HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN II

---□📖□---

BÁO CÁO ĐỒ ÁN

Môn: An Toàn Mạng

Đề tài: Thiết lập kết nối OpenVPN cho người dùng từ xa

Giảng viên hướng dẫn:
Trần Thị Dung

Nhóm sinh viên 18 thực hiện:

Họ tên:	MSSV:
Vũ Phạm Đức Thịnh (leader)	N18DCAT087
Đoàn Ngọc Chuẩn	N18DCAT011
Nguyễn Quốc Bảo Hiệp	N18DCAT021
Nguyễn Trung Tín	N18DCAT071
Nguyễn Văn Thành	N18DCAT083

A. TỔNG QUAN

1. VPN là gì?

Đầu tiên PN (privite network) là 1 hệ thống mạng LAN riêng biệt sử dụng các địa chỉ IP cùng dải với nhau để chia sẻ dữ liệu. VPN (virtual privite network) là 1 mạng dành riêng để kết nối các máy tính với nhau thông qua đường truyền Internet, là 1 dịch vụ mạng ảo được triển khai trên Cơ sở hạ tầng của hệ thống mạng công cộng (Internet).

Virtual Private Network sử dụng kỹ thuật Tunneling Protocols. Đây là kỹ thuật đóng gói một gói tin dữ liệu bên trong một gói tin khác để tạo ra một kênh truyền an toàn.

VPN cung cấp những lợi ích bao gồm:

-Chi phí thiết lập mạng VPN tương đối thấp, do sử dụng chung hạ tầng Internet.

-Tính linh hoạt: VPN xóa bỏ mọi rào cản về vị trí địa lý, sẵn sang kết nối các mạng với nhau thông qua Internet.

-Tính bảo mật: Các dữ liệu quan trọng sẽ được che giấu đối với những người được phép truy cập VPN. VPN sử dụng các giao thức, thuật toán mã hóa các phương pháp chứng thực để bảo mật dữ liệu trong quá trình truyền tin.

-Bảo mật về địa chỉ IP: Các thông tin được gửi đi trên VPN đã được mã hóa, do đó địa chỉ IP bên trong mạng riêng được che giấu, và chỉ sử dụng các IP ở bên ngoài Internet.

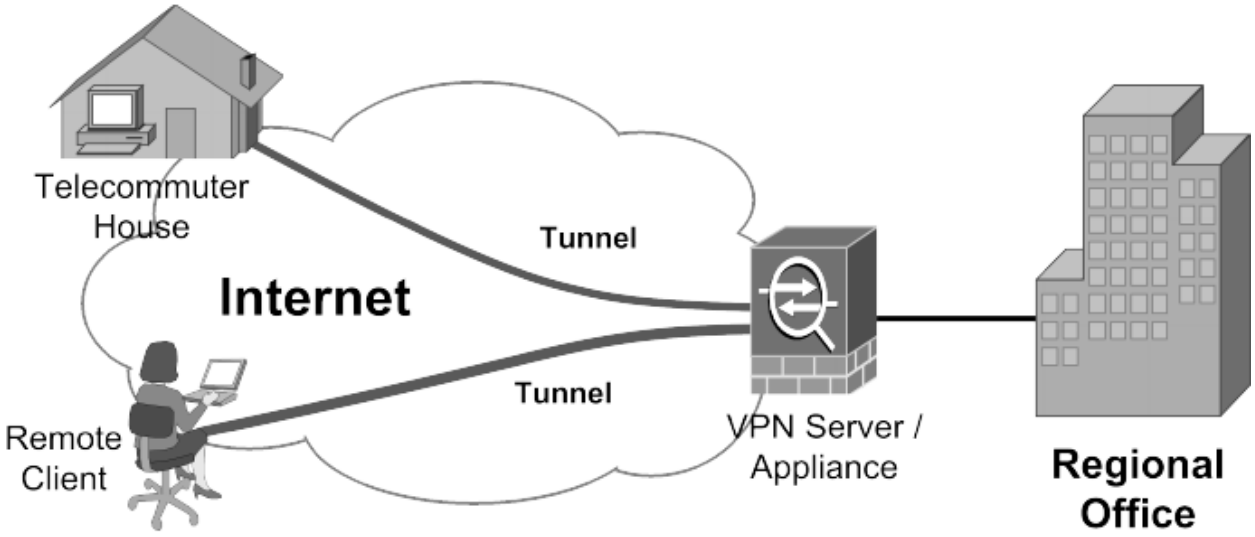
2. Phân loại VPN

Có 3 loại VPN thông dụng:

- VPN Cục bộ (Intranet VPN)
- VPN truy cập từ xa (Remote Access VPN)
- Mạng riêng ảo mở rộng (Extranet VPN)

2.1 Remote Access VPN

Remote Access VPN thường được sử dụng cho các kết nối có băng thông thấp giữ một thiết bị của người dùng như PC, Ipad, … và một thiết bị Gateway VPN. Remote Access VPN thông thường sử dụng tunnel mode cho các kết nối.



Người dùng ở xa sử dụng các phần mềm VPN để truy cập vao mạng của công ty thông qua Gateway hoặc VPN concentrator (bản chất là một server), giải pháp này thường được gọi là client/server), giải pháp này thường được gọi là client/server. Trong giải pháp này, người dùng thường sử đụng các công nghệ truyền thống để tạo lại các tunnel về mạng của họ.

2.2 VPN Cục bộ (Intranet VPN)

Intranet VPN thường được dùng để kết nối các nhánh Văn phòng từ xa của một tổ chức với Intranet trung tâm của tổ chức đó.

2.3 Mạng riêng ảo mở rộng (Extranet VPN)

Khi một công ty có mối quan hệ mật thiết với một công ty khác (ví dụ nhờ đối tác cung cấp, khách hàng...), họ có thể xây dựng một VPN extranet kết nối LAN với LAN để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung.

3.Cách thức hoạt động VPN

VPN là một công cụ cho phép truy cập internet một cách an toàn mọi lúc mọi nơi. VPN hoạt động bằng cách tạo một "đường hầm" an toàn giữa thiết bị của cá nhân và nhà cung cấp VPN và nó bảo vệ user theo hai cách chính:

-Che giấu địa chỉ IP của user, bảo vệ danh tính và vị trí của user.

-Mã hóa lưu lượng giữa user và nhà cung cấp VPN để không ai trong mạng cục bộ có thể giải mã hoặc sửa đổi nó.

4. Window VPN

- Trên các hệ điều hành đều tích hợp sẵn. Đối với windows 8/8.1, windows 10 thì bạn vào click chuột phải vào biểu tượng wifi chọn Open Network & Internet -> Chọn VPN -> Add a VPN connection.

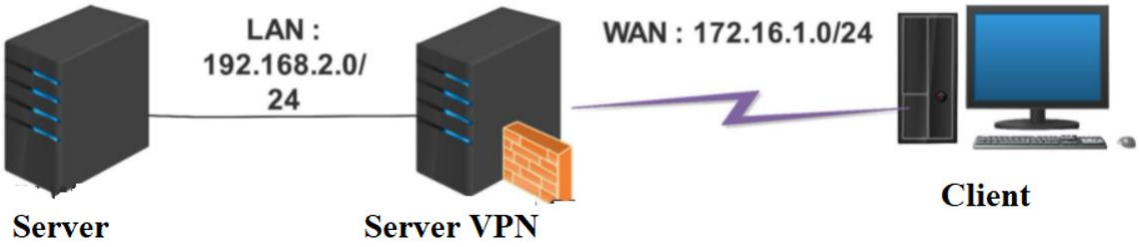
-Trên Windows Server các phiên bản thì dịch vụ Routing and Remote Access Service(RRAS) có chức năng VPN Server cho phép một máy tính trở thành một VPN Server, hỗ trợ các giao thức PPTP, L2TP trên IPsec, chấp nhận kết nối từ xa và kết nối Router-to-Router.

B. THỰC HIỆN

Tạo 1 VPN để nhân viên của doanh nghiệp, công ti có thể kết nối vào tài liệu từ xa, sử dụng khả năng kết nối từ xa của VPN, cùng với khả năng phân quyền của Window Server có thể tối ưu hóa khả năng hoạt động của doanh nghiệp công ti.(Remote Access VPN)

1. MÔ HÌNH

1.1 Mô hình thực hiện



Hình 1. Hình ảnh mô hình

1.2 Bảng địa chỉ

STT	Server name		Interface 1	Interface 1
1	VPN Server	IP	192.168.2.1	172.16.1.1
		SM	255.255.255.0	255.255.255.0
2	Client	IP	172.16.1.10	
		SM	255.255.255.0	
		DG	172.16.1.1	
3	Server	IP	192.168.2.3	
		SM	255.255.255.0	
		DG	192.168.2.1	
		DNS	192.168.2.3	

2. CÀI ĐẶT

2.1 Máy Server

-Máy Server làm File server chứa tài liệu để client remote access vào lấy tài liệu khi đang công tác ở xa.
-Cài đặt: Trên máy ảo, Card mạng VMnet 2(192.168.2.3/24)

-Thăng cấp lên domain controller

2.2 Máy Server VPN

-Máy Server VPN làm VPN Server, trên máy server này có 2 card mạng, 1 nối với mạng LAN, 1 card nối ra đường WAN cho client ở dải IP WAN có thể remote access vào và lấy tài liệu. Đã cài đặt dịch vụ Routing and Remote Access Service.
-Cài đặt máy áo: 2 card mạng
+Card 1: VMnet 2(192.168.2.1/24)

+Card 2: VMnet 3(172.16.1.1/24)

2.3 Máy Client

-1 máy Client làm người dùng client ở ngoài Internet có thể VPN vào mạng doanh nghiệp để lấy tài liệu làm việc. Đã join domain. IP: 172.16.1.10
-1 máy cùng mạng Internal với **máy Server.** Cài đặt trên máy ảo, card mạng VMnet 2, cùng card mạng với máy Server Domain. Đã join domain. IP: 192.168.2.10/24

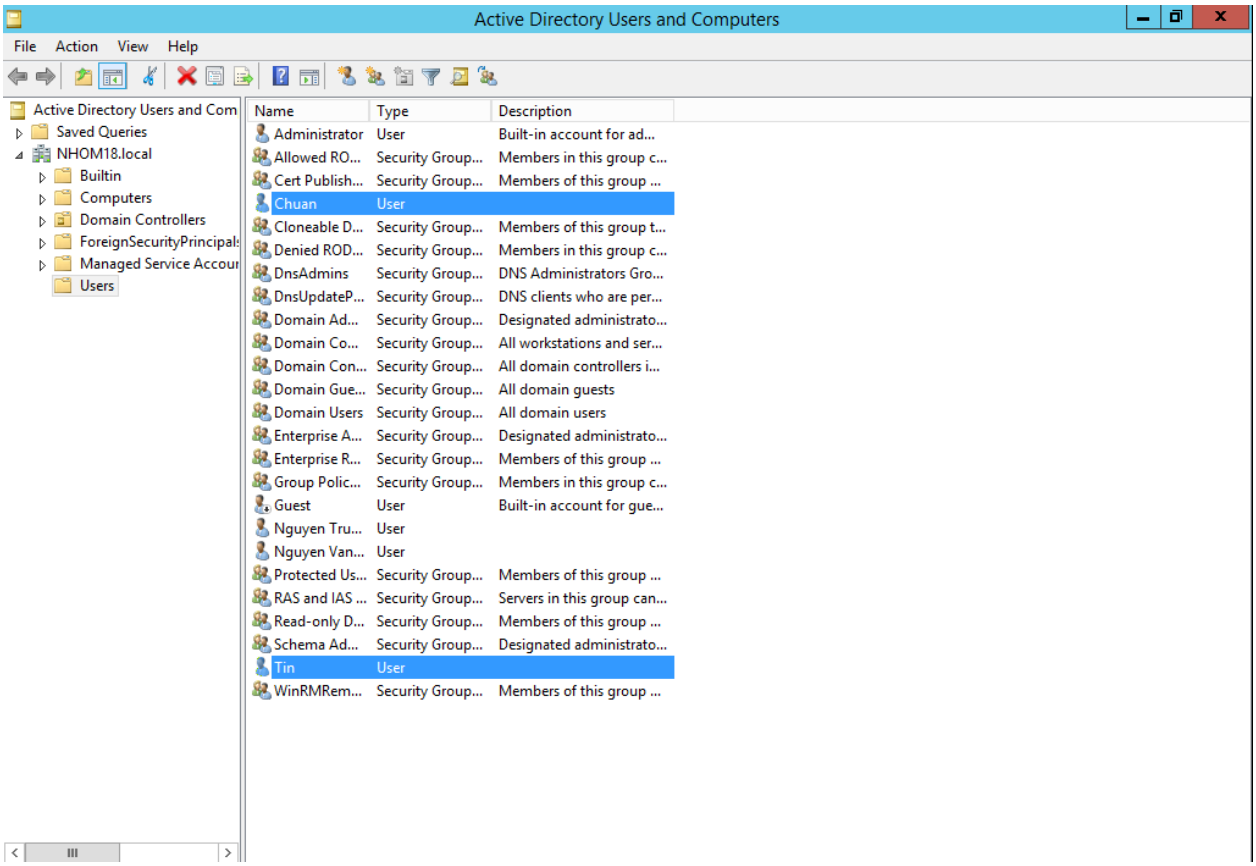
3. QUÁ TRÌNH THỰC HÀNH

3.1 Lab cơ bản

3.1.1 Cấu hình trên máy Windows Server

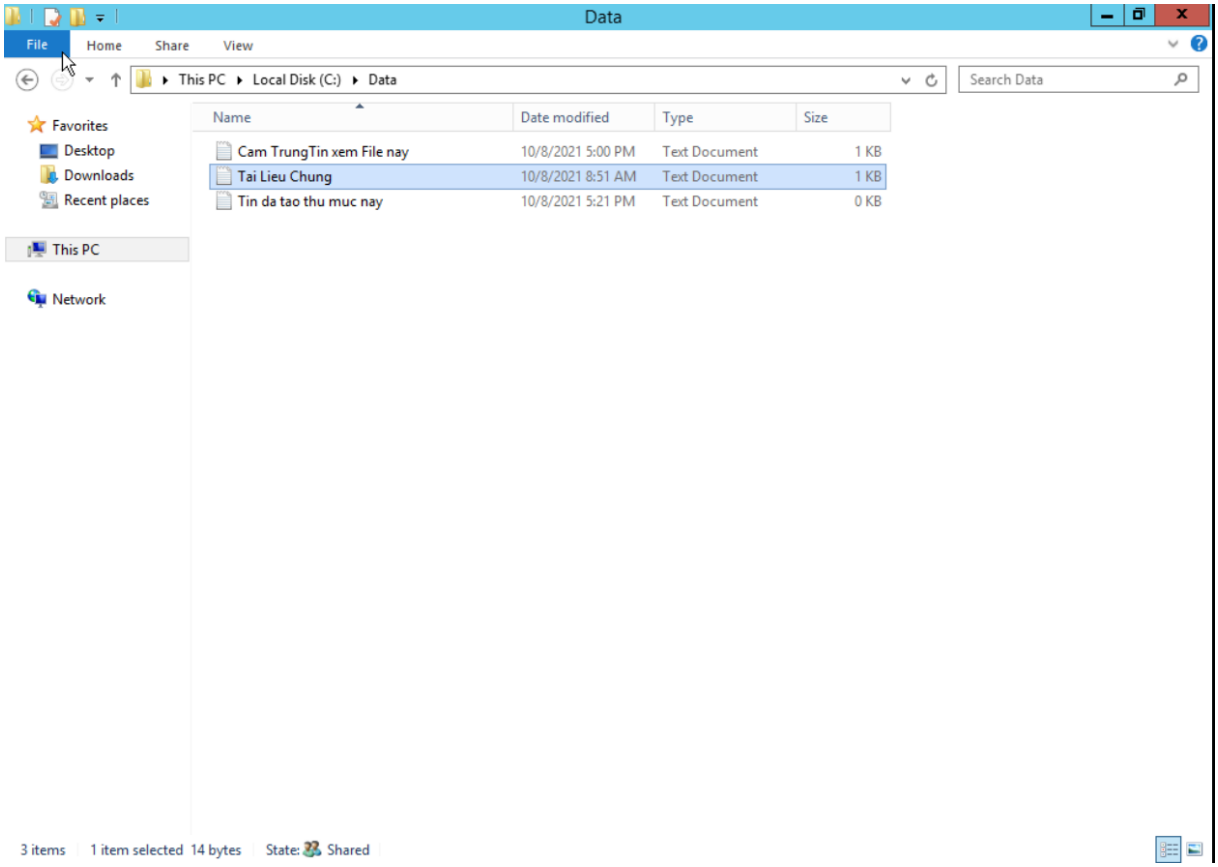
Bước 1: Tạo 2 tài khoản User: doanchuan và trungtin để thiết lập quyền Remote access, lấy tài liệu tại máy chủ từ xa

-Vào Active Directory User Computers→nhom18.local→User→New Users



Hình 2. Tạo Thành công 2 User trungtin và doanchuan

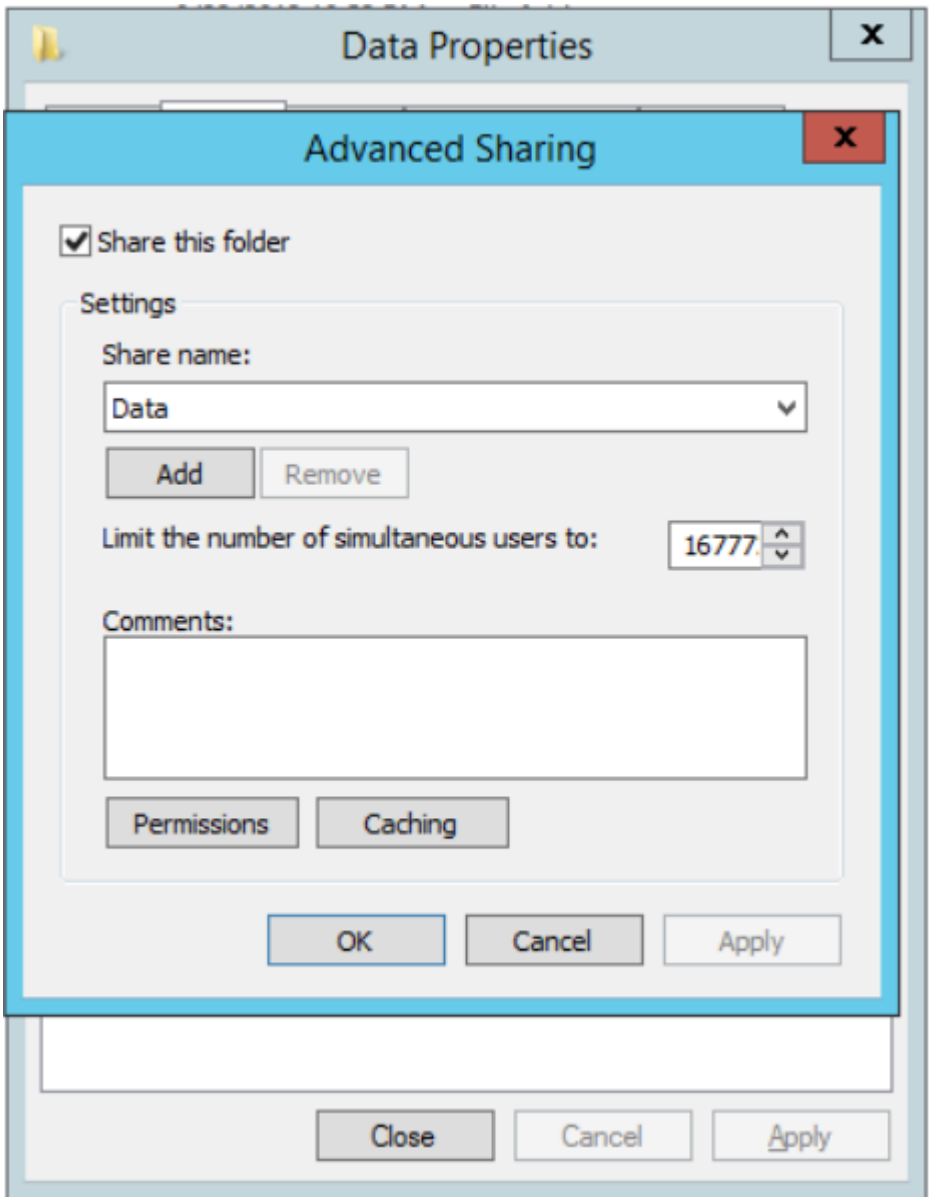
Bước 2: Tại ổ C tạo folder Data→ Tạo file Tailieuchung



Hình 3. Tạo File tài liệu để User truy cập từ xa lấy

Bước 3: Tiến hành thiết lập quyền truy cập cho User

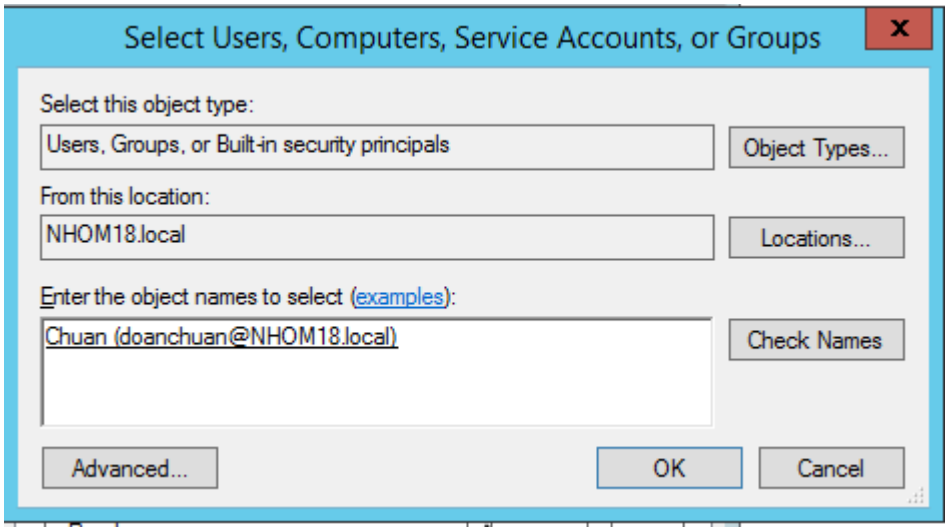
-Chuột phải vào thư muc Data→Properties→Sharing→Share→ Advanced Sharing



Hình 4. Hộp thoại Advanced Sharing xuất hiện

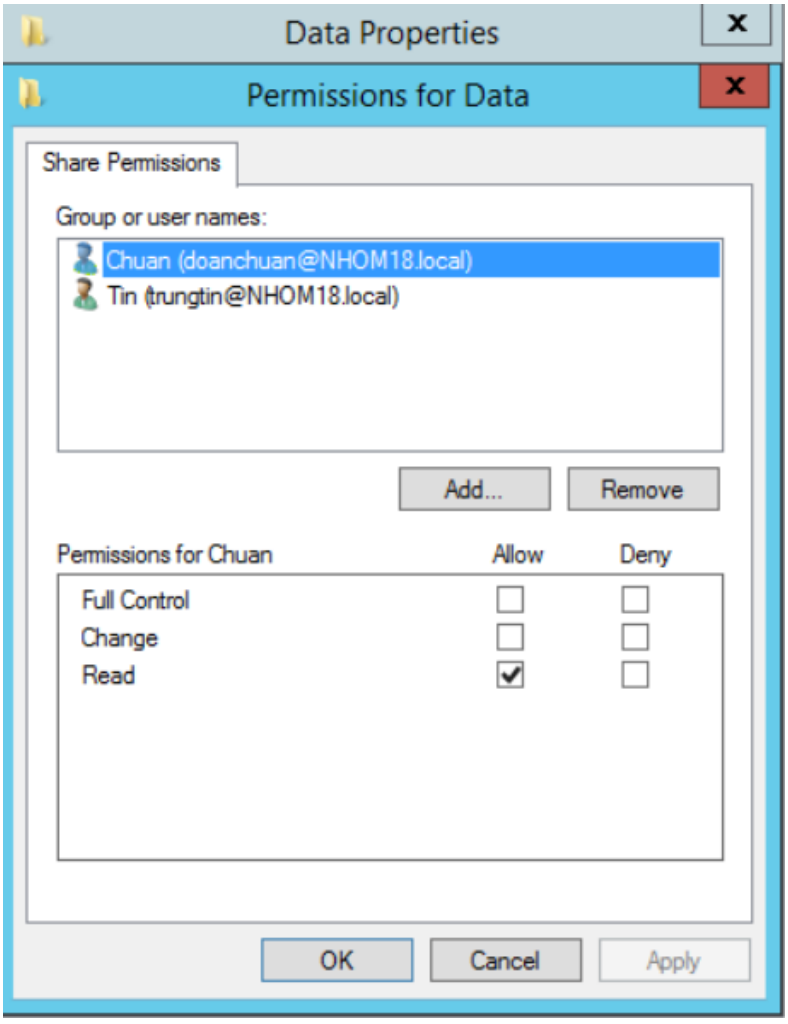
Bước 4: Thiết lập quyền cho 2 user **trungtin** và **doanchuan** vừa tạo

Phân quyền: Tại hộp thoại Advanced Sharing chọn Permissions→Add để thêm User



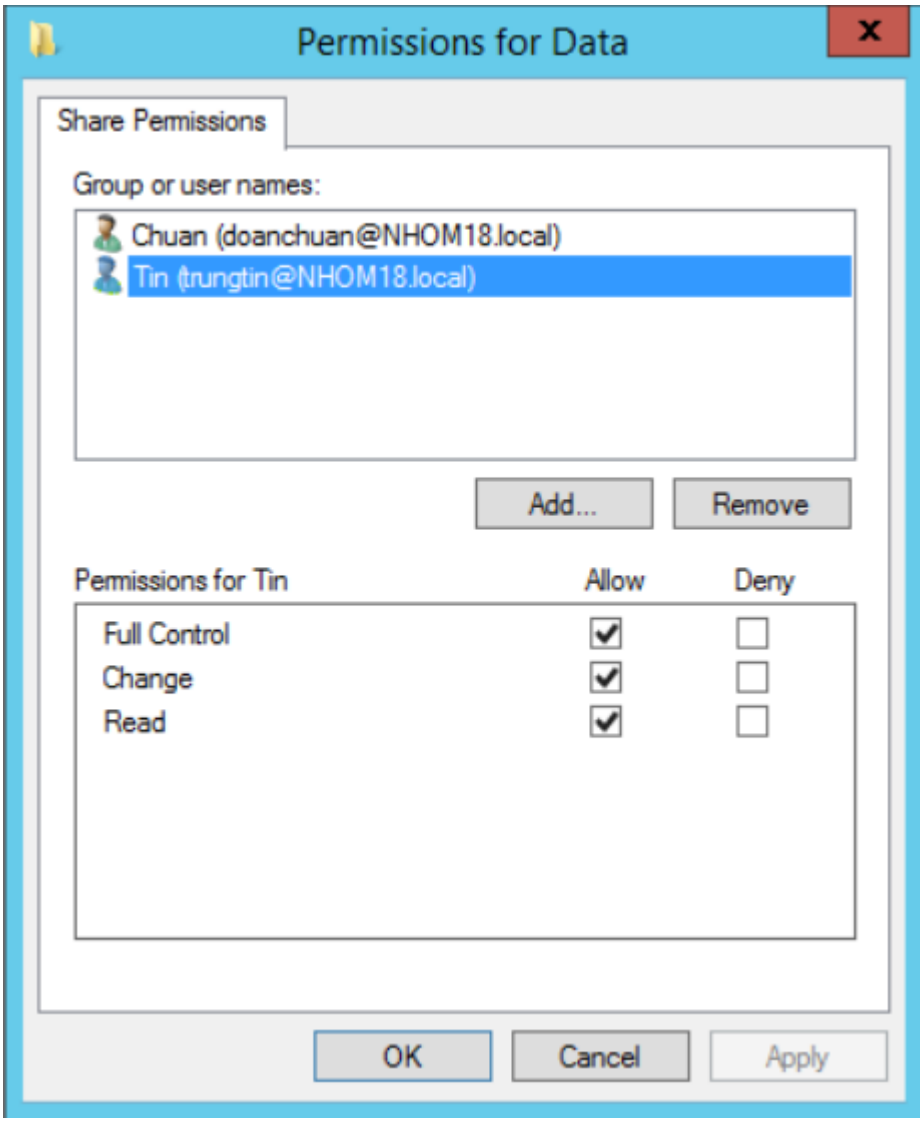
Hình 5: Thêm User để phân quyền, bấm OK

User **doanchuan** chỉ được phép đọc/xem và **không được** phép thay đổi thư mục **Data**



Hình 6. User doanchuan được phép đọc thư mục TaiLieu

User **trungtin** được phép đọc và thay đổi thư mục **Data**

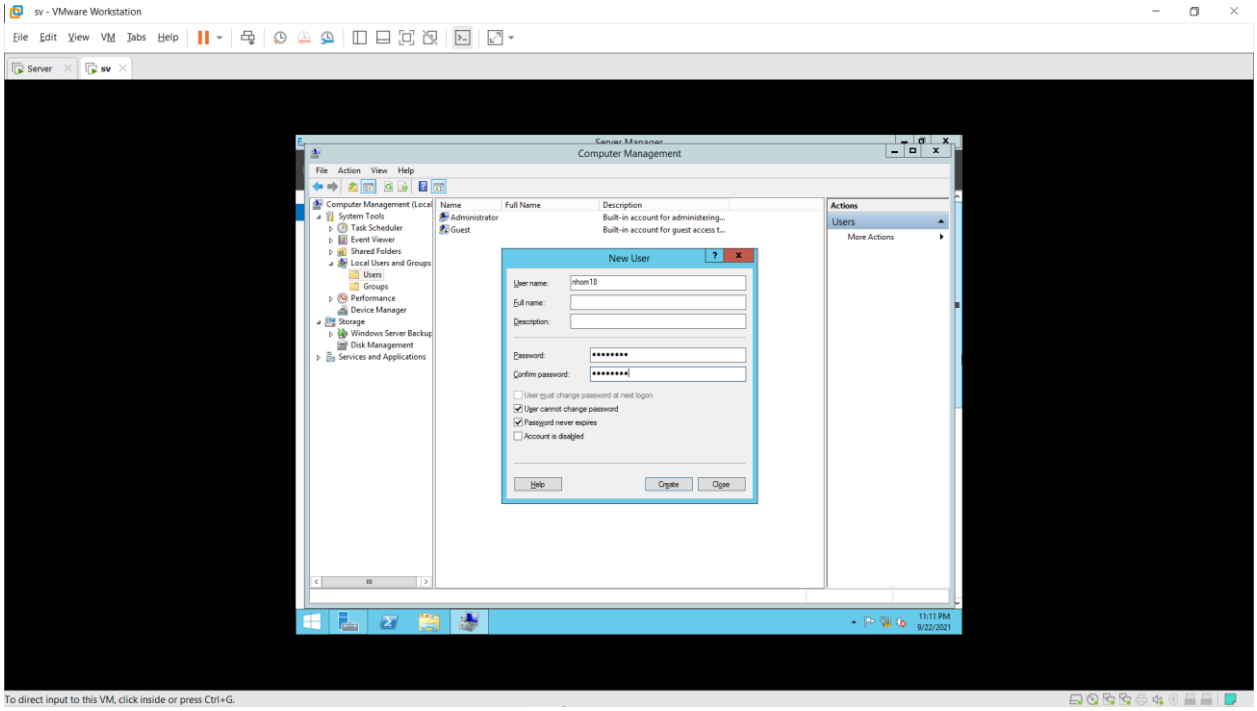


Hình 7. User trungtin được phép đọc và thay đổi thư mục TaiLieu

3.1.2 Cấu hình trên máy Server VPN

Bước 1: Tạo 1 tài khoản dùng để thiết lập dịch vụ **VPN.**

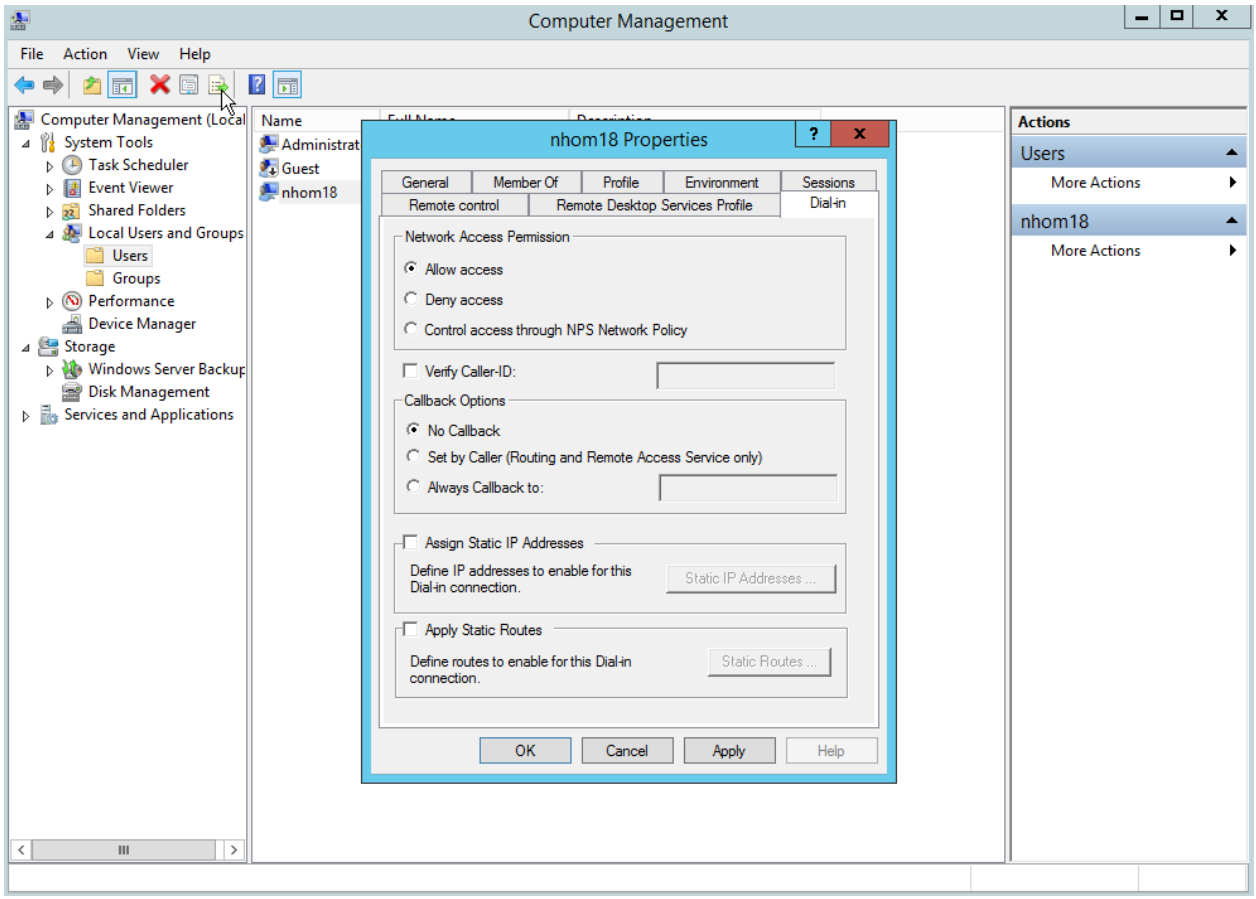
Vào **Server Manager / Tools / Computer Management** , chọn vào **Local Users and Groups /Users**, click chuột phải chọn **New User…** User name: **nhom18**



Hình 8. Tạo tài khoản dịch vụ VPN

Bước 2: Cho phép **User** được quyền truy cập từ xa

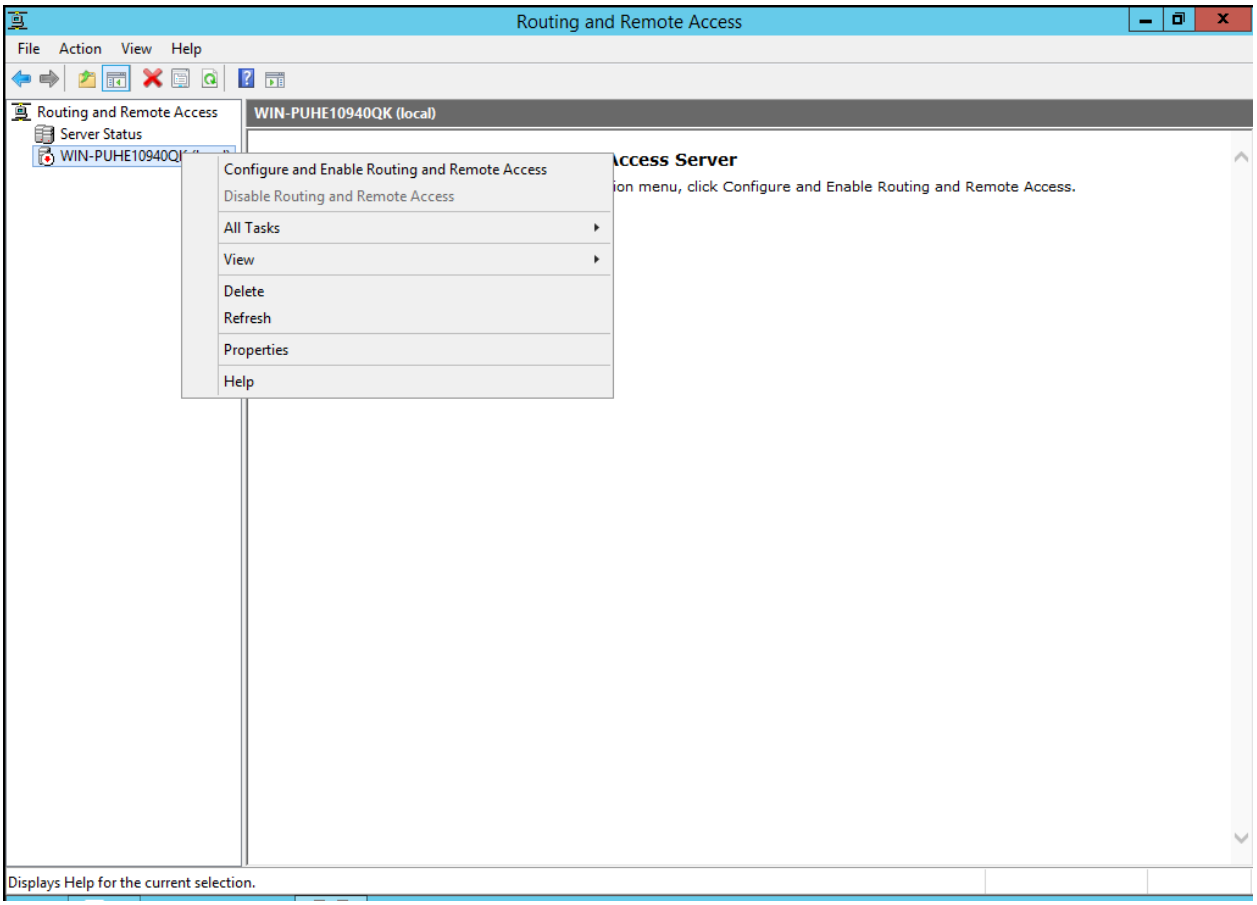
-Click chuột phải tại **user** vừa tạo, chọn **Properties.** Chuyển sang tab **Dial-in,** tại **Network Access Permission,** chọn vào **Allow access, Apply OK.**



Hình 9. Bật mode cho phép user truy cập từ xa

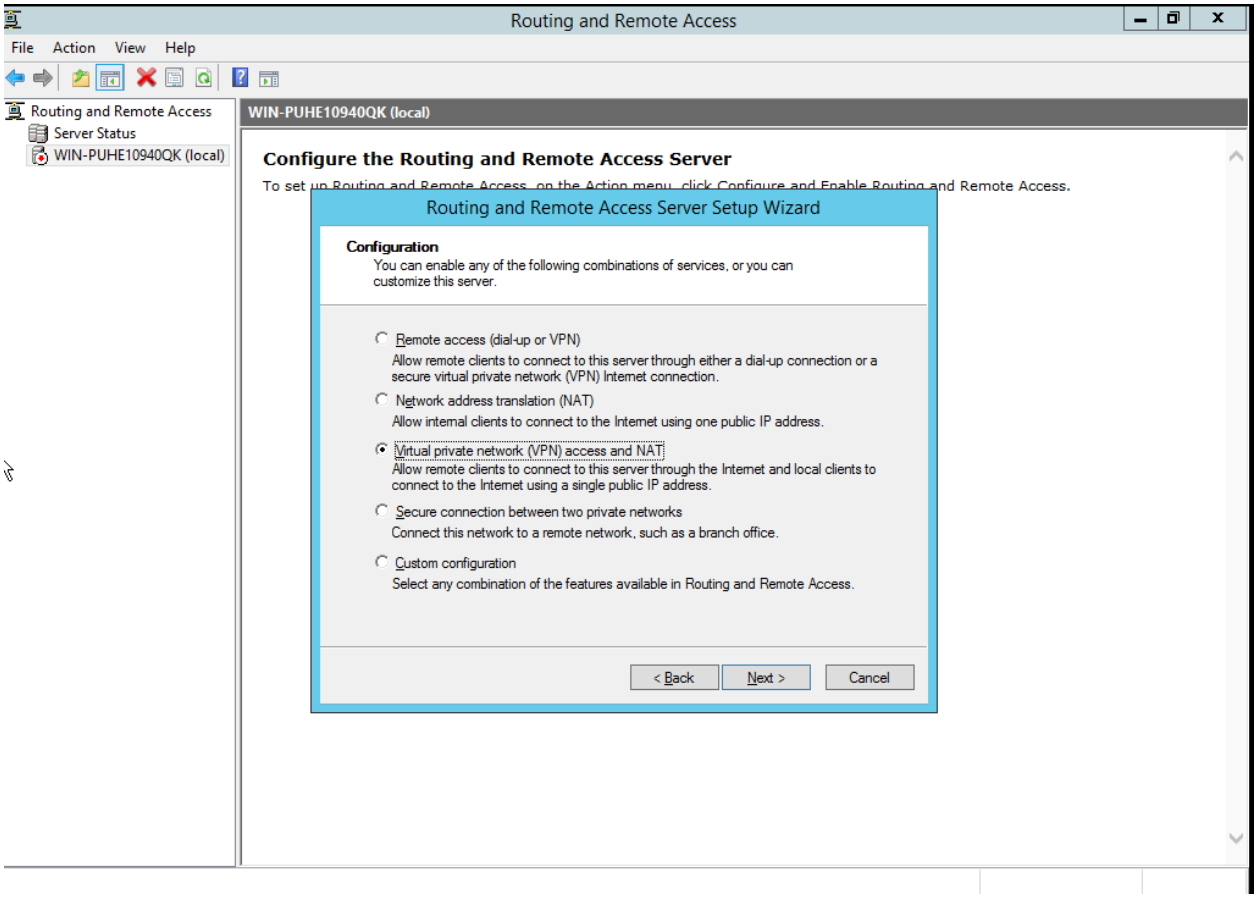
Bước 3: Tiến hành cấu hình dịch vụ **VPN Server. Mở Tools / Routing and Remote Access**

-Tại cửa sổ **Routing and Remote Access**, click chuột phải tại **win-PUHE10940QK(local)**, chọn vào **Configure and Enable Routing and Remote Access.**



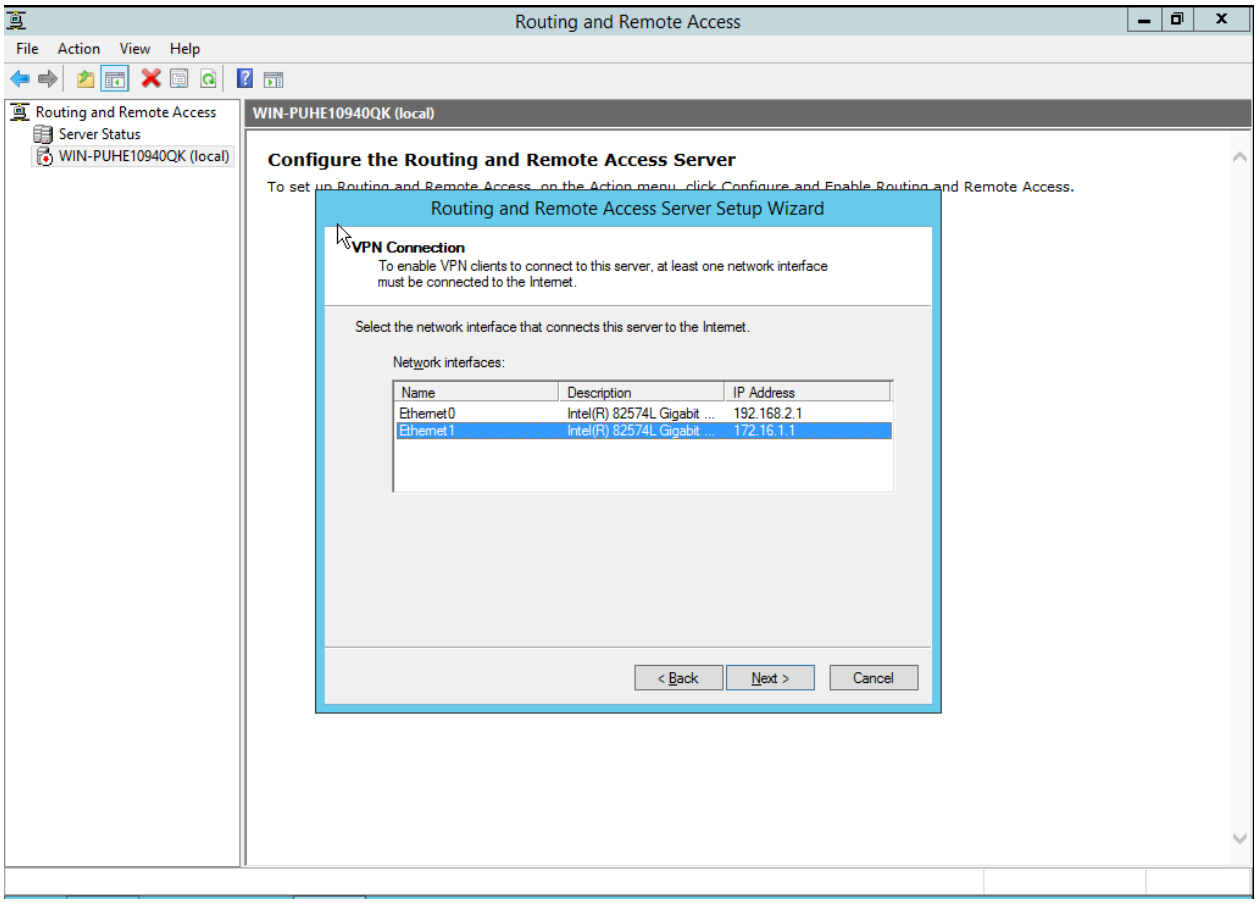
Hình 10. Cửa sổ Routing and Remote Access

-Ta sẽ chọn mục **Virtual Private Network (VPN) access and NAT**



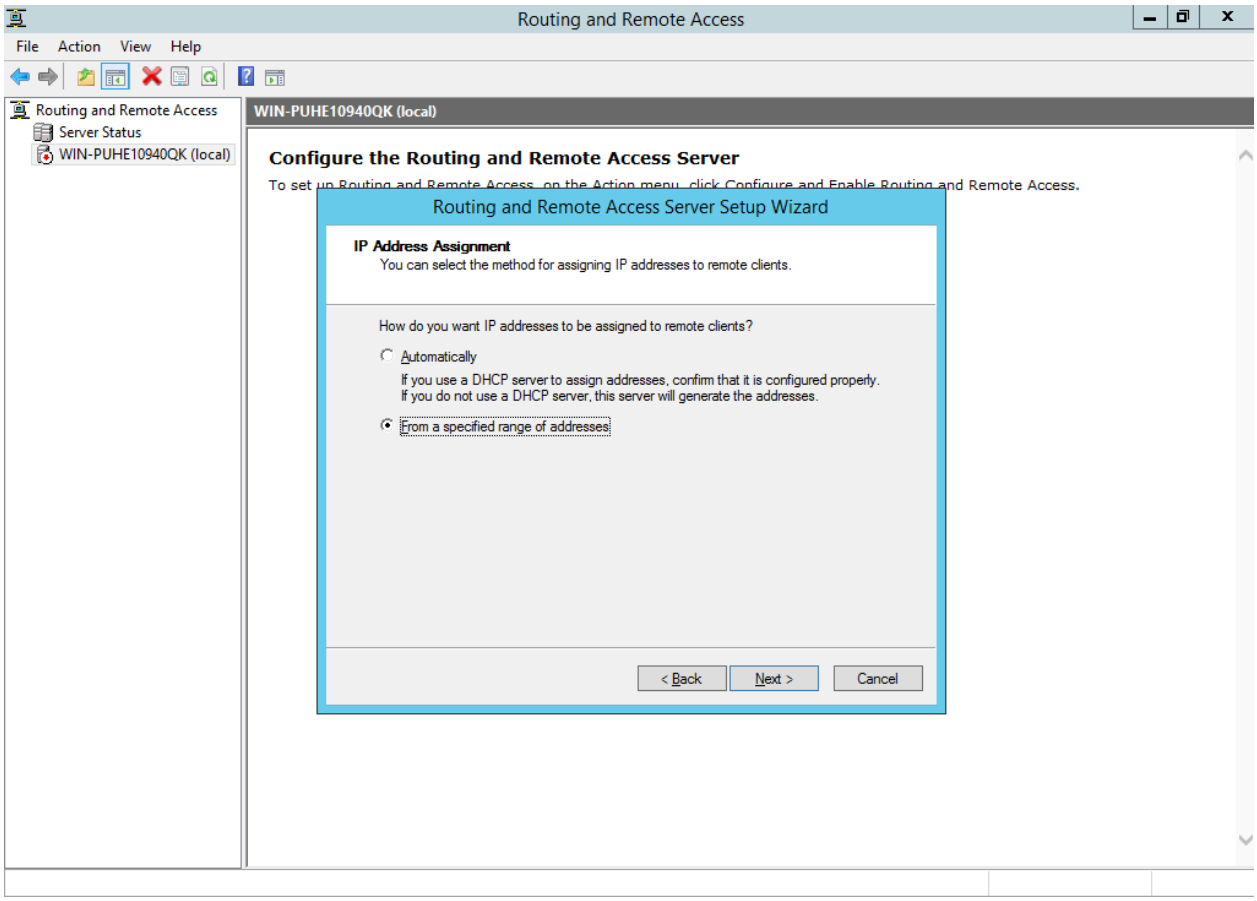
Hình 11. Chọn mục Virtual Private Network (VPN) access and NAT

-Ở mục **VPN Connection** ta sẽ chọn card 2 WAN để ra ngoài Internet, cho người dùng ngoài Internet remote access vào **VPN Server** nên ta chọn **Ethenet 1** (172.16.1.1)



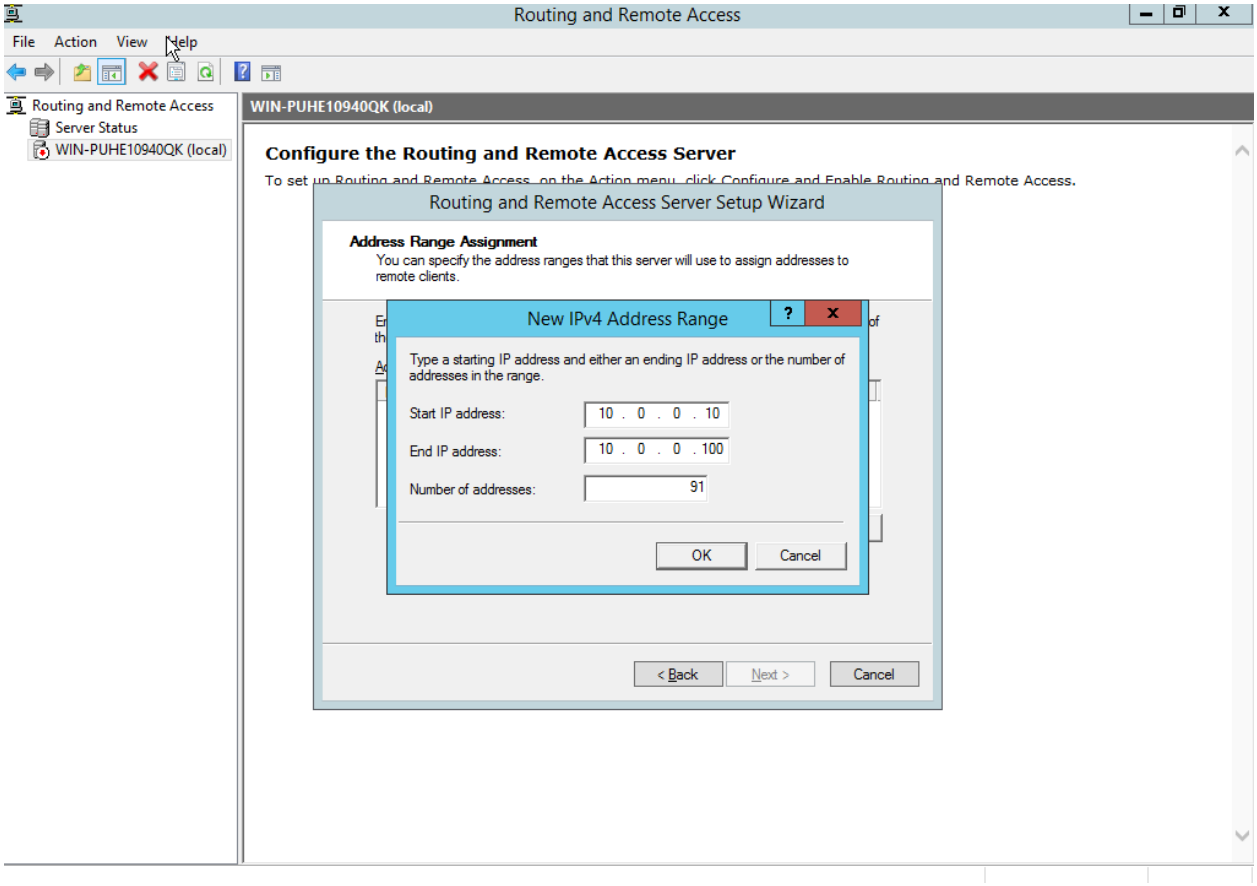
Hình 12. Chọn Ethenet 1(172.16.1.1)

-Tại cửa sổ **IP Address Assignment**, chọn vào **From a specified range of address**… **Next.**



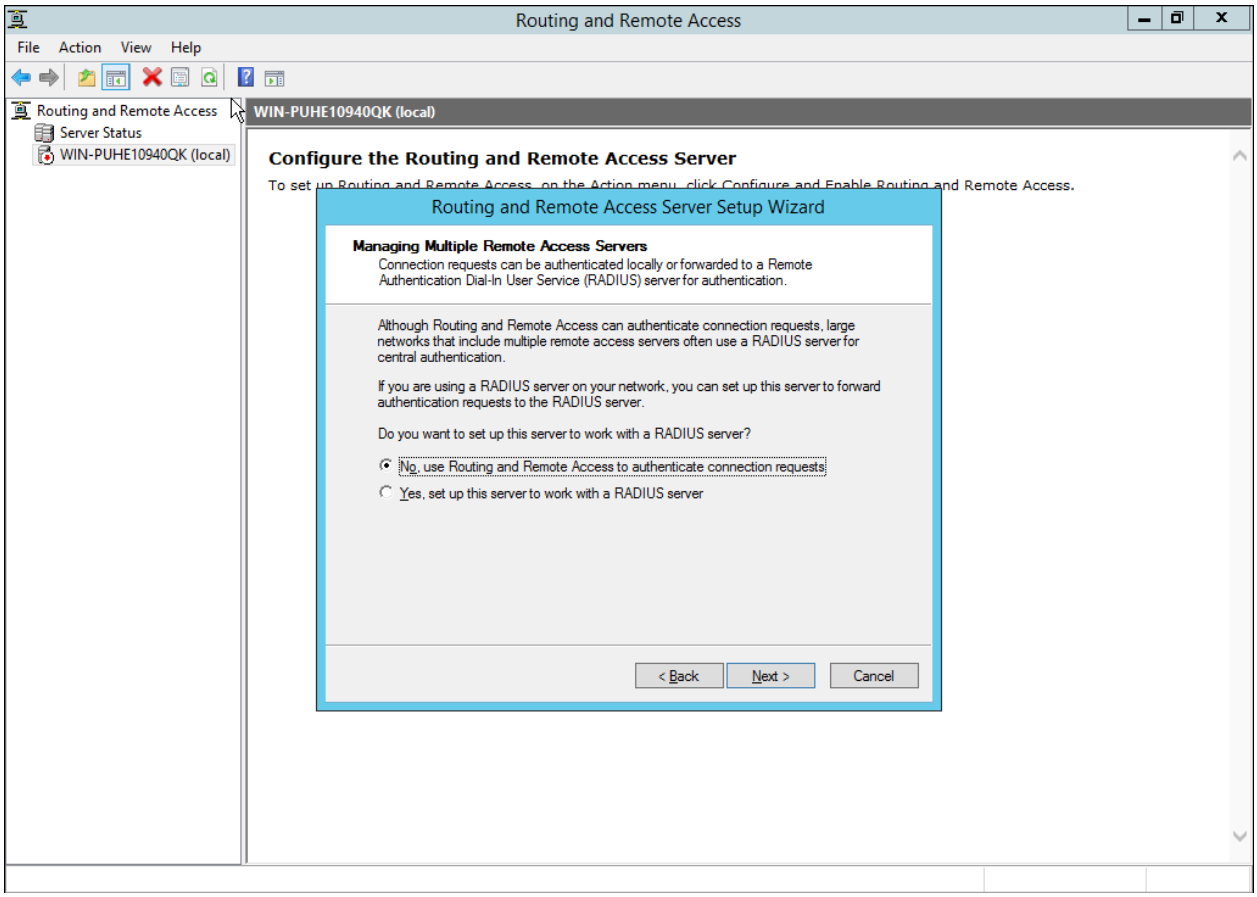
Hình 13. Chọn mục From a specified range of address

-Tại cửa sổ **Address Range Assignment**, click vào **New…**, Tại cửa sổ **New IPv4 Address Range**, nhập vào dải địa chỉ IP *10.0.0.10 – 10.0.0.100* → Next. Đây là dải IP Private mà Client được phép VPN khi nằm trong dải IP này.



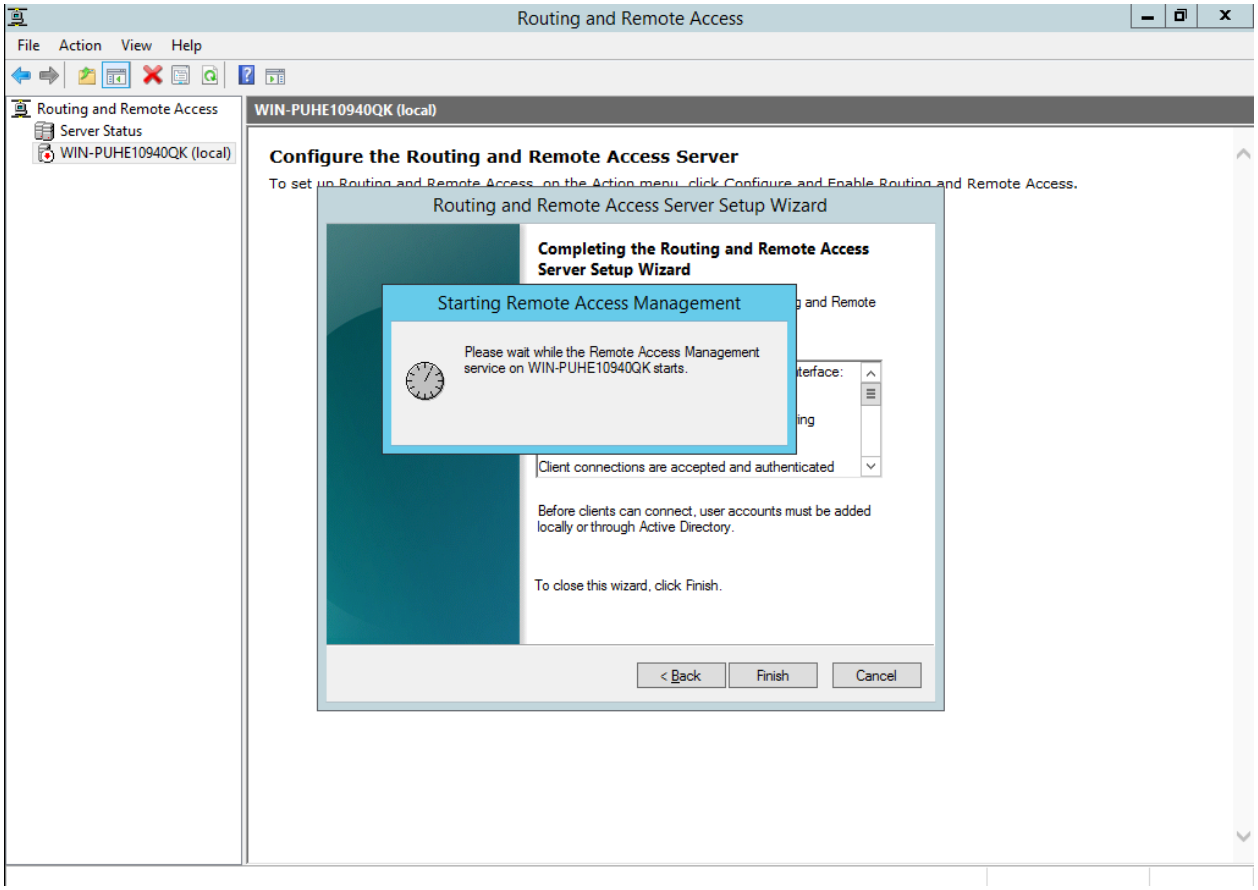
Hình 14. Thiết lập dải miền mà client sẽ nhận được

-Tại cửa sổ **Managing Multiple Remote Access Servers**, click chọn vào **No, use Routing and Remote Access to authenticate connection requests**.



Hình 15. Chọn No, use Routing and Remote Access to authenticate connection requests.

-Click **Finish / OK** để kết thúc quá trình cấu hình dịch vụ **VPN Server.**

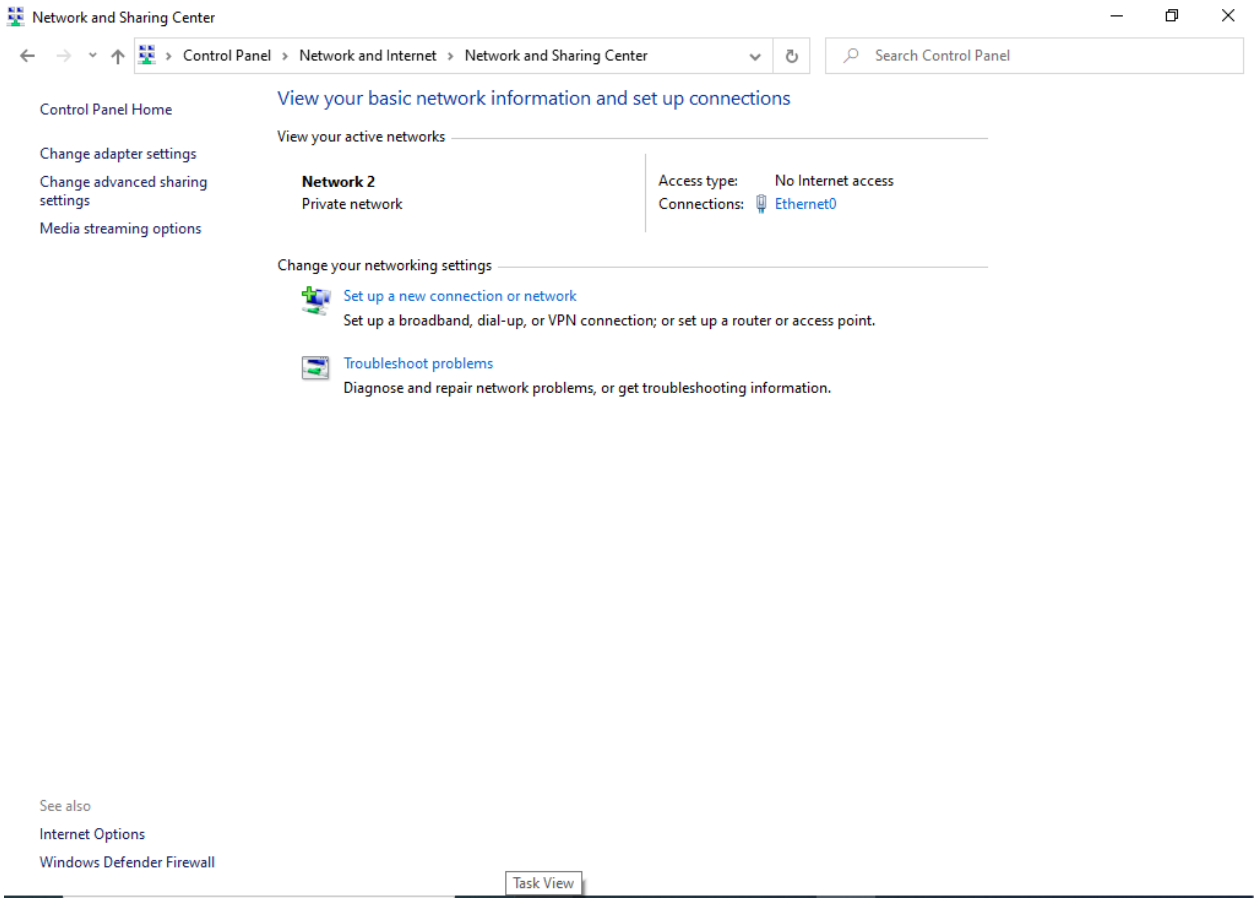


Hình 16. Hoàn tất mục cài đặt

3.1.3 Cấu hình trên máy Window 10 Client

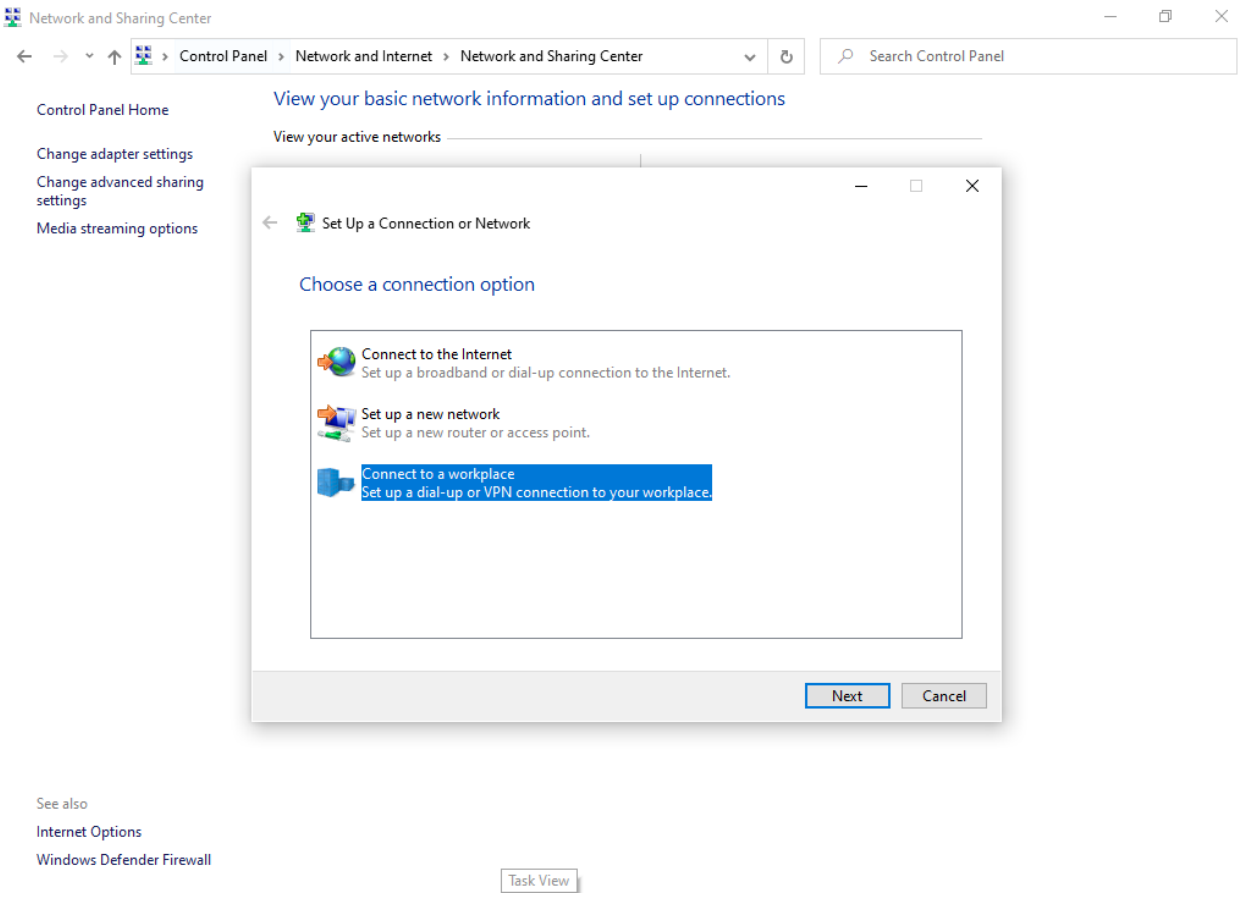
Bước 1: Tiến hành thiết lập kết nối VPN cho máy.

-Tại cửa sổ **Network and Sharing Center**, click chọn vào **Set up a new connection or network.**



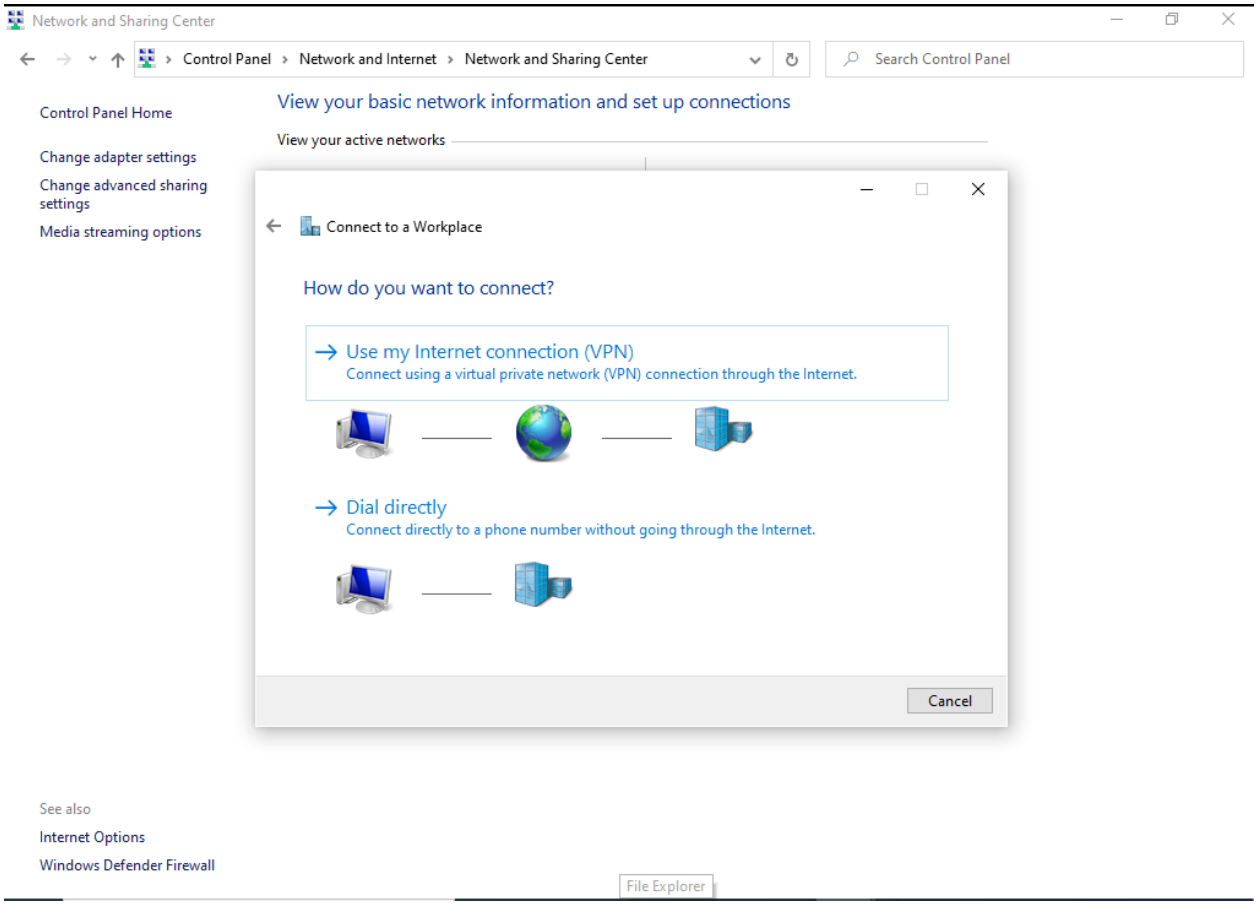
Hình 17. Tại Network and Sharing Center

-Tại cửa sổ **Set Up a Connection or Network**, click chọn vào **Connect to a workplace**… Next.



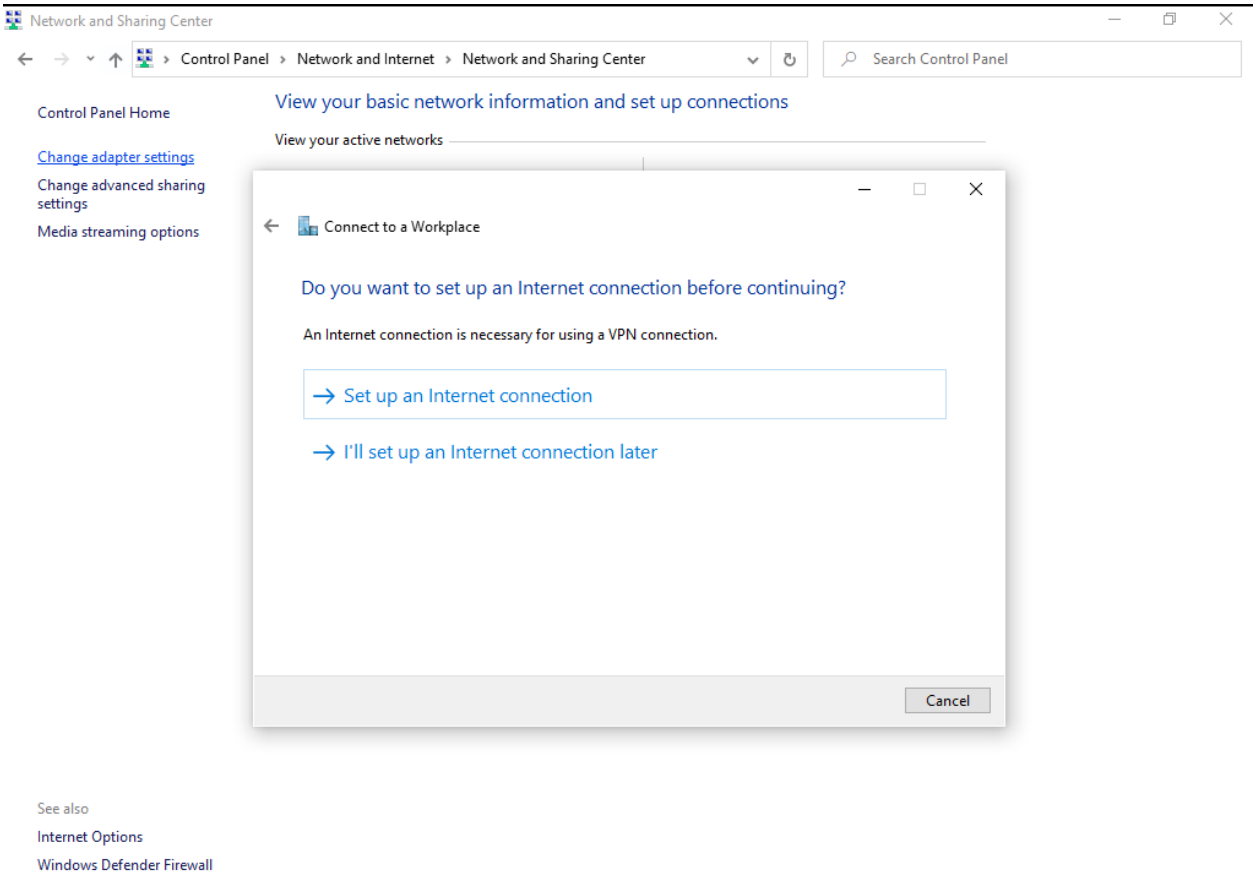
Hình 18. Chọn Connect to a workplace

-Tại cửa sổ **Connect to a Workplace**, click chọn vào **Use my Internet connection (VPN).**



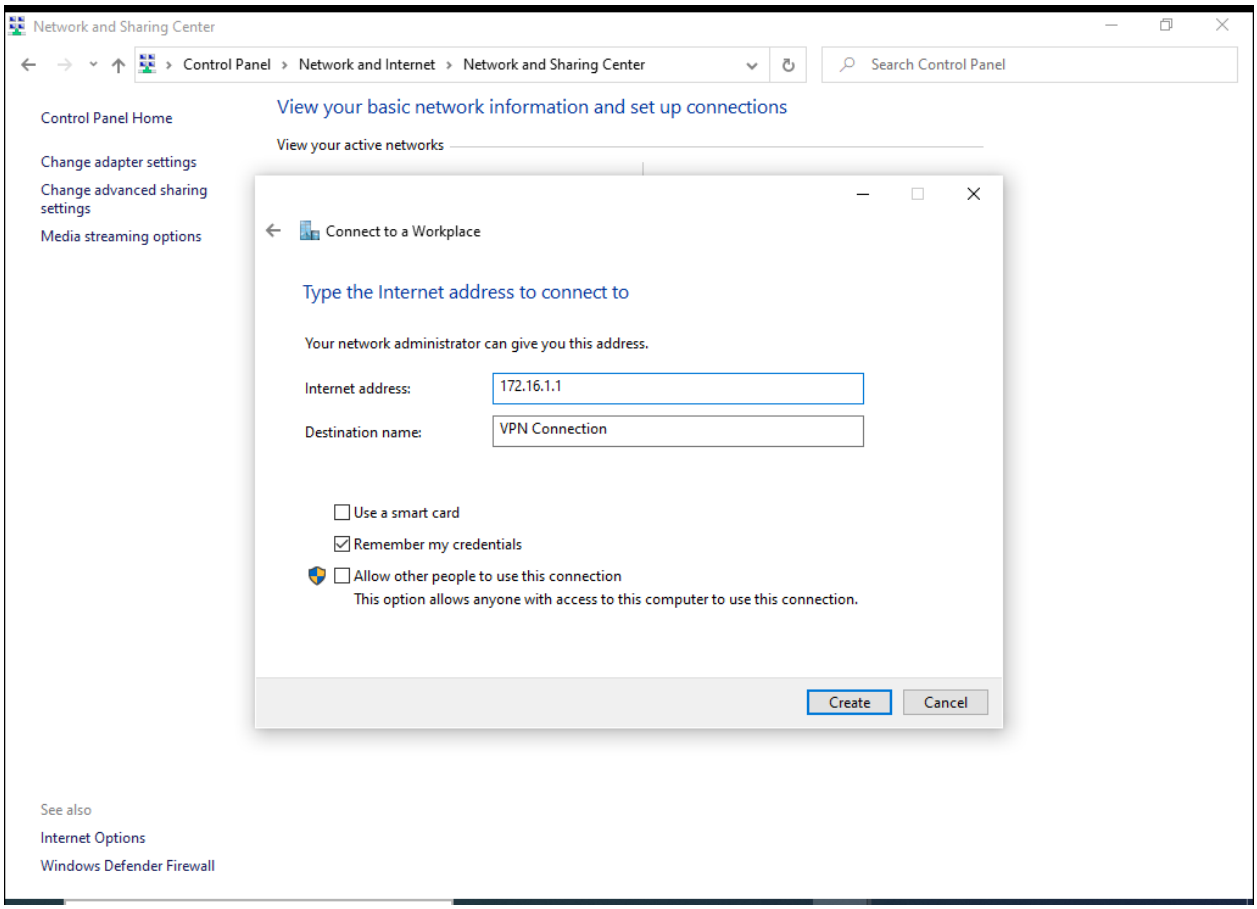
Hình 19. Chọn Use my Internet connection (VPN).

Chọn **vào I’ll set up an Internet connection later**.



Hình 20. Chọn vào I’ll set up an Internet connection later.

Nhập vào địa chỉ *Gateway* của mạng bên ngoài *Internet address 172.16.1.1*
Click vào **Create** và chờ nó tạo kết nối VPN .

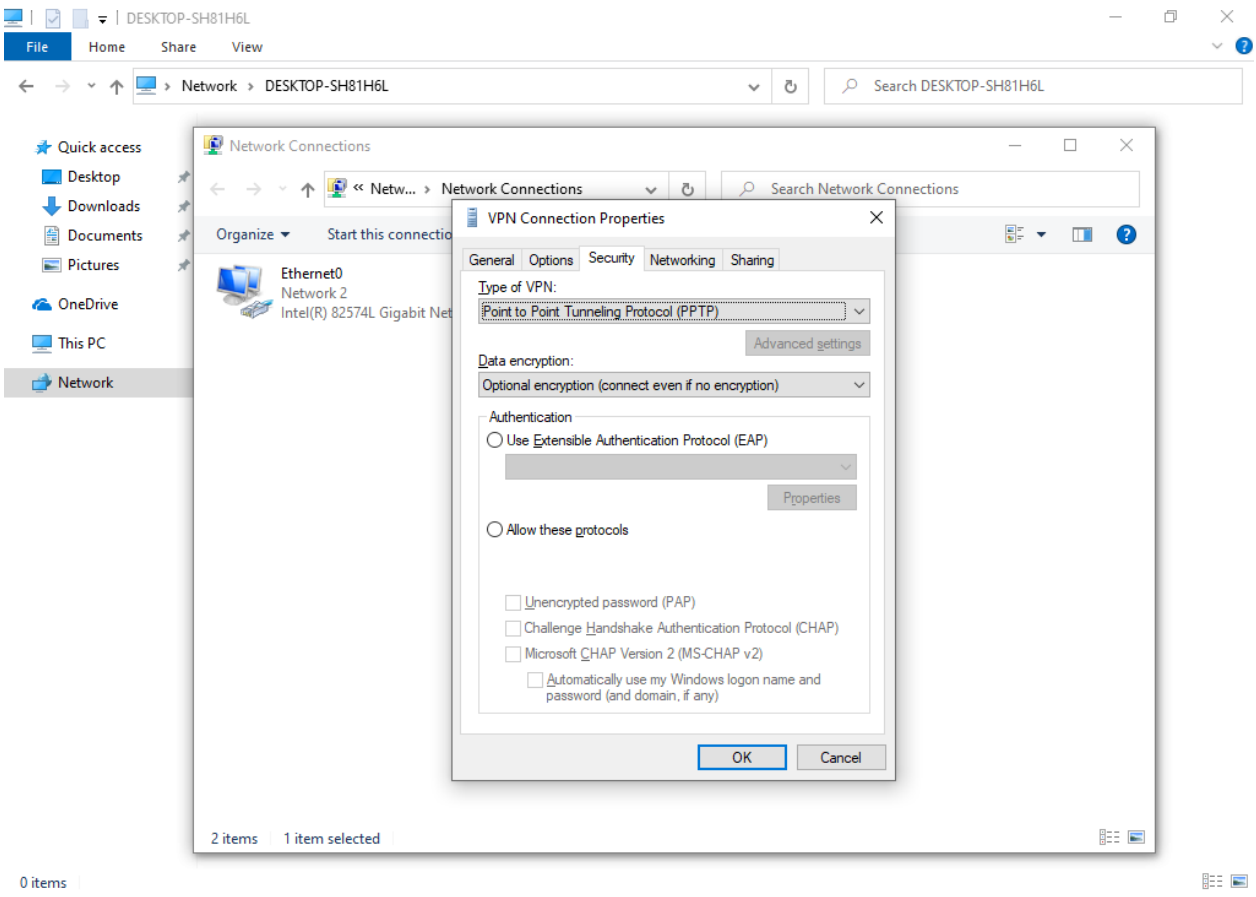


Hình 21. Nhập vào địa chỉ Gateway của mạng bên ngoài Internet address 172.16.1.1

Bước 2: Chọn giao thức cho VPN vừa tạo

-Click chuột phải tại Card mạng **VPN Connection** vừa tạo, chọn **Properties.**

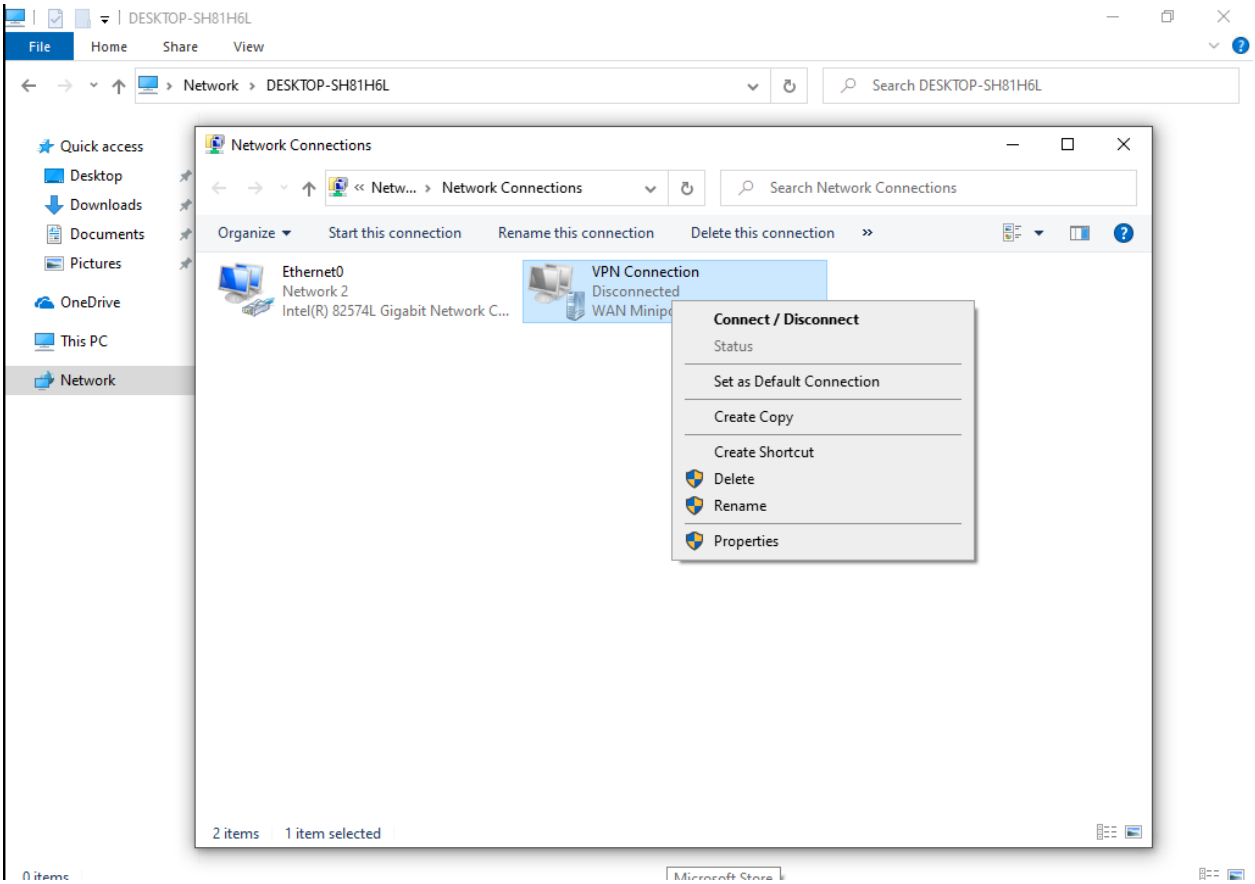
-Tại cửa sổ **VPN Connection Properties**, chuyển sang tab **Security**, tại mục **Type of VPN**, chọn kiểu giao thức kết nối **VPN** là **Point to Point Tunneling Protocol (PPTP)**…OK.



Hình 22. Chọn giao thức Point to Point Tunneling Protocol (PPTP) cho VPN

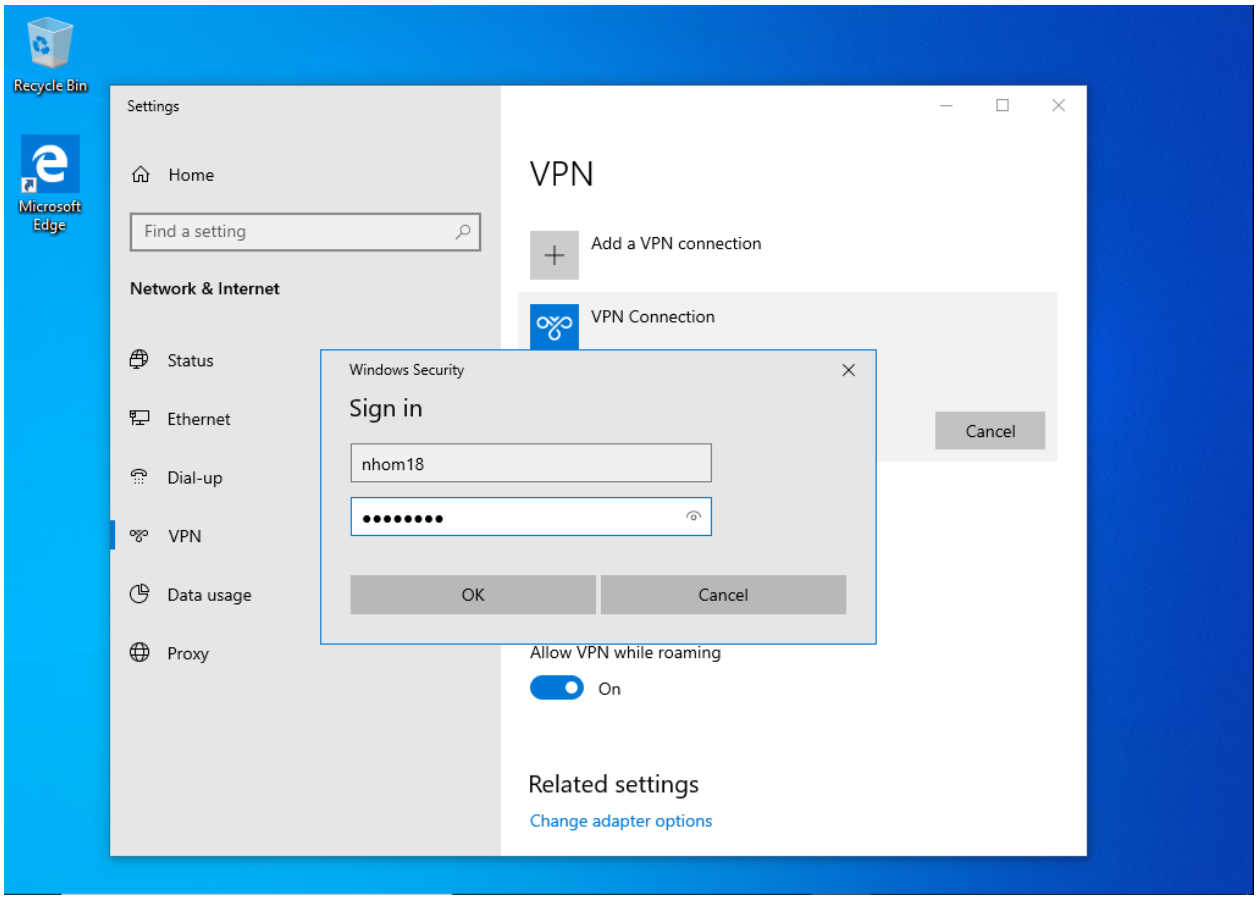
Bước 3: Tiến hành kết nối VPN

-Click chuột phải tại **Card mạng VPN Connection**, chọn **Connect / Disconnect.**



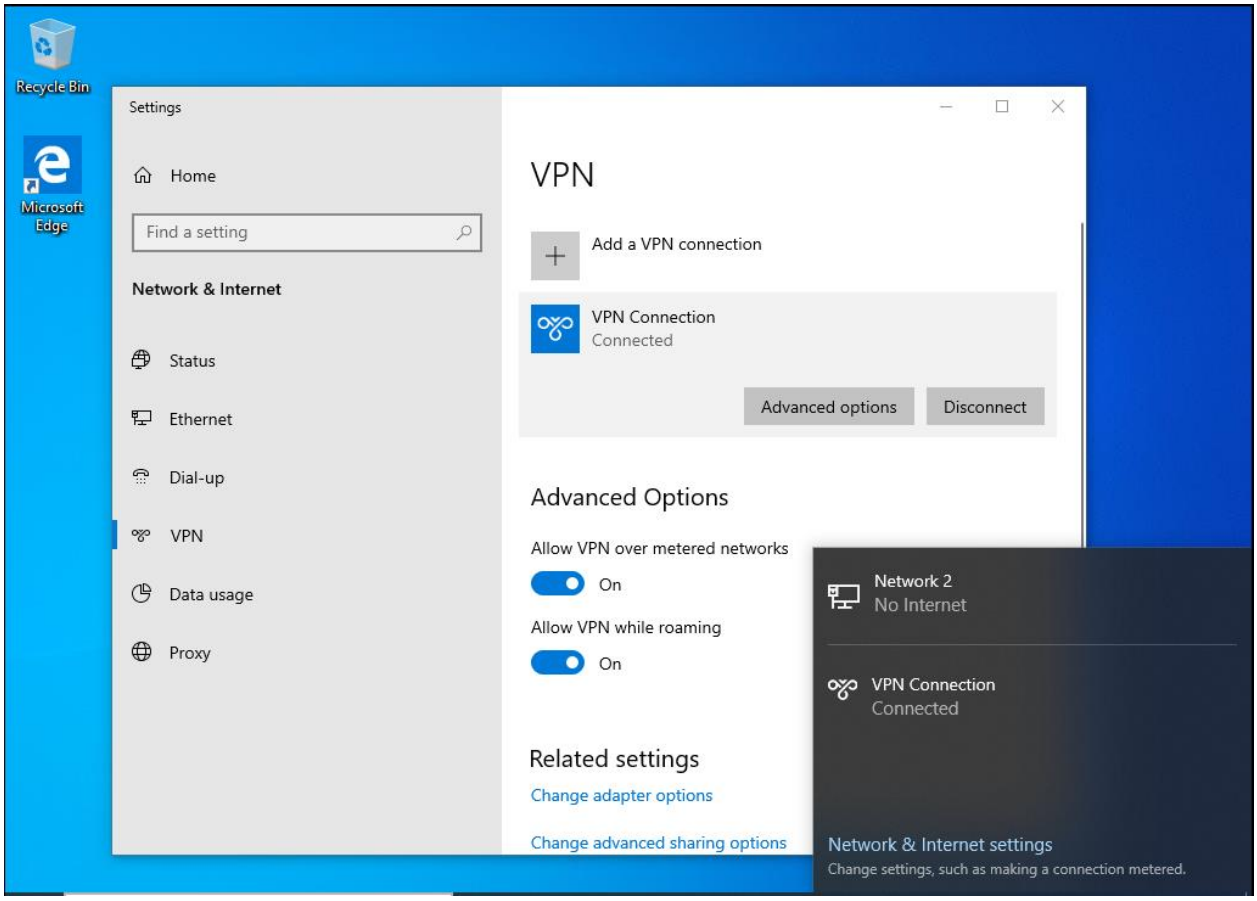
Hình 23. Tiến hành kết nối tới VPN ta vừa thiết lập

Bước 4: Nhập vào tài khoản VPN **nhom18** mà ta đã tạo và cấp quyền truy cập từ xa lúc nãy.



Hình 24. Đăng nhập tài khoản vào VPN

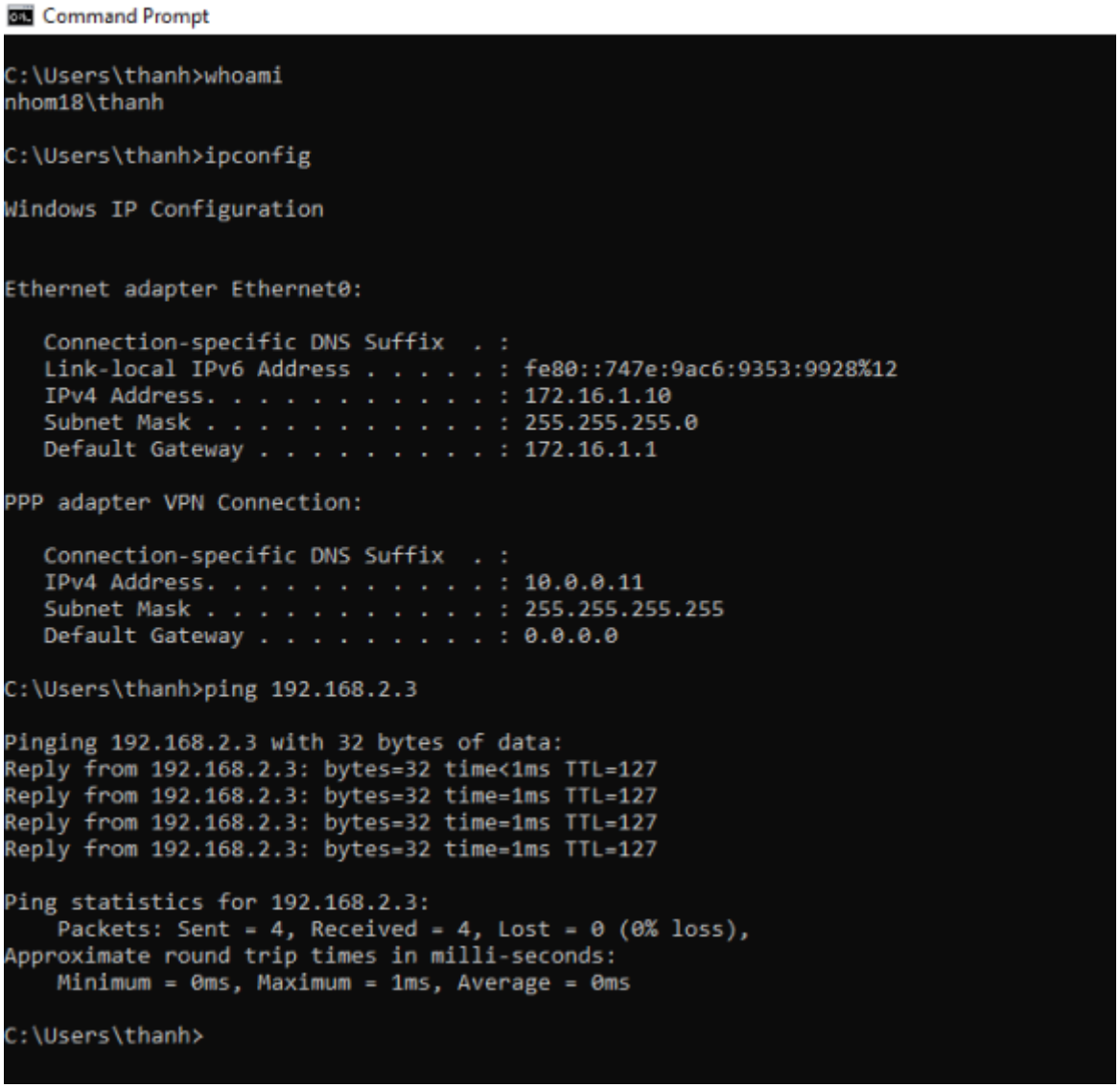
-Kết nối **VPN** thành công.



Hình 25. đăng nhập thành công VPN

3.1.4 Kiểm tra kết quả

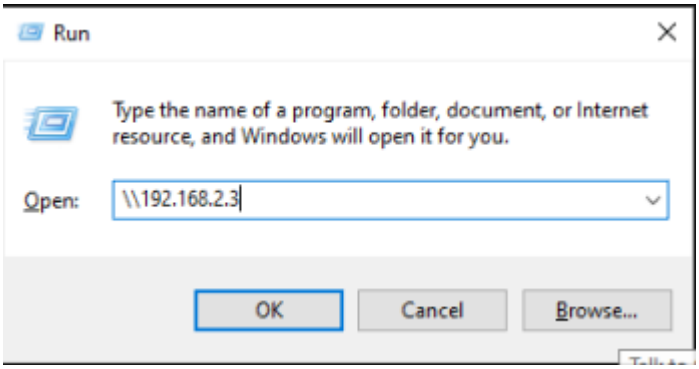
Bước 1: Đăng nhập vào User **bất kì** để kiểm tra Kết Quả



Hình 26. Kết nối VPN thành công và ping thành công đến máy Server

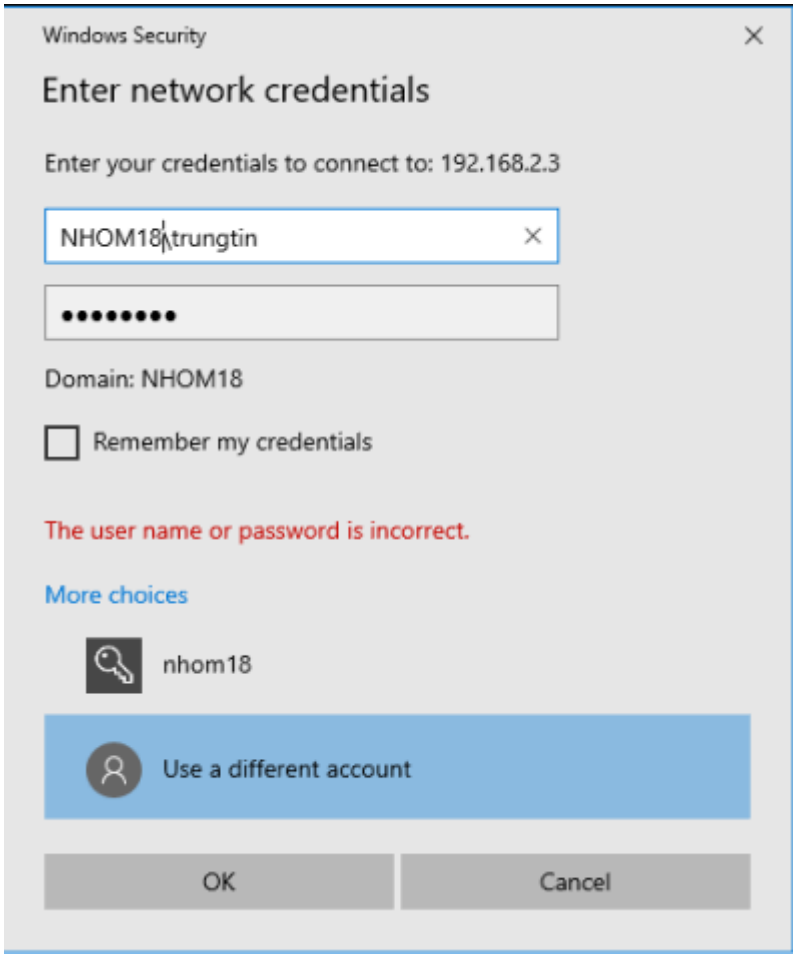
Bước 2: Kiểm tra quyền

Chọn Run và nhập: \\192.168.2.3

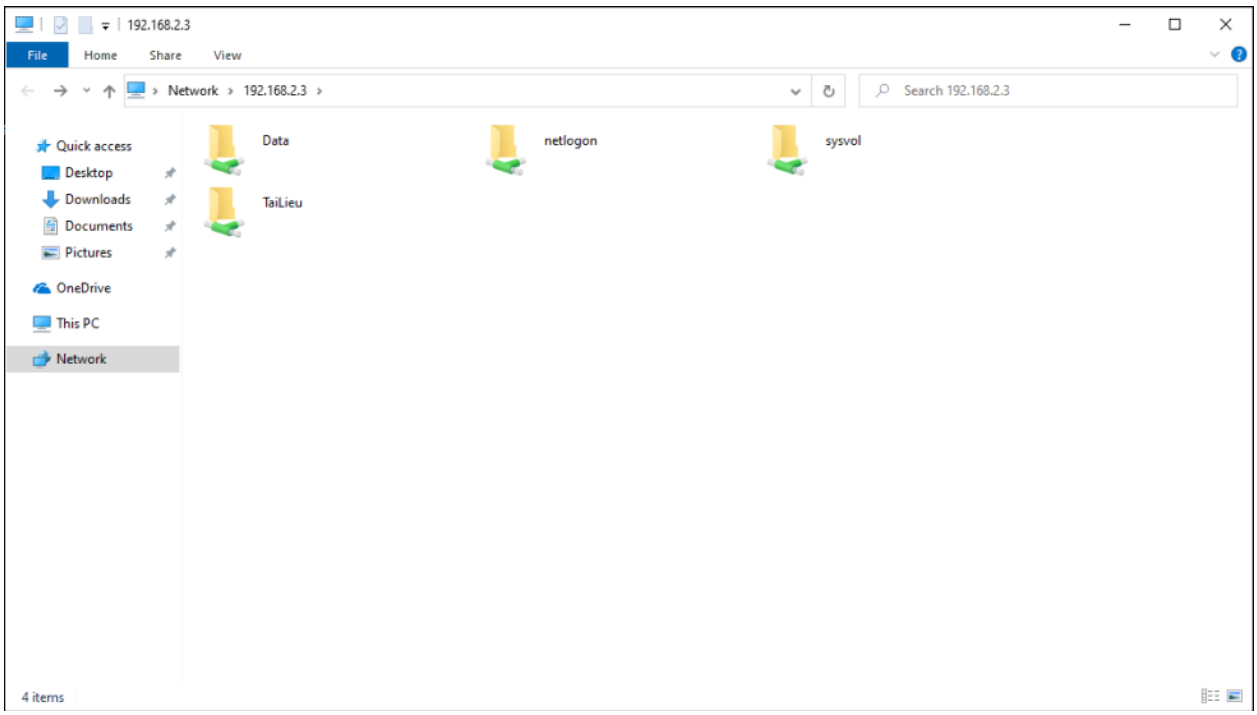


Hình 27. Windows+R: \\192.168.2.3 để kết nối vào Server

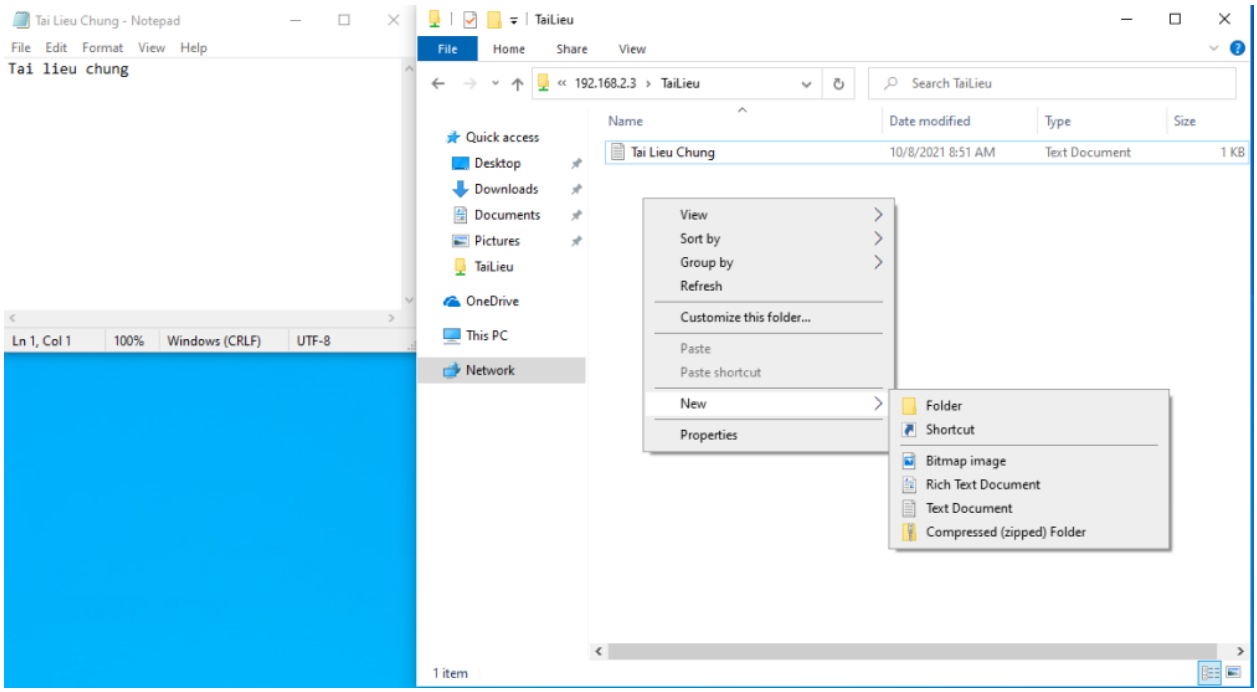
-Đối với User trungtin



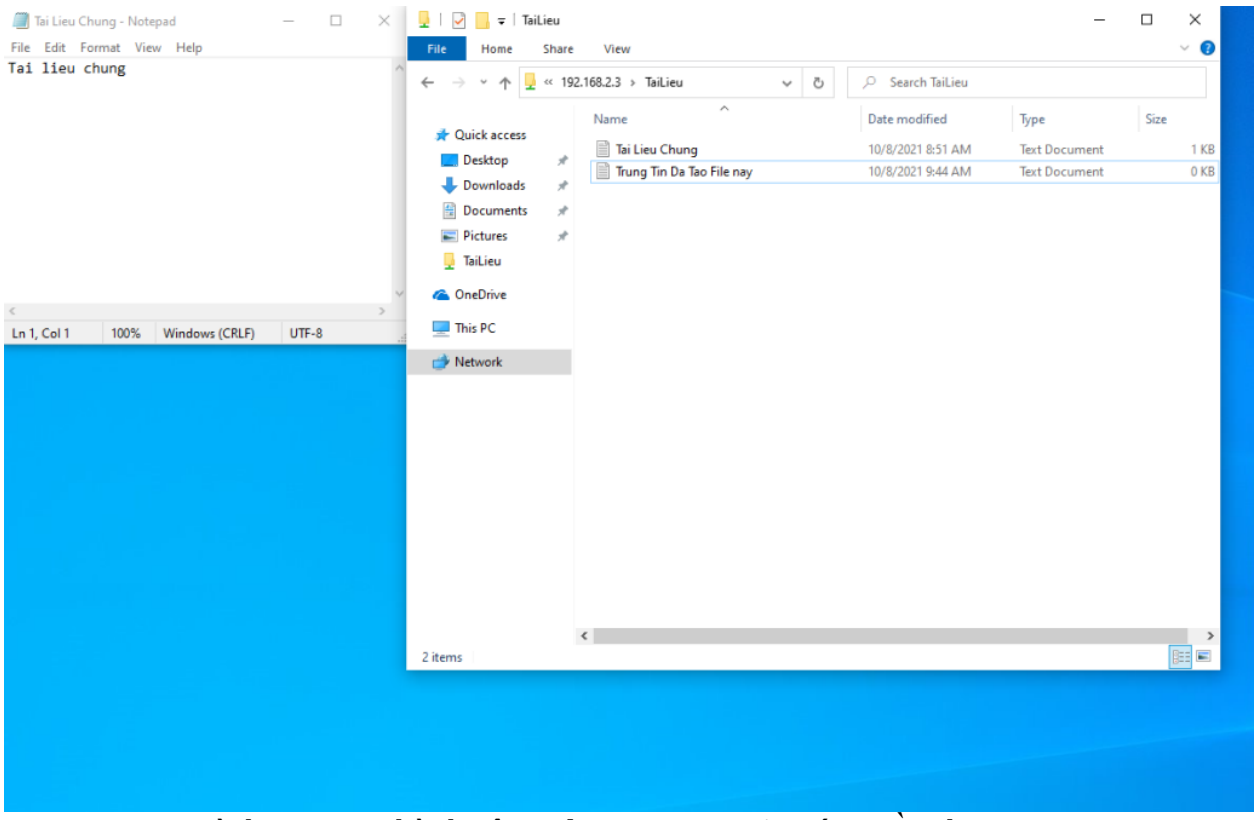
Hình 28. Đăng nhập vào User trungtin đã tạo ở trên để truy cập từ xa



Hình 29. Kết nối thành công tới máy chủ bằng User trungtin



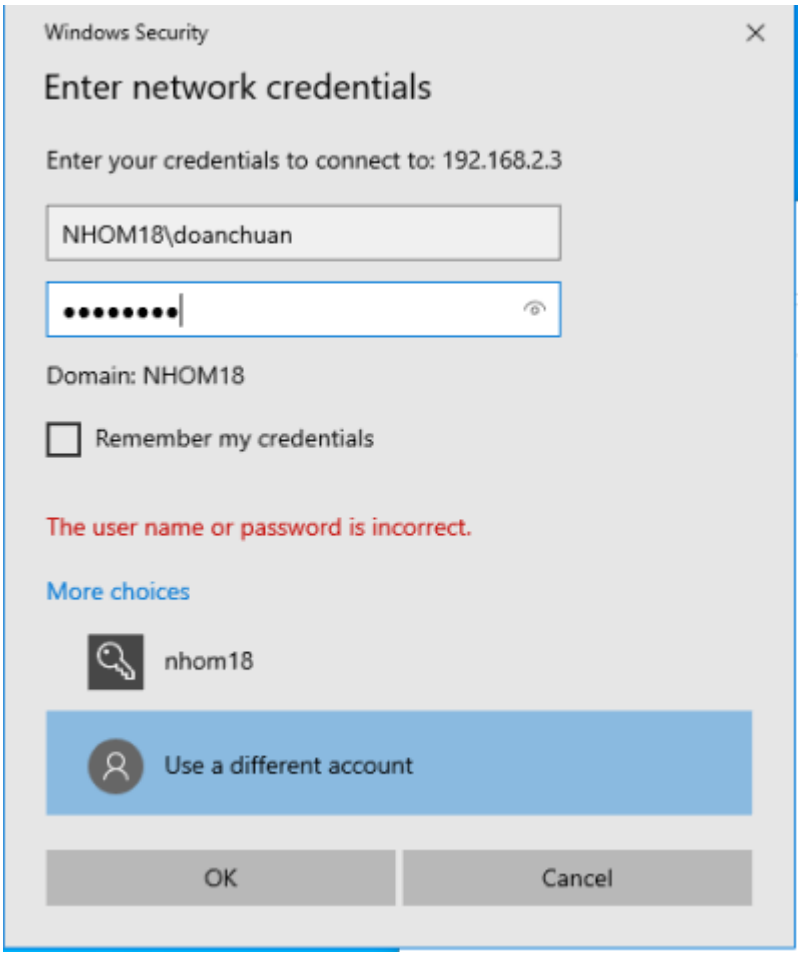
Hình 30. Truy cập thành công file tailieu và thử tạo 1 file khác



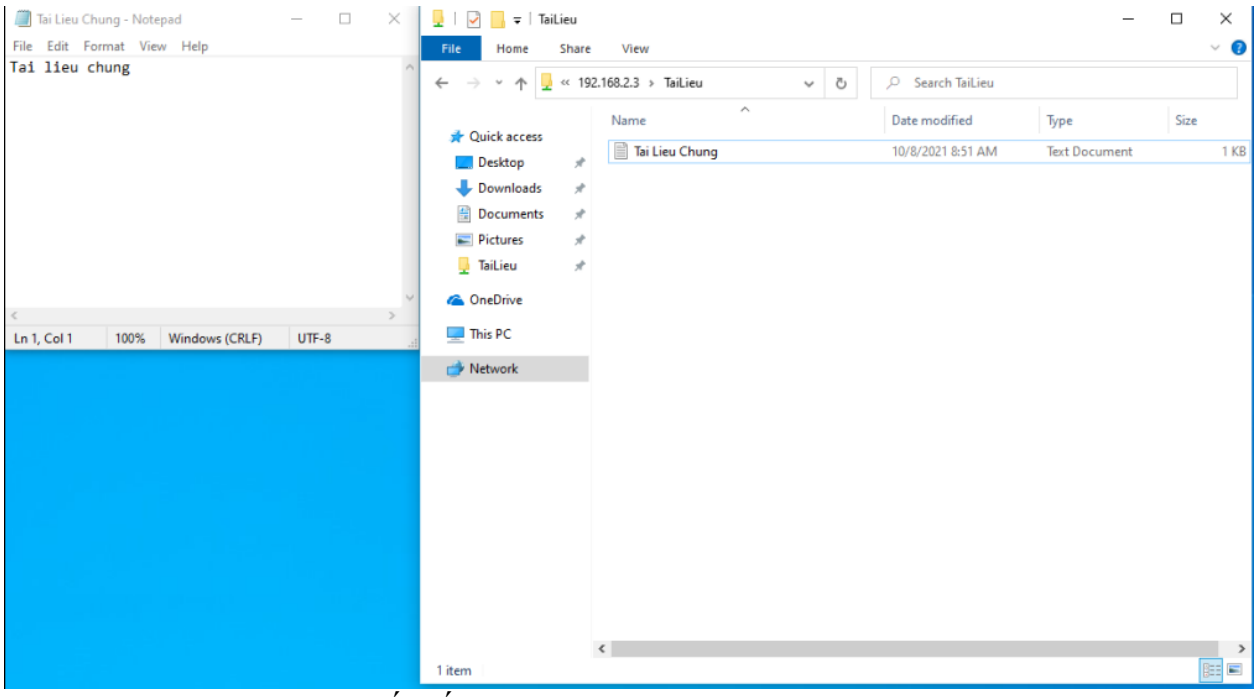
Hình 31. Tạo thành công, do User trungtin có quyền change

-Đối với User doanchuan

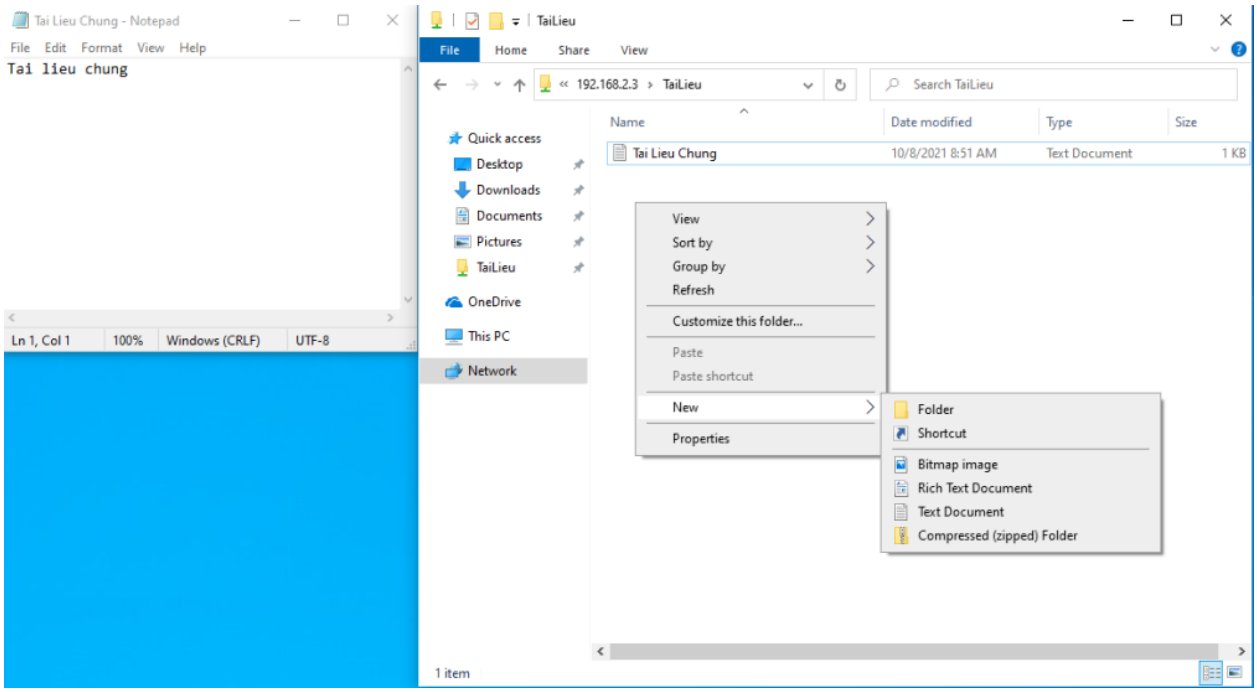
Chọn Run và nhập: \\192.168.2.3



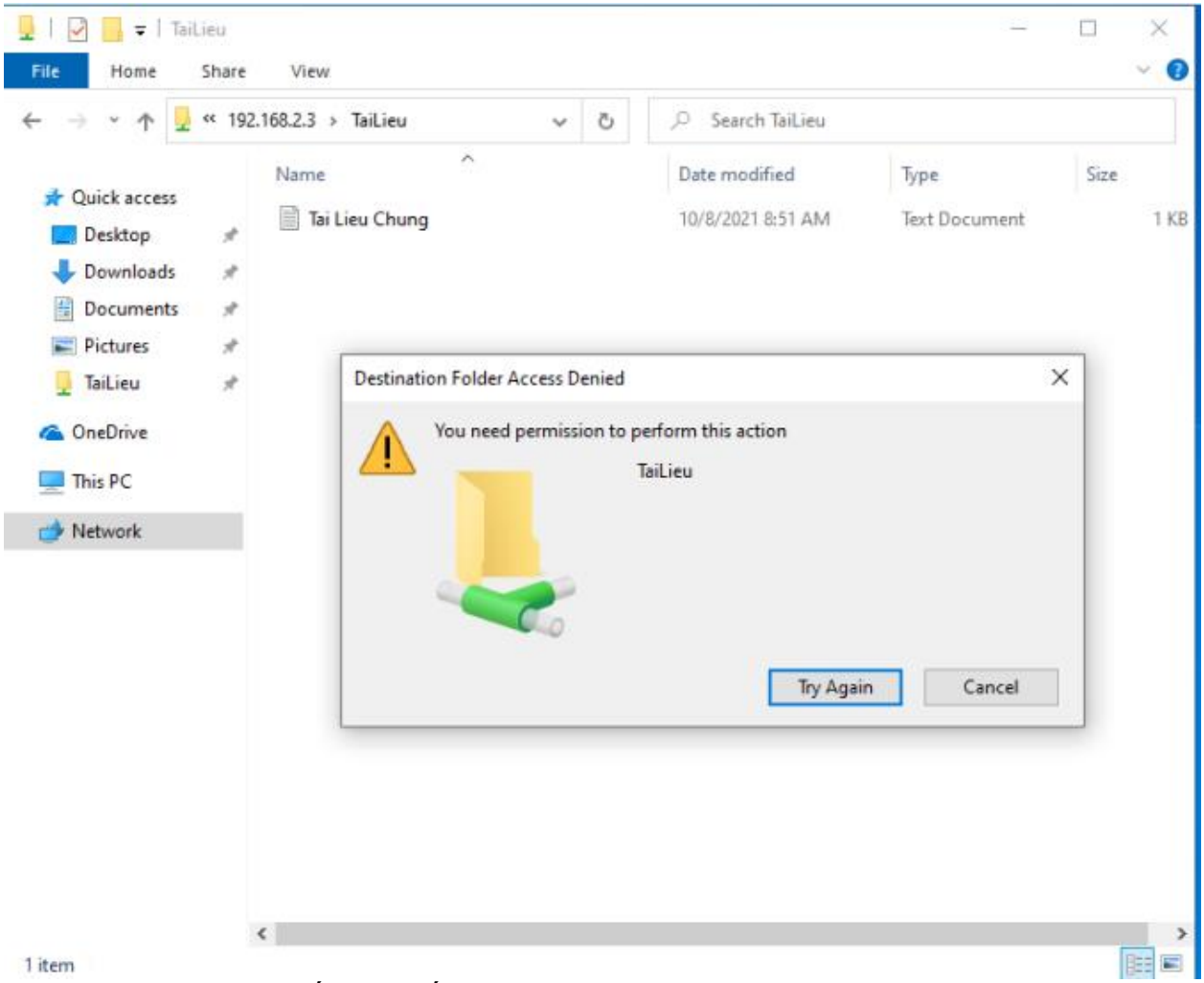
Hình 32. Đăng nhập vào User doanchuan



Hình 33. Kết nối thành công và xem được tailieuchung



Hình 34. Tạo File mới trong thư mục

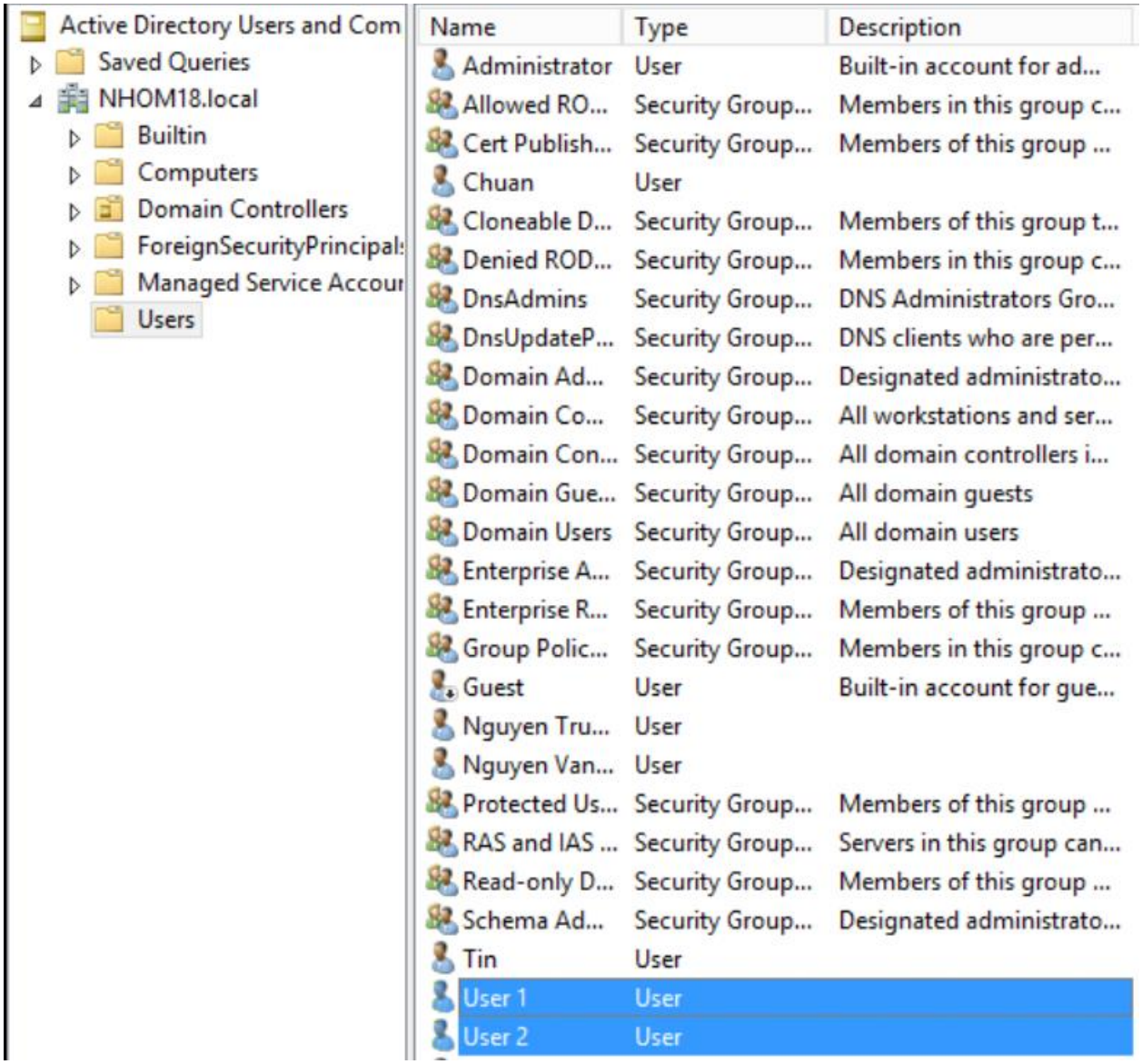


Hình 35. Kết quả thất bại vì user doanchuan chỉ được phép xem

3.2 Lab nâng cao

3.2.1 Cấu hình trên máy Server Domain(192.168.2.3)

-Tạo 2 User: user1 và user2 để cấp quyền Remote Desktop

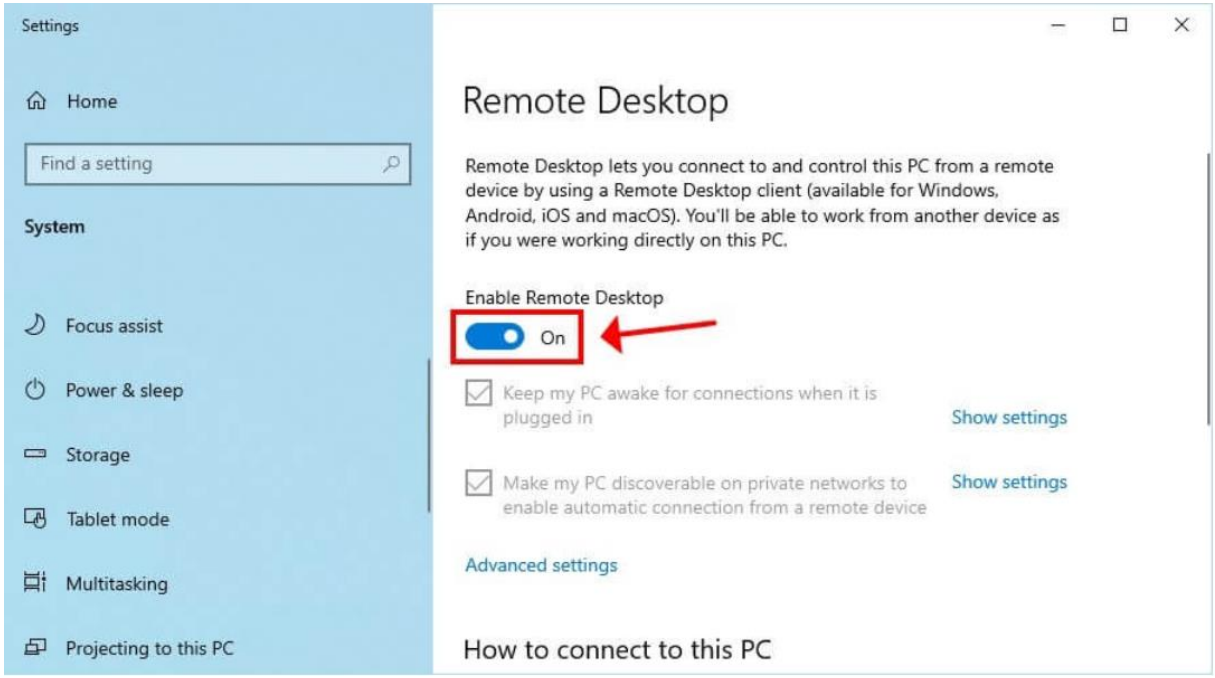


Hình 36. Tạo thành công tài khoản 2 User

3.2.2 Cấu hình trên máy Window 10(192.168.2.10/24)

Bước 1: Vào User **Administrator** để bật chế độ **Remote desktop**

Window+R: Remote desktop setting

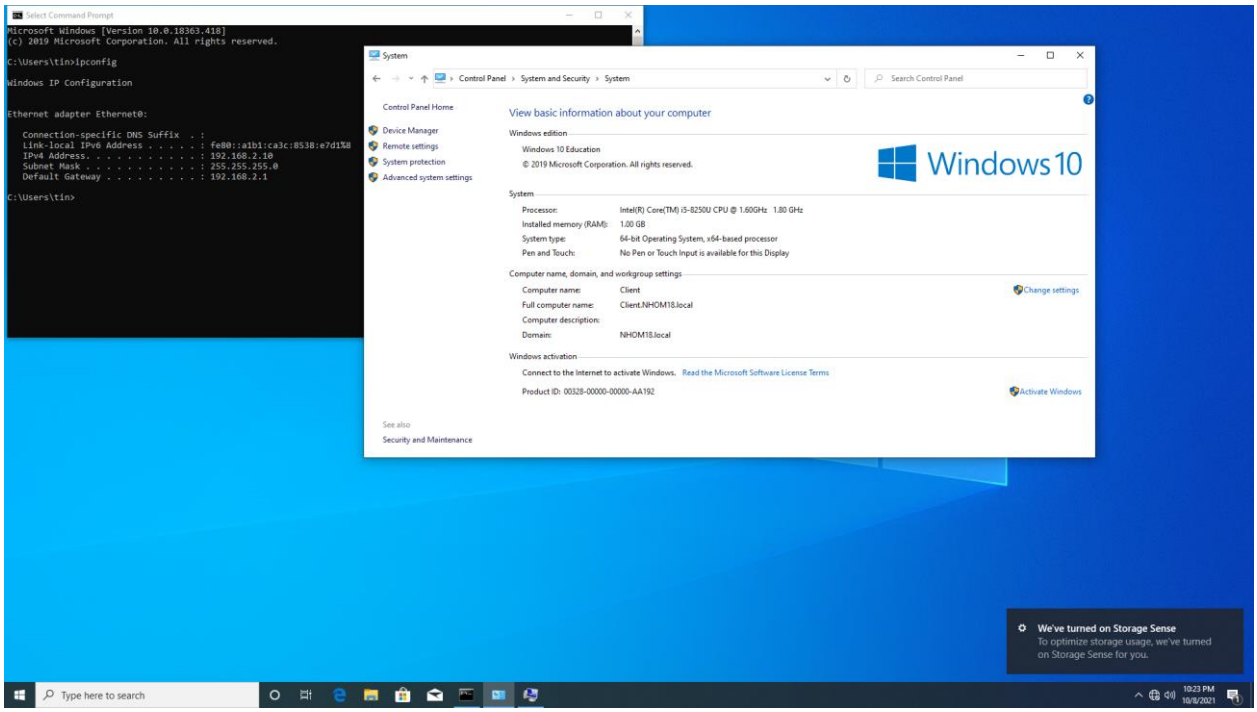


Hình 37. Chế độ Remote Desktop ON

Bước 2: Tiến hành cấp quyền cho User Remote desktop

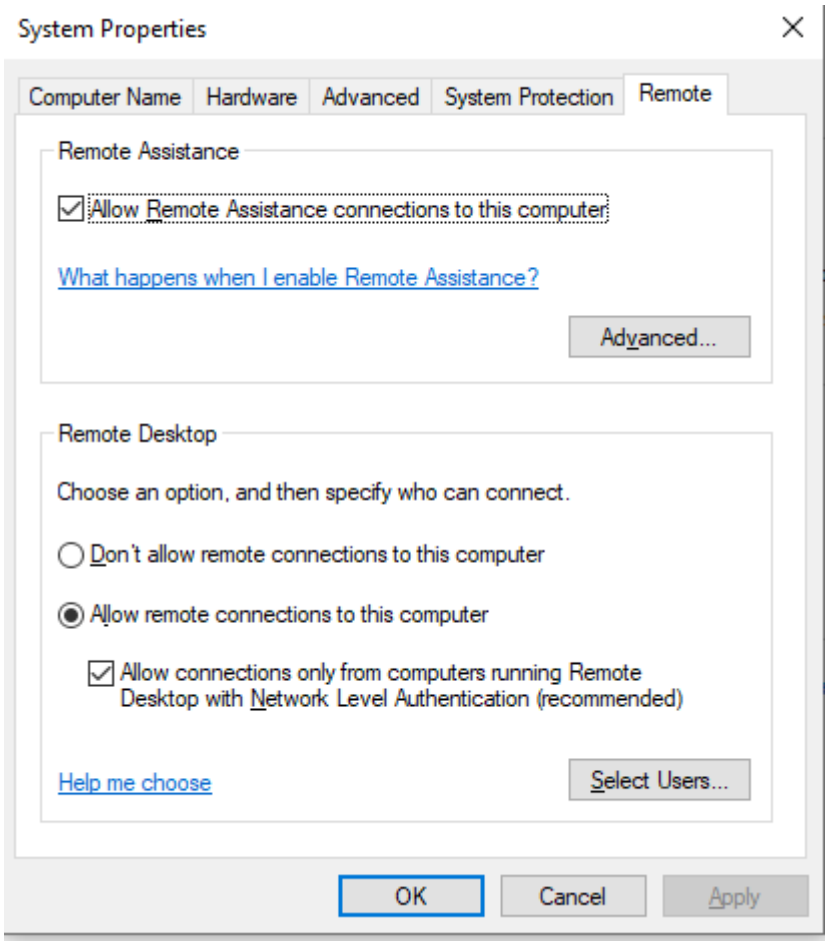
-Giả sử **User1** được phép, còn **User2** thì không

-Vào **Control Panel→System and Security→System→Advanced system settings**



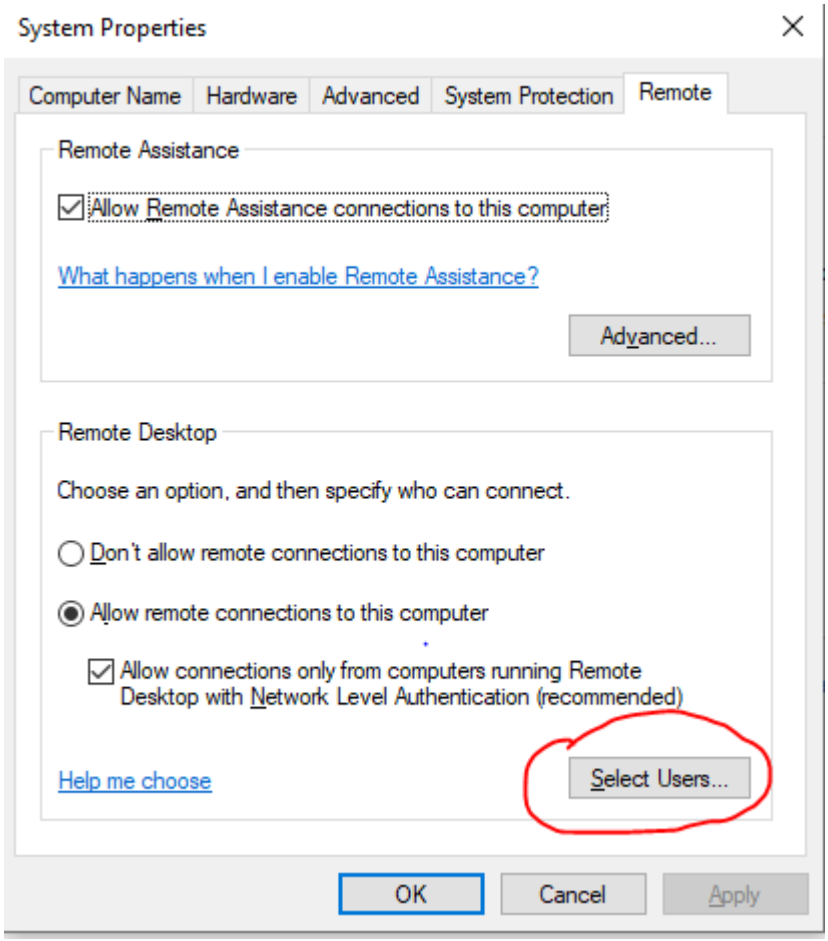
*Hình 38. Hộp thoại **System Properties** xuất hiện*

-Hộp thoại **System Properties** xuất hiện → Chọn **Allow remote connections to this computer** và tích vào mục (**recommended**) như hình



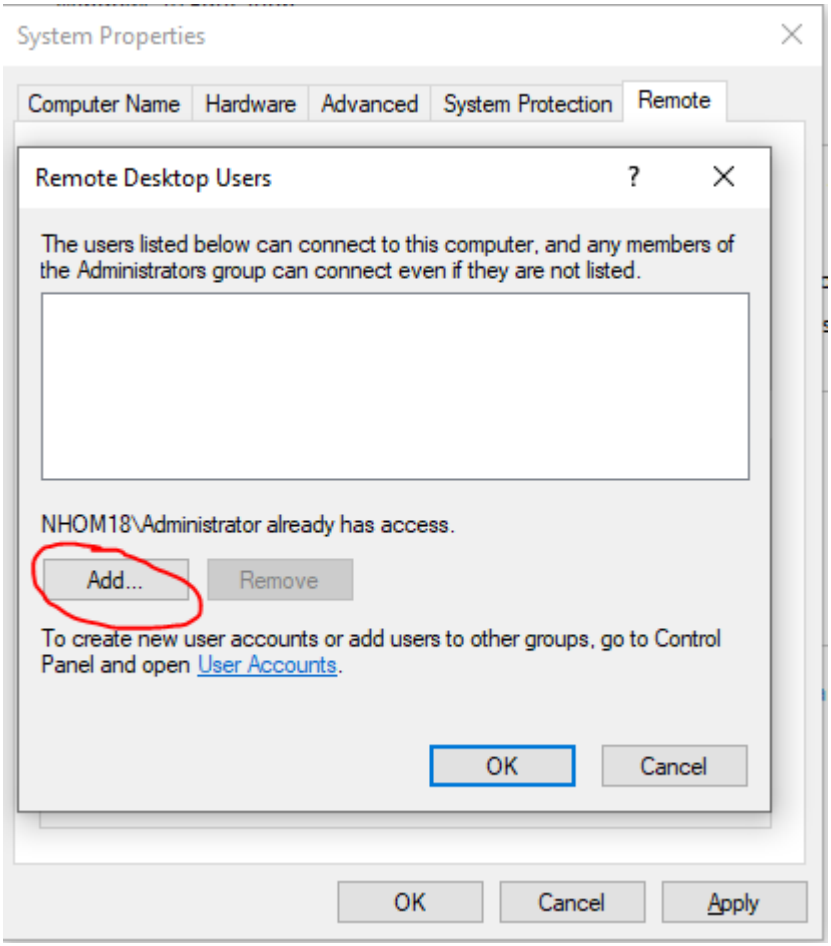
Hình 39. Chọn Allow remote connections to this computer

-Kế tiếp chọn **Select User**



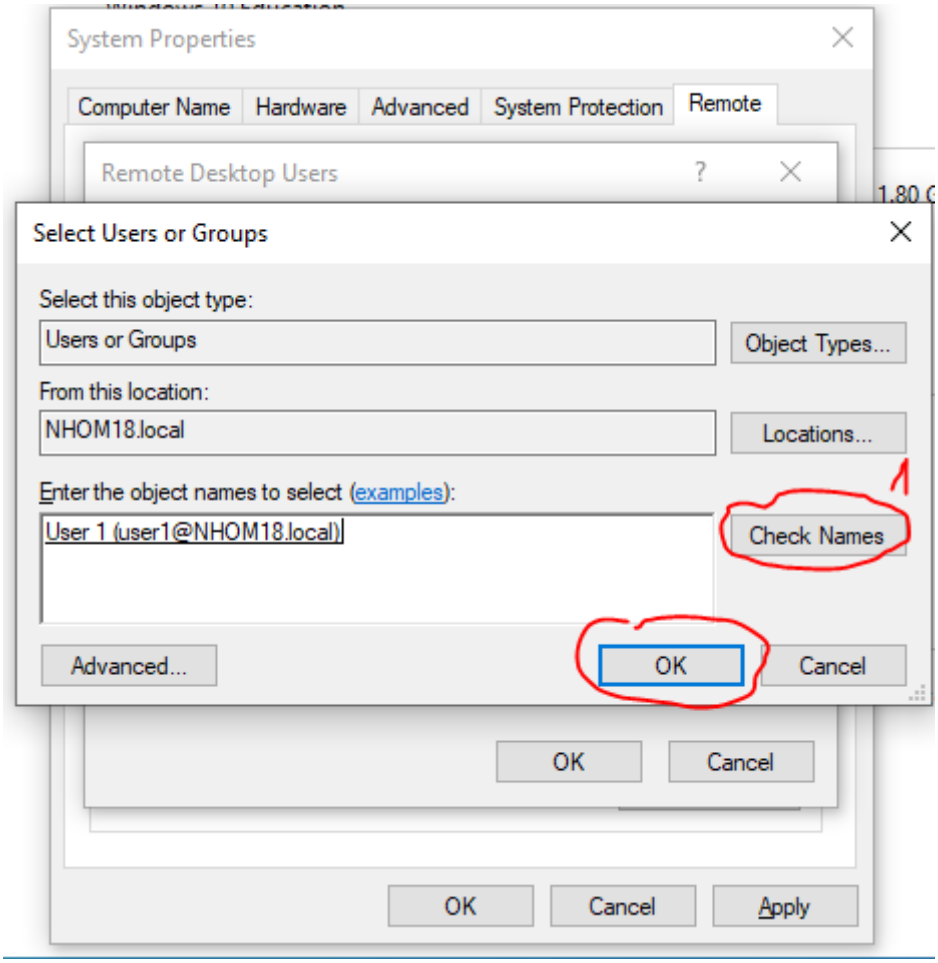
Hình 40. Chọn Select User

-Kế tiếp chọn **Add**



Hình 41. Chọn Add để thêm user

-Điền **user1** và bảng **Enter the object names to select(examples)→Check names→OK**

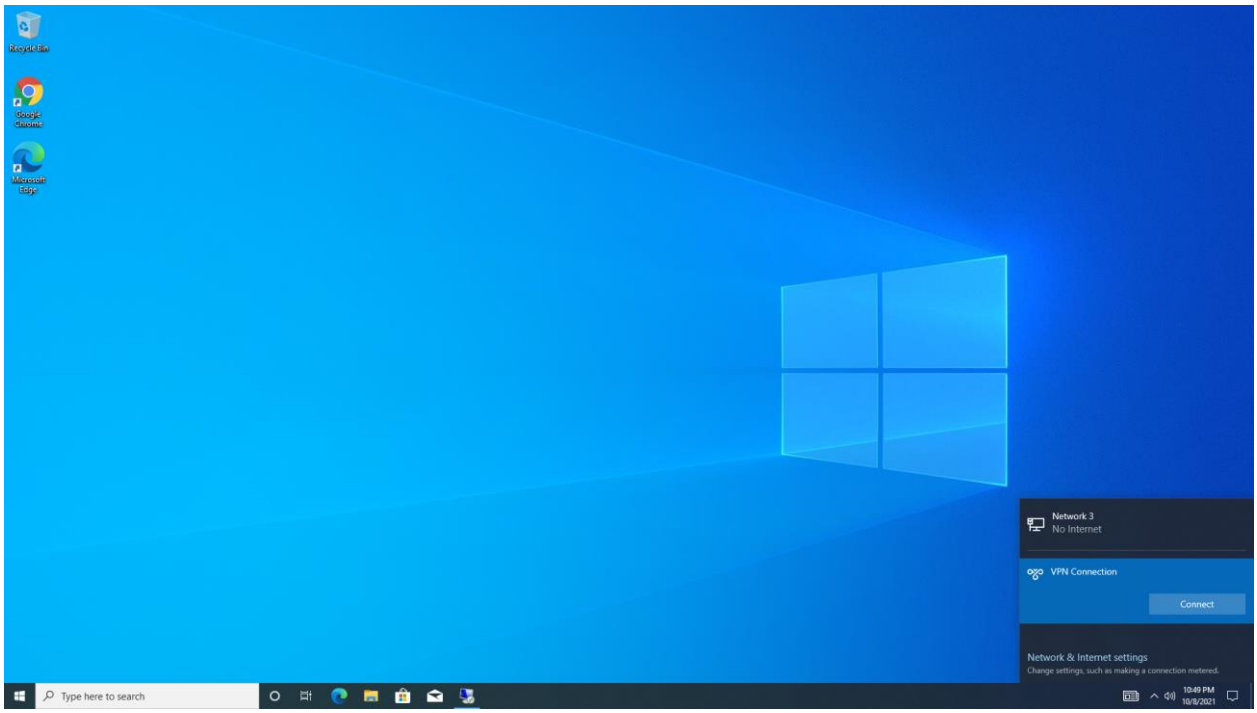


Hình 42. Bấm Check Names rồi bấm OK để hoàn tất quá trình thêm user

→Như vậy máy Win10 cùng mạng với máy Server đã cho phép **User1** Remote desktop, **User2** thì không.

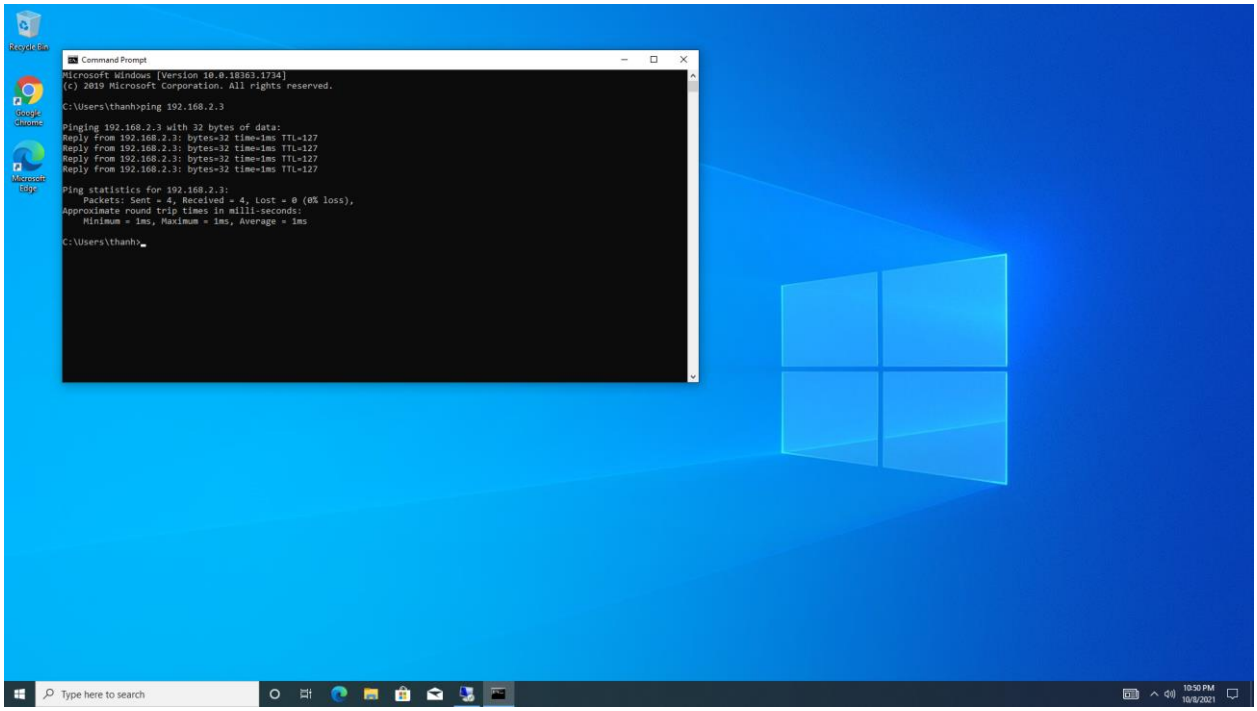
3.2.3 Cấu hình trên máy Window 10 (172.16.1.10/24)

Bước 1: Kết nối VPN



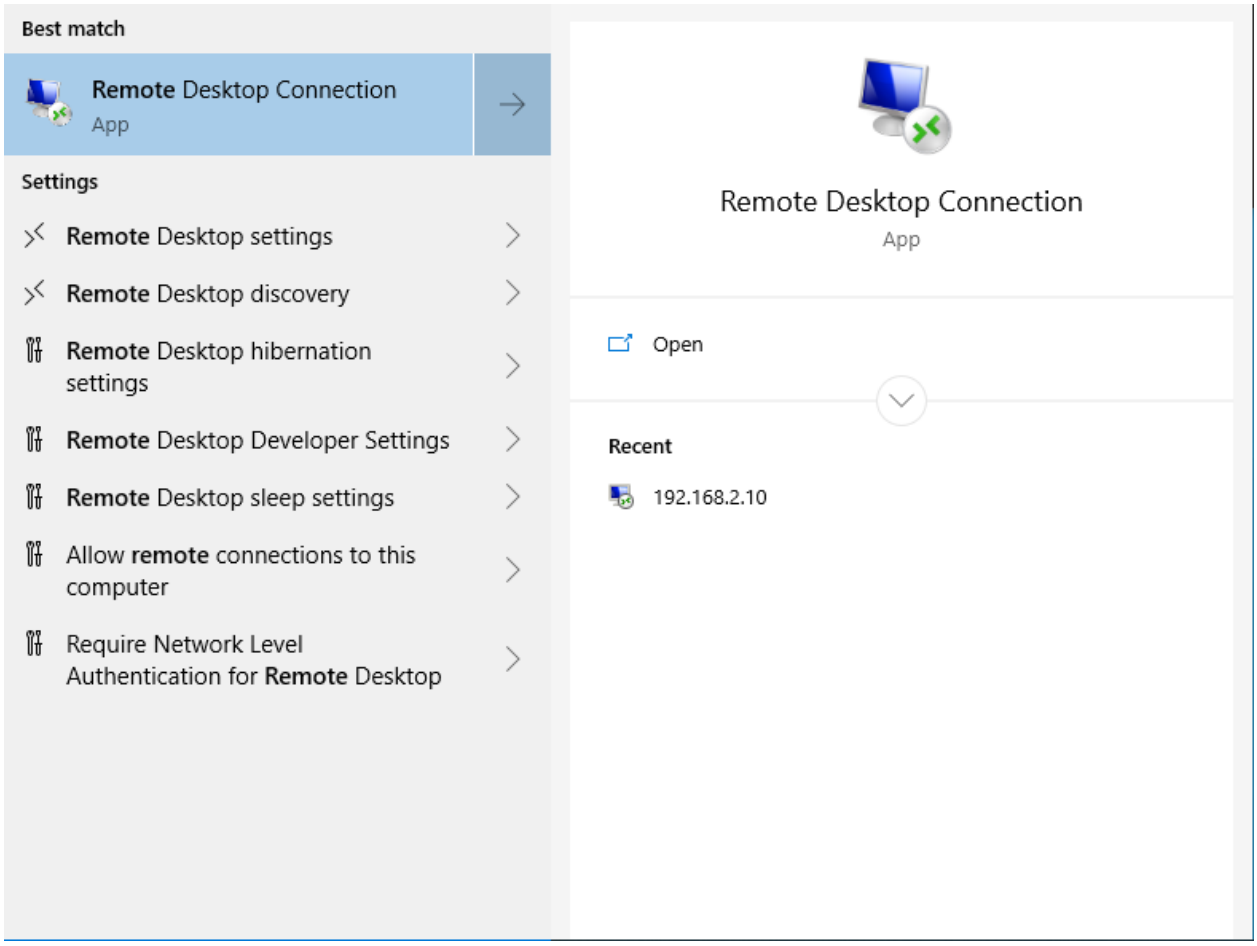
Hình 43. Tiến hành kết nối VPN

Bước 2: Test kết nối đến máy **Server(192.168.2.3)**



Hình 44. Ping thành công đến Server

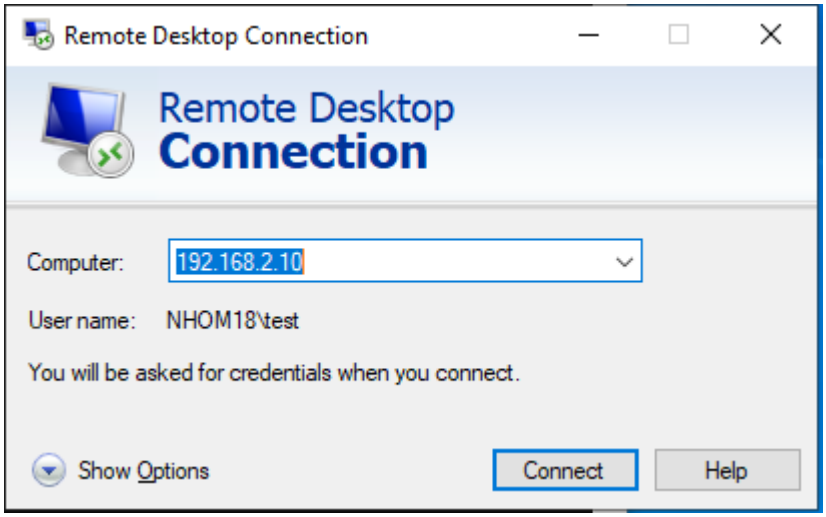
Bước 3: Mở app **Remote Desktop connection**



Hình 45. Tại mục Start menu tìm app Remote Desktop connetion

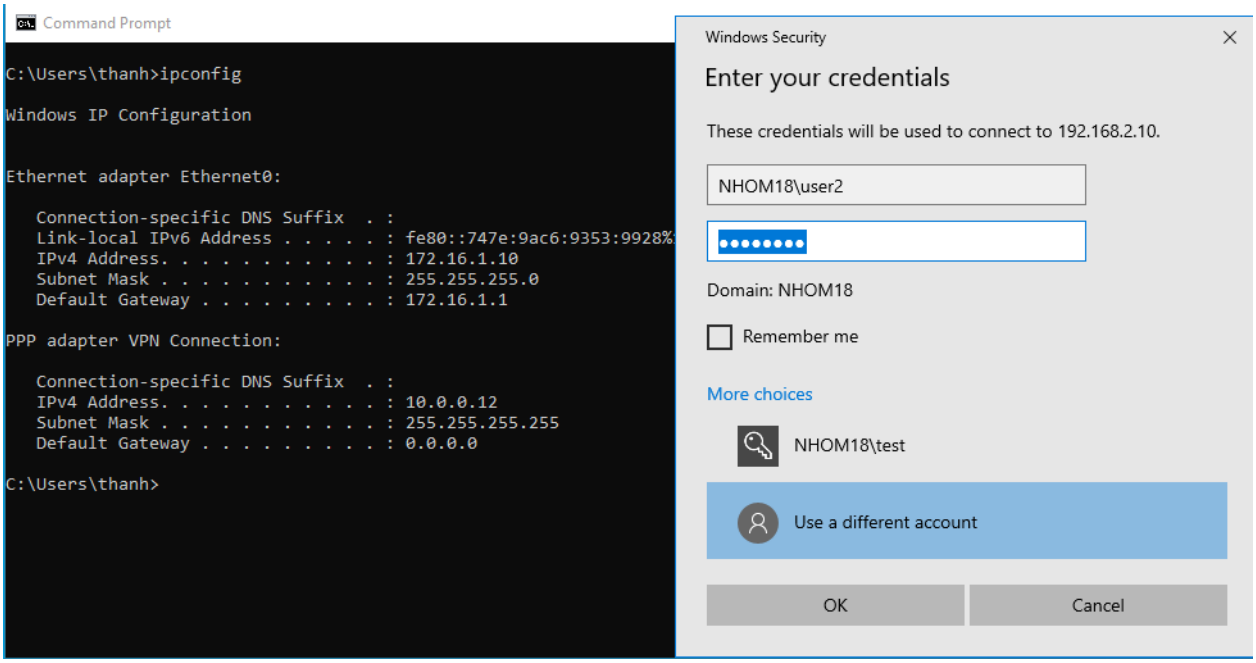
Bước 4: Nhập địa chỉ máy **Win10(192.168.2.10/24)** cùng mạng với máy **Server**

Bấm connect



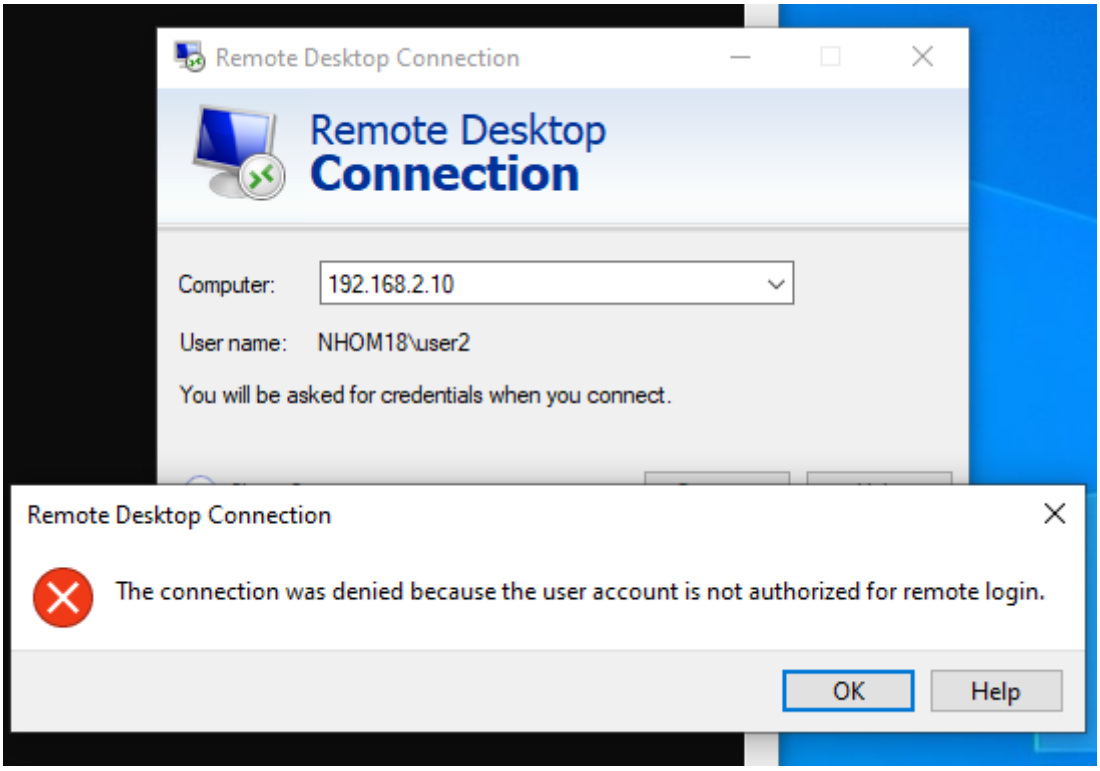
Hình 46. Nhập địa chỉ máy Window 10 cần kết nối vào hộp thoại

Bước 5: Nhập tài khoản **user2** được tạo ở trên và kiểm tra kết quả



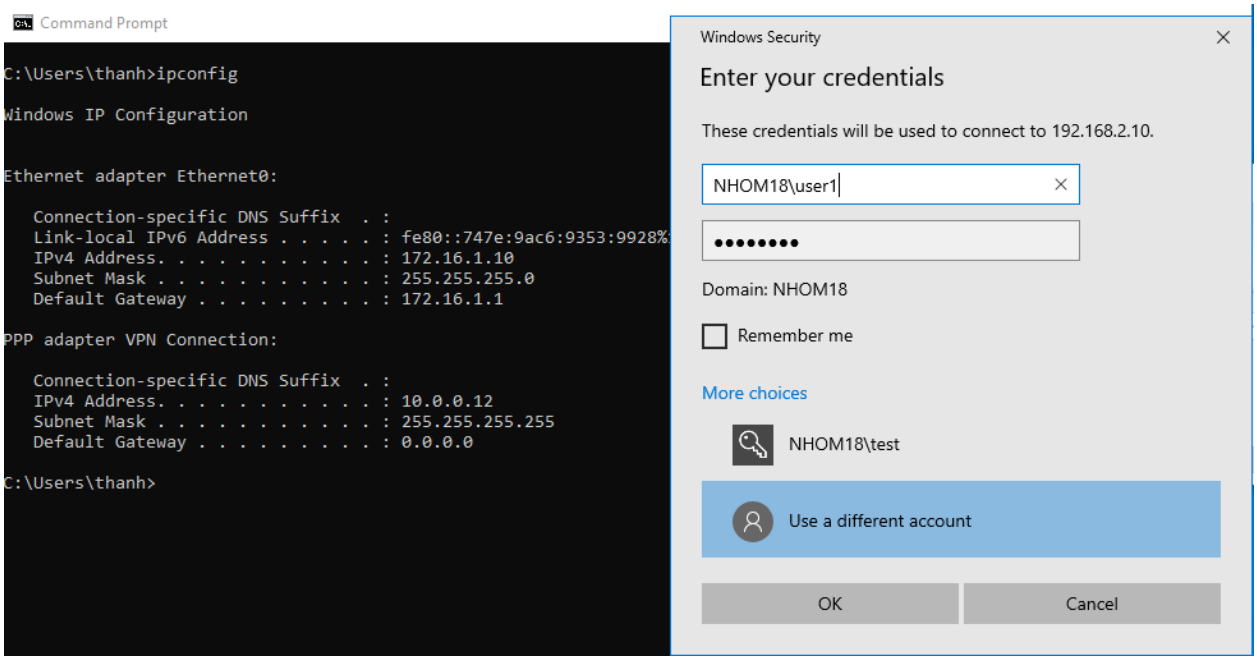
Hình 47. Nhập tài khoản User2

Do **User2** không được cho phép nên không thể kết nối

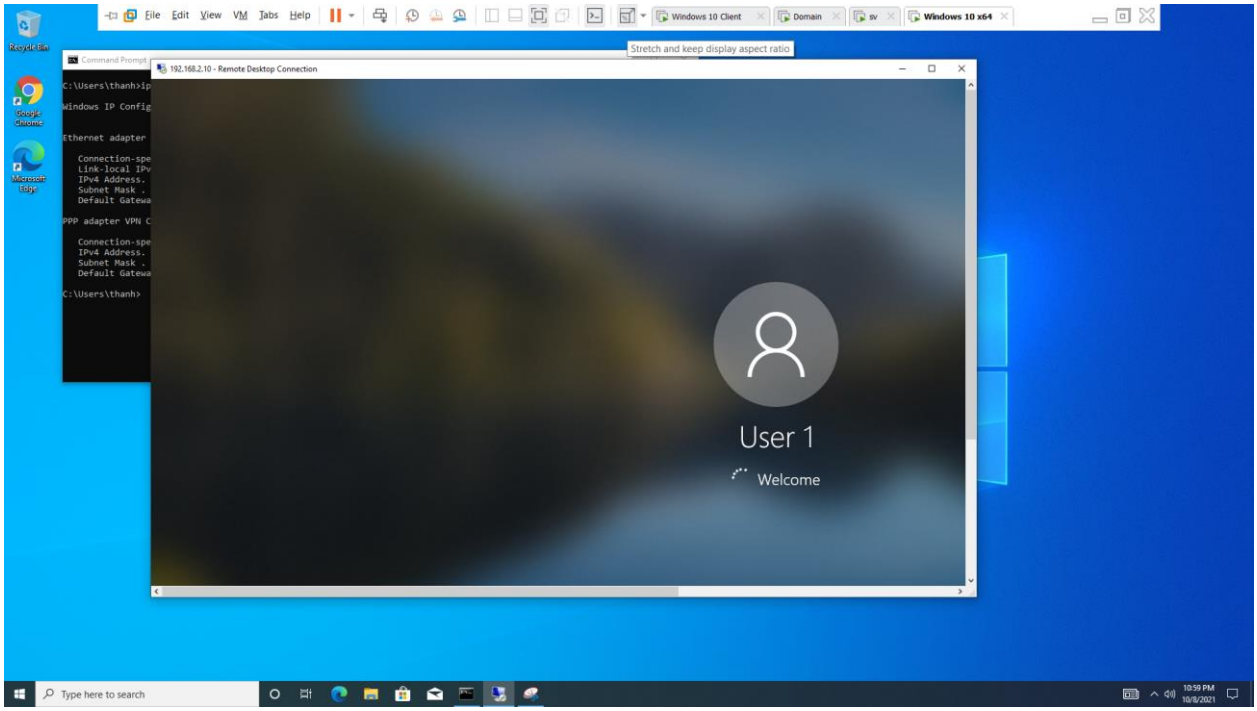


Hình 48. Kết nối thất bại

Tiếp tục với **User1**

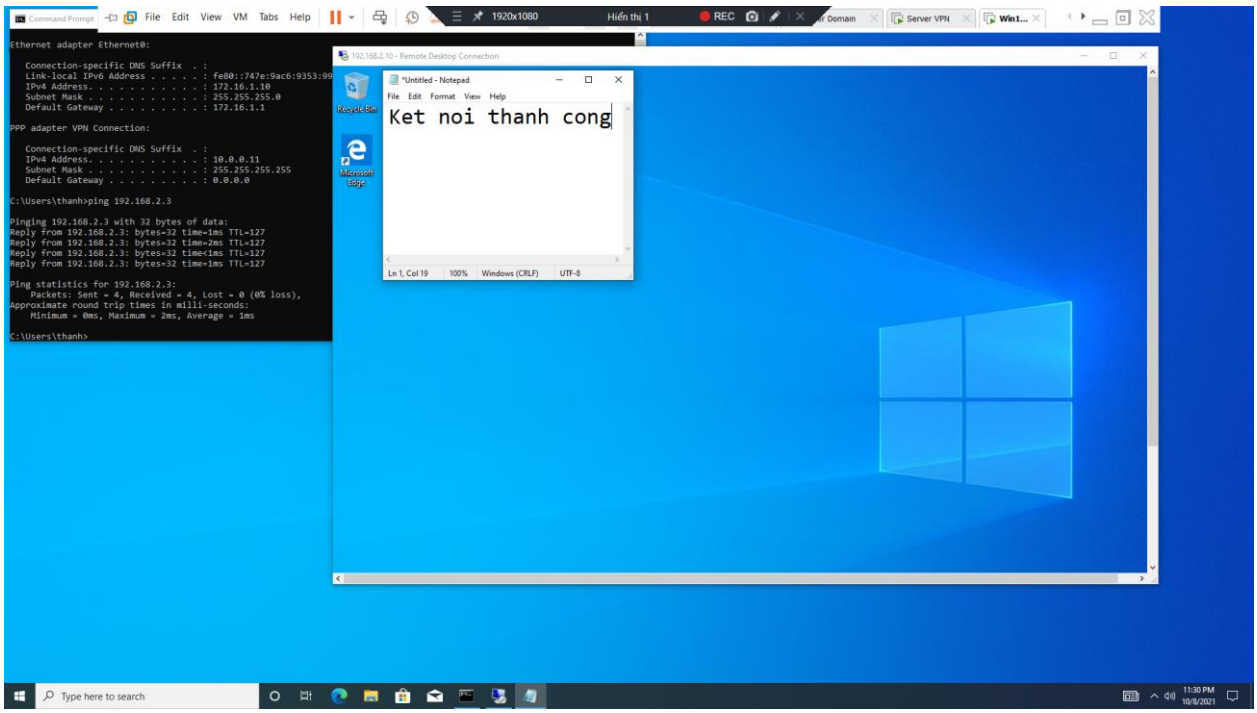


Hình 49. Nhập tài khoản mật khẩu của User1



Hình 50. Hình ảnh kết nối thành công

→Kết nối thành công, do ta đã thiết lập cho phép **user1**



Hình 51. Giao diện khi Remote Desk thành công

C. NHẬN XÉT KẾT QUẢ

-Trên đây Lab hướng dẫn cấu hình VPN Client to Site (Remote Access VPN) trên Windows Server 2012 sử dụng giao thức kết nối PPTP(**Point to Point Tunneling Protocol**)

Ưu điểm

-Dễ dàng thực hiện, nhanh chóng hiệu quả.

- Những kết nối với khoảng cách xa sẽ được thay thế bởi các kết nối cục bộ, mang lại nhiều lợi ích: tiết kiệm chi phí, tính linh hoạt, khả năng mở rộng…

-Do đây là một kết nối mang tính cục bộ, nên tốc độ nối kết sẽ cao hơn so với kết nối trực tiếp đến những khoảng cách xa.

Nhược điểm

-Remote Access VPN cũng không bảo đảm được chất lượng phục vụ.

-Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát.

Kết luận:

-Đối với doanh nghiệp

+Nhân viên nên sử dụng VPN để cung cấp khả năng truy cập Internet an toàn khi sử dụng mạng WiFi chung.

+VPN phải được triển khai bởi các nhân viên để đảm bảo truy cập từ xa an toàn vào mạng công ty và những tài nguyên trong đó.

-Đối với cá nhân

+ Nếu bạn muốn truy cập Internet một cách an toàn, riêng tư và tự do, hãy sử dụng VPN.

+ Để phát trực tuyến nội dung không có sẵn từ mọi nơi.

+ Để tránh bị giám sát.

D. PHÂN CÔNG CÔNG VIỆC

	Đoàn Ngọc Chuẩn	**Nguyễn Quốc Bảo Hiệp**	**Nguyễn Trung Tín**	**Nguyễn Văn Thành**	**Vũ Phạm Đức Thịnh**
Phần Tổng quan	x	x		x	
Mô hình & Cài đặt			x	x	x
Phần Lab cơ bản	x		x		x
Phần Lab nâng cao			x	x	x
Phần nhận xét kết quả		x			
Làm Word	x	x	x	x	x
Chỉnh sửa word	x				x
Thuyết trình		x		x	

Phần tự nhận xét:

-Phần lý thuyết chủ yếu nói về VPN, ít về phần Window VPN.

-Phần lab đơn giản, dễ thực hiện.

-(5-7) điểm trong tiêu chí chấm báo cáo