

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN 2

-----oO¤¤¤Oo-----



BÁO CÁO GIỮA KỲ

Môn học

Hệ Điều Hành Windows & Linux

Giảng viên : Đàm Minh Linh

Sinh viên thực hiện: Trần Quốc Trưởng

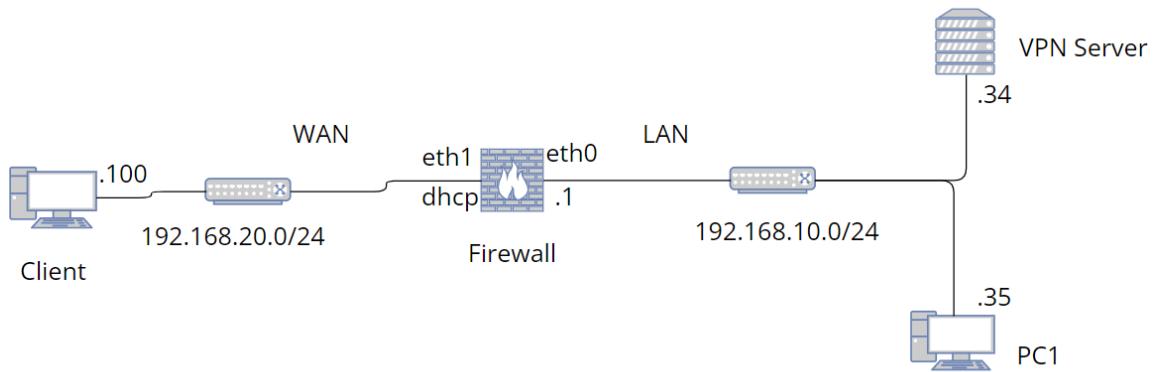
MSSV : N18DCAT100

TP.HCM, tháng 10/2022

MỤC LỤC

1. Sơ đồ mạng	1
2. Triển khai hệ thống	2
2.1. Cài đặt domain controller	2
2.2. Cài đặt firewall Sophos	13
2.3. Cấu hình chính sách Sophos chặn user truy cập facebook	21
2.4. Cài đặt và cấu hình vpn server	26
2.5. Cấu hình cho phép admin remote desktop	39
2.6. Cấu hình cho phép user1 remote desktop vào PC1	42
2.7. Cài đặt và cấu hình DHCP server trên Windows Server.....	48

1. Sơ đồ mạng



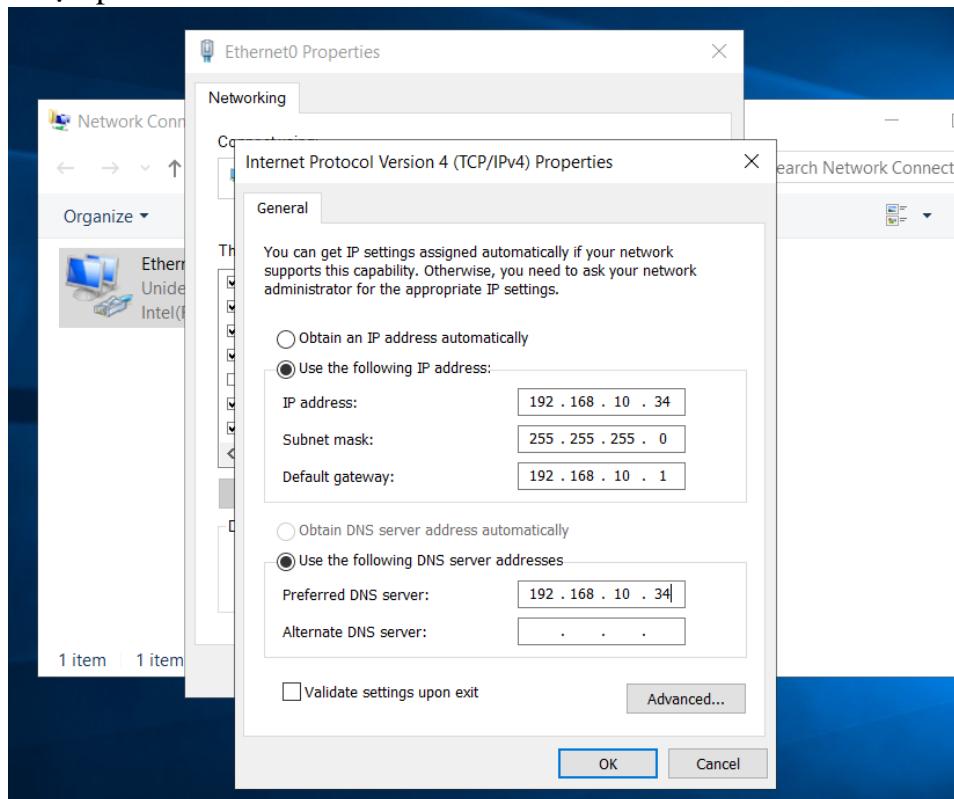
Trong đó:

Tên thiết bị	Thông tin	Interface 1	Interface 2
Client	Windows 11 máy thật	Ip address	192.168.20.100
		Netmask	/24
		Default Gateway	
		DNS	
Firewall	Sophos UTM 9.6	Ip address	dhcp
		Netmask	/24
		Default Gateway	
		DNS	
VPN Server	Windows Server 2019	Ip address	192.168.10.34
		Netmask	/24
		Default Gateway	192.168.10.1
		DNS	192.168.10.34
PC1	Windows 10 pro	Ip address	192.168.10.35
		Netmask	/24
		Default Gateway	192.168.10.1
		DNS	192.168.10.34

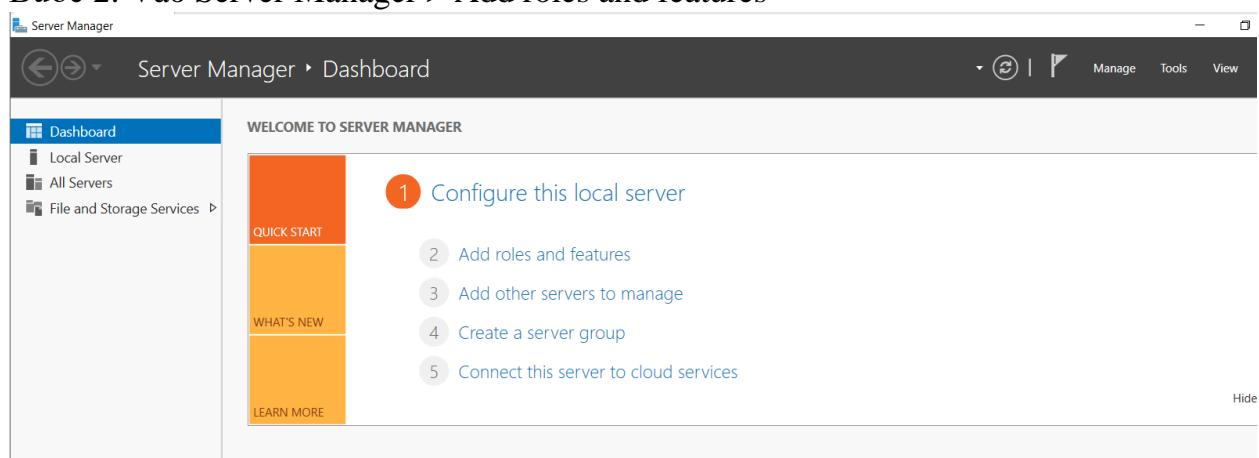
2. Triển khai hệ thống

2.1. Cài đặt domain controller

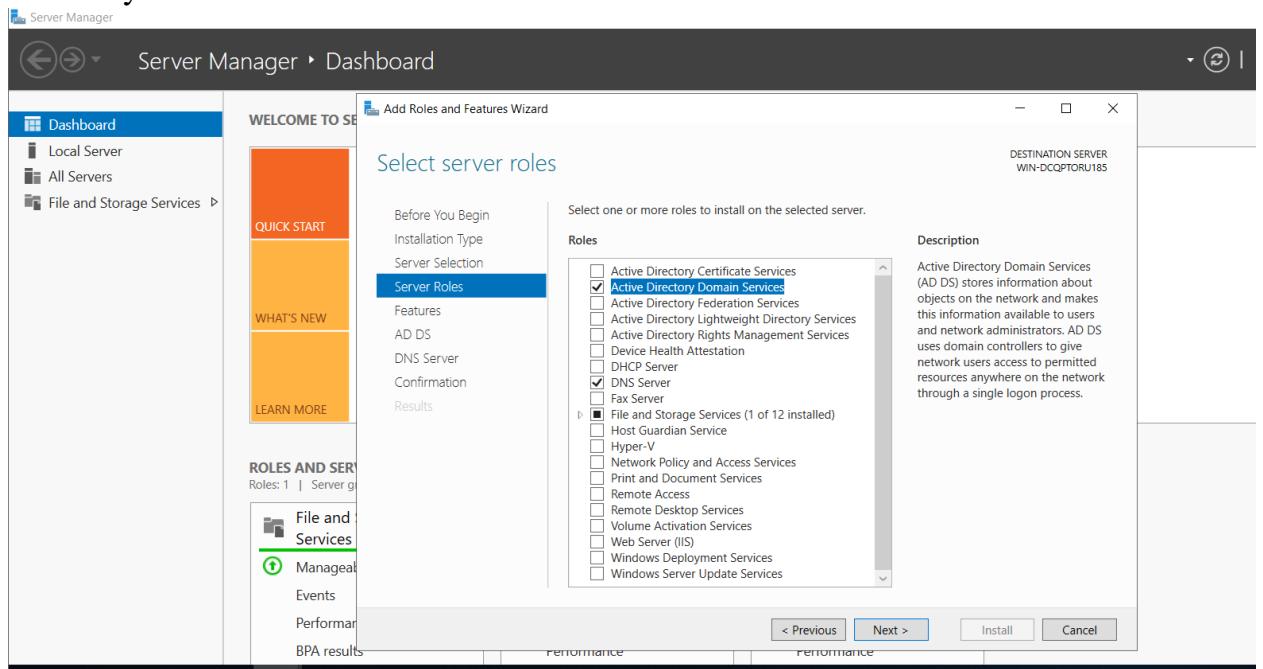
- Bước 1: Đặt ip cho domain



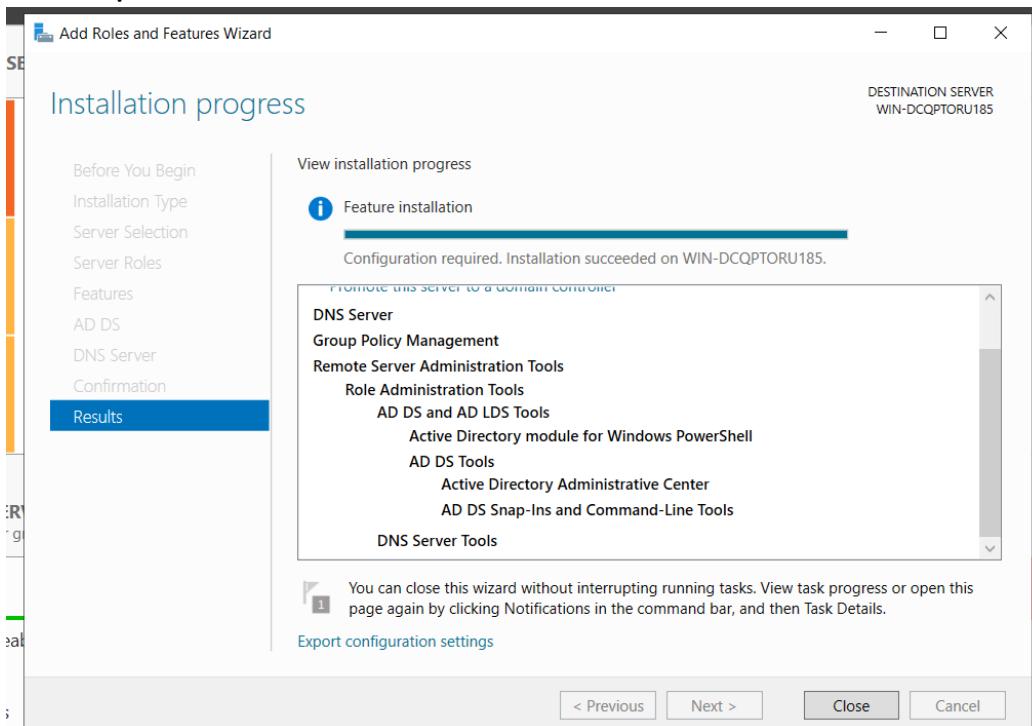
- Bước 2: Vào Server Manager > Add roles and features



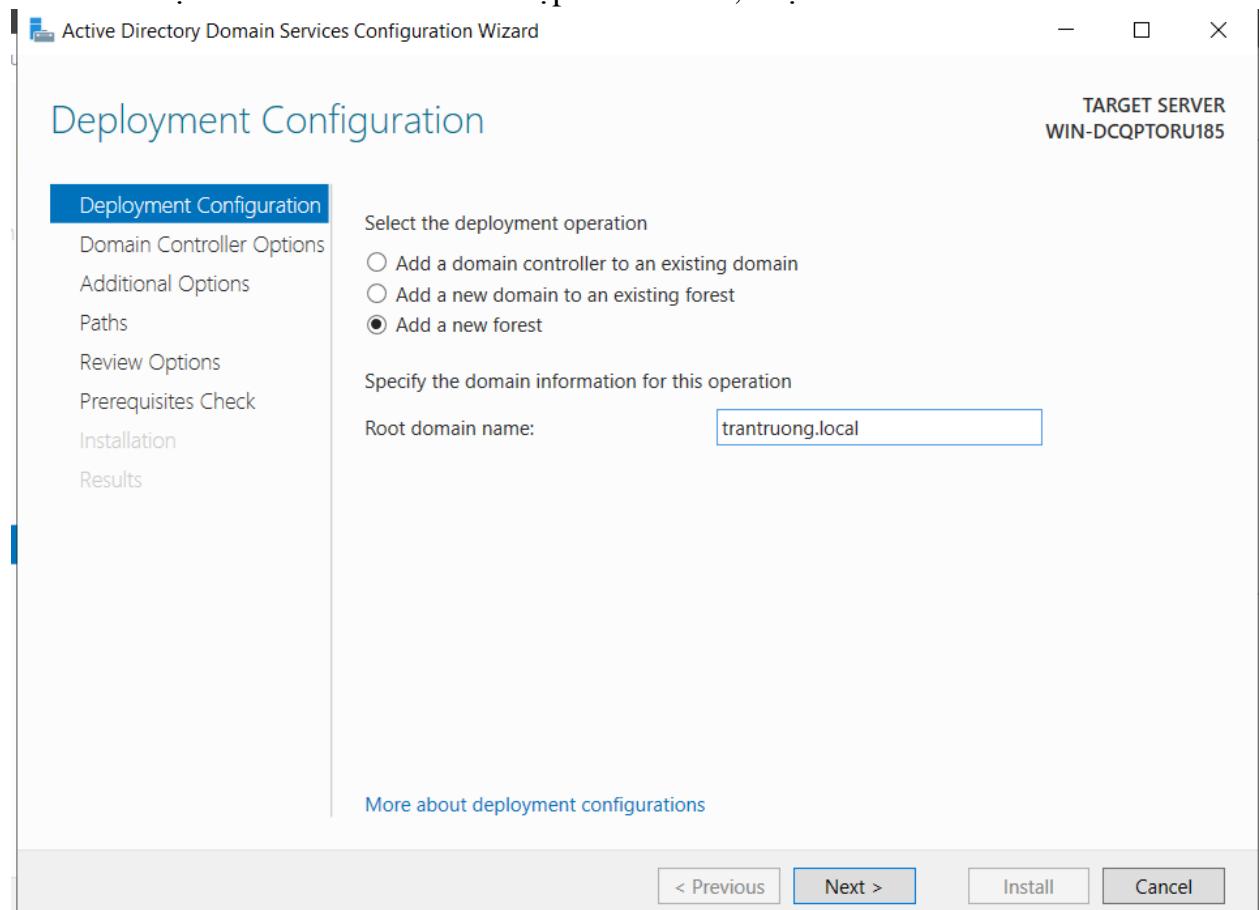
- Bước 3: Bấm Next cho đến khi xuất hiện cửa sổ dưới thì tích chọn Active Directory Services



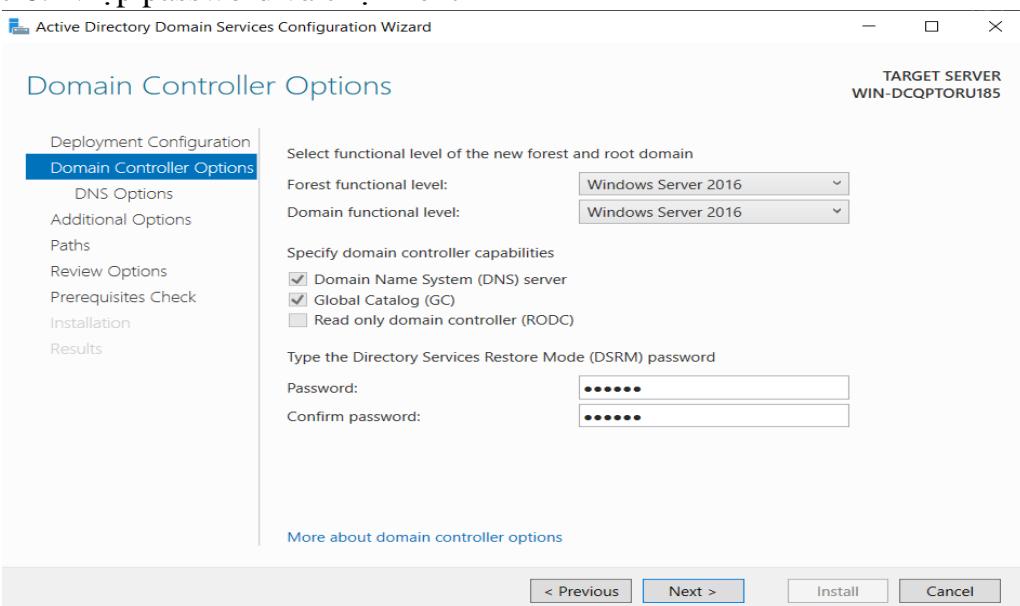
- Bước 4: Chọn Promote this server to a domain controller



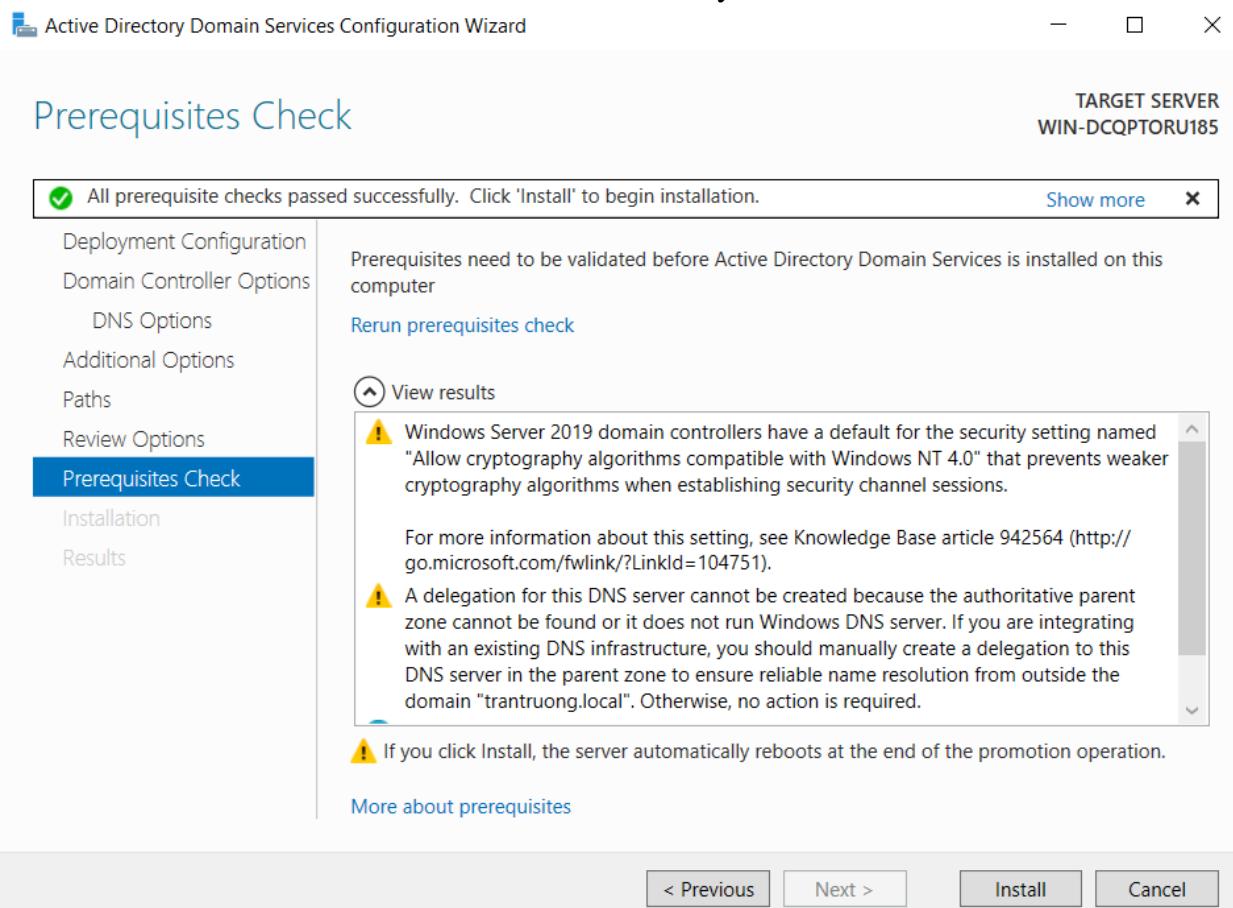
- Bước 5: Chọn Add a new forest và nhập tên domain, chọn next



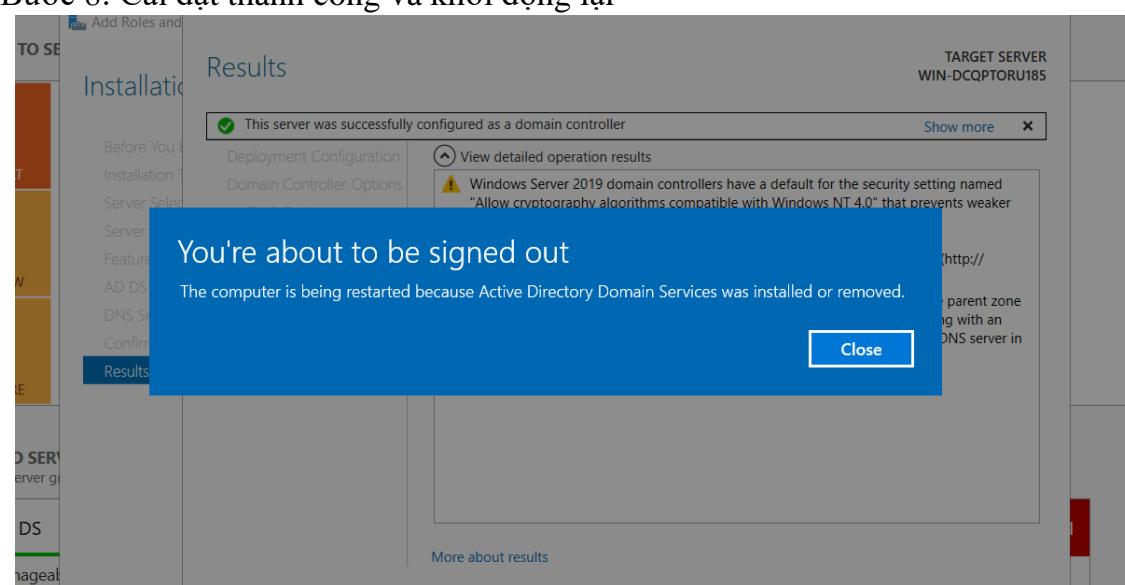
- Bước 6: Nhập password và chọn next



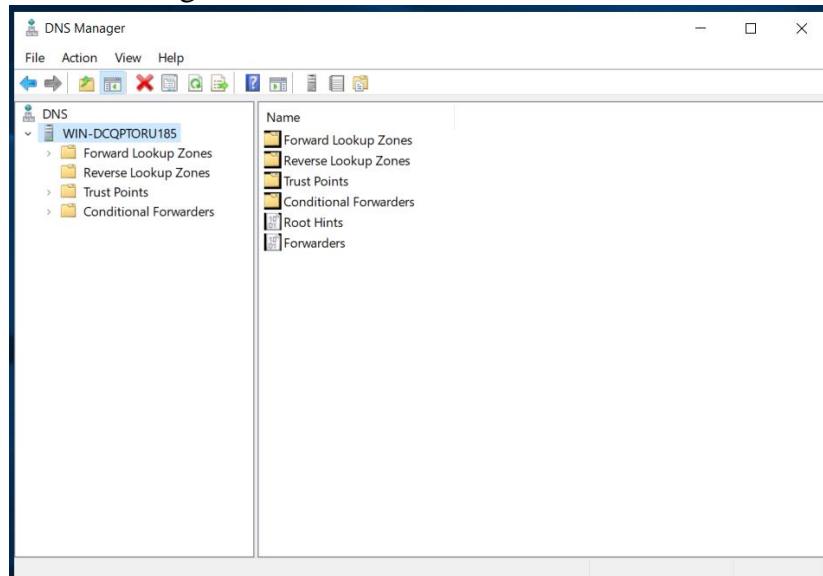
- Bước 7: Chọn Next cho đến khi xuất hiện cửa sổ này thì bấm Install



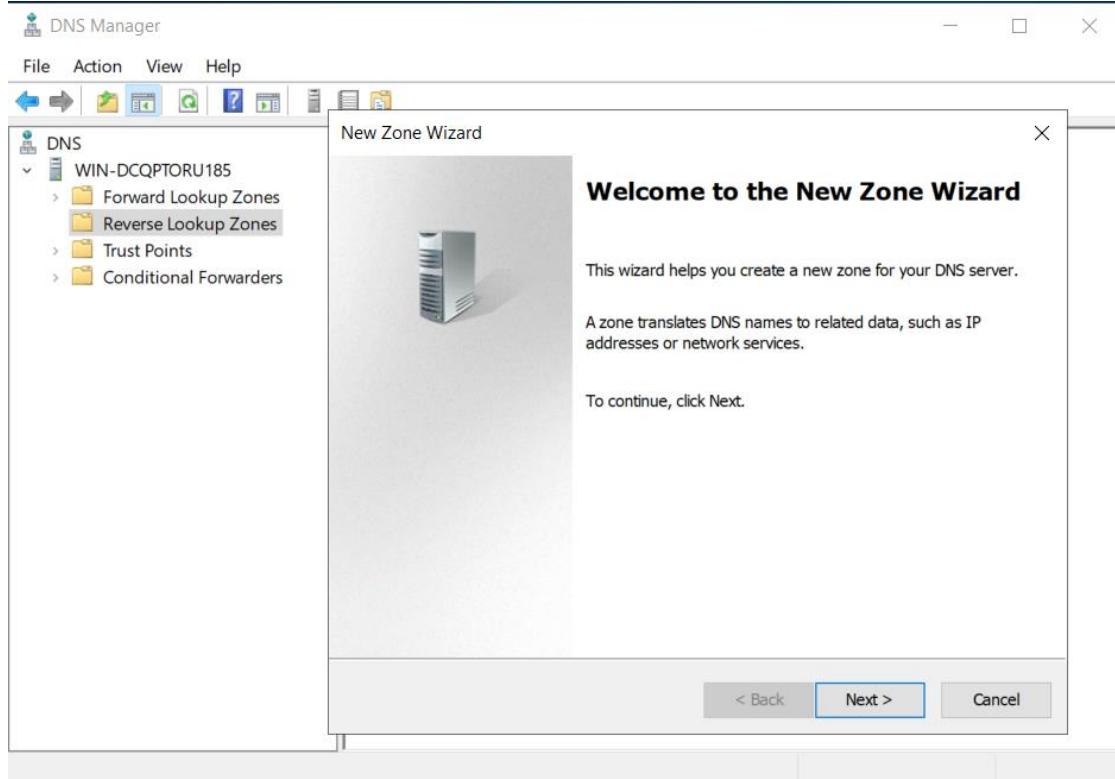
- Bước 8: Cài đặt thành công và khởi động lại



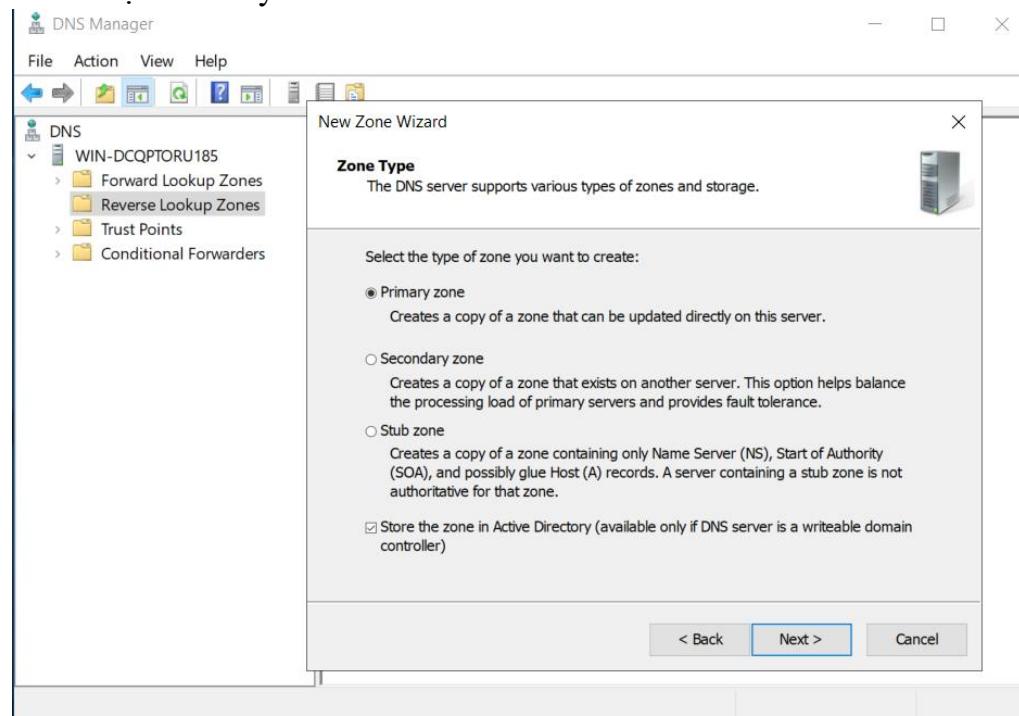
- Bước 9: Mở DNS Manager



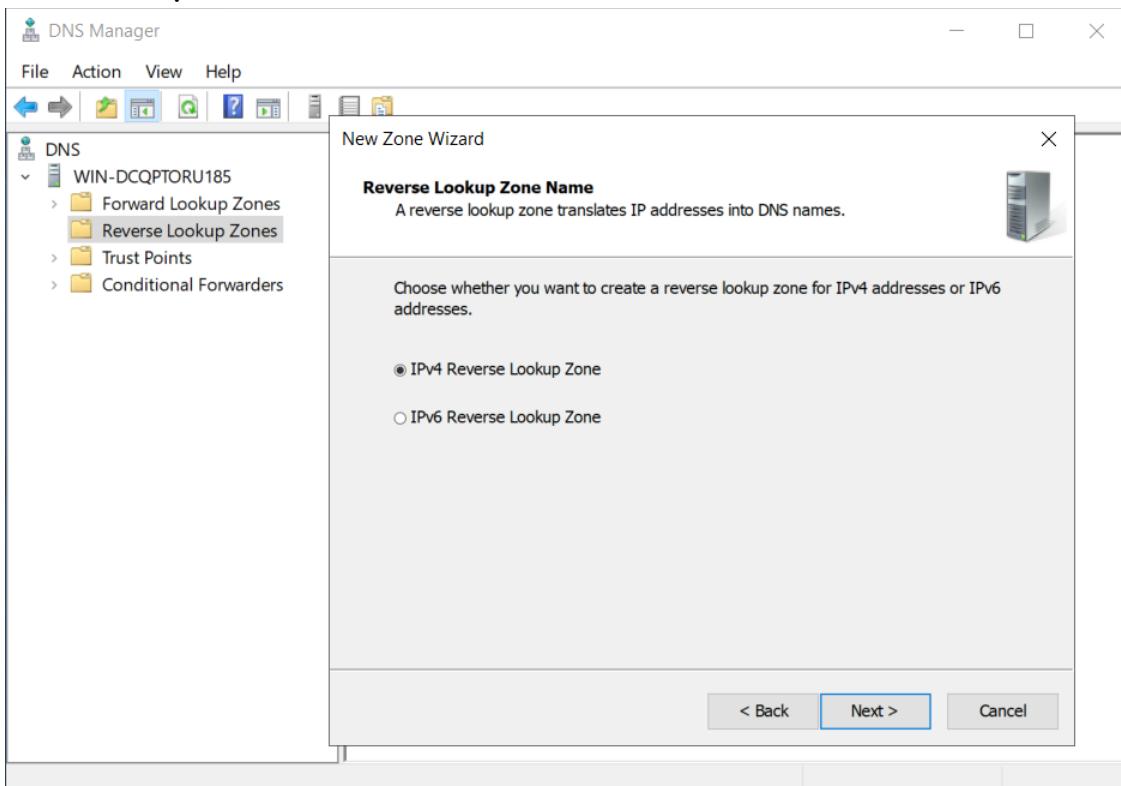
- Bước 10: Click chuột phải vào Reverse Lookup Zones và chọn New Zone



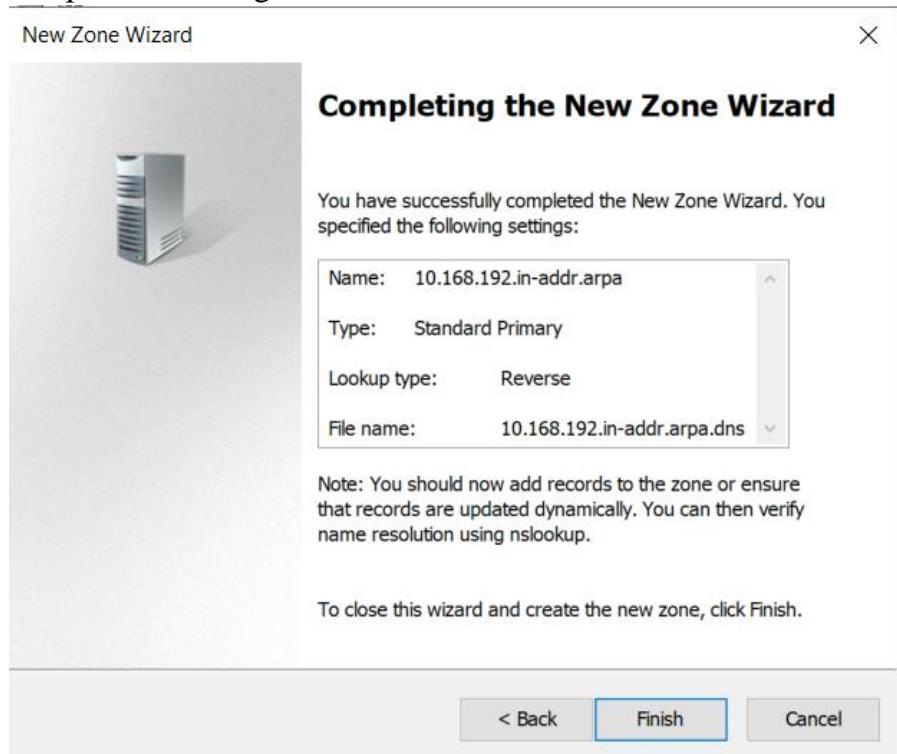
- Bước 11: Chọn Primary zone và bấm Next



- Bước 12: Chọn IPv4 và bấm Next



- Bước 13:Nhập địa chỉ mạng của server, chọn OK, Chọn Finish



- Bước 14: Cập nhật lại DNS

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
PS C:\Users\Administrator>

```

- Bước 15: Tạo DNS thành công

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2], win-dcqptoru185.trantr...	static
(same as parent folder)	Name Server (NS)	win-dcqptoru185.trantru...	static
192.168.10.34	Pointer (PTR)	WIN-DCQPTORU185.trantr...	10/11/2022 1:00:00

- Bước 16: Kết quả kiểm tra

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> nslookup
Default Server: localhost
Address: 127.0.0.1

> exit
PS C:\Users\Administrator> nslookup
Default Server: localhost
Address: 127.0.0.1

> trantruong.local
Server: localhost
Address: 127.0.0.1

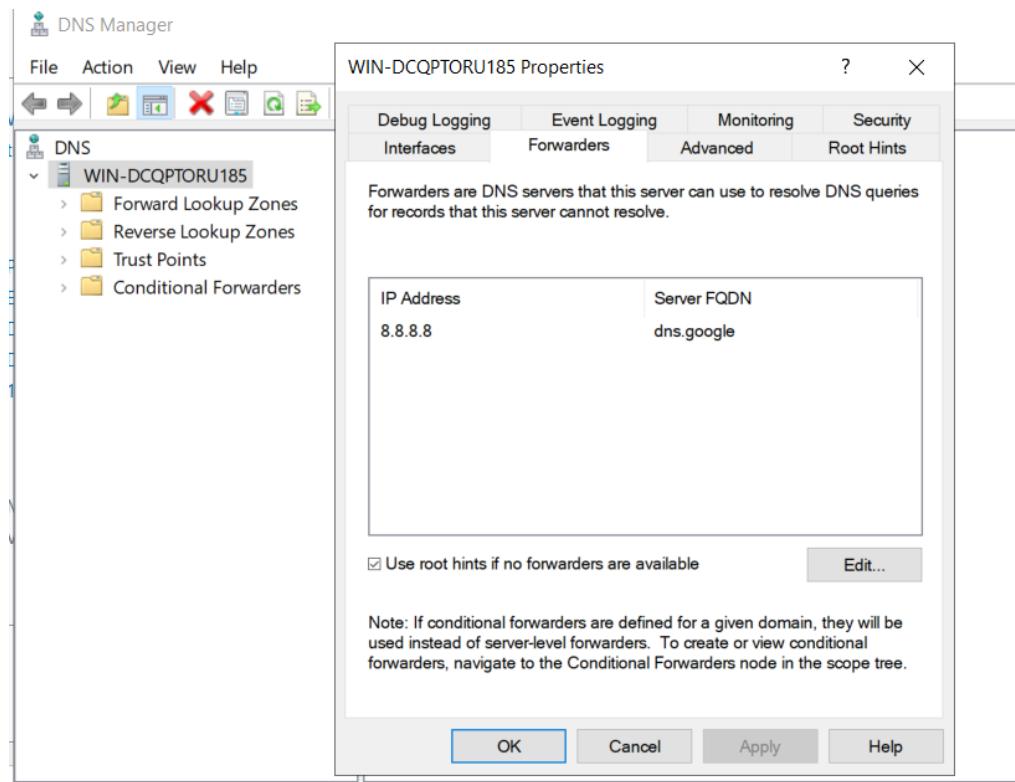
Name:   trantruong.local
Address: 192.168.10.34

> 192.168.10.34
Server: localhost
Address: 127.0.0.1

Name:   WIN-DCQPTORU185.trantruong.local
Address: 192.168.10.34

> -
```

- Bước 17: Chuột phải vào server chọn property > Chọn tab Forwarders > Bấm Edit > Chọn Add > Nhập 8.8.8.8 > Bấm OK > Apply > OK

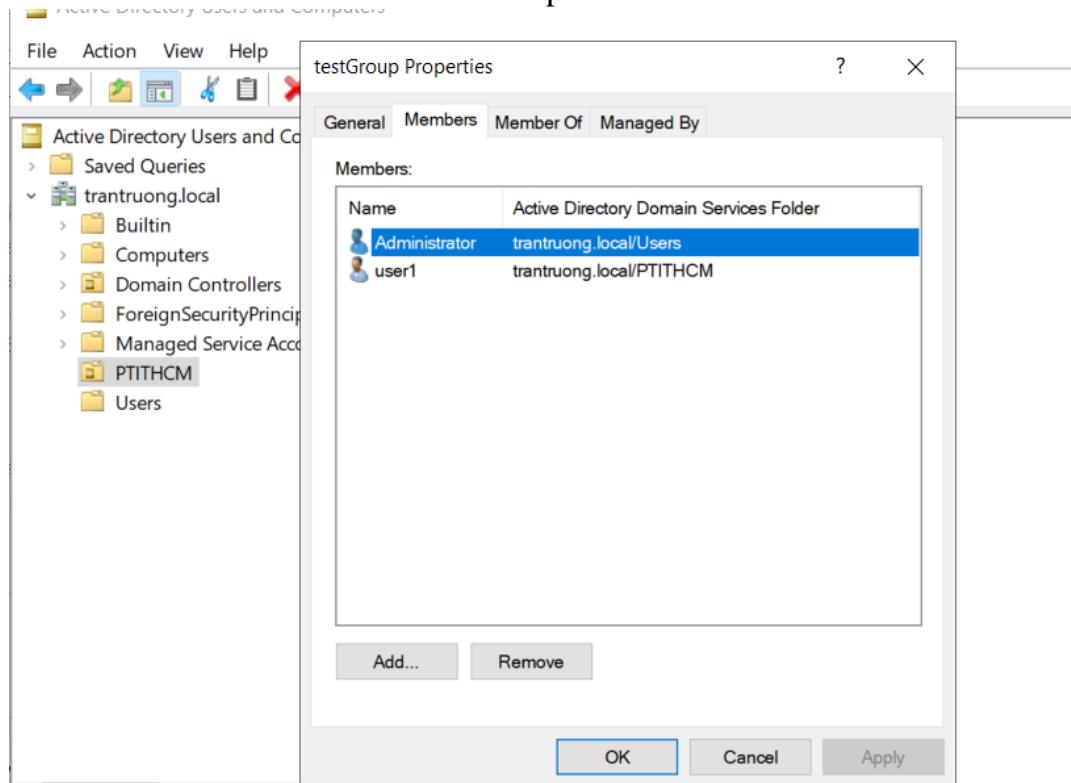


- Bước 18: Vào Server Manager > Tools > Active Directory Users and Computers > Tạo User và group như sau

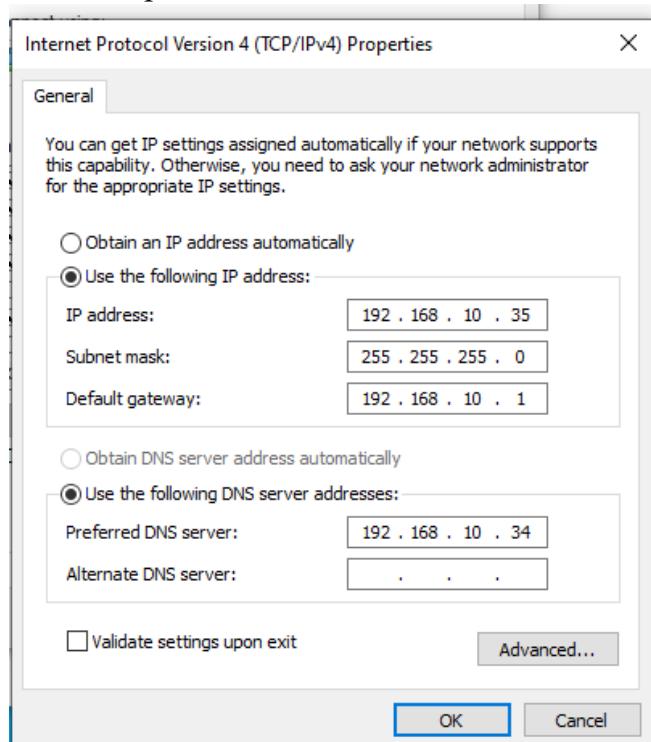
Active Directory Users and Computers

Name	Type	Description
testGroup	Security Group ...	
user1	User	

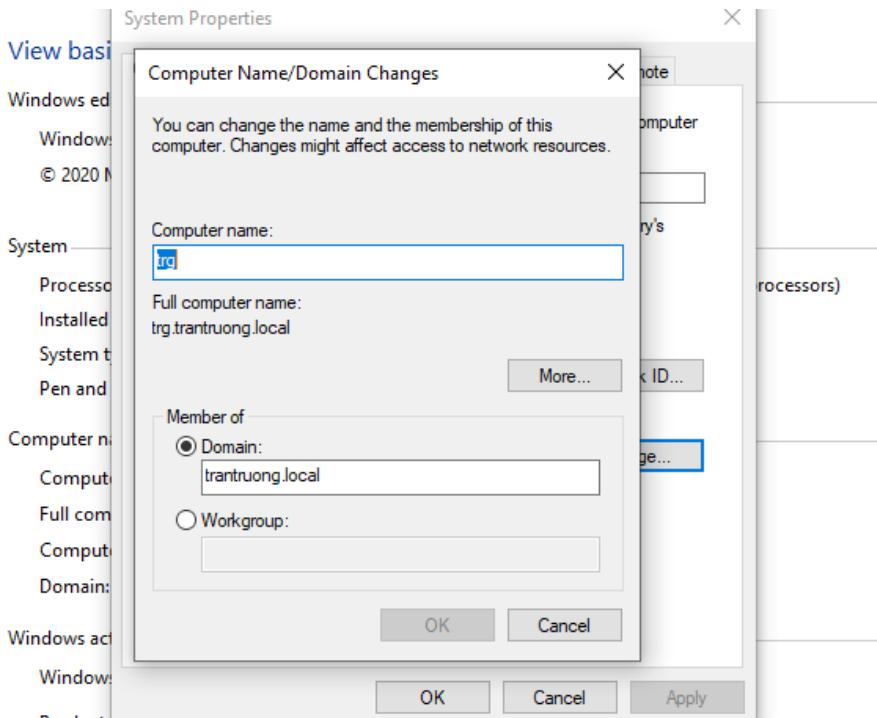
- Bước 19: Thêm user1 và admin vào Group



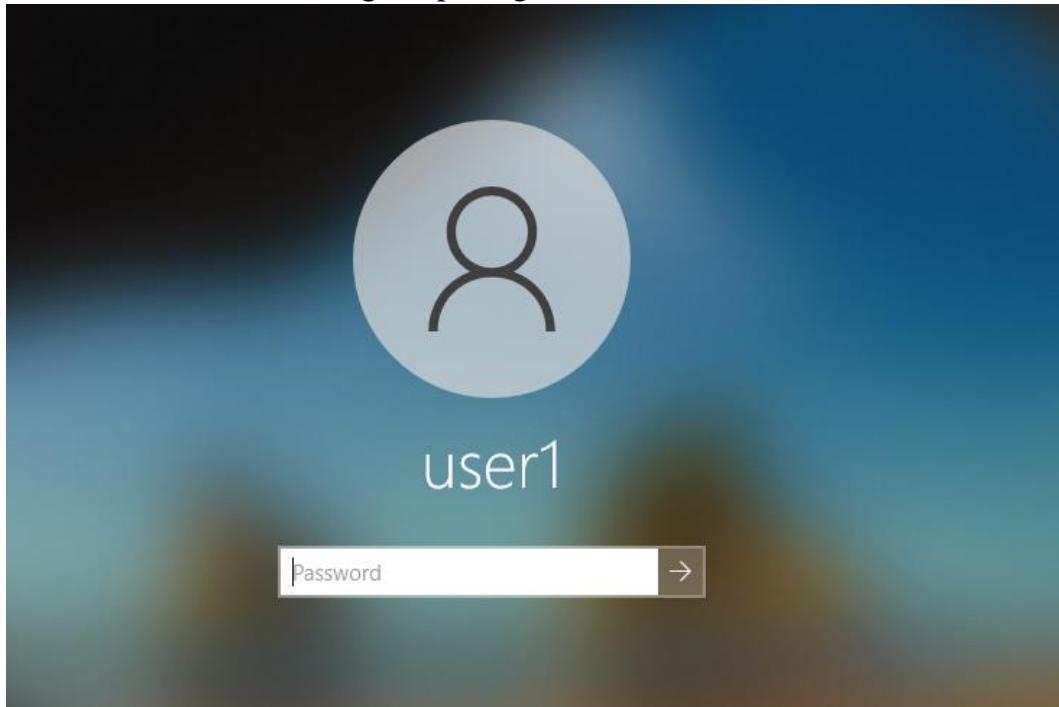
- Bước 20: Trên PC1 đặt lại ipv4 như sau



- Bước 21: Thêm PC1 vào domain

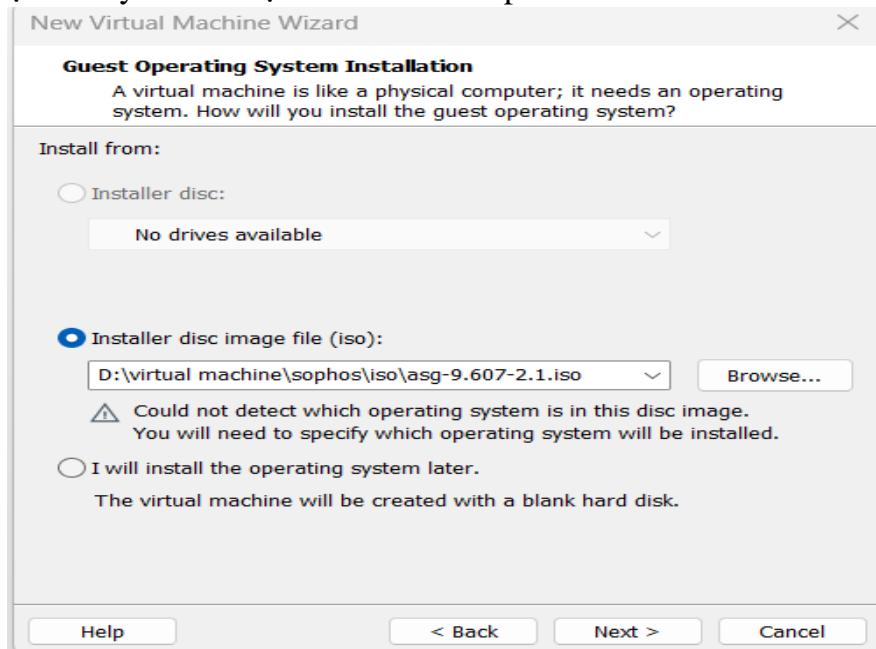


- Bước 22: Restart PC1 và đăng nhập bằng tài khoản đã tạo trên domain



2.2. Cài đặt firewall Sophos

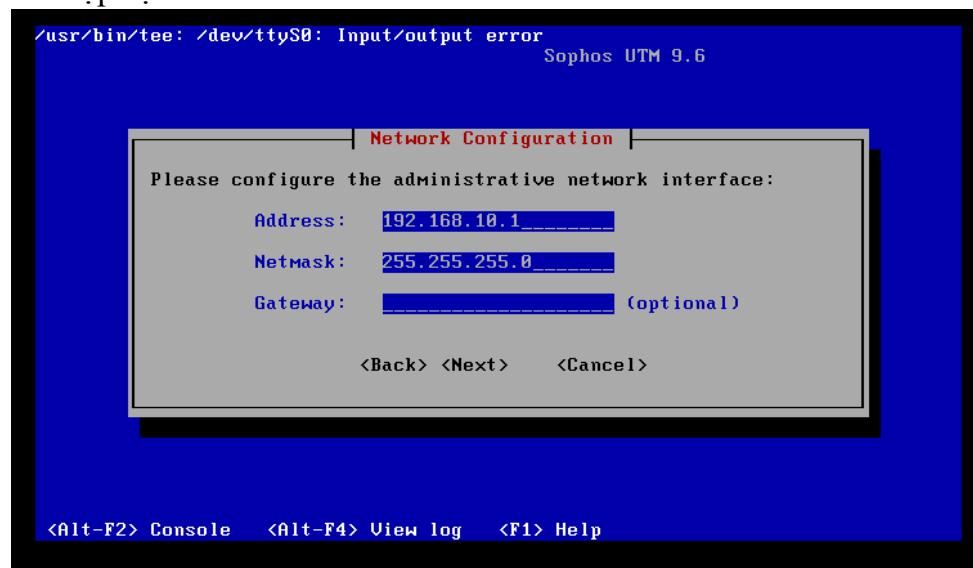
- Bước 1: Tạo 1 máy ảo và chọn file iso cho Sophos



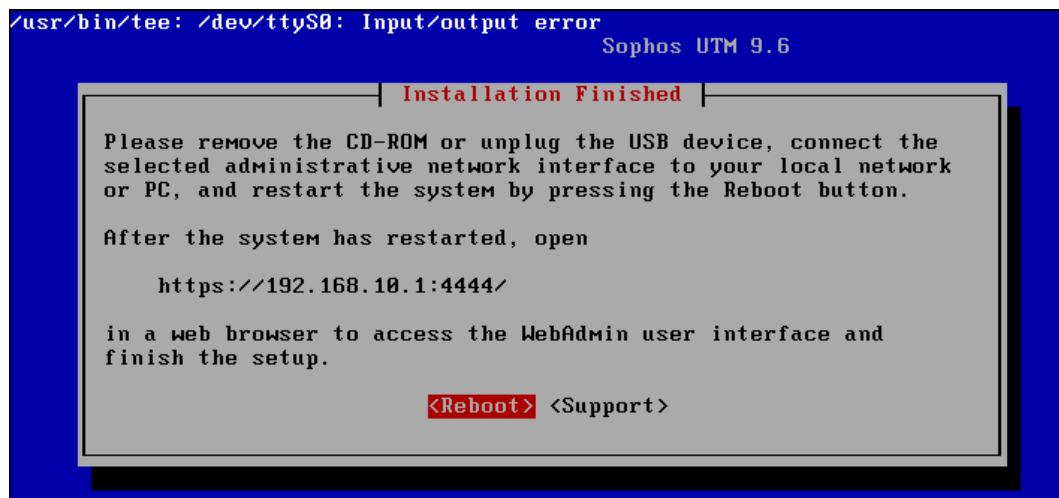
- Bước 2: Thiết lập thông số cho Sophos như sau

Device Type	Configuration
Memory	1.3 GB
Processors	4
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\virt...
Network Adapter	Custom (VMnet1)
Network Adapter 2	NAT
USB Controller	Present
Display	Auto detect

- Bước 3: Nhập địa chỉ cho LAN interface



- Bước 4: Reboot



- Bước 5: Truy cập web Admin và nhập thông tin như bên dưới, sau đó nhấn Apply

Welcome to WebAdmin

Basic system setup

Hostname: truong

Company or organization name: trantruong

City: Ho Chi Minh

Country: Vietnam

admin account password:

Repeat password:

admin account email address: neuertrg@gmail.com

SOPHOS LICENSE AGREEMENT

- Bước 6: Cấu hình interface WAN

Interfaces

Dashboard Management Definitions & Users Interfaces & Routing Interfaces Quality of Service (QoS) Uplink Monitoring IPv6 Static Routing Dynamic Routing (OSPF) Border Gateway Protocol Multicast Routing (PIM-SM) Network Services Network Protection Web Protection

Add Interface

Name:	External
Type:	Ethernet
Hardware:	eth1 Intel Corporation 82E
Dynamic IPv4:	<input checked="" type="checkbox"/>
IPv4 Default GW:	<input type="checkbox"/>
Comment:	
Advanced	

Action Sort by: Name asc

Edit Delete Clone

Internal [Up] on eth0 [192.168.10.1/24]
MTU 1500
Auto-created on installation

- Bước 7: Kết quả tạo interface

Interfaces

Dashboard Management Definitions & Users Interfaces & Routing Interfaces Quality of Service (QoS) Uplink Monitoring IPv6 Static Routing Dynamic Routing (OSPF) Border Gateway Protocol Multicast Routing (PIM-SM) Network Services

Action Sort by: Name asc

Edit Delete Clone

External [Up] on eth1 [192.168.20.128/24]
MTU 1500

Edit Delete Clone

Internal [Up] on eth0 [192.168.10.1/24]
MTU 1500
Auto-created on installation

- Bước 8: Vào Support > Tools > ping google kiểm tra firewall truy cập internet

Ping host: Custom hostname/IP add

Hostname/IP address: google.com

Ping over interface: External

Ping Check Result

```
PING google.com (172.217.27.46) from 192.168.20.128 eth1: 56(84) bytes of data.
64 bytes from hkg12s37-in-f14.1e100.net (172.217.27.46): icmp_seq=1 ttl=128 time=35.7 ms
64 bytes from hkg12s37-in-f14.1e100.net (172.217.27.46): icmp_seq=2 ttl=128 time=34.6 ms
64 bytes from hkg12s37-in-f14.1e100.net (172.217.27.46): icmp_seq=3 ttl=128 time=33.4 ms
64 bytes from hkg12s37-in-f14.1e100.net (172.217.27.46): icmp_seq=4 ttl=128 time=33.8 ms
64 bytes from hkg12s37-in-f14.1e100.net (172.217.27.46): icmp_seq=5 ttl=128 time=35.4 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4022ms
rtt min/avg/max/mdev = 33.446/34.637/35.723/0.910 ms
```

- Bước 9: Tạo nat để các mạng có thể ra internet

Edit Masquerading Rule

Network: Any

Position: 1

Interface: External

Use address: << Primary address >>

Comment:

Action

Sort by: Position asc

<input type="checkbox"/> Edit		Any		External
<input type="checkbox"/> Delete				
<input type="checkbox"/> Clone				

- Bước 10: Tạo rule cho phép domain controller kết nối internet

The screenshot shows a network management interface with a sidebar on the left containing various protection modules like Firewall, NAT, Intrusion Prevention, and Web Protection. The main area is titled 'Firewall' and shows a 'Rules' tab selected. A 'New Rule...' button is visible. The 'Edit Rule' dialog is open, allowing configuration of sources, services, and destinations. The list of existing rules on the right shows two rules defined.

- **Bước 11: Ping google từ Domain Controller**

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [172.217.25.14] with 32 bytes of data:
Reply from 172.217.25.14: bytes=32 time=38ms TTL=127
Reply from 172.217.25.14: bytes=32 time=38ms TTL=127
Reply from 172.217.25.14: bytes=32 time=38ms TTL=127
Reply from 172.217.25.14: bytes=32 time=39ms TTL=127

Ping statistics for 172.217.25.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 39ms, Average = 38ms

C:\Users\Administrator>

```

- Bước 12: Tích hợp domain vào Sophos

The screenshot shows the Sophos XG Firewall's 'Authentication Services' section. On the left, there's a sidebar with various service definitions. The 'Authentication Services' option is selected. In the main area, a 'New Authentication Server...' button is highlighted. A modal window titled 'Add Authentication Server' is open, with 'Backend' set to 'Active Directory' and 'Position' set to 'Top'. A smaller modal window titled 'Add Network Definition' is nested within it, containing fields for 'Name' (set to 'AD Server'), 'Type' (set to 'Host'), and an 'IPv4 address' (set to '192.168.10.34'). There are also tabs for 'DHCP Settings', 'DNS Settings', and 'Advanced'. At the bottom of the inner modal, there are 'Save' and 'Cancel' buttons.

- Bước 13: Bind DN nhập
“CN=administrator,CN=Users,DC=trantruong,DC=local”

This screenshot shows a configuration form for a bind DN. It has two main input fields: 'Port' (set to 389) and 'Bind DN' (containing the value 'CN=administrator,CN=Users,DC=trantruong,DC=local'). Below these fields is a 'Test' button.

- Bước 14: Nhập password cho tài khoản administrator và nhấn test server settings

This screenshot shows a 'Test server settings' dialog. It contains fields for 'Bind DN' (set to 'CN=administrator,CN=Users,DC=trantruong,DC=local'), 'Password' (with several dots), and 'Base DN' (empty). Below these are 'Username' and 'Password' fields (both empty). A 'Test' button is present. To the right, a separate 'Information:' dialog box displays the message 'Server test passed.' and has an 'OK' button.

- Bước 15: Nhấn save và thu được kết quả

The screenshot shows the 'Authentication Services' tab selected in the top navigation bar. On the left, there's a sidebar with 'Definitions & Users' and 'Authentication Services' highlighted. The main panel displays a table with one row for 'adirectory'. The row contains an 'Edit' button, a 'Delete' button, and a 'Clone' button. The table header includes 'Action', 'Sort by: Position asc', and a search bar. The details for 'adirectory' show 'Host: 192.168.10.34 (192.168.10.34:389)' and a 'Base DN' button.

- Bước 16: Authentication Services > Tab Advanced > Mục Prefetch Directory
Users nhấn chọn biểu tượng thư mục rồi chọn user > nhấn save

The screenshot shows the 'Active Directory Browser' window. The left pane shows a tree view of the Active Directory structure under 'Active Directory'. The right pane displays a table for a user named 'user1'. The table has columns for various attributes, all of which are set to 'DND'. At the bottom of the table, there are two buttons: a green checkmark labeled 'Save' and a red X labeled 'Cancel'.

- Bước 17: Tích chọn “Enable backend sync on login” sau đó nhấn Apply

Prefetch Directory Users

Server: 192.168.10.34 (192.168.1)

Prefetch interval: Never

Prefetch time (hh:mm): 00 : 00

Groups:

- CN=user1,OU=PTITHCM,DC=trantruong,DC=local

Enable backend sync on login

Here you can set a regular interval at which users in a backend are synchronized with the local device and you can also trigger an intermediate synchronization with the corresponding directory service. This will prevent long authentication times, when a lot of users log in at the same time. **This option is not required unless you experience extremely high load when authenticating many new users.**

Prefetch Now

Enable backend sync on login

- Bước 18: User 1 đã được tạo

search

Users & Groups

Dashboard

Management

Definitions & Users

Network Definitions

Service Definitions

Time Period Definitions

Users & Groups

Client Authentication

AWS Profiles

Authentication Services

Interfaces & Routing

Network Services

Users

New User...

All

Display: 10

Action	Sort by: Name asc
<input type="checkbox"/> Edit	admin Locally authenticated Default Super-Admin user
<input type="checkbox"/> Delete	
<input type="checkbox"/> Edit	user1 Remotely authenticated [User data updated from backend automatically] synced from directory
<input type="checkbox"/> Delete	

2.3. Cấu hình chính sách Sophos chặn user truy cập facebook

- Bước 1: Vào Web Protection > Web Filtering >bật web filtering

- Bước 2: Vào Web Protection > Web Filter Profiles > Filter Actions > New Filter Action > tạo action block site facebook.com

- Bước 3: Vào tab Policies add policy cho user1

Web Filtering

Global HTTPS Policies

1 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.

Add Policy

Name: user1

Users/Groups

DND DND DND
DND DND DND
DND DND DND

Time event: << Always >>

Filter action: block site facebook

Comment:

Advanced Settings

Save Cancel

Base Policy Any Anytime Default content filter action

- Bước 4: Click active

Web Filtering

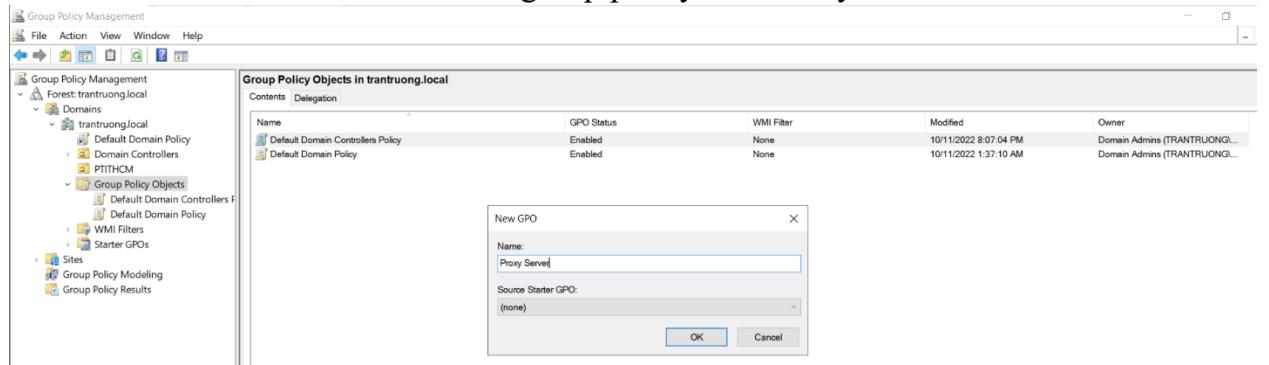
Global HTTPS Policies

1 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.

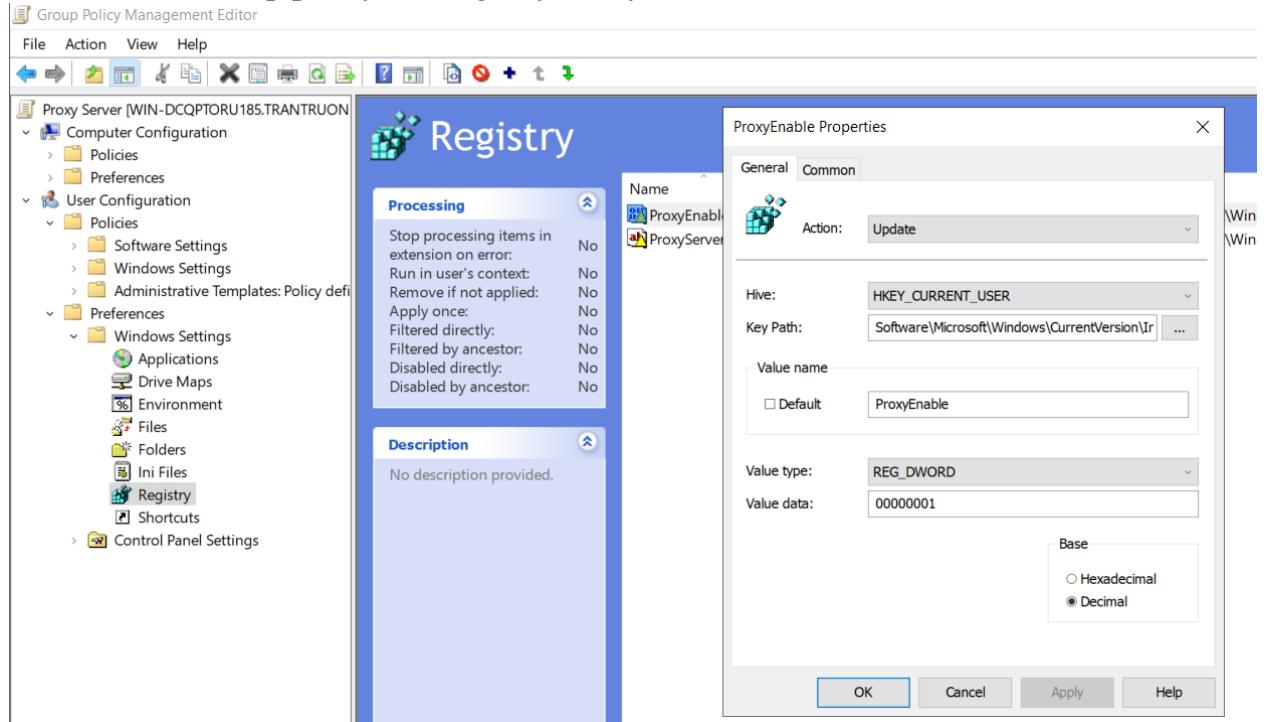
Active Name	Users/Groups	Time	Filter action
1 user1	user1	Anytime	block site facebook

Base Policy Any Anytime Default content filter action

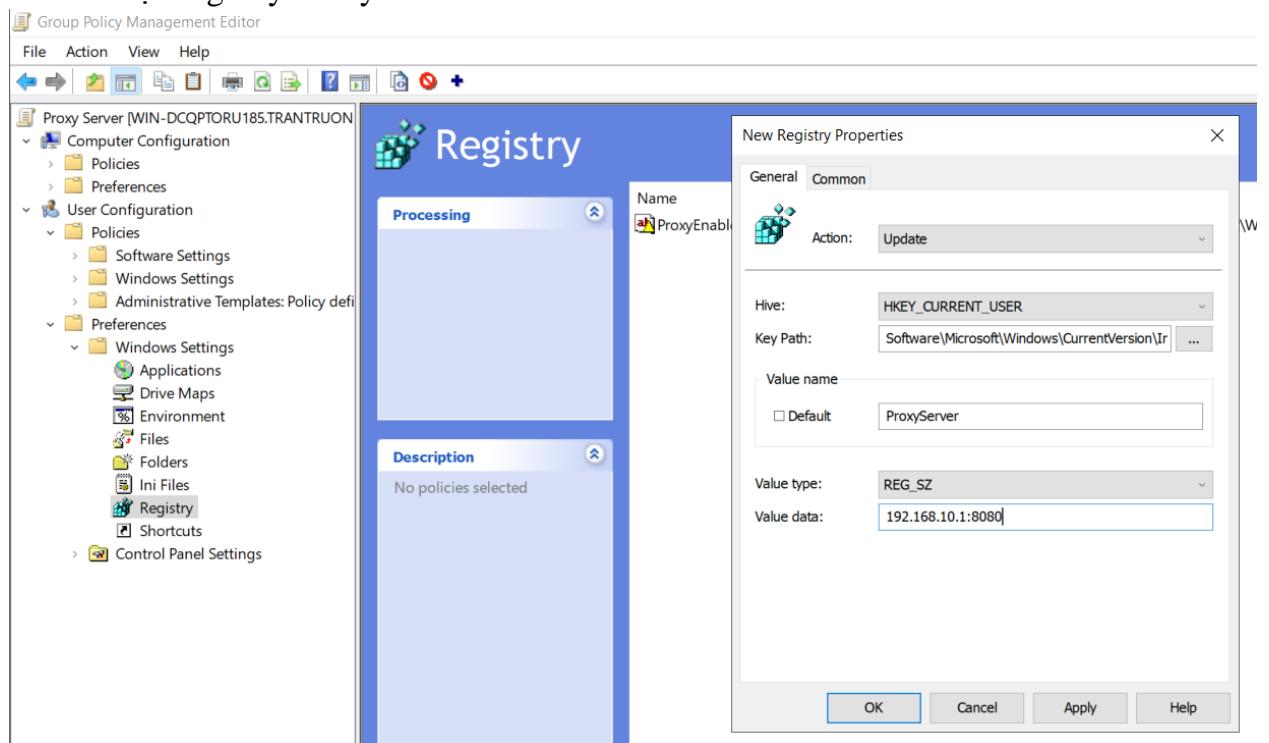
- Bước 5: tại Domain Controller tạo 1 group policy tên “Proxy Server”



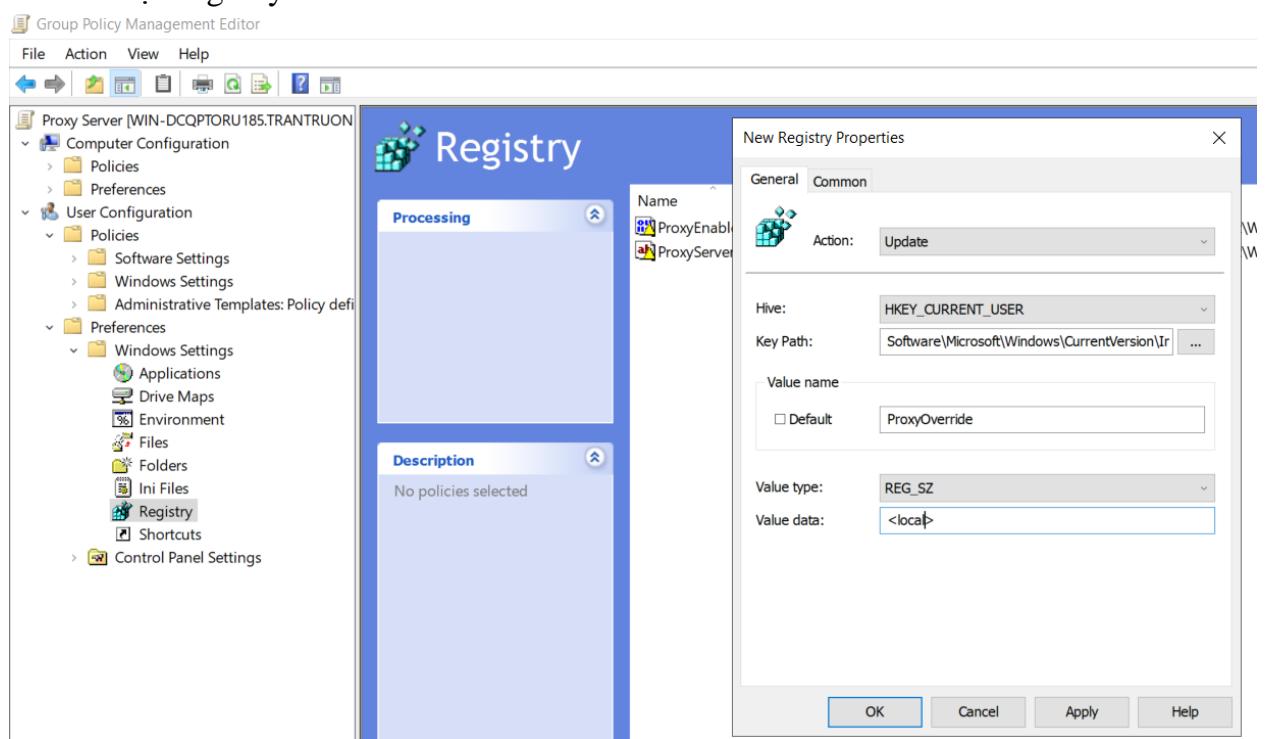
- Bước 6: Edit Group policy, tạo registry ProxyEnable



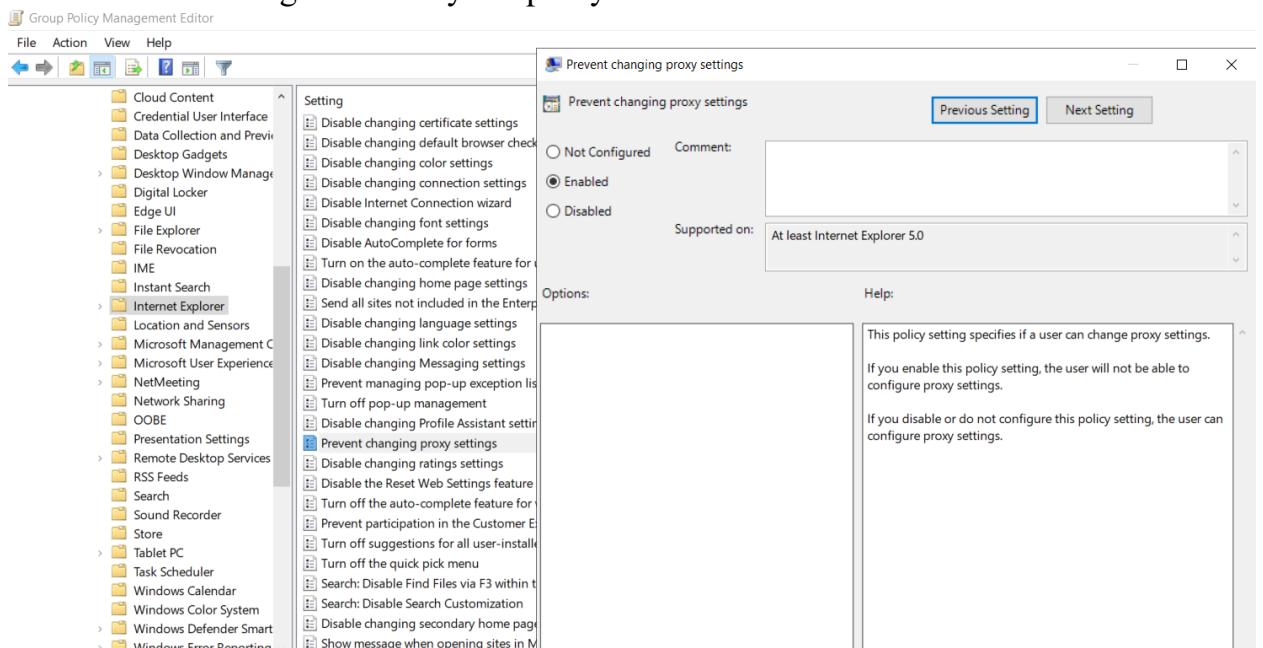
- Bước 7: tạo registry ProxyServer



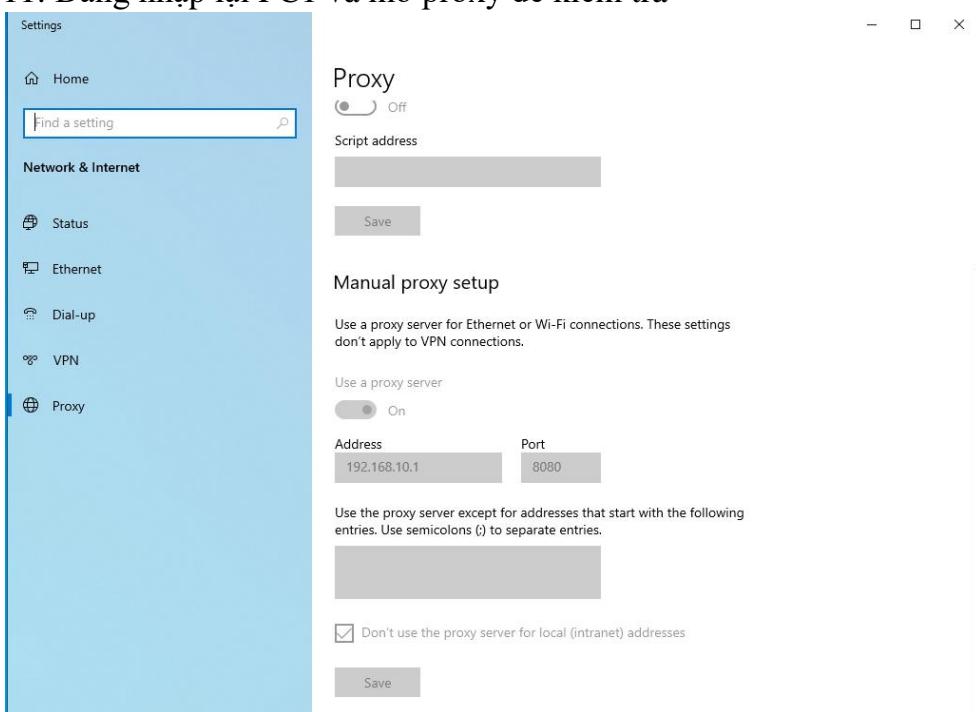
- Bước 8: tạo registry Override



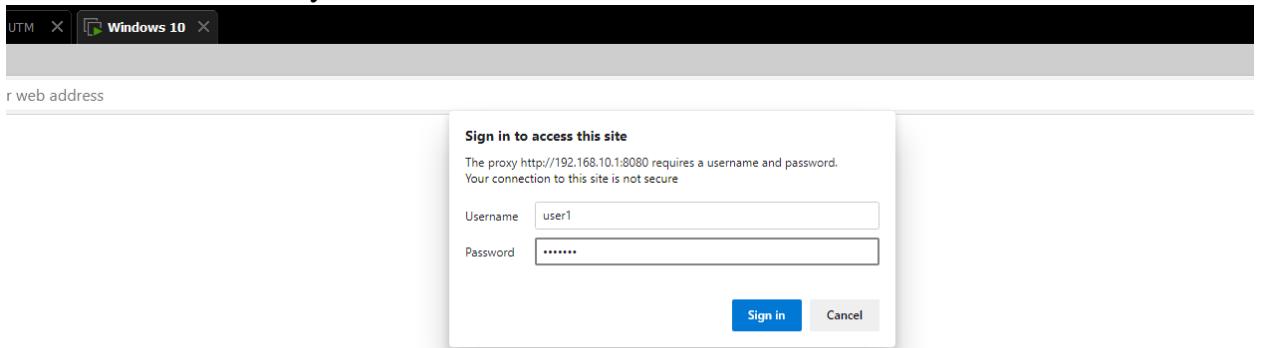
- Bước 9: Cấu hình ngăn user thay đổi proxy



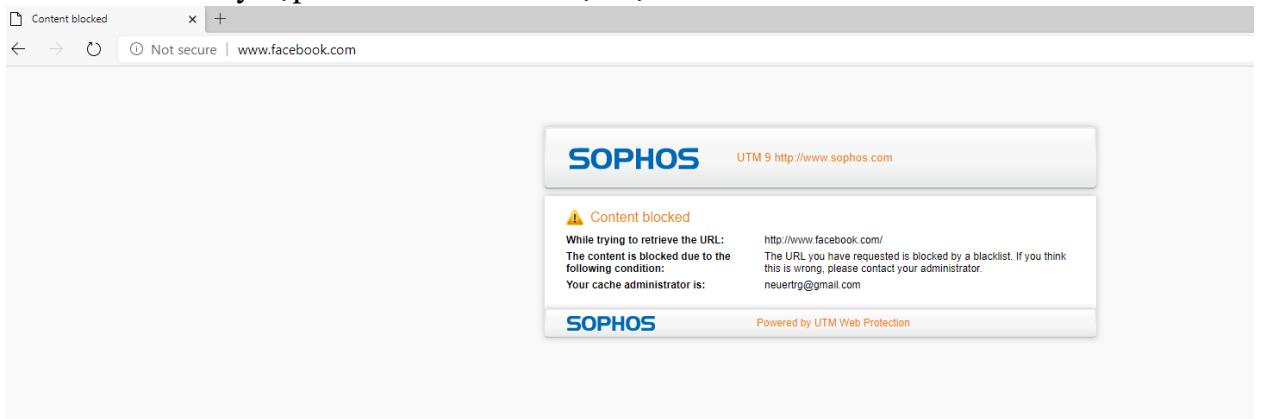
- Bước 10: Chạy “gpupdate /force” để cập nhật lại chính sách
- Bước 11: Đăng nhập lại PC1 và mở proxy để kiểm tra



- Bước 12: Mở trình duyệt trên PC1

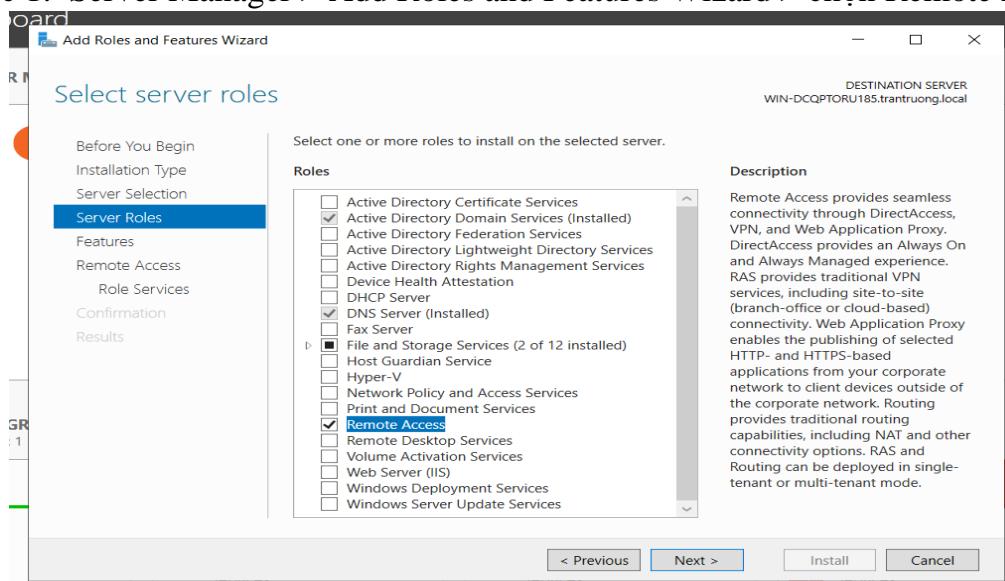


- Bước 13: thử truy cập facebook.com và bị chặn

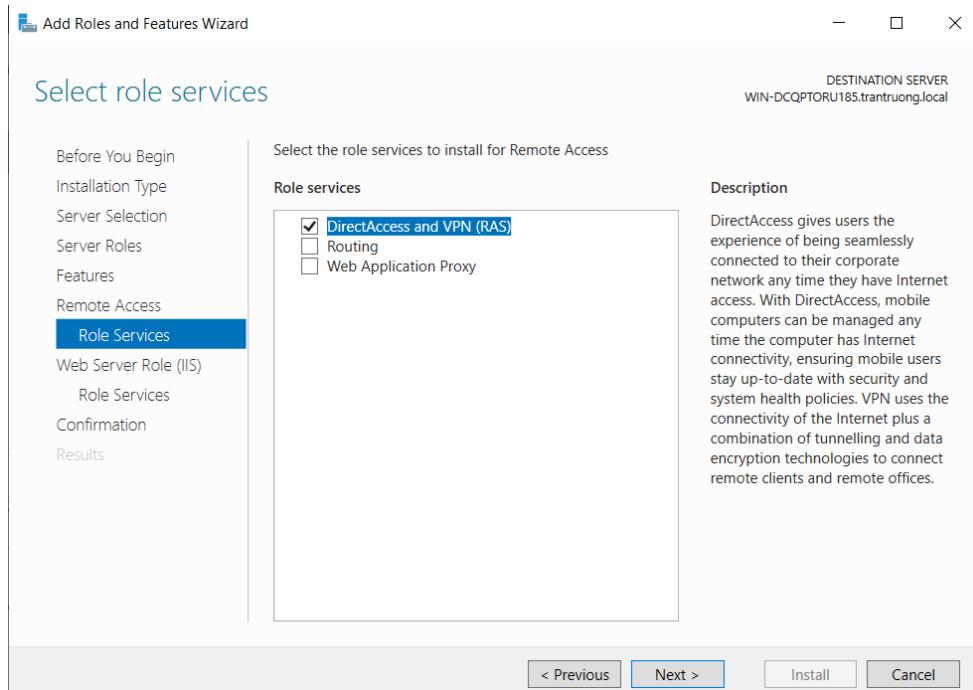


2.4. Cài đặt và cấu hình vpn server

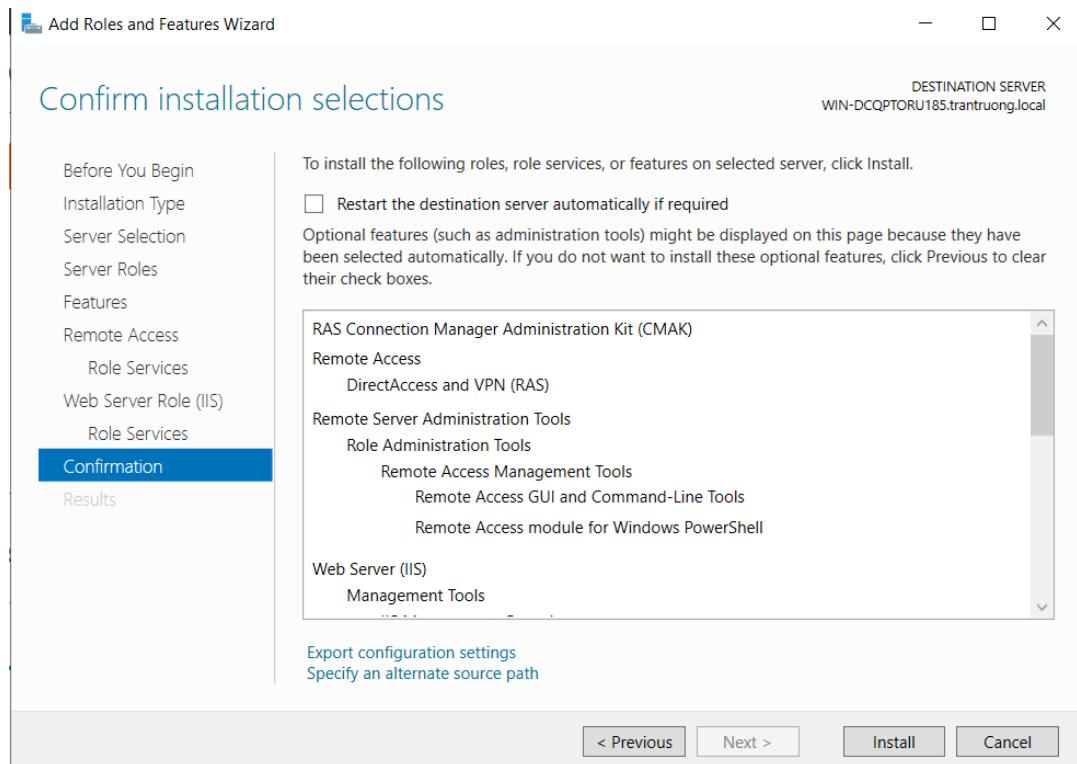
- Bước 1: Server Manager > Add Roles and Features Wizard > chọn Remote Access



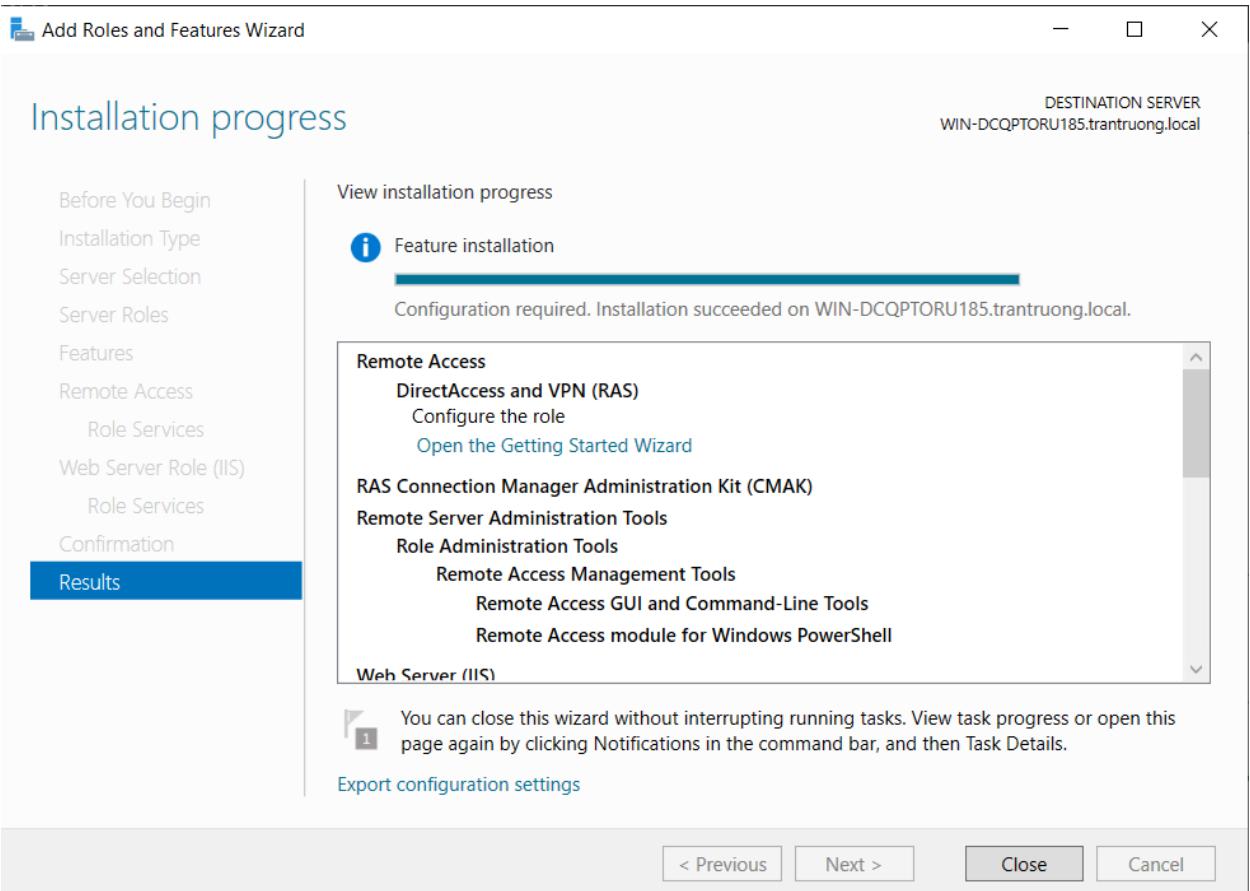
- Bước 2: Chọn RAS



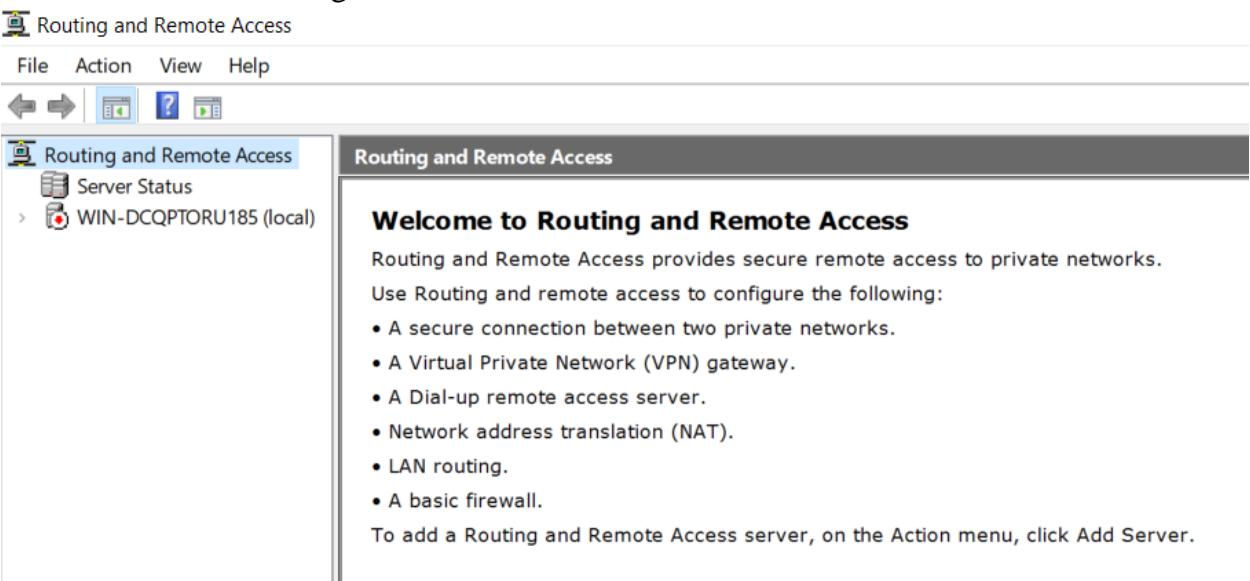
- Bước 3: Click Install



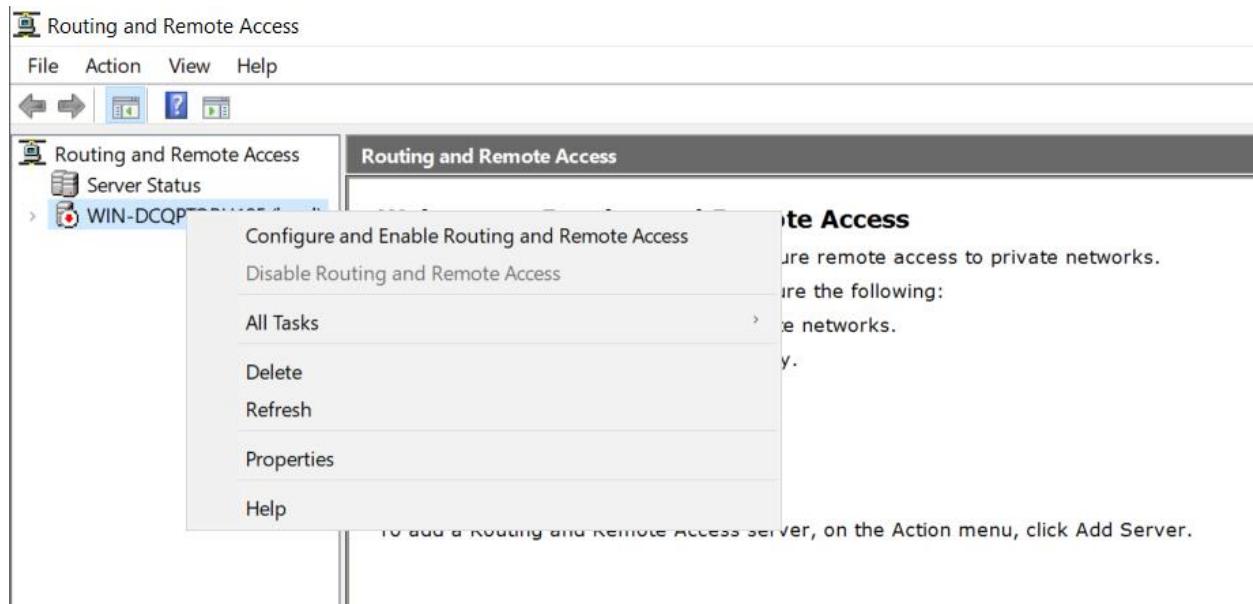
- **Bước 4: Hoàn thành cài đặt**



- **Bước 5: Tools > Routing and Remote Access**



- Bước 6: Chuột phải vào server > Configure and Enable Routing and Remote Access



- Bước 7: Custom config, nhấn next

Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

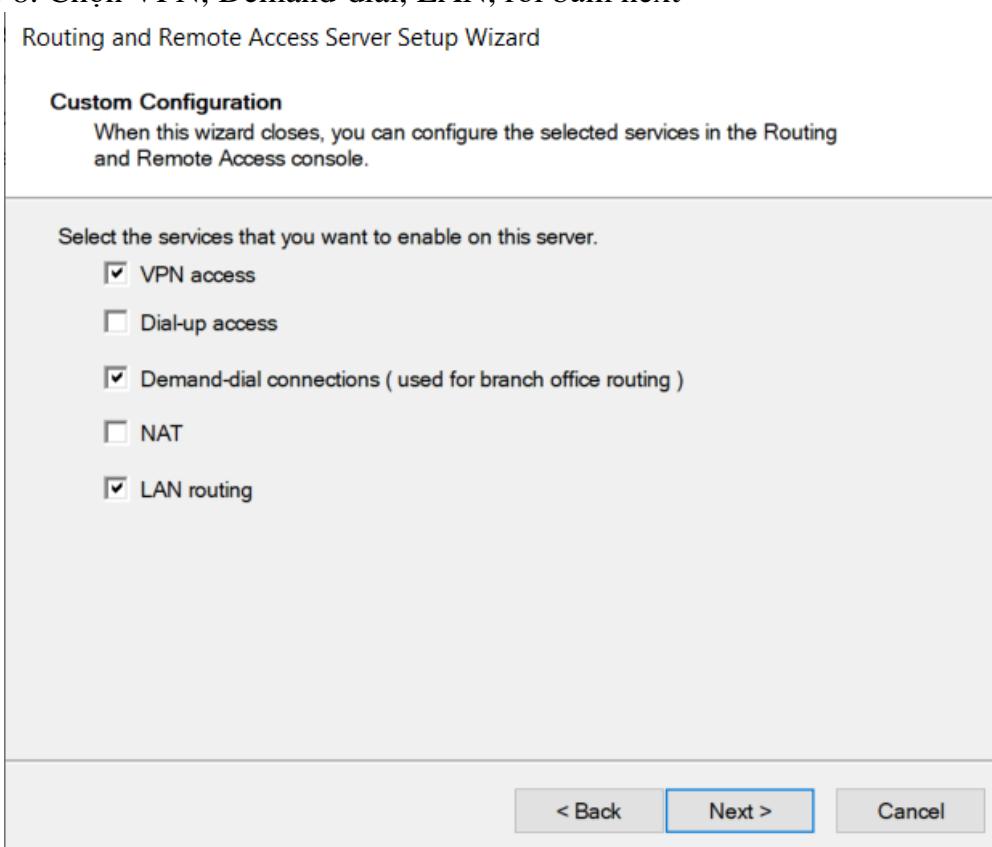
- Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
- Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
- Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
- Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
- Custom configuration
Select any combination of the features available in Routing and Remote Access.

< Back

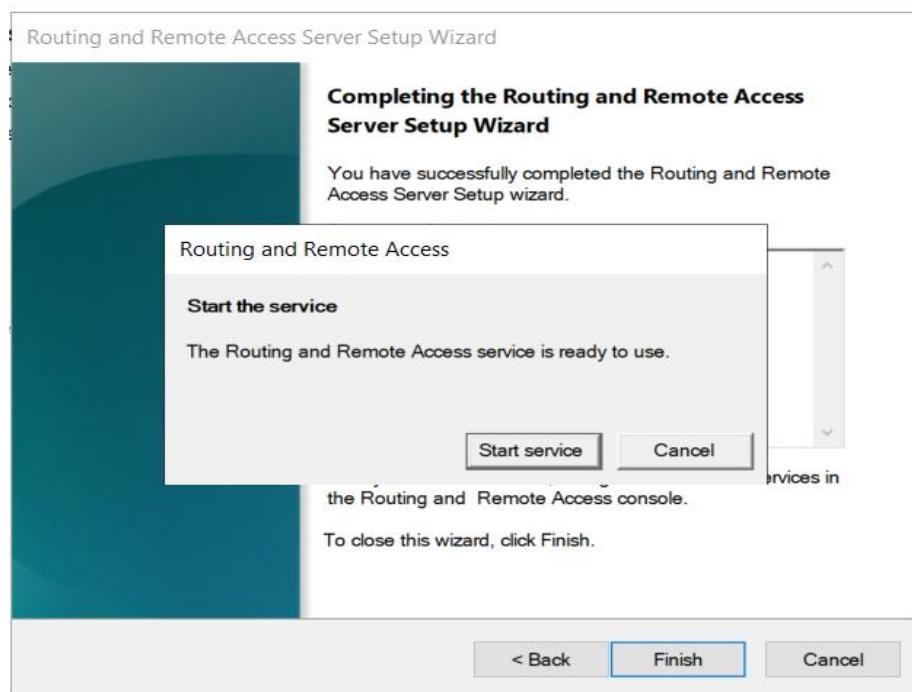
Next >

Cancel

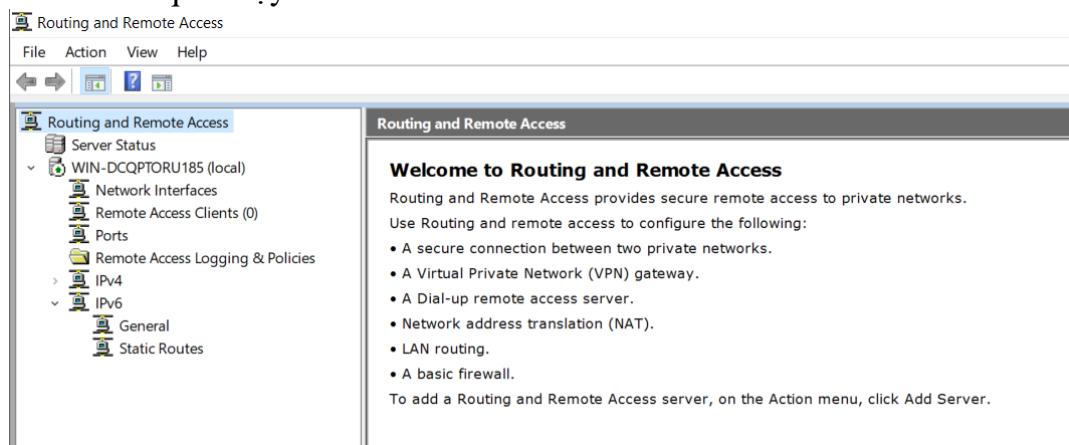
- Bước 8: Chọn VPN, Demand-dial, LAN, rồi bấm next



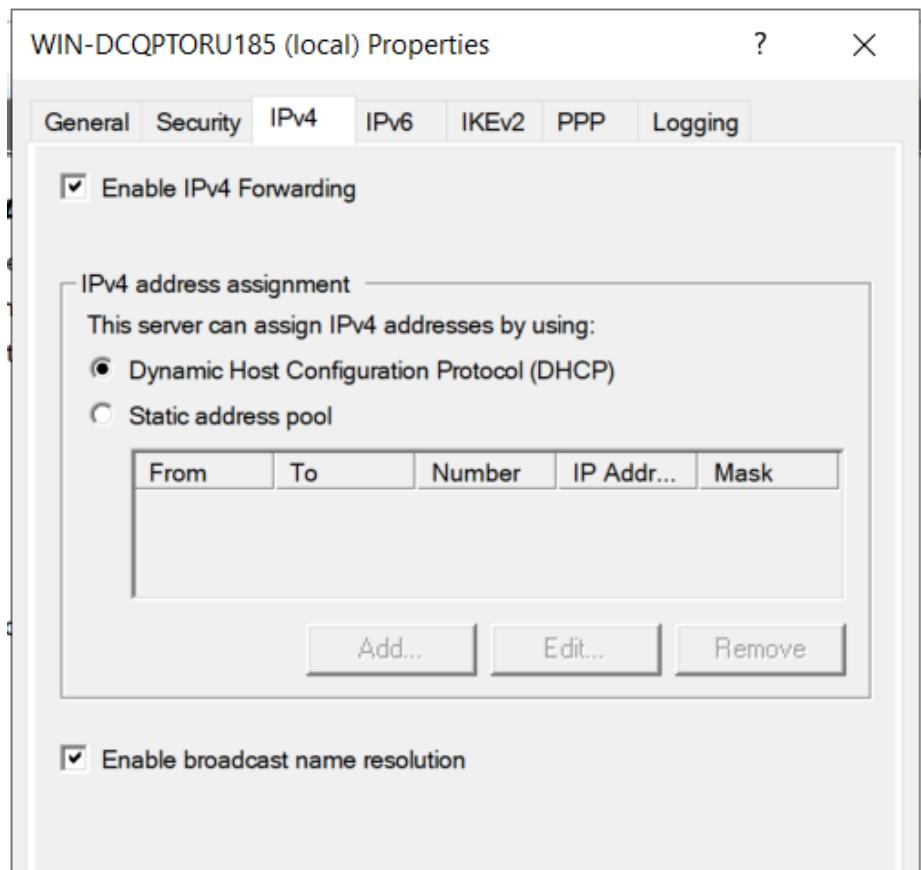
- Bước 9: Start service



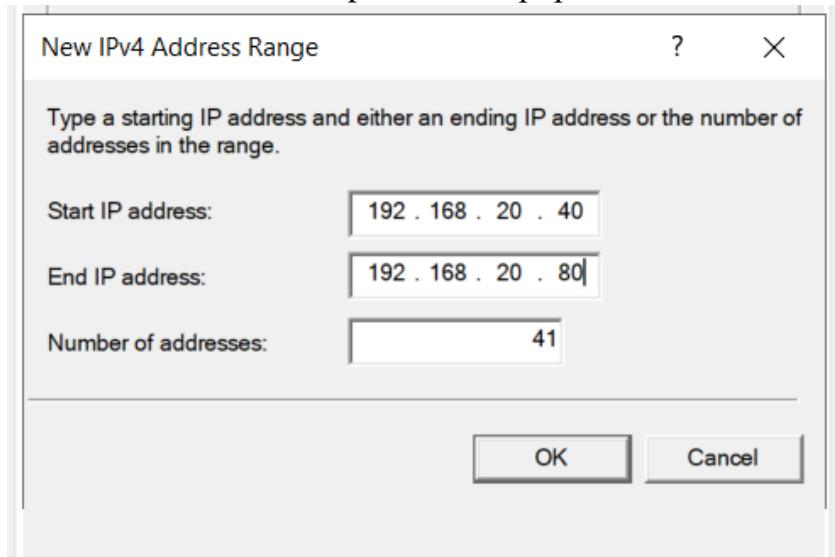
- Bước 10: Kết quả chạy service



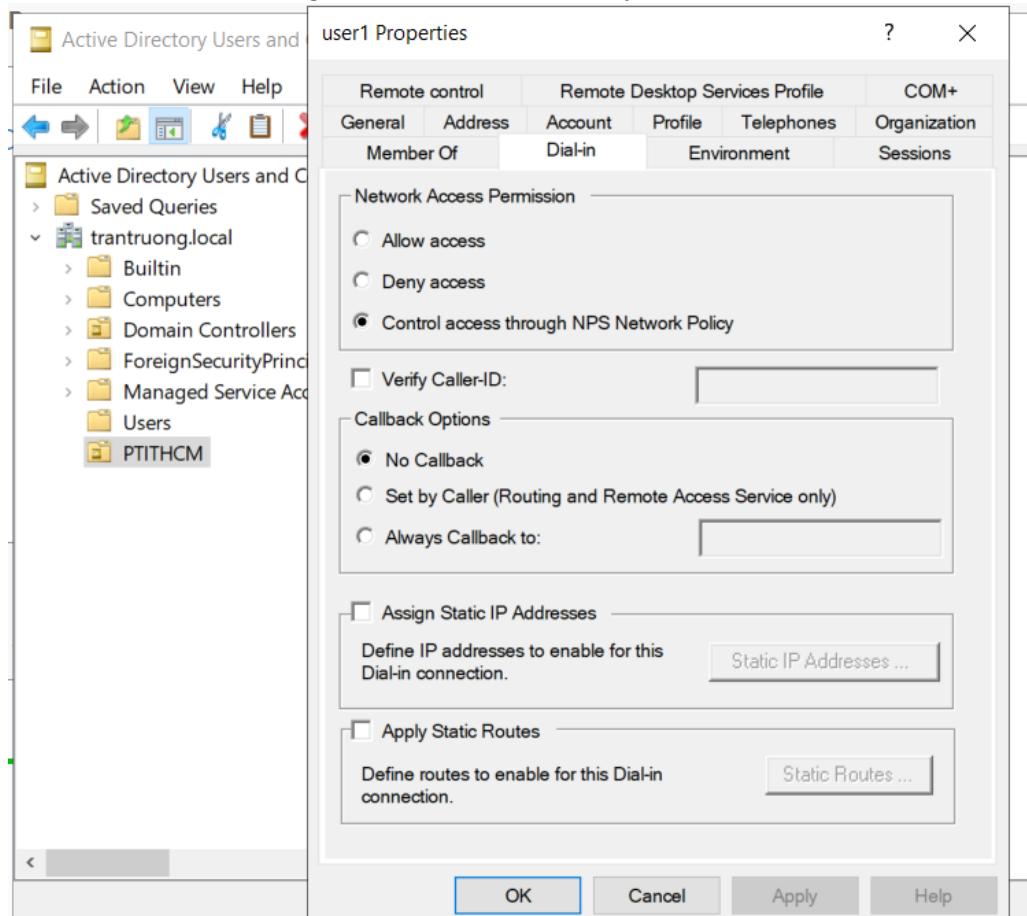
- Bước 11: Chuột phải vào server chọn Properties



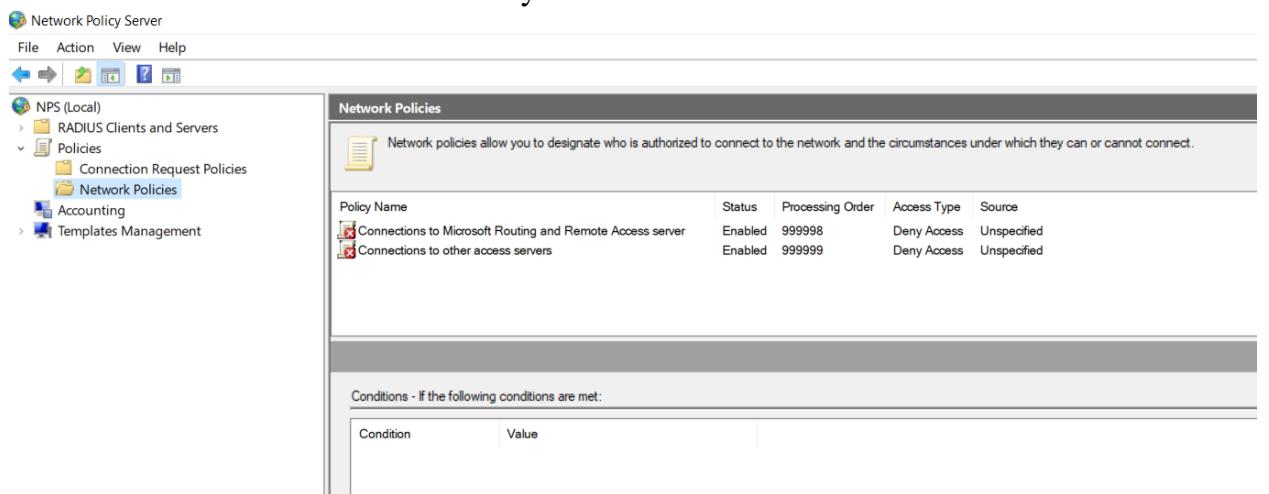
- Bước 12: Click chọn Static address pool, và nhập ip và lưu lại



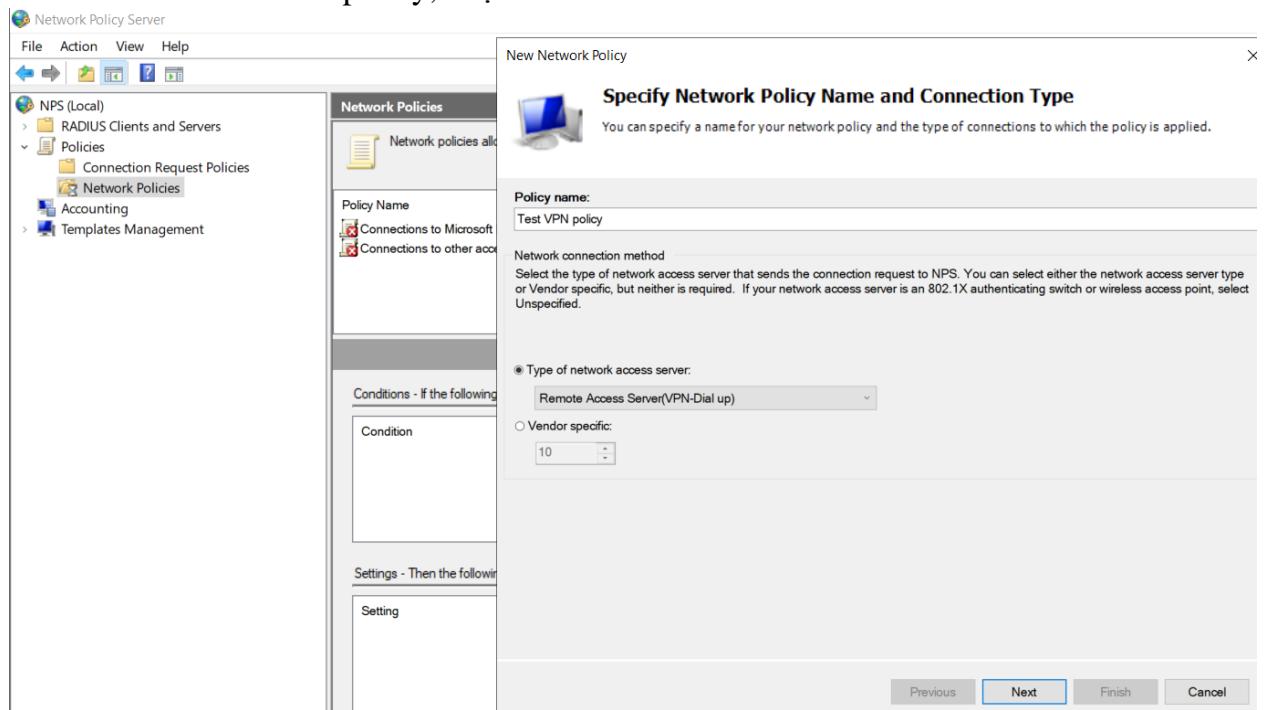
- Bước 13: Chọn user được phép kết nối vpn, chọn properties > tab Dial-in > click chọn Control access through NPS Network Policy



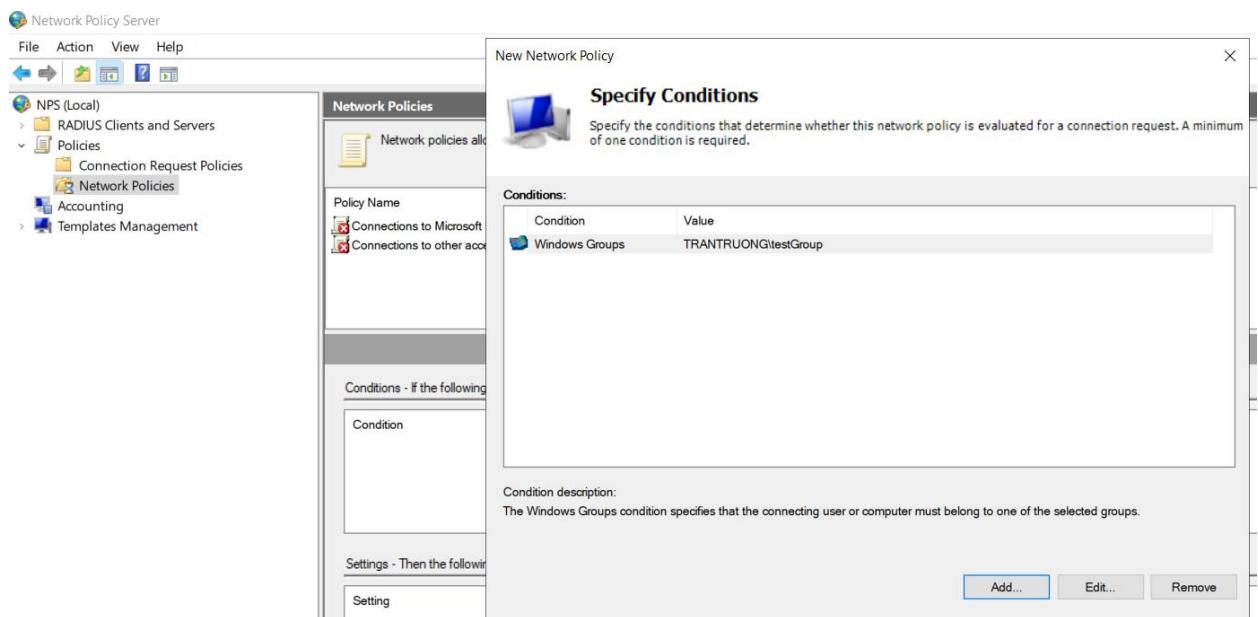
- Bước 14: Mở Tools > Network Policy Server



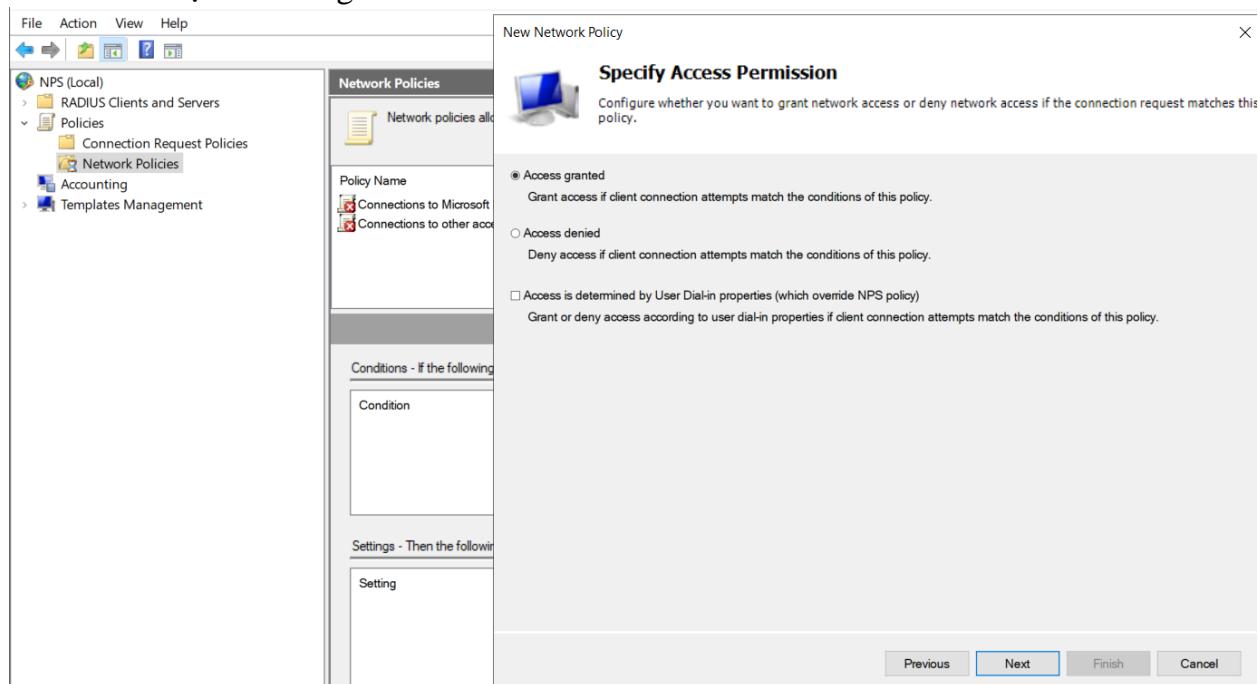
- Bước 15: New network policy, chọn next



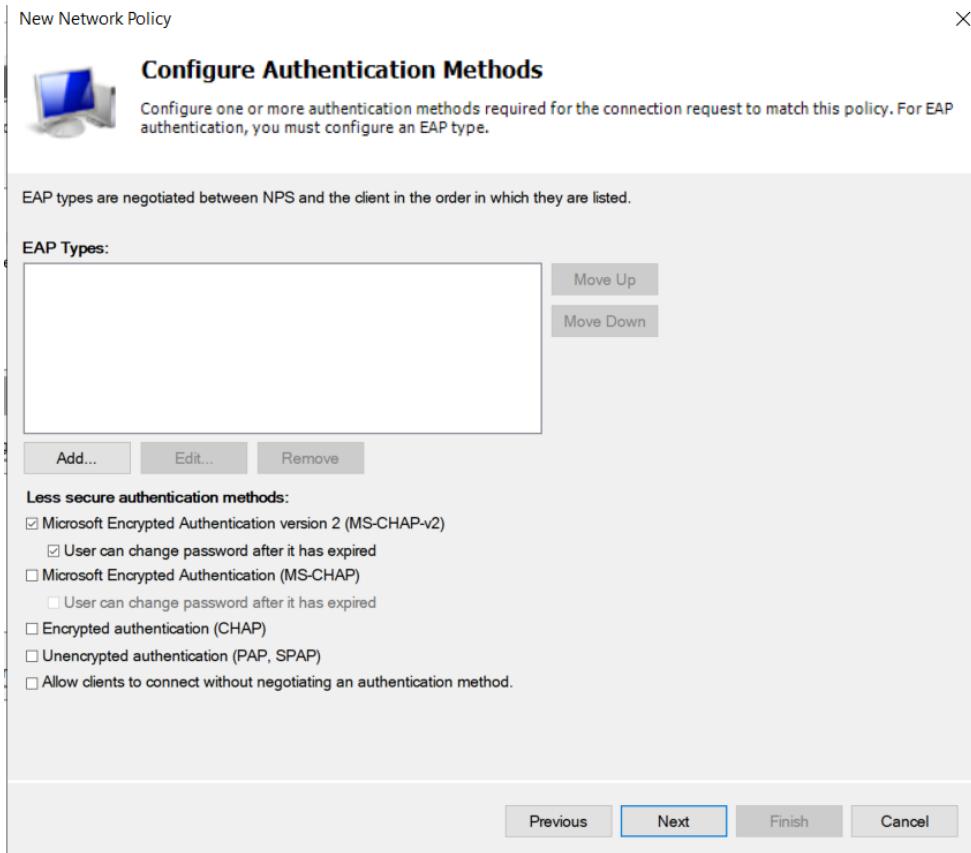
- Bước 16: Thêm Group



- Bước 17: Chọn Access granted > Next



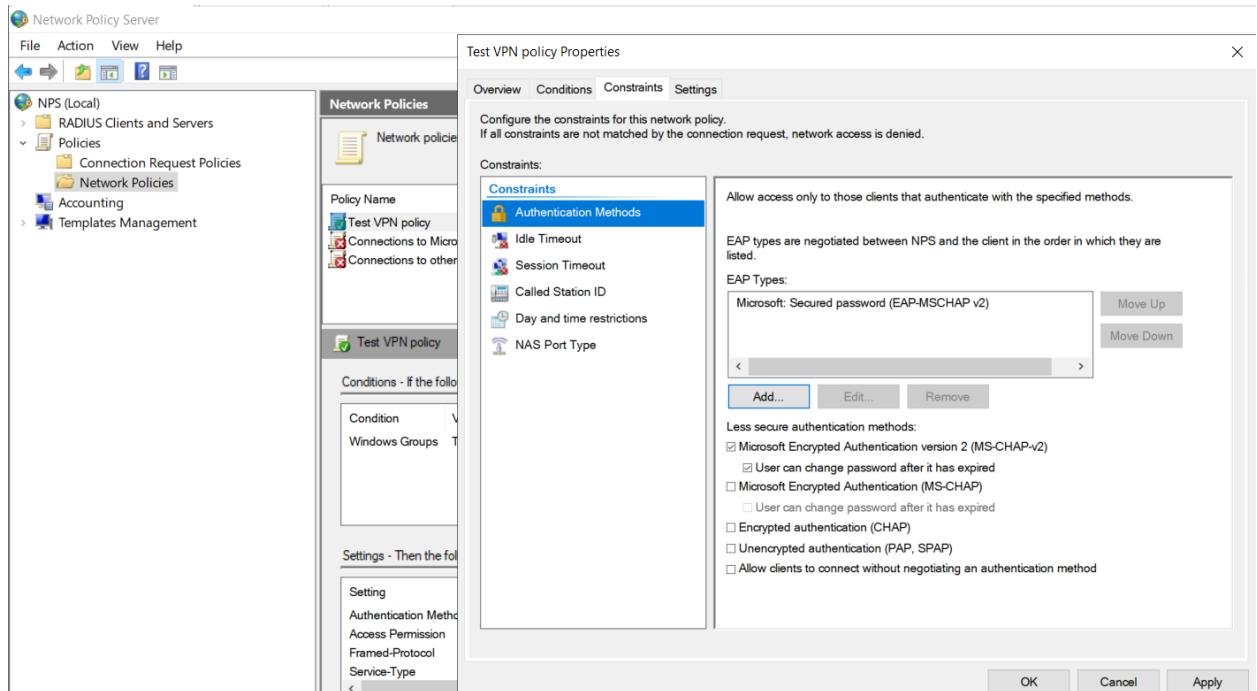
- Bước 18: Chọn MS-CHAP-V2



- Bước 19: Kết quả sau khi finish

Policy Name	Status	Processing Order	Access Type	Source
Test VPN policy	Enabled	1	Grant Access	Remote Access Server(VPN-Dial up)
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

- Bước 20: Chuột phải vào network Policies > Properties > Contraints > Add EAP-MSCHAP v2 > Apply > OK



- Bước 21: Trên Sophos tạo rule NAT port 1723 của VPN service để bên ngoài có thể truy cập được

Action	Sort by:	Position asc
Edit		1
Delete		
Clone		

Traffic selector: Any → vpn → External (Address)
Destination translation: vpn server
Automatic Firewall rule: ✓
Initial packets are logged: ✓

- Bước 22: Tạo rule cho phép các mạng khác kết nối VPN

The screenshot shows the Sophos Firewall interface under the 'Firewall' tab. On the left sidebar, 'Network Protection' and 'Firewall' are selected. In the main area, a 'New Rule...' button is highlighted. The 'Edit Rule' dialog is open, showing the following configuration:

- Group:** :: Please select ::
- Position:** 3
- Sources:** Any (DND, DND, DND)
- Services:** vpn server (DND, DND, DND)
- Destinations:** vpn ss (DND, DND, DND)
- Action:** Allow
- Comment:**

To the right of the dialog, a list of existing rules is displayed:

Action	Sort by: Position asc	Any
Edit	2	
Delete		
Clone		
Edit	3	
Delete		
Clone		

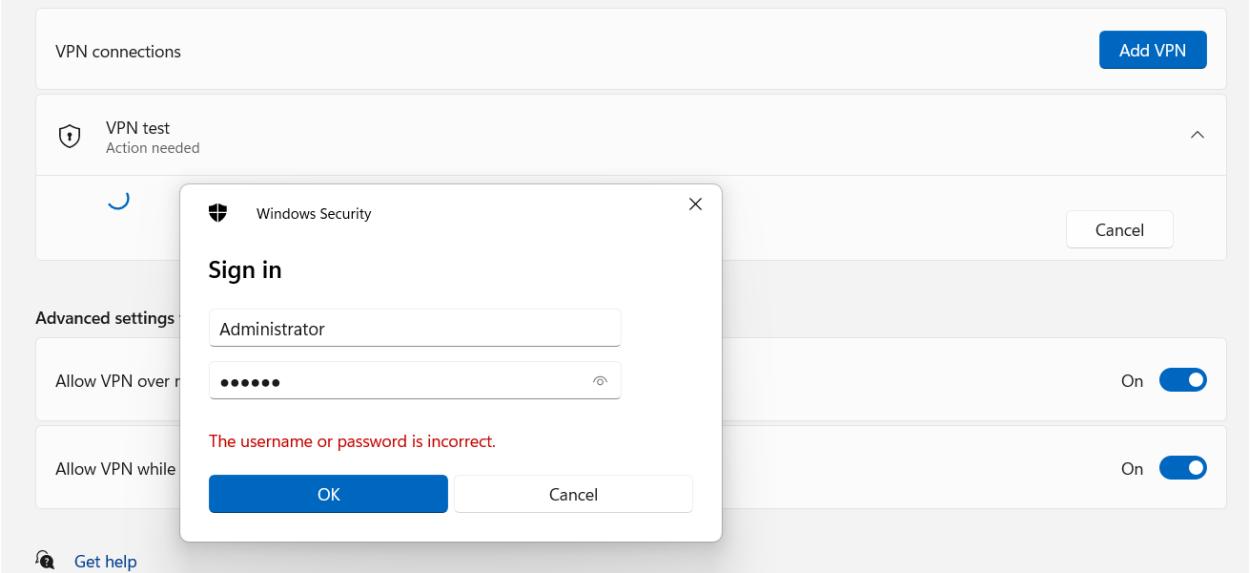
- Bước 23: tại máy client (máy thật) tạo 1 kết nối VPN đến domain thông qua port đã NAT của sophos

The screenshot shows the 'Add a VPN connection' dialog. The fields are as follows:

- VPN provider:** Windows (built-in)
- Connection name:** VPN test
- Server name or address:** 192.168.20.128
- VPN type:** Point to Point Tunneling Protocol (PPTP)
- Type of sign-in info:** Username and password

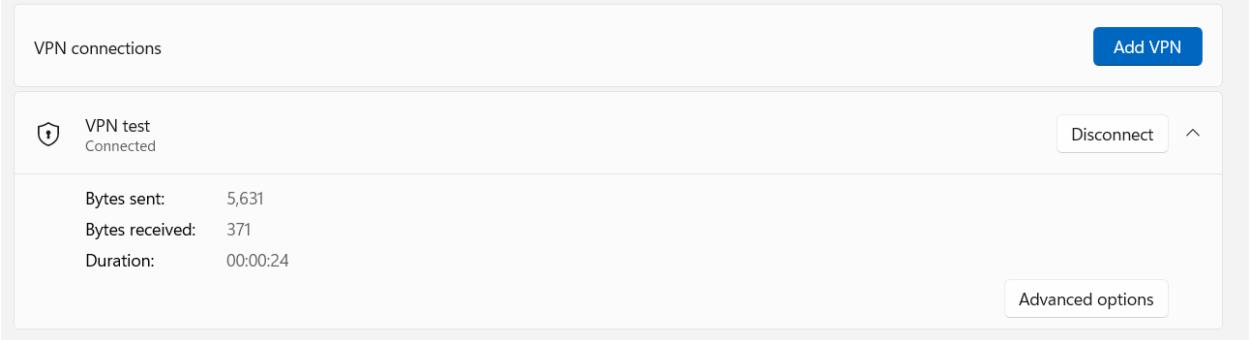
- Bước 24: Nhập mật khẩu admin

Network & internet > VPN



- Bước 25: Kết nối thành công

Network & internet > VPN



- Bước 26: Máy Client đã nhận IP nội bộ do domain cấp

```
PPP adapter VPN test:
```

```
Connection-specific DNS Suffix . : 
IPv4 Address . . . . . : 192.168.10.42
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0
```

- Bước 27: Từ máy Client ping tới Domain để kiểm tra kết nối VPN

```
C:\Users\neuer>ping 192.168.10.34
```

```
Pinging 192.168.10.34 with 32 bytes of data:
```

```
Reply from 192.168.10.34: bytes=32 time=7ms TTL=127
```

```
Reply from 192.168.10.34: bytes=32 time=1ms TTL=127
```

```
Reply from 192.168.10.34: bytes=32 time=2ms TTL=127
```

```
Reply from 192.168.10.34: bytes=32 time=2ms TTL=127
```

```
Ping statistics for 192.168.10.34:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

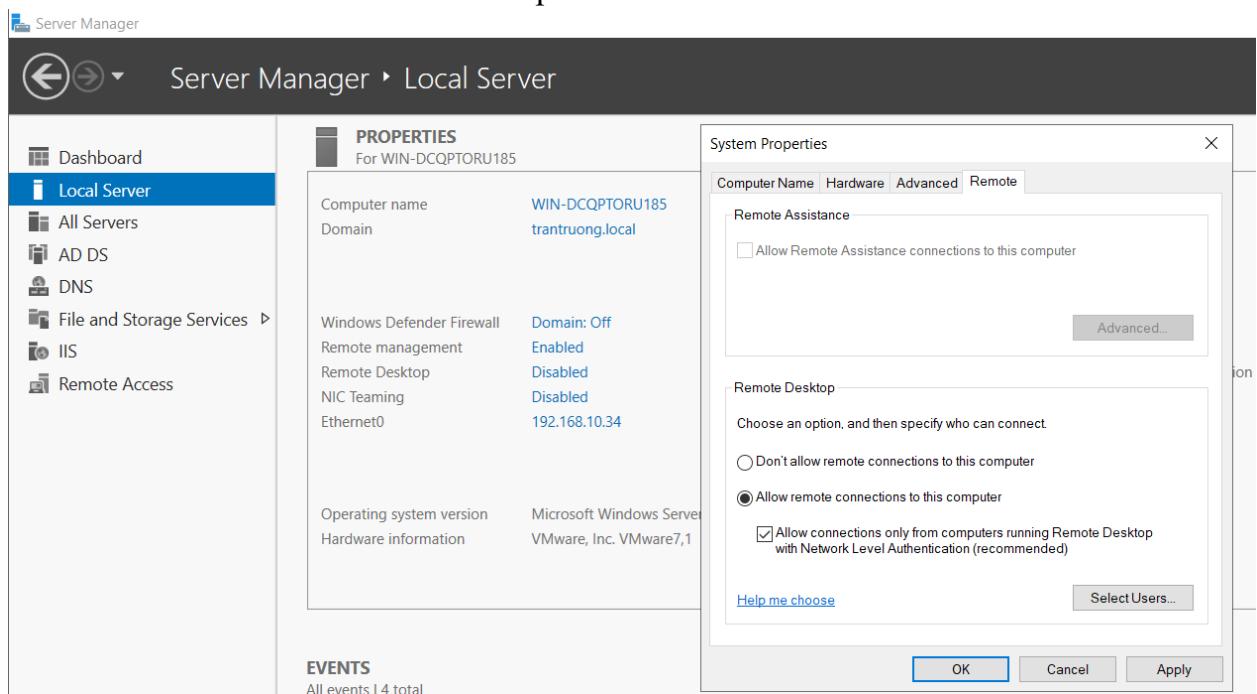
```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 7ms, Average = 3ms
```

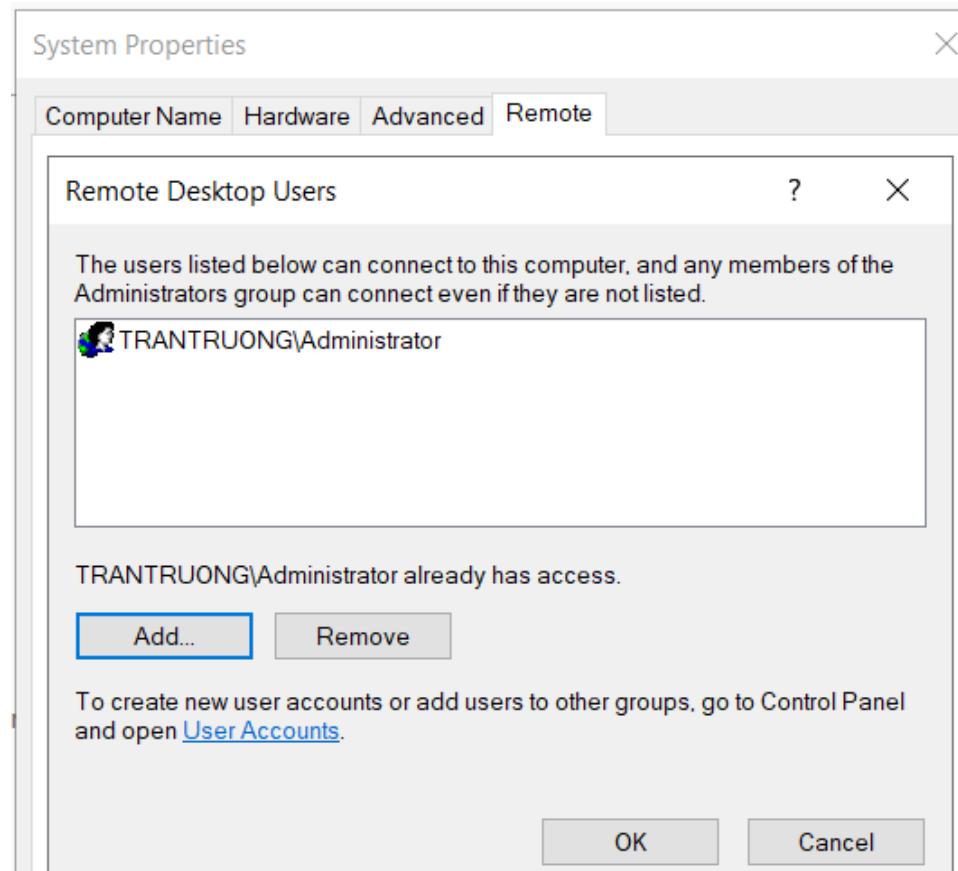
```
C:\Users\neuer>
```

2.5. Cấu hình cho phép admin remote desktop

- Bước 1: Vào Server Manager > Local Server > Click Remote Desktop > Chọn Allow remote connections to this computer > Select Users...



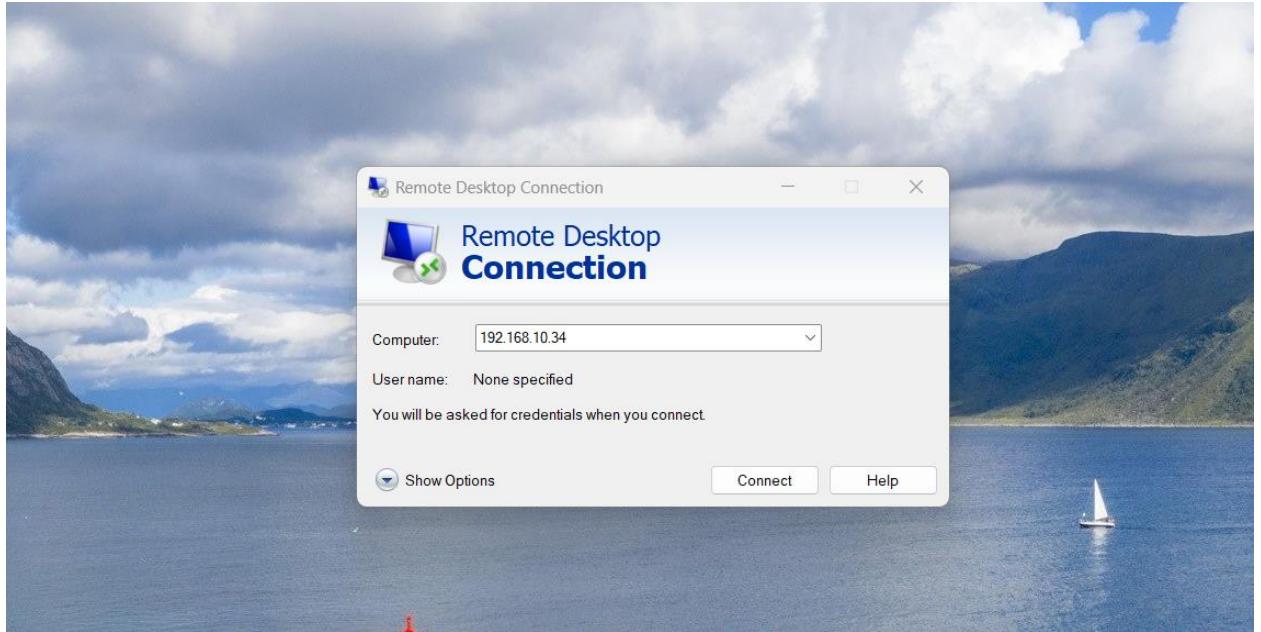
- Bước 2: Add user Administrator > OK



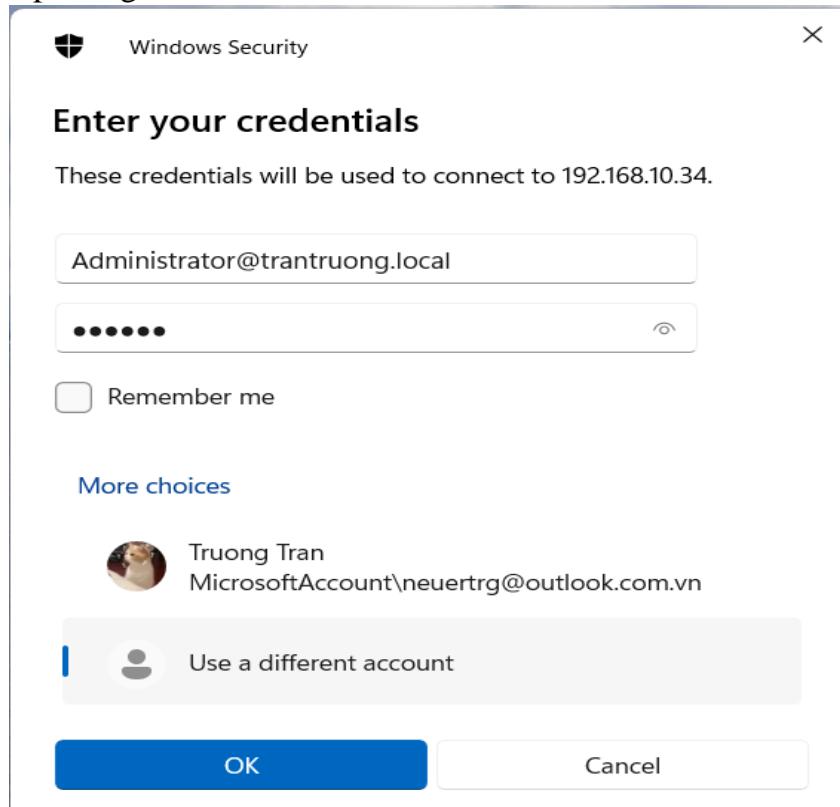
- Bước 3: Remote Desktop đã được bật

PROPERTIES	
For WIN-DCQPTORU185	
Computer name	WIN-DCQPTORU185
Domain	trantruong.local
Windows Defender Firewall	Domain: Off
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet0	192.168.10.34

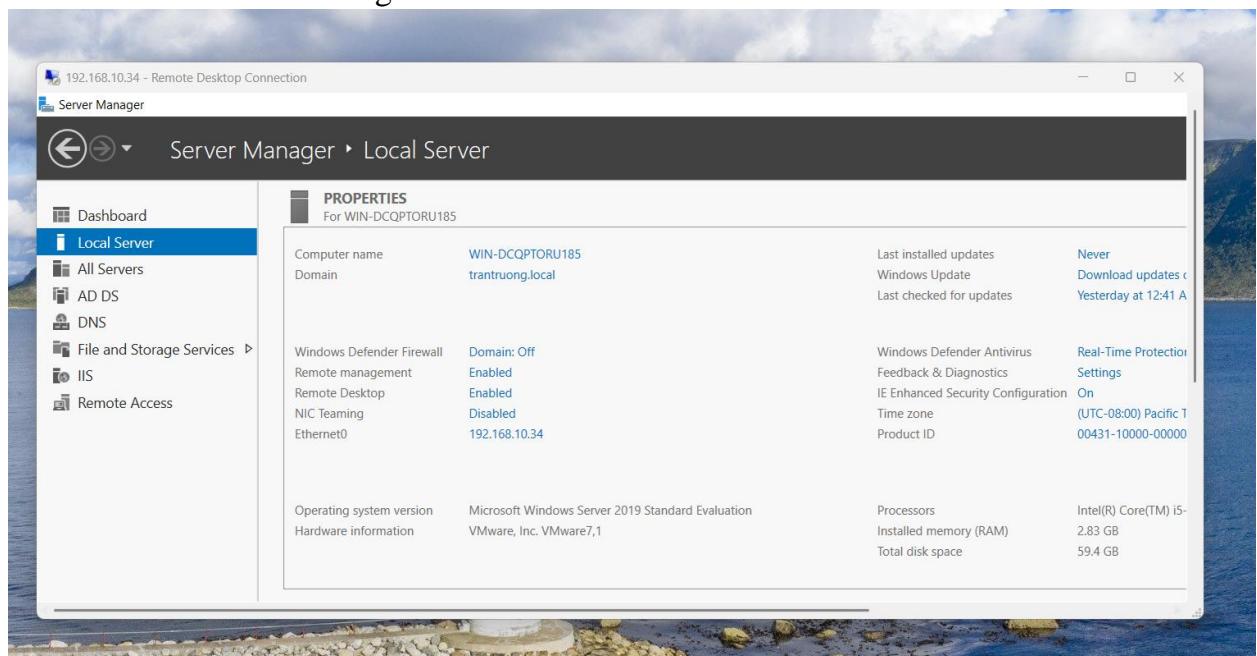
- Bước 4: Từ máy Client nhập địa chỉ Domain Controller, nhấn Connect



- Bước 5: Nhập thông tin xác thực rồi nhấn OK

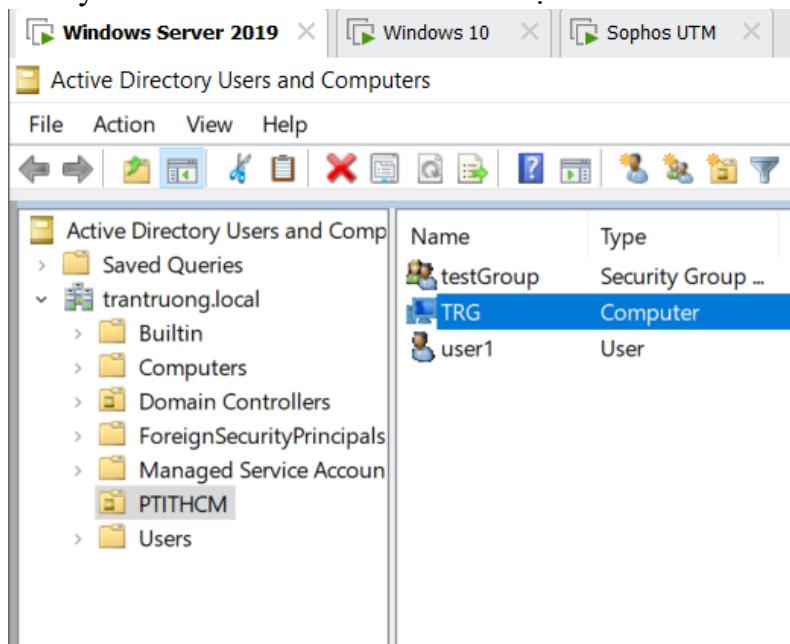


- Bước 6: Kết nối thành công

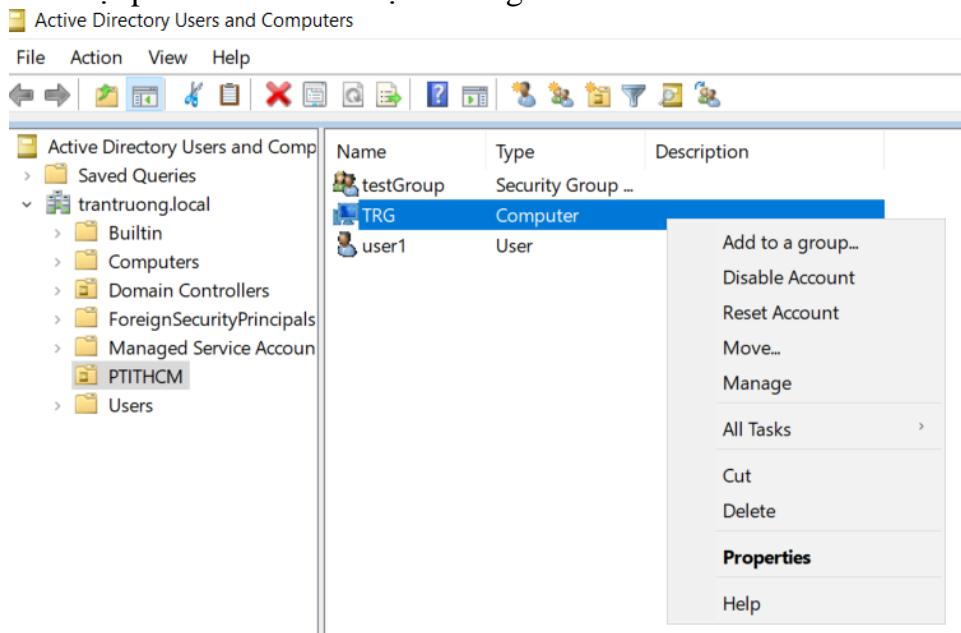


2.6. Cấu hình cho phép user1 remote desktop vào PC1

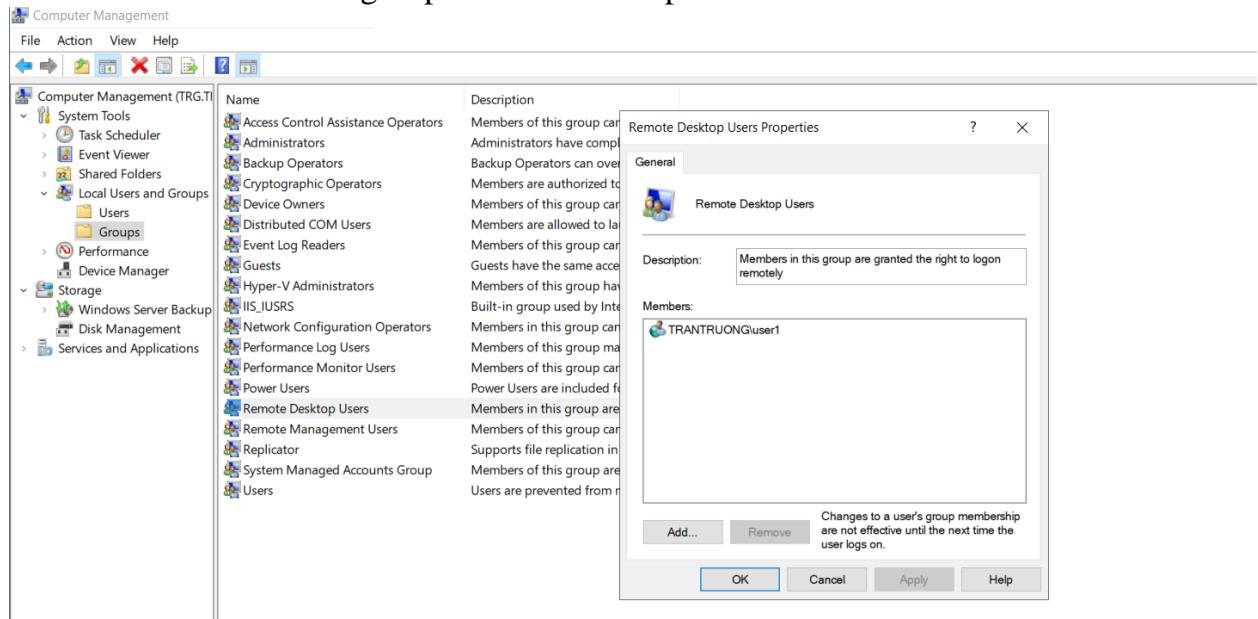
- Bước 1: Thêm máy PC1 vào OU “PTITHCM” đã tạo ở trên



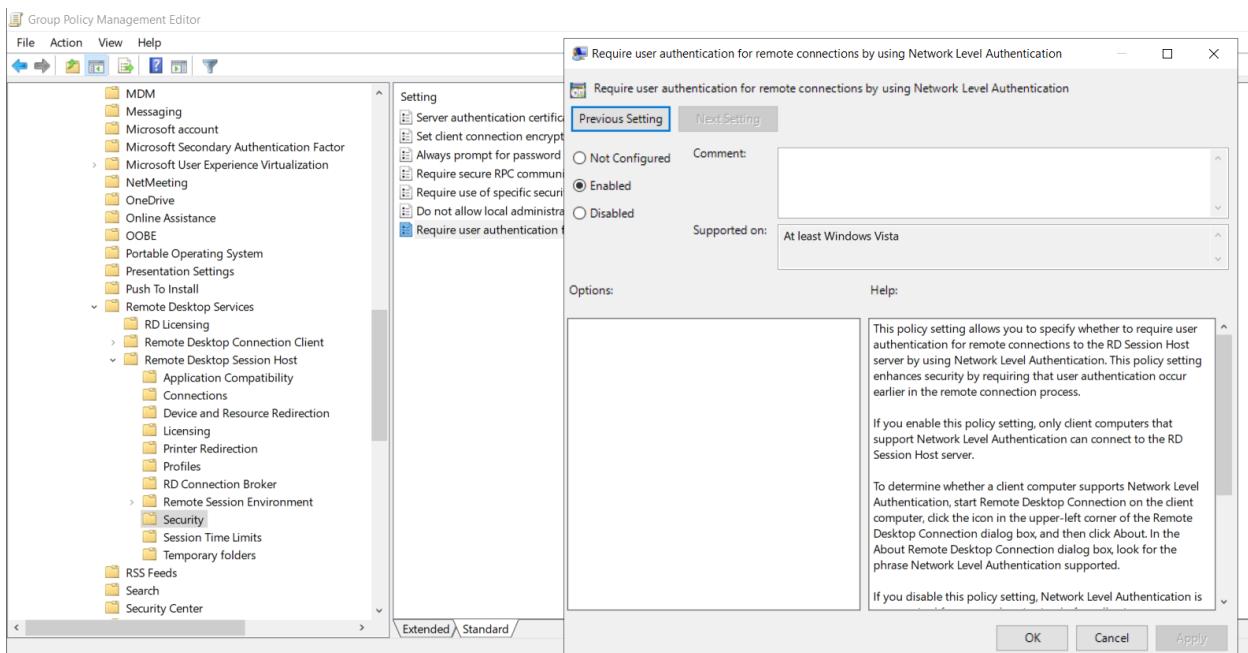
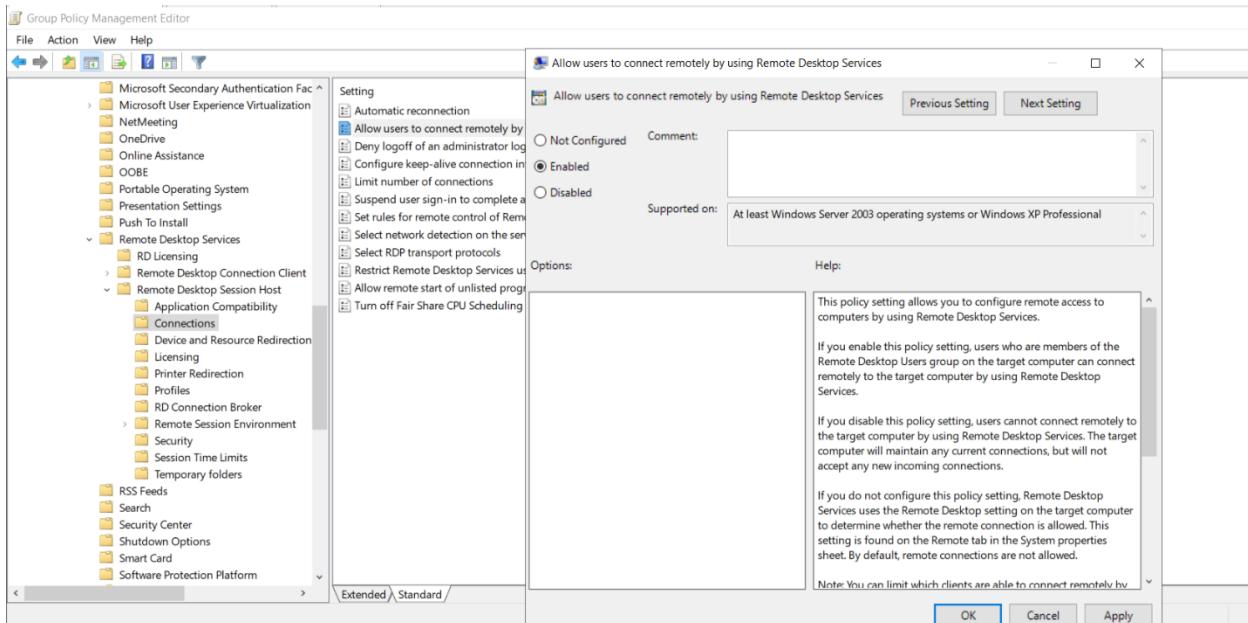
- Bước 2: Chuột phải vào PC và chọn Manage



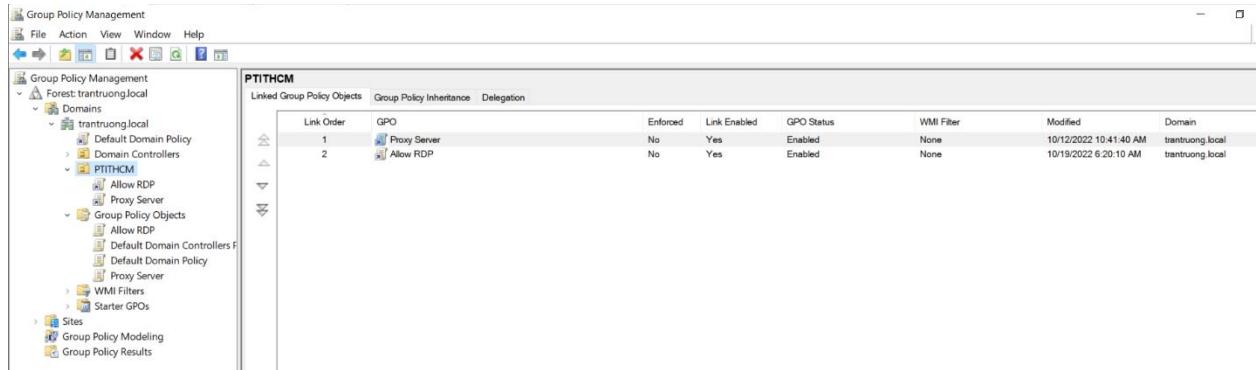
- Bước 3: Thêm user1 vào group Remote Desktop Users



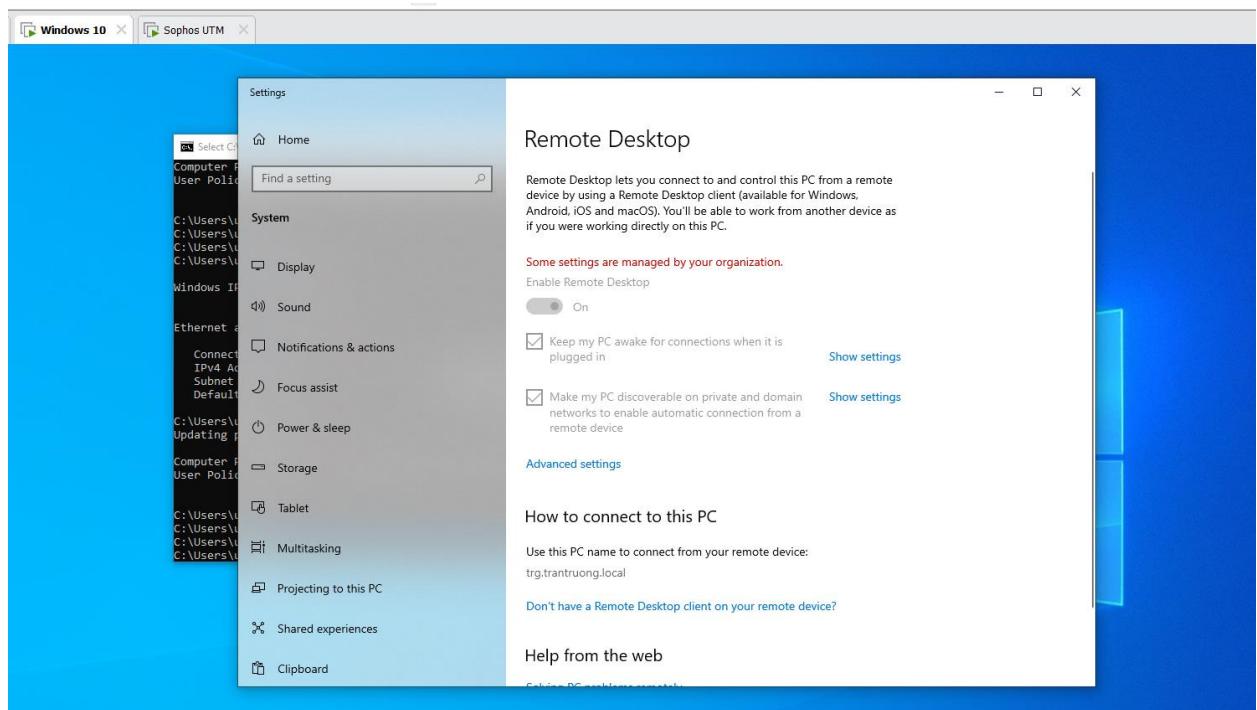
- Bước 4: Tạo Group Policy cho phép remote desktop PC1



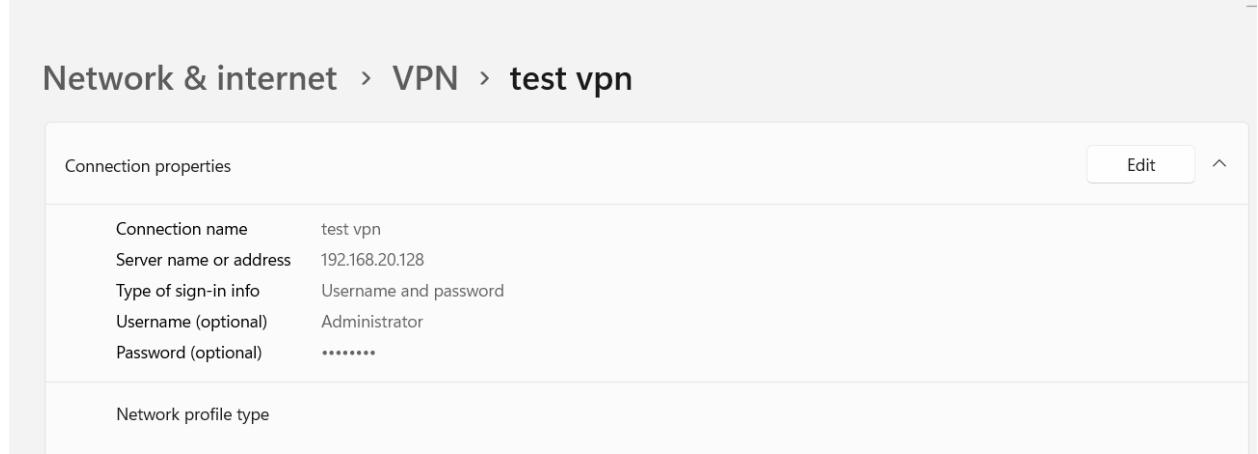
- Bước 5: Link GPO với OU “PTITHCM” đã tạo ở trên và chạy lệnh “gpupdate /force để cập nhật lại”



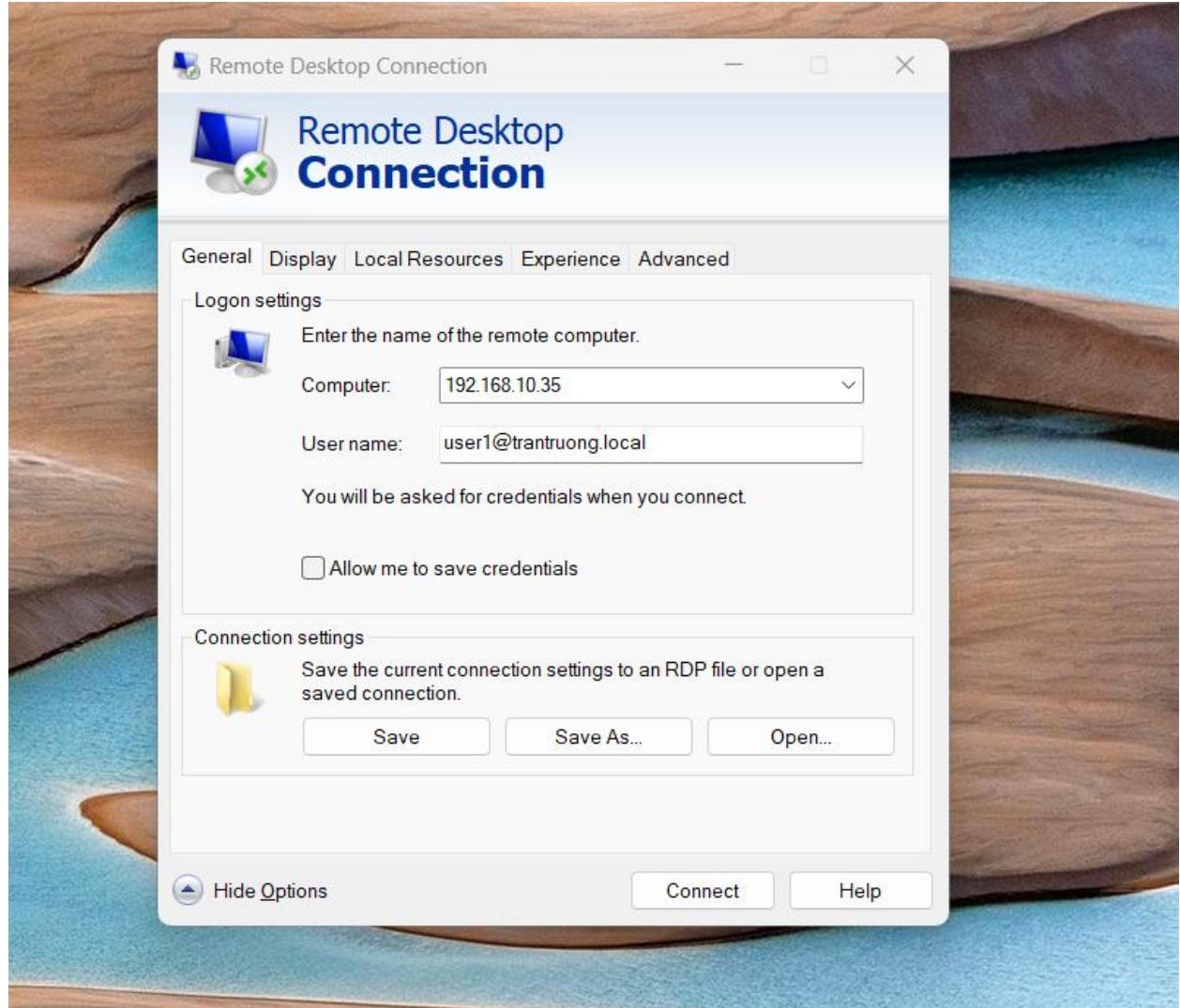
- Bước 6: Khởi động lại PC1 và kiểm tra lại cài đặt Remote Desktop đã được bật chưa



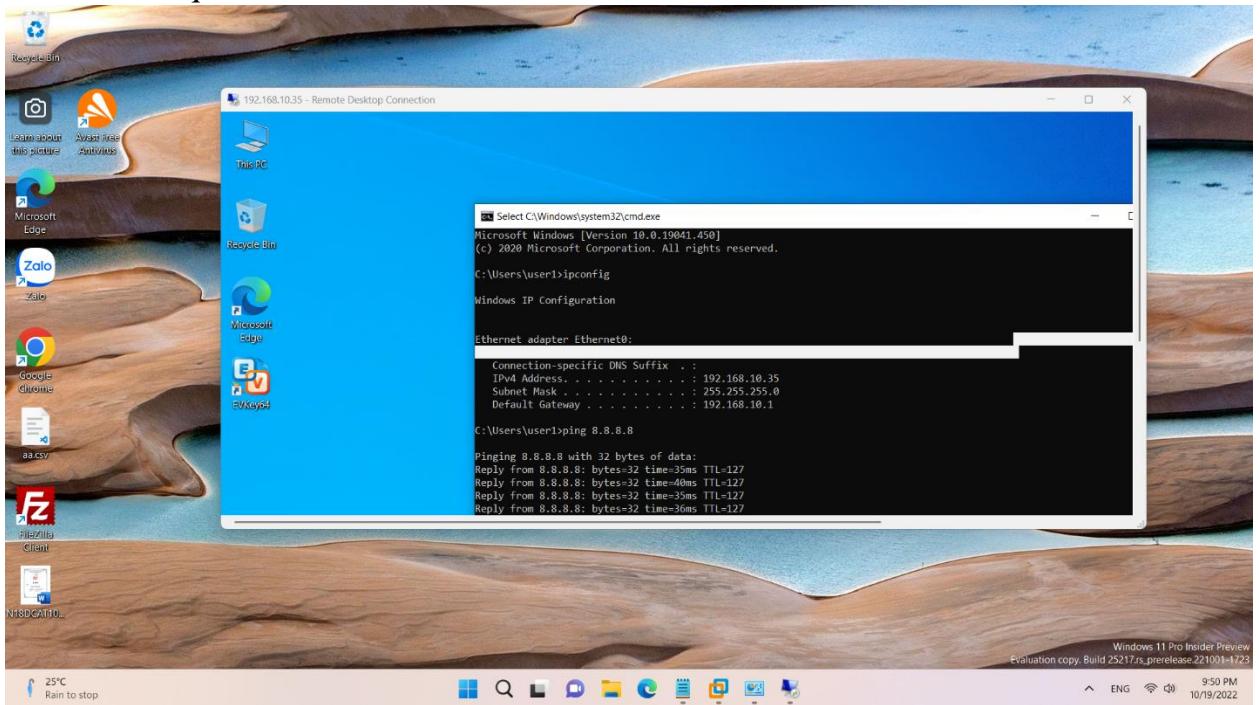
- Bước 7: Từ máy Client kết nối lại VPN



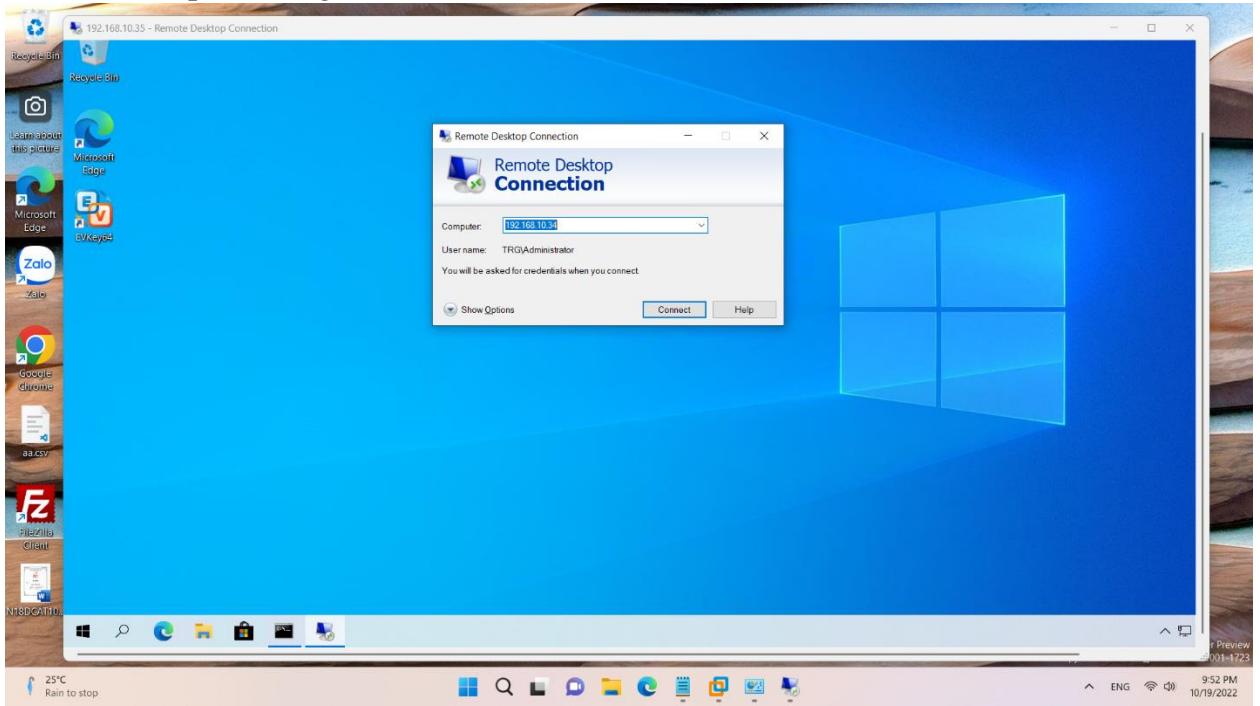
- Bước 8: Thực hiện remote desktop đến PC1



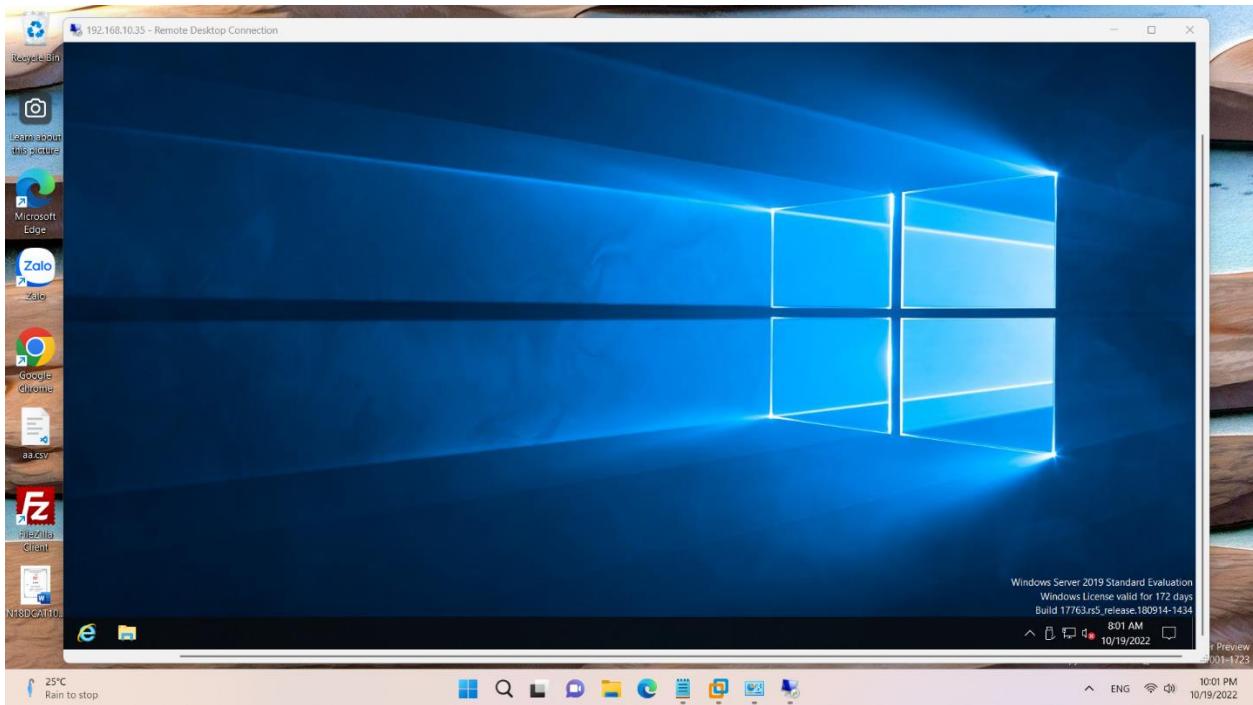
- Bước 9: Kết quả remote



- Bước 10: Tiếp tục dùng kết nối remote ở trên để remote tới Windows Server

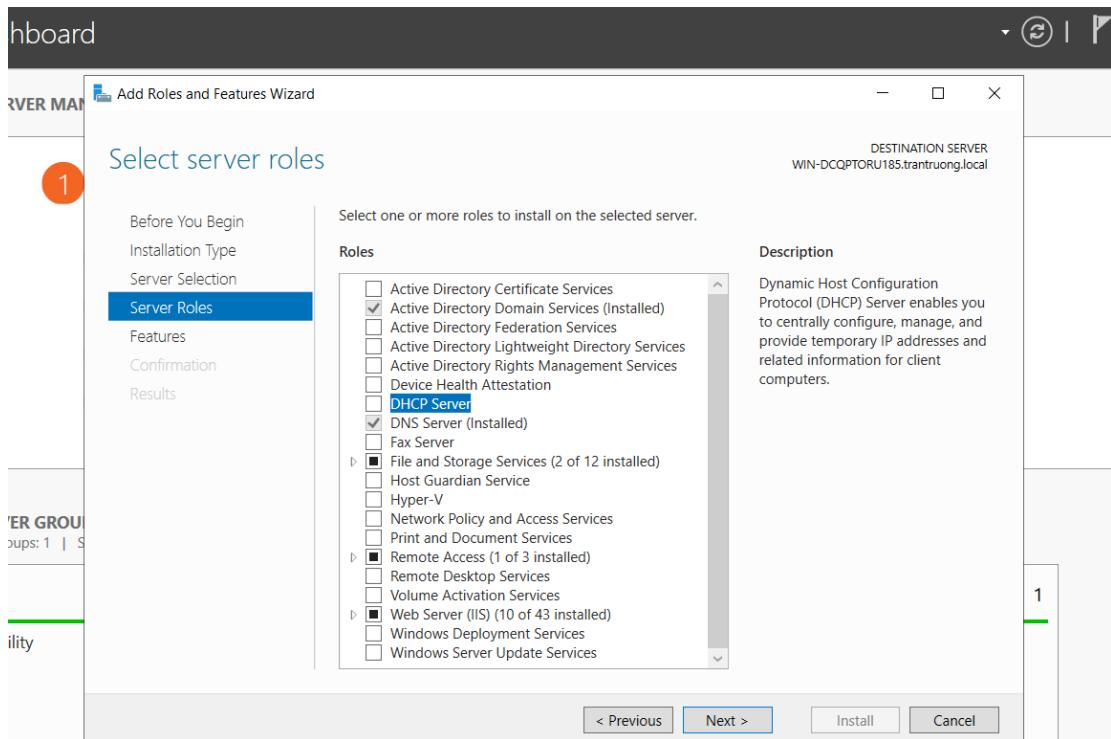


- Bước 11: Kết quả

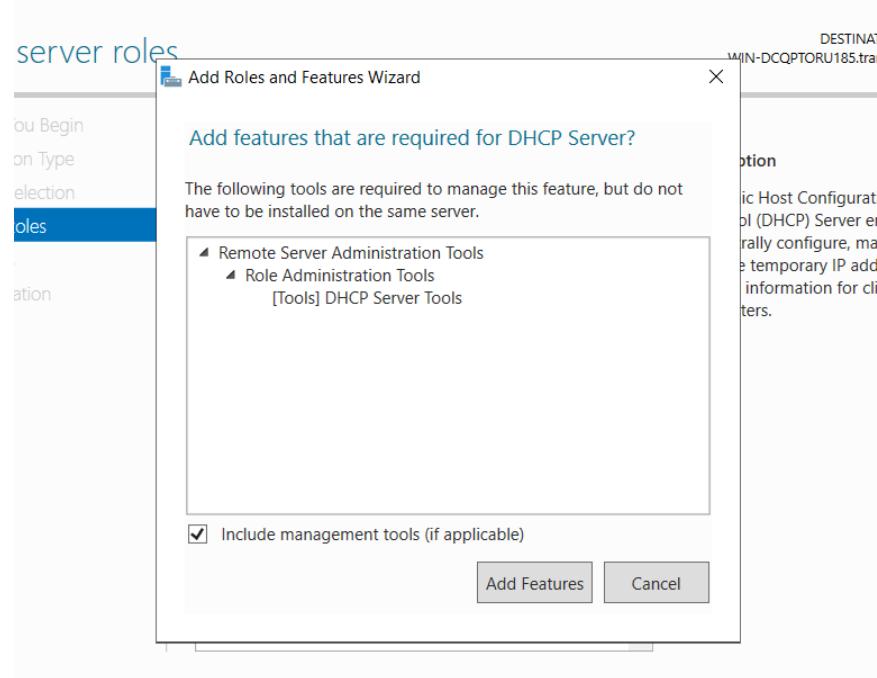


2.7. Cài đặt và cấu hình DHCP server trên Windows Server

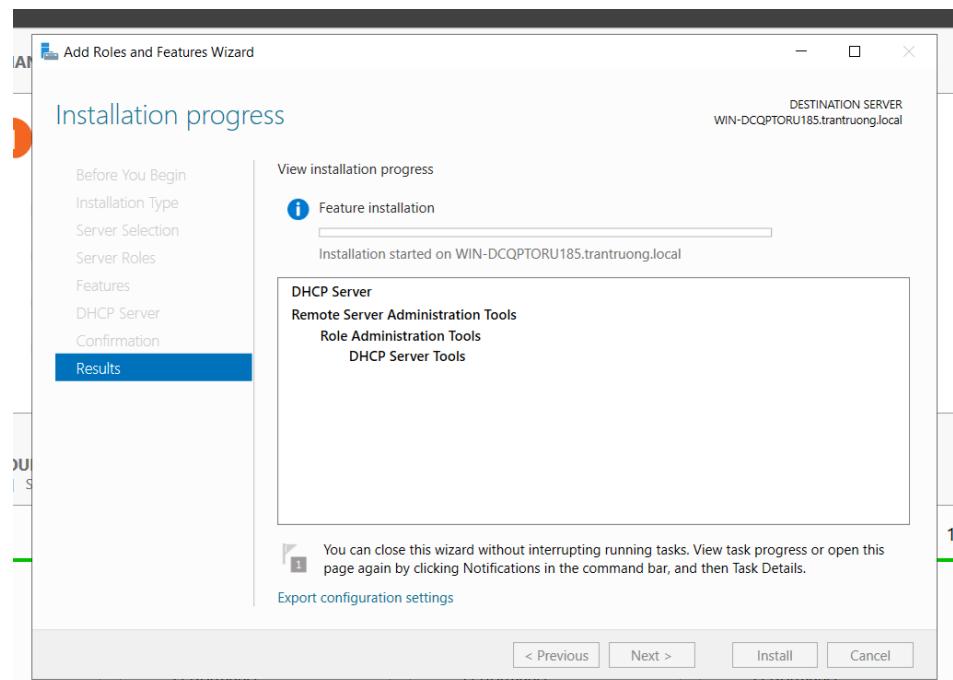
- Bước 1: Tích chọn DHCP Server



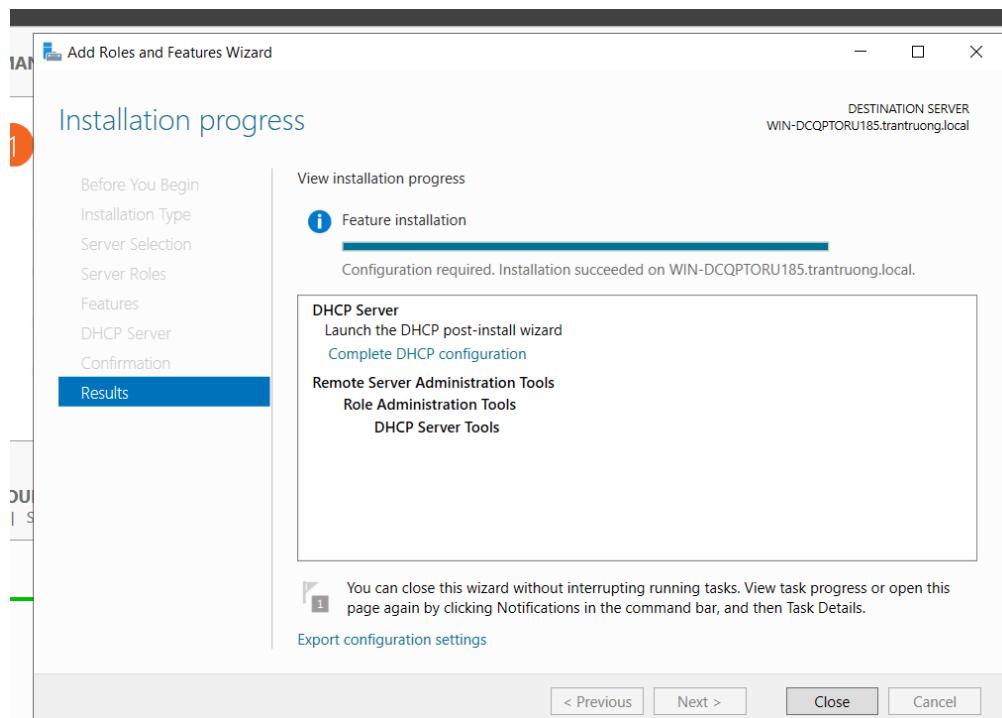
- Bước 2: Chọn Add Futures



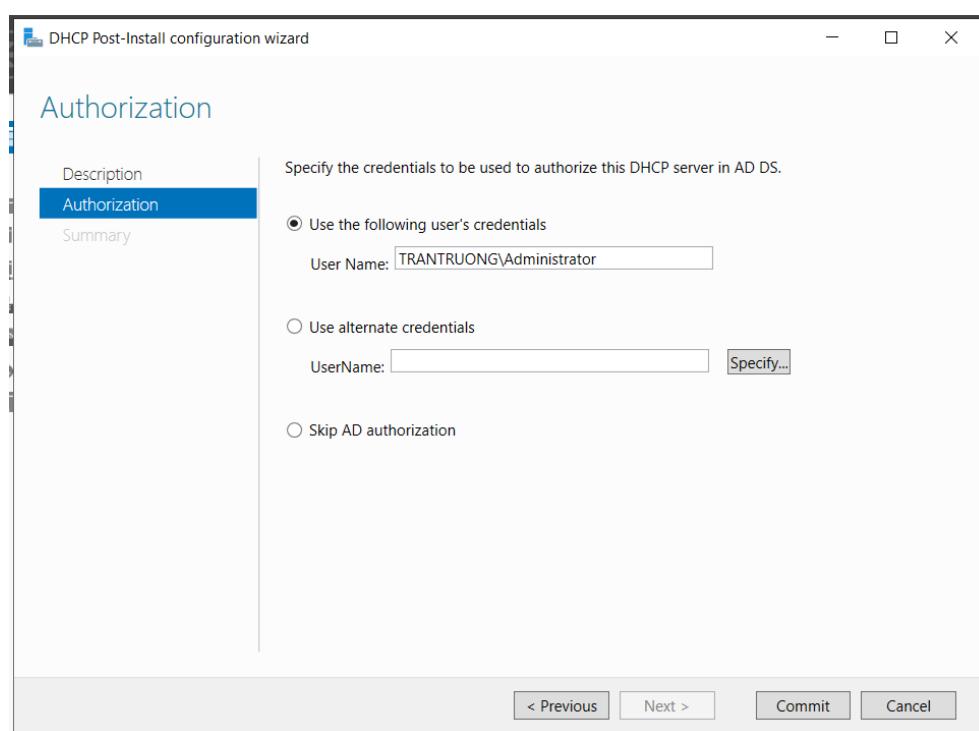
- Bước 3: Nhấn Install và đợi quá trình cài đặt hoàn tất



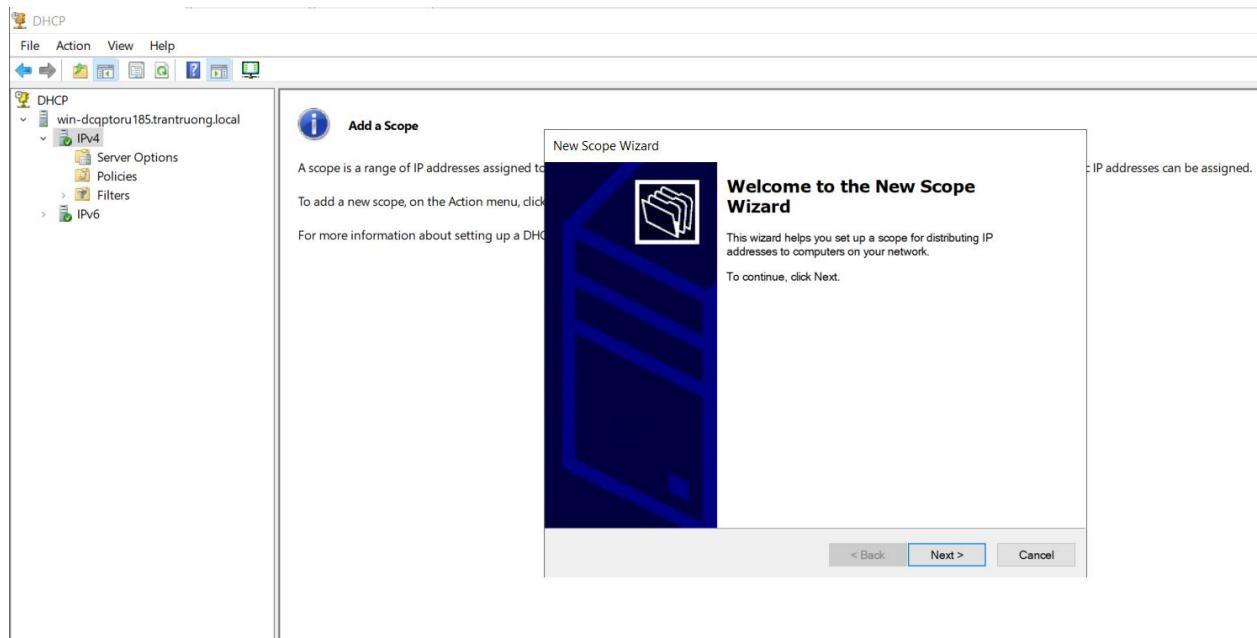
- Bước 4: Click “Complete DHCP configuration”



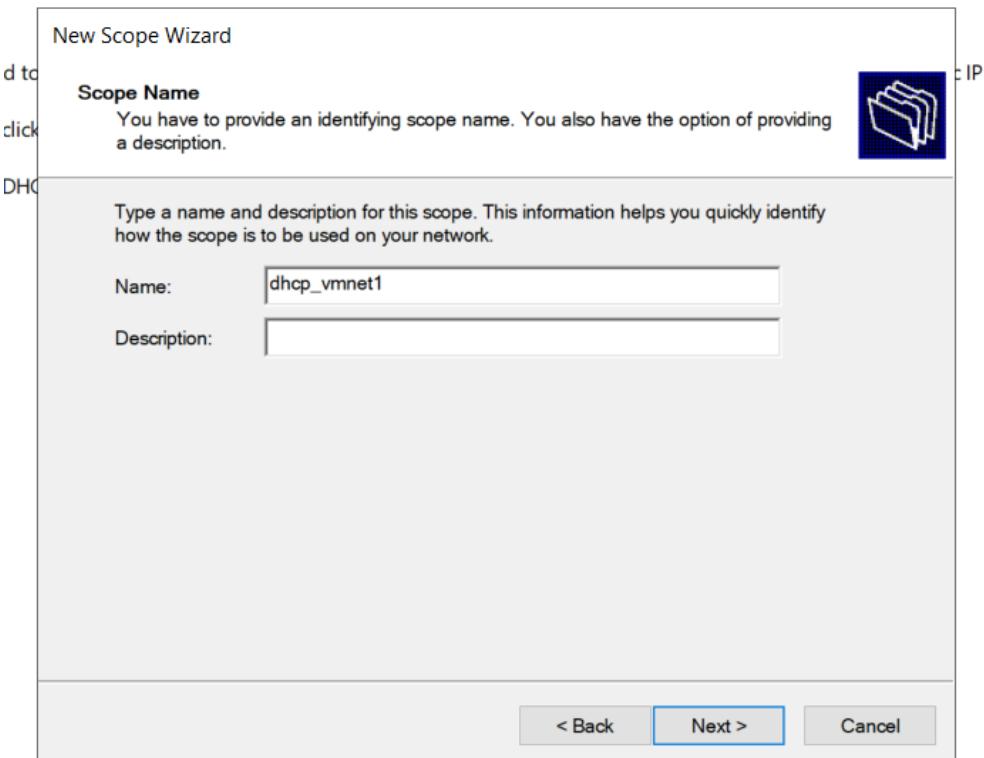
- Bước 5: Nhấn Commit



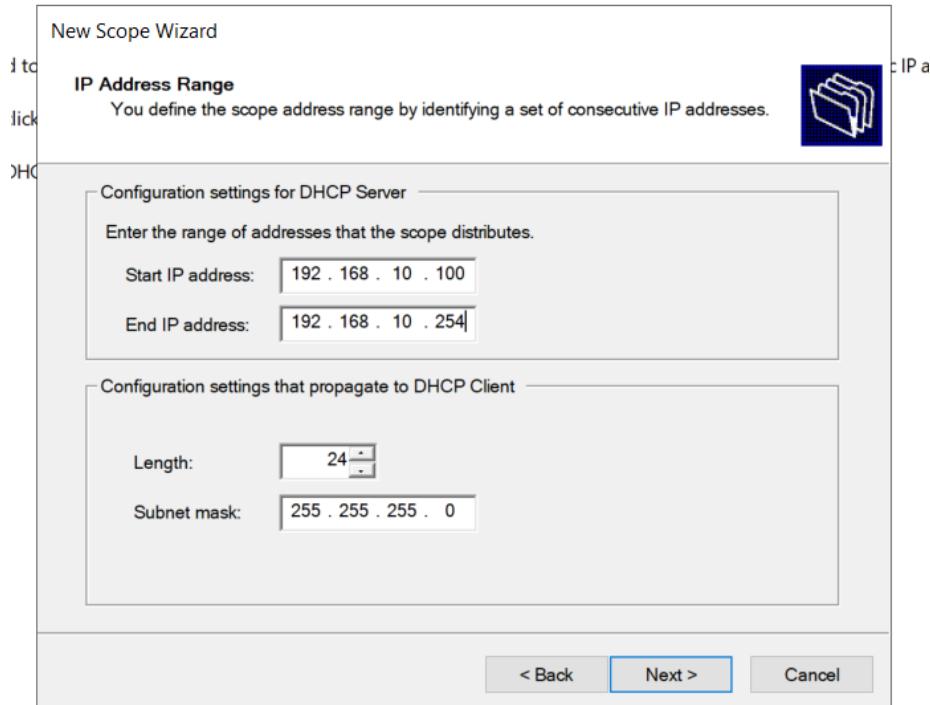
- Bước 6: Vào tools > DHCP > Ipv4 >new scope



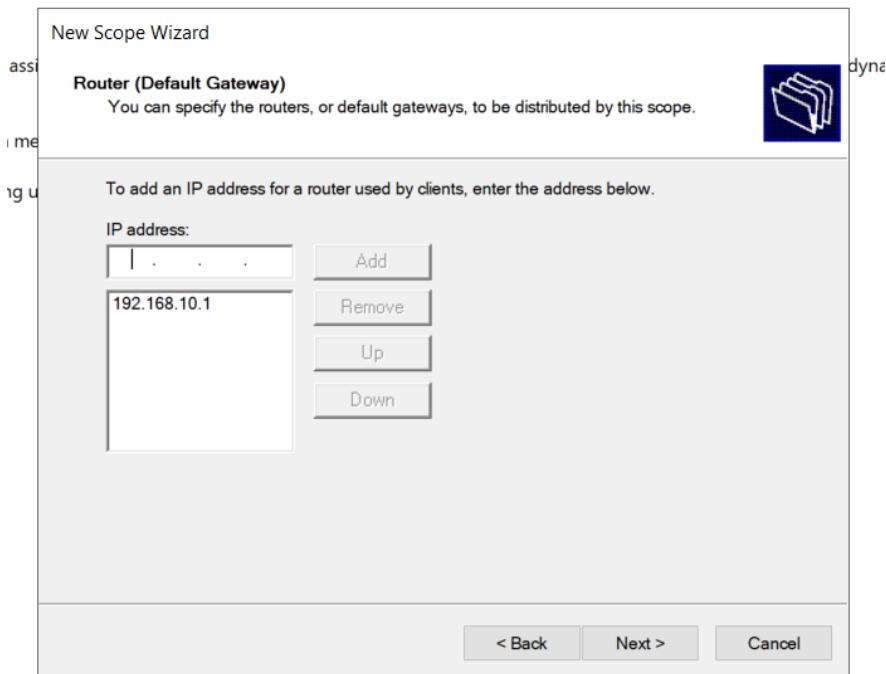
- Bước 7: Đặt tên Scope



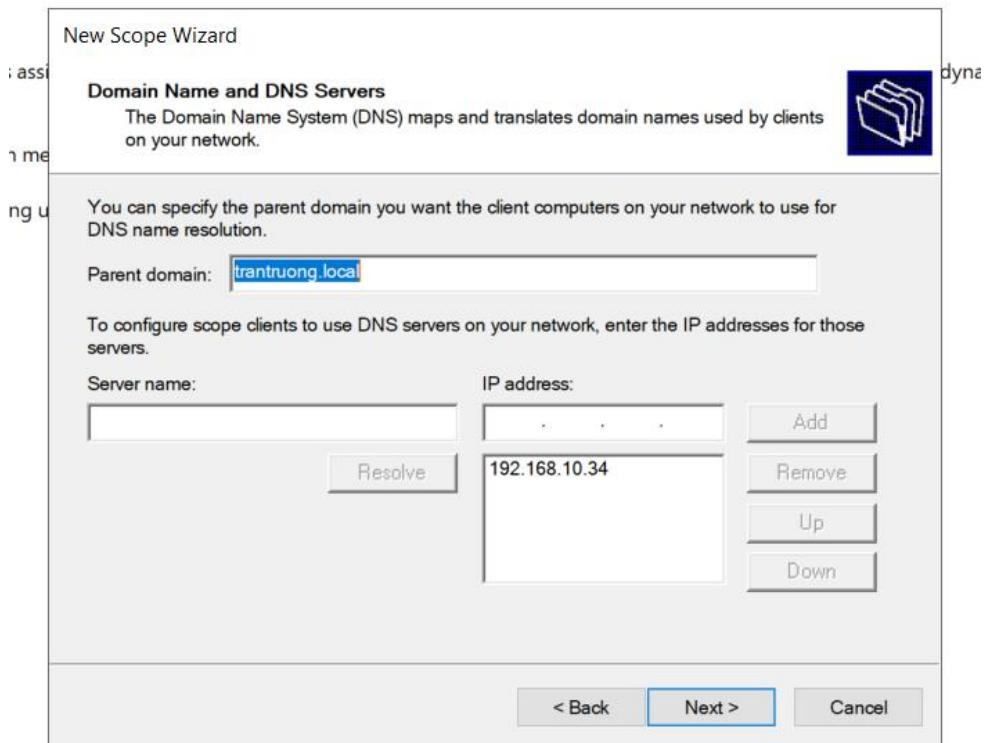
- Bước 8: Dải ip sẽ cấp phát



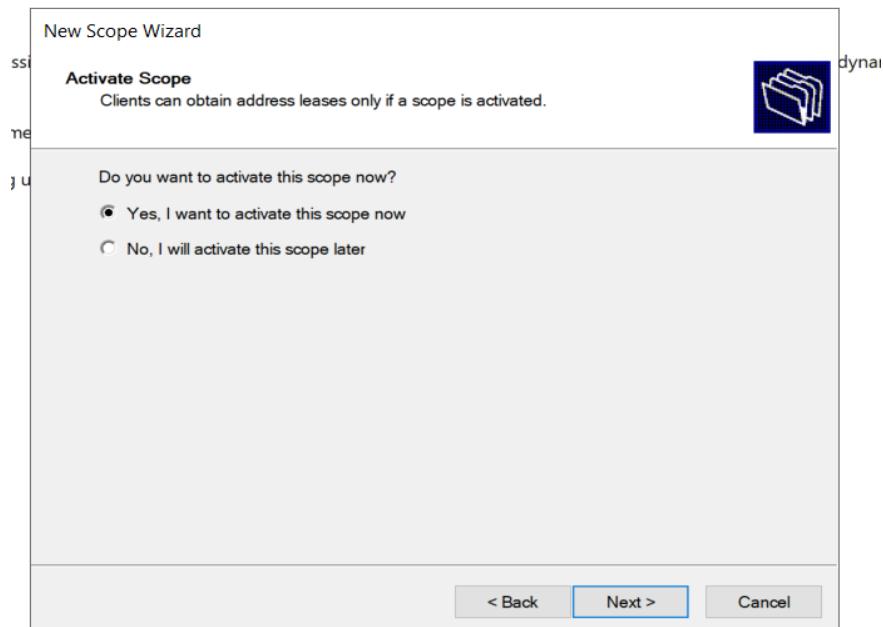
- Bước 9: Thêm Default Gateway



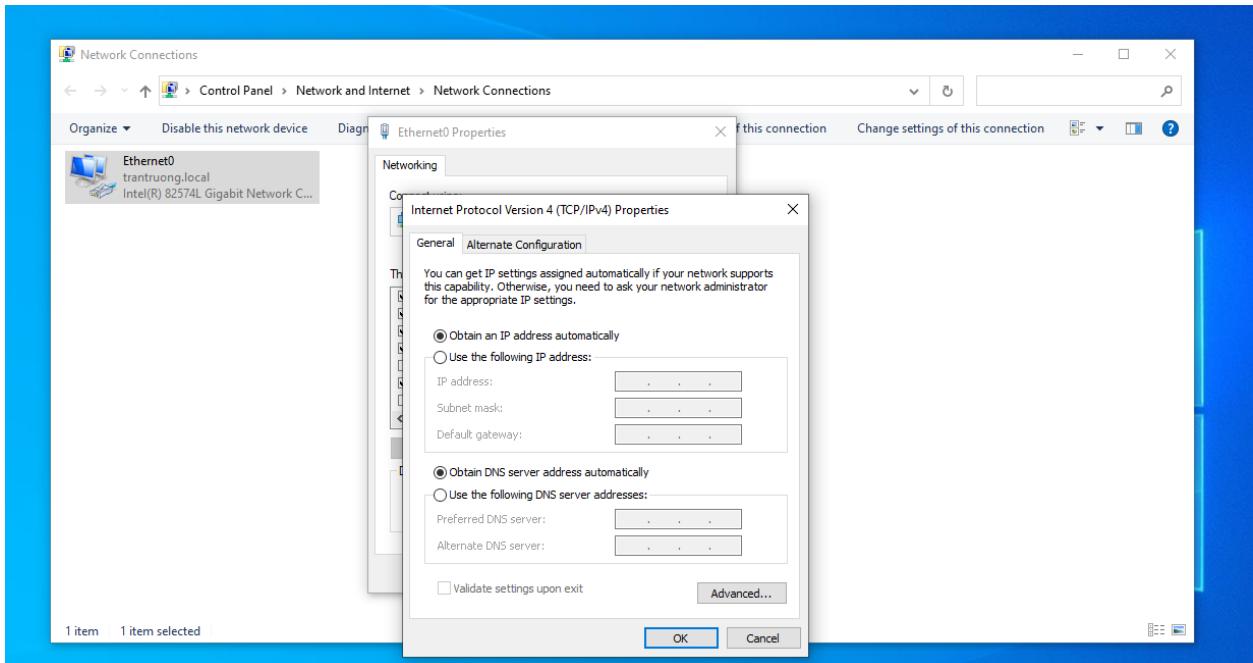
- Bước 10: Thêm DNS Server



- Bước 11: Kích hoạt Scope



- Bước 12: Trên máy PC1 điều chỉnh cài đặt ip dhcp



- Bước 13: Kiểm tra kết quả máy tính đã nhận IP động do server cấp

