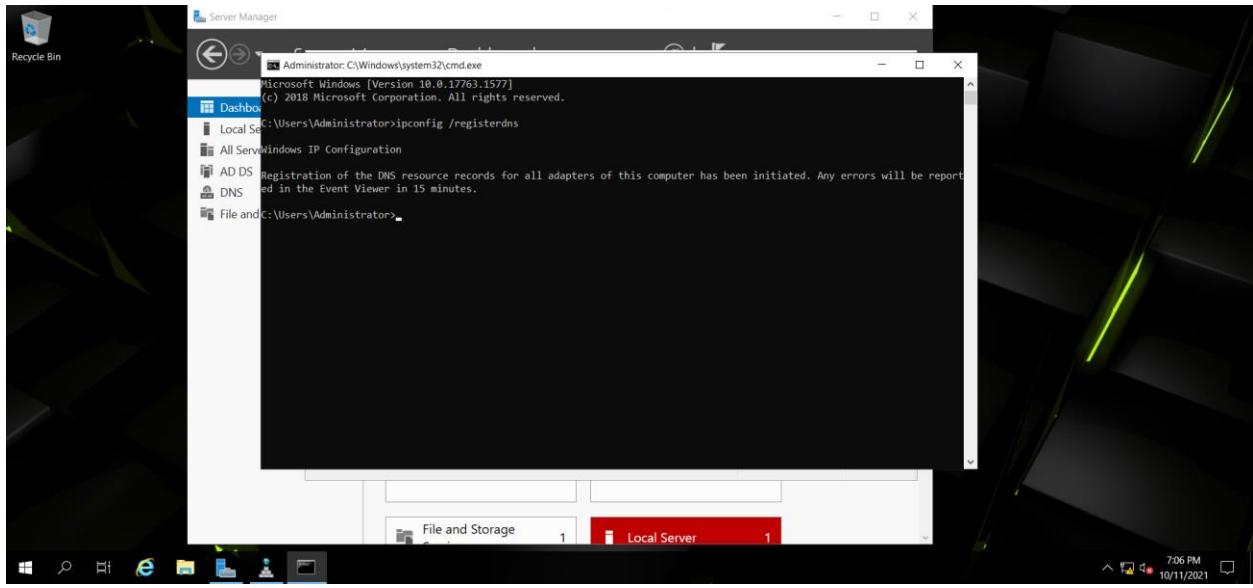
Dùng lệnh ipconfig /registerdns trên cmd để thực hiện cập nhật lại thiết lập DNS



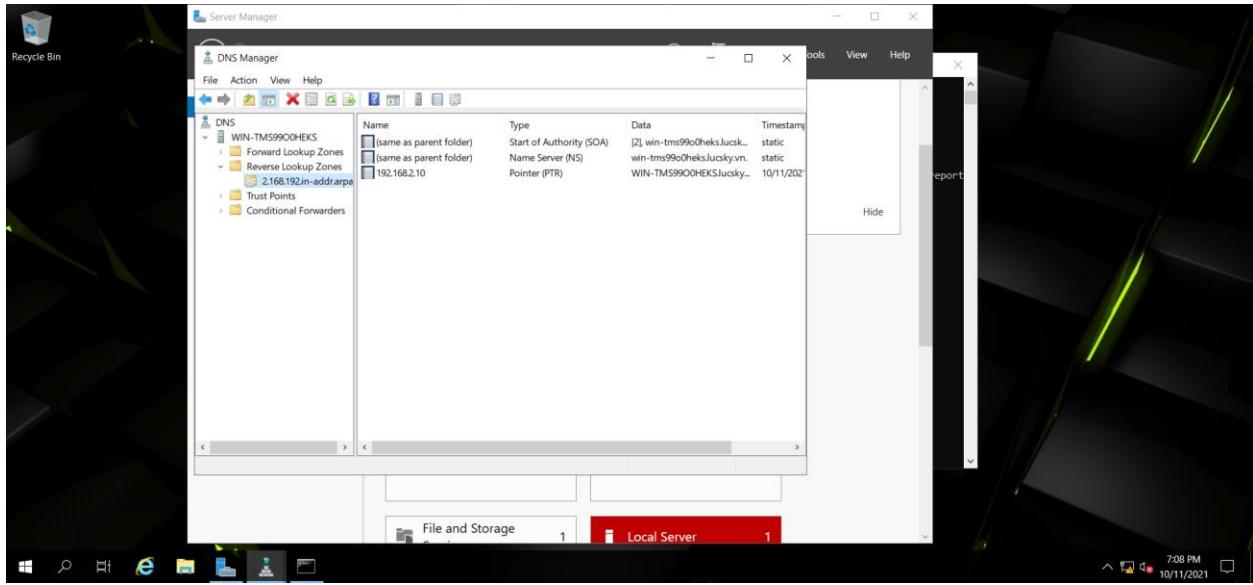
Vào properties của file sv2019



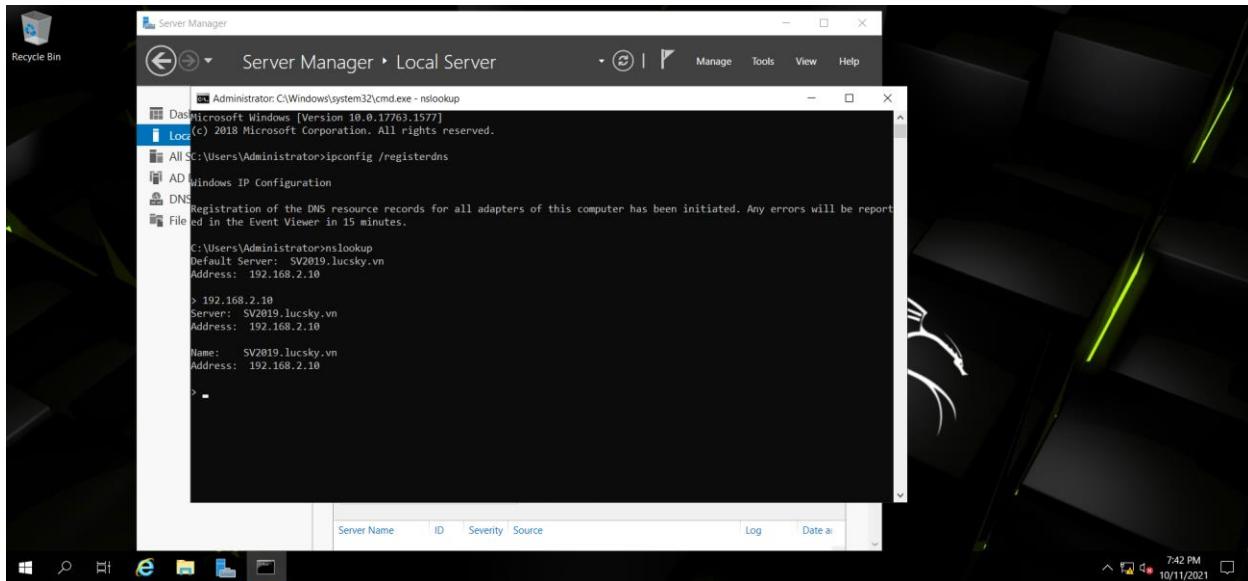
Nhấn chọn vào ô update....



Hình 1. 25: Cập nhật thiết lập DNS

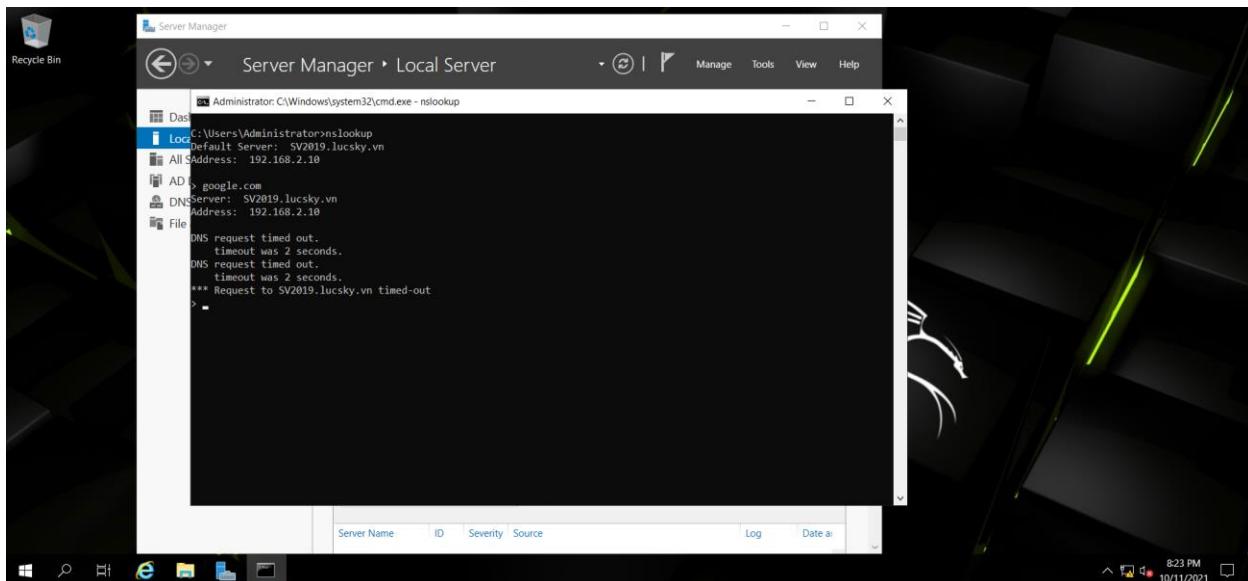


Hình 1. 26: Đã thiết lập Reverse Lookup Zone



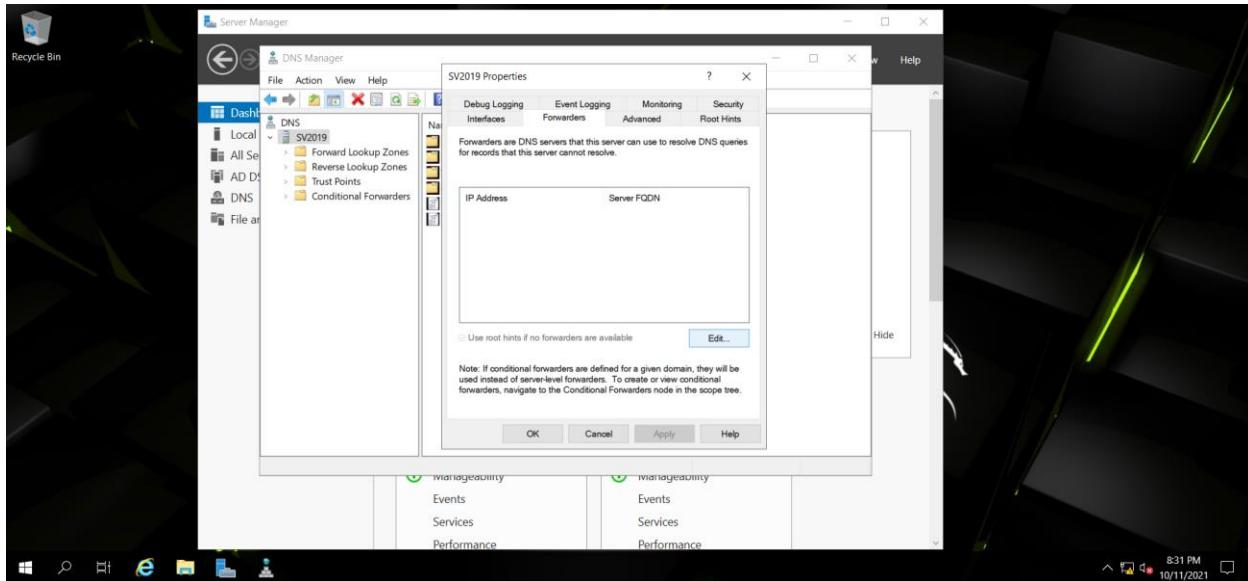
Hình 1. 27: Kết quả cài đặt

4. Cấu hình DNS Forwarder



Hình 1. 28: Thực hiện thử phân giải tên miền

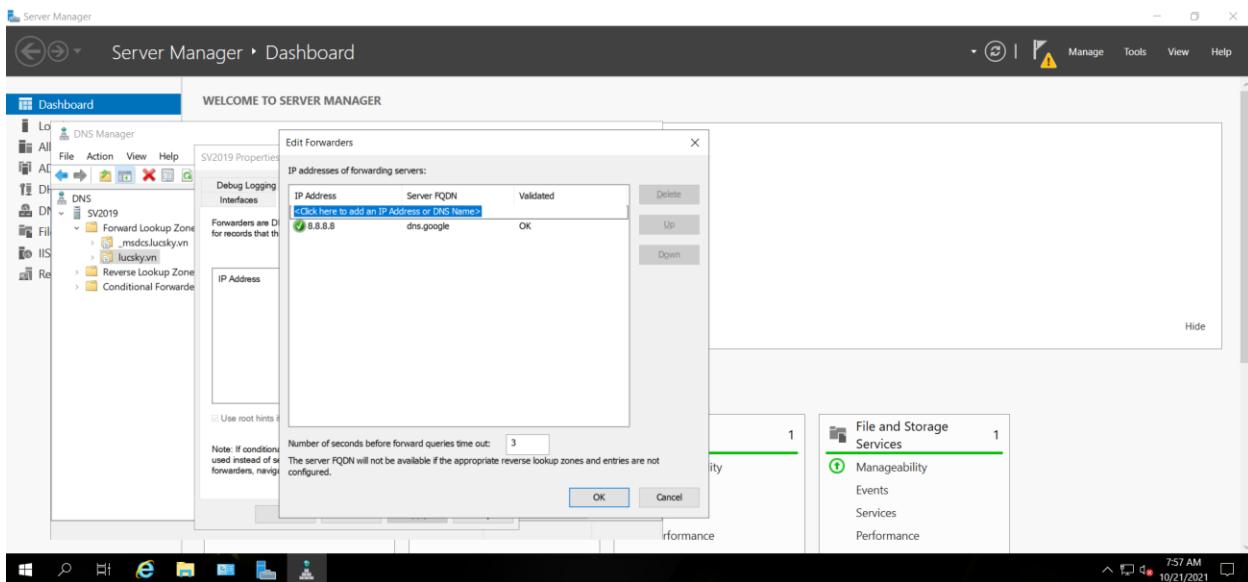
Mở Server Manager chọn Tools và chọn DNS sau đó chuột phải vào Domain Controller chọn properties



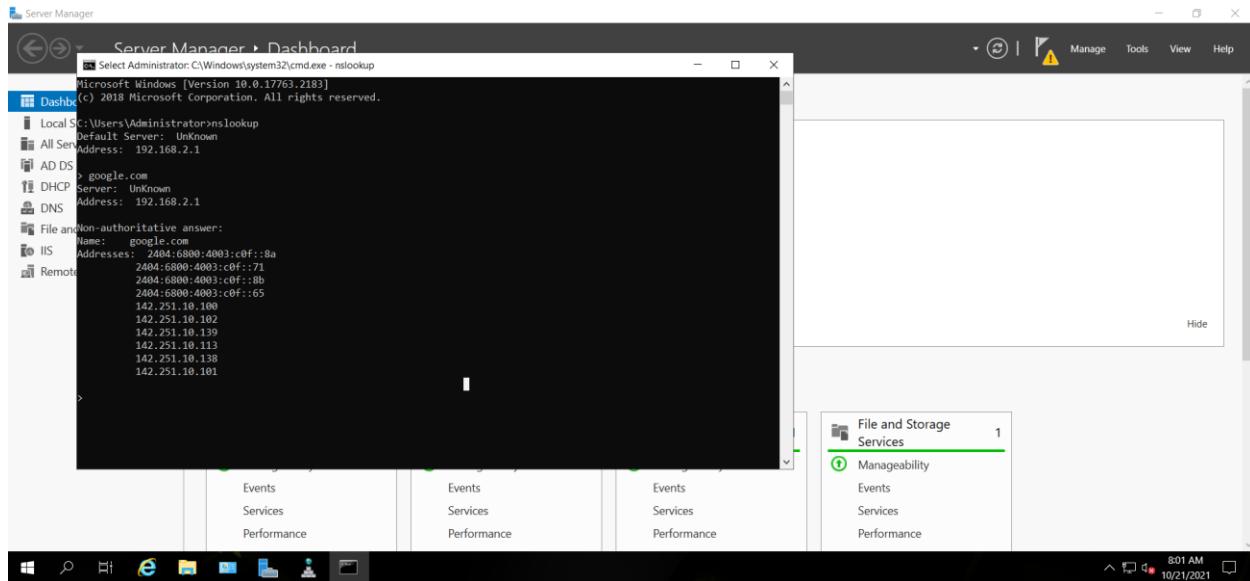
Hình 1. 29: DNS Forwarder

Cài xong sophos, cấu hình lại các địa chỉ ip, card mạng, đến khi có internet thì mới thêm được DNS trong trường hợp đã thay đổi ip như bài lab này

Thêm DNS của Google (8.8.8.8) sau đó chọn OK



Hình 1. 30: Forward DNS của Google



Hình 1. 31: Kiểm tra phân giải tên miền

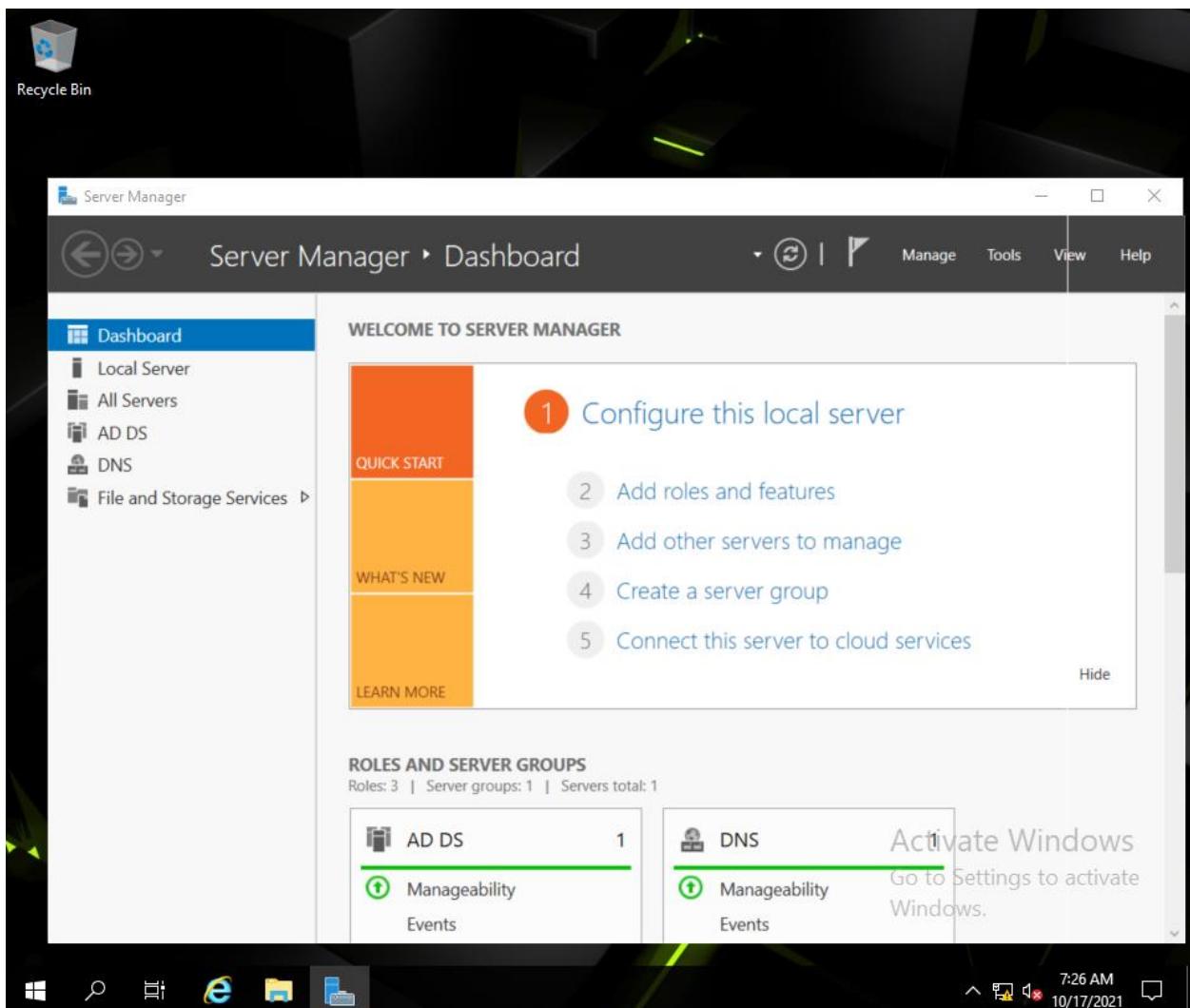
B. Cài đặt VPN Server

Thực hiện cài đặt VPN Server trên máy đã tiến hành cài Domain Controller

Các bước thực hiện:

B.1 Cài đặt dịch vụ Remote Access

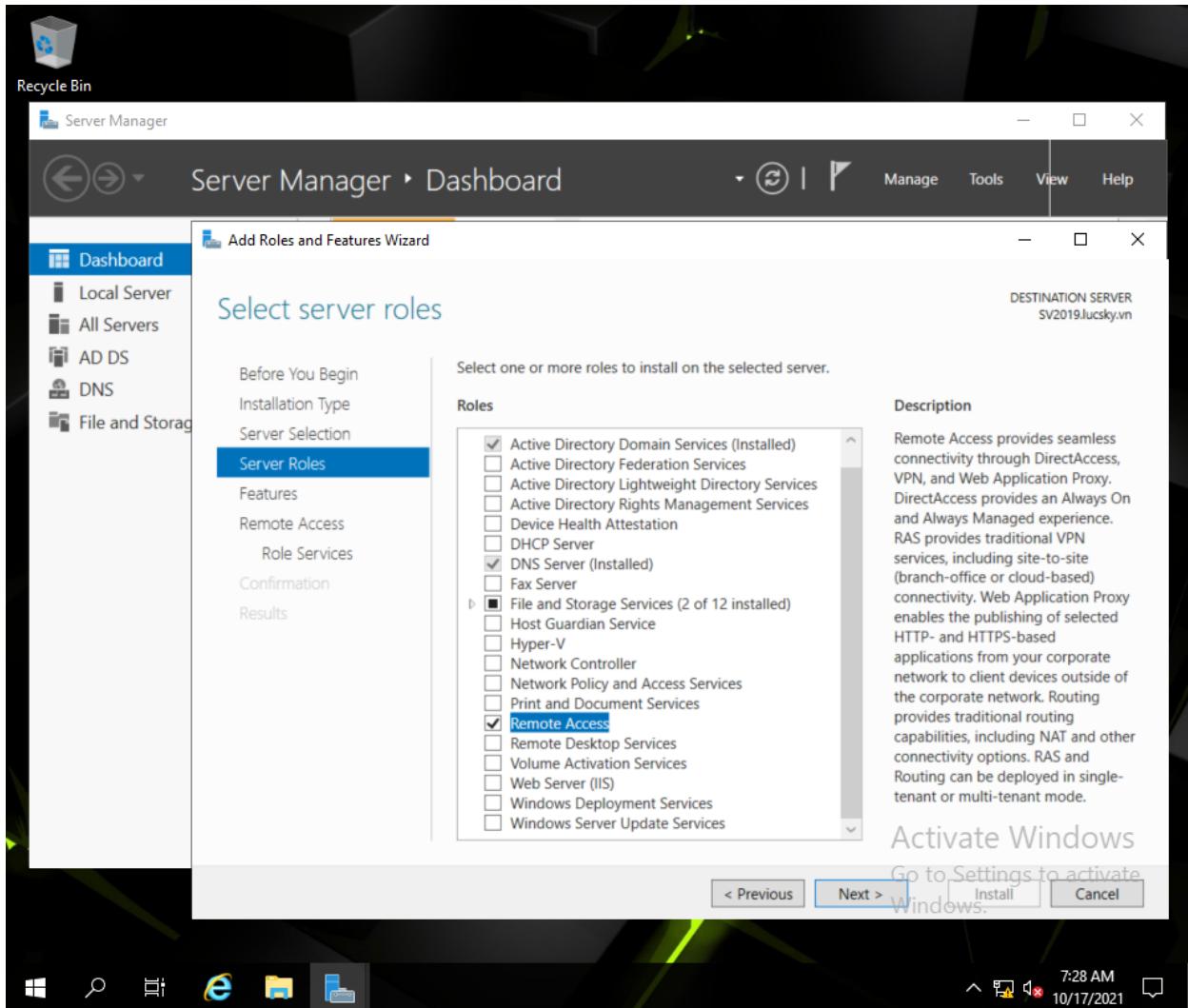
Vào Server Manager và chọn Add roles and features



Hình 1. 32: Màn hình Server Manager

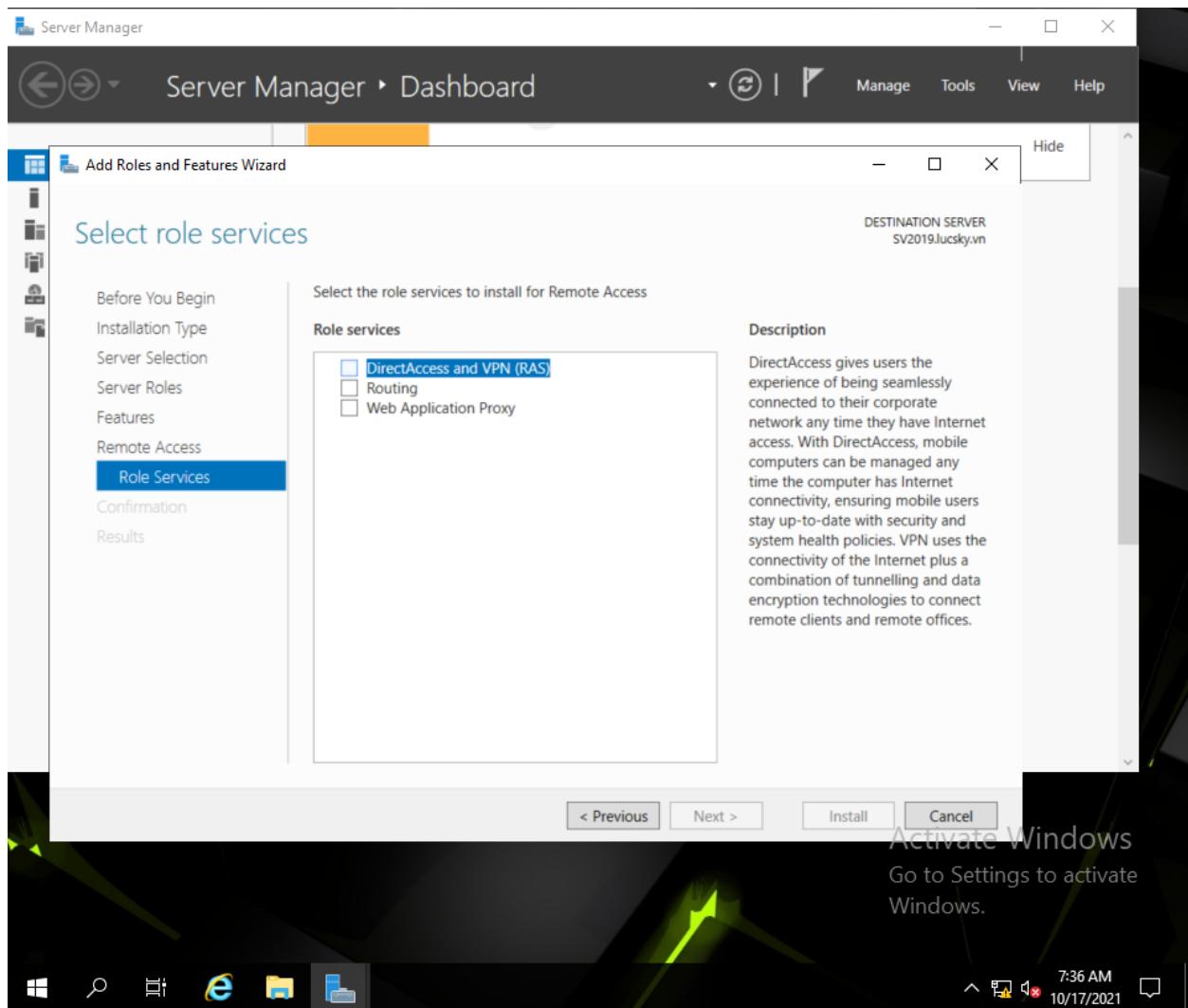
Thực hiện next 3 lần

Tại Server Roles chọn vào Remote Access và tiếp tục next 3 lần



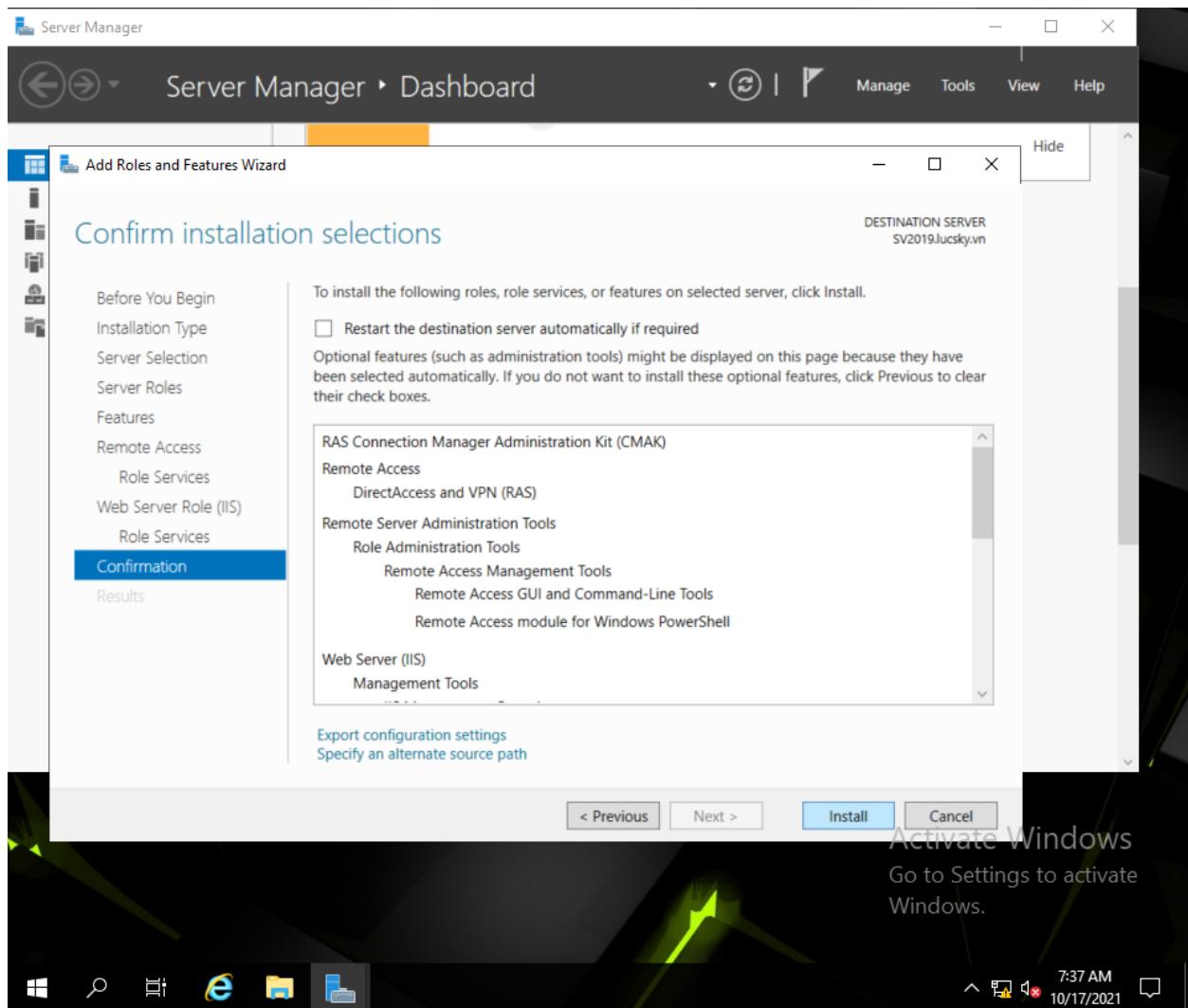
Hình 1. 33: Chọn Remote Access

Tại Role Services chọn DirectAccess and VPN (RAS) và next 3 lần

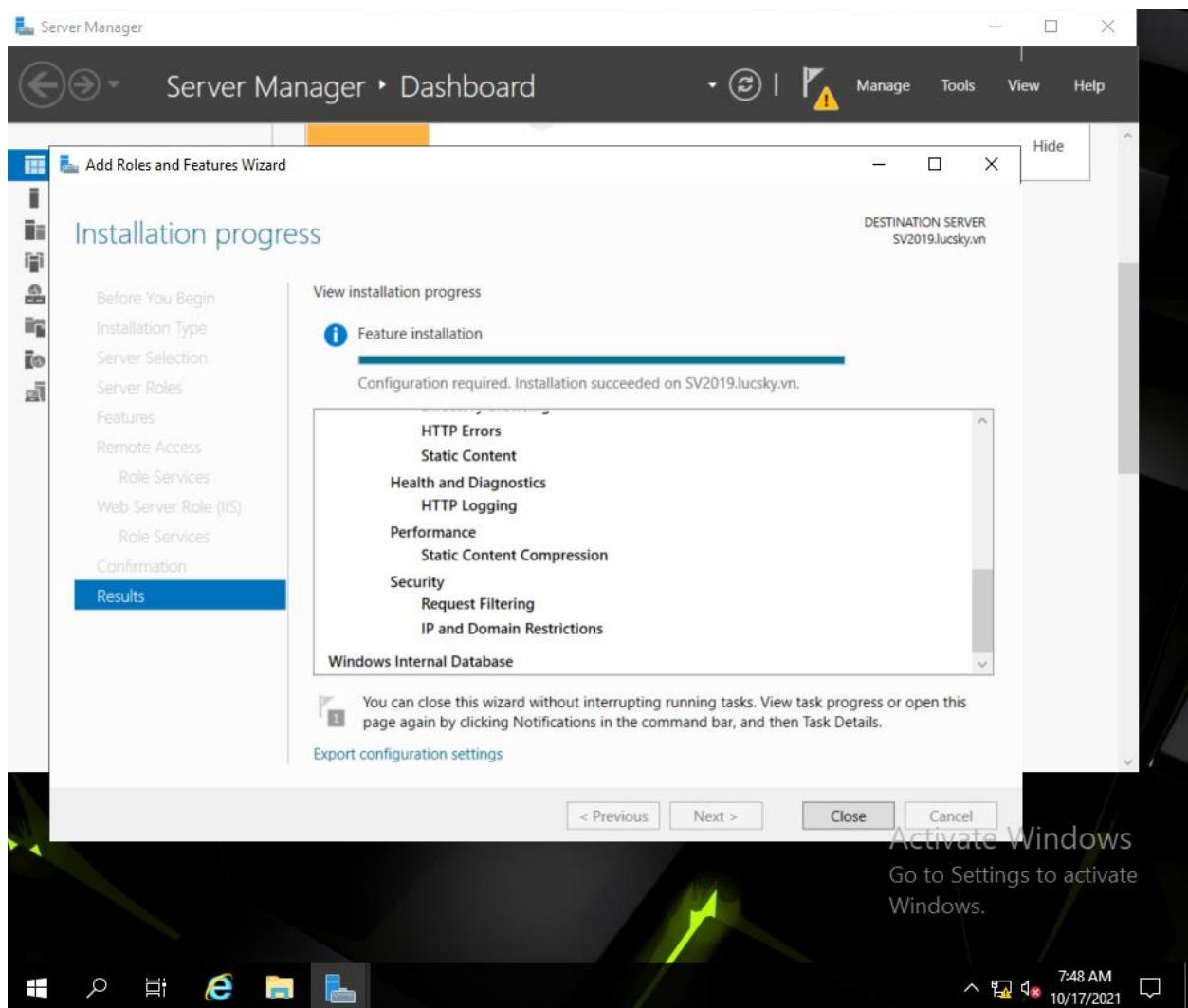


Hình 1. 34: DirectAccess and VPN (RAS)

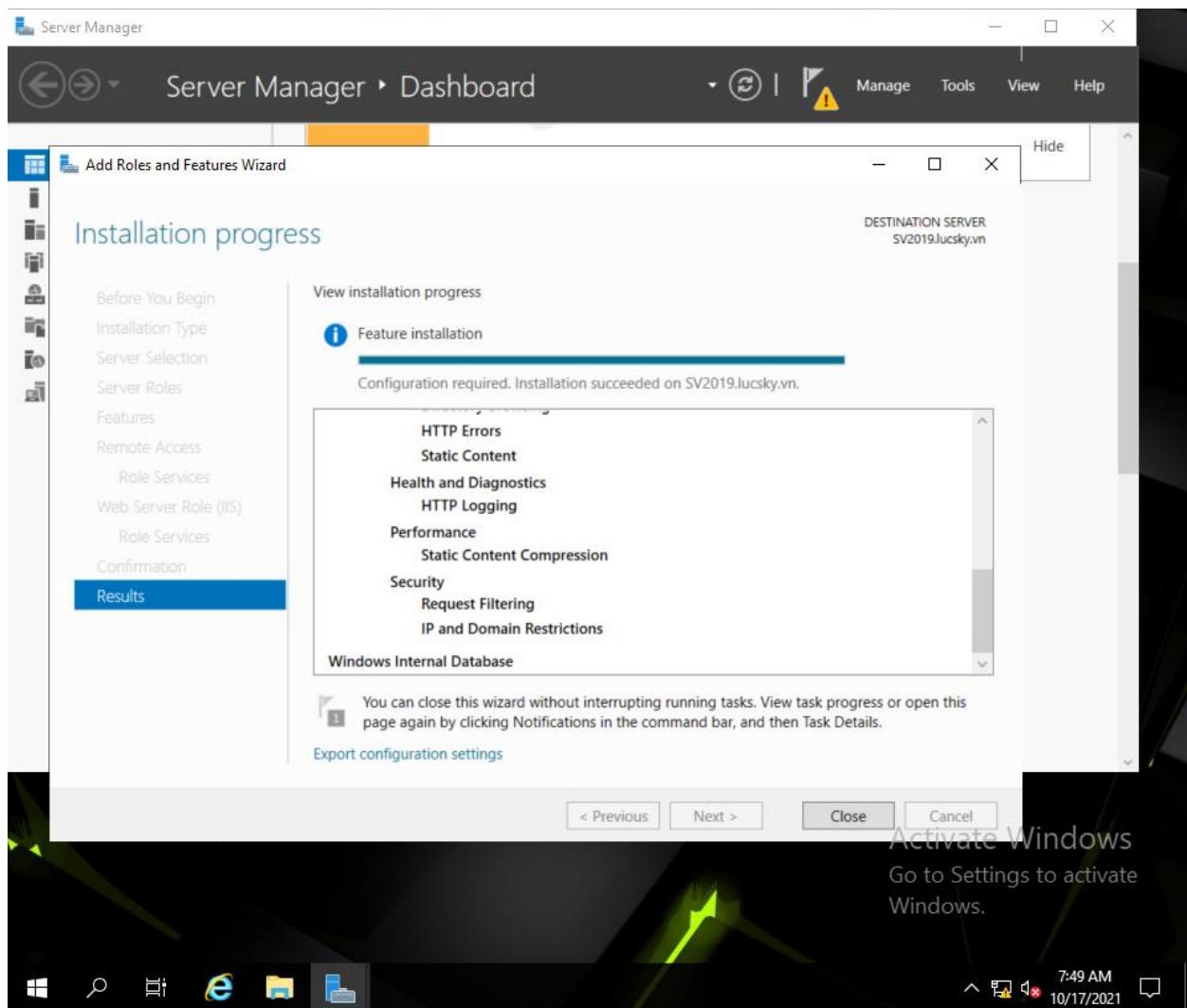
Kiểm tra lại các lựa chọn và nhấn Install



Hình 1. 35: Xác nhận cài đặt



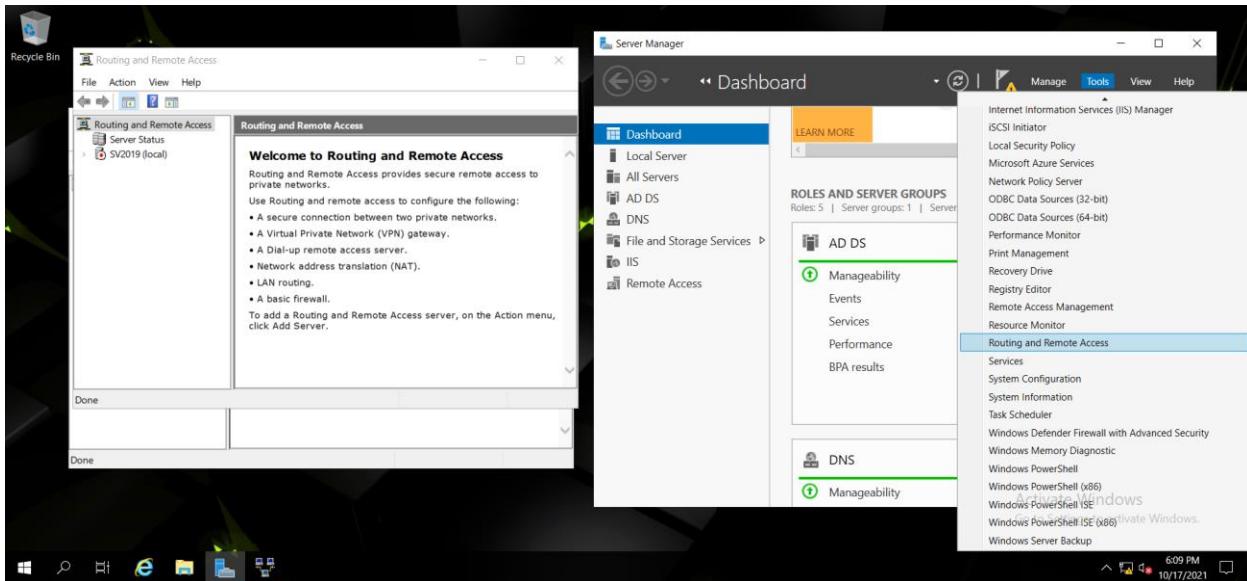
Hình 1. 36: Quá trình cài đặt



Hình 1. 37: Cài đặt thành công

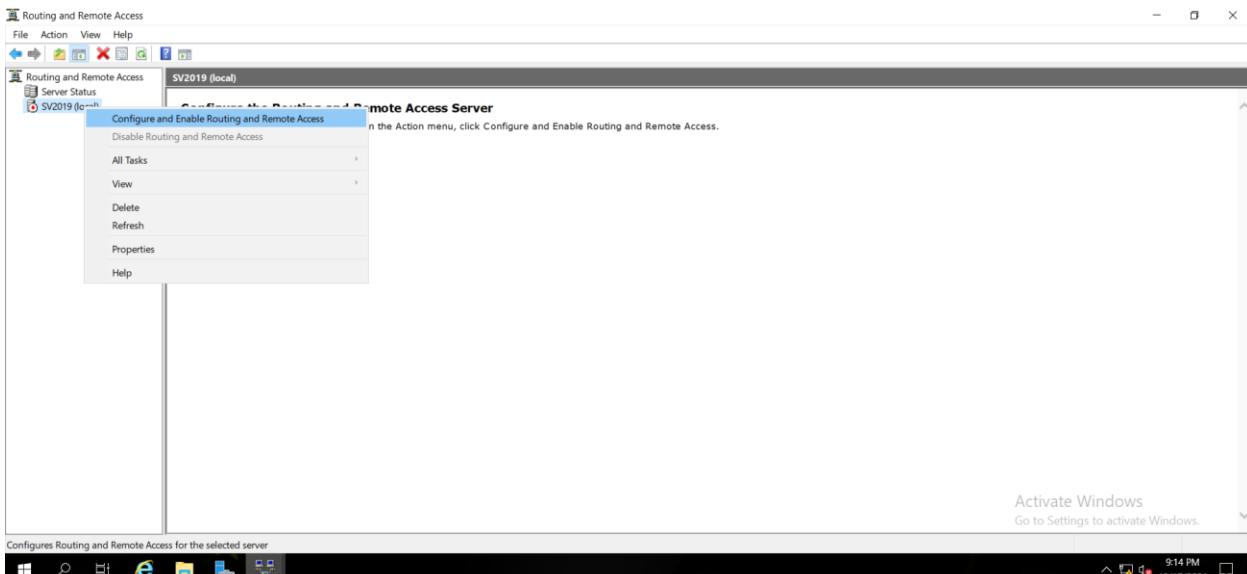
B.2 Cài đặt VPN Server

Vào Server Manager chọn Tools sau đó chọn Routing and Remote Access



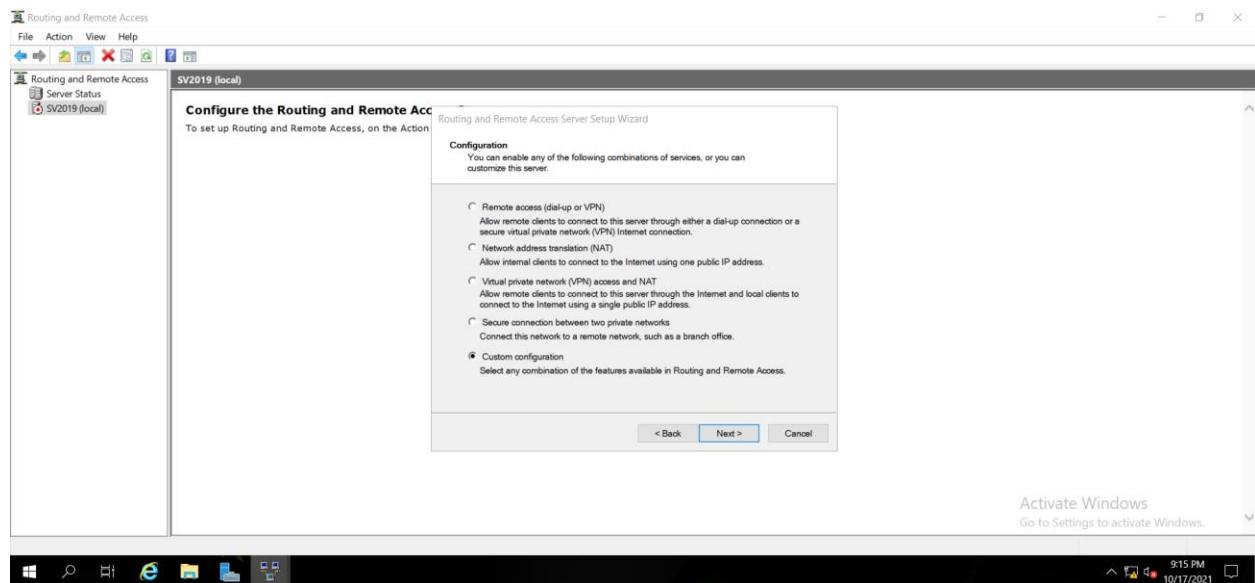
Hình 1. 38: Routing and Remote Access

Chuột phải vào SV2019 chọn Configure and Enable Routing and Remote Access rồi chọn Next



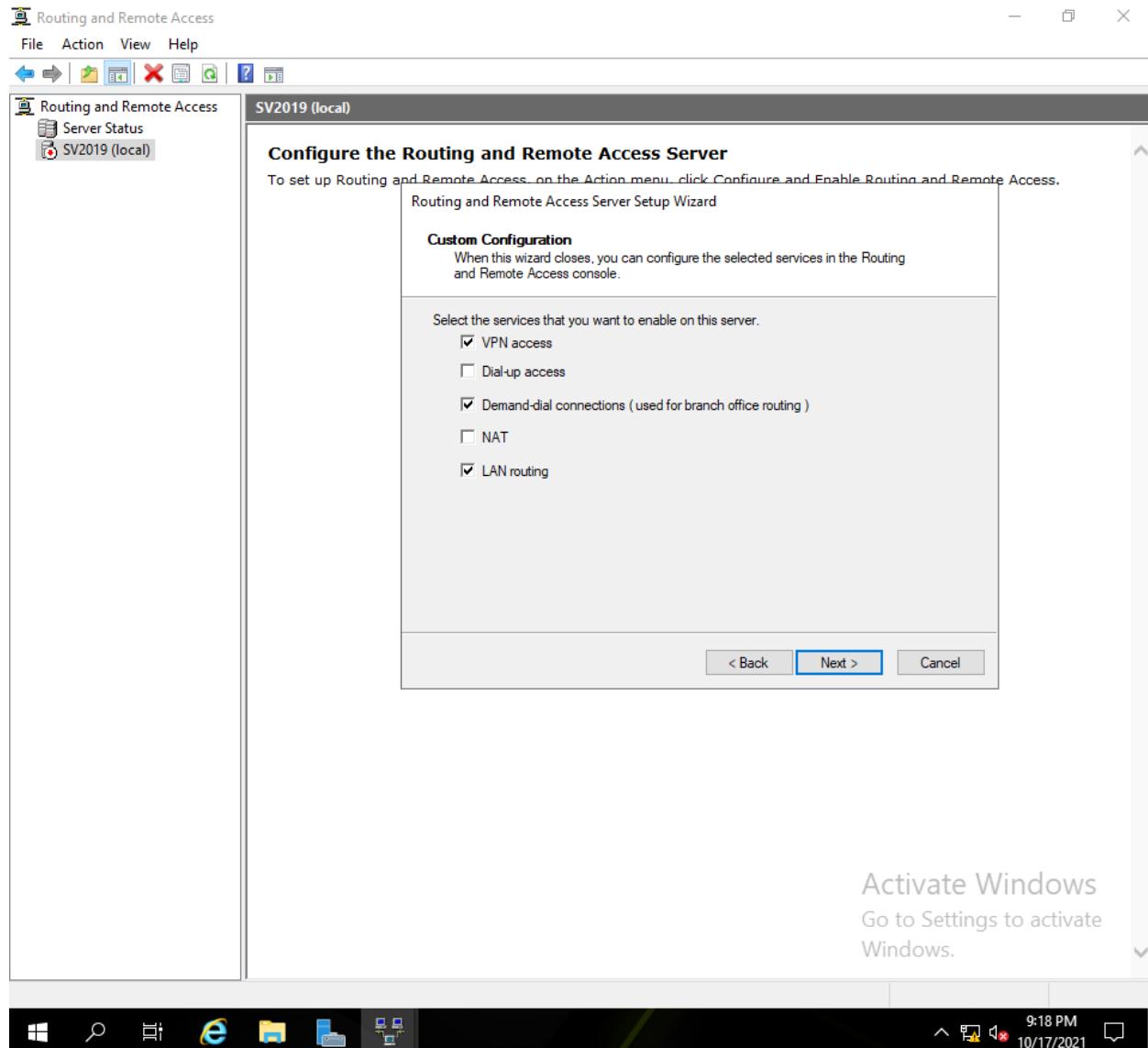
Hình 1. 39: Cấu hình Routing and Remote Access

Chọn Custom configuration rồi chọn Next

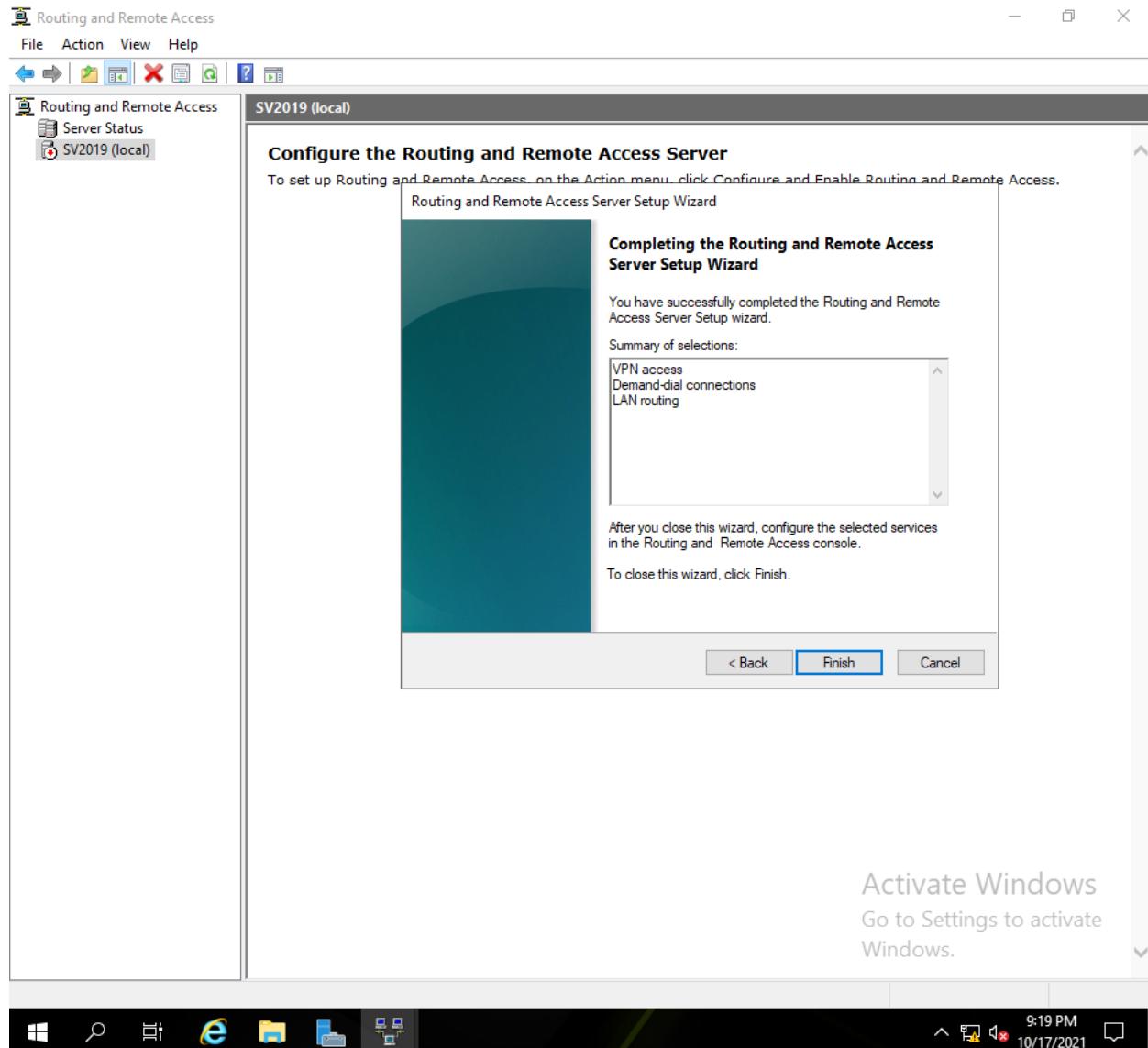


Hình 1. 40: Dịch vụ cấu hình

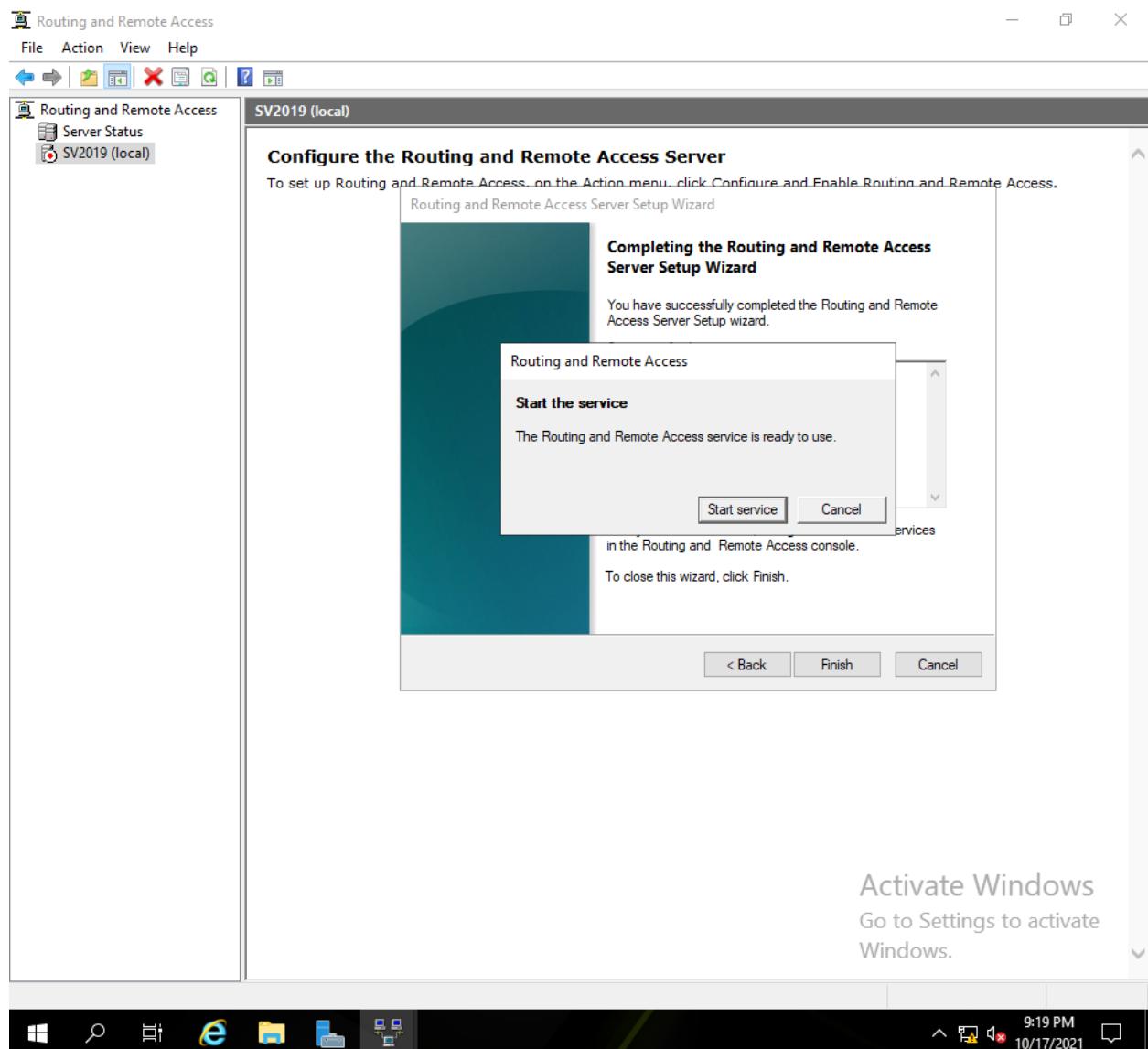
Chọn VPN access, Demand-dial connections, LAN Routing rồi chọn Next và Finish



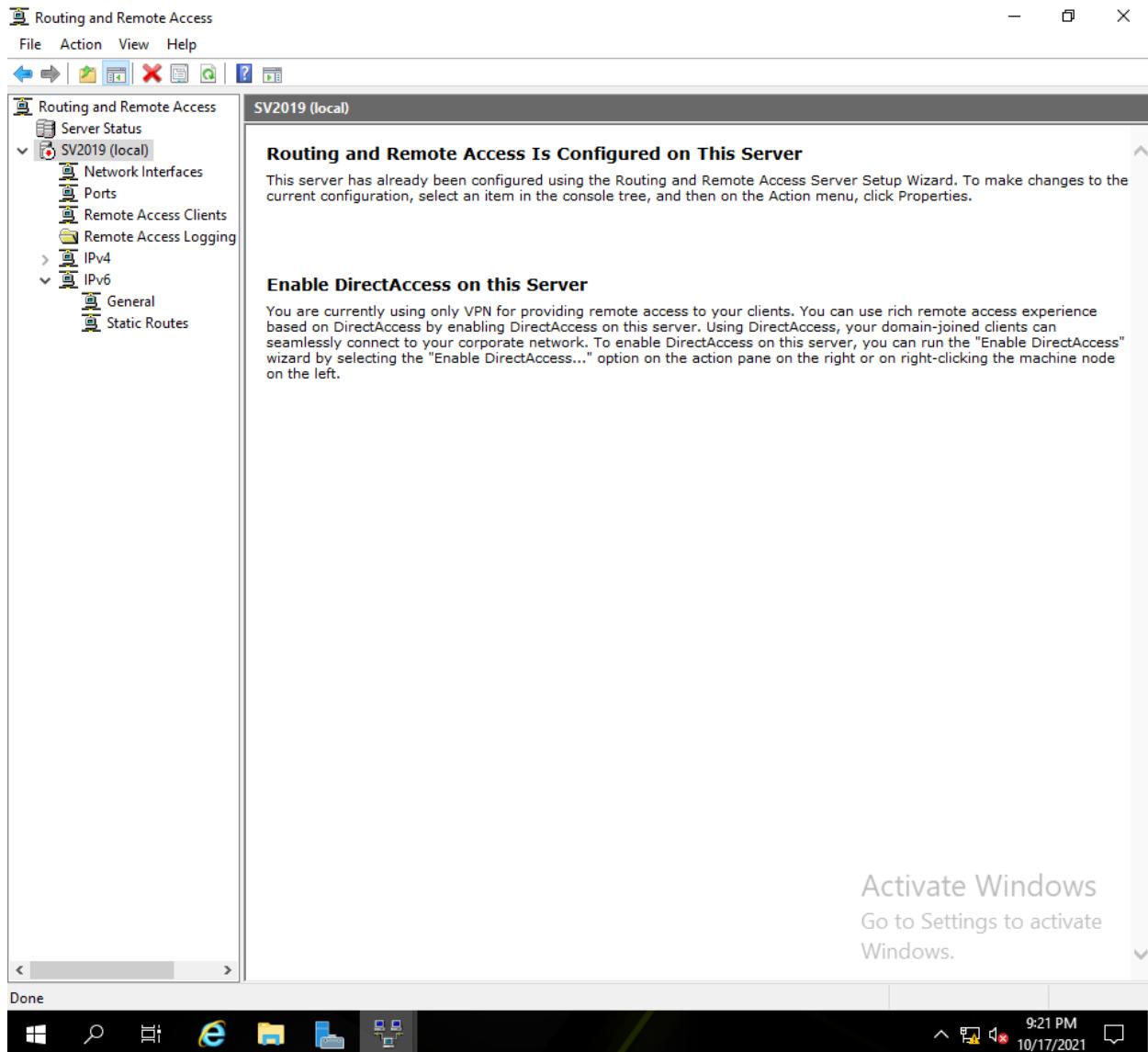
Hình 1. 41: Dịch vụ được chọn



Hình 1. 42: Kiểm tra lại dịch vụ đã chọn
Chọn Start service để chạy dịch vụ đã chọn

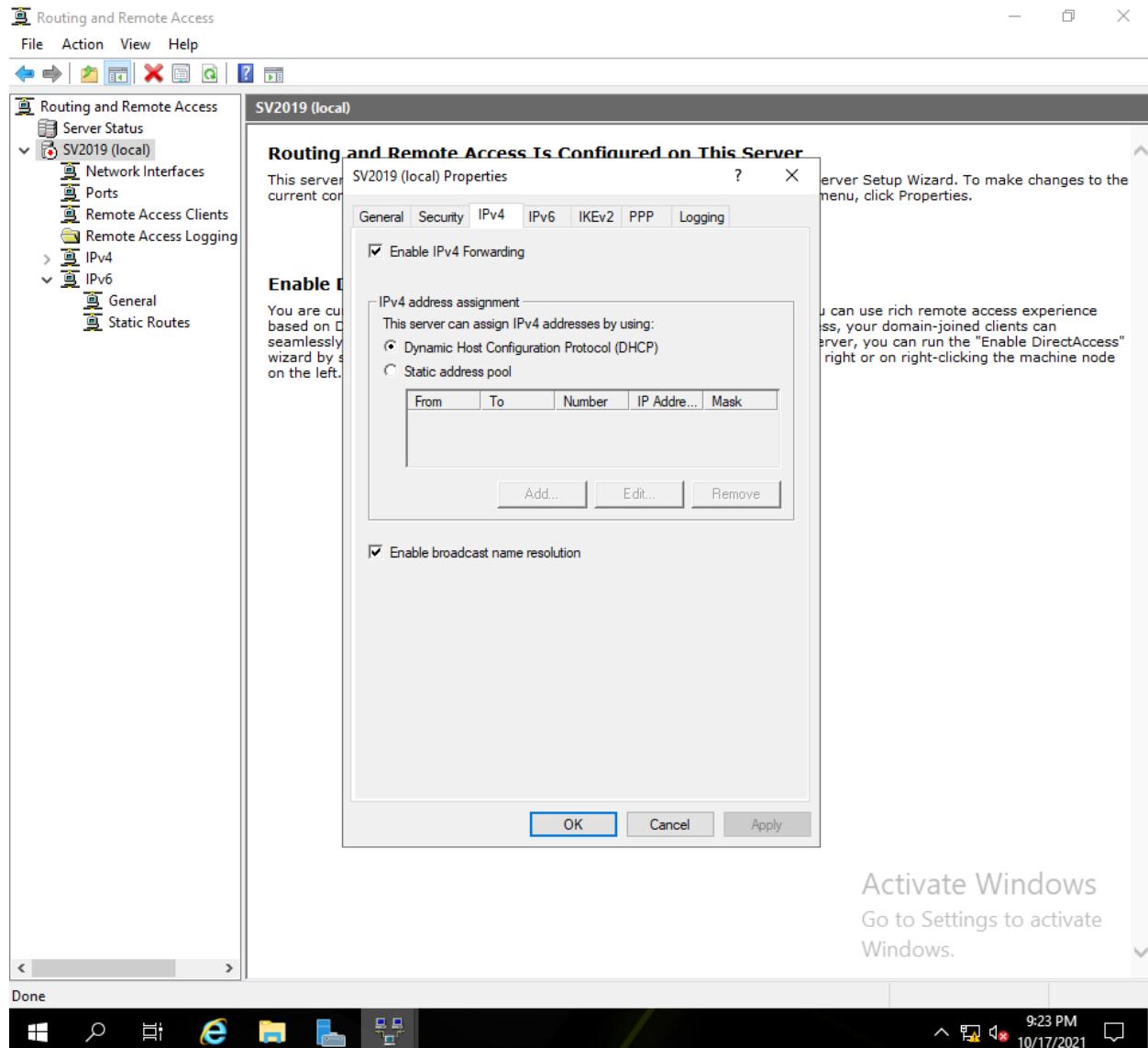


Hình 1.43: Tiến hành chạy dịch vụ



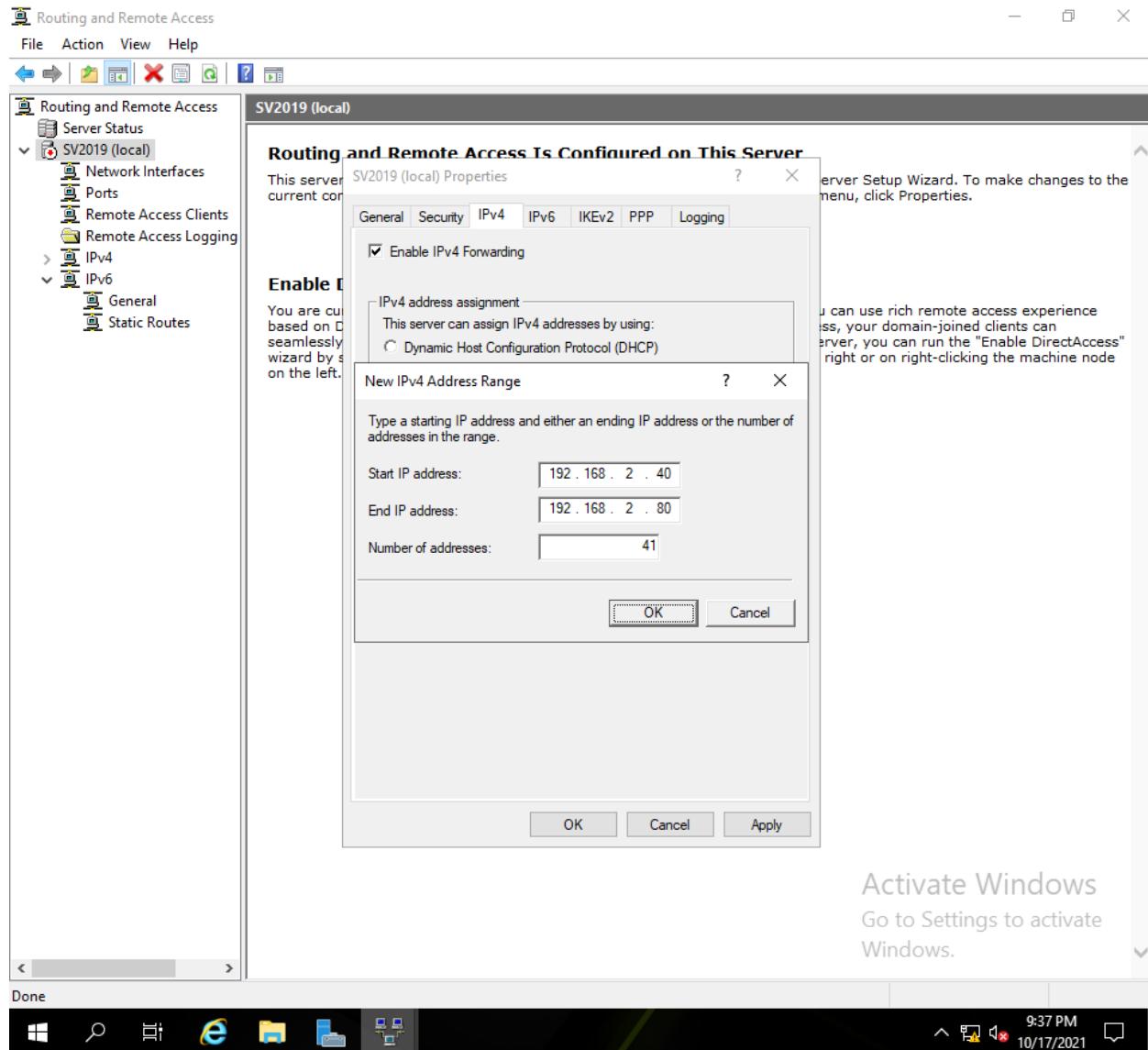
Hình 1. 44: Dịch vụ chạy thành công

Chuột phải vào Server chọn Properties và chọn tab IPv4



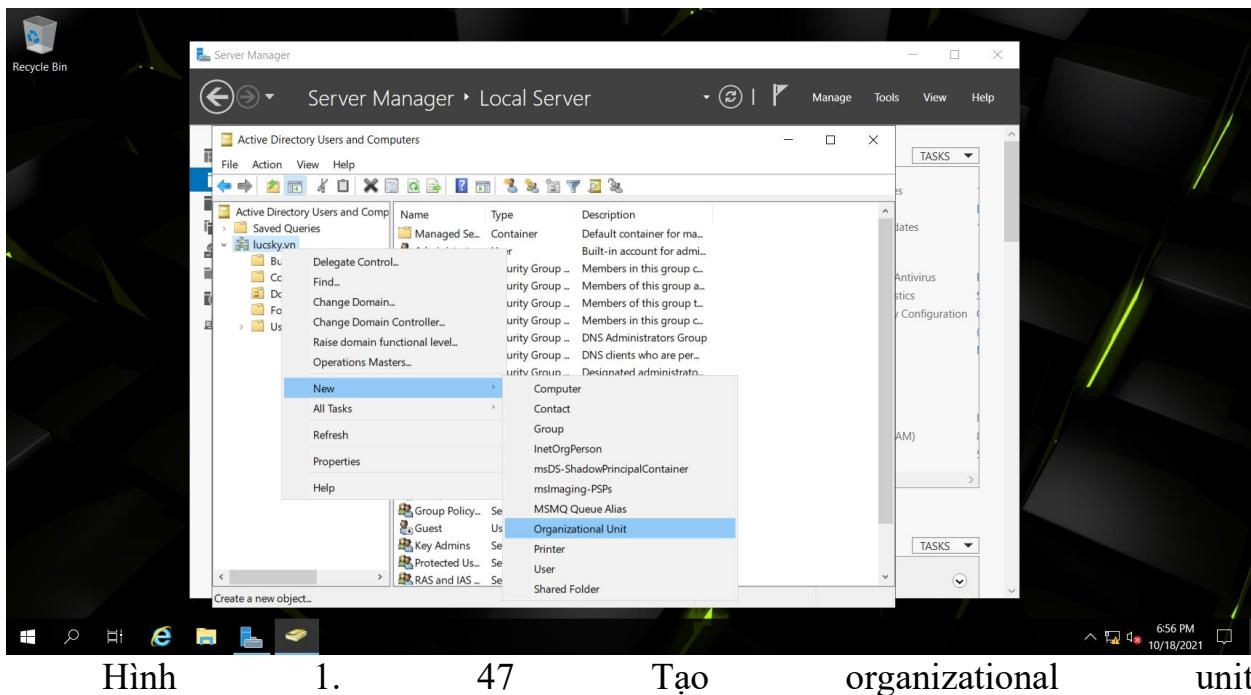
Hình 1. 45: Tiến hành cấp phát IPv4

Chọn static address pool và chỉ định dãy IP muốn cấp phát sau đó chọn OK

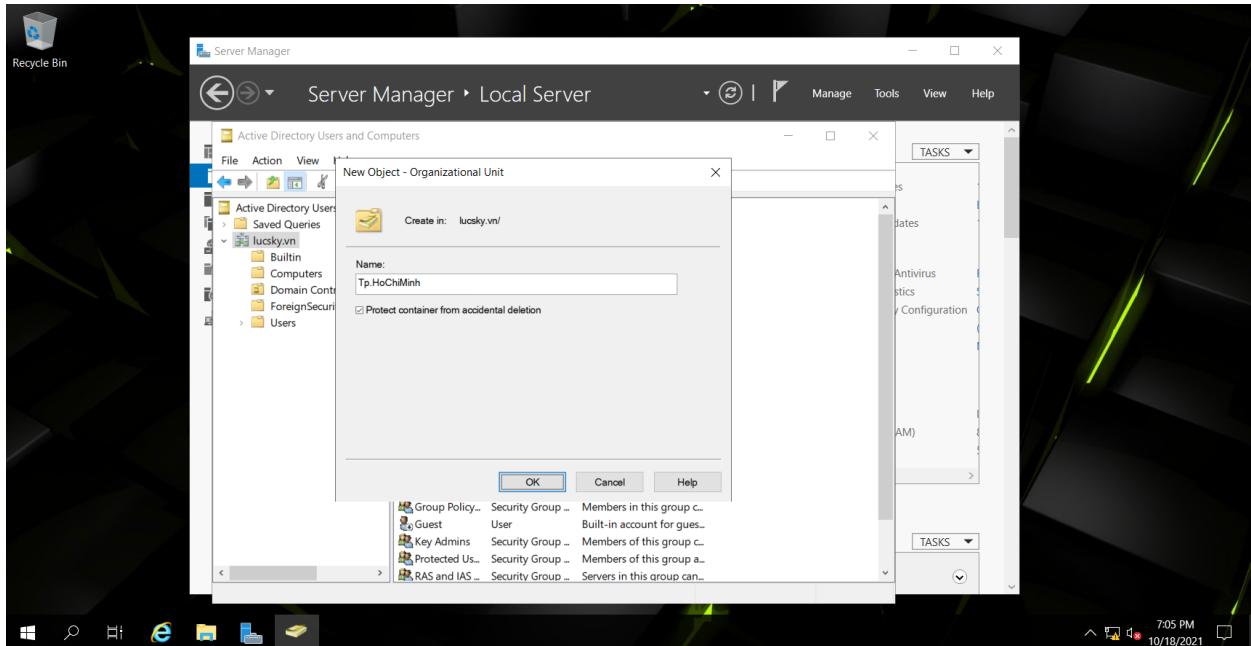


Hình 1. 46: Dãy IP cấp phát tĩnh

A.3 Cấp quyền Network Access Permission cho User

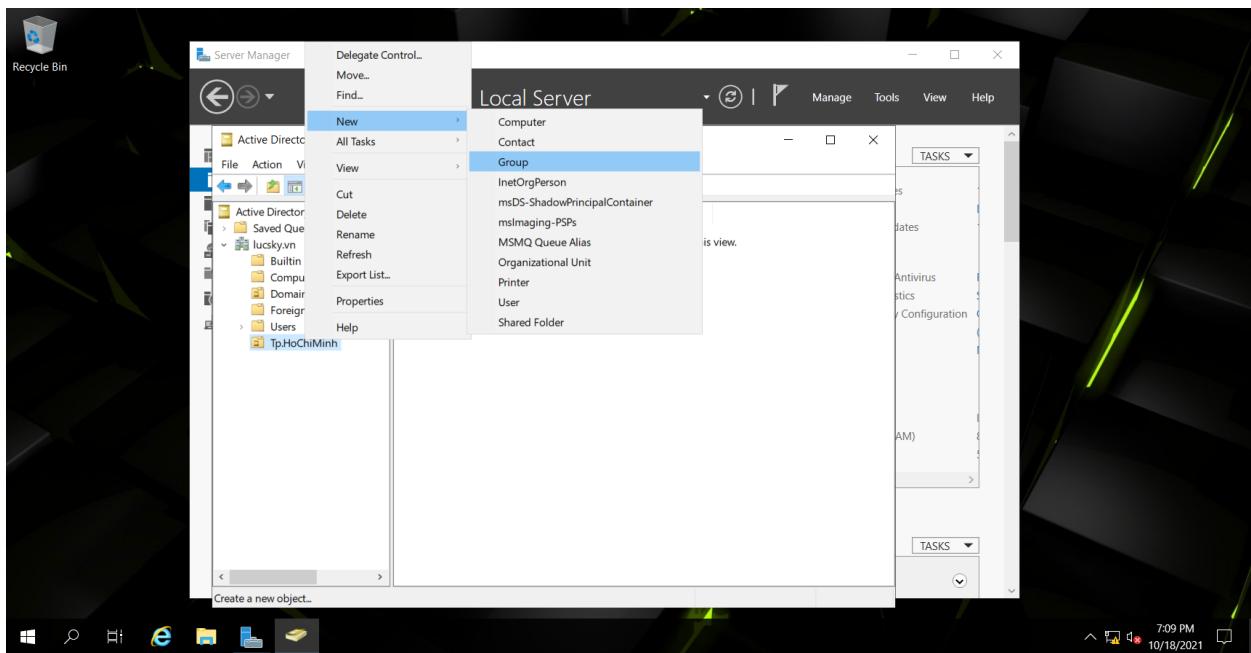


Hình 1.47 Tạo organizational unit

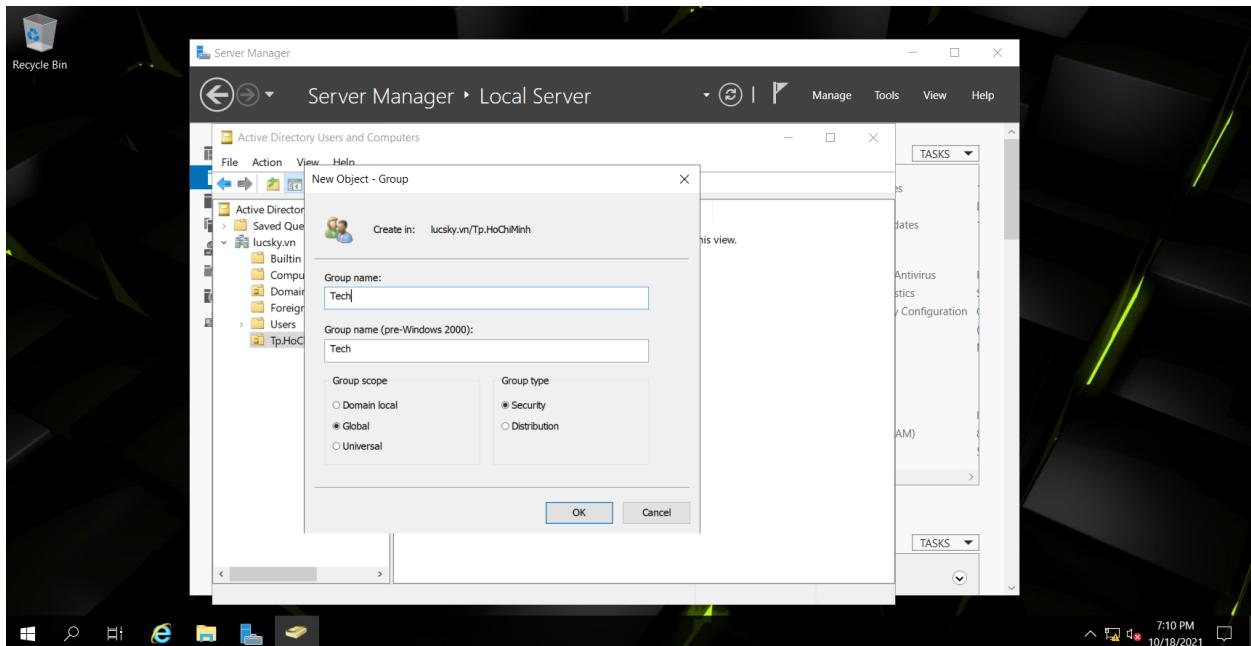


Hình 1.48 Đặt tên cho OU và click OK

Click chuột phải vào OU vừa tạo -> New -> Group



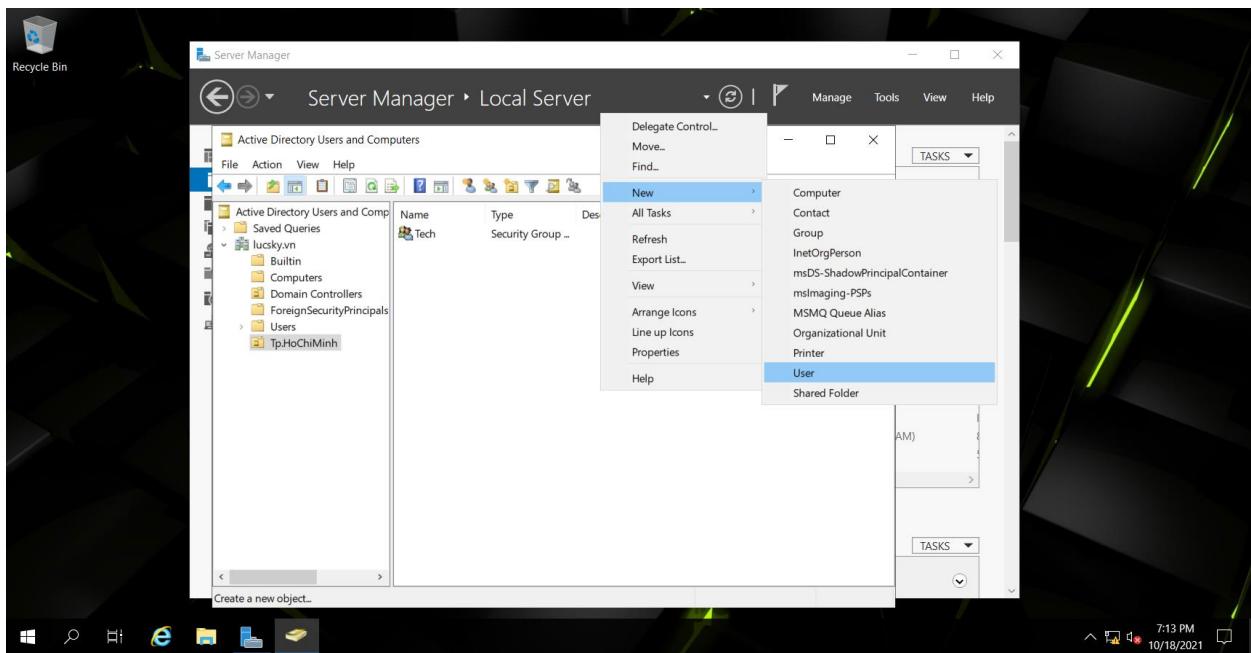
Hình 1.49 Tạo group



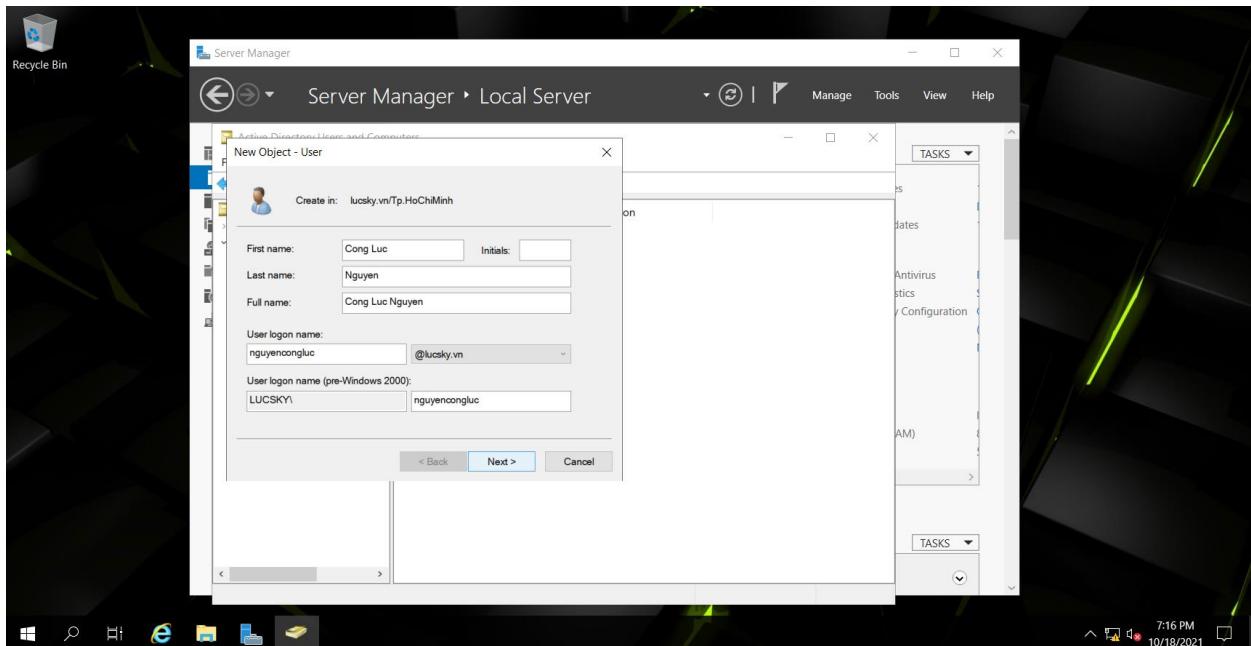
Hình 1.50 Đặt tên group

Tạo user và thêm user vào group

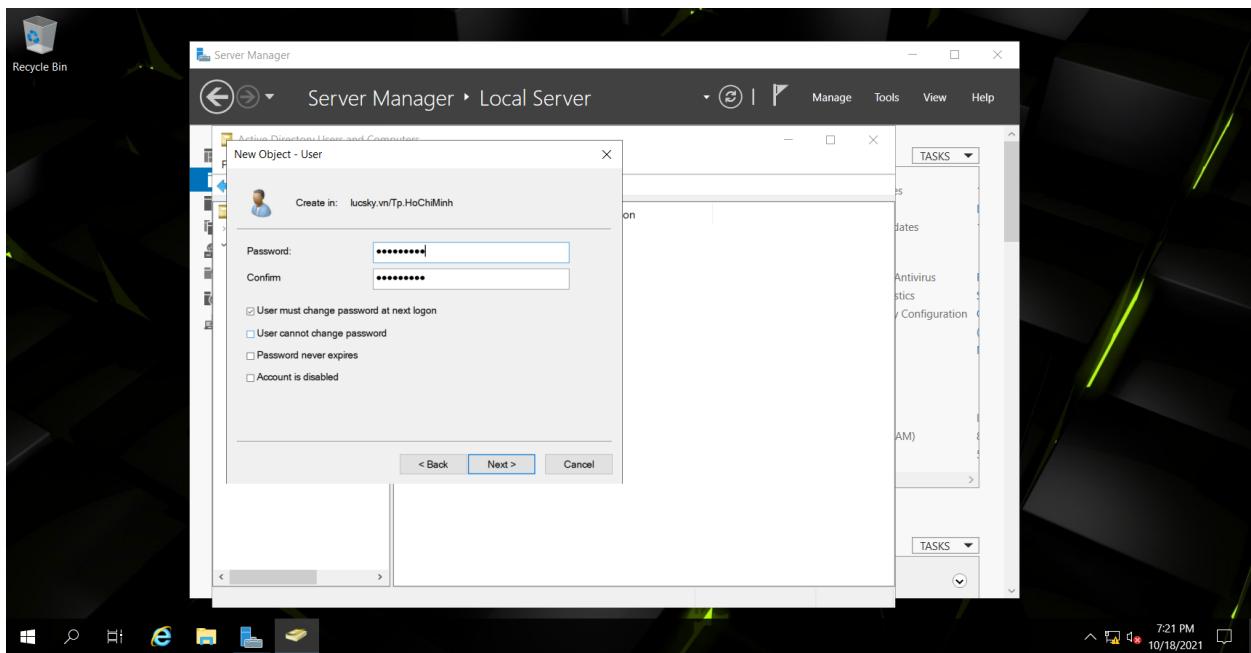
Chuột phải vào màn hình trắng bên phải chọn New -> User



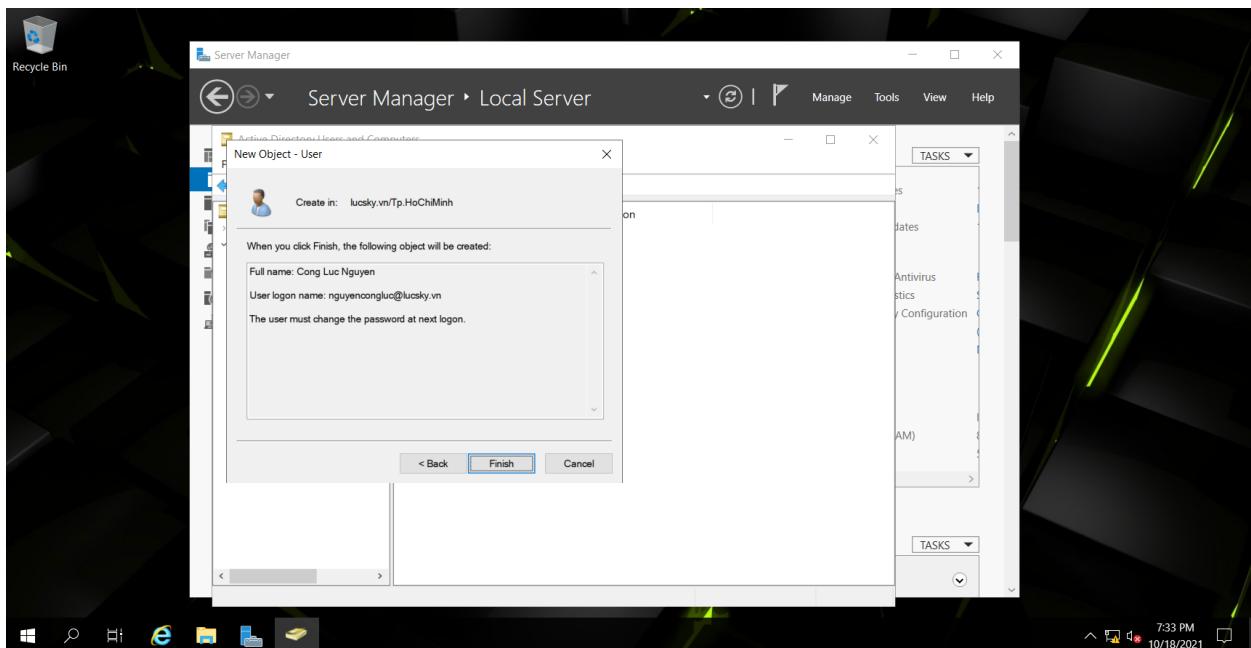
Hình 1.51 Tạo user



Hình 1.52 Nhập thông tin user

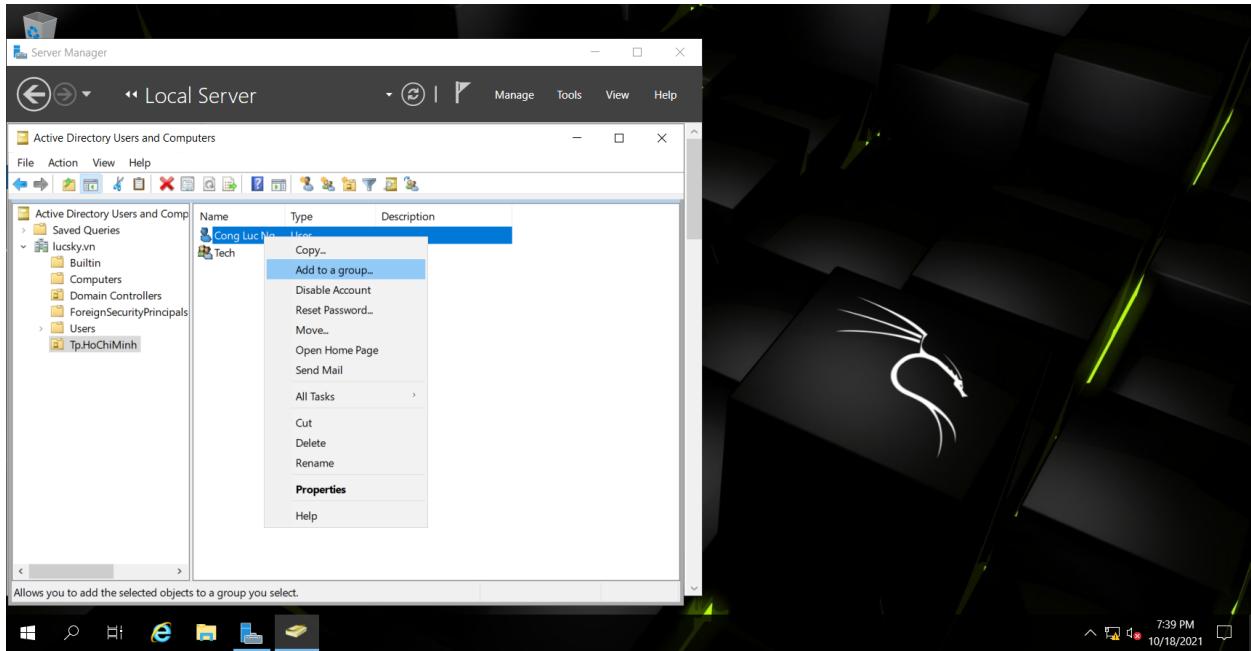


Hình 1.53 Đặt mật khẩu cho user



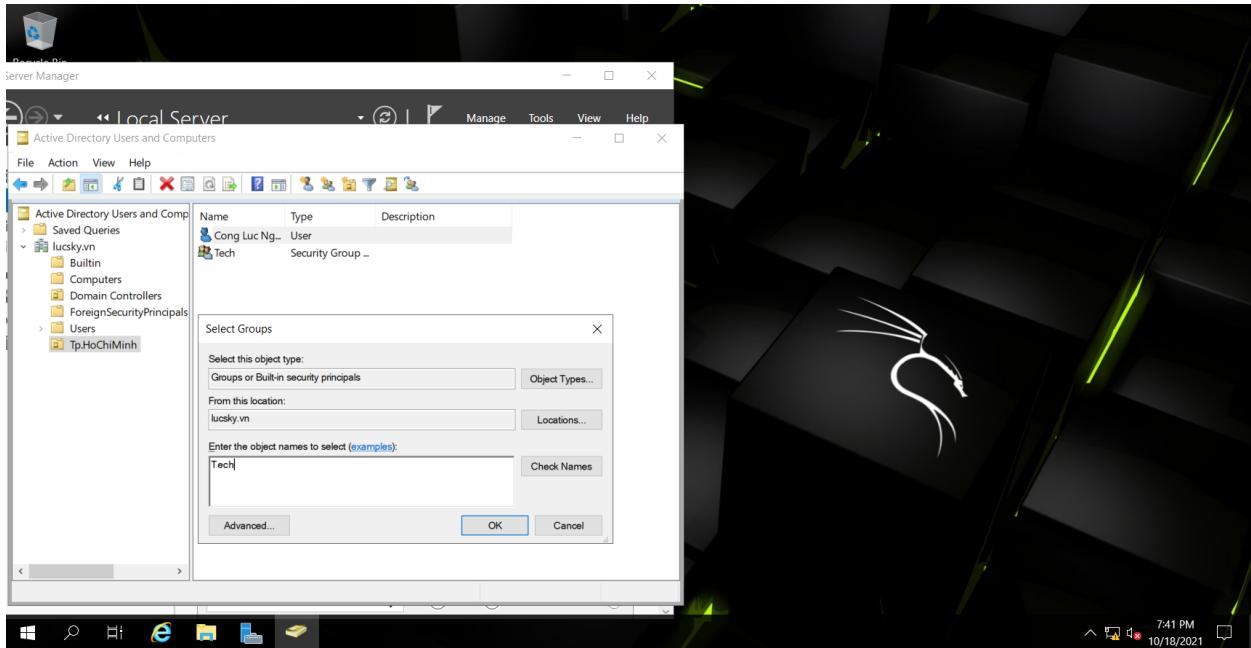
Hình 1.54 Nhấn finish

Thêm user vào group ta làm như sau:



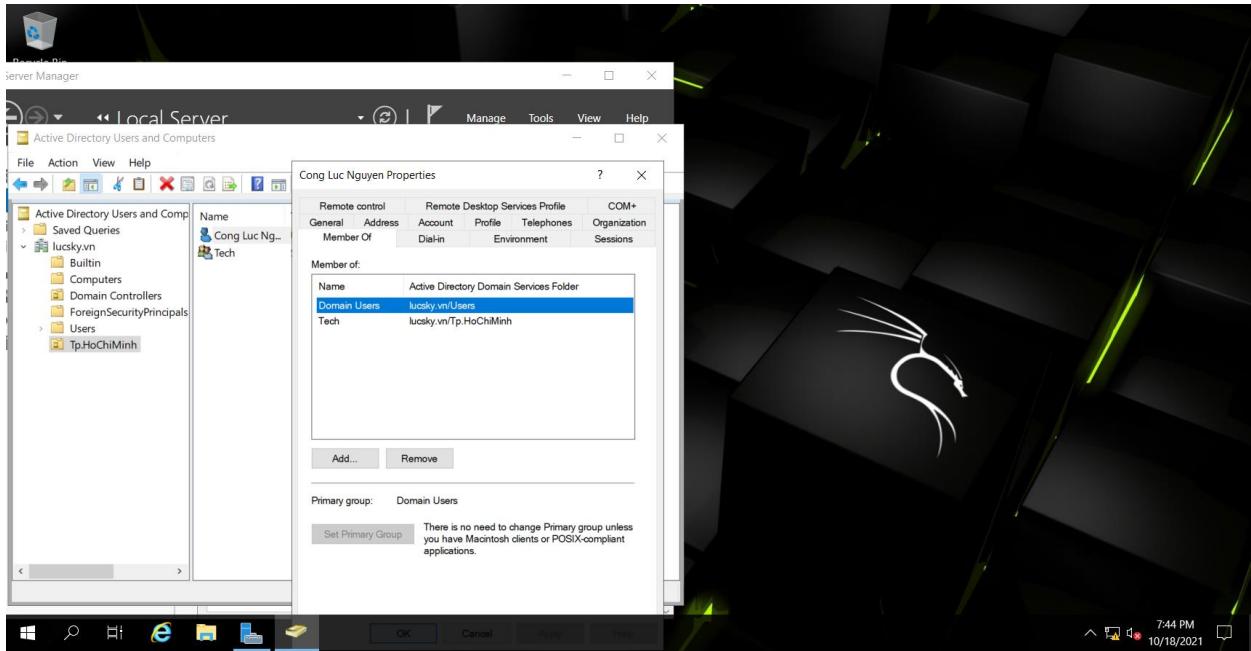
Hình 1.55 Click chuột phải vào User chọn Add to a Group

Cần thêm user vào group nào thì nhập tên group đó.



Hình 1.56 Ở đây nhập tên Group là Tech để thêm user vào group Tech

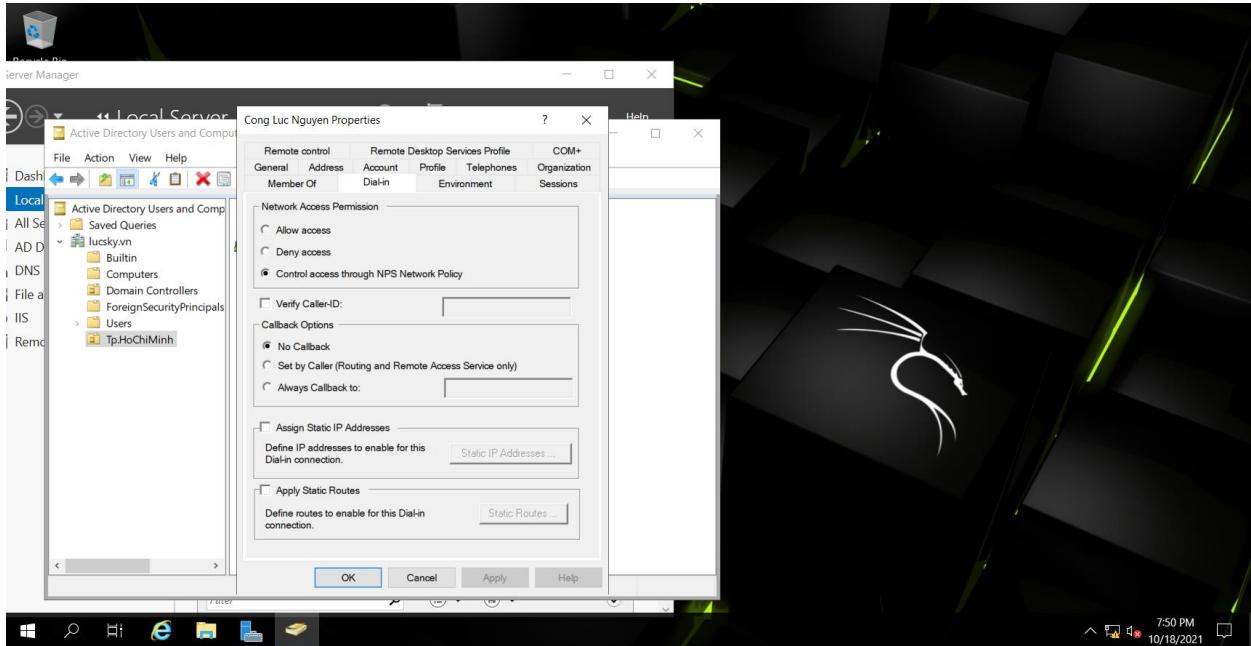
Sau khi thêm user vào group. Kiểm tra lại bằng cách. Chuột phải vào user cần kiểm tra -> Properties -> Member of



Hình 1.57 Đã thêm user vào group thành công

Cấp quyền Network Access Permission cho User

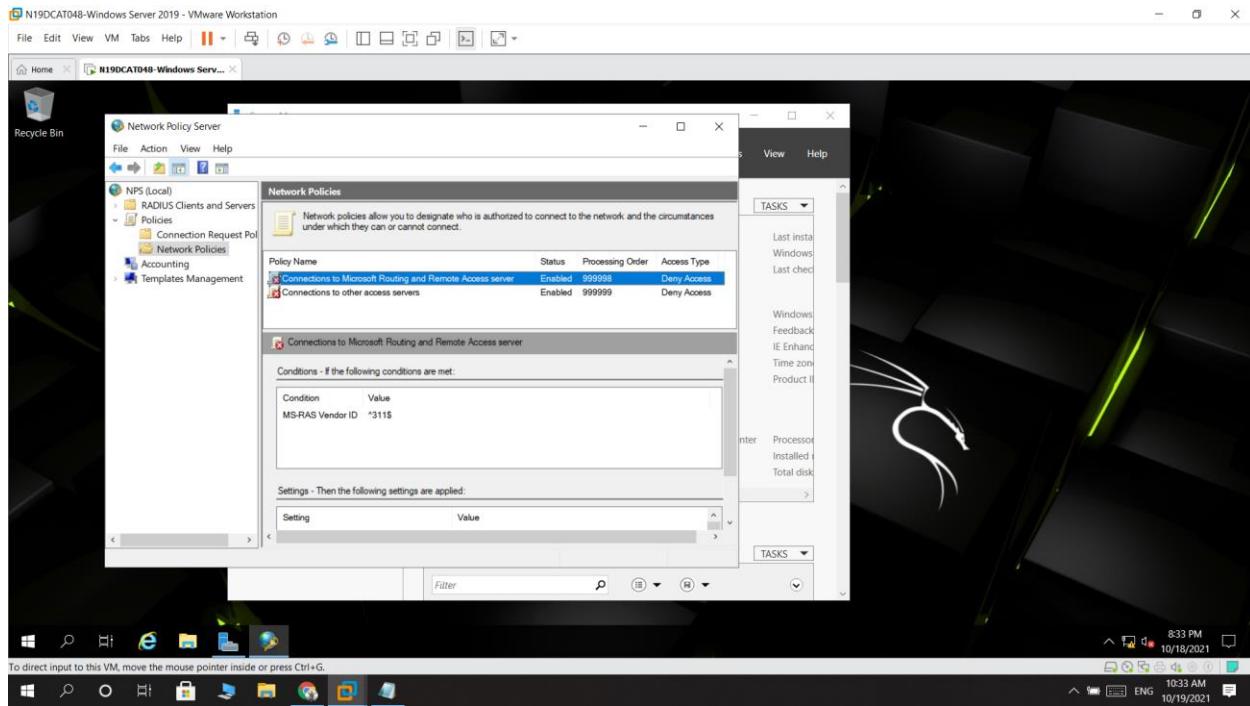
Chuột phải vào User muốn cấp quyền chọn Properties rồi chọn tab Dial-in. Ở mục Network Access Permission chọn Control access through NPS Network Policy rồi Apply và OK



Hình 1. 58: Cho phép Remote Access

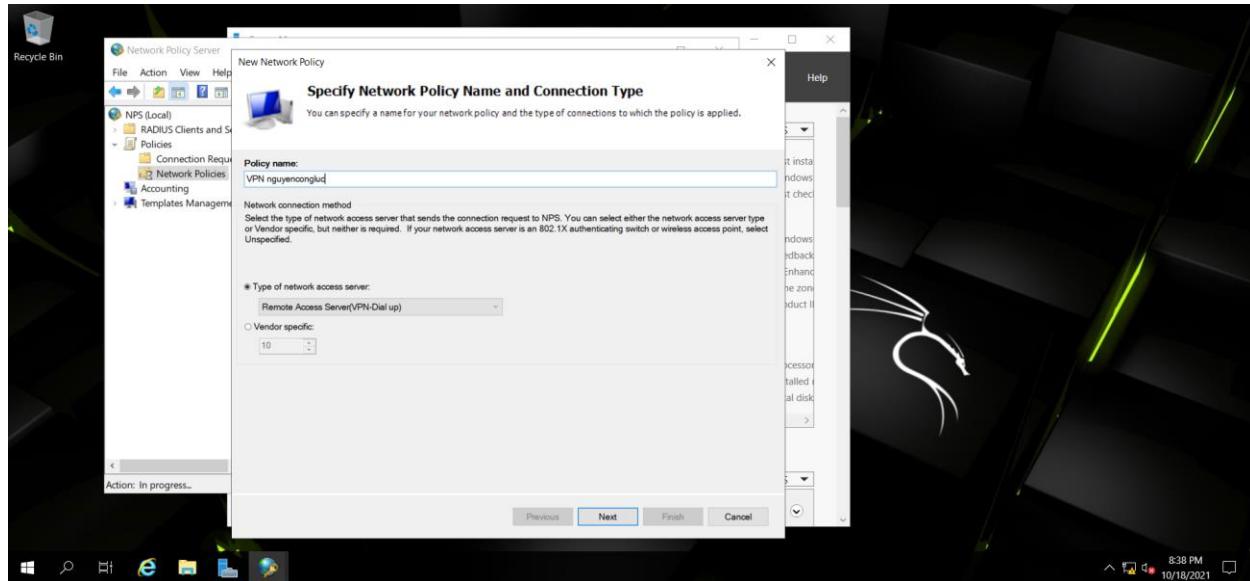
4. Cài đặt NPS Network Policy

Vào Server Manager ở Tools chọn Network Policy Server

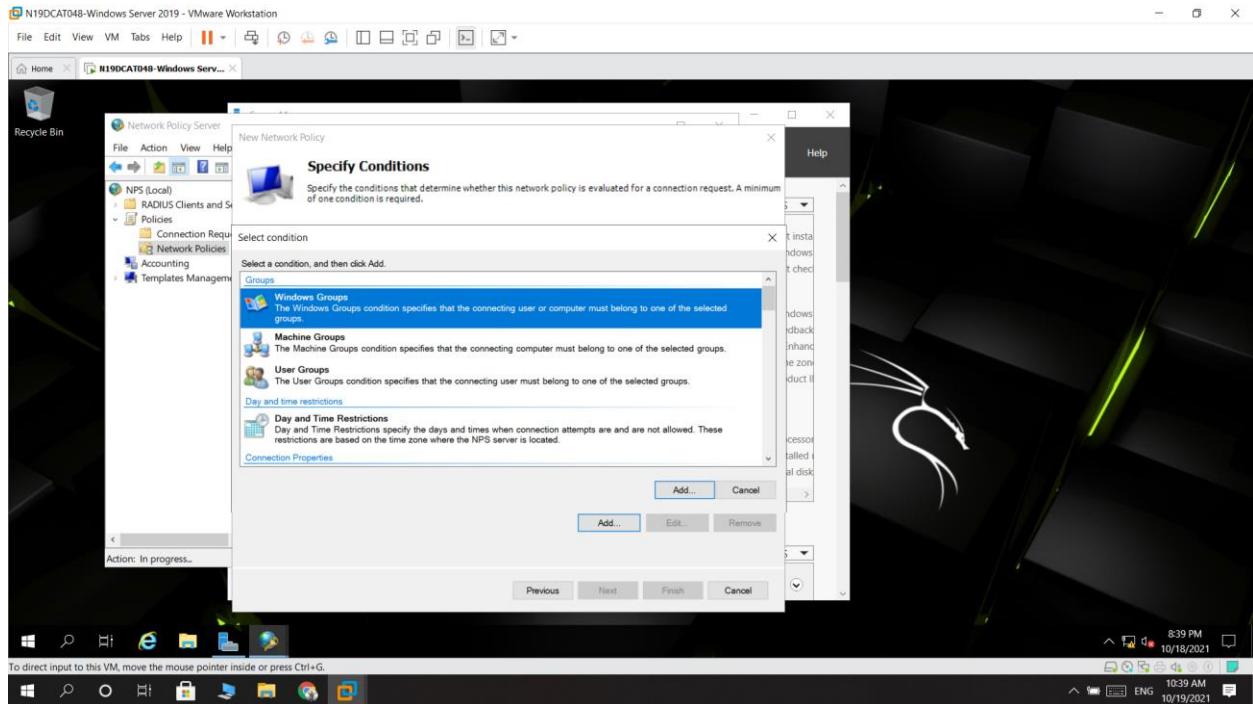


Hình 1. 59: Network Policy Server

Chuột phải vào Network Policies chọn new. Nhập tên và chọn Remote Access Server ở Type of network access server. Sau đó chọn Add

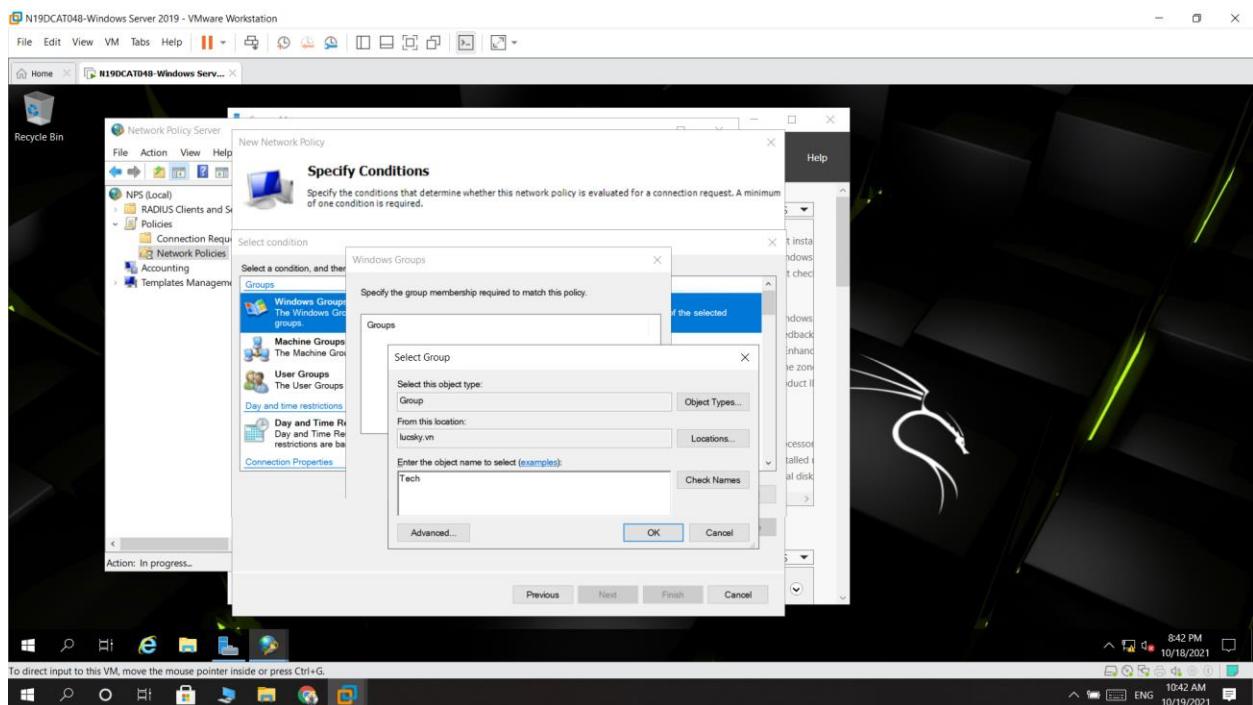


Hình 1. 60: Thêm Policy ở Network Policies

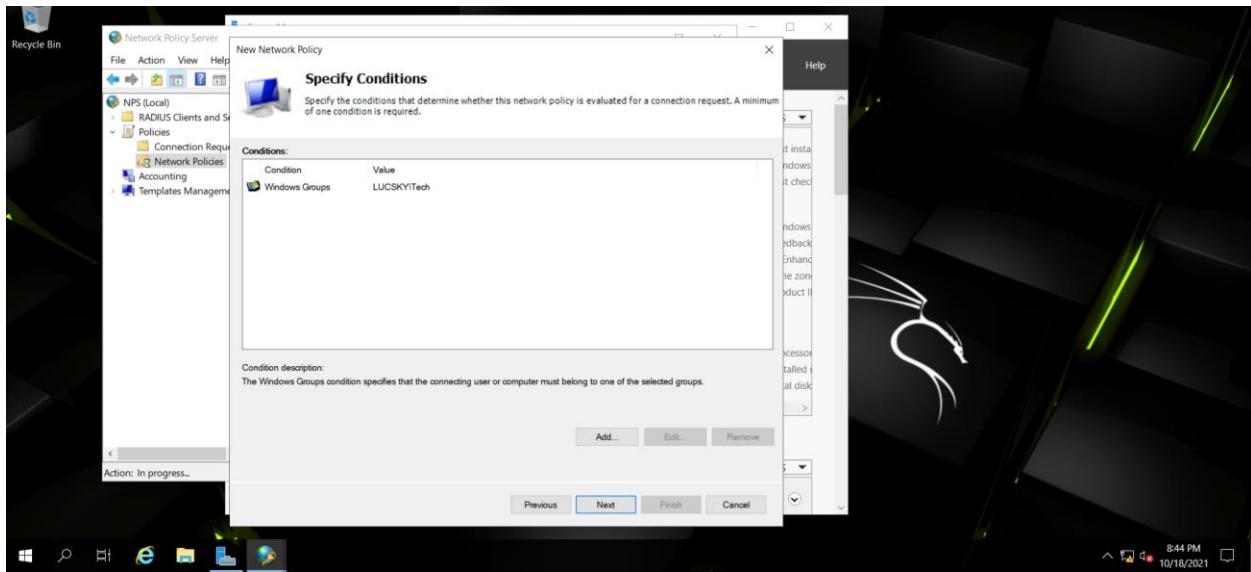


Hình 1. 61: Xác định đối tượng

Chọn Windows Groups rồi chọn Add. Tiếp theo, chọn Add Groups và chọn nhóm đối tượng muốn thêm sau đó chọn OK

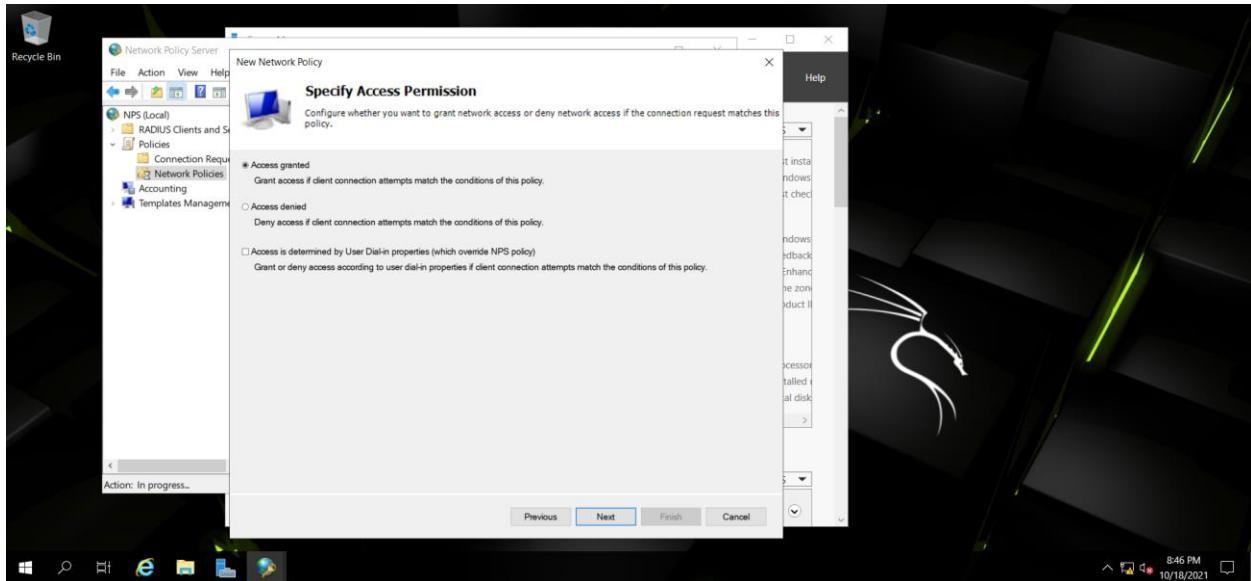


Hình 1. 62 Nhập nhóm đối tượng muốn thêm

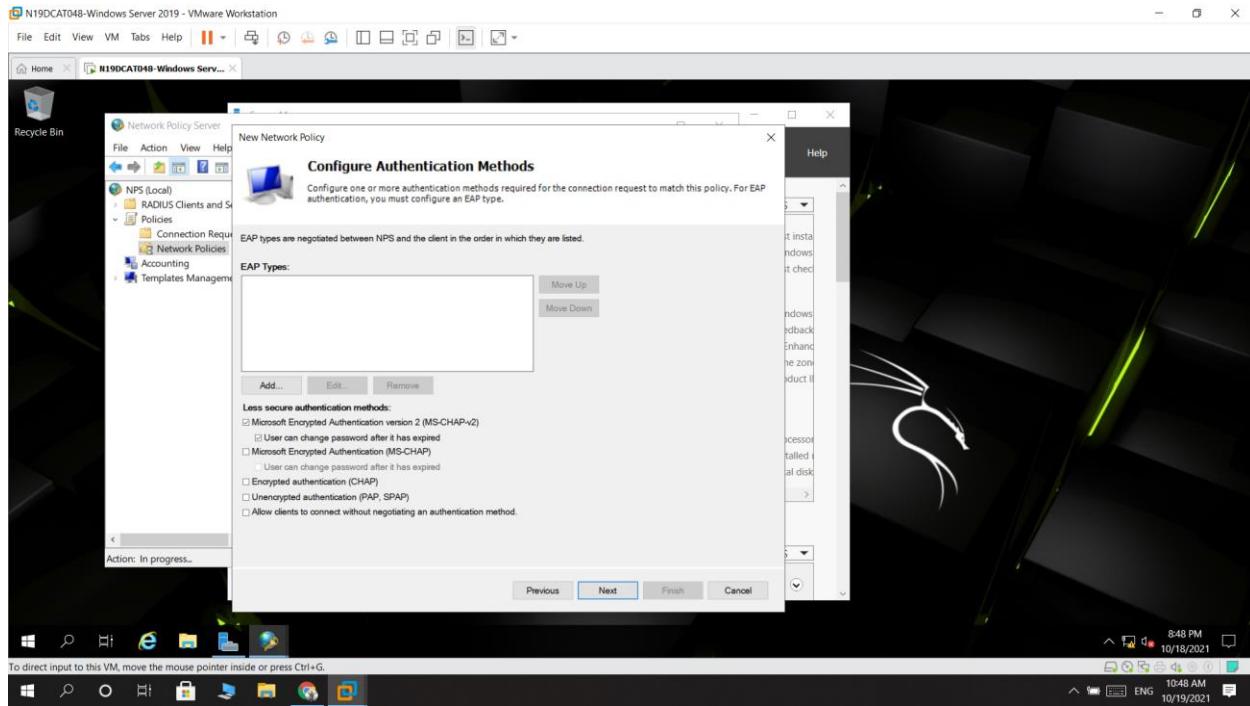


Hình 1.63 Thêm nhóm đối tượng thành công

Chọn Access granted rồi chọn Next

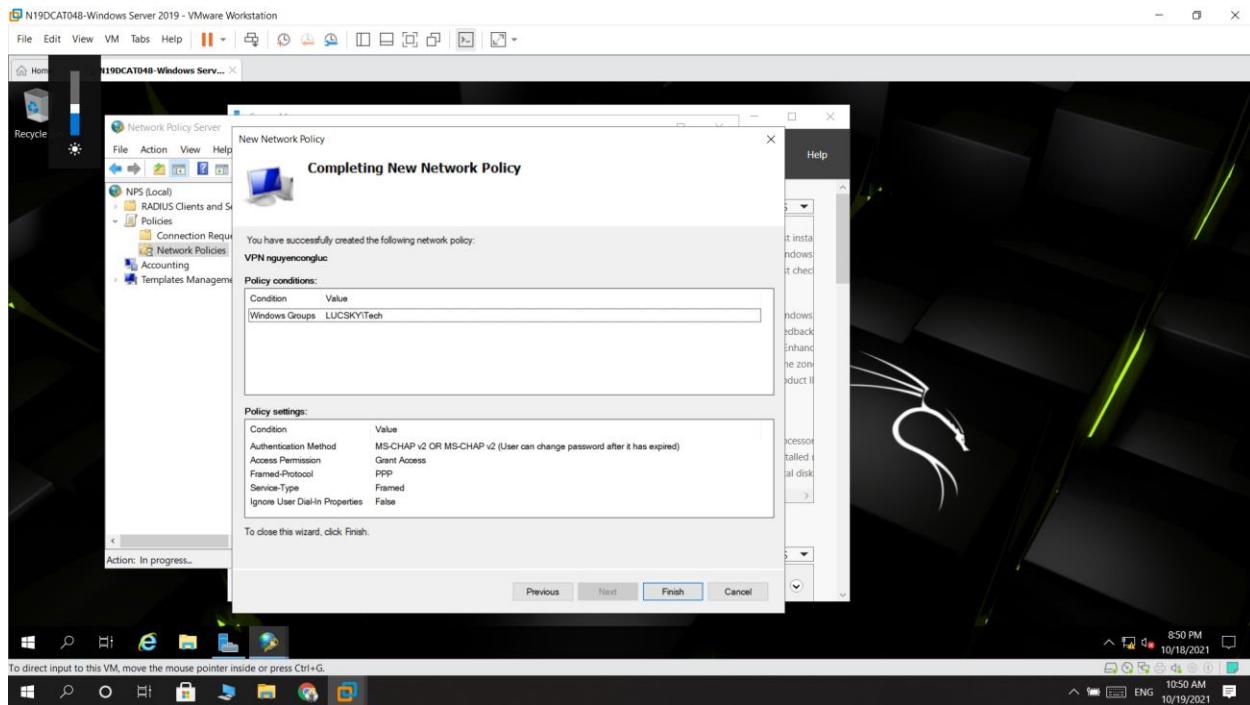


Hình 1. 64: Xác định quyền truy cập



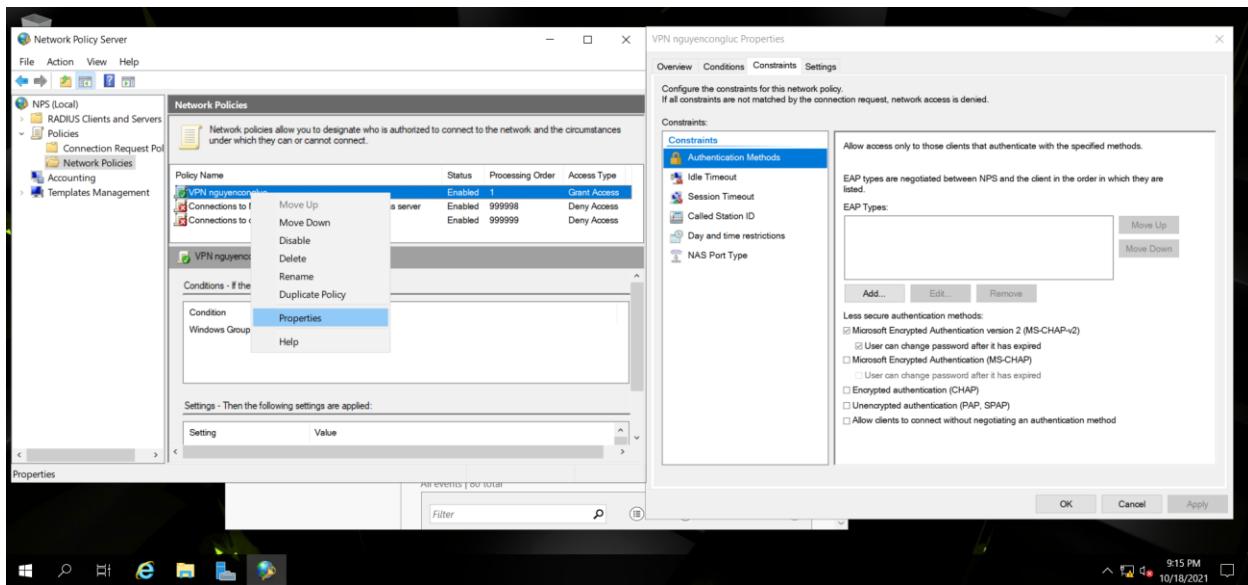
Hình 1. 65: Phương pháp xác thực

Nhấn Next 3 lần sau đó chọn Finish



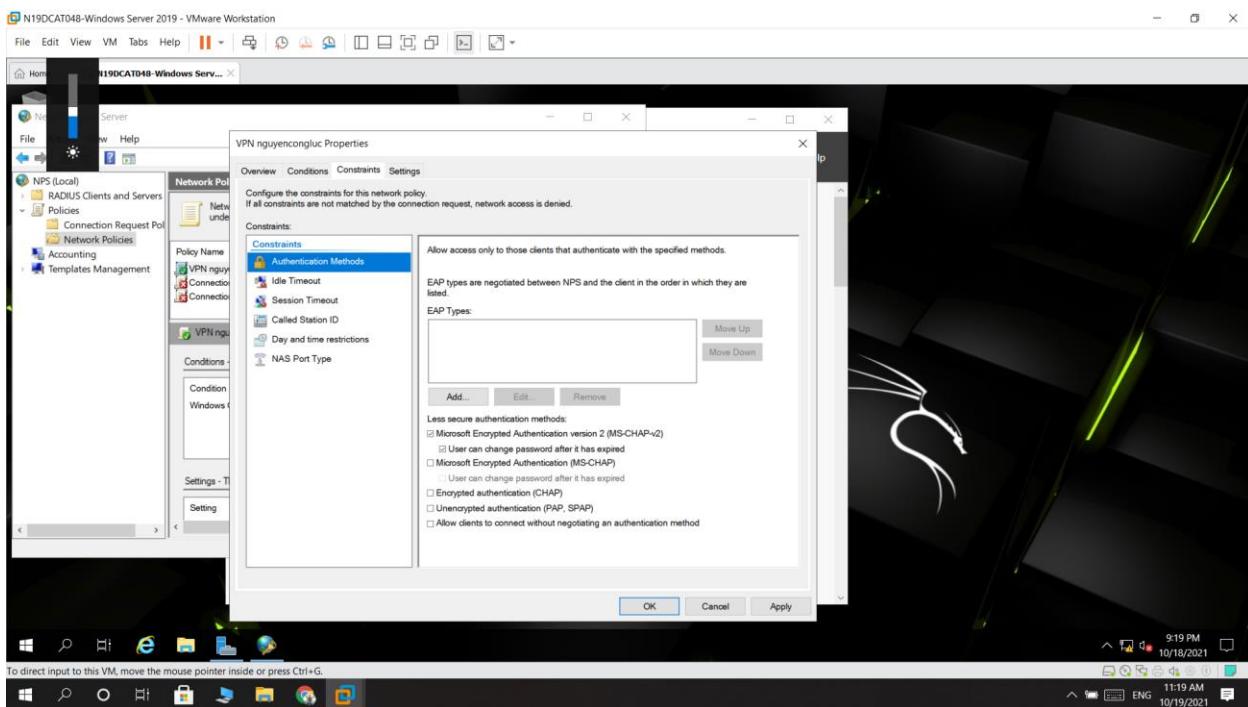
Hình 1. 66: Hoàn thành tạo một Network Policies

Chuột phải vào Policy vừa tạo chọn Properties và chọn tab Constraints



Hình 1. 67: Phương pháp xác thực

Chọn Secured password (EAP-MSCHAP v2)sau đó chọn ok



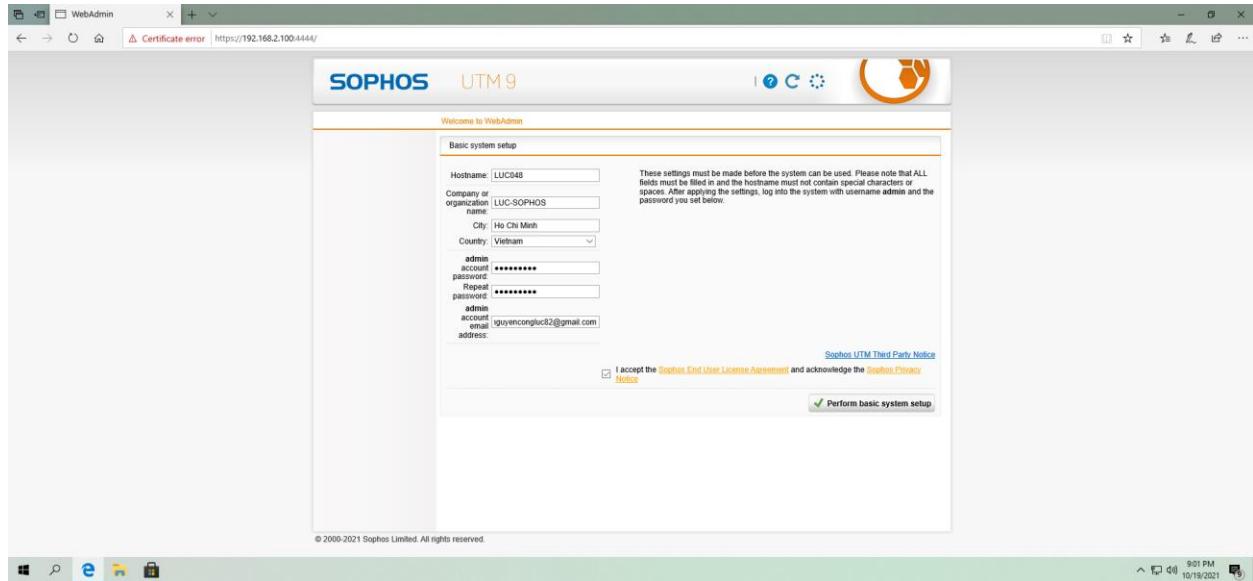
Hình 1. 68: Secured password

C. Cài đặt Sophos Firewall và chính sách truy cập Internet

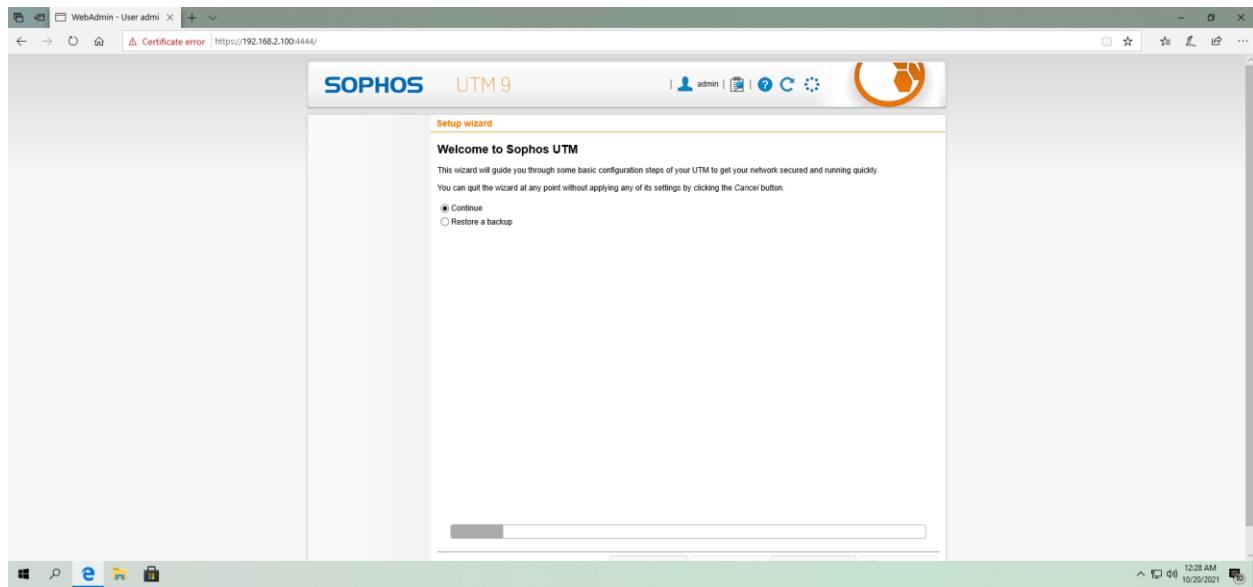
Các bước thực hiện:

1. Cài đặt cơ bản

Điền thông tin theo yêu cầu rồi chọn Perform basic system setup

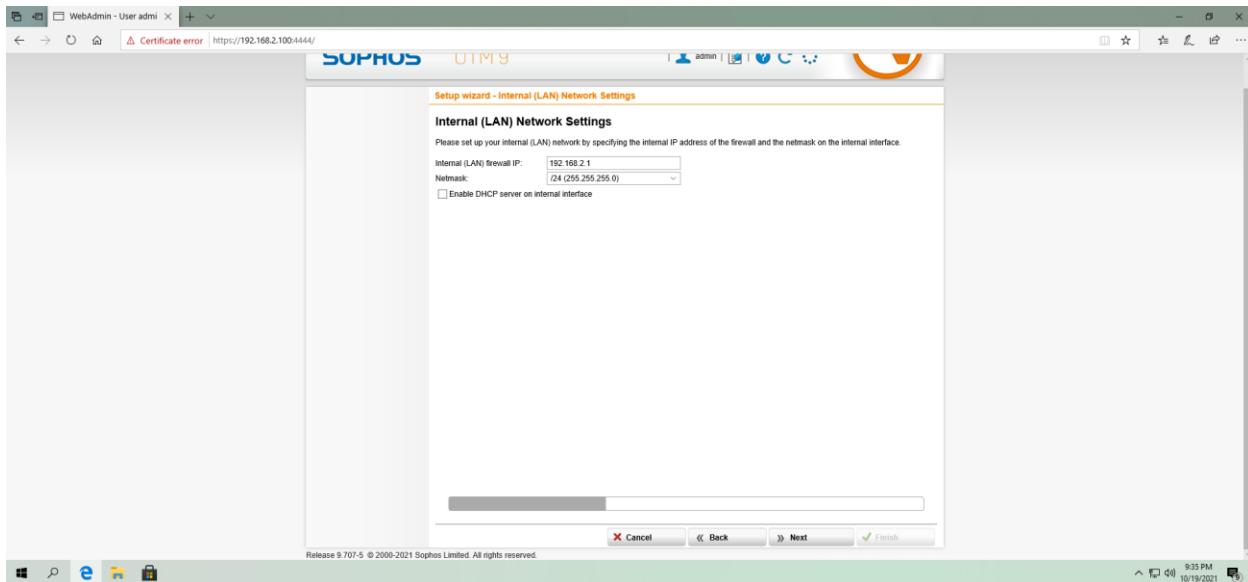


Hình 1. 69: Khai báo thông số ban đầu

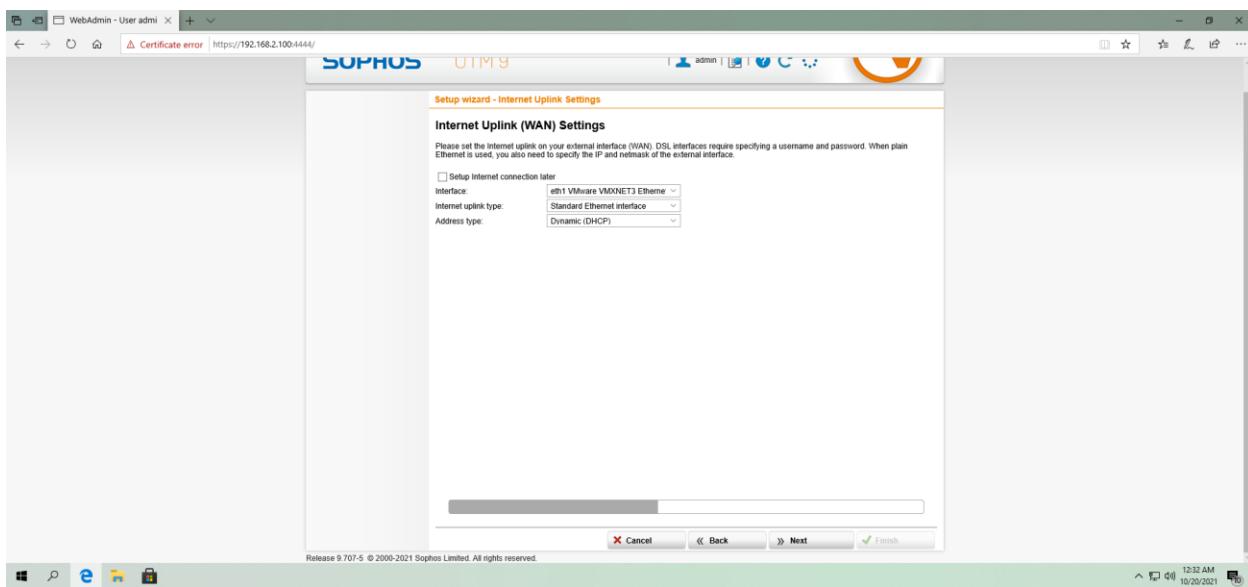


Hình 3. 59: Cấu hình

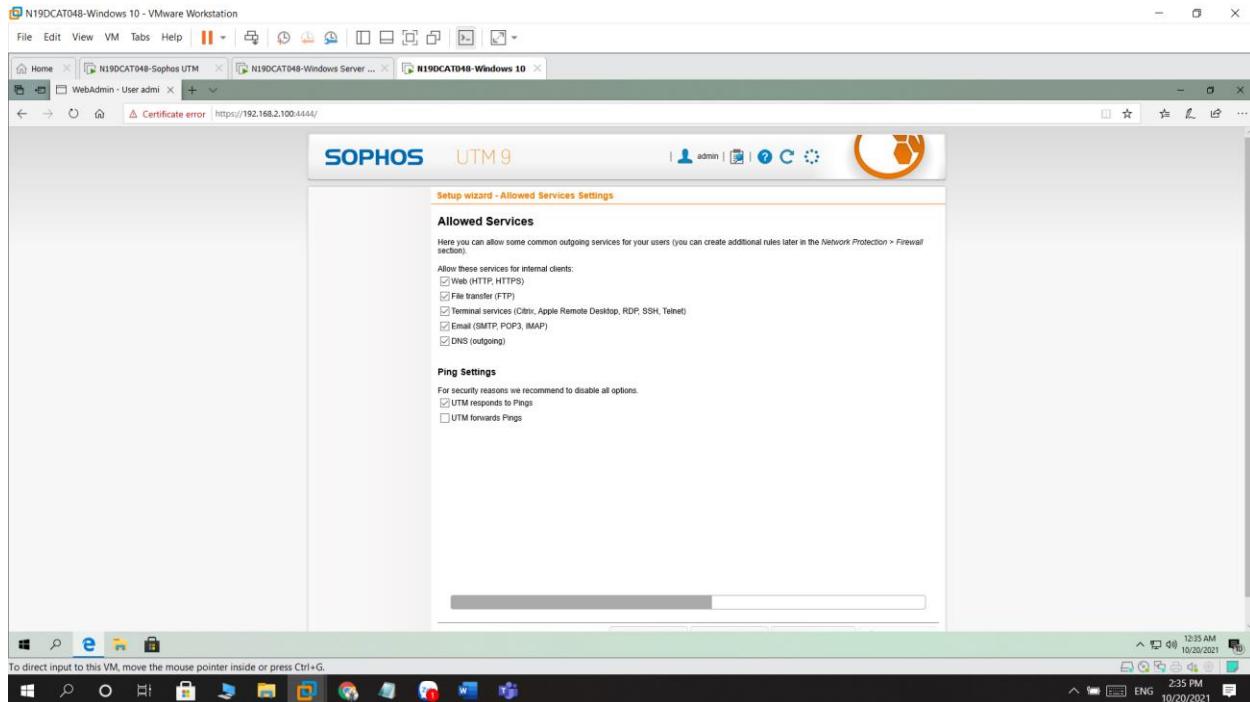
Tiếp theo cấu hình thông số cho Sophos



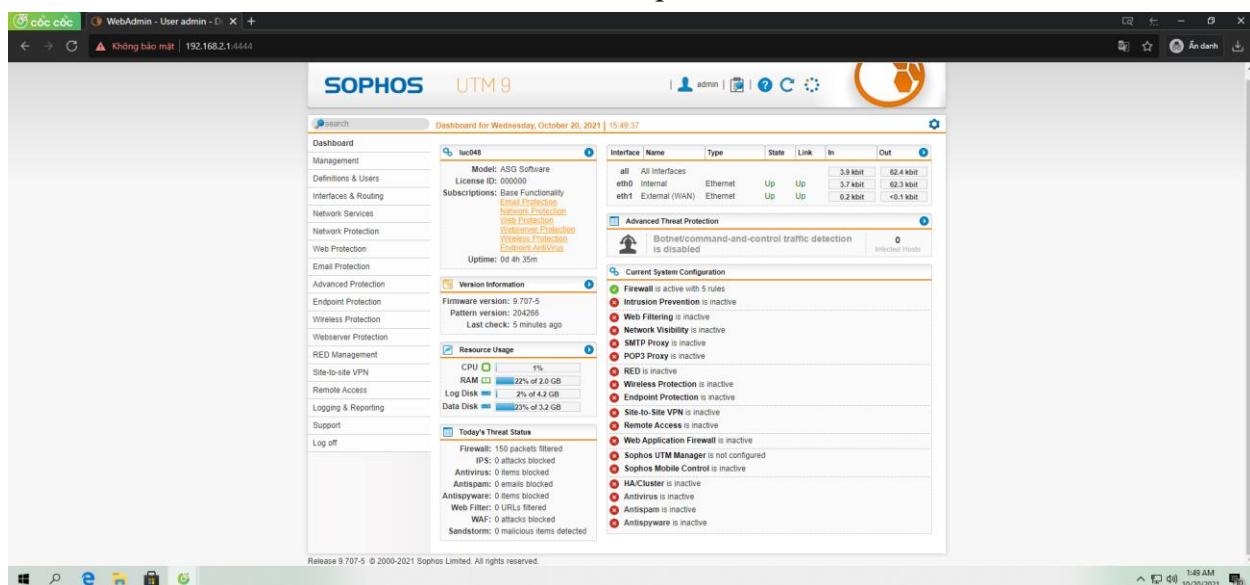
Hình 1. 70: Thiết lập mạng LAN



Hình 1. 71: Thiết lập mạng WAN



Hình 1.72: Thiết lập các dịch vụ

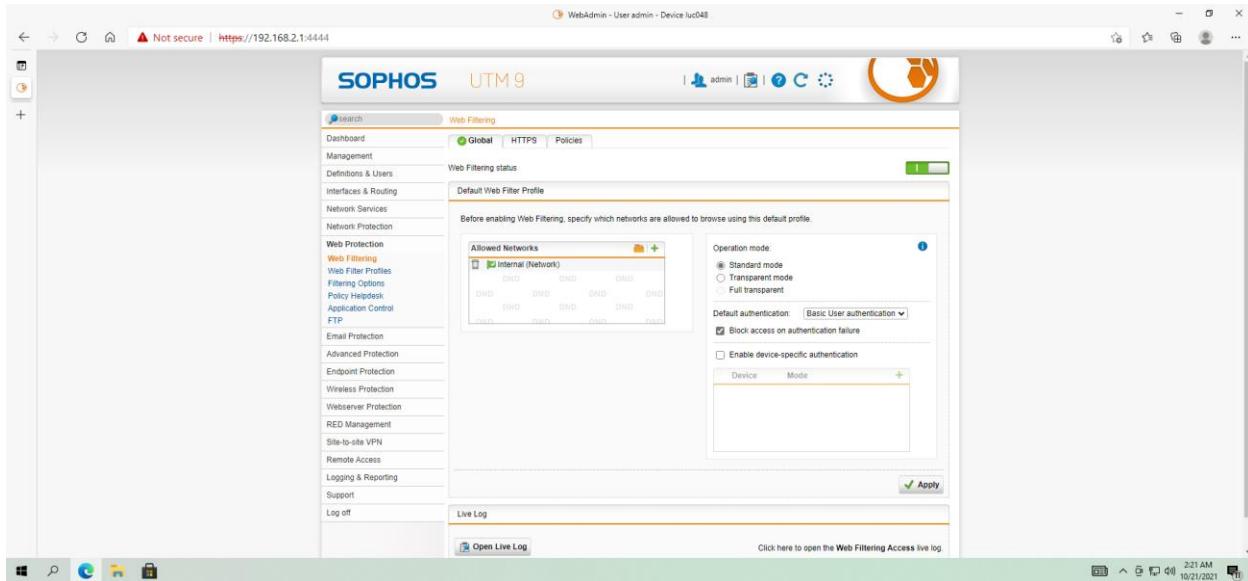


Hình 1.73: Màn hình chính của Sophos

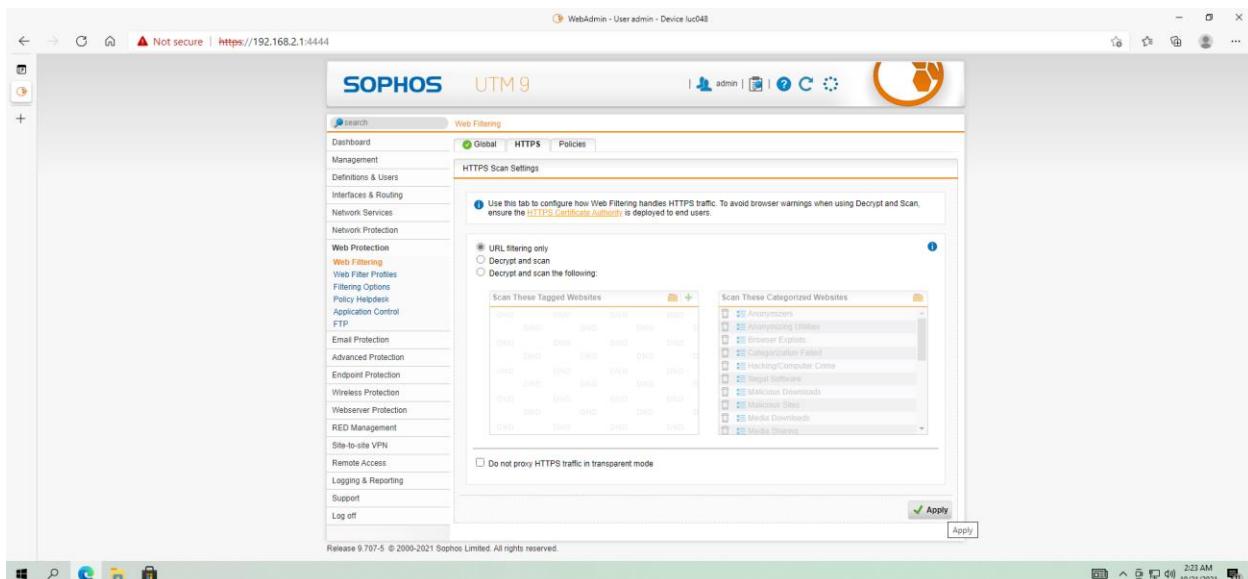
2. Cài đặt truy cập Internet cho nhân viên

Cấu hình mạng LAN hoạt động theo Standard mode thông qua Proxy xác

thực bằng tài khoản của nhân viên được cấp

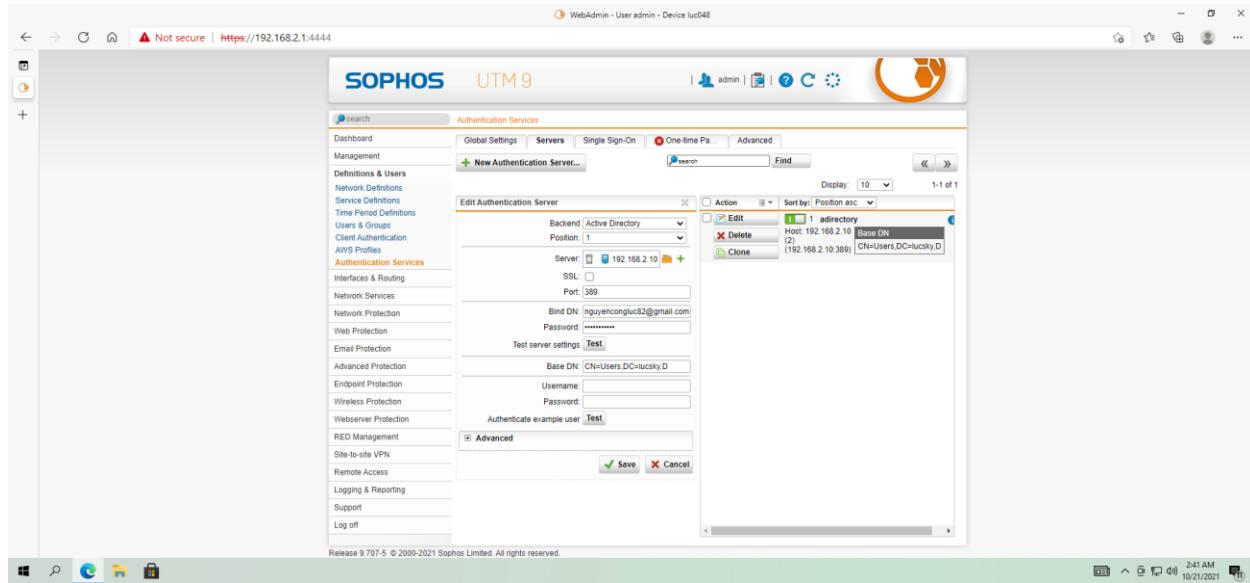


Hình 1. 78: Cài đặt Web Filtering



Hình 1. 79: HTTPS

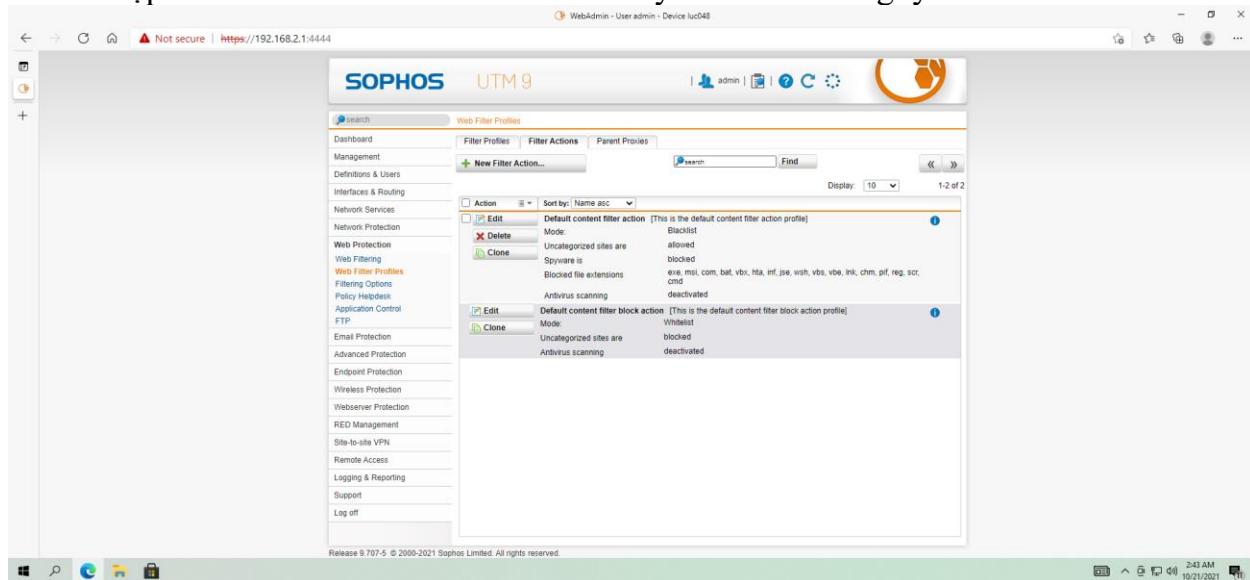
Tích hợp với Domain Controller để xác thực tài khoản của nhân viên khi truy cập Internet



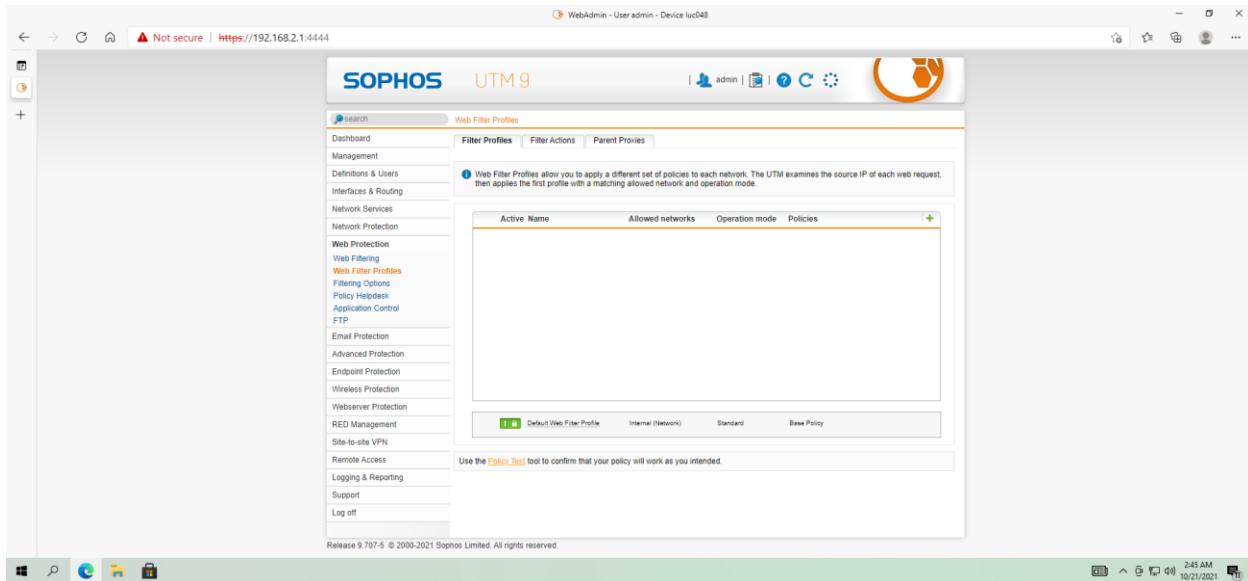
Hình 1. 80: Xác thực User

3. Thiết lập chính sách cho nhân viên

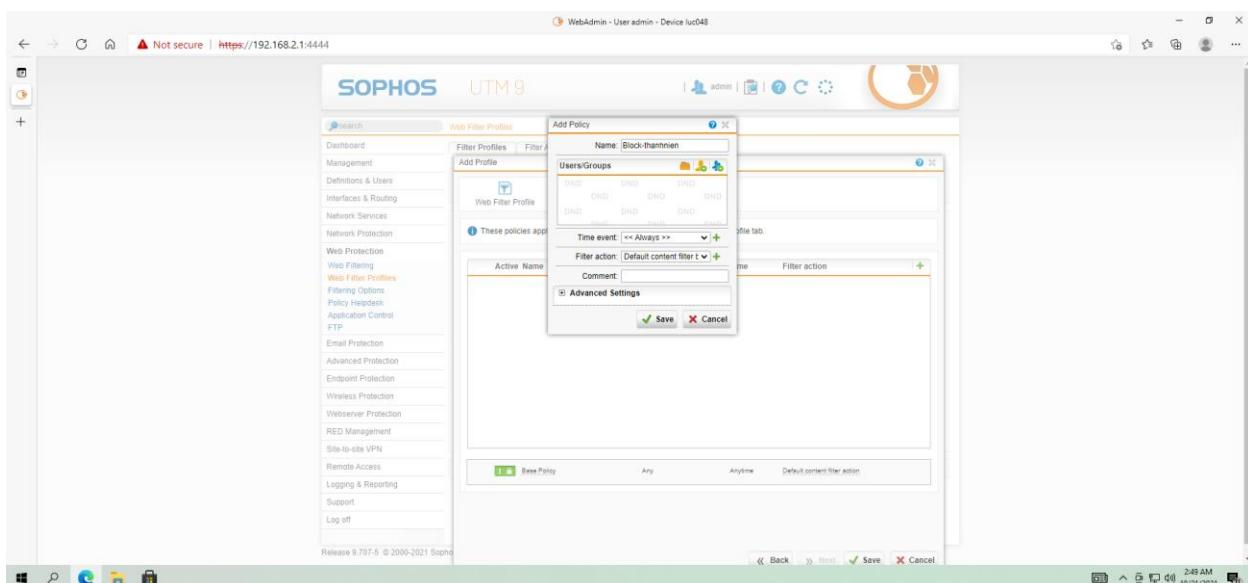
Sẽ thiết lập các chính sách cho nhân viên theo yêu cầu của công ty



Hình 1. 81: Filter Actions



Hình 1. 82: Filter Profiles



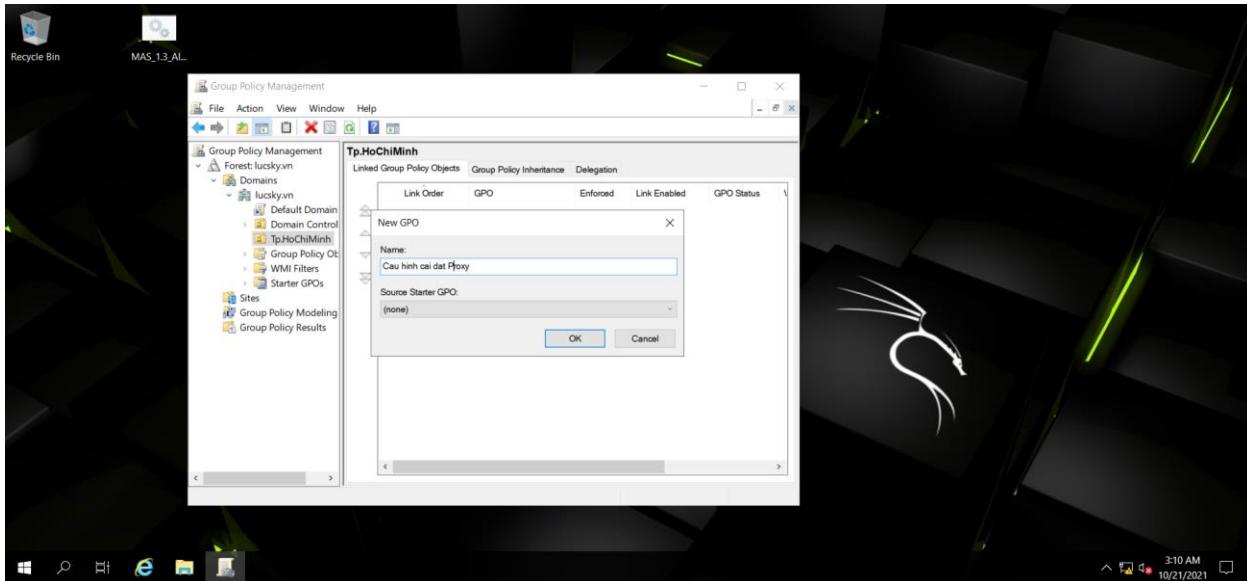
Hình 1. 83: Thiết lập chính sách

3.1.1 Cài đặt chính sách Proxy Server cho máy nhân viên

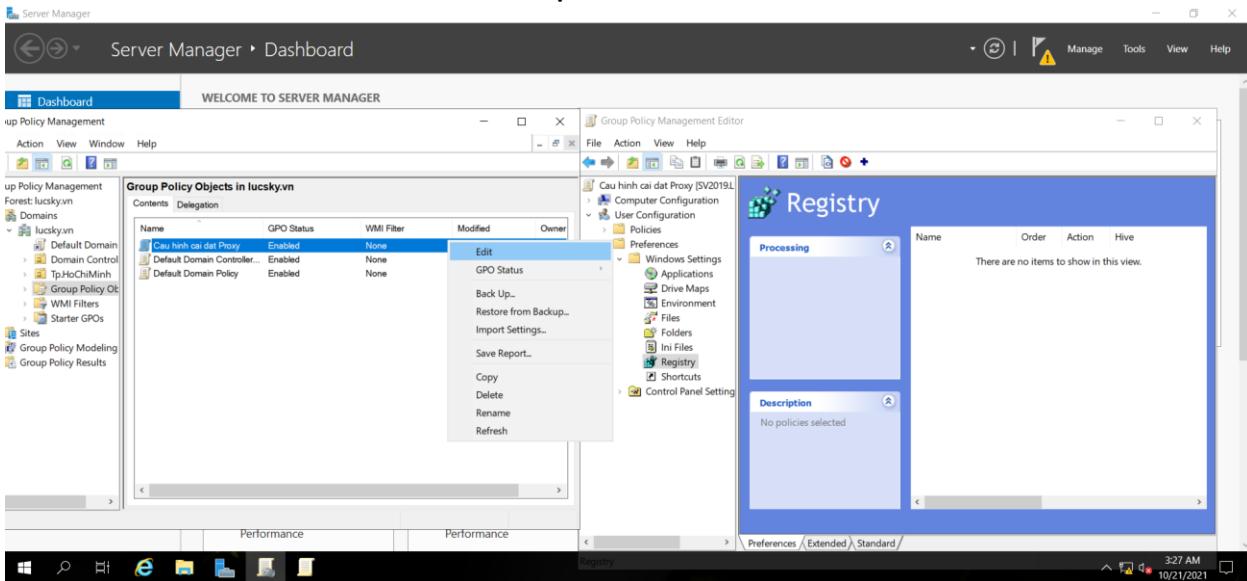
Yêu cầu: Các máy của nhân viên đã tham gia vào môi trường domain

của công ty Các bước thực hiện:

Thiết lập chính sách cho các máy của nhân viên khi sử dụng web phải thông qua Proxy Server của công ty



Hình 1. 84: Tạo chính sách mới

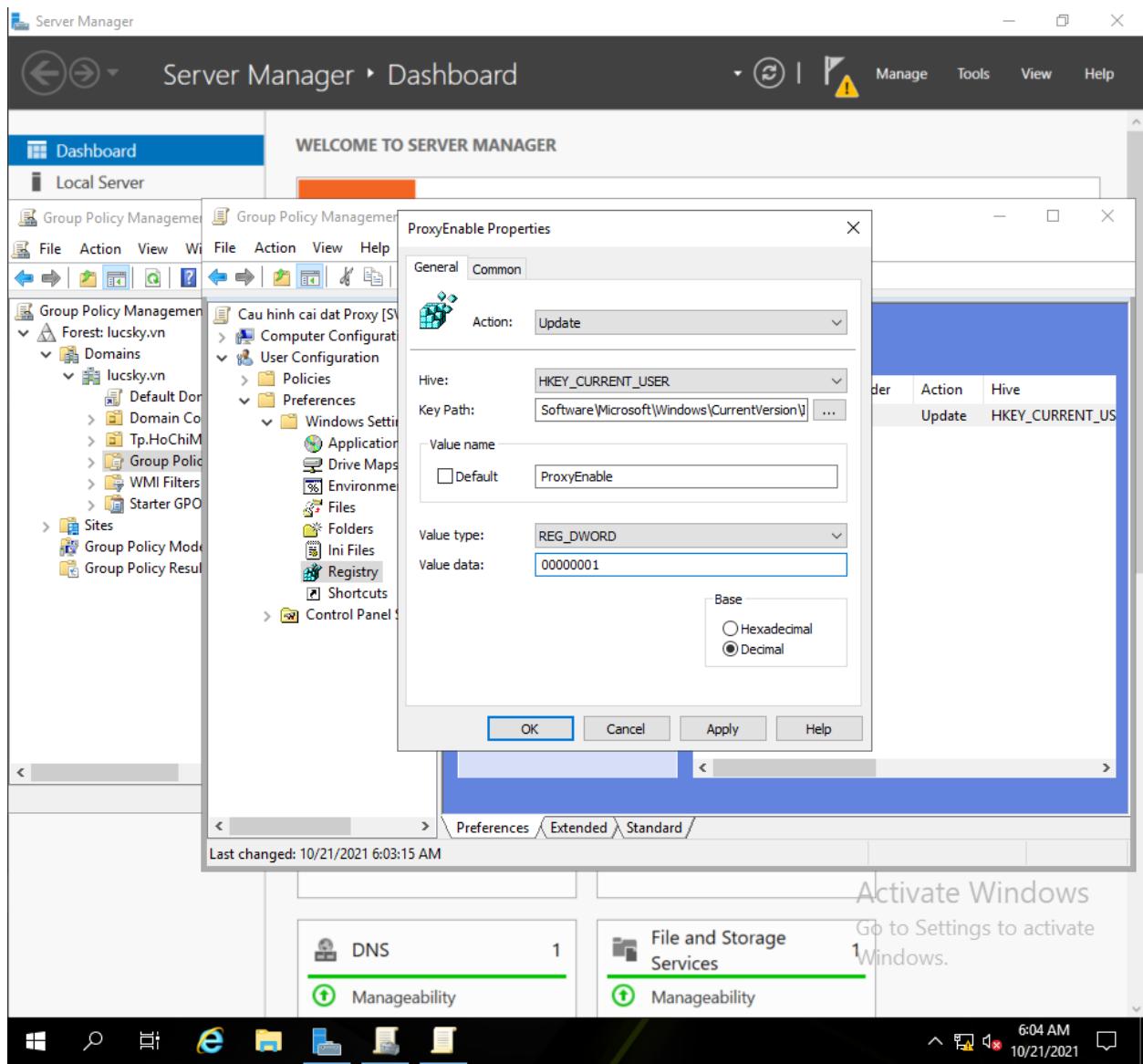


Hình 1. 85: Registry

Nhấp chuột phải vào vùng trống rồi chọn new registry item.

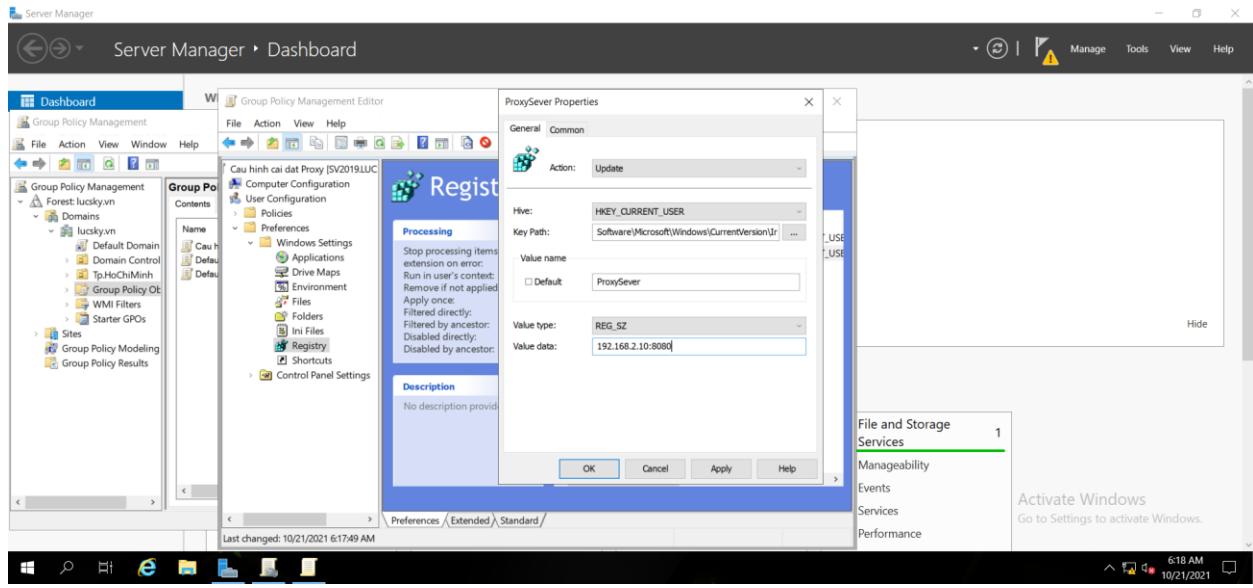
Nhập key path với đường dẫn:

Software\Microsoft\Windows\CurrentVersion\Internet Settings

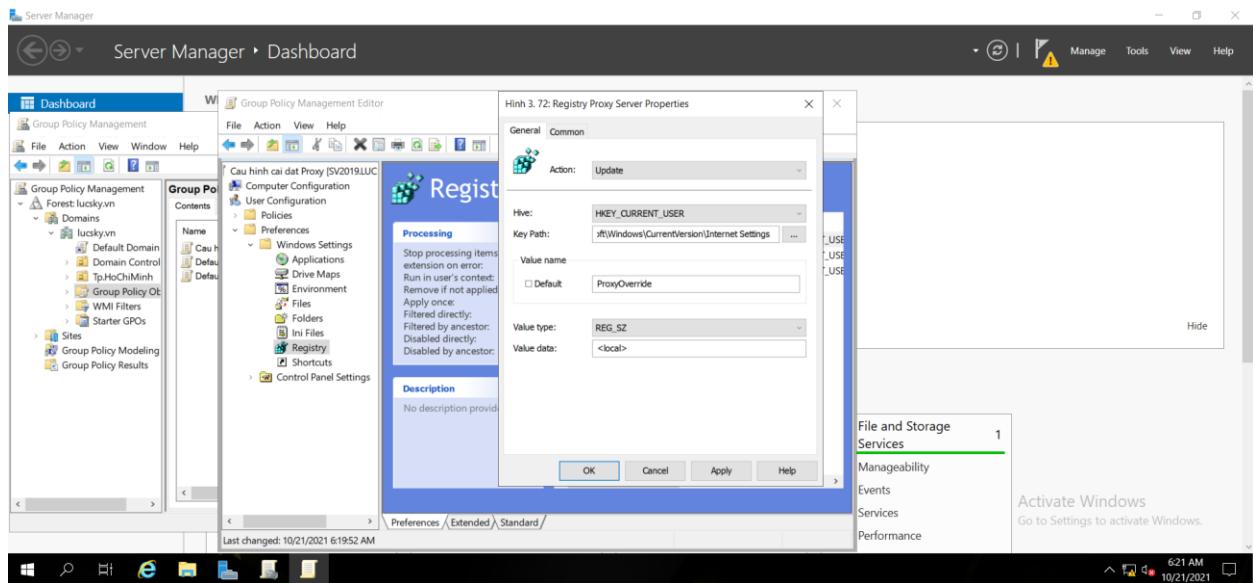


Hình 1. 85: Registry Proxy Enable

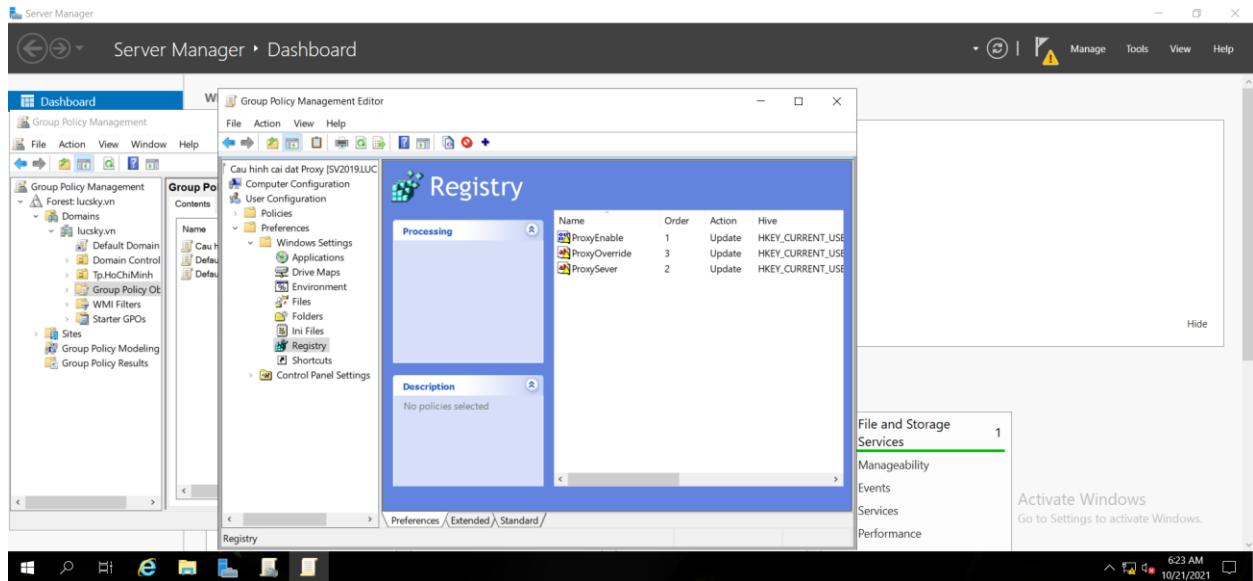
Tạo thêm 1 registry item nữa



Hình 1. 86: Registry Proxy Server



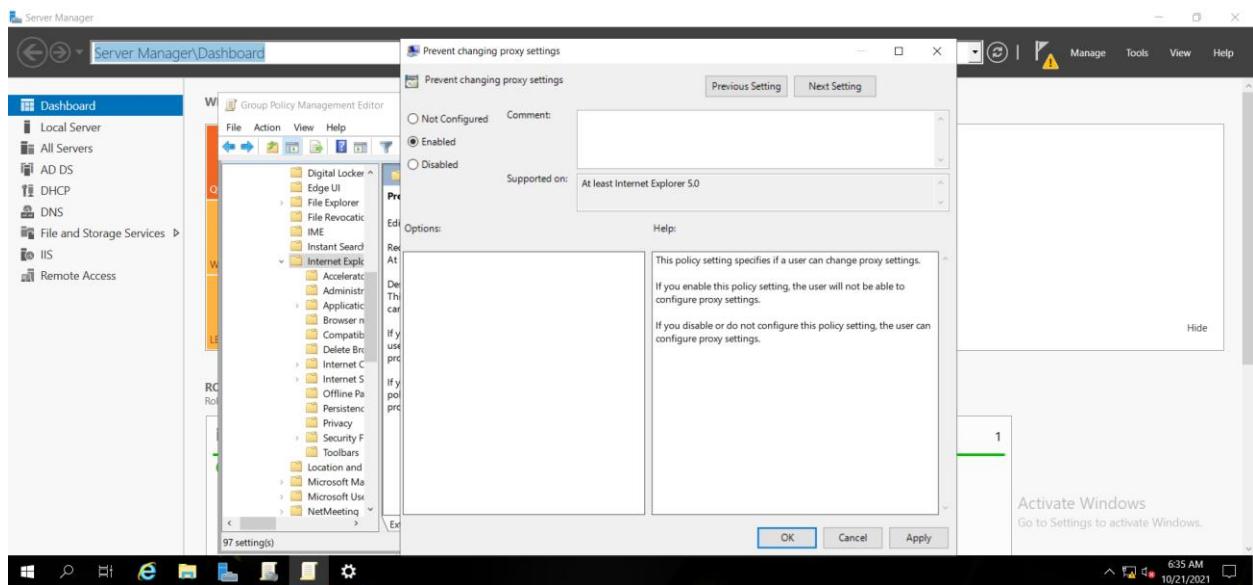
Hình 1. 87: Registry Proxy Override



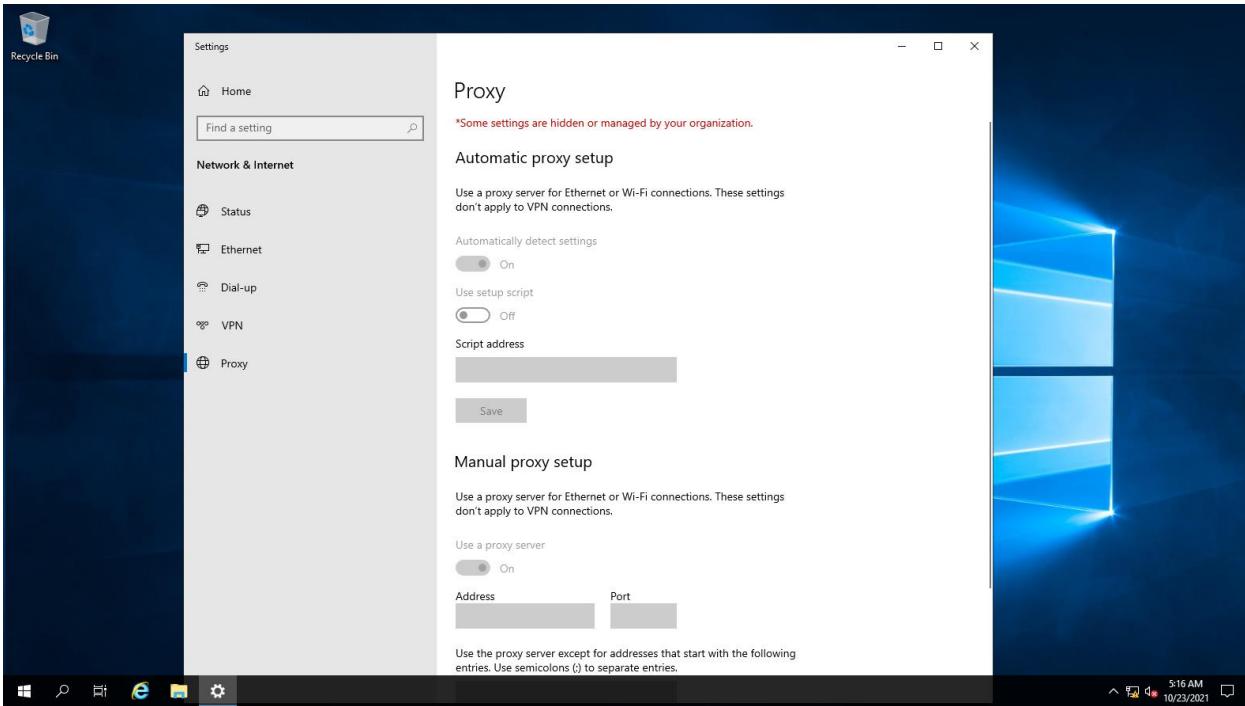
Hình 1. 88: Đã tạo xong 3 registry

Thiết lập chính sách không cho phép nhân viên thay đổi

Proxy



Hình 1. 89: Chặn thay đổi Proxy

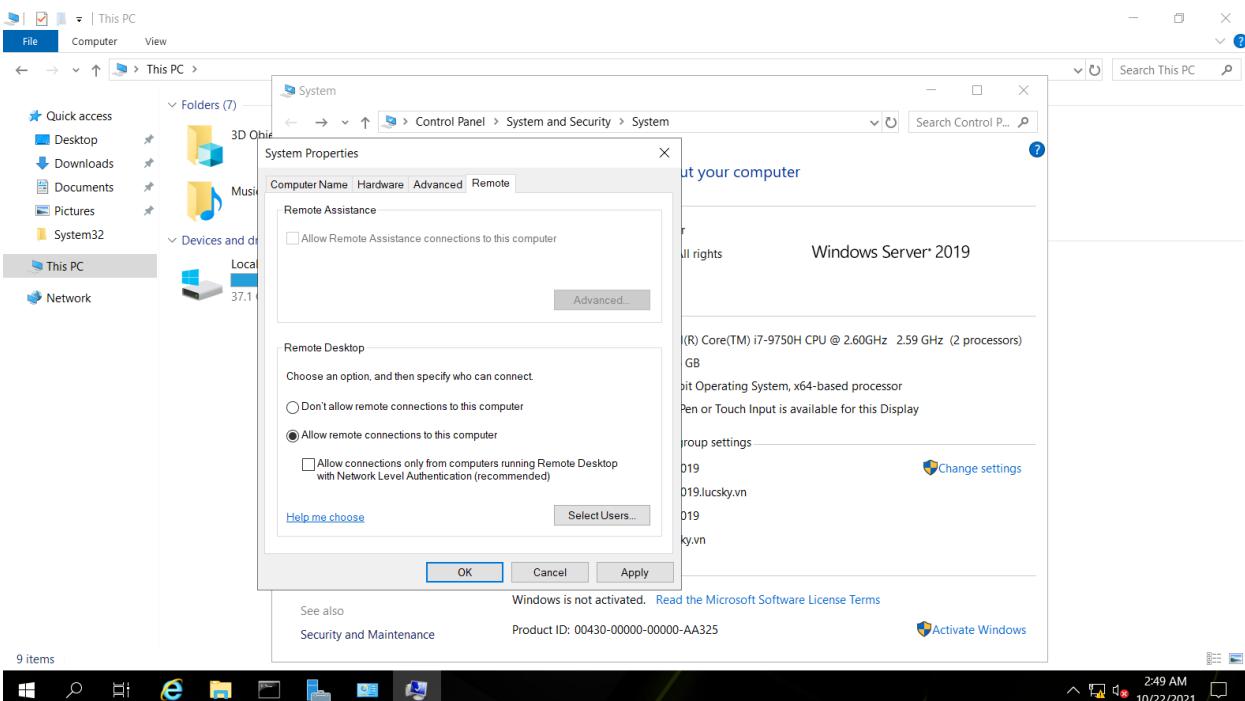


Hình 1. 90: Kết quả Proxy Server

3.1.1 Cài đặt điều khiển Server từ xa cho quản trị viên

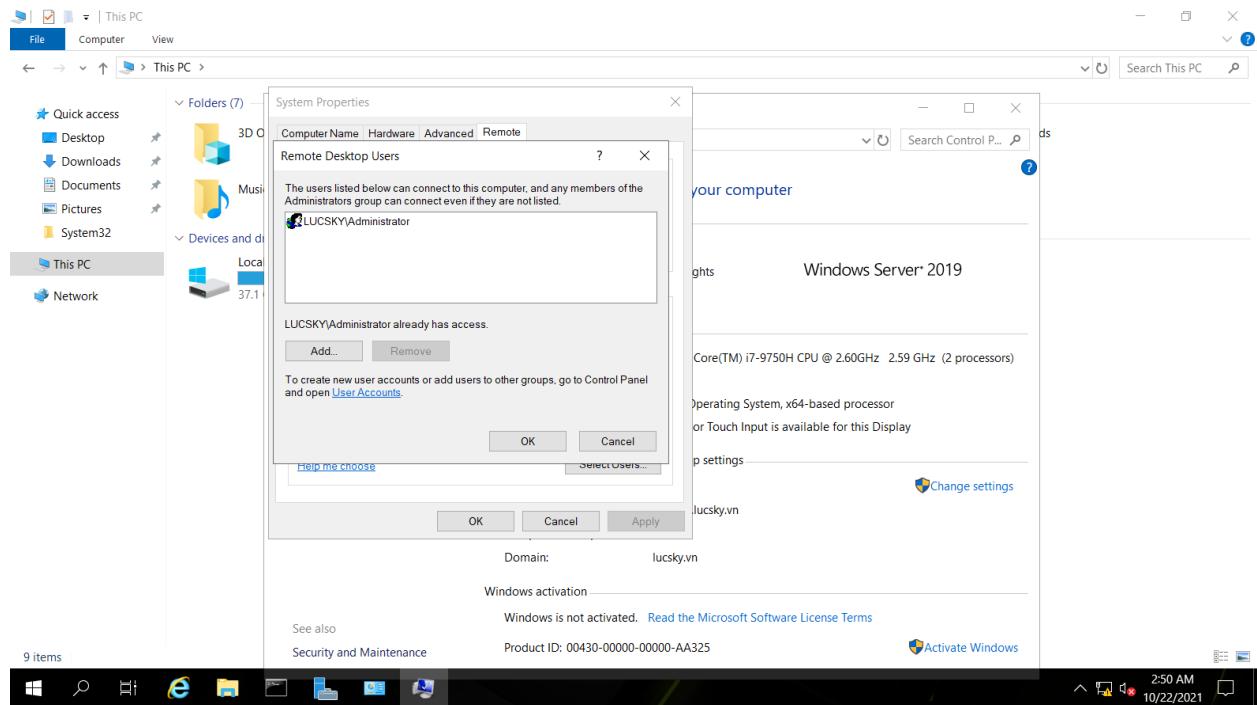
3.2.5 Thực hiện cho phép người quản trị viên có thể điều khiển Domain Controller từ xa thông qua Remote Desktop

Chọn mục Allow remote connections to this computer để cho phép remote tới Server

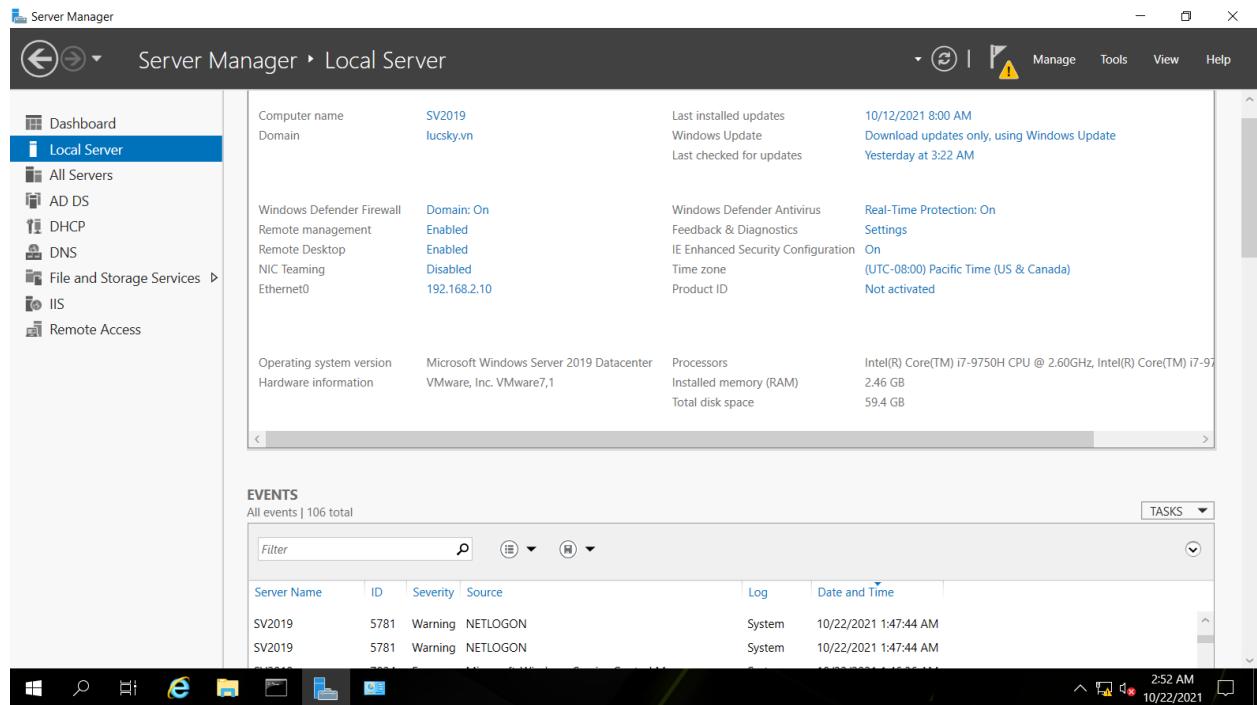


Hình 1. 91: Allow remote connection

Tiến hành thêm người dùng được phép remote

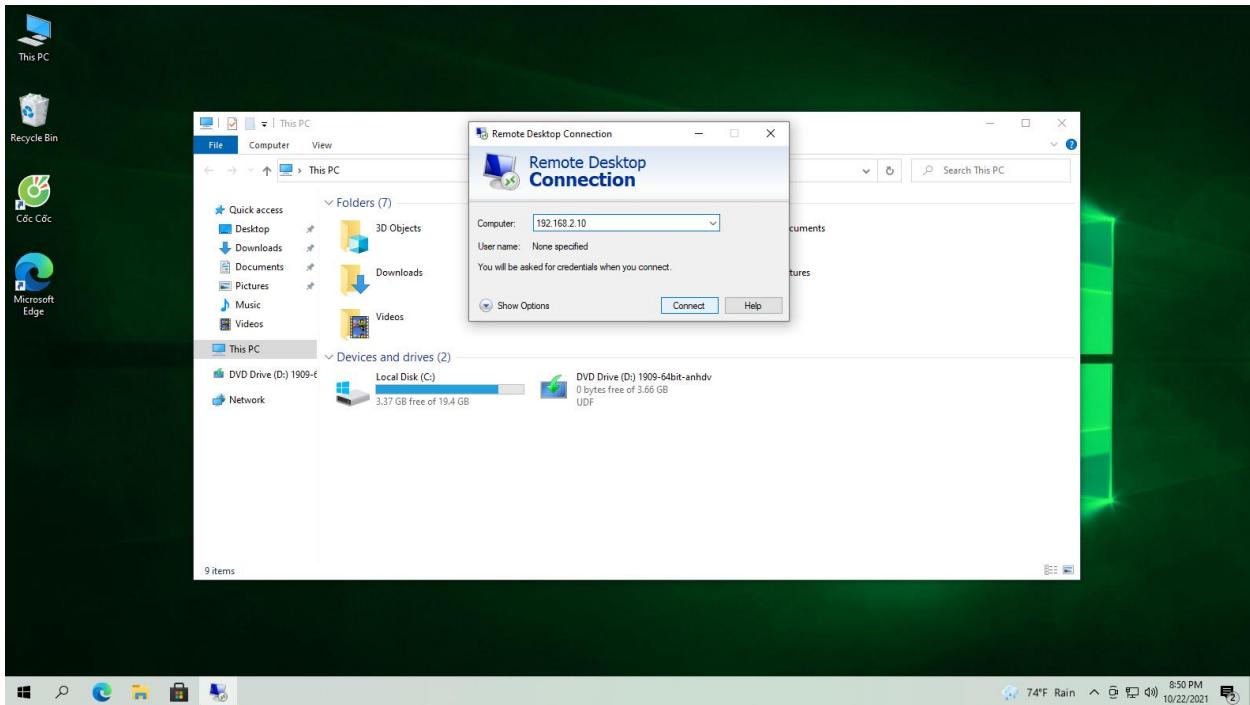


Hình 1. 92: Add Remote Desktop Users

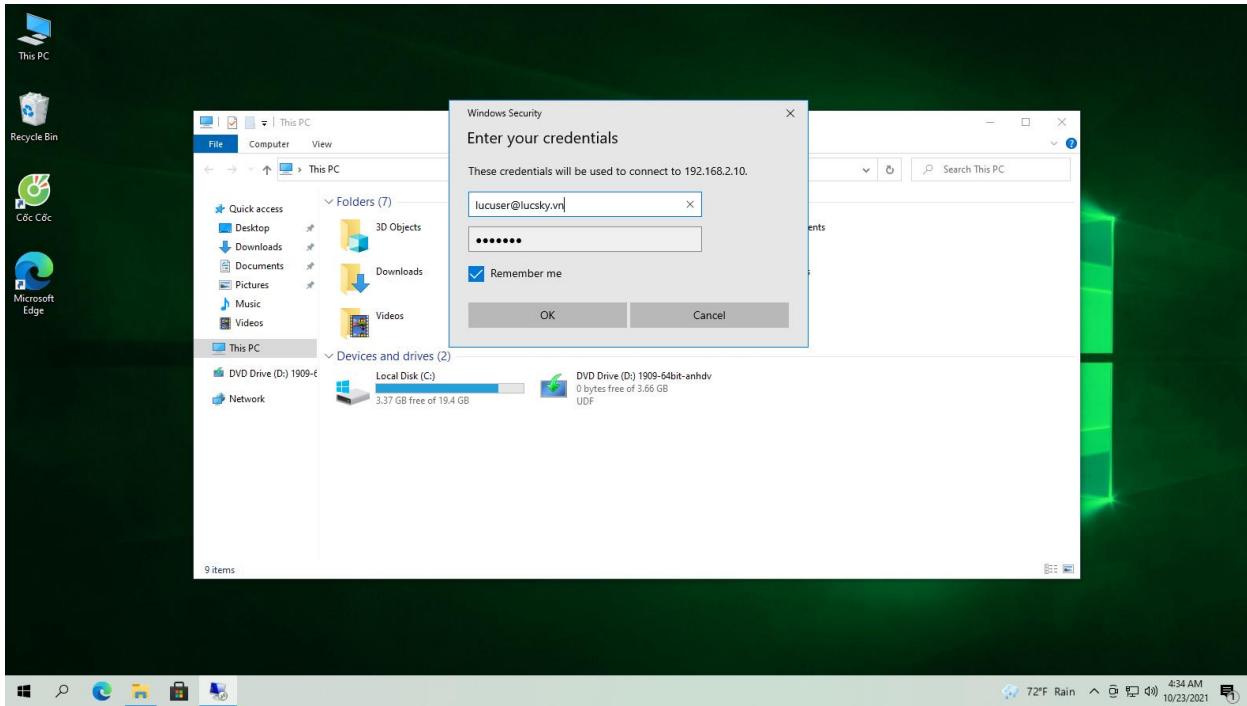


Hình 1. 93: Remote Desktop Enabled

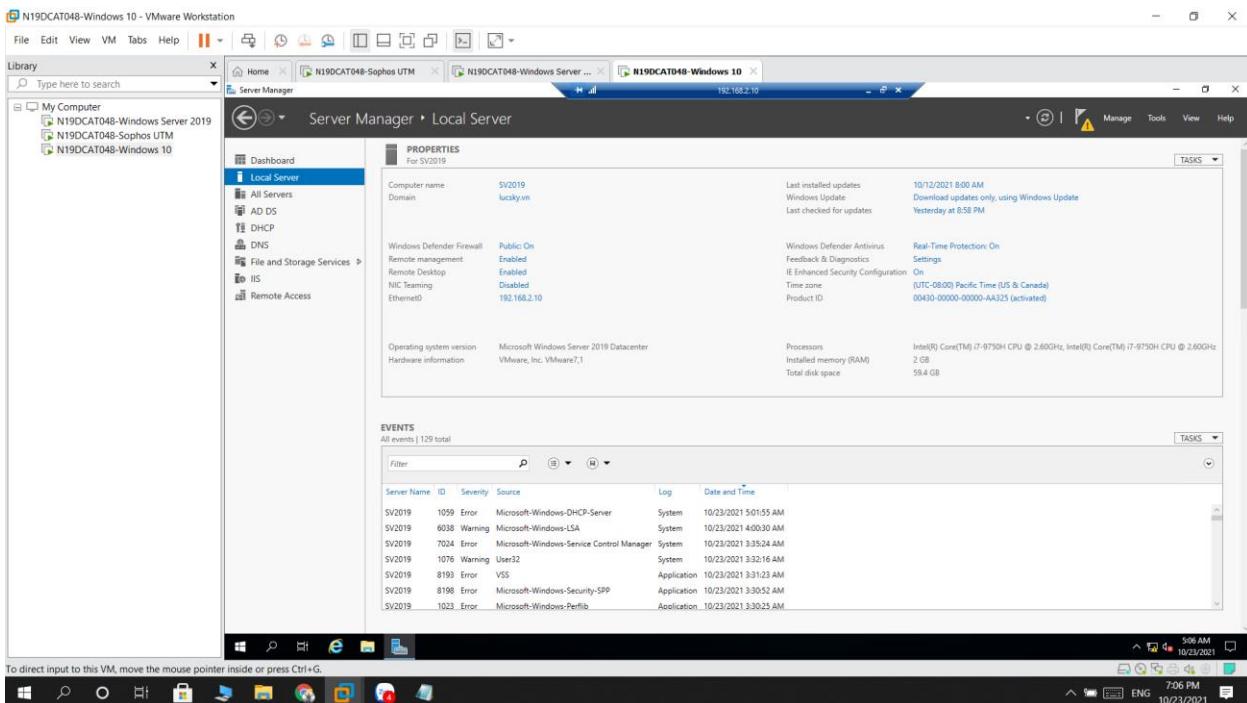
Thực hiện kết nối tới Server



Hình 1. 94: Connection Server



Hình 1. 95 Log acc user được quyền remote

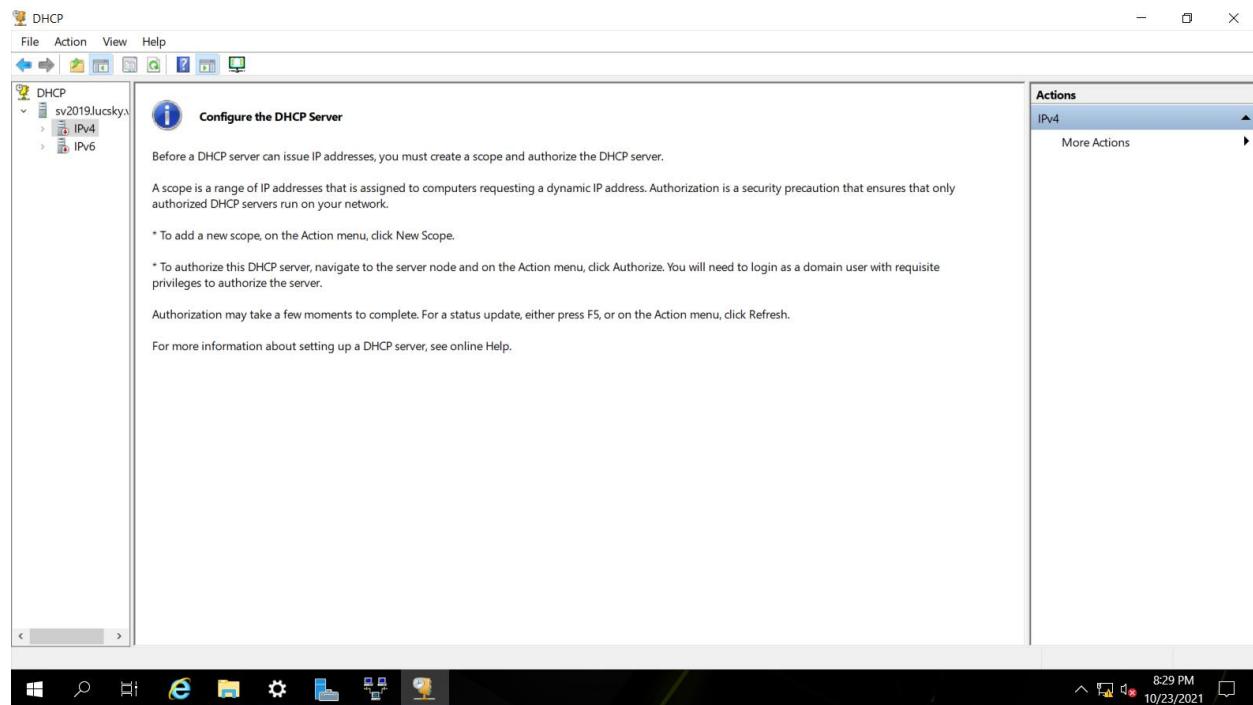


Hình 1. 96 Đã remote được window sever từ máy khác

Cấu hình DHCP sever

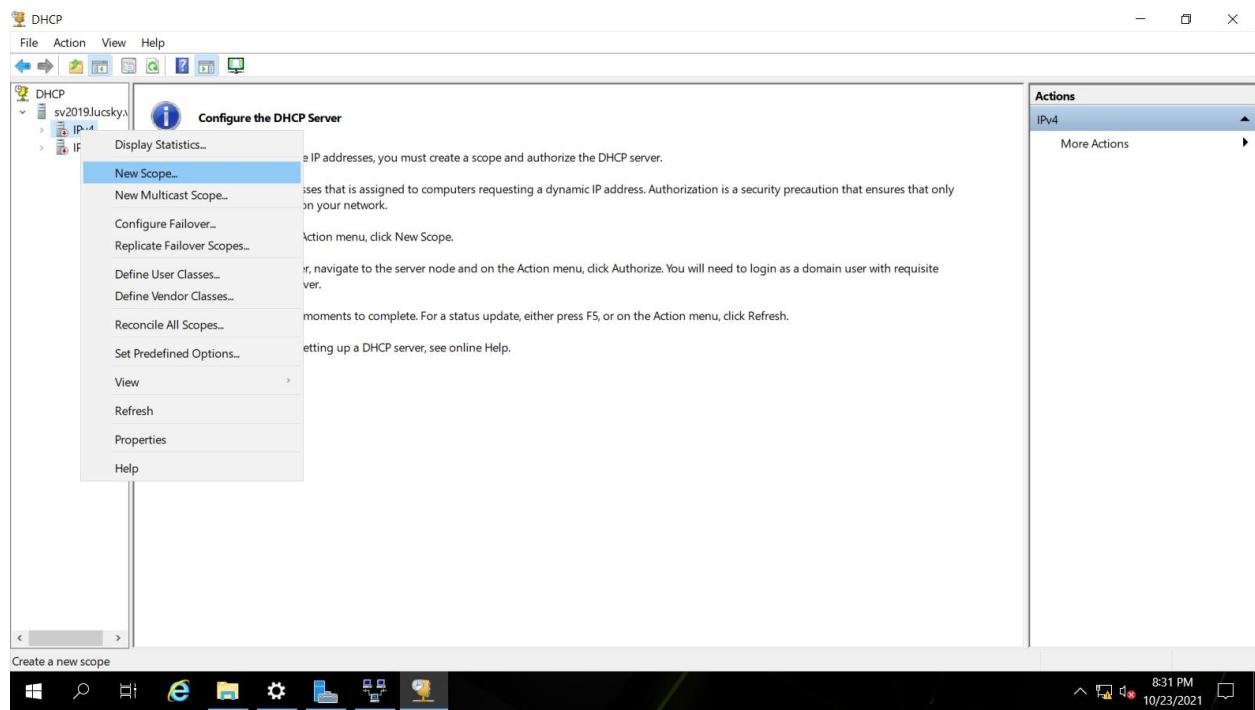
1. Cấu hình scope

Vào server manager chọn tools, mở công cụ DHCP



Hình 1. 97 DHCP console

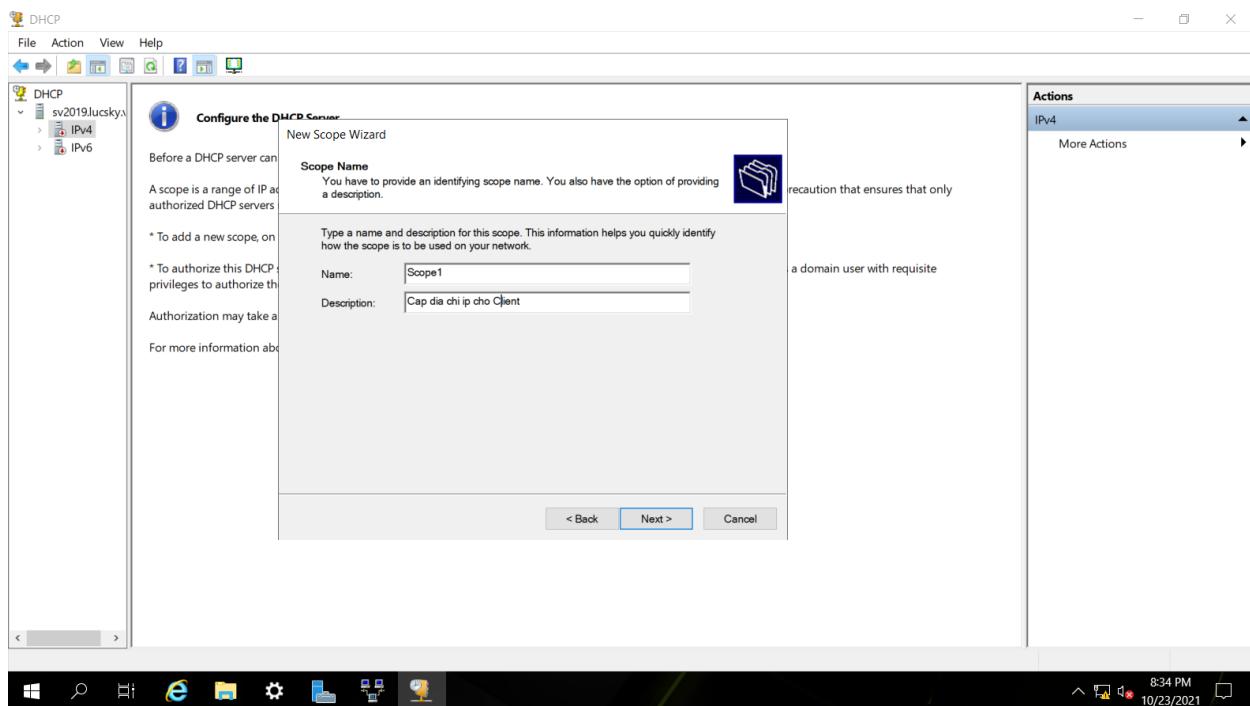
Tạo scope trên DHCP



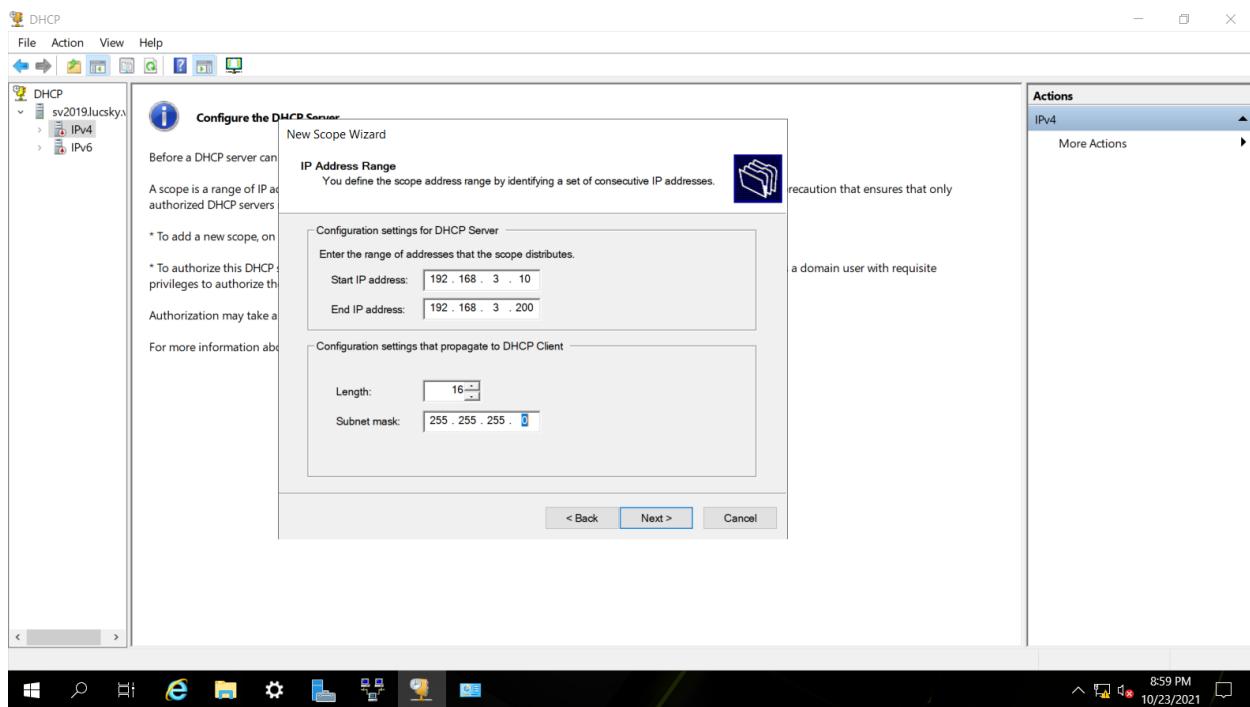
Hình 1. 98 New scope

Màn hình welcome to the New Scope chọn Next

Màn hình Scope Name, nhập Scope1 vào ô Name và
chọn Next

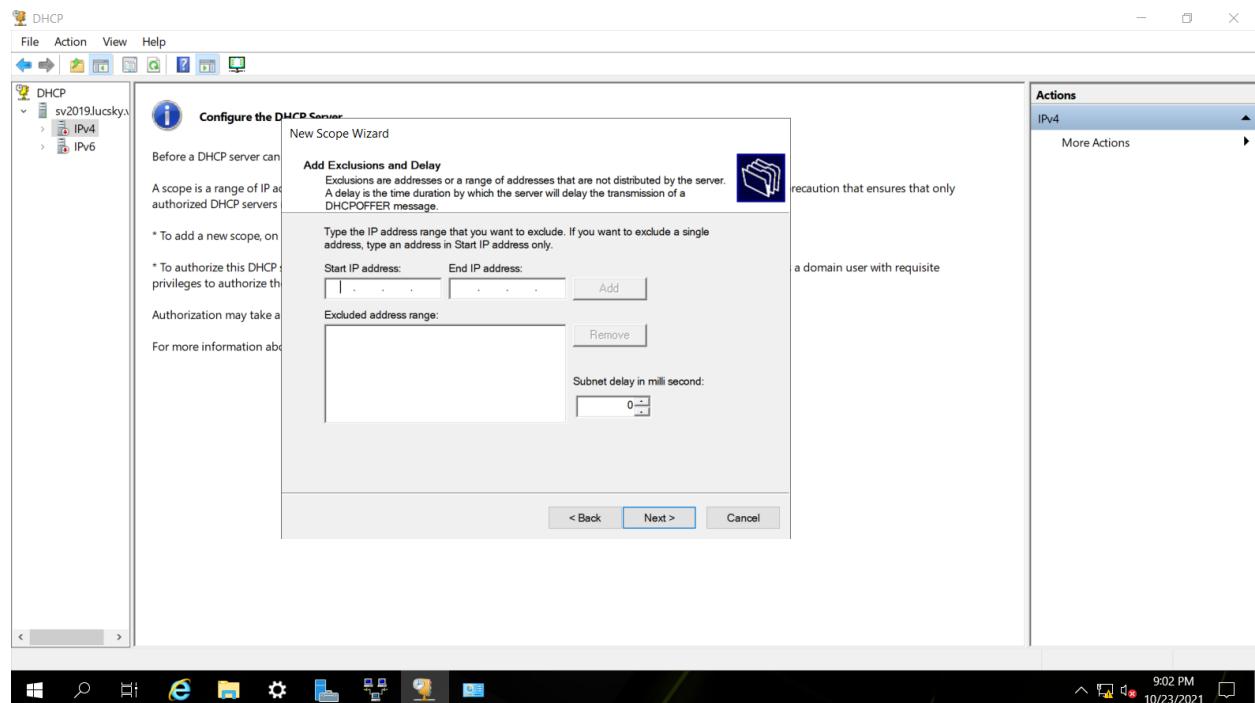


Hình 1.99 Màn hình Scope Name

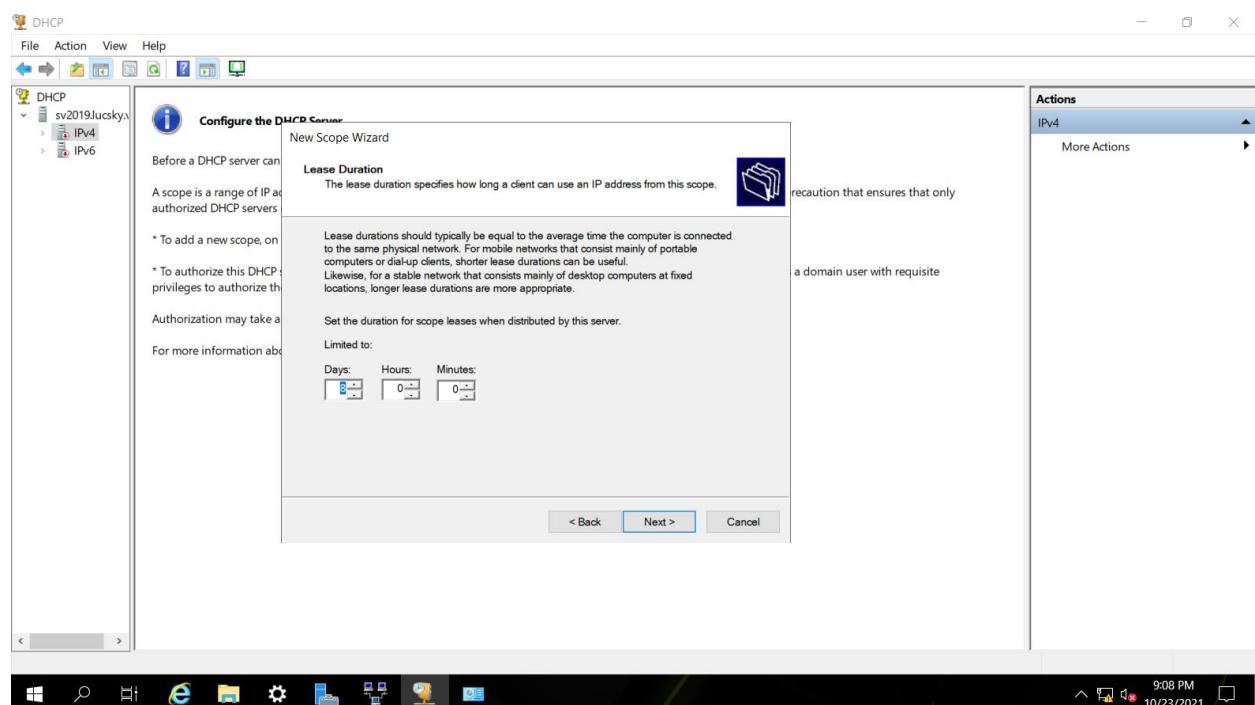


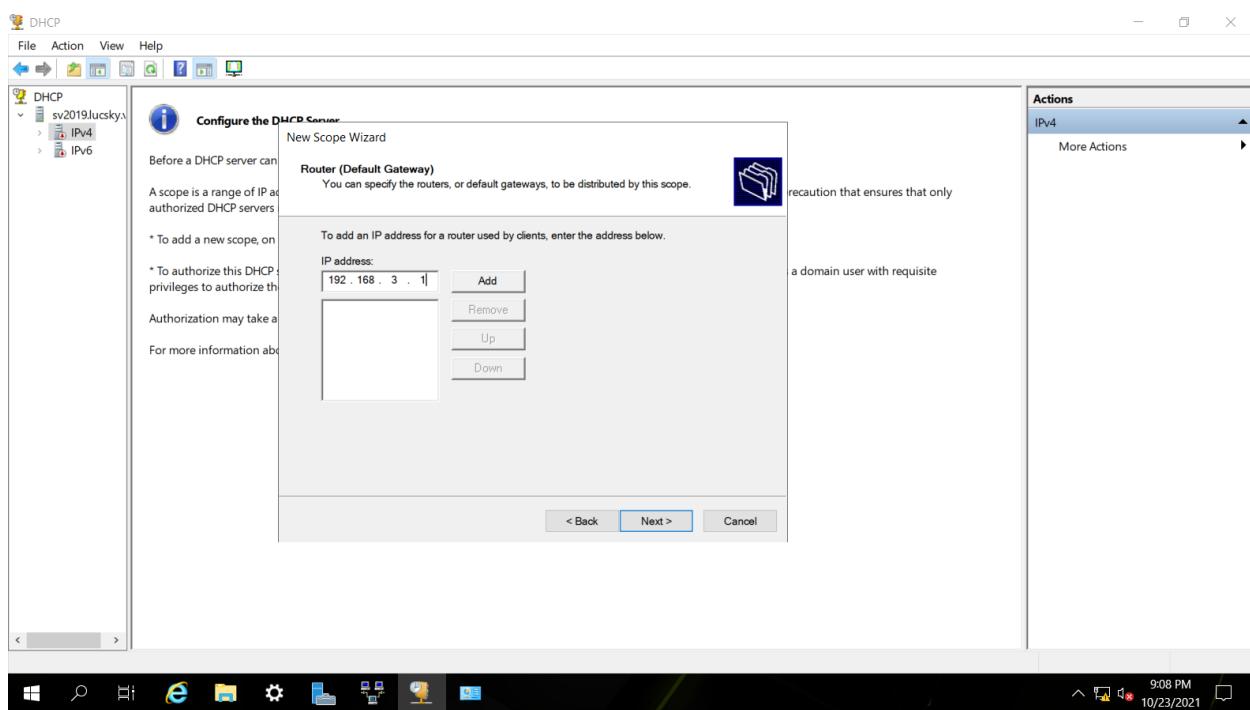
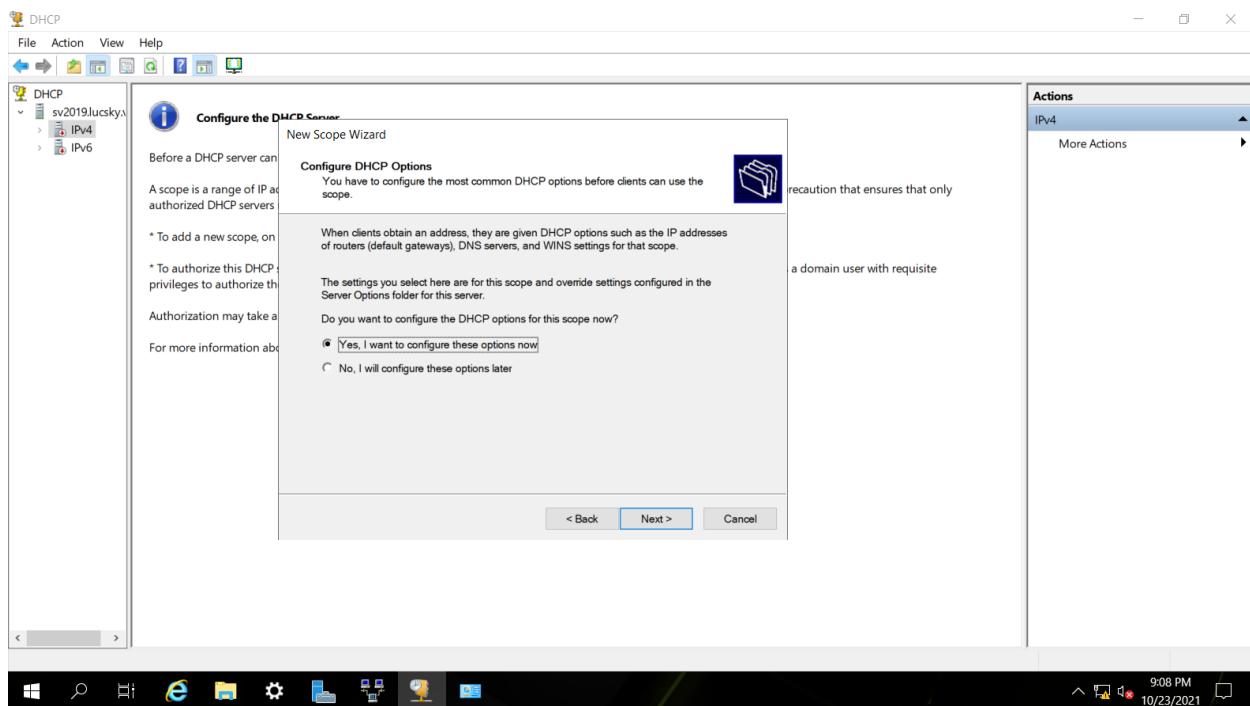
Hình 1.100 Nhập địa chỉ muôn setup, phải đặt chung
lớp mạng với máy sever(subnet mask)

Chọn Next

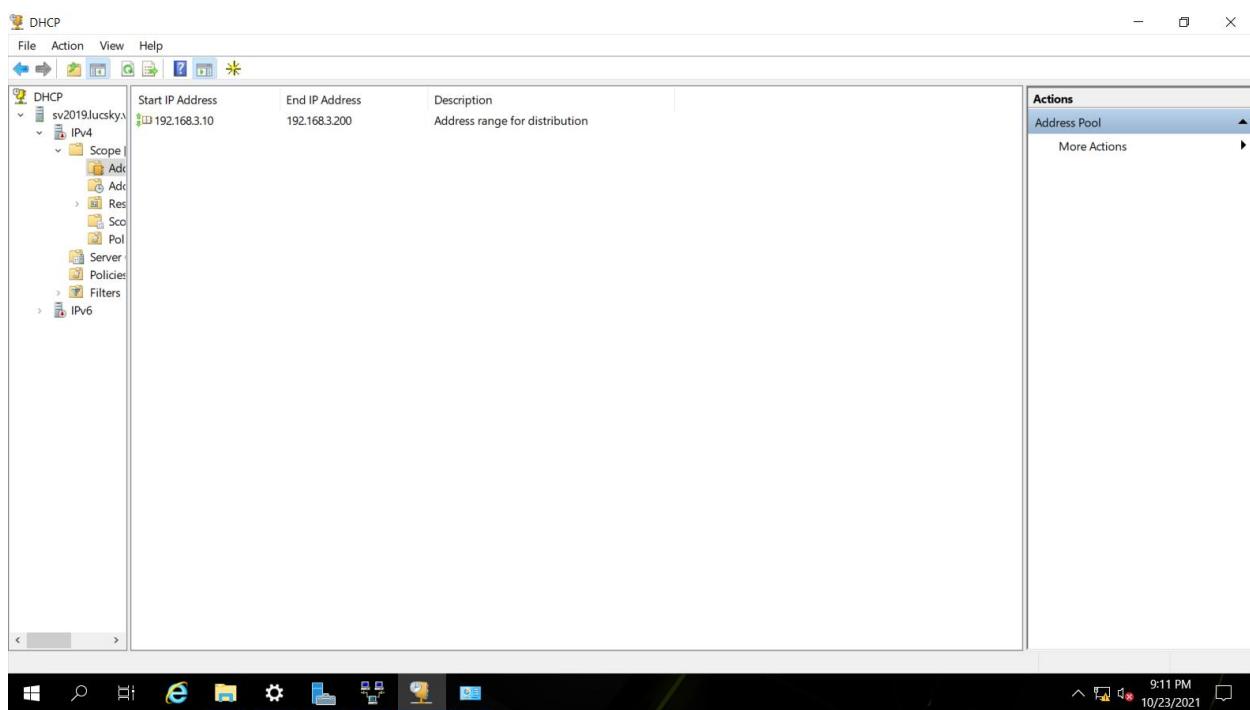
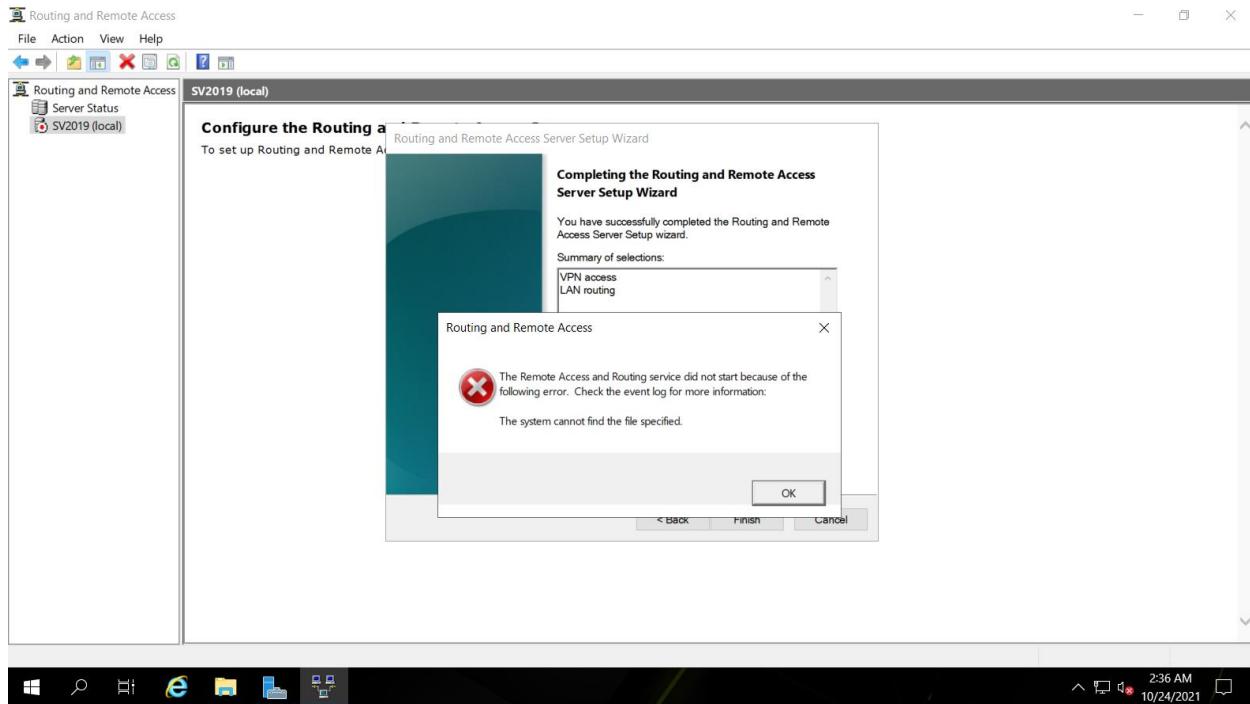


Hình 1. 101 Add Exclusion and delay

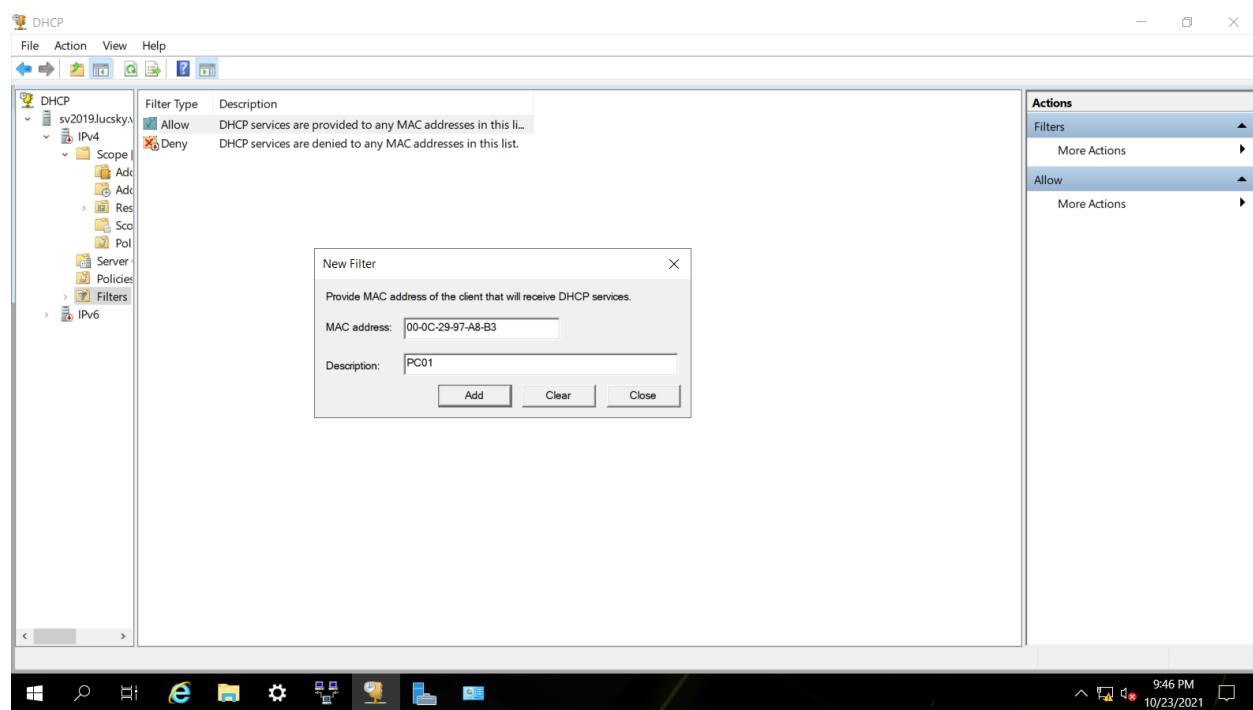
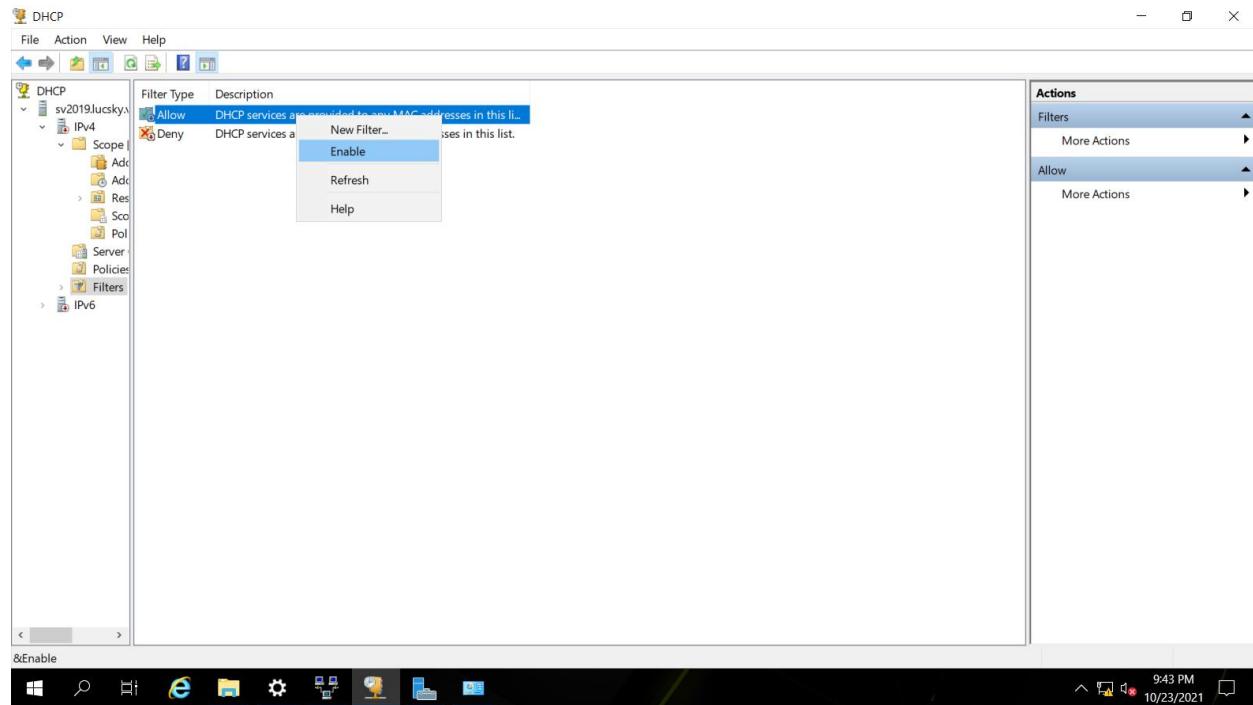


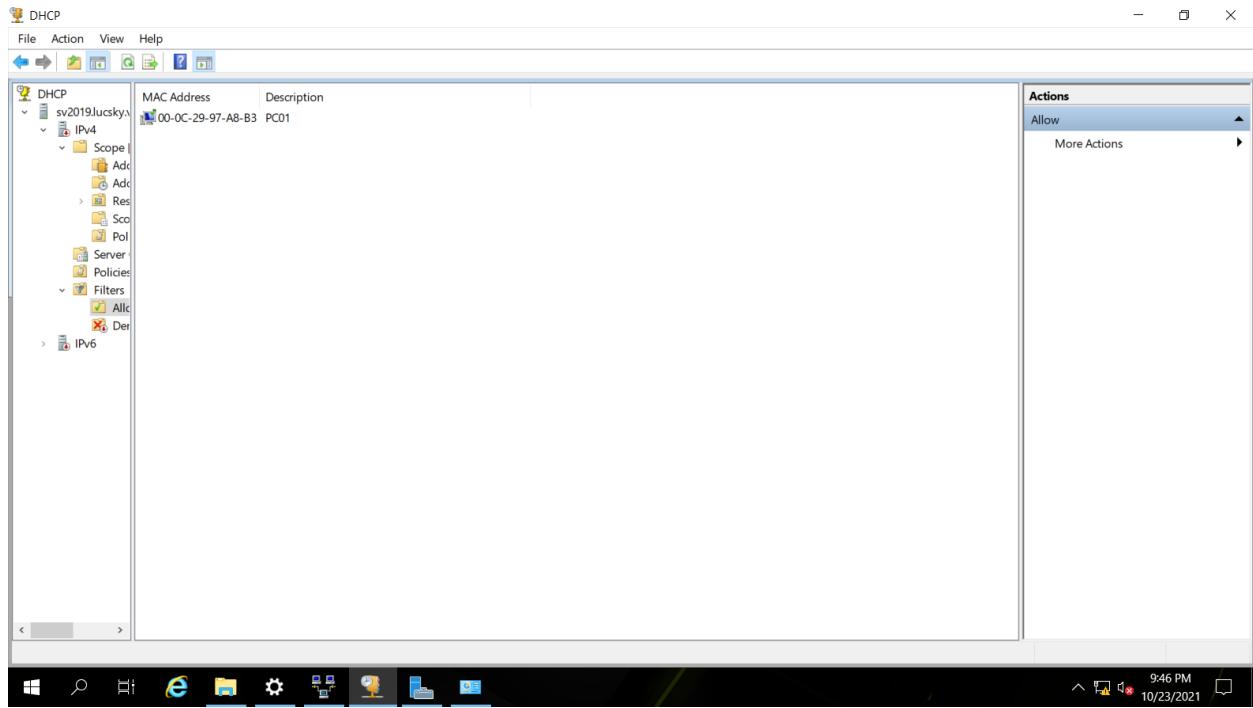


Thực hiện next các lần liên tiếp và chọn finish để kết thúc



Đã cài đặt DHCP thành công



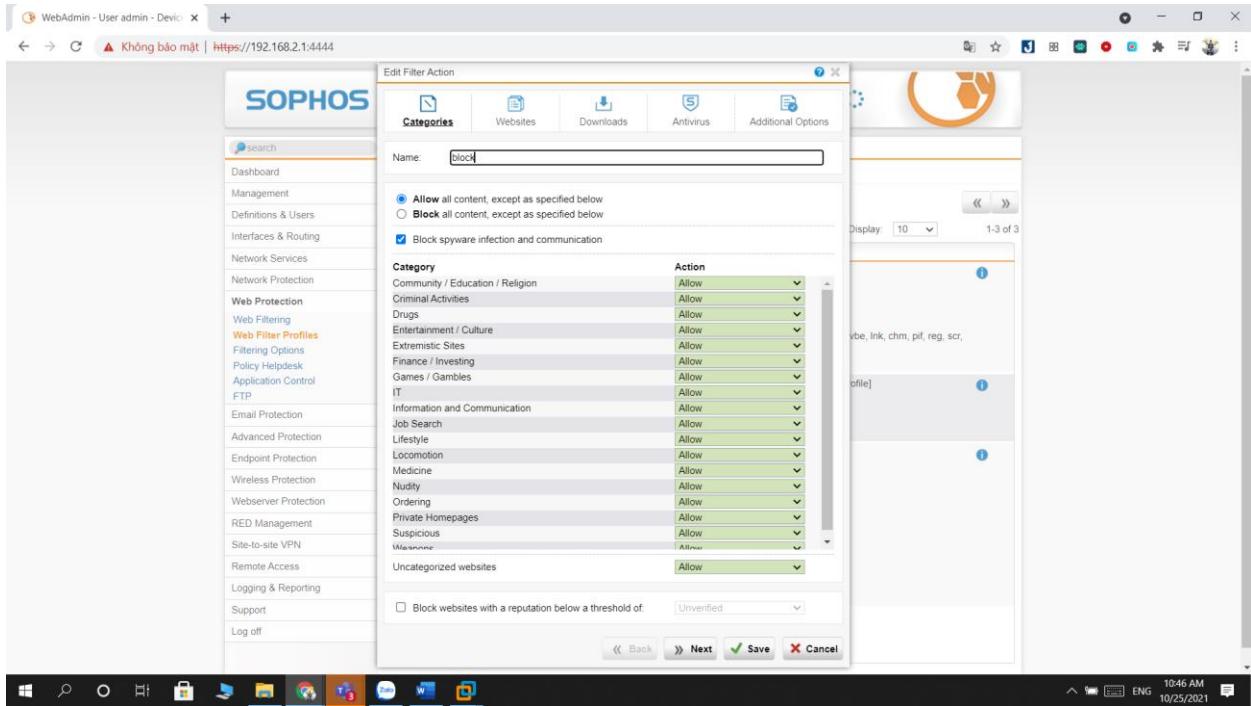


Địa chỉ Mac vừa nhập đã được thêm vào trong phần
cho phép cấp IP

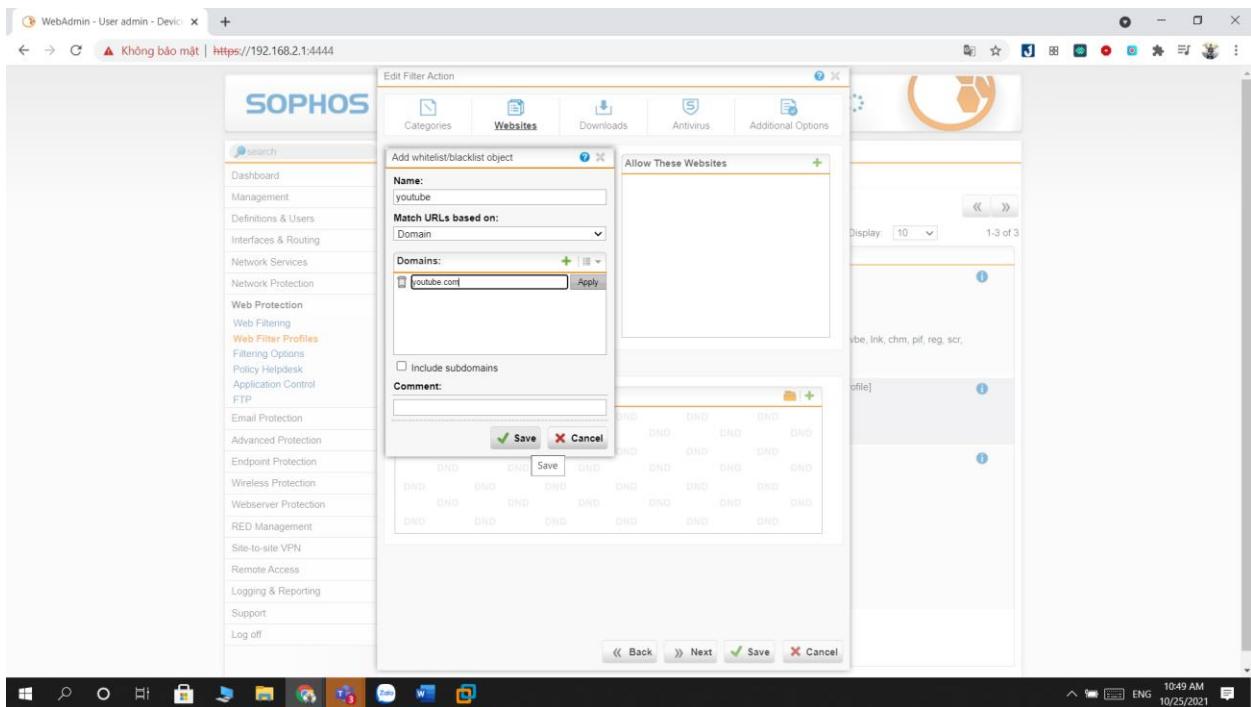
Block web bằng sophos

Vào web filter profiles, chọn new filter action

Đặt tên filter action và chọn next

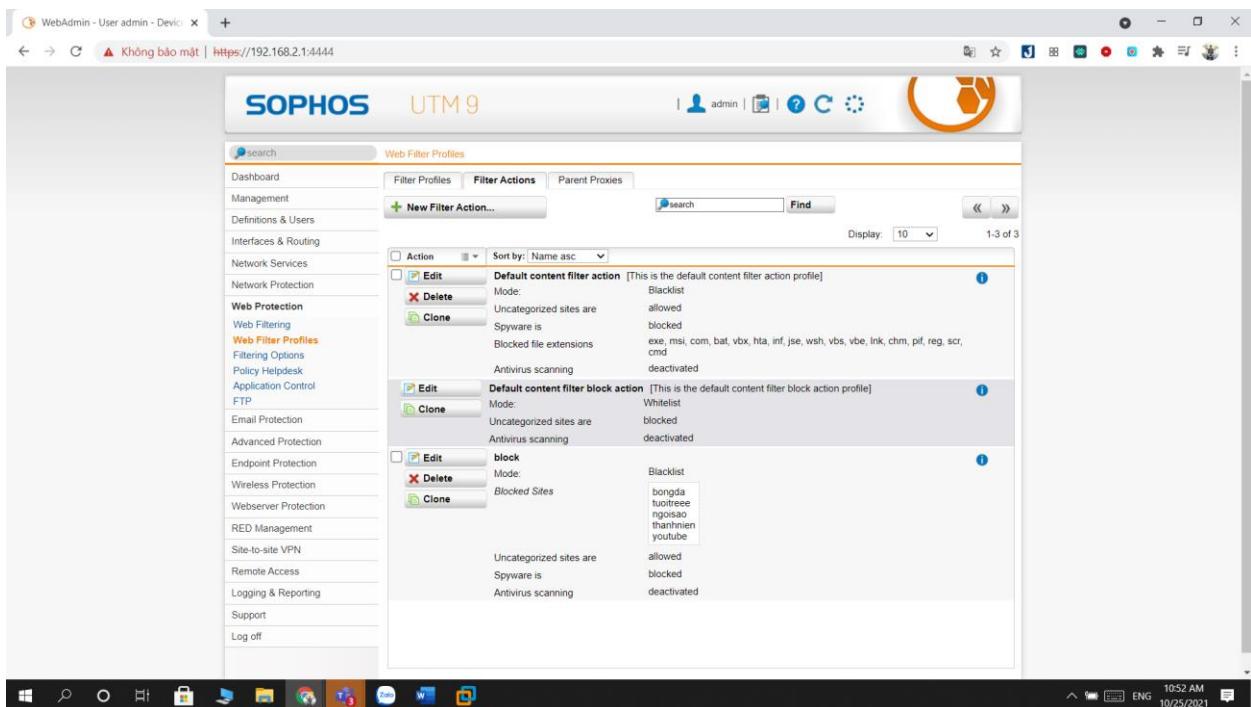
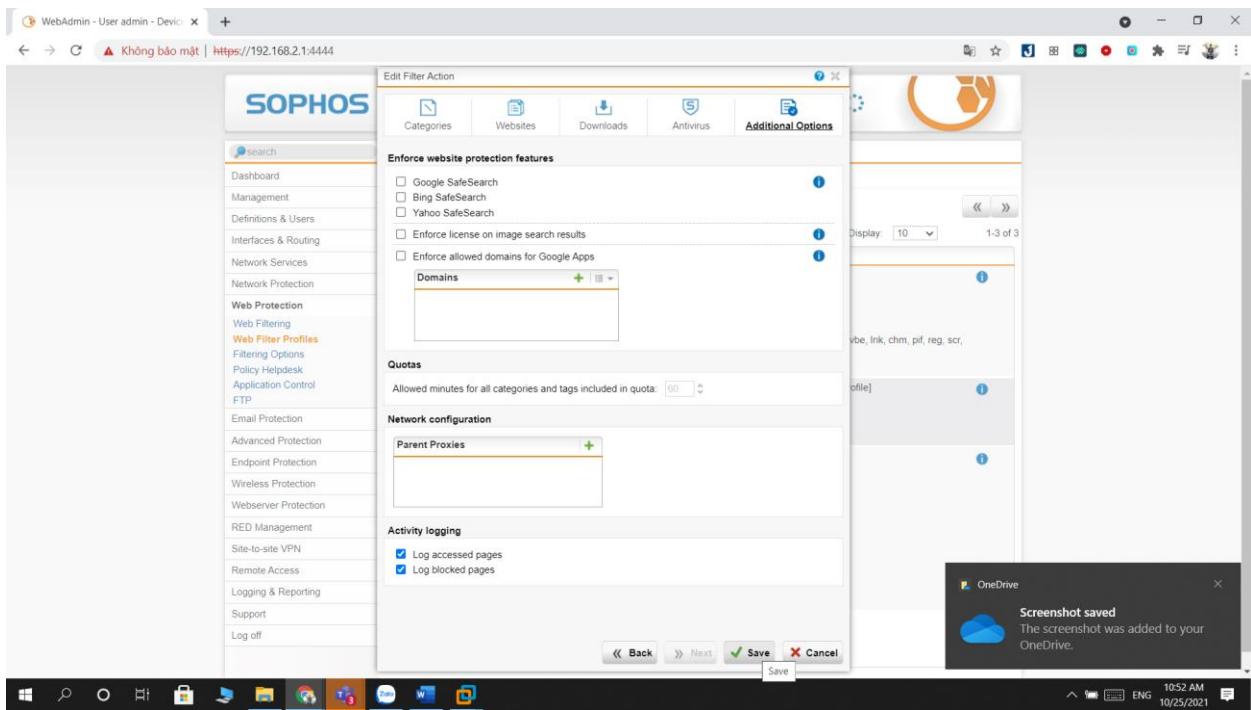


Edit Filter Action



Nhập tên và domain của web muốn chặn

Tiếp tục nhấn apply, save và next 3 lần rồi save lần nữa.



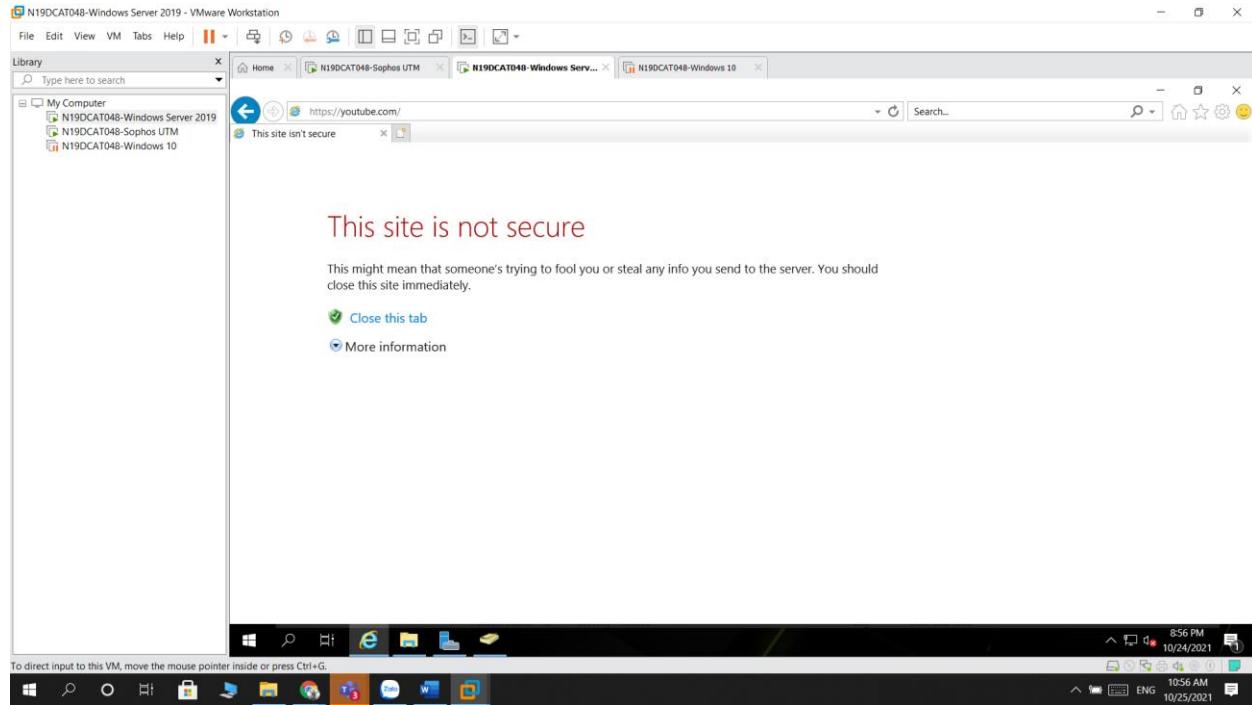
Tạo filter action thành công

The screenshot shows the Sophos UTM 9 Web Filter Profiles configuration page. On the left, a navigation menu includes options like Dashboard, Management, Network Services, Network Protection, Web Protection, Web Filtering, Web Filter Profiles, Filtering Options, Policy Helpdesk, Application Control, FTP, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, Site-to-site VPN, Remote Access, Logging & Reporting, Support, and Log off. The main content area is titled "Web Filter Profiles" and contains tabs for "Filter Profiles", "Filter Actions", and "Parent Proxies". A note states: "Web Filter Profiles allow you to apply a different set of policies to each network. The UTM examines the source IP of each web request, then applies the first profile with a matching allowed network and operation mode." Below this is a table with columns: Active, Name, Allowed networks, Operation mode, Policies, and a status indicator. One row is shown: "1 Block Internal (Network) Transparent Block, Base Policy". A note at the bottom says: "Use the Policy Test tool to confirm that your policy will work as you intended." The system status bar at the bottom right shows "10:53 AM ENG 10/25/2021".

Vào lại filter profiles để enable

The screenshot shows the Sophos UTM 9 Web Filtering Policies configuration page. The left navigation menu is identical to the previous screen. The main content area is titled "Web Filtering" and contains tabs for "Global", "HTTPS", and "Policies". A note states: "Policies are used to apply different Filtering Actions to specific users, groups, or time periods. These policies apply to the Allowed Networks that are on the Global tab. The first policy that matches the user and time will be applied, with the Base Policy applied if no others match." Below this is a table with columns: Active, Name, Users/Groups, Time, Filter action, and a status indicator. Two rows are shown: "1 Block Any Anytime block" (Status: Enabled) and "Base Policy Any Anytime Default content filter action". A note at the bottom says: "Use the Policy Test tool to confirm that your policy will work as you intended." The system status bar at the bottom right shows "10:54 AM ENG 10/25/2021".

Tiếp tục vào public của web filtering để enable



Đã block web youtube.com trên window server bằng sophos thành công.

KẾT LUẬN

- Kết quả nghiên cứu đề tài có thêm nhiều phương pháp xây dựng hệ thống mạng doanh nghiệp góp phần làm cho hệ thống an toàn và dễ dàng quản trị hơn.
- Nâng được tổng quan về xây dựng và phát triển hệ thống, bảo mật hệ thống mạng.
- Hiểu thêm được về công nghệ VPN, VPN Server, các chính sách áp dụng cho người dùng trong Domain Controller.
- Thực hiện được yêu cầu thiết lập, cài đặt và cấu hình về Domain Controller, Remote Access VPN, SOPHOS Firewall.