

**TRƯỜNG CAO ĐẲNG KỸ THUẬT CAO THẮNG  
KHOA ĐIỆN TỬ VIỄN THÔNG  
BỘ MÔN ĐIỆN – ĐIỆN TỬ**

**---o0o---**



**THIẾT KẾ & QUẢN TRỊ  
HỆ THỐNG MẠNG**

**ĐỀ TÀI:**

**TERMINAL SERVICES & VPN**

**GVHD: ThS. TRẦN TÚ NAM KHA**

**SVTH:BÙI MINH THIÊN**

**LỚP: CĐ ĐTTT19MT**

**NGUYỄN HUỲNH TRUNG TÍNH LỚP: CĐ ĐTTT19MT**

**TẠ MINH TIẾN**

**LỚP: CĐ ĐTTT19MT**

**HUỲNH THÀNH ĐẠT**

**LỚP: CĐ ĐTTT19MT**

**TP. HỒ CHÍ MINH, 12 - 2021**

## **NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

Tác phong: (tinh thần, thái độ làm việc trong quá trình thực hiện)

.....  
.....  
.....

Quyển báo cáo: (hình thức, nội dung)

.....  
.....  
.....  
.....

Những kết quả đạt được của môn học:

.....  
.....  
.....  
.....  
.....  
.....

Những hạn chế của môn học:

.....  
.....  
.....

Đánh giá chung đề tài

Xuất sắc  Giỏi  Khá  Trung bình  Yếu

Đề nghị:

Được phản biện

Không được bảo vệ

Điểm đánh giá: (từng SVTH)

.....  
.....  
.....

TP.HCM, ngày ... tháng .... năm 2020

**Giảng viên hướng dẫn**

(ký và ghi rõ họ tên)

## LỜI CẢM ƠN



Nhóm thực hiện đề tài xin gửi lời cảm ơn chân thành đến tập thể giáo viên khoa Điện – Điện tử Trường Cao đẳng Kỹ thuật Cao Thắng, đặc biệt là sự hướng dẫn và giúp đỡ nhiệt tình của thầy Trần Tú Nam Kha đã hết lòng giúp đỡ nhóm thực hiện đề tài.

Trải qua thời gian học tập tại trường Cao đẳng Kỹ thuật Cao Thắng, mặc dù không phải là dài nhưng với những kiến thức quý báu mà thầy cô tận tình chỉ bảo đã giúp cho nhóm rất nhiều trong thực tiễn. Thực tế thì nhờ những kiến thức đó mà nhóm có được sự tự tin trong công việc, vững vàng hơn khi va chạm thực tế.

Với sự kính trọng và biết ơn sâu sắc, nhóm xin gửi đến Ban Giám hiệu nhà trường cùng toàn thể quý thầy cô lời cảm ơn chân thành về những kiến thức hữu ích mà nhóm nhận được từ sự truyền đạt tận tình của quý thầy cô, đặc biệt là thầy Trần Tú Nam Kha đã trực tiếp hướng dẫn giúp nhóm hoàn thành báo cáo này.

Vì thời gian có hạn, và kiến thức còn nhiều hạn chế nên báo cáo của nhóm chắc chắn không tránh khỏi sai sót, vì vậy nhóm rất mong nhận được sự đóng góp ý kiến của quý thầy cô để có thể nhận ra được những sai sót của nhóm từ đó có thể hoàn thiện được kiến thức của mình hơn.

Cuối cùng kính chúc thầy cô sức khỏe, hạnh phúc và thành công!

Sinh viên thực hiện

1. Bùi Minh Thiên
2. Nguyễn Huỳnh Trung Tính
3. Tạ Minh Tiến
4. Huỳnh Thành Đạt

# MỤC LỤC

DANH MỤC CÁC HÌNH .....	1
DANH MỤC TỪ VIẾT TẮT .....	4
LỜI MỞ ĐẦU .....	5
CHƯƠNG 1: TERMINAL SERVICES .....	6
I. Terminal Services .....	6
I.1. Giới thiệu terminal services .....	6
I.1.1. Các thành phần của terminal services .....	7
I.1.2. Các phương án triển khai terminal services: .....	7
I.1.3. Một số tính năng của terminal services.....	8
I.1.4. Lợi ích của việc sử dụng terminal services .....	9
I.2.Cài đặt terminal services .....	10
I.2.1 Yêu cầu:.....	10
I.2.2 Chuẩn bị: .....	10
I.2.3. Thực hiện: .....	11
I.2.3.1. Cài đặt terminal services .....	11
I.2.3.2. Tạo user và cấp quyền remote desktop cho user.....	19
I.2.3.3. Client kết nối vào terminal server bằng remote desktop connection .....	24
I.2.3.4. Client kết nối vào terminal server bằng web access .....	26

I.2.3.5. Cấu hình remote application .....	32
I.2.3.6. Client kết nối remote application .....	37
CHƯƠNG 2: VIRTUAL PRIVATE NETWORK .....	40
II. Virtual Private Network (VPN).....	40
II.1. Giới thiệu virtual private network.....	40
II.1.1. VPN hoạt động như thế nào? .....	41
II.1.2. Phân loại VPN .....	41
II.1.3. Phương thức hoạt động của VPN .....	43
II.1.4. Lợi ích của VPN .....	45
II.1.5. Ưu điểm và hạn chế của VPN.....	46
II.2. Cài đặt virtual private network .....	47
II.2.1. Yêu cầu .....	47
II.2.2. Chuẩn bị .....	47
II.2.3. Thực hiện .....	48
II.2.3.1 Tạo Folder và chia sẻ thư mục.....	48
II.2.3.2 Tạo tài khoản dùng để thiết lập dịch vụ VPN.....	51
II.2.3.3 Thực hiện cài đặt dịch vụ Remote Access .....	53
II.2.3.4. Thực hiện cấu hình dịch vụ VPN Server .....	59
II.2.3.5. Cài đặt VPN connection cho Client.....	64
II.2.3.6. Kết nối và kiểm tra.....	69

KẾT LUẬN .....	72
TÀI LIỆU THAM KHẢO .....	73

## DANH MỤC CÁC HÌNH

STT	Kí hiệu hình	Tên hình	Trang
1	Hình 1.1	Mô hình triển khai Remote Desktop	6
2	Hình 1.2	Mô hình triển khai TS	10
3	Hình 1.3	Cửa sổ Sever Manager	11
4	Hình 1.4	Cửa sổ Before you begin	11
5	Hình 1.5	Cửa sổ Select installation type	12
6	Hình 1.6	Cửa sổ Select destination server	12
7	Hình 1.7	Cửa sổ Select server roles	13
8	Hình 1.8	Cửa sổ Select features	13
9	Hình 1.9	Cửa sổ Remote Desktop Services	14
10	Hình 1.10	Cửa sổ Select Role Services	14
11	Hình 1.11	Cửa sổ Add Roles and Features Wixard	15
12	Hình 1.12	Cửa sổ Select role servies	15
13	Hình 1.13	Cửa sổ Add Roles and Features Wizard	16
14	Hình 1.14	Cửa sổ Select role services	16
15	Hình 1.15	Cửa sổ Web Server Role (IIS)	17
16	Hình 1.16	Cửa sổ Select role servies	17
17	Hình 1.17	Cửa sổ Confirm installation selections	18
18	Hình 1.18	Cửa sổ Installation progress	18

19	Hình 1.19	Cửa sổ đăng nhập Server	19
20	Hình 1.20	Cửa sổ Server Manager	19
21	Hình 1.21	Cửa sổ New User	20
22	Hình 1.22	Cửa sổ Computer Management	20
23	Hình 1.23	Cửa sổ Computer Management	21
24	Hình 1.24	Cửa sổ Remote Desktop User Properties	21
25	Hình 1.25	Cửa sổ Select Users	22
26	Hình 1.26	Cửa sổ Remote Desktop User Properties	22
27	Hình 1.27	Cửa sổ Computer Management	23
28	Hình 1.28	Cửa sổ groupit Properties	23
29	Hình 1.29	Cửa sổ Start Client	24
30	Hình 1.30	Cửa sổ Remote Desktop Connection	24
31	Hình 1.31	Cửa sổ Windows Security	25
32	Hình 1.32	Cửa sổ Remote Desktop Connection	25
33	Hình 1.33	Cửa sổ Client kết nối windows Server	26
34	Hình 1.34	Cửa sổ Windows Server	26
35	Hình 1.35	Cửa sổ Administrative Tools	27
36	Hình 1.36	Cửa sổ Local Security Policy	27
37	Hình 1.37	Tap Local Security Setting	28
38	Hình 1.38	Cửa sổ Computer Name/Domain Changes	28
39	Hình 1.39	Cửa sổ Windows Internet Explorer	29

40	Hình 1.40	Cửa sổ Windows Internet Explorer	29
41	Hình 1.41	Tab RD Web Access	30
42	Hình 1.42	Tab RemoteApp and Desktops	30
43	Hình 1.43	Cửa sổ Windows Security	31
44	Hình 1.44	Client kết nối Desktop Windows Server	31
45	Hình 1.45	Cửa sổ Select installation type	32
46	Hình 1.46	Cửa sổ Select deployment type	32
47	Hình 1.47	Cửa sổ Select deployment scenario	33
48	Hình 1.48	Cửa sổ Select a server	33
49	Hình 1.49	Cửa sổ Confirmation selections	34
50	Hình 1.50	Cửa sổ View progress	34
51	Hình 1.51	Cửa sổ QuickSessionCollection	35
52	Hình 1.52	Cửa sổ Select RemoteApp	35
53	Hình 1.53	Cửa sổ Confirmation	36
54	Hình 1.54	Cửa sổ Completion	36
55	Hình 1.55	Cửa sổ RD Web	37
56	Hình 1.56	Cửa sổ RemoteApp	37
57	Hình 1.57	Cửa sổ Windows Security	38
58	Hình 1.58	Cửa sổ User Account Control	38
59	Hình 1.59	Client kết nối App program trên Server	39
55	Hình 2.1	Mô Hình VPN	40

56	Hình 2.2	Mô hình hoạt động của VPN	41
57	Hình 2.3	Mô hình Site-to-site VPN	42
58	Hình 2.4	Mô hình Remote-access VPN	43
59	Hình 2.5	Kỹ thuật GRE tunnel	44
60	Hình 2.6	Sơ đồ khung IP Sec	45
40	Hình 2.7	Mô hình kết nối VPN	47
53	Hình 2.8	Local Disk(C:)	48
54	Hình 2.9	Thư mục DATA	48
55	Hình 2.10	Local Disk(C:)	49
56	Hình 2.11	Cửa sổ Properties	49
57	Hình 2.12	Cửa sổ Advanced Sharing	50
58	Hình 2.13	Tab Share Permissions	50
59	Hình 2.14	Cửa sổ Server Manager	51
60	Hình 2.15	Cửa sổ Computer Management	51
53	Hình 2.16	Cửa sổ New User	52
54	Hình 2.17	Cửa sổ Tab Dial-in	52
55	Hình 2.18	Cửa sổ Server Manager	53
55	Hình 2.19	Cửa sổ Before you begin	53
56	Hình 2.20	Cửa sổ Select destination server	54
57	Hình 2.21	Cửa sổ Select server roles	54
58	Hình 2.22	Cửa sổ Select features	55

59	Hình 2.23	Cửa sổ Remote Access	55
60	Hình 2.24	Cửa sổ Select role services	56
40	Hình 2.25	Cửa sổ Add Roles and Features Wizard	56
53	Hình 2.26	Cửa sổ Web Server Role (IIS)	57
54	Hình 2.27	Cửa sổ Select role services	57
55	Hình 2.28	Cửa sổ Confirm installation selections	58
56	Hình 2.29	Cửa sổ Installation progress	58
57	Hình 2.30	Cửa sổ Server Manager	59
58	Hình 2.31	Cửa sổ Routing and Remote Access	59
59	Hình 2.32	Cửa sổ Configuration	60
60	Hình 2.33	Cửa sổ Remote Access	60
53	Hình 2.34	Cửa sổ VPN Connection	61
54	Hình 2.35	Cửa sổ IP Address Assignment	61
55	Hình 2.36	Cửa sổ Address Range Assignment	62
56	Hình 2.37	Cửa sổ New Ipv4 Address Range	62
57	Hình 2.38	Cửa sổ Address Range Assignment	63
58	Hình 2.39	Managing Multiple Remote Access Server	63
59	Hình 2.40	Cửa sổ Routing and Remote Access	64
60	Hình 2.41	Cửa sổ Completing Initialization	64
55	Hình 2.42	Cửa sổ Network and Sharing Center	64
56	Hình 2.43	Cửa sổ Set Up a Connection or Network	65

57	Hình 2.44,45,46,47	Cửa sổ Connect to a Workplace	65-67
58	Hình 2.48	Cửa sổ Network and Sharing Center	67
59	Hình 2.49	Cửa sổ Network Connections	68
60	Hình 2.50	Cửa sổ VPN Connection Properties	68
40	Hình 2.51	Cửa sổ Network Connections	69
53	Hình 2.52	Cửa sổ Connect VPN Connections	69
54	Hình 2.53	Cửa sổ Network Connections	70
55	Hình 2.54	Cửa sổ Run	70
56	Hình 2.55	Cửa sổ Windows Security	70
57	Hình 2.56	Kết nối Client sang Server	71

## DANH MỤC CÁC BẢNG

STT	Ký Hiệu	Tên Bảng	Trang
1	Bảng 1.1	Các tính năng của Terminal Services	8
2	Bảng 1.2	Cấu hình IP cho cài đặt terminal servicer	10
3	Bảng 2.1	Cấu hình IP cho cài đặt VPN	47

## **DANH MỤC TỪ VIẾT TẮT**

Từ viết tắt	Từ đầy đủ (tiếng Anh)
RDS	Remote Desktop Service
RDP	Remote Desktop Protocol
TS	Terminal Server
VPN	Virtual Private Network
LAN	Local Area Network
PPTP	Point to Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
GRE	Generic Route Encapsulation
L2F	Layer 2 Forward
PPP	Point - to – Point Protocol
NAS	Network Access Server
HTTPS	Hypertext Transfer Protocol Secure
TCP	Transmission Control Protocol

## LỜI MỞ ĐẦU

Trong thập kỷ qua, Internet đã phát triển bùng nổ với tốc độ chóng mặt trên toàn thế giới cả về số lượng và về kĩ thuật. Và sự phát triển đó không có dấu hiệu sẽ dừng lại. Sự phát triển không chỉ đơn giản là số lượng lớn thành viên mới kết nối vào hệ thống Internet mỗi giờ mà còn là sự xâm nhập của nó vào các khía cạnh cuộc sống hiện đại, vào các hoạt động thương mại với quy mô lớn nhỏ khác nhau...

Vì vậy nên các windows server đã cung cấp thêm các dịch vụ remote desktop để phục vụ cho công việc điều khiển từ xa.

Remote Desktop là một tính năng trong Windows Server 2012, nó cho phép người quản trị viên thực hiện một phiên làm việc từ xa và trực tiếp trên giao diện đồ họa giống như là đang ngồi trực tiếp trên máy chủ thông qua một máy tính client. Ngoài ra còn có bàn phím và chuột trên máy tính client sẽ được sử dụng trên máy chủ từ xa. Remote Desktop có thể được thực hiện trong một số mạng như mạng điện rộng (WAN), mạng cục bộ (LAN) hoặc qua internet.

Trong Windows Server 2012 dịch vụ này được cung cấp bởi dịch vụ đầu cuối (Terminal Services).

Vấn đề phát sinh là tính bảo mật và hiệu quả kinh tế của việc truyền tải dữ liệu qua mạng trung gian công cộng không an toàn như Internet. Để giải quyết vấn đề này, một giải pháp đưa ra là mạng riêng ảo VPN. Chính điều này là động lực cho sự phát triển mạng mẽ của VPN như ngày nay.

## CHƯƠNG 1: TERMINAL SERVICES

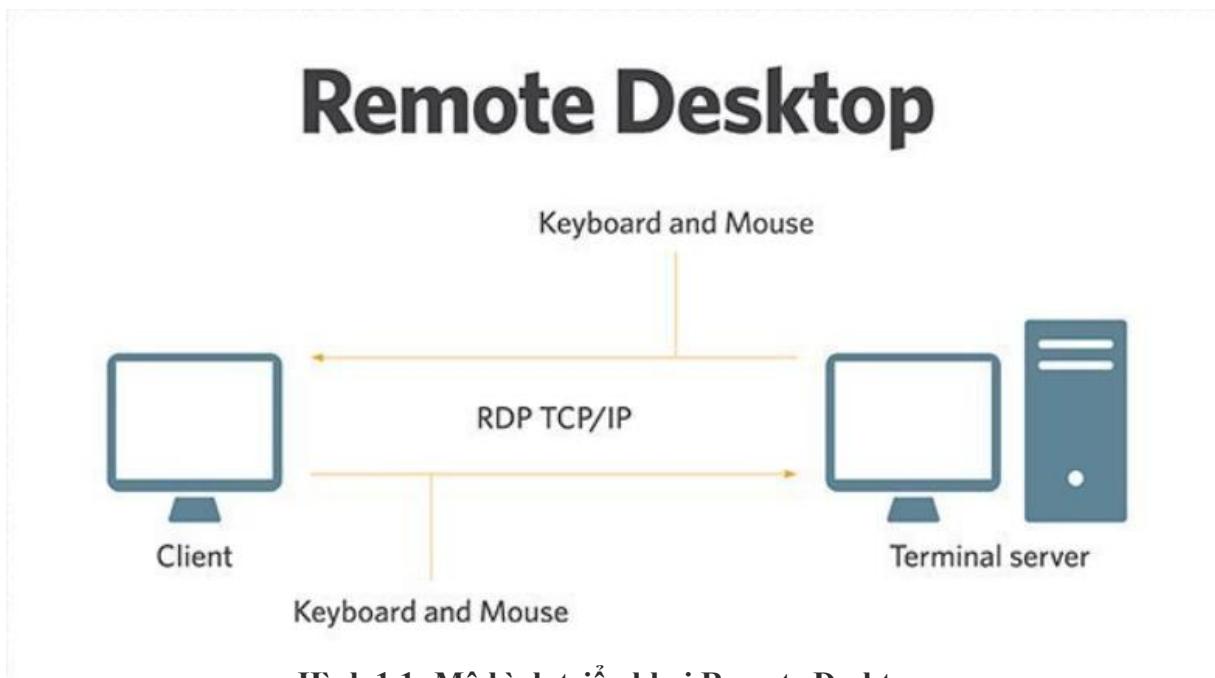
### I. TERMINAL SERVICES

#### I.1. Giới thiệu terminal services

Remote Desktop Service – RDS trước đây được biết đến với cái tên là Terminal Server. Là dịch vụ cho phép nhiều người dùng cùng một lúc kết nối từ xa đến và dùng chung một máy tính thông qua Remote Desktop hoặc RemoteApp.

Trước khi các thế hệ ứng dụng sử dụng Webapp trở nên phổ biến như ngày nay, thì RDS có thể nói là một dịch vụ rất hữu ích. Nó cho phép người dùng có thể sử dụng ứng dụng từ xa thông bên ngoài công ty thông qua môi trường internet. Nó còn giúp chi phí triển khai phần mềm có thể giảm đi đáng kể, tận dụng tối đa phần mềm.

Một ưu điểm của RDS là cho phép người dùng sử dụng các phần mềm người dùng sử dụng phần mềm chỉ cài đặt được trên nền tảng Windows khi máy trạm là Linux hoặc OSx. Máy trạm chỉ cần cài đặt các phần mềm hỗ trợ Remote Desktop (RDP).



Hình 1.1: Mô hình triển khai Remote Desktop

Với mục đích chạy các ứng dụng hay thực hiện lệnh trên máy tính ở xa. Những câu lệnh, phím bấm hay cả click chuột cũng sẽ được gửi đến máy tính từ xa và hình ảnh thực thi sẽ gửi lại người dùng tương tự như người dùng đang thao tác trực tiếp trên máy của mình vậy.

### I.1.1. Các thành phần của terminal services

Terminal Services bao gồm 3 thành phần: Terminal Services Server, giao thức Remote Desktop và Terminal Services Client.

- **Terminal Services Server**

Hầu hết các hoạt động của Terminal Services xảy ra trên Terminal Services server (hay gọi là Terminal server). Khi Terminal Services ở trong chế độ ứng dụng của máy chủ (application server mode), tất cả các ứng dụng đều chạy trên server. Terminal server sẽ gửi các thông tin về màn hình tới client và chỉ nhận các input từ chuột và bàn phím, Server phải theo dõi các session đang hoạt động.

- **Giao thức Remote Desktop**

Khi cài đặt Terminal Services, giao thức Remote Desktop (RDP) được tự động cài đặt. RDP là một kết nối duy nhất mà cần phải cấu hình để client có thể kết nối Terminal server. Bạn có thể cấu hình chỉ một kết nối RDP trên mỗi bộ điều hợp mạng.

Có thể sử dụng công cụ cấu hình của Terminal Services để cấu hình các thuộc tính của kết nối RDP. Bạn có thể thiết lập mật mã và quyền, và hạn chế lượng thời gian mà các session của client có thể còn hoạt động.

- **Terminal Services Client**

Terminal Services client (hay còn gọi là Terminal client) sử dụng công nghệ *thin client* để phân phối tới người dùng. Máy trạm chỉ cần thiết lập một kết nối tới máy chủ và hiển thị thông tin về giao diện đồ họa mà máy chỉ gửi tới.

### I.1.2. Các phương án triển khai terminal services:

- Có 4 cách để máy trạm kết nối đến máy chủ khi khai thác chương trình ứng dụng trên máy chủ:
  - **Sử dụng trình duyệt web:** Máy chủ phải cài đặt thêm Terminal Services Web Access, máy trạm phải được cài đặt Remote Desktop Connection.
  - **Sử dụng Network Accesss:** Máy chủ tạo sẵn file .rdp và được share trên máy chủ, máy trạm truy cập vào máy chủ, chạy trực tiếp file đó để khai thác chương trình ứng dụng trên máy chủ.
  - **Sử dụng Network Access:** Máy chủ tạo sẵn file .msi và được share trên máy chủ, máy trạm truy cập vào máy chủ, chạy trực tiếp file đó để cài đặt các shortcut liên kết đến chương trình ứng dụng trên máy chủ. Các shortcut này được cài đặt trong Start menu của máy trạm, cụ thể là mục Remote Application. Máy trạm chạy các shortcut đó để khai thác chương trình ứng dụng trên máy chủ.
  - **Sử dụng policy:** Để triển khai hàng loạt việc cài đặt shortcut liên kết đến chương trình ứng dụng trên máy chủ cho nhiều máy trạm.

### I.1.3. Một số tính năng của terminal services

Terminal Services bao gồm nhiều đặc tính làm nó dễ sử dụng và quản lý. Các đặc tính này được mô tả trong bảng.

**Bảng 1.1: Các tính năng của Terminal Services**

Đặc tính	Mô tả
Hỗ trợ logon nhiều lần	Người dùng có thể logon nhiều lần cùng lúc, kể cả từ nhiều client hay từ một client và cũng có thể logon vào nhiều server. Điều này cho phép người dùng thực hiện nhiều tác vụ cùng lúc.
Hỗ trợ roaming disconnect	người dùng có thể disconnect khỏi một session mà không cần phải log off. Session này sẽ vẫn còn hoạt động khi đã disconnect, cho phép người dùng connect lại vào lúc khác từ một client khác.
Nâng cao hoạt động	Việc sử dụng bộ đệm (catching) được nâng cao làm cải thiện đáng kể hoạt động.
Gửi lại clipboard	Người dùng có thể cắt và dán (cut & paste) giữa các ứng dụng trên máy cục bộ với các ứng dụng trên Terminal Services.
Hỗ trợ máy in cục bộ tự động	Các máy in được nối vào client được tự động bổ sung và kết nối lại.
Bảo mật	Quá trình logon được mã hoá và người quản trị có thể xác định số lần logon và thời gian connect của một người dùng. Dữ liệu được truyền giữa các server và client có thể được mã hoá ở 3 mức độ (thấp, trung bình, cao) tùy thuộc vào nhu cầu bảo mật của bạn.
Điều khiển từ xa các session	Hai người dùng có thể xem một session cùng một lúc. Điều này giúp hỗ trợ các vấn đề chẩn đoán nhân sự hay đào tạo người dùng.
Cân bằng tải mạng	Terminal Services có thể phân đều các kết nối của client cho một nhóm các server, do đó làm giảm bớt tải trên mỗi server.
Thiết bị đầu cuối dựa trên Windows	Các thiết bị đầu cuối dựa trên Windows chạy trên một phiên bản được sửa đổi của Windows CE và giao thức Remote Desktop.
Bộ quản trị kết nối của client	Tiện ích này tạo một icon trên nền Desktop cho phép kết nối nhanh tới server cho các chương trình đơn lẻ hay các truy cập đầy đủ của Desktop.
Việc cấp quyền của Terminal Services	Công cụ này giúp người quản trị theo dõi người dùng và quyền của họ.
Hỗ trợ DFS	Người dùng có thể connect tới một chia sẻ DFS và người quản trị để <b>host</b> một chia sẻ hệ thống file phân tán từ một Terminal Services server.
Bộ quản trị Terminal	Công cụ này được người quản trị sử dụng để truy vấn và quản trị các session, người dùng và các quá trình.

Services	
Cấu hình Terminal Services	Công cụ này để tạo, sửa, và xoá các session.
Tích hợp với người dùng cục bộ và Active Directory	Người quản trị có thể tạo các tài khoản của Terminal Services theo cách tương tự như khi tạo các tài khoản cho người dùng.
Tích hợp với System Monitor	Các đặc điểm hoạt động của hệ thống của Terminal Services có thể được System Monitor theo dõi
Hỗ trợ truyền thông điệp	Người quản trị có thể gửi thông điệp tới các client
Quản trị từ xa	Người dùng với các quyền thích hợp có thể quản trị từ xa tất cả các khía cạnh của một Terminal Services server
Thời gian tạm ngưng session có thể cấu hình	Người quản trị có thể cấu hình thời gian một session có thể tồn tại ở trạng thái hoạt động hay trạng thái nghỉ trước khi ngắt kết nối.

#### I.1.4. Lợi ích của việc sử dụng terminal services

Terminal Services cung cấp nhiều lợi ích làm cho nó trở thành giải pháp ưu việt nhất cho mạng:

**Sự phát triển rộng hơn của Windows 2000:** Thay vì cài đặt một phiên bản đầy đủ của Windows 2000 trên tất cả các máy thì bạn có thể triển khai Terminal Services. Các máy tính có phần cứng không được phiên bản đầy đủ của Windows 2000 hỗ trợ vẫn có thể sử dụng nhiều đặc tính của Windows 2000.

**Sự hoạt động đồng thời của cả phần mềm thin client và các hệ điều hành độc lập:** Với Terminal Services, người dùng mạng có thể tiếp tục sử dụng hệ thống có sẵn trong máy của họ, nhưng vẫn có thể dùng các lợi ích của môi trường Windows 2000.

**Sự phát triển các ứng dụng được đơn giản hóa:** Thay vì cài đặt và cập nhật các ứng dụng trên tất cả các máy trong mạng thì người quản trị có thể cài đặt một bản sao trên Terminal Services server. Điều này đảm bảo rằng mọi người dùng đều truy cập được vào phiên bản mới nhất của ứng dụng.

**Việc quản trị từ xa của máy chủ:** Terminal Services cho phép bạn quản trị server từ xa. Điều này rất hữu ích nếu người quản trị cần phải rời xa máy chủ trong một khoảng thời gian nào đó.

## I.2. Cài đặt Terminal Services

### I.2.1 Yêu cầu:

Quá trình cài đặt và cấu hình Terminal Services gồm các bước cơ bản sau đây:

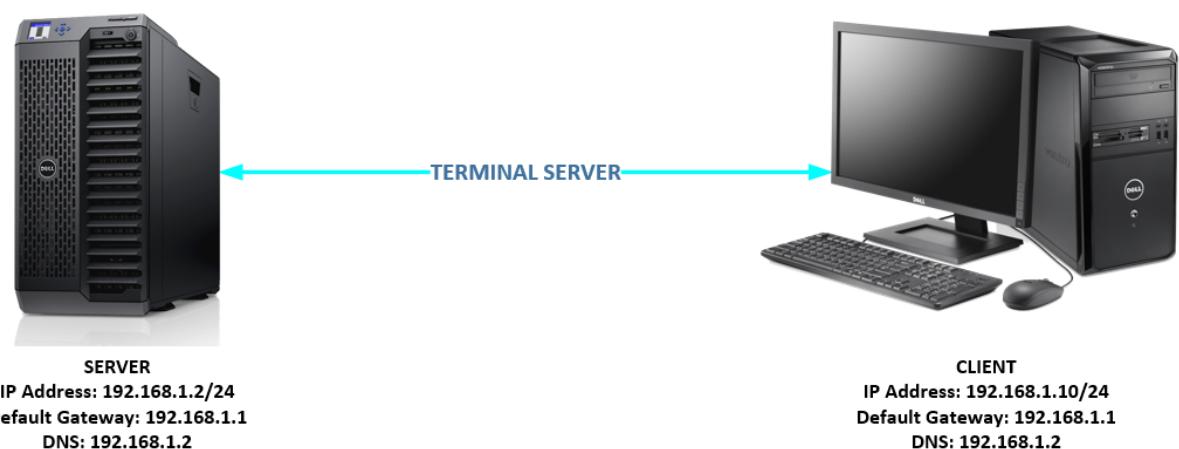
- 1) Cài đặt Terminal Services
- 2) Tạo user và cấp quyền Remote Desktop cho user
- 3) Client kết nối Terminal Server bằng Remote Desktop Connection
- 4) Client kết nối vào Terminal Server bằng Web Access
- 5) Cấu hình Remote Application
- 6) Client kết nối Remote Application

### I.2.2 Chuẩn bị:

Gồm 2 máy cấu hình IP như hình 1.2

**Bảng 1.2: Cấu hình IP**

Server	Client
Window Server 2012	Window 7
IP Address: 192.168.1.2/24	IP Address: 192.168.1.10/24
Default Gateway: 192.168.1.1	Default Gateway: 192.168.1.1
DNS: 192.168.1.2	DNS: 192.168.1.2

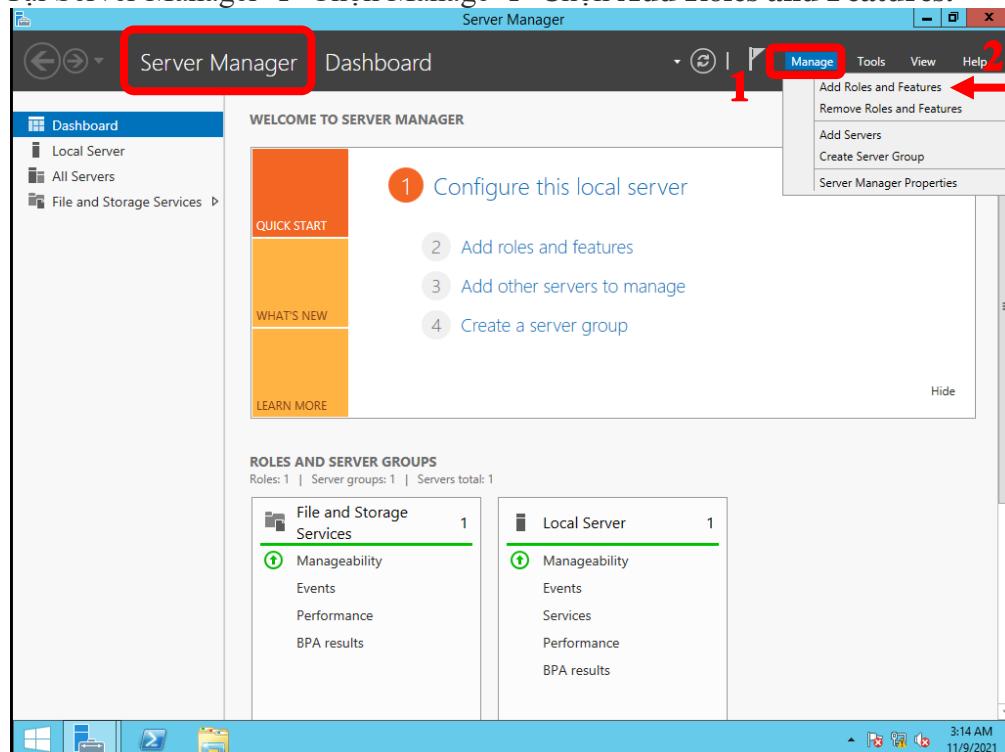


**Hình 1.2: Mô hình triển khai TS**

### I.2.3. Thực hiện:

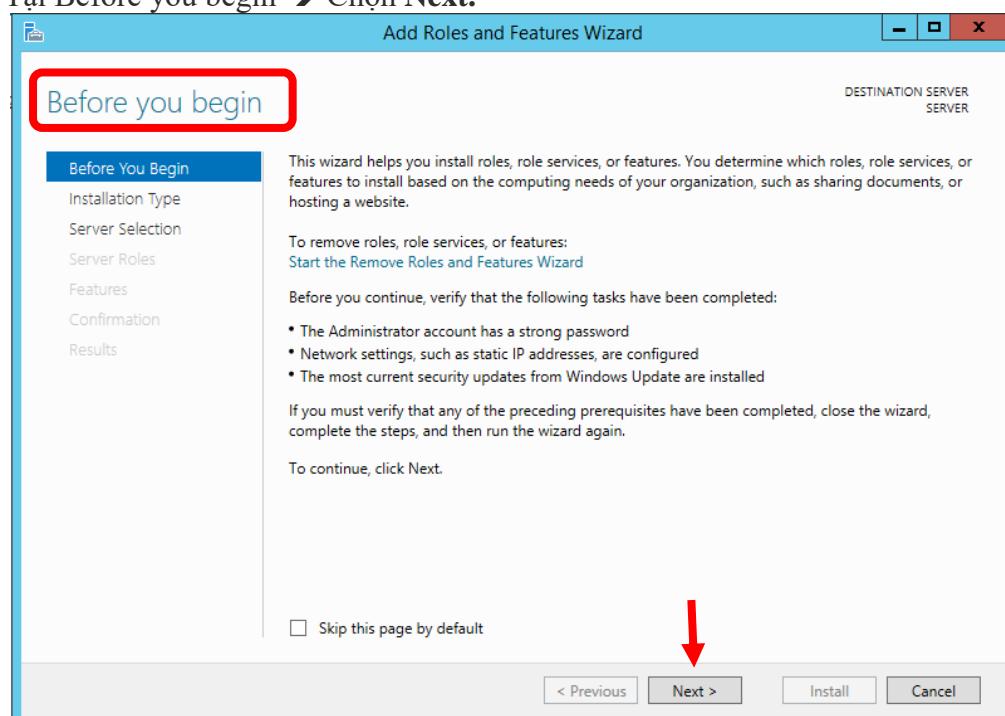
#### I.2.3.1. Cài đặt Terminal Services

- Tại máy Server → Chọn Server Manager.
- Tại Server Manager → Chọn Manage → Chọn Add Roles and Features.



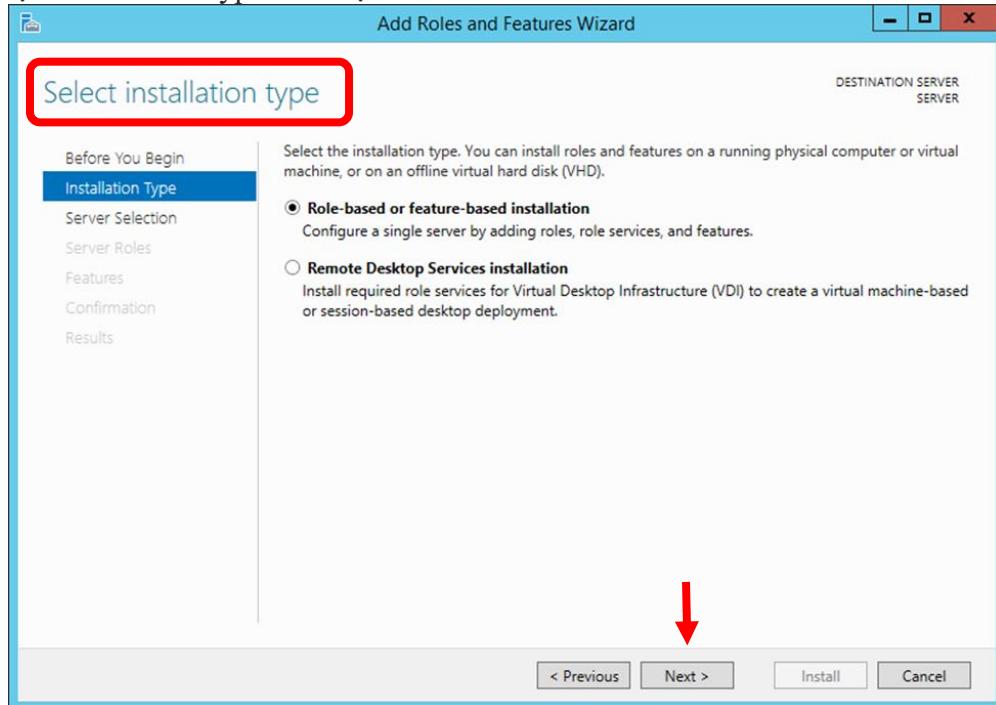
Hình 1.3: Cửa sổ Sever Manager

- Tại Before you begin → Chọn Next.



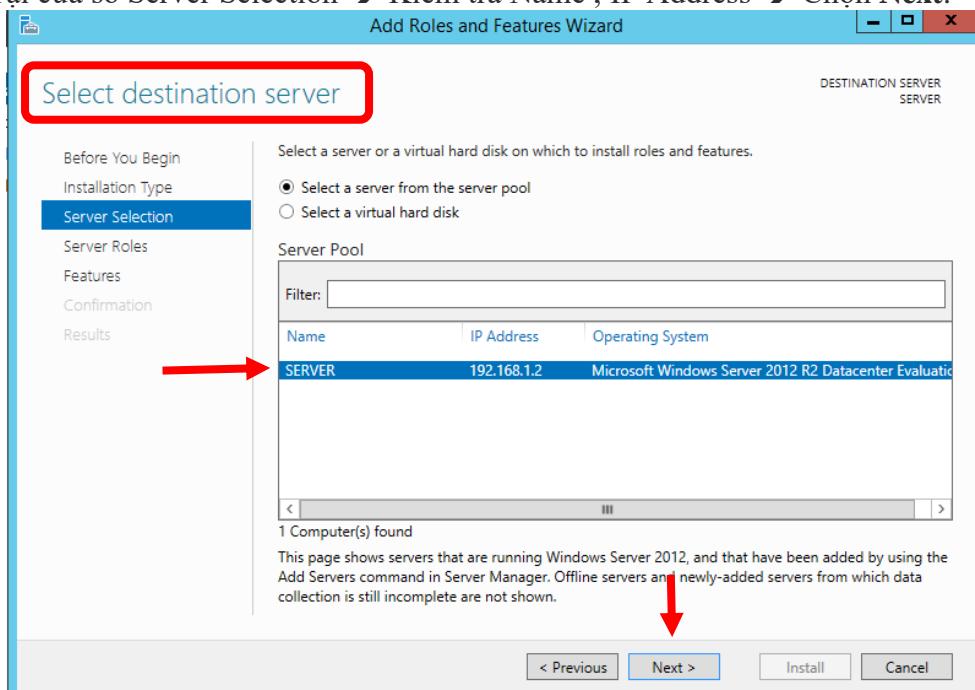
Hình 1.4: Cửa sổ Before you begin

- Tại Installation Type → Chọn Next.



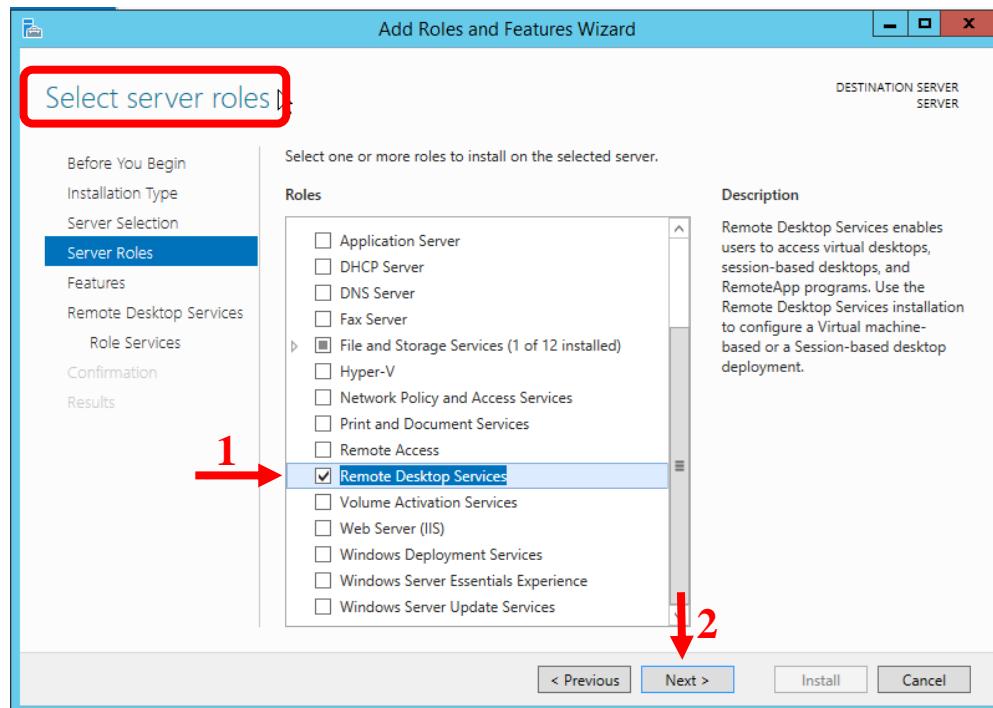
Hình 1.5: Cửa sổ Select installation type

- Tại cửa sổ Server Selection → Kiểm tra Name , IP Address → Chọn Next.



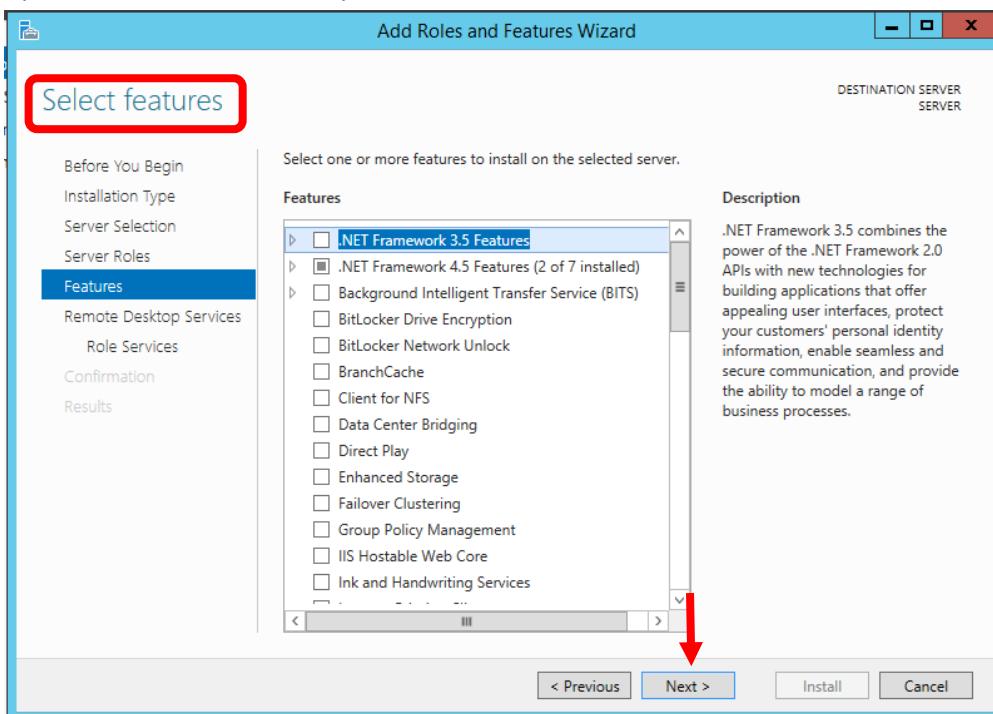
Hình 1.6: Cửa sổ Select destination server

- Tại cửa sổ Sever Roles → Từ Roles → Chọn Remote Desktop Services → Chọn Next.



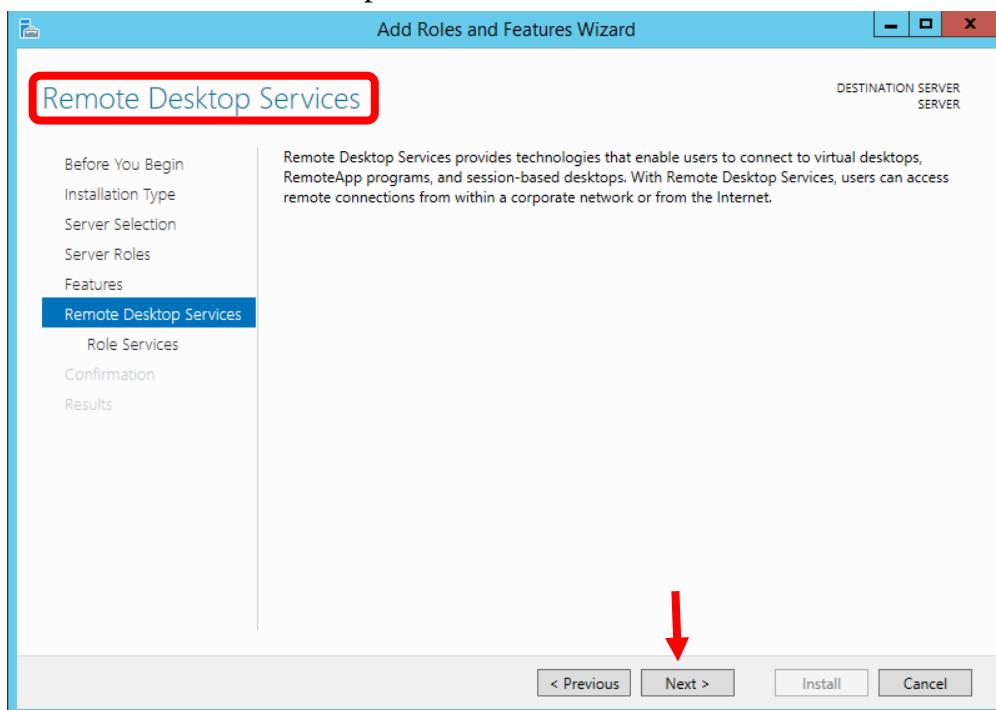
Hình 1.7: Cửa sổ Select roles

- Tại cửa sổ Features → Chọn Next.



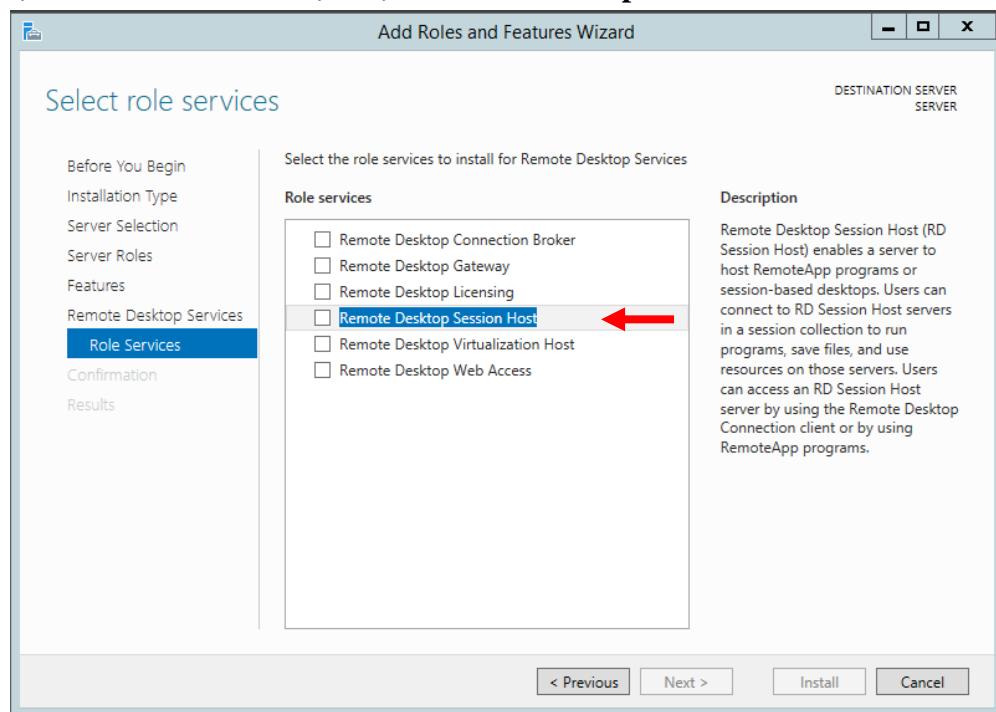
Hình 1.8: Cửa sổ Select features

- Tại cửa sổ Remote Desktop Services ➔ Chọn Next



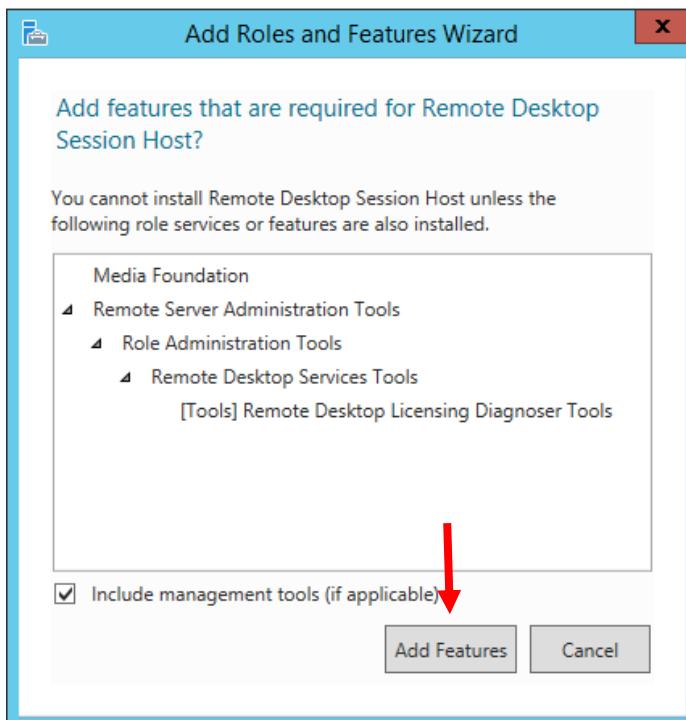
**Hình 1.9: Cửa sổ Remote Desktop Services**

- Tại Role Services ➔ Chọn mục **Remote Desktop Session Host**.



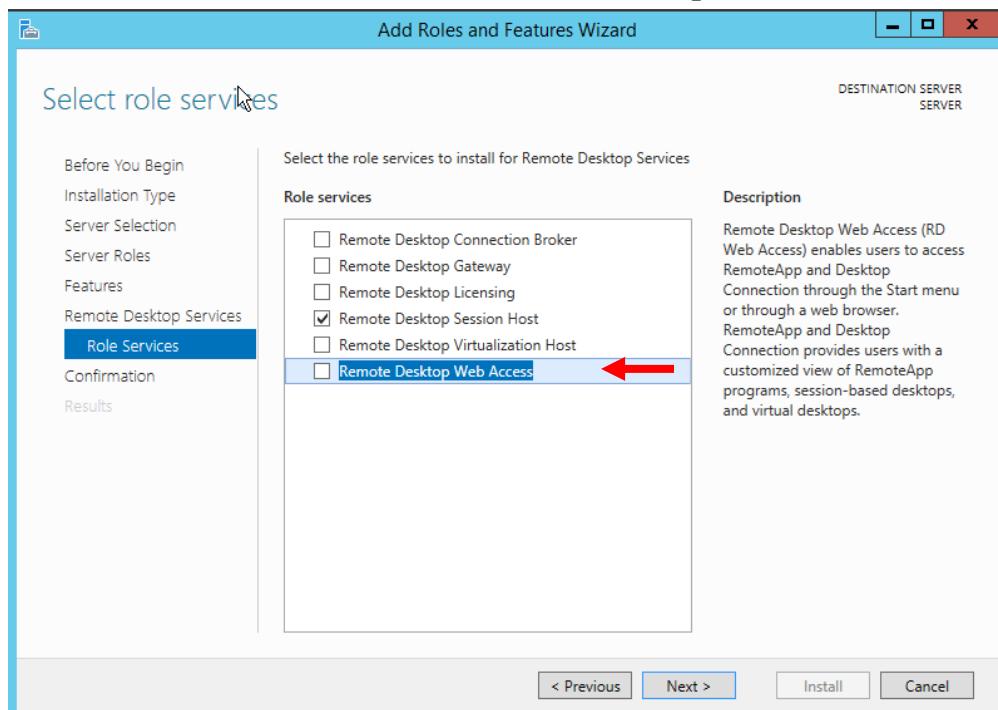
**Hình 1.10: Cửa sổ Role Services**

- Cửa sổ Add Roles and Features Wizard được hiện lên → chọn **Add Features**.



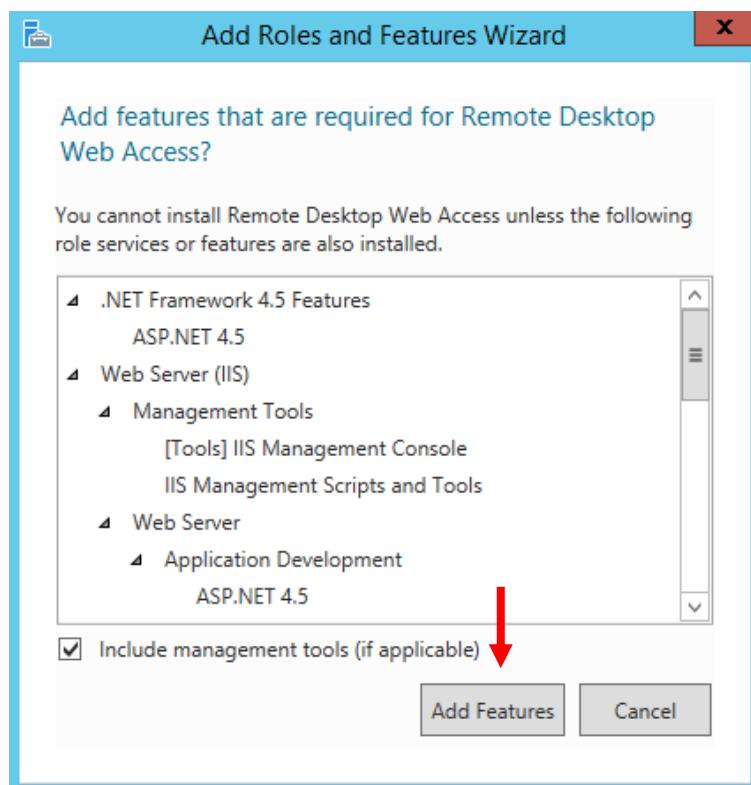
Hình 1.11: Cửa sổ Add Roles and Features Wixard

- Trở về cửa sổ Role services → Chọn **Remote Desktop Web Access**.



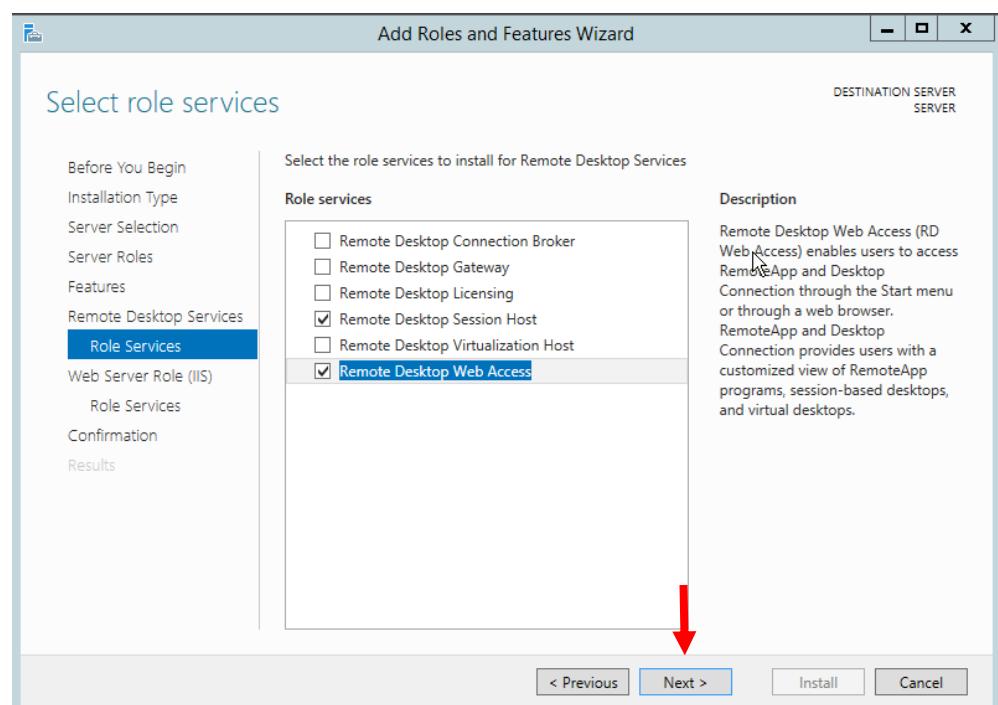
Hình 1.12: Cửa sổ Select role servies

- Cửa sổ Add Roles and Features Wizard ➔ Chọn **Add Features**.



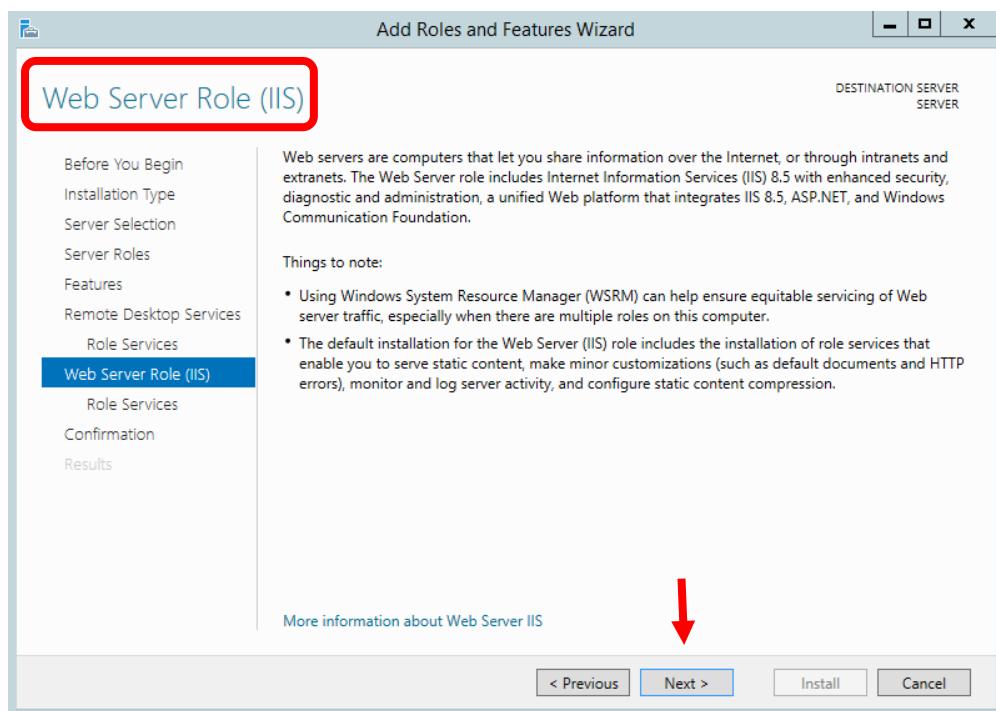
Hình 1.13: Cửa sổ Add Roles and Features Wizard

- Trở về cửa sổ Select role services ➔ Tiếp tục chọn **Next**.



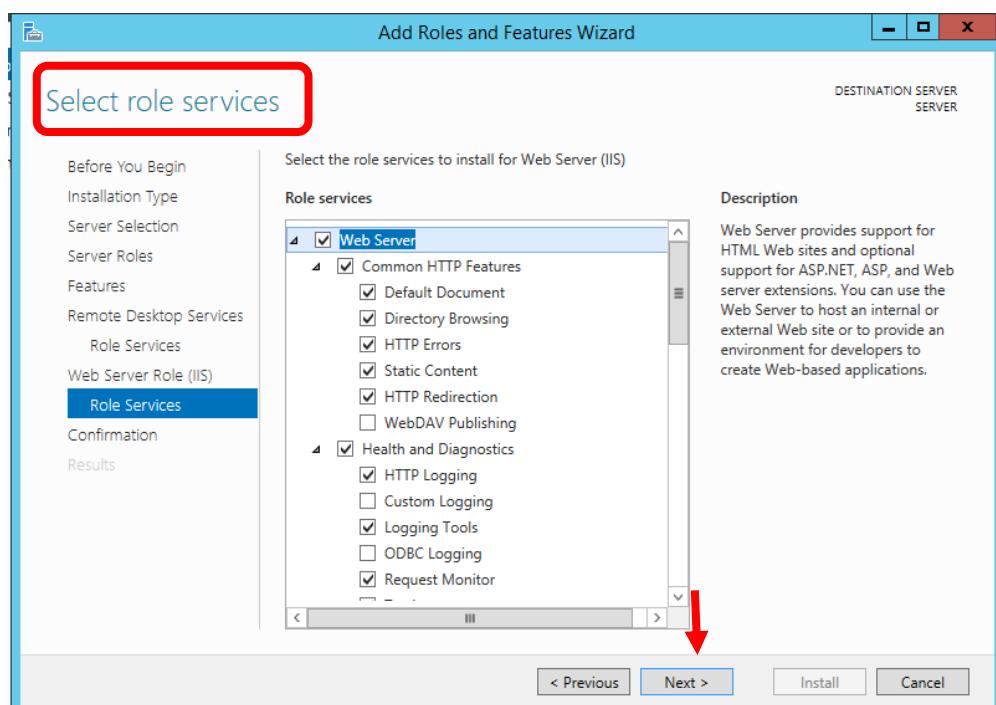
Hình 1.14: Cửa sổ Select role services

- Tại cửa sổ Web Server Role (IIS) ➔ Chọn Next.



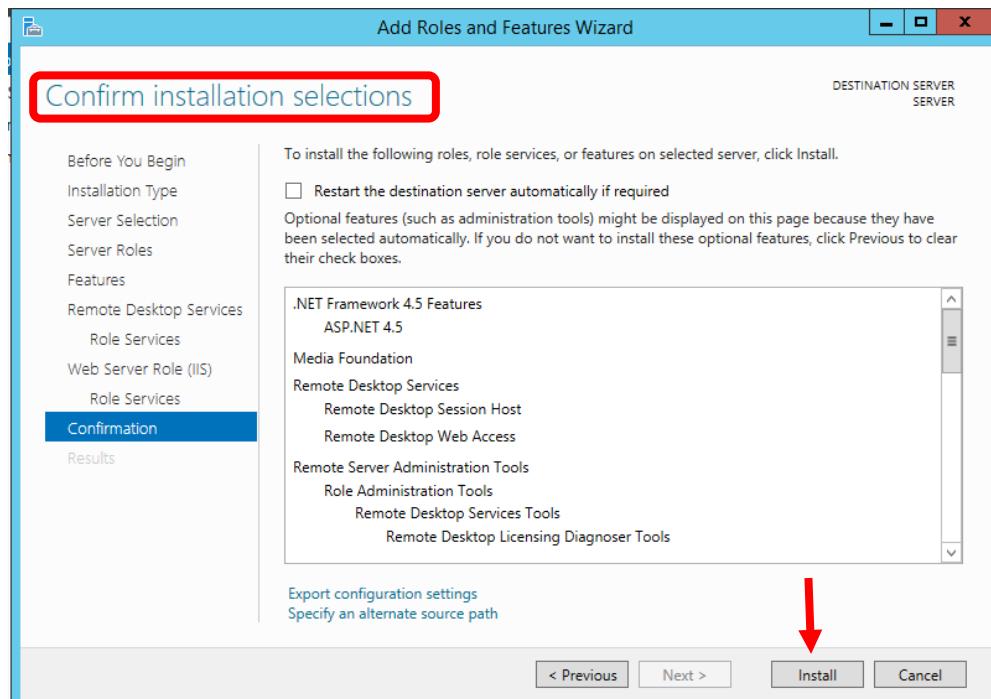
Hình 1.15: Cửa sổ Web Server Role (IIS)

- Tiếp tục tại cửa sổ Select role Services ➔ Chọn Next.



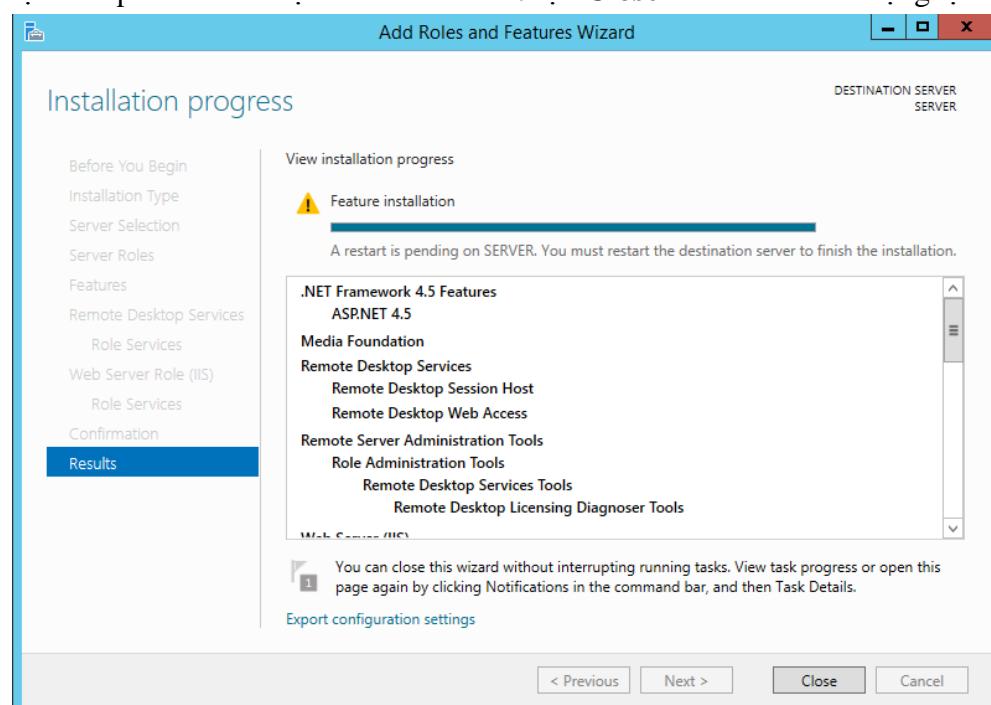
Hình 1.16: Cửa sổ Select role services

- Tại cửa sổ Confirm installation selections → Chọn **Install**.



**Hình 1.17: Confirm installation selections**

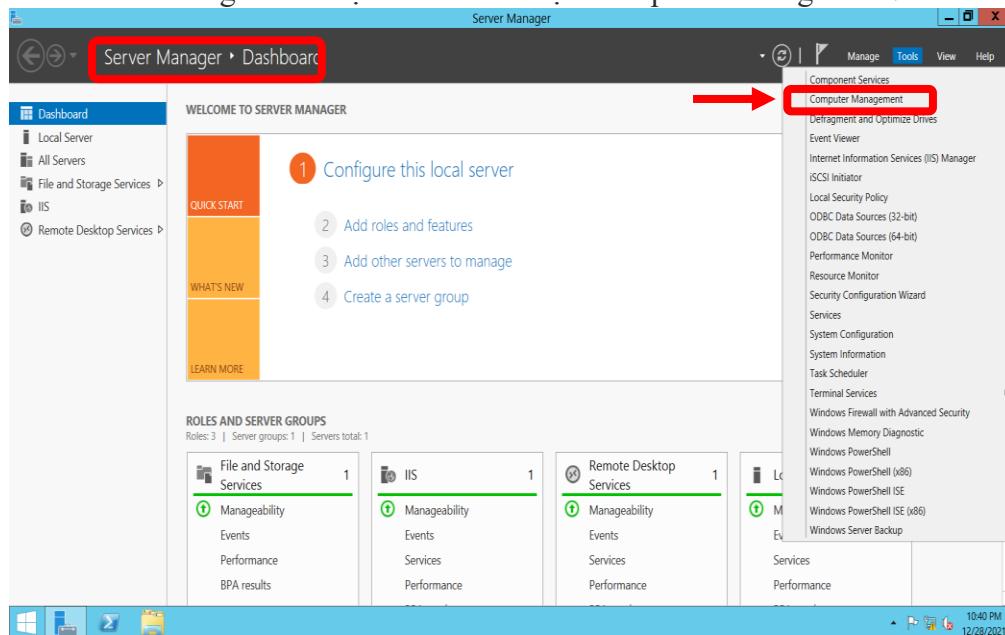
- Đợi cho quá trình cài đặt hoàn thành → chọn **Close** → sau đó khởi động lại máy.



**Hình 1.18: Cửa sổ Installation progress**

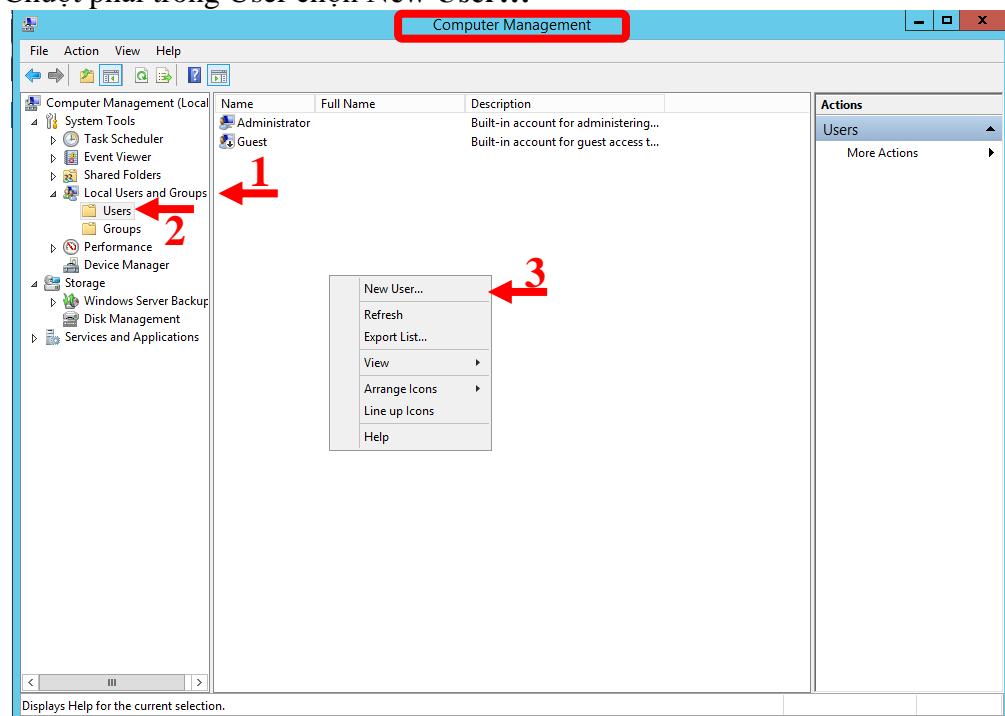
### I.2.3.2. Tạo user và cấp quyền Remote Desktop cho user

- Mở Server Manager → Chọn Tools → Chọn Computer Management.



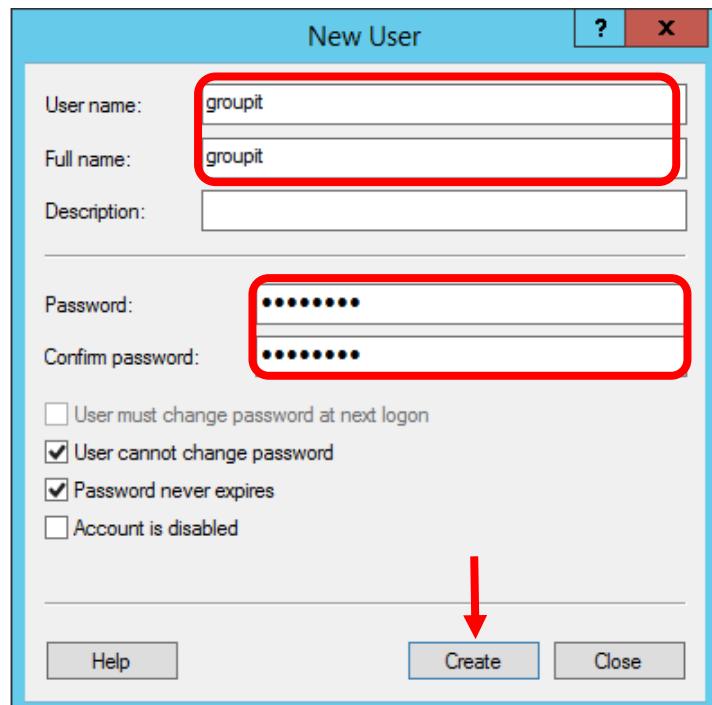
Hình 1.19: Cửa sổ Server Manager

- Tại cửa sổ Computer Management → Chọn Local User and Groups → Chọn User
- Chuột phải trong User chọn New User...



Hình 1.20: Cửa sổ Computer Management

- Trong New User → Nhập User name, Full name, tạo Password ở đây mình đặt User name là **groupit**, password là **@user100** → Nhập lại password → Chọn **Create**.



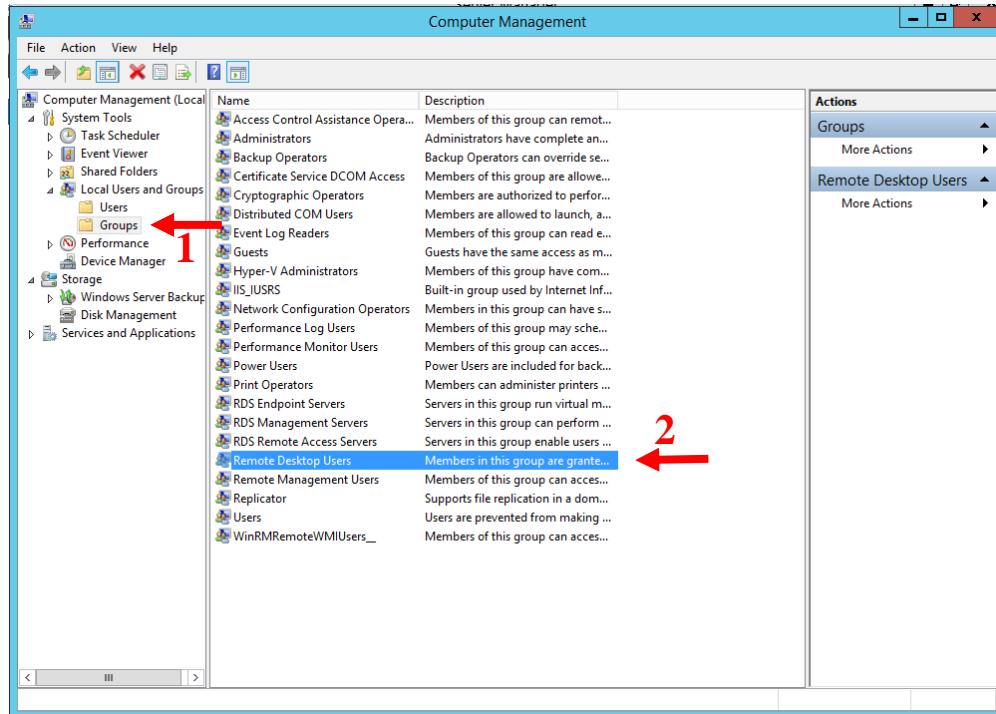
Hình 1.21: Cửa sổ New User

- Khi tạo User thành công sẽ hiển thị giống **Hình 1.22**

Computer Management			
File	Action	View	Help
Computer Management (Local)	Name	Full Name	Description
System Tools	Administrator	groupit	Built-in account for administering...
Task Scheduler	groupit	groupit	
Event Viewer			
Shared Folders			
Local Users and Groups	Users		Built-in account for guest access t...
Groups			
Performance			
Device Manager			
Storage			
Windows Server Backup			
Disk Management			
Services and Applications			
Actions			
Users			
More Actions ▾			

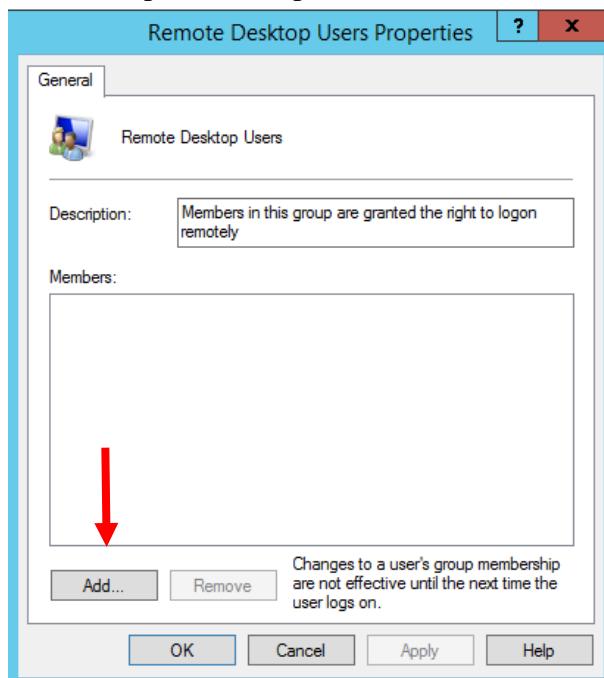
Hình 1.22: Cửa sổ Computer Management

- Tiếp tục vào cửa sổ **Groups** → Chọn **Remote Desktop User**



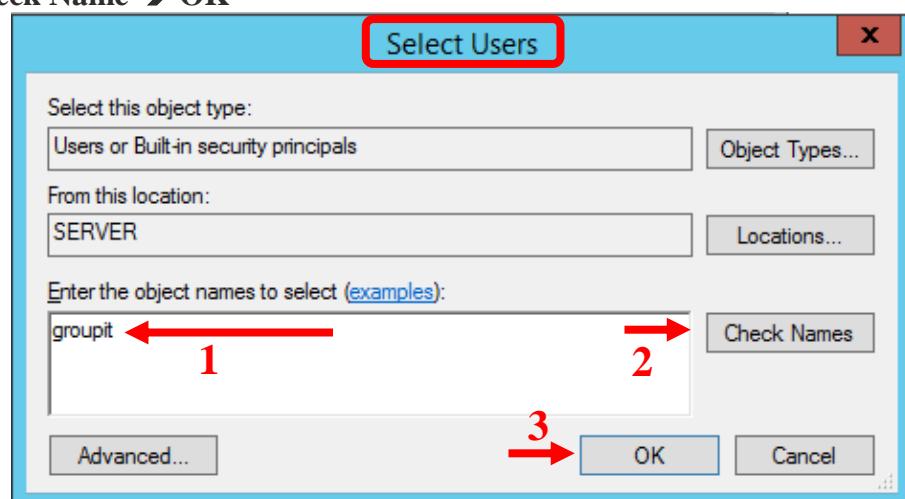
Hình 1.23: Cửa sổ Computer Management

- Tại cửa sổ Remote Desktop Users Properties → Chọn **Add...**



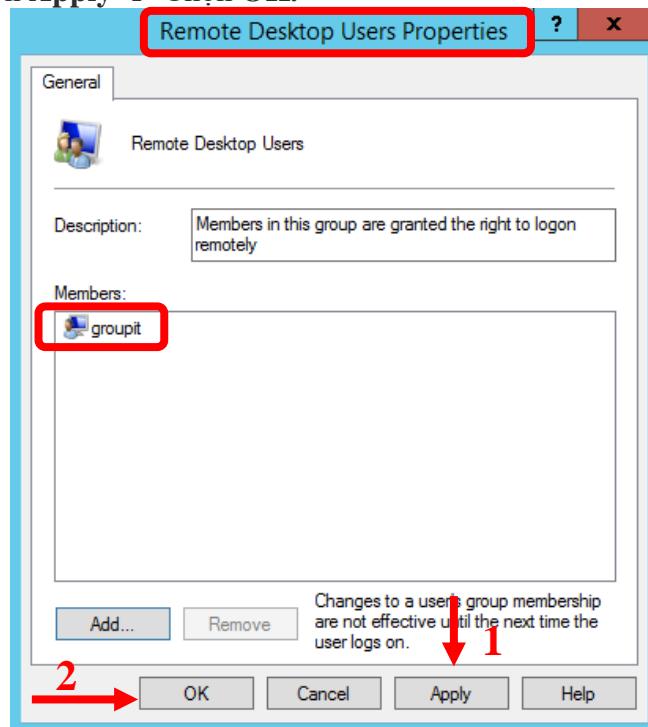
Hình 1.24: Cửa sổ Remote Desktop User Properties

- Cửa sổ Select User được mở → Nhập User name đã được tạo ở cửa sổ User → Chọn Check Name → OK



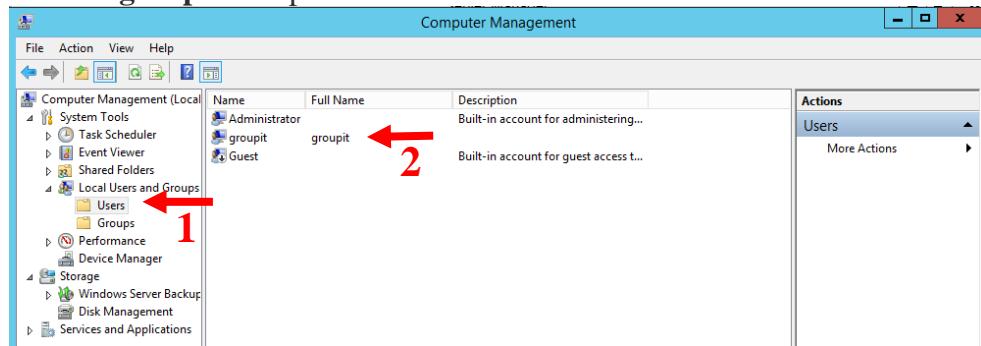
Hình 1.25: Cửa sổ Select Users

- Tại cửa sổ Remote Desktop Users Properties → Thấy User groupit đã được Add vào group → Chọn Apply → Chọn OK.



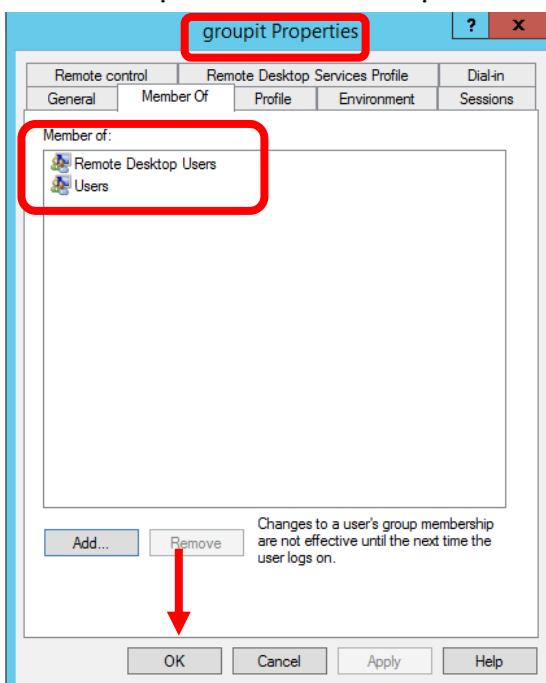
Hình 1.26: Cửa sổ Remote Desktop User Properties

- Kiểm tra → User → Ở user groupit → Chuột phải Properties → Vào cửa sổ groupit Properties.



Hình 1.27: Cửa sổ Computer Management

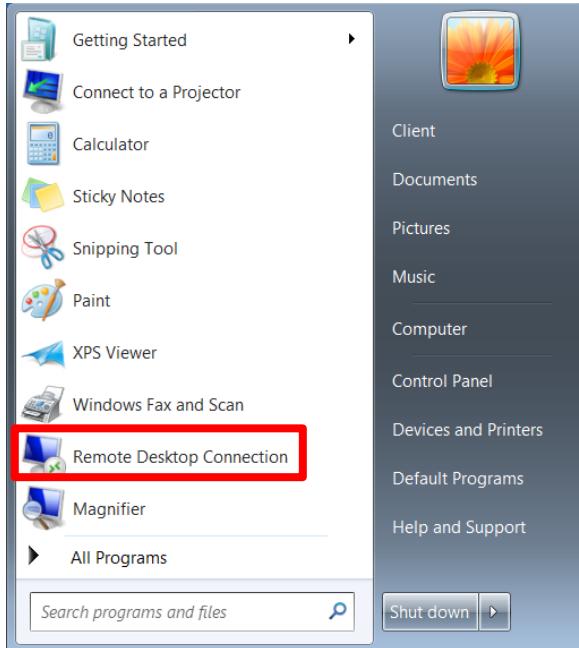
- Trong tab Member Of hiển thị ở hình bên dưới chọn OK.



Hình 1.28: Cửa sổ groupit Properties

### I.2.3.3. Client kết nối vào Terminal Server bằng Remote Desktop Connection

- Tại máy **Client** Log on Administrator
- Vào Start ➔ Ở khung tìm kiếm nhập **Remote Desktop Connection** ➔ truy cập vào **Remote Desktop Connection** ta được **Hình 1.29**:



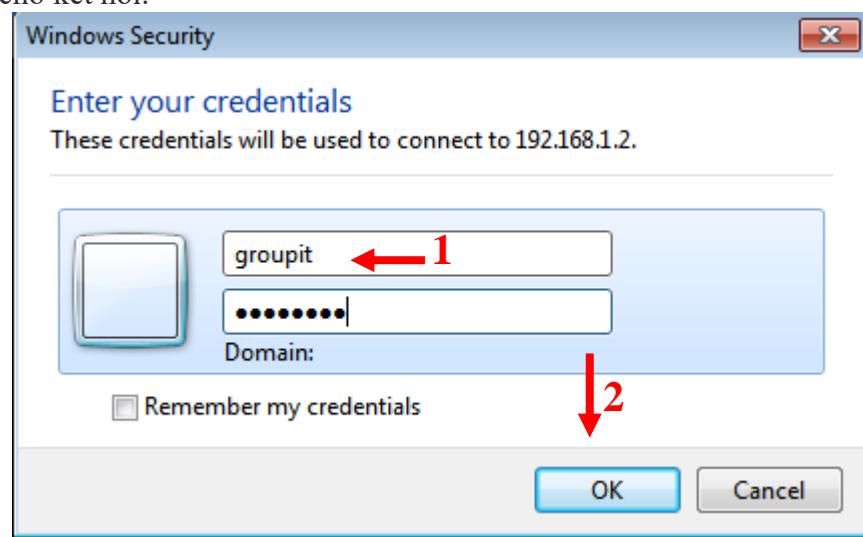
**Hình 1.29: Cửa sổ Start Client**

- Ở Remote Desktop connection nhập địa chỉ IP của máy **Server** sao đó để thực hiện kết nối chọn **Connect**.



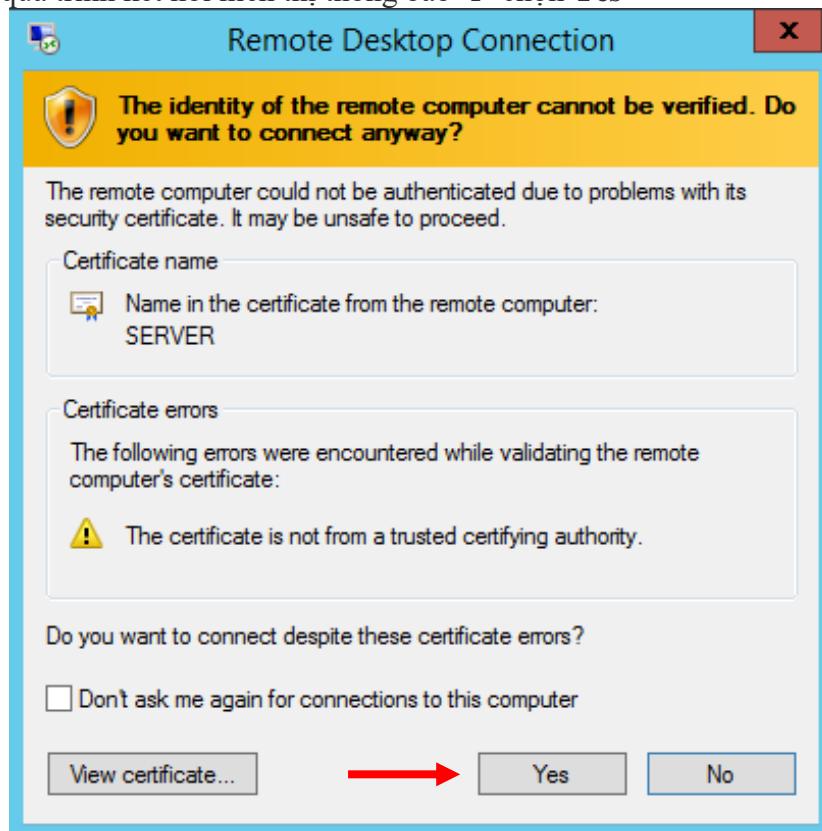
**Hình 1.30: Cửa sổ Remote Desktop Connection**

- Tại cửa sổ Windows Security nhập User Name và Password đã đặt ở Server ➔ Chọn OK, chờ kết nối.



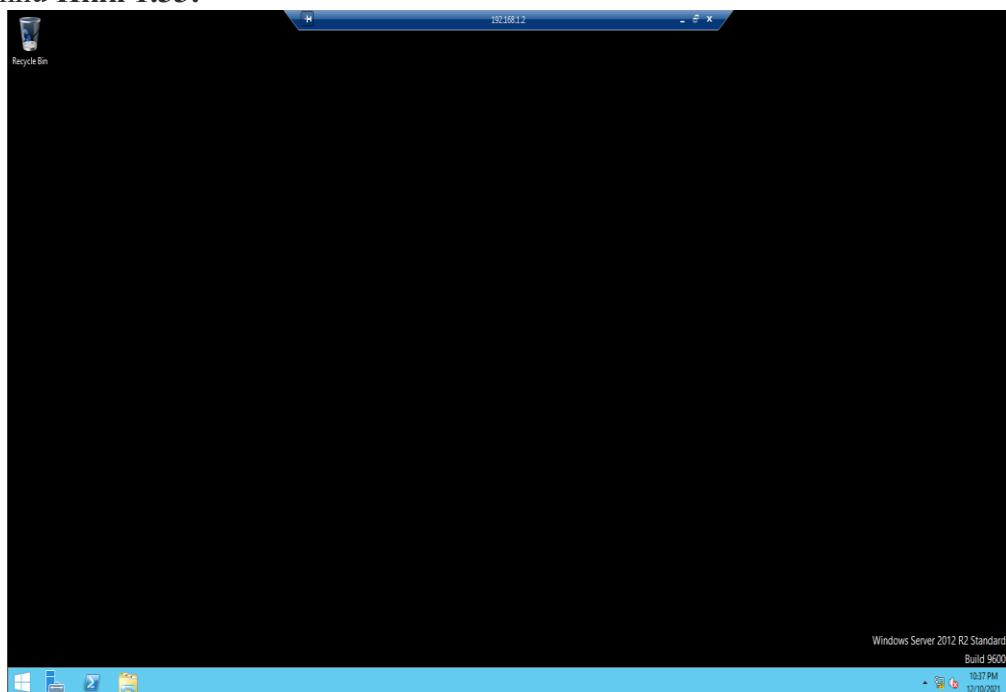
Hình 1.31: Cửa sổ Windows Security

- Trong quá trình kết nối hiển thị thông báo ➔ chọn Yes



Hình 1.32: Cửa sổ Remote Desktop Connection

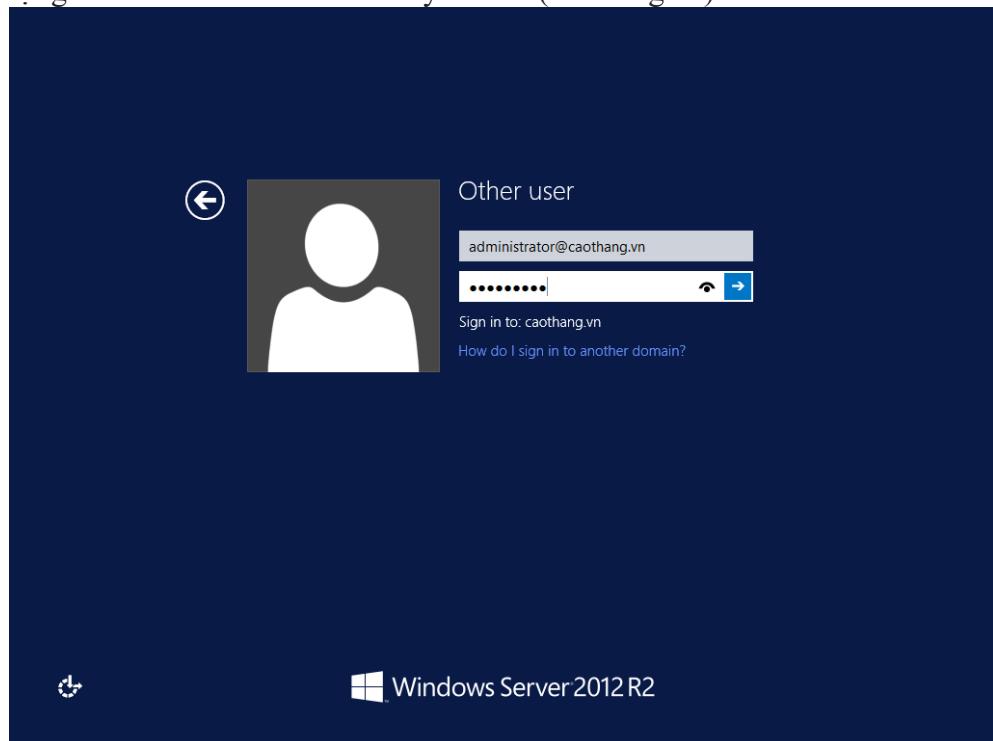
- Nếu thành công máy Client sẽ kết nối với máy Server và nhận được Desktop của Server như **Hình 1.33:**



**Hình 1.33: Cửa sổ Client kết nối windows Server**

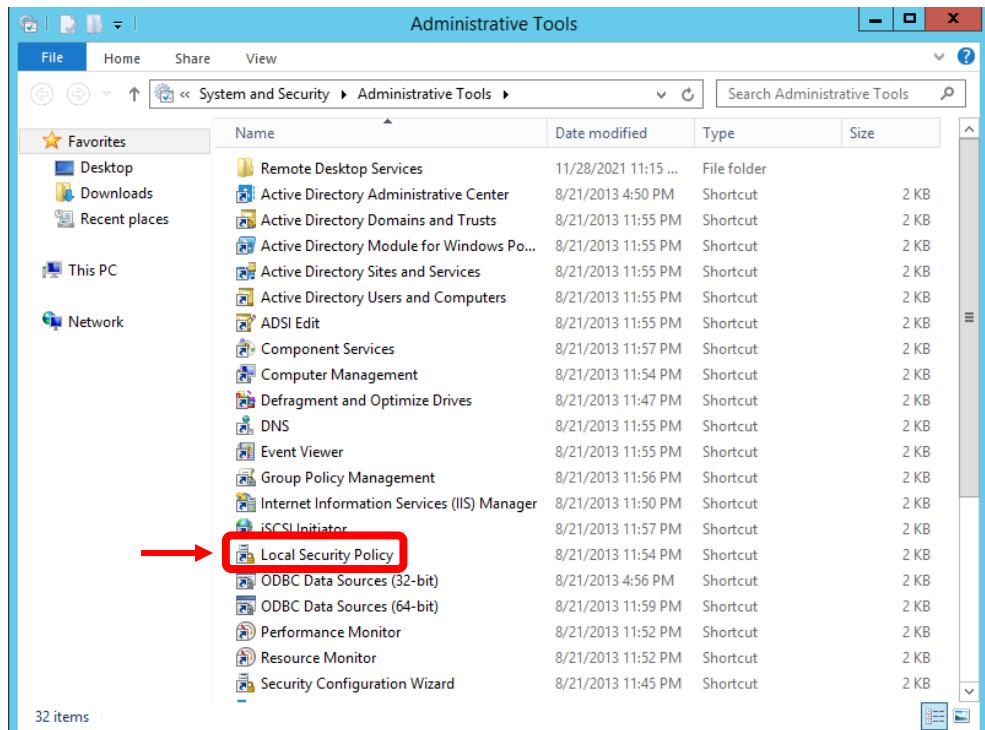
#### I.2.3.4. Client kết nối vào Terminal Server bằng Web Access

- Dùng Domain Controller trên máy Server (caothang.vn)



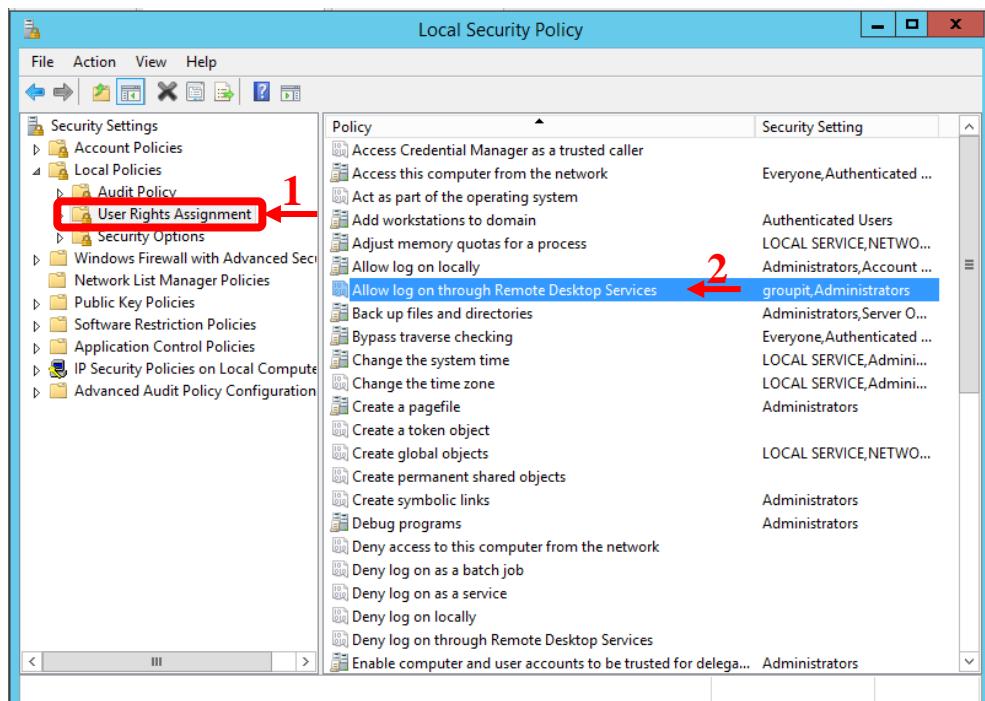
**Hình 1.34: Cửa sổ windows Server**

- Vào Local Security Policy trong Administrative Tools



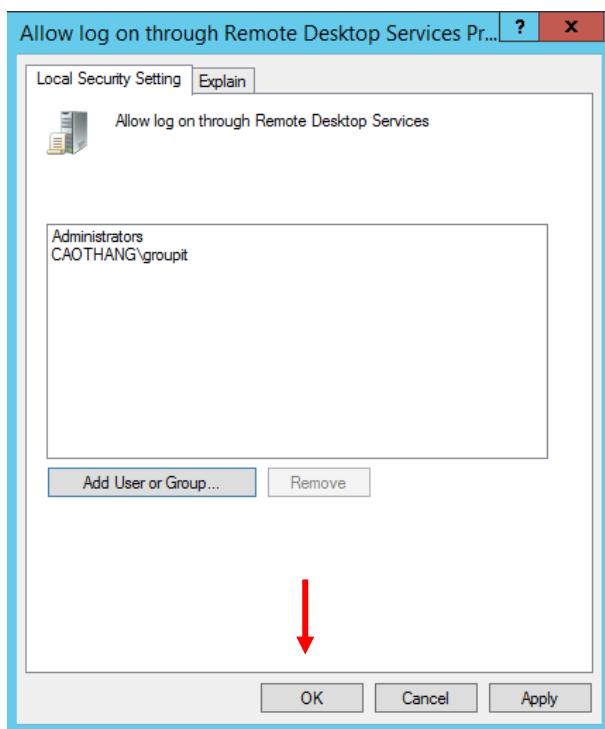
Hình 1.35: Cửa sổ Administrative Tools

- Bung Local Policies, chọn User Rights Assignment
- Chuột phải vào Allow log on through Remote Desktop Services, chọn Properties



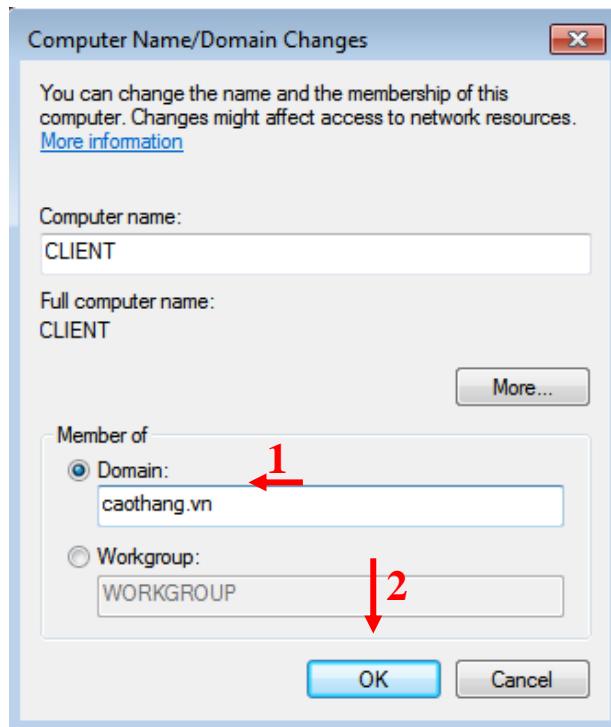
Hình 1.36: Cửa sổ Local Security Policy

- Add groupit và chọn OK



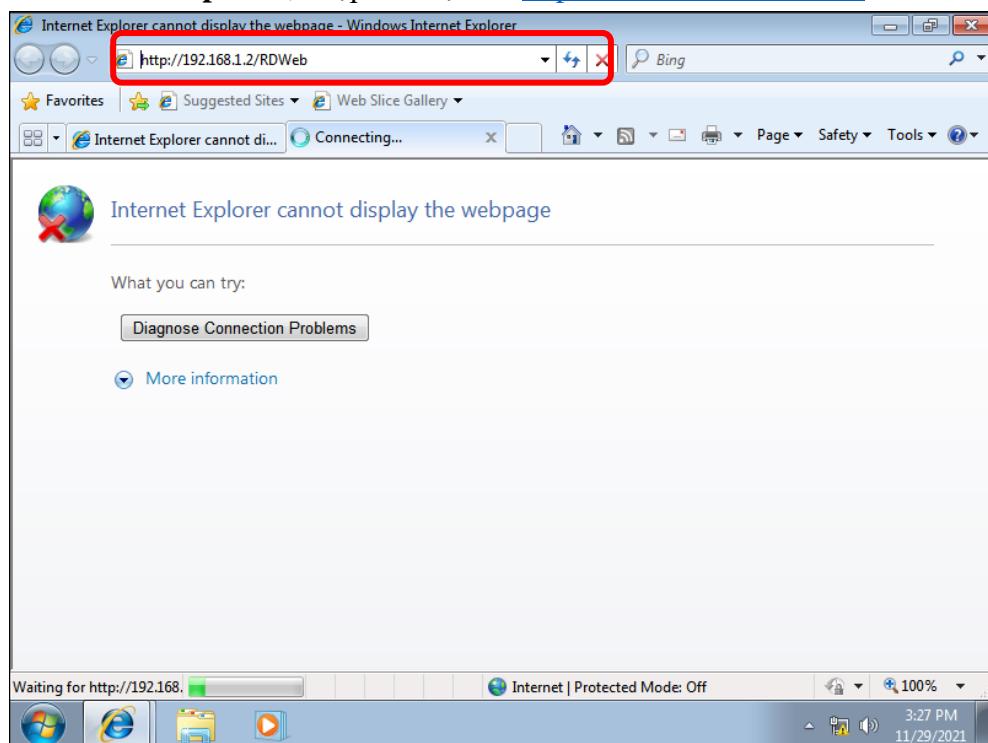
Hình 1.37: Tap Local Security Setting

- Truy cập máy Client **Join domain** vào Server → Restart lại máy Client



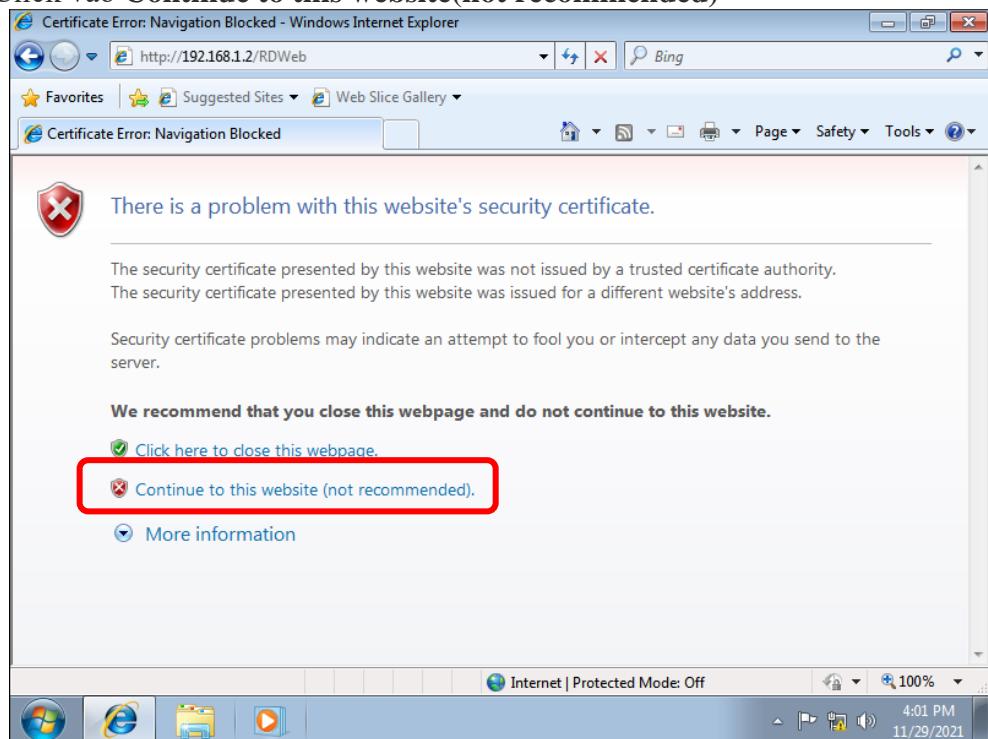
Hình 1.38: Cửa sổ Computer Name/Domain Changes

- Tại máy Client
- Mở Internet Explorer, nhập vào địa chỉ <http://192.168.1.2/RDWeb>



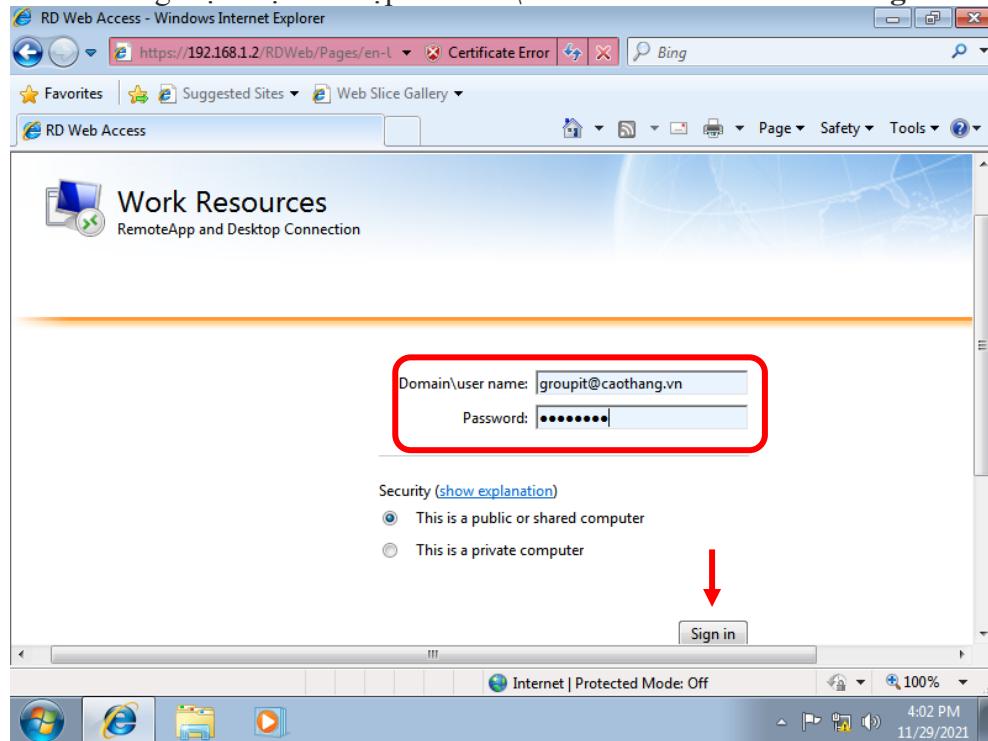
Hình 1.39: Cửa sổ Windows Internet Explorer

- Click vào Continue to this website(not recommended)



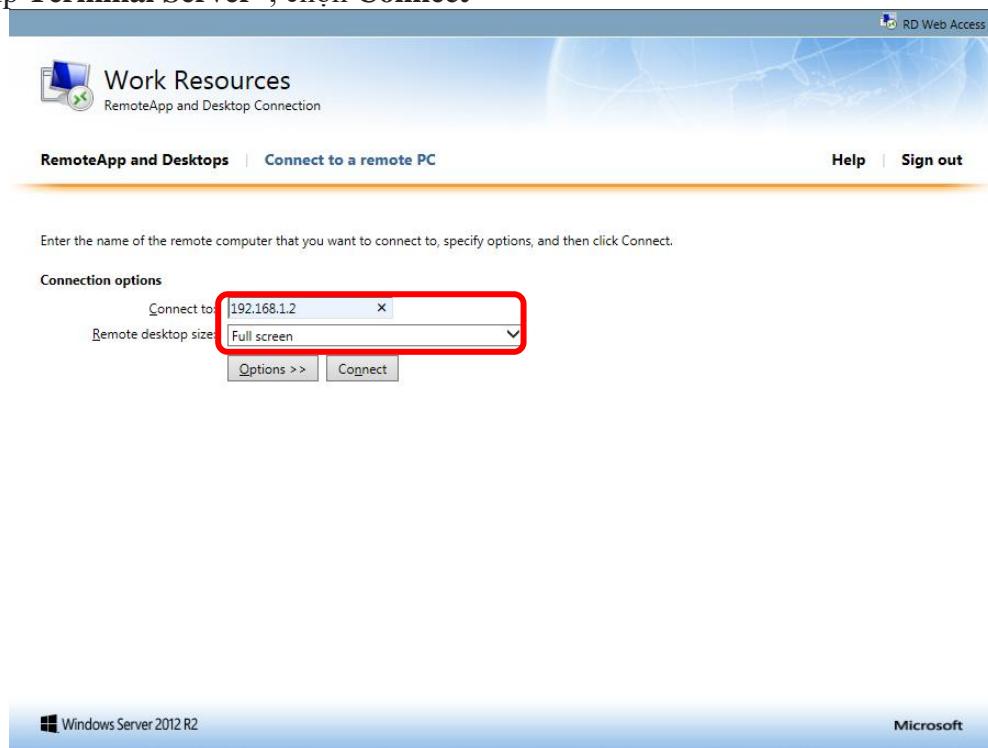
Hình 1.40: Cửa sổ Windows Internet Explorer

- Cửa sổ chứng thực hiện ra nhập Domain\username và Password → Sign in



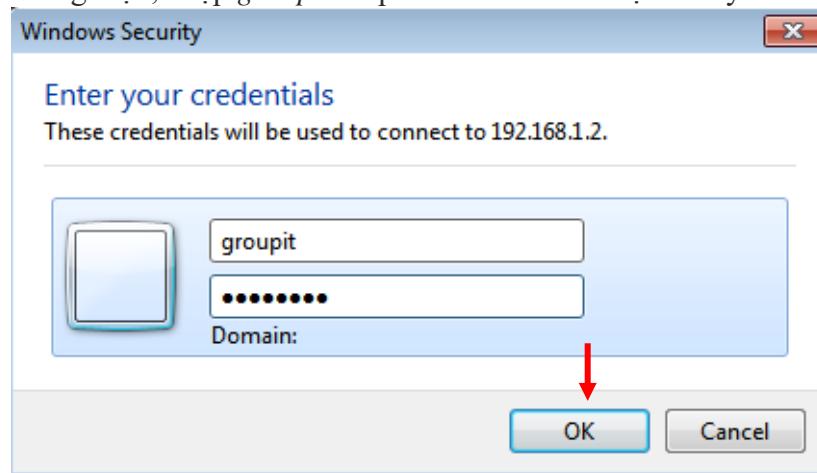
Hình 1.41: Tab RD Web Access

- Trong cửa sổ **RD Web Access**, vào tab **Connect to a remote PC**, nhập vào địa chỉ ip **Terminal Server**, chọn **Connect**



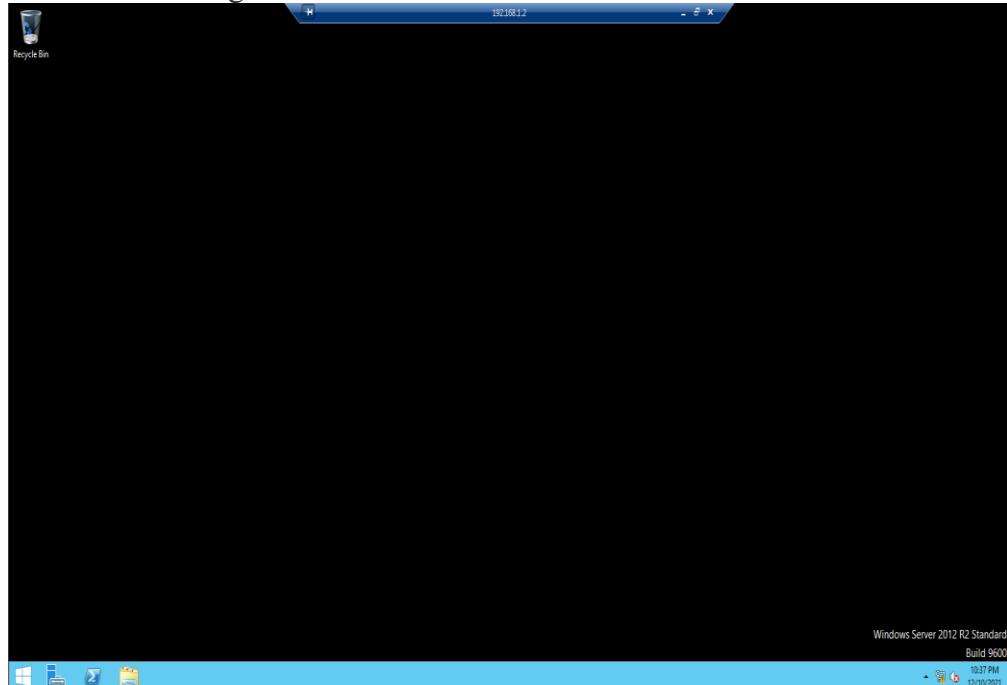
Hình 1.42: Tap RemoteApp and Desktops

- Cửa sổ chứng thực, nhập groupit và password và ta đã đặt ở máy Server → OK



Hình 1.43: Cửa sổ Windows Security

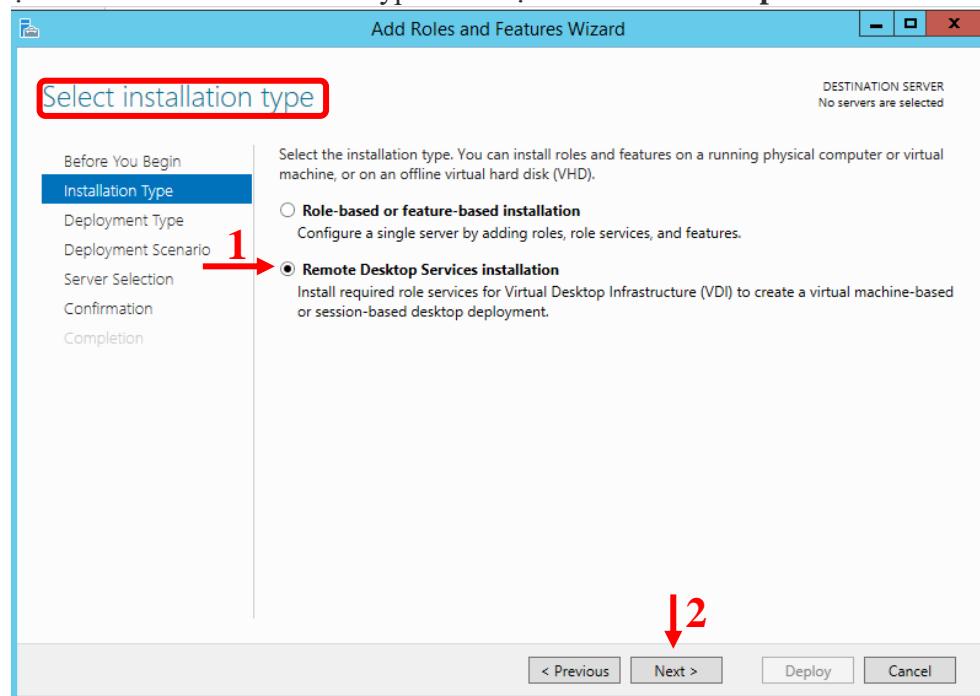
- Kết nối thành công



Hình 1.44: Cửa sổ Client kết nối Desktop Window Server

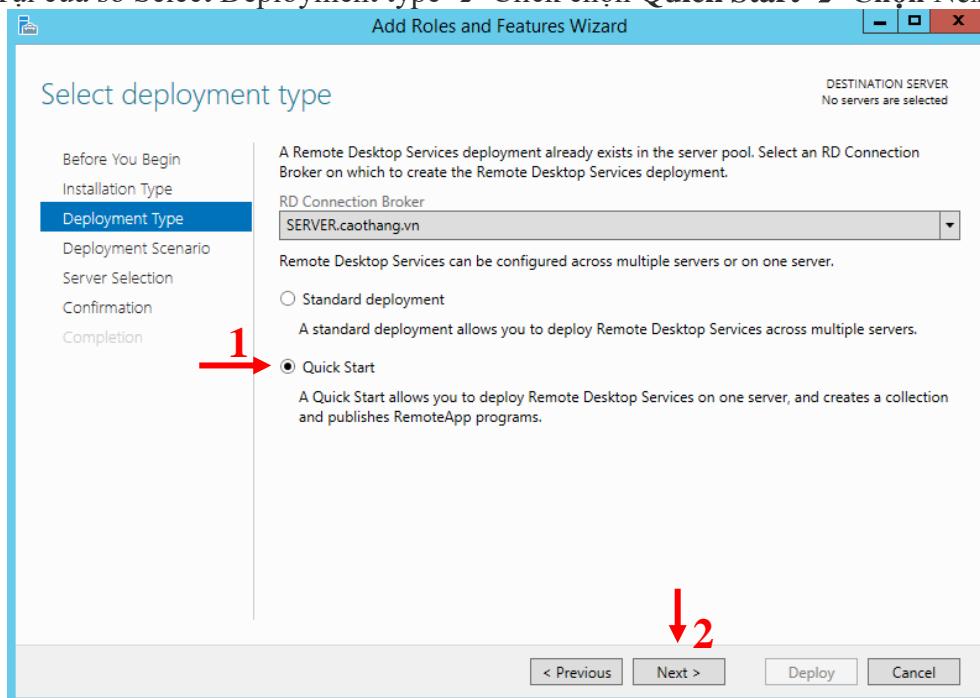
### I.2.3.5. Cấu hình Remote Application

- Tại máy Server → Chọn Server Manager
- Tại Server Manager → Chọn Manage → Chọn Add Roles and Features.
- Tại cửa sổ Select installation type → Chọn **Remote Desktop Services installation**



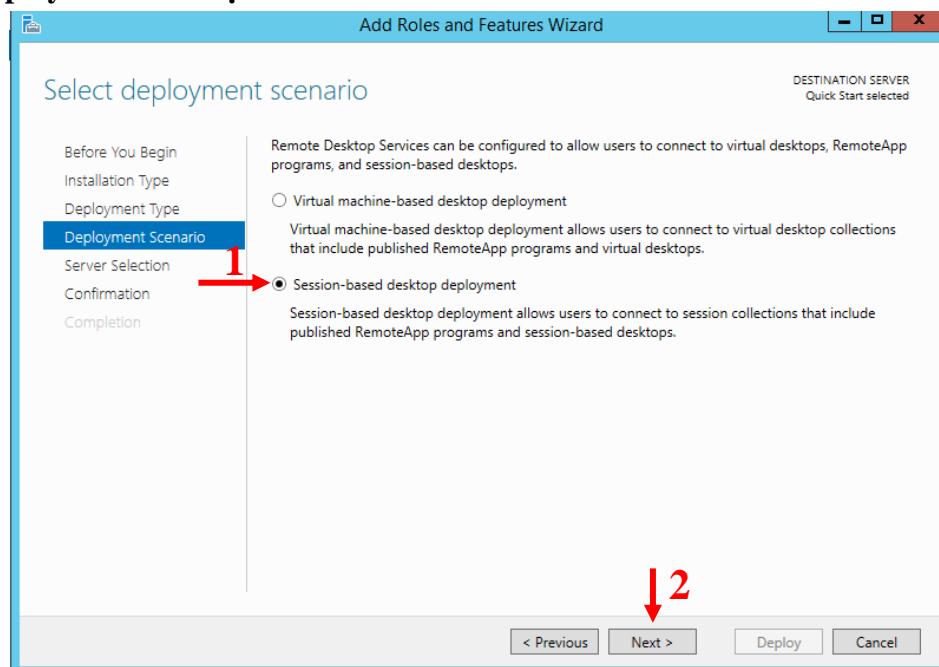
Hình 1.45: Cửa sổ Select installation type

- Tại cửa sổ Select Deployment type → Click chọn **Quick Start** → Chọn Next >



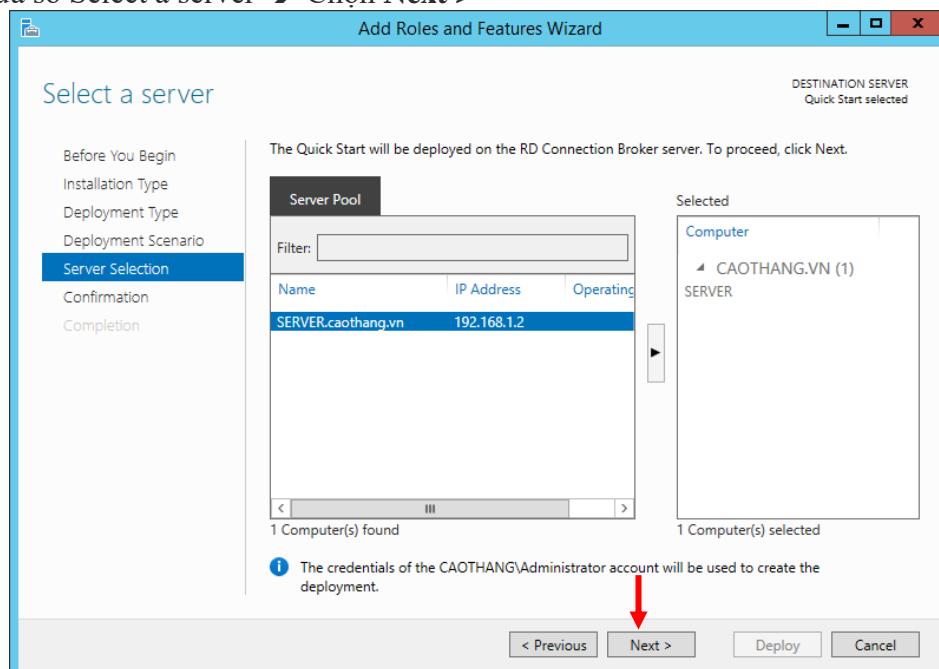
Hình 1.46: Cửa sổ Select deployment type

- Tại cửa sổ Select deployment scenario → Click chọn **Session-based desktop deployment** → Chọn Next >



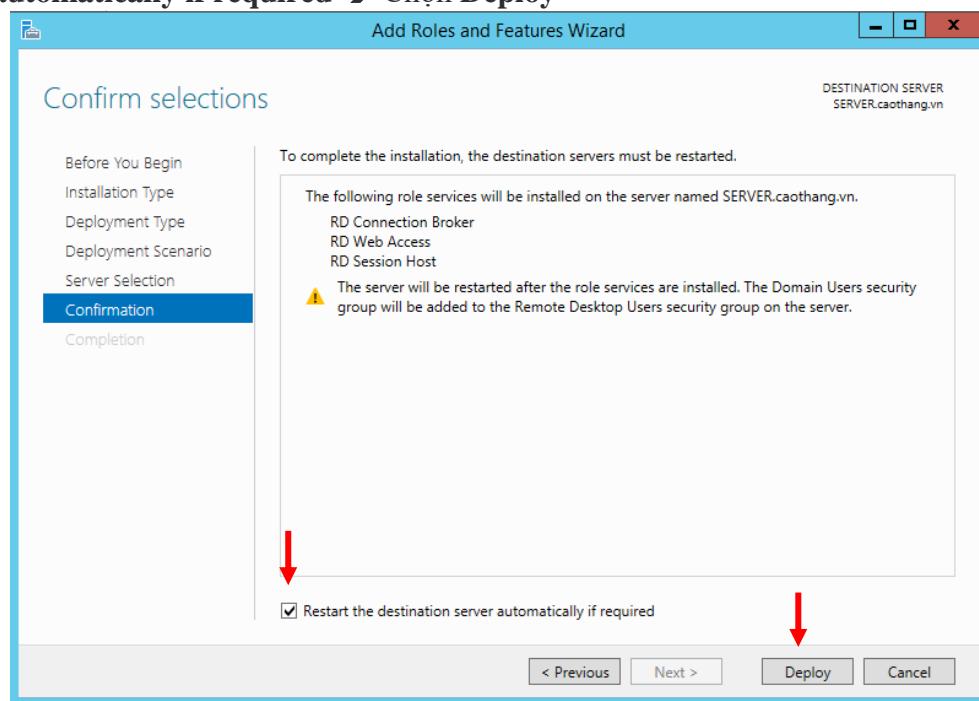
Hình 1.47: Cửa sổ Select deployment scenario

- Cửa sổ Select a server → Chọn Next >



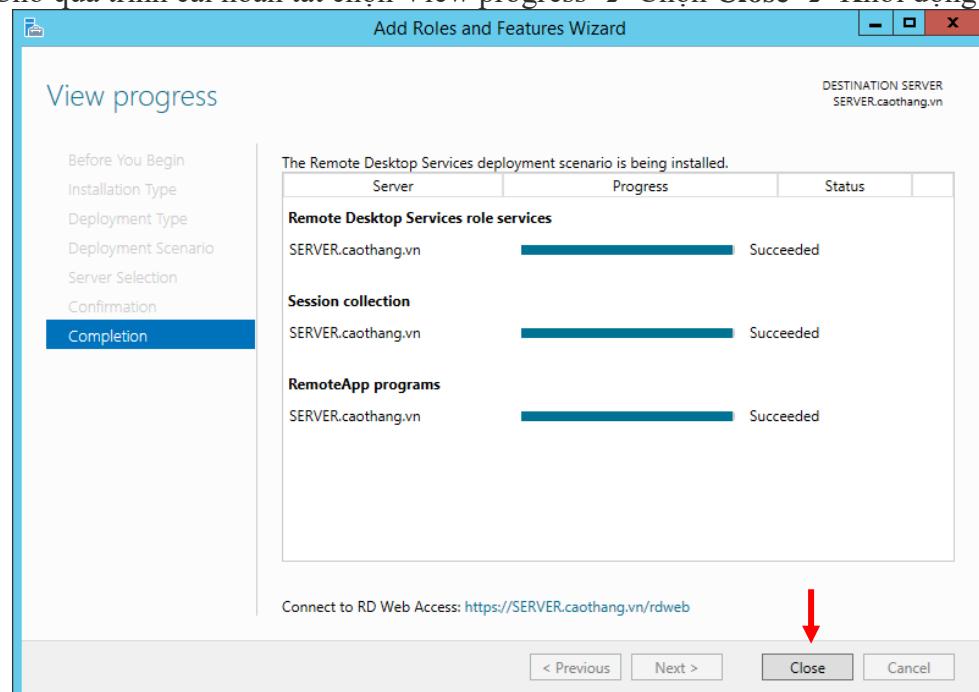
Hình 1.48: Cửa sổ Select a server

- Cửa sổ **Confirm selections** → click chọn **Restart the destination server automatically if required** → Chọn **Deploy**



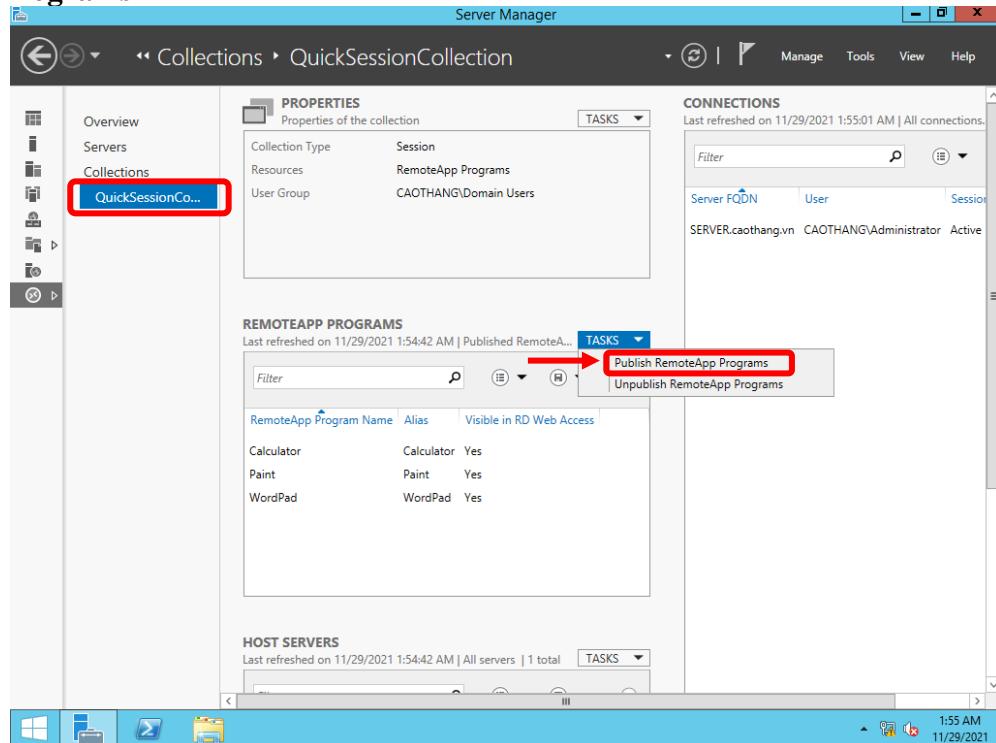
Hình 1.49: Cửa sổ Confirmation selections

- Chờ quá trình cài hoàn tất chọn **View progress** → Chọn **Close** → Khởi động lại máy



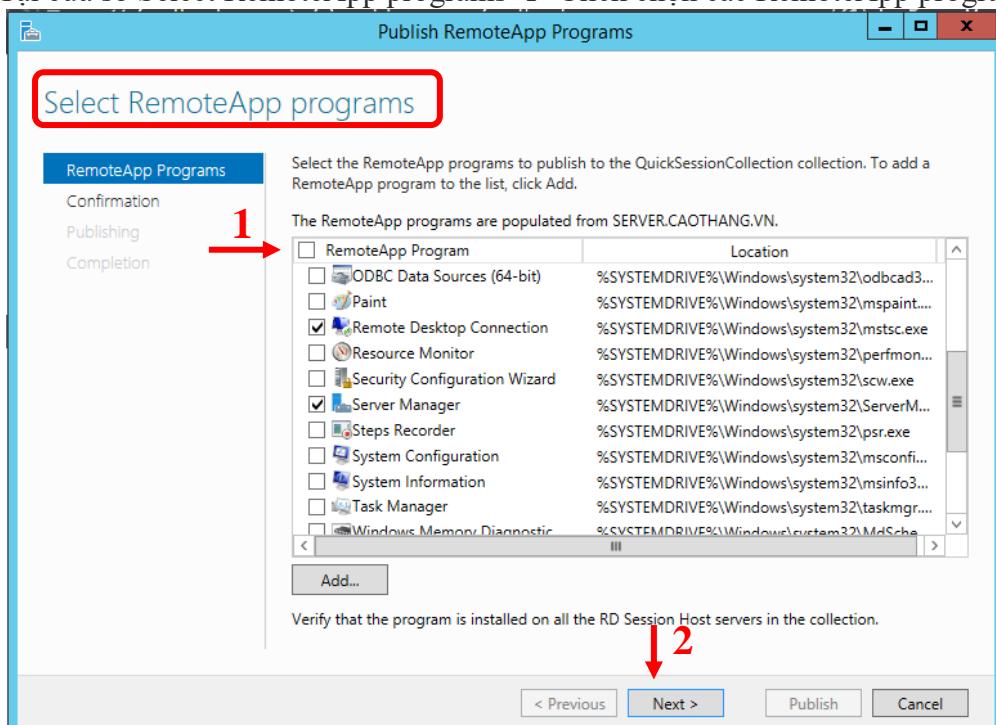
Hình 1.50: Cửa sổ View progress

- Tại Server Manager → Chọn Remote Desktop Services → Chọn QuickSessionCollection trong Tap Collections
- Trong QuickSessionCollection → Bung mục TASKS → Chọn Publish RemoteApp Programs



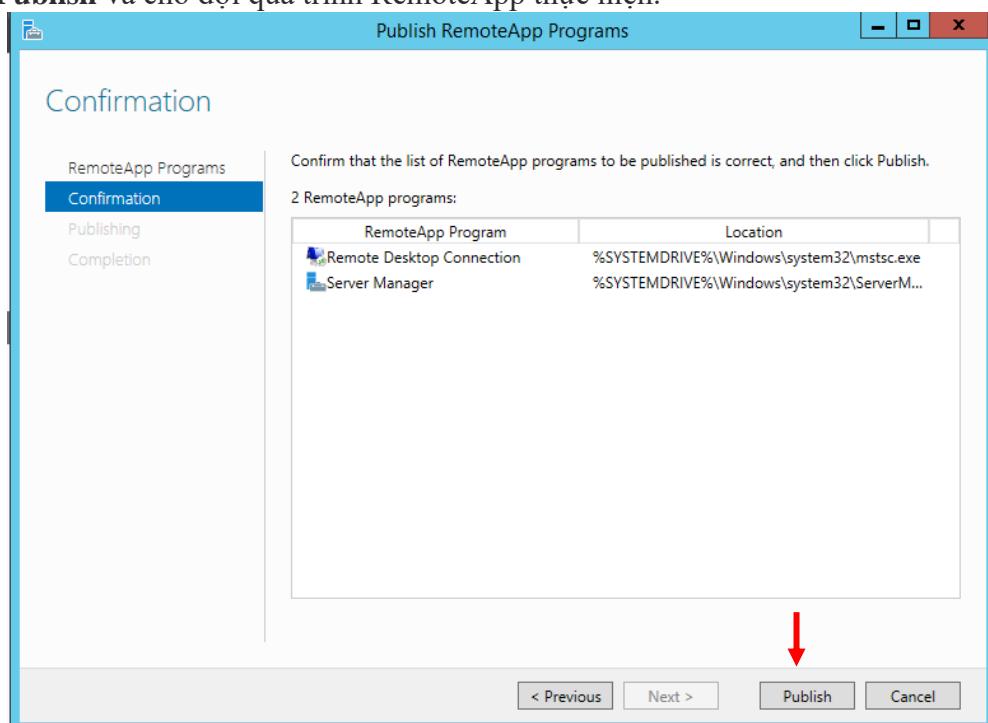
Hình 1.51: Cửa sổ QuickSessionCollection

- Tại cửa sổ Select RemoteApp programs → Click chọn các RemoteApp programs



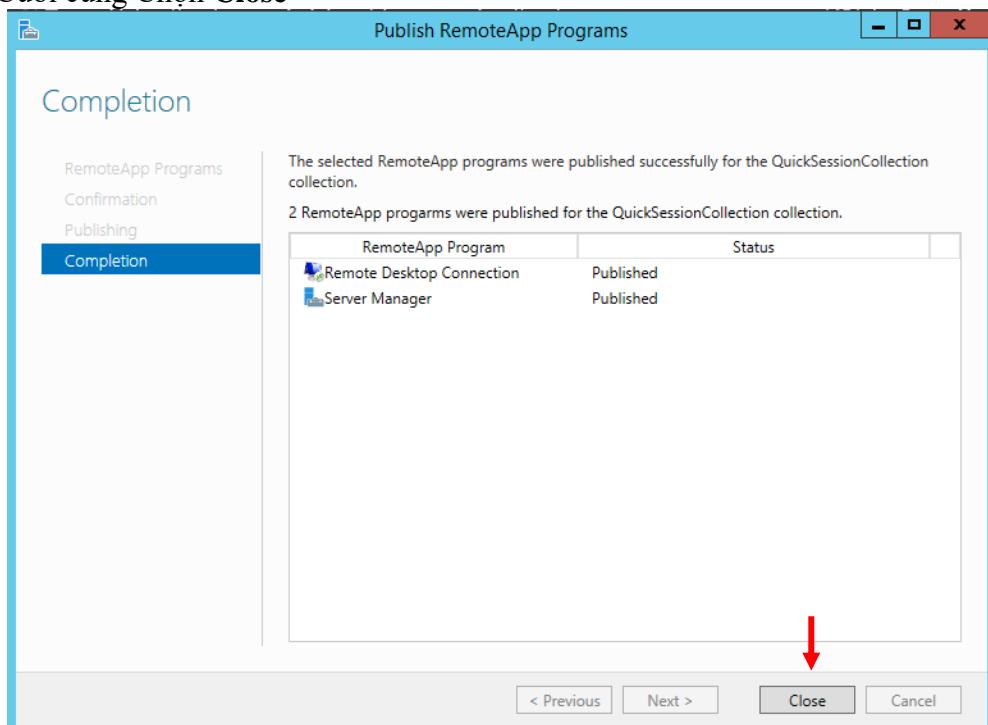
Hình 1.52: Cửa sổ Select RemoteApp

- Tại Cửa sổ Confirmation xác nhận các RemoteApp Program đã chọn → Chọn **Publish** và chờ đợi quá trình RemoteApp thực hiện.



Hình 1.53: Cửa sổ Confirmation

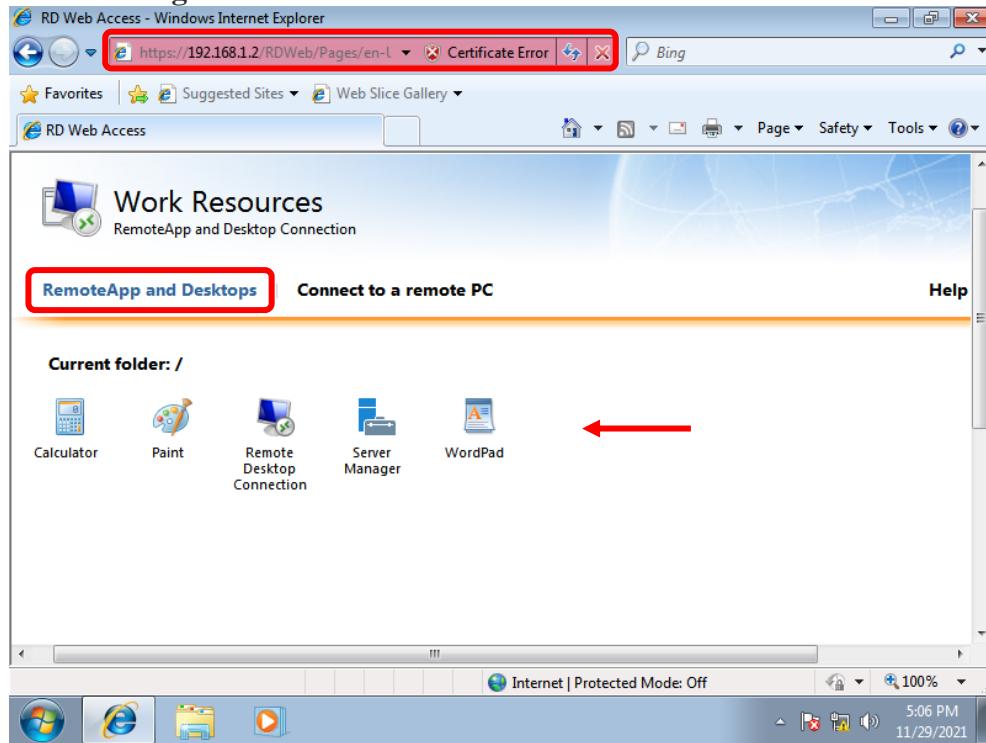
- Cuối cùng Chọn **Close**



Hình 1.54: Cửa sổ Completion

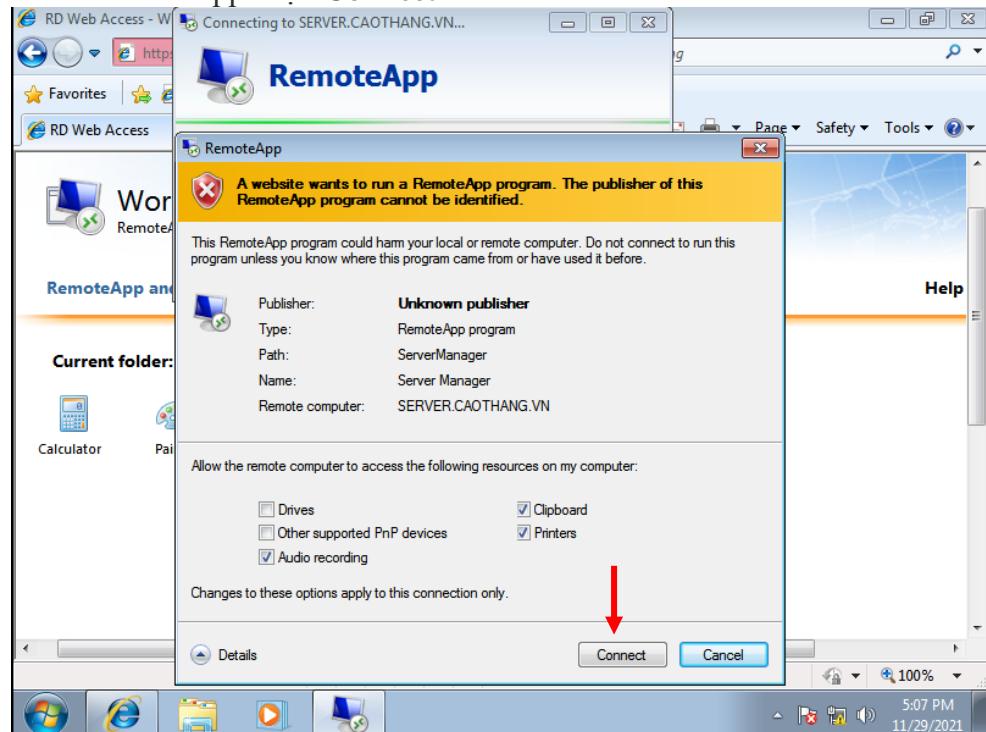
### I.2.3.6. Client kết nối Remote Application

- Tại máy Client mở **Internet Explorer**, truy cập vào địa chỉ <http://192.168.1.2/RDWeb>
- Cửa sổ chứng thực nhập username : *groupit* và passwork
- Cửa sổ RD Web Access → Chọn Tab **RemoteApp and Desktops** → Ở đây Chọn **Server Manager** → Connect.



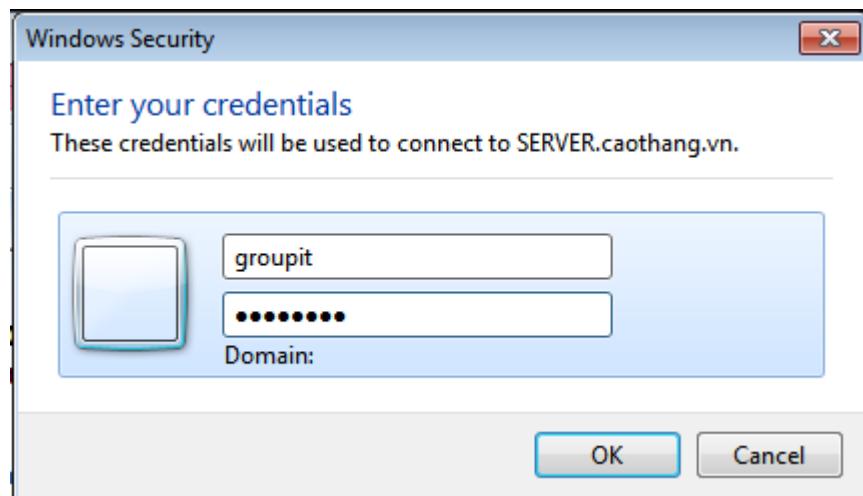
Hình 1.55: Cửa sổ RD Web

- Cửa sổ RemoteApp chọn **Connect**



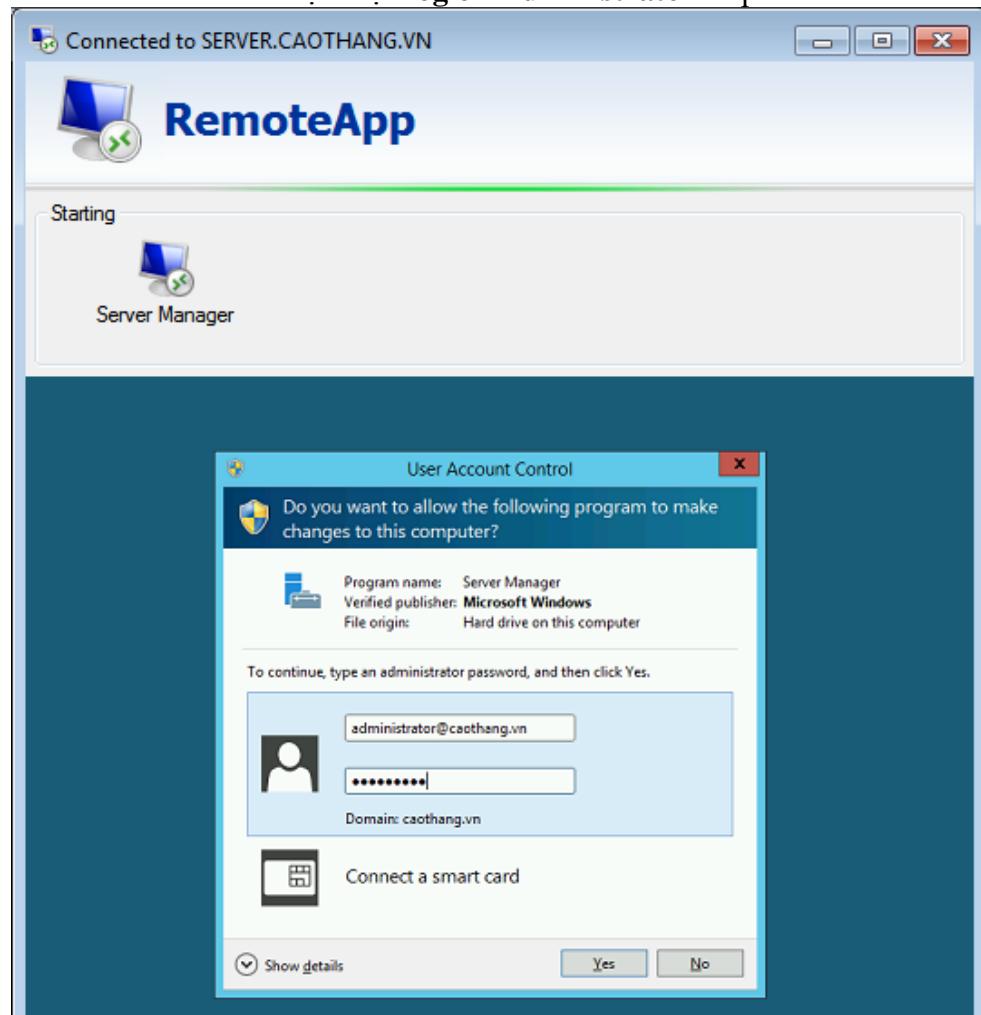
Hình 1.56: Cửa sổ RemoteApp

- Tại cửa sổ Windows Security, nhập *groupit* và passwork đã tạo trên máy Server



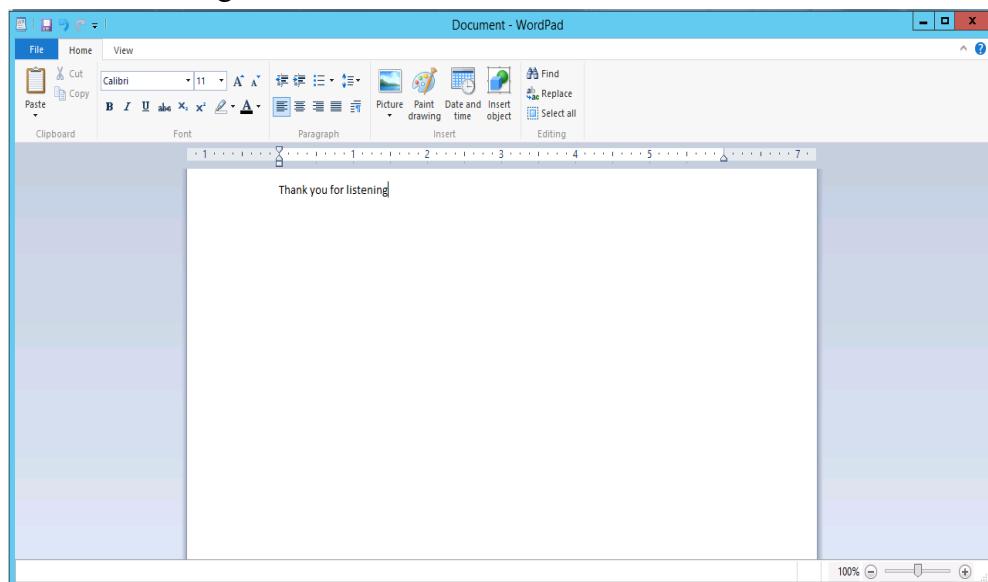
Hình 1.57: Cửa sổ Windows Security

- Để kết nối đến Server thực hiện **log on Administrator** và passwork



Hình 1.58: Cửa sổ User Account Control

- Kết nối thành công.



Hình 1.59: Cửa sổ Client kết nối App program trên server

## CHƯƠNG 2: VIRTUAL PRIVATE NETWORK

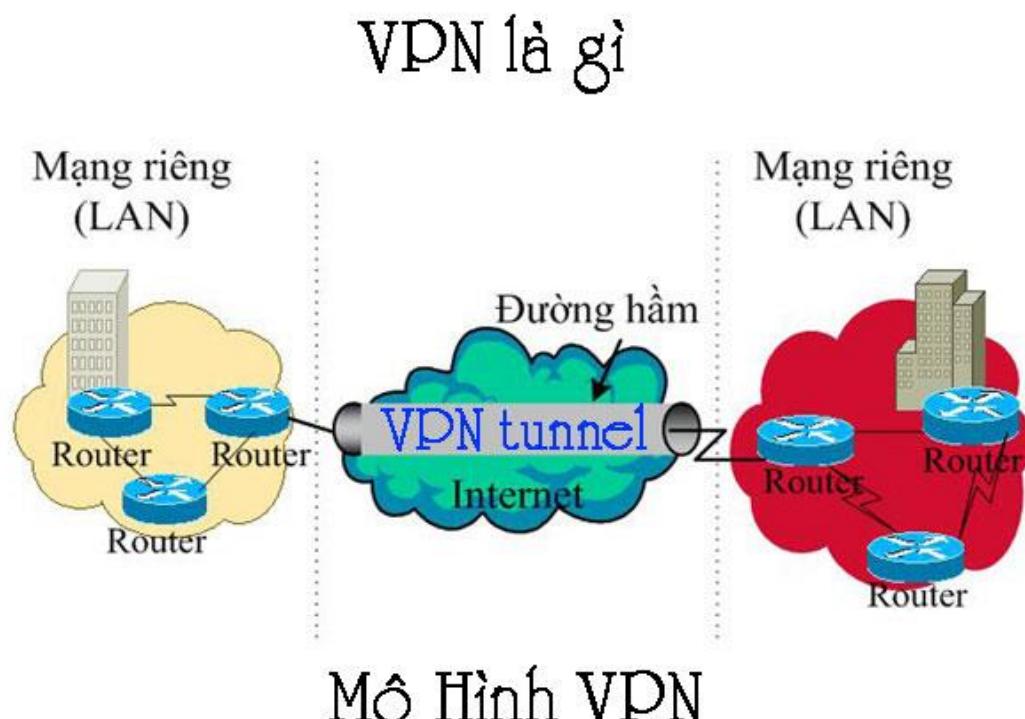
### II. VIRTUAL PRIVATE NETWORK (VPN)

#### II.1. Giới thiệu virtual private network

VPN viết tắt của Virtual Private Network (mạng riêng ảo) cho phép bạn tạo ra những kết nối tới liên kết mạng khác một cách an toàn thông qua Internet.

Về căn bản, mỗi VPN là một mạng riêng rẽ sử dụng một hạ tầng chung (Internet) để kết nối cùng với các site (mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng kết nối thực mỗi VPN sử dụng các kết nối ảo được thiết lập qua Internet từ mạng riêng của các Công ty tới các chi nhánh hay các nhân viên từ xa.

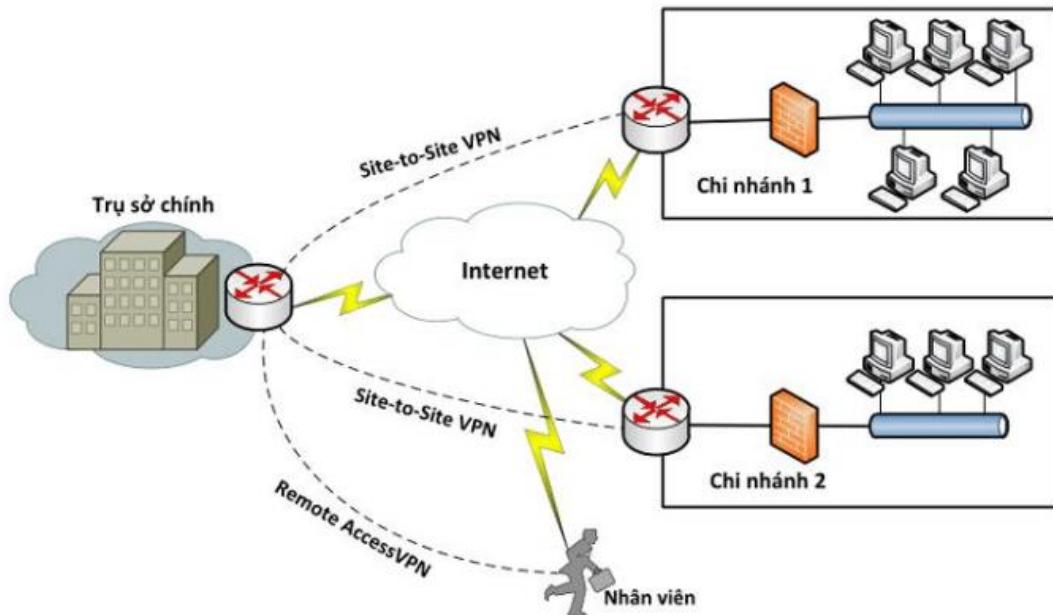
Để có thể gửi và nhận dữ liệu thông qua mạng công cộng mà vẫn đảm bảo tính an toàn và bảo mật, VPN cung cấp các cơ chế mã hóa dữ liệu trên đường truyền tại ra một đường ống (tunnel) bảo mật giữa nơi gửi và nơi nhận. Để tạo ra một đường ống bảo mật đó, dữ liệu phải được mã hóa, chỉ cung cấp phần đầu gói dữ liệu là có thể đi đến đích thông qua mạng công cộng một cách nhanh chóng.



Hình 2.1: Mô Hình VPN

### II.1.1. VPN hoạt động như thế nào?

Khi kết nối máy tính của bạn hoặc các thiết bị thông minh với VPN, máy tính sẽ hoạt động như thể kết nối cục bộ như VPN. Tất cả các lưu lượng mạng sẽ được gửi thông qua một kết nối an toàn.



**Hình 2.2: Mô hình hoạt động của VPN**

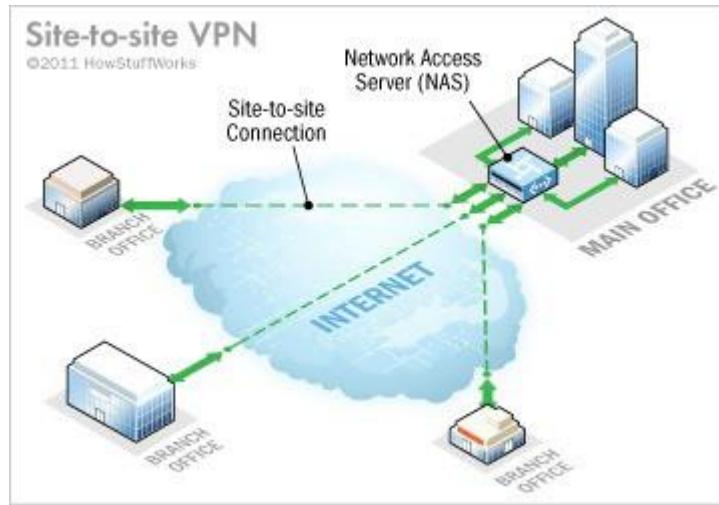
Máy tính của bạn hoạt động trên hệ thống mạng VPN, điều này cho phép bạn truy cập nguồn tài nguyên mạng cục bộ ngay cả khi bạn đang ở cách xa nhau từ châu lục này sang châu lục kia. Ngoài ra bạn cũng có thể sử dụng Internet giống như bạn đang ở tại vị trí mà bạn đang kết nối VPN tới. Đây cũng là lợi ích trong một vài trường hợp khi vị trí của bạn đang bị hạn chế về kết nối tới địa chỉ website hoặc ứng dụng mà bạn muốn truy cập đến thì VPN sẽ giải quyết được vấn đề này.

### II.1.2. Phân loại VPN

- ❖ Công nghệ VPN có thể được phân thành 2 loại cơ bản: Site-to-Site VPN và Remote Access VPN.

➤ **Site-to-Site VPN:** là mô hình dùng để kết nối các hệ thống mạng ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất. Ở loại kết nối này thì việc chứng thực ban đầu phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi đặt nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site.

Kết nối Site – to – Site VPN được thiết kế để tạo một kết nối mạng trực tiếp, hiệu quả bất chấp khoảng cách vật lý giữa chúng. Có thể kết nối này luôn chuyển thông qua Internet hoặc một mạng không được tin cậy. Phải đảm bảo ván đề bảo mật bằng cách sử dụng sự mã hóa dữ liệu trên tất cả các gói dữ liệu đang luân chuyển giữa các mạng đó.



Hình 2.3: Mô hình Site-to-site VPN

Site – to – Site VPN được chia làm hai loại nhỏ là VPN Intranet và VPN Extranet.

- **Intranet VPN:** Kết nối văn phòng trung tâm, các chi nhánh và văn phòng ở xa vào mạng nội bộ của công ty dựa trên hạ tầng mạng được chia sẻ.
- **Extranet VPN:** Kết nối bộ phận khách hàng của công ty, bộ phận tư vấn, hoặc các đối tác của công ty thành một hệ thống mạng dựa trên hạ tầng được chia sẻ. Extranet VPN khác nhau với Intranet VPN ở chỗ cho phép các user ngoài công ty truy cập và hệ thống.

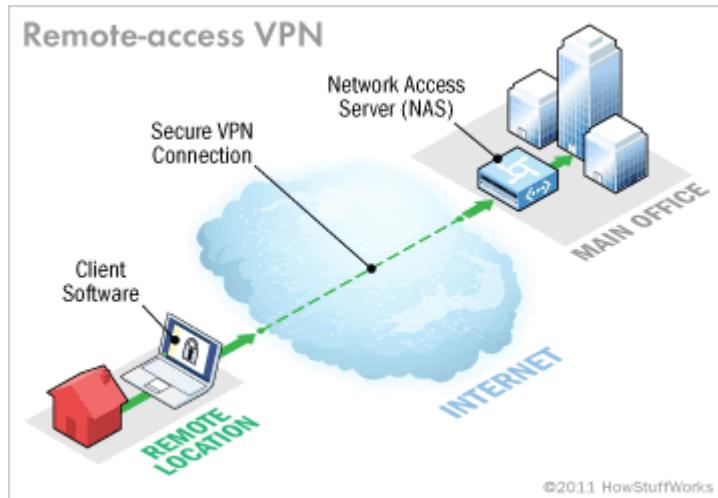
➤ **Remote Access VPN ( VPN client to site):** cho phép truy cập bất cứ lúc nào bằng Remote, mobile, và các thiết bị truyền thông của nhân viên các chi nhánh kết nối đến tài nguyên mạng của tổ chức.

Remote Access VPN mô tả việc các người dùng ở xa sử dụng các phần mềm VPN để truy cập vào mạng Intranet của công ty thông qua gateway hoặc VPN concentrator (bản chất là một server). Vì lý do này, giải pháp này thường được gọi là client/server. Trong giải pháp này, các người dùng thường sử dụng các công nghệ WAN truyền thống để tạo lại các tunnel về mạng HO của họ.

Loại này thường áp dụng cho nhân viên làm việc lưu động hay làm việc ở nhà muốn kết nối vào mạng công ty một cách an toàn. Cũng có thể áp dụng cho văn phòng nhỏ ở xa kết nối vào Văn phòng trung tâm của công ty.

Remote Access VPN còn được xem như là dạng User-to-LAN, cho phép người dùng ở xa dùng phần mềm VPN Client kết nối với VPN Server.

Một hướng phát triển khá mới trong remote access VPN là dùng wireless VPN, trong đó một nhân viên có thể truy cập về mạng của họ thông qua kết nối không dây. Trong thiết kế này, các kết nối không dây cần phải kết nối về một trạm wireless (wireless terminal) và sau đó về mạng của công ty. Trong cả hai trường hợp, phần mềm client trên máy PC đều cho phép khởi tạo các kết nối bảo mật, còn được gọi là tunnel.

**Hình 2.4: Mô hình Remote-accessVPN**

### II.1.3. Phương thức hoạt động của VPN

Hầu hết các VPN đều dựa vào kỹ thuật gọi là Tunneling để tạo ra một mạng riêng trên nền Internet. Về bản chất, đây là quá trình đặt toàn bộ gói tin vào trong một lớp header (tiêu đề) chứa thông tin định tuyến có thể truyền qua hệ thống mạng trung gian theo những “đường ống” riêng (tunnel).

Khi gói tin được truyền đến đích, chúng được tách lớp header và chuyển đến các trạm cuối cùng cần nhận dữ liệu. Để thiết lập kết nối Tunnel, máy khách và máy chủ phải sử dụng chung một giao thức (tunnel protocol).

Giao thức của gói tin bọc ngoài được cả mạng và hai điểm đầu cuối nhận biết. Hai điểm đầu cuối này được gọi là giao diện Tunnel (tunnel interface), nơi gói tin đi vào và đi ra trong mạng.

Để bảo mật các dữ liệu trong hệ thống VPN, có 1 vài giao thức – Protocol phổ biến được áp dụng trong các mô hình VPN như sau :

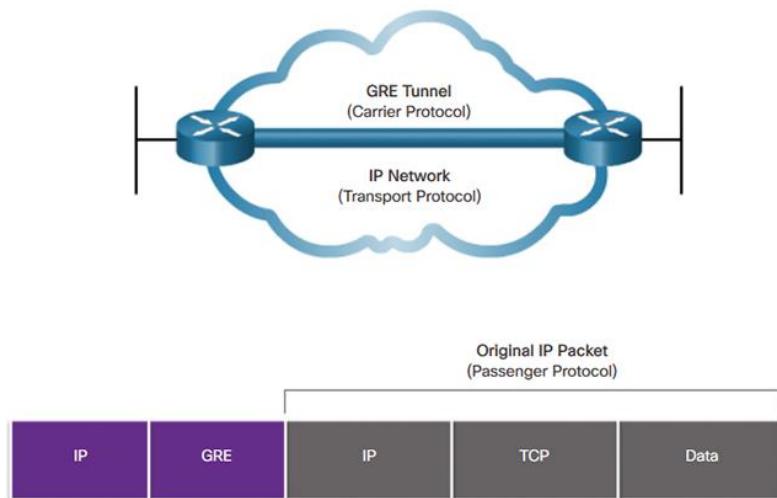
#### c.1. GRE (Generic Route Encapsulation)

Đây là đa giao thức truyền thông đóng gói IP, CLNP và tất cả cá gói dữ liệu bên trong đường ống IP (IP tunnel).

Với GRE Tunnel, Cisco router sẽ đóng gói cho mỗi vị trí một giao thức đặc trưng chỉ định trong gói IP header, tạo một đường kết nối ảo (virtual point-to-point) tới Cisco router cần đến. Và khi gói dữ liệu đến đích IP header sẽ được mở ra.

Bằng việc kết nối nhiều mạng con với các giao thức khác nhau trong môi trường có một giao thức chính. GRE tunneling cho phép các giao thức khác có thể thuận lợi trong việc định tuyến cho gói IP.

Khi thực hiện đóng gói, mặc định GRE thêm vào một overhead 24 byte gồm 20 byte IP header và 4 byte GRE header.

**Hình 2.5: Kỹ thuật GRE tunnel**c.2. L2F (Layer 2 Forward)

Là giao thức lớp 2 được phát triển bởi Cisco System. L2F được thiết kế cho phép tạo đường hầm giữa NAS và một thiết bị VPN Gateway để truyền các Frame, người sử dụng từ xa có thể kết nối đến NAS và truyền Frame PPP từ remote user đến VPN Gateway trong đường hầm được tạo ra.

c.3. L2TP (Layer 2 Tunneling Protocol)

là sản phẩm của sự hợp tác giữa các thành viên PPTP Forum, Cisco và IETF. Kết hợp các tính năng của cả PPTP và L2F, L2TP cũng hỗ trợ đầy đủ IPSec. L2TP có thể được sử dụng làm giao thức Tunneling cho mạng VPN điểm-nối-điểm và VPN truy cập từ xa. Trên thực tế, L2TP có thể tạo ra một tunnel giữa máy khách và router. NAS và router, router và router. So với PPTP (Point to Point Tunneling Protocol) thì L2TP có nhiều đặc tính mạng và an toàn hơn.

c.4. PPTP (Point to point Tunneling Protocol)

là giao thức kết nối điểm – điểm , đây là phương pháp cấu hình đơn giản nhất của VPN , độ bảo mật kém nhất . Ưu điểm của giao thức này là dễ cấu hình , client kết nối nhanh đến server .PPTP là sự mở rộng của giao thức Internet chuẩn Point-to-Point (PPP) và sử dụng cùng kiểu xác thực như PPP (PAP, SPAP, CHAP, MS-CHAP, EAP). Là phương pháp VPN được hỗ trợ rộng rãi nhất giữa các máy trạm chạy Windows. PPTP thiết lập đường hầm (tunnel) nhưng không mã hóa. Ưu điểm khi sử dụng PPTP là nó không yêu cầu hạ tầng mã khóa công cộng (Public Key Infrastructure).

c.5. SSTP(Secure Socket Tunneling Protocol)

là một dạng của kết nối VPN bằng HTTPS sử dụng Port 443 , SSTP sử dụng các kết nối HTTP đã được mã hóa SSL để thiết lập một kết nối VPN đến VPN gateway. SSTP là một giao thức rất an toàn vì các thông tin quan trọng của người dùng không được gửi cho tới khi có một “đường hầm” SSL an toàn được thiết lập với VPN gateway. SSTP cũng được biết đến với tư cách là PPP trên SSL, chính vì thế nó cũng có nghĩa là

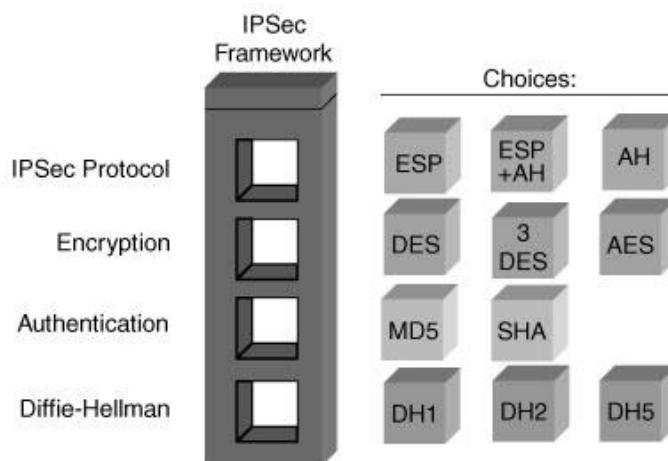
bạn có thể sử dụng các cơ chế chứng thực PPP và EAP để bảo đảm cho các kết nối SSTP được an toàn hơn.

#### c.6. IPSec (Internet Protocol Security)

IP Security (viết tắt là IP Sec) là một framework cho phép sử dụng nhiều phương pháp bảo mật khác nhau để bảo vệ các gói tin IP khi chúng phải đi qua một môi trường mạng công cộng không an toàn.

#### **IPSec cung cấp các dịch vụ sau trong việc bảo vệ dữ liệu:**

- Mã hóa dữ liệu (data confidentiality): dữ liệu sẽ được mã hóa bởi các thuật toán mã hóa tin cậy để tránh việc bị đọc trộm hoặc đánh cắp nội dung trên đường di chuyển.
- Toàn vẹn dữ liệu (data integrity): dữ liệu sẽ được bảo vệ chống lại việc bị thay đổi nội dung trên đường đi.
- Xác thực dữ liệu (data authentication): dữ liệu sẽ được xác thực nguồn gốc khi nhận được tại phía nhận để đảm bảo rằng dữ liệu này đến từ đúng thiết bị gửi mong muốn.



Hình 2.6: - Sơ đồ khung IP Sec

Từ trên hình trên có thể thấy:

- Giao thức IP Sec được sử dụng có thể là ESP hoặc AH hoặc kết hợp cả hai giao thức này.
- Kỹ thuật mã hóa dữ liệu (encryption) được sử dụng có thể là DES, 3DES hay AES.
- Kỹ thuật xác thực được sử dụng có thể là MD5 hoặc SHA.
- Phương pháp trao đổi và phát sinh các key mã hóa/xác thực có thể là thuật toán DH1, DH2 hoặc DH5.

#### **II.1.4. Lợi ích của VPN**

Mặc dù là công cụ khá đơn giản, nhưng VPN lại có khá nhiều lợi ích:

- **Truy cập Business Network trong khi đi du lịch:** VPN thường được các du khách đi du lịch với mục đích kinh doanh (business traveler) sử dụng để truy cập mạng lưới kinh doanh của họ, bao gồm tất cả các nguồn tài nguyên mạng cục bộ. Các nguồn tài nguyên mạng cục bộ không được tiếp xúc trực tiếp với Internet để tăng cường tính bảo mật.

- **Truy cập Home Network trong khi đi du lịch :** Ngoài ra bạn có thể thiết lập một VPN của riêng mình để truy cập khi đi du lịch. Điều này sẽ cho phép bạn truy cập Windows Remote Desktop thông qua Internet, tức là bạn sẽ được phép truy cập vào máy tính cá nhân của mình thông qua Internet, chia sẻ các tập tin, làm việc trên dữ liệu máy tính ở nhà và thậm chí là chơi game trên máy tính đó.
- **Ẩn hoạt động duyệt web từ mạng cục bộ và ISP :** Nếu đang sử dụng kết nối Wifi công cộng, và bạn duyệt web trên các trang web không phải HTTPS, khi đó các hoạt động của bạn sẽ được hiển thị với mọi người (nếu họ biết cách để xem hoạt động của bạn). Nếu muốn ẩn hoạt động duyệt web của mình để đảm bảo tính bảo mật, quyền riêng tư, bạn có thể kết nối với VPN. Mạng cục bộ sẽ chỉ nhìn thấy một kết nối VPN an toàn và duy nhất. Tất cả các traffic khác sẽ thông qua kết nối VPN. Và có thể sử dụng để bỏ qua việc giám sát của nhà cung cấp dịch vụ Internet (ISP) của bạn.
- **Truy cập các trang web bị chặn về mặt địa lý :** Dù cho bạn là công dân sinh sống tại Hoa Kỳ, nhưng bạn đang đi du lịch tại một các quốc gia khác, không phải Hoa Kỳ và bạn muốn truy cập Netflix, Pandora hay Hulu thì điều này là không thể. Tuy nhiên nếu kết nối với một VPN đặt tại Hoa Kỳ thì việc truy cập Netflix, Pandora hay Hulu lại là hoàn toàn có thể.
- **Sử dụng VPN để bỏ qua kiểm duyệt Internet .**
- **Tải các file :** Nhiều người dùng sử dụng kết nối VPN để tải các file thông qua BitTorrent. Điều này thực sự hữu ích nếu bạn muốn tải toàn bộ Torrent hợp lệ - nếu ISP của bạn đang điều khiển BitTorrent và nó khá chậm, bạn có thể sử dụng BitTorrent trên VPN để được trải nghiệm tốc độ nhanh hơn.

## II.1.5. Ưu điểm và hạn chế của VPN

### Ưu điểm

- Lưu lượng cá nhân của người dùng được mã hóa, đồng thời truyền an toàn qua Internet. Điều này giúp người dùng dễ dàng tránh xa khỏi các mối đe dọa trên Internet.
- VPN khiến tin tặc gặp khó khăn khi xâm nhập hay gây trở ngại tới công việc của cá nhân hoặc doanh nghiệp.
- Với VPN người dùng hoàn toàn có thể yên tâm sử dụng Wifi công cộng, không phải lo nghĩ về những tên tin tặc, đồng thời có thể an toàn kết nối từ xa với máy chủ.
- Với trình bảo mật cao như vậy, bạn hoàn toàn có thể ẩn danh khi lướt web. Không những thế, đa số các VPN còn có giao diện rất dễ cấu hình, những người không rành công nghệ cũng có thể thao tác được.

### Nhược điểm

- Ngày nay, rất nhiều các trang web đã trở nên cảnh giác với VPN nên tạo ra nhiều trở ngại nhằm ngăn cản, giảm lượng truy cập vào nội dung bị hạn chế.
- Nhiều người sử dụng VPN vào các hoạt động xấu, bất hợp pháp.
- Việc sử dụng VPN đòi hỏi bạn phải có ngân sách kha khá để chi trả cho việc sử dụng hàng tháng. Bởi các VPN miễn phí được đánh giá là không an toàn.

## II.2. Cài đặt virtual private network

### II.2.1. Yêu cầu

Quá trình cài đặt và cấu hình VPN gồm các bước cơ bản sau:

- Xây dựng một máy VPN Server để tiếp nhận các yêu cầu kết nối mạng từ xa (còn gọi là Remote Access Server)
- Cấp cho người dùng VPN Client một tài khoản có quyền đăng nhập vào VPN Server (gọi là Dial-In User)
- Tại các VPN Clients tạo mới một kết nối riêng ảo đến VPN Server (gọi là VPN Connection). Đăng nhập vào VPN Server bằng Dial-In User
- Chọn giao thức truyền dữ liệu: L2TP, PPTP hay GRE/Ipsec tương ứng tại VPN Server và VPN Clients
- Xác định phương thức mã hóa và chứng thực tương ứng tại VPN Server và VPN Clients

### II.2.2. Chuẩn bị

Gồm 3 máy cấu hình IP như hình 2.7

- Trường hợp hệ thống tại VPN Server có sử dụng Firewall thì phải mở cổng (TCP port) cho luồng dữ liệu dịch vụ VPN từ các Clients đi vào được hệ thống nội bộ.

**Bảng 2.1: Cấu hình IP**

DC	VPN_Server	VPN_Client
Card 1: IP 192.168.10.2/24 Card 2: IP 172.16.1.1/24 Gateway: 192.168.10.1	Card 1: IP 192.168.10.1/24 Card 2: IP 172.16.1.1/24	Card 2: IP 172.16.1.2/24
		Gateway: 172.16.1.1

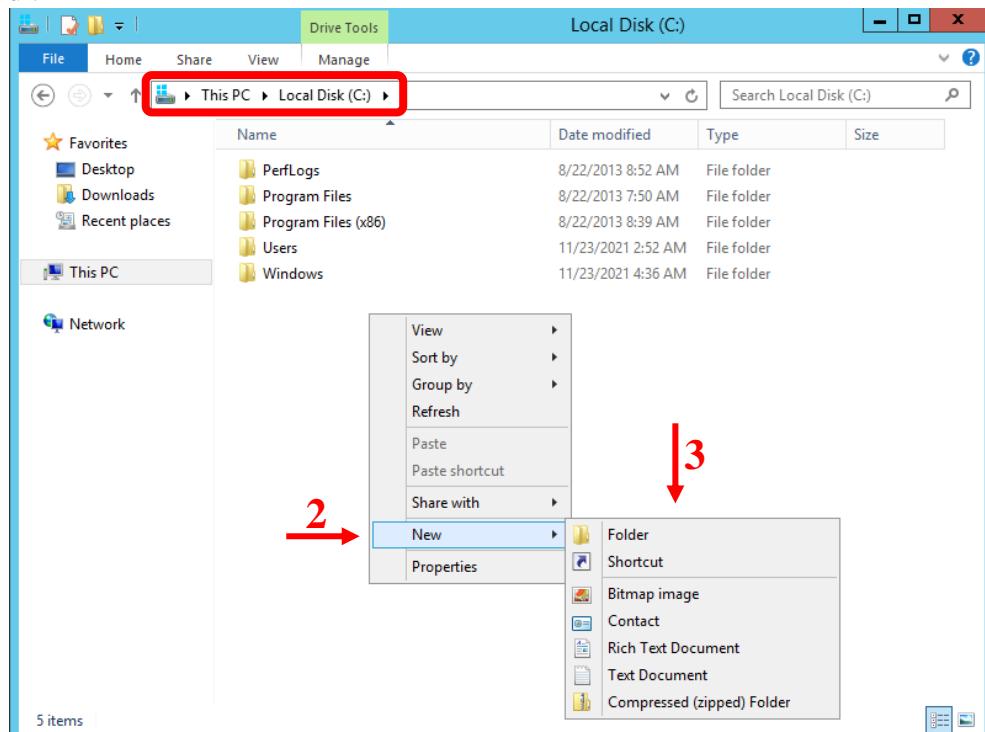


**Hình 2.7: Mô Hình Kết Nối VPN**

### II.2.3. Thực hiện

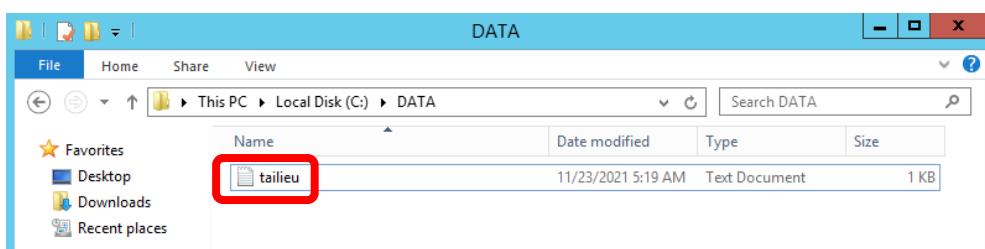
#### II.2.3.1 TẠO FOLDER VÀ CHIA SẺ THƯ MỤC

- Truy cập máy DC tạo 1 Folder tên là DATA trong ổ C và chia sẻ thư mục này cho user được phép truy cập từ xa vào lấy tài liệu.
- This PC → Local Disk(C:) → Click chuột phải chọn new → Folder → đặt tên vd : DATA



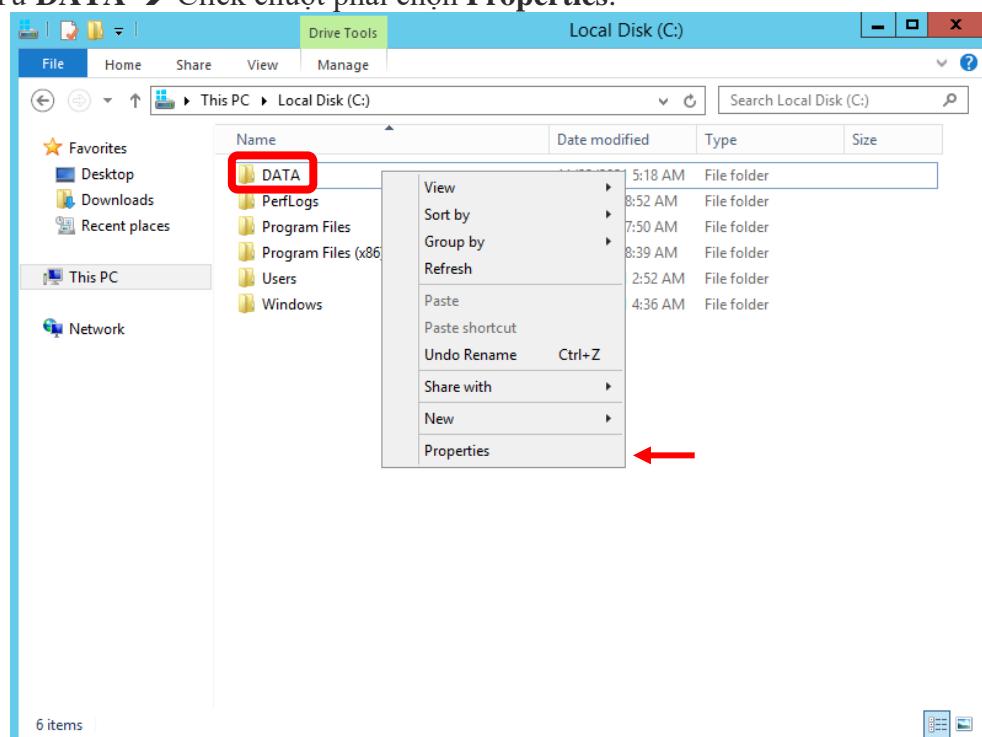
Hình 2.8: Cửa sổ ổ (C:)

- Trong thư mục DATA tạo một file tailieu.



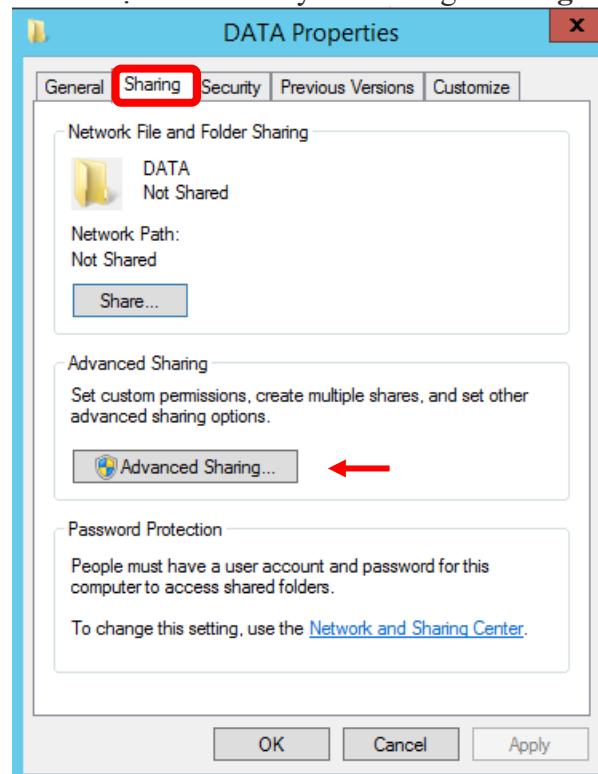
Hình 2.9: Folder DATA

- Để chia sẻ dữ liệu cho người dùng từ xa
- Từ DATA → Click chuột phải chọn Properties.



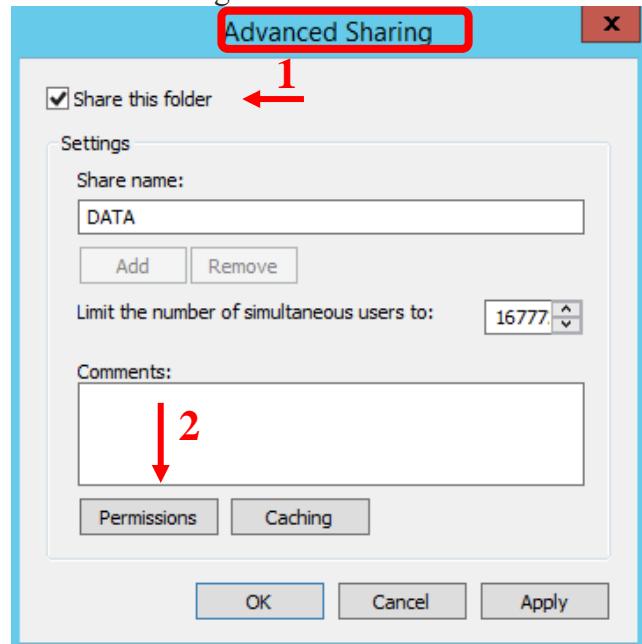
Hình 2.10: Cửa sổ ổ (C:)

- Cửa sổ Properties được mở → chuyển tab sang Sharing → Advanced Sharing...



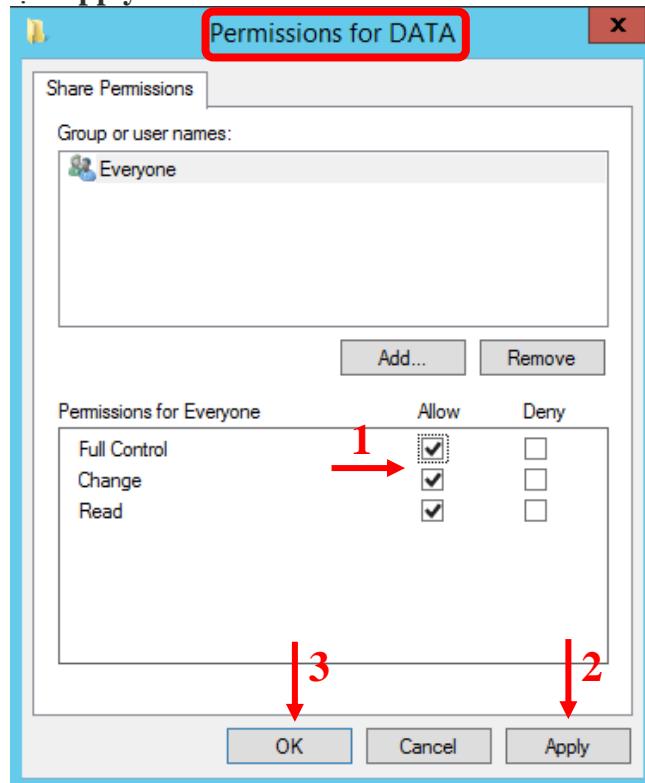
Hình 2.11: Cửa sổ Properties

- Ở cửa sổ Advanced Sharing → Click Share this folder → Permissions



Hình 2.12: Cửa sổ Advanced Sharing

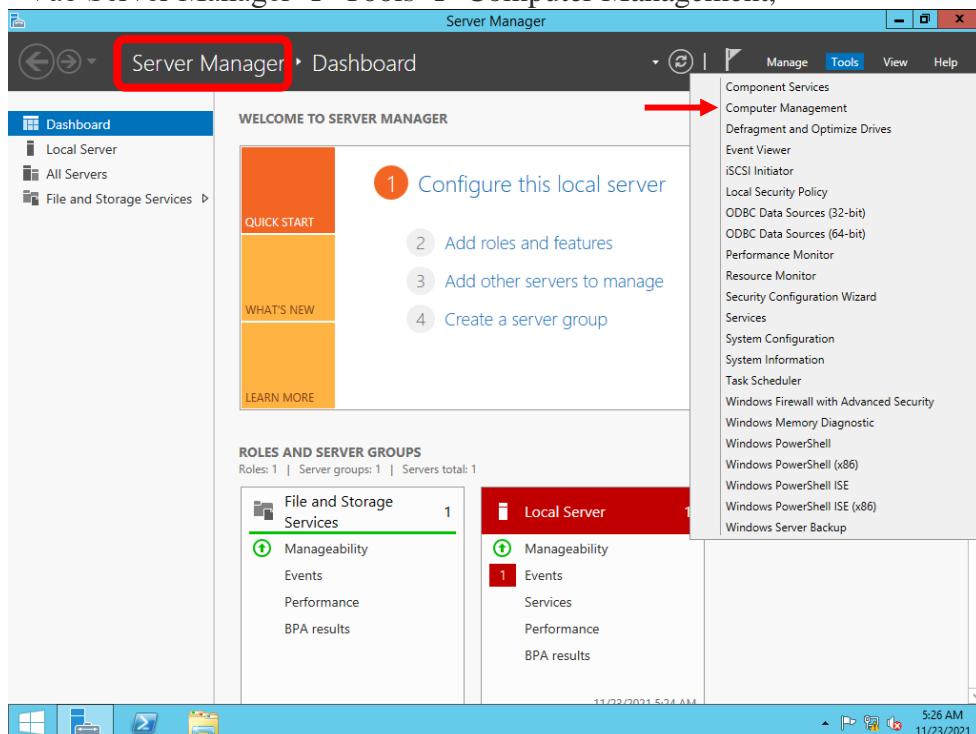
- Trong Permissions for DATA click chọn Allow cho Full Control và Change
- Tiếp tục chọn Apply và OK .



Hình 2.13: Tab Share Permissions

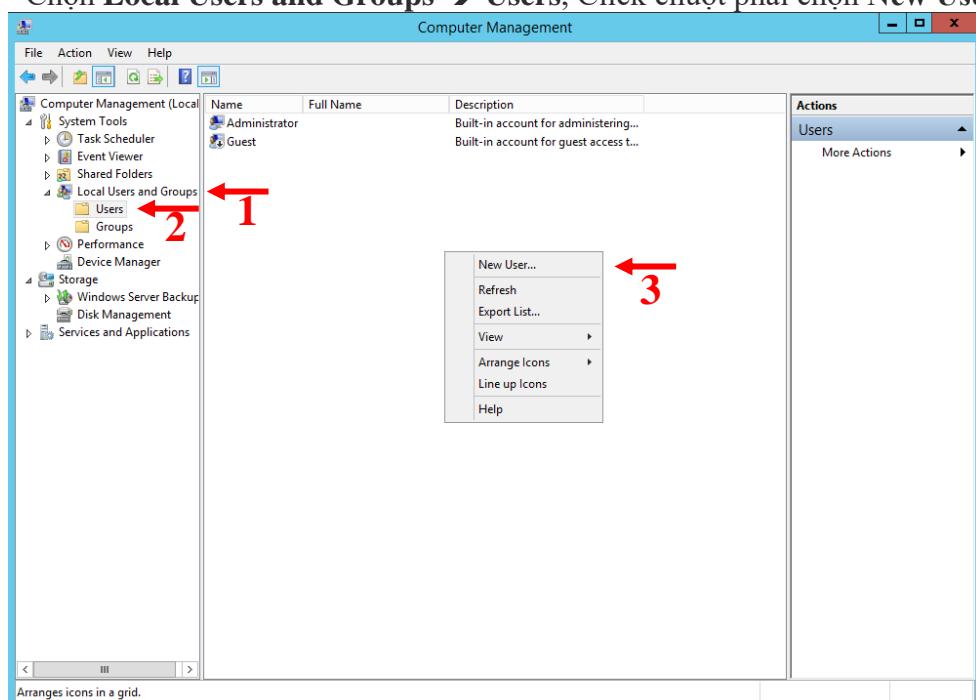
### II.2.3.2 TẠO TÀI KHOẢN DÙNG ĐỂ THIẾT LẬP DỊCH VỤ VPN

- Tiếp tục mở **Máy VPN\_Server**, thực hiện:
- Vào Server Manager → Tools → Computer Management,



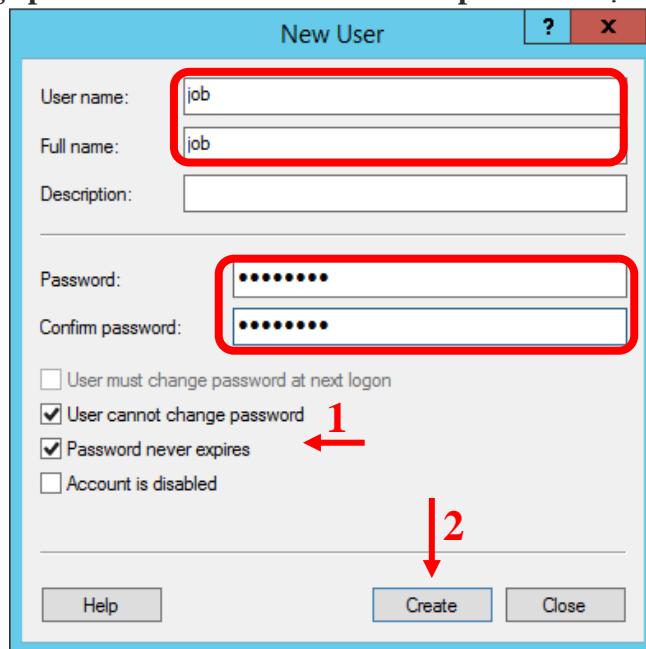
Hình 2.14: Cửa sổ Server Manager

- Chọn **Local Users and Groups** → **Users**, Click chuột phải chọn **New User...**



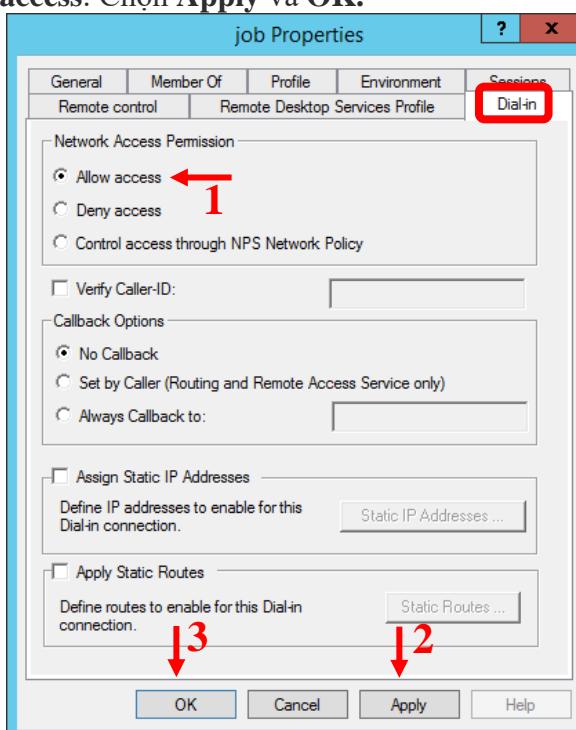
Hình 2.15: Cửa sổ Computer Management

- Tại cửa sổ New User, nhập tên user cần tạo. Ví dụ ở đây đặt tên User name và Full name: là job → Tiếp tục nhập Password và Confirm password → Click vào **User cannot change password** và **Password never expires** → chọn Create.



Hình 2.16: Cửa sổ New User

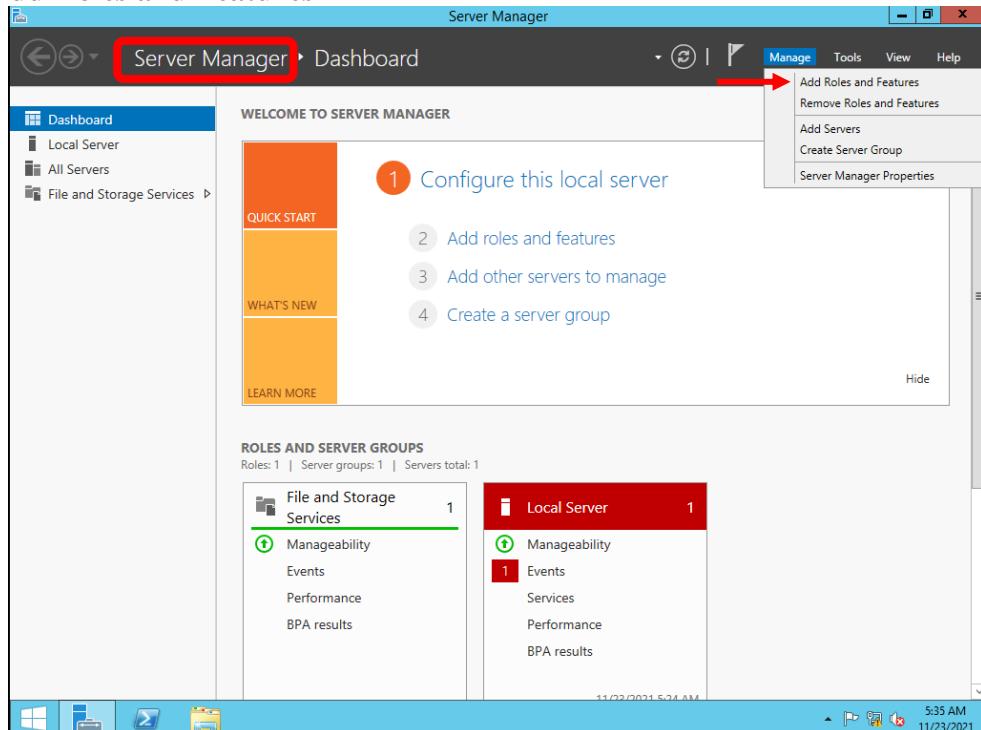
- Để cho phép User được quyền truy cập từ xa
- Click chuột phải tại user(job) vừa tạo, chọn **Properties**.
- Trong cửa sổ Properties chuyển sang tab **Dial-in**, tại mục **Network Access Permission**, chọn vào **Allow access**. Chọn **Apply** và **OK**.



Hình 2.17: Tab Dial-in

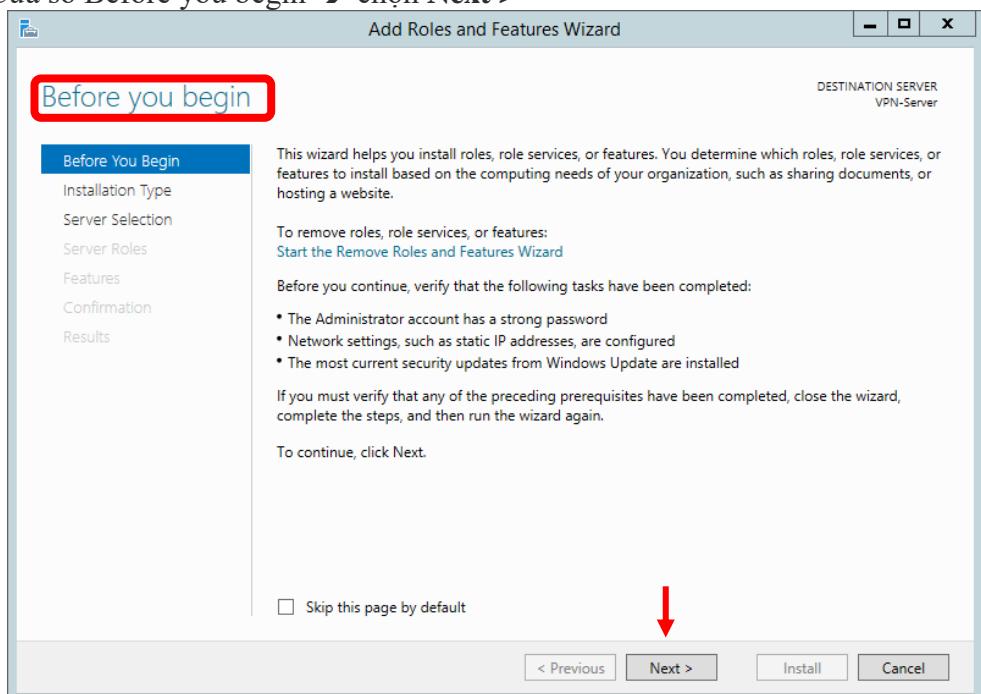
### II.2.3.3 THỰC HIỆN CÀI ĐẶT DỊCH VỤ REMOTE ACCESS

- Thực hiện cài đặt dịch vụ Remote Access. Mở Server Manager → Chọn Manage → Add Roles and Features



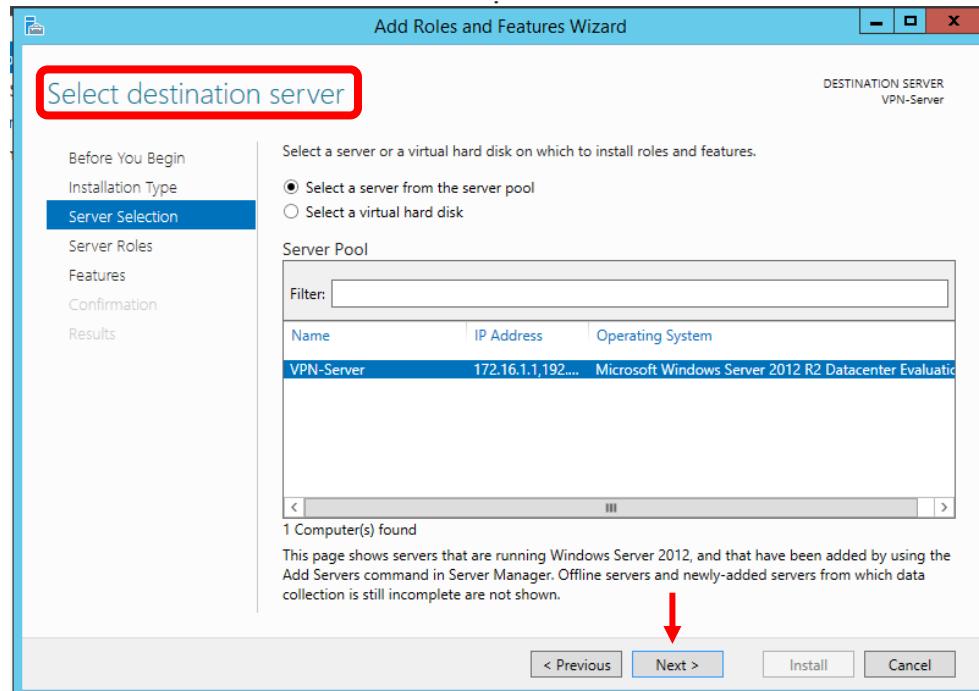
Hình 2.18: Cửa sổ Server Manager

- Cửa sổ Before you begin → chọn Next >



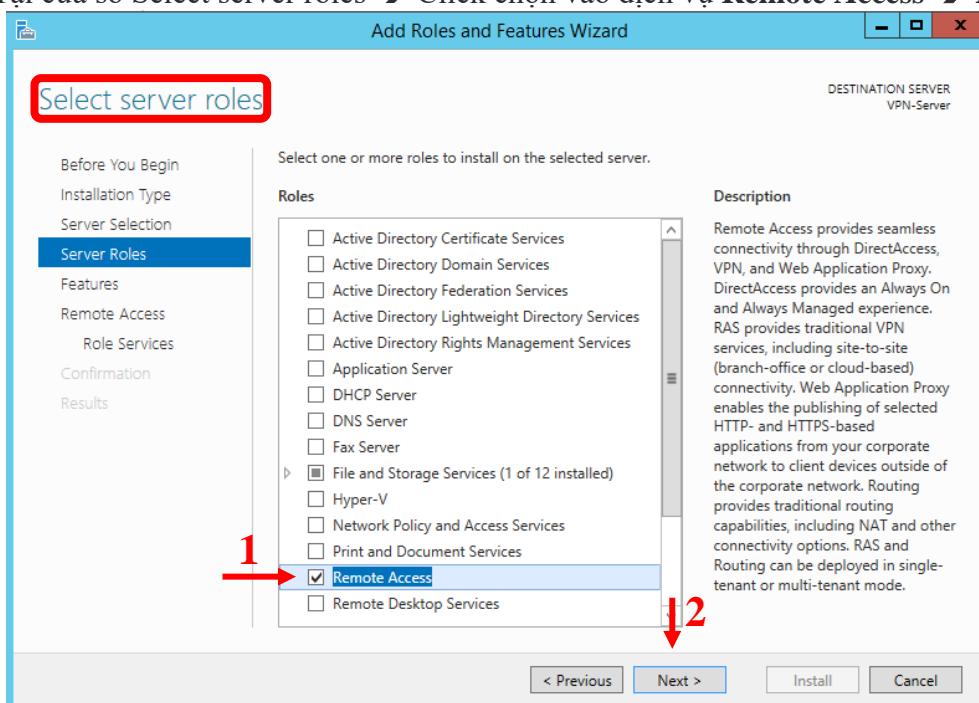
Hình 2.19: Cửa sổ Before you begin

- Cửa sổ Select destination server ➔ Chọn Next >



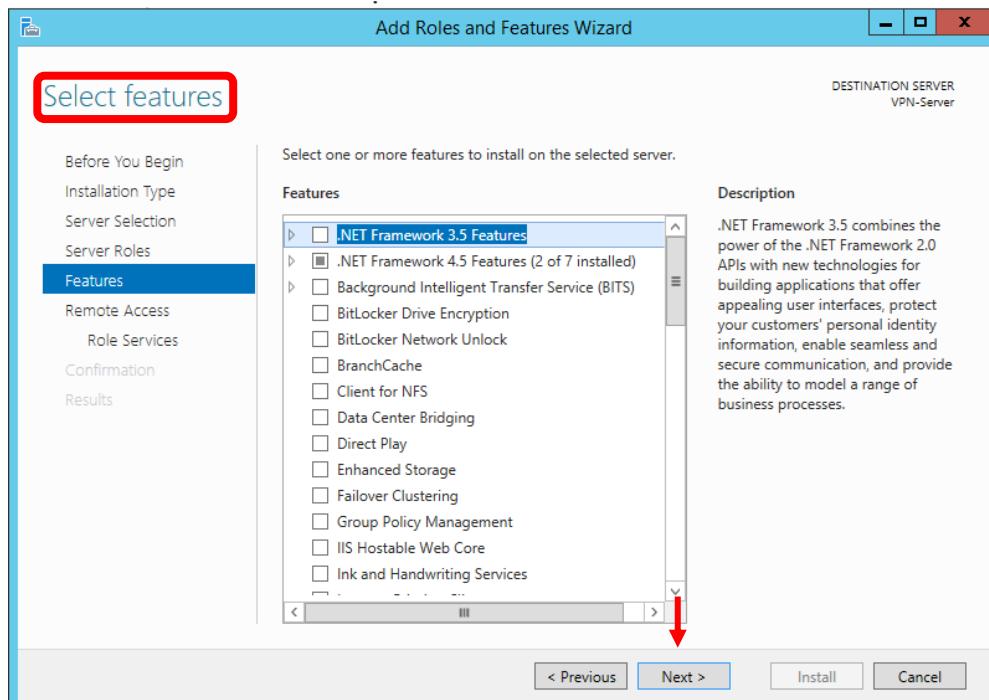
Hình 2.20: Cửa sổ Select destination server

- Tại cửa sổ Select server roles ➔ Click chọn vào dịch vụ **Remote Access** ➔ Next >



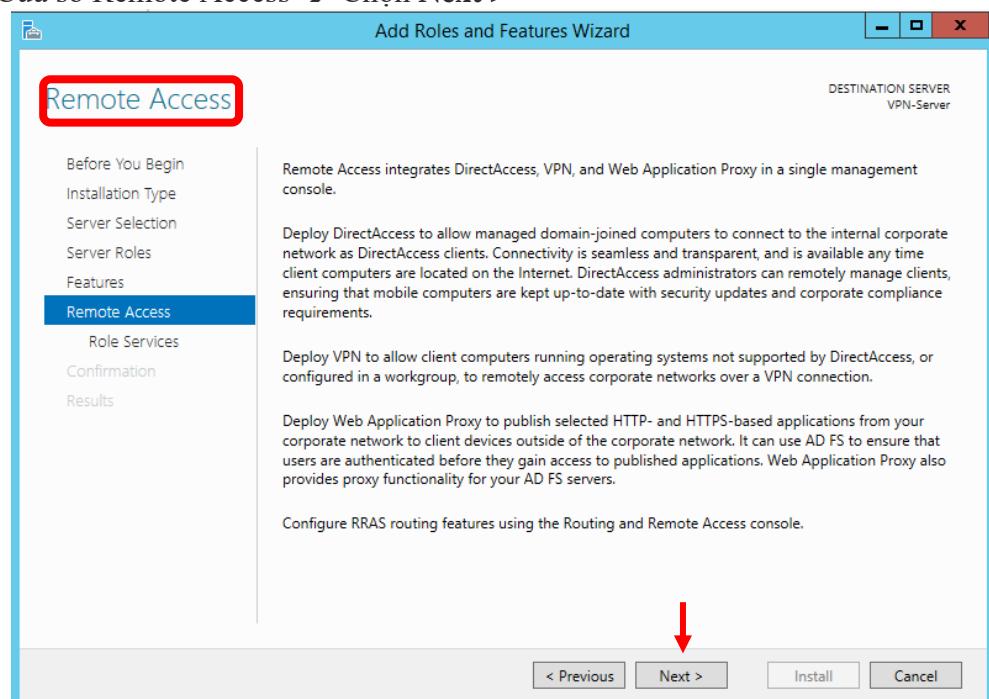
Hình 2.21: Cửa sổ Select server roles

- Cửa sổ Select features → Chọn Next >



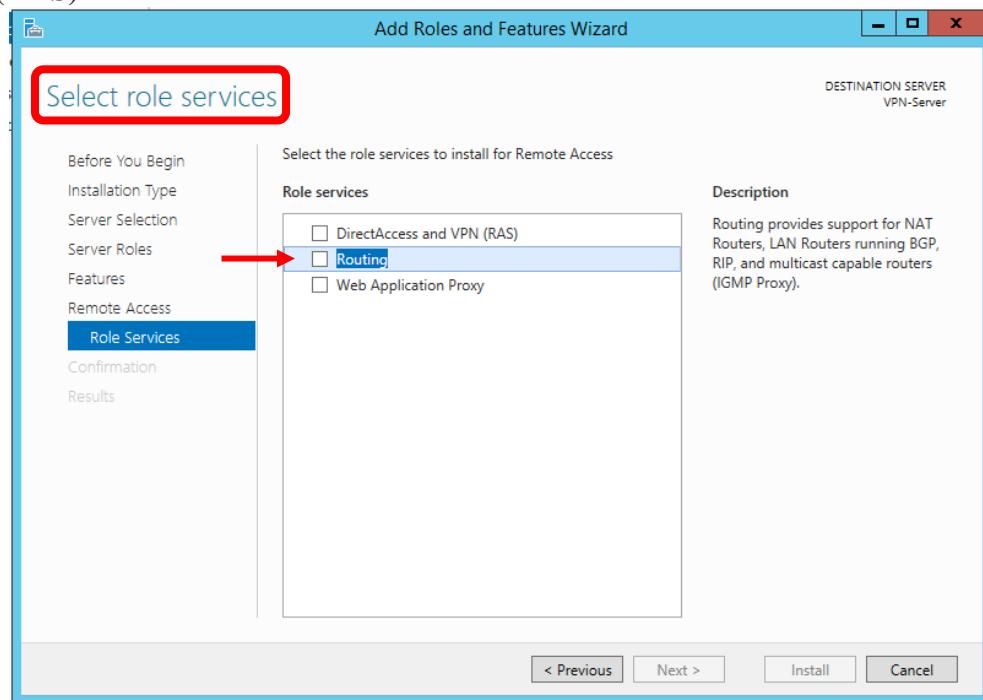
Hình 2.22: Cửa sổ Select features

- Cửa sổ Remote Access → Chọn Next >



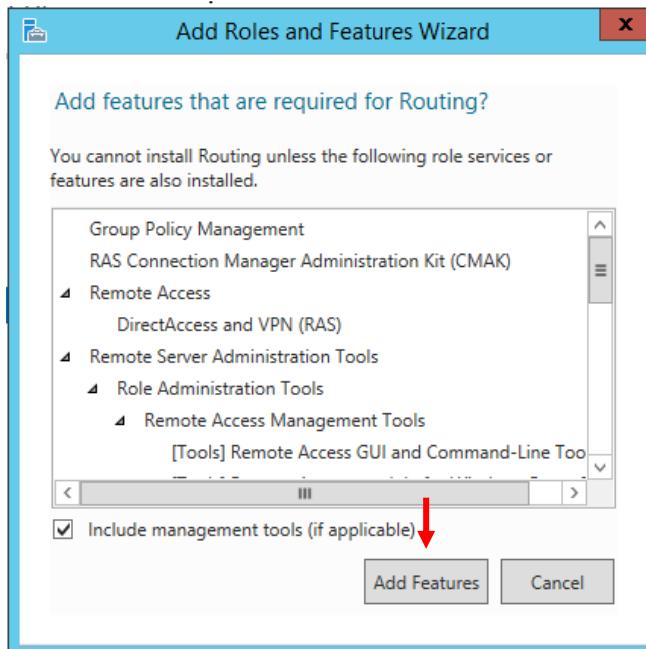
Hình 2.23: Cửa sổ Remote Access

- Tại cửa sổ Select role services, click chọn vào **Routing** và **DirectAccess and VPN (RAS)**



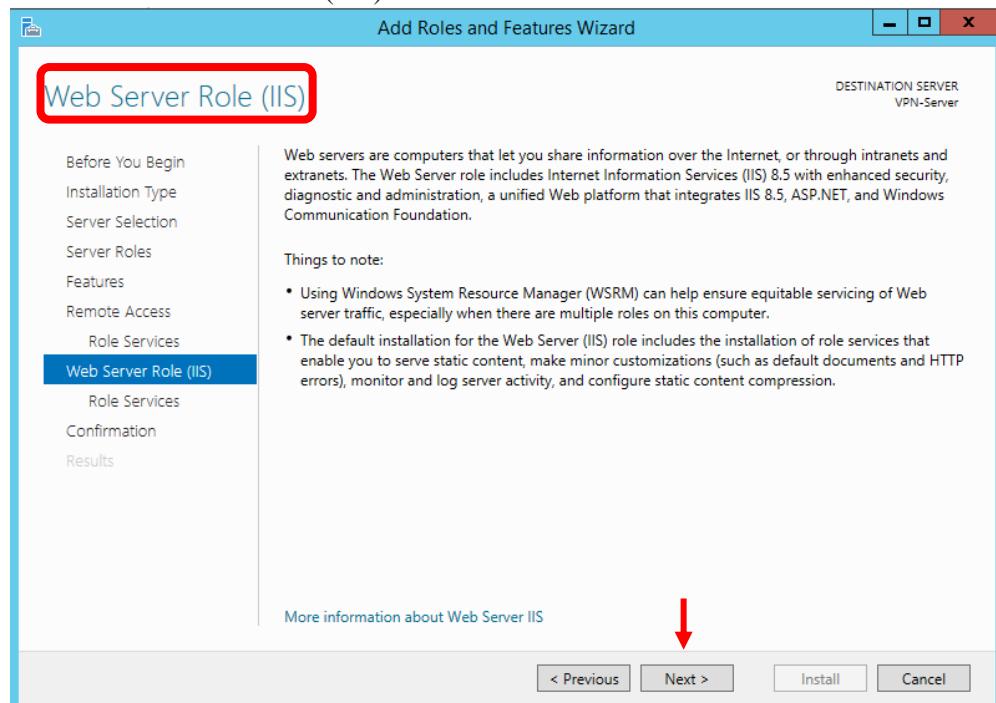
Hình 2.24: Cửa sổ Select role services

- Cửa sổ Add Roles and Features Wizard được mở → Chọn **Add Features**
- Trở về Select role services chọn **Next >**



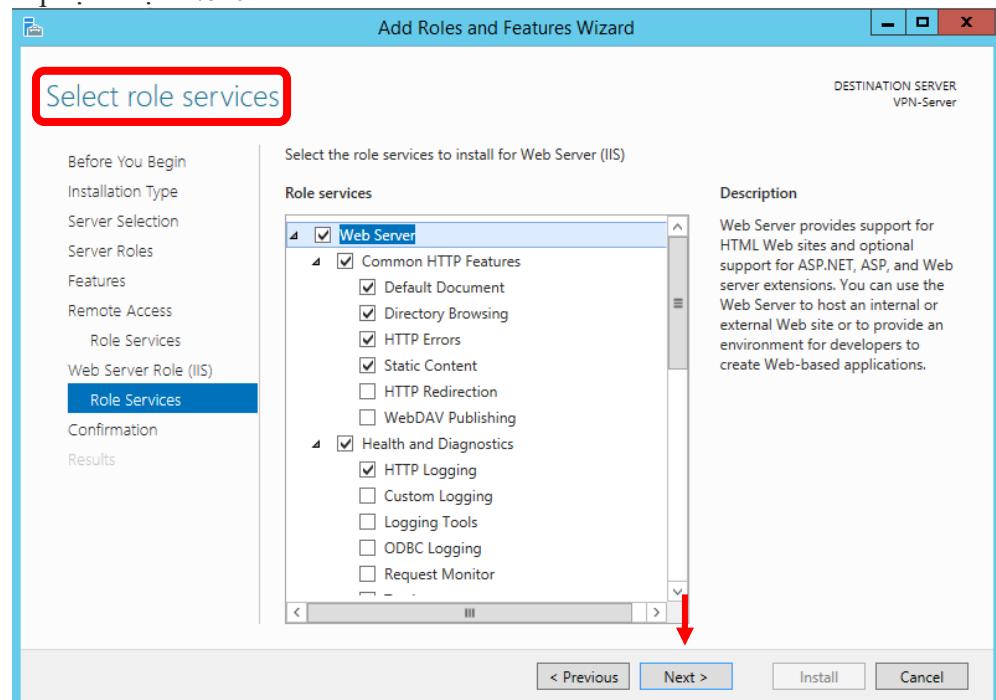
Hình 2.25: Cửa sổ Add Roles and Features Wizard

- Cửa sổ Web Server Role (IIS) ➔ Next >



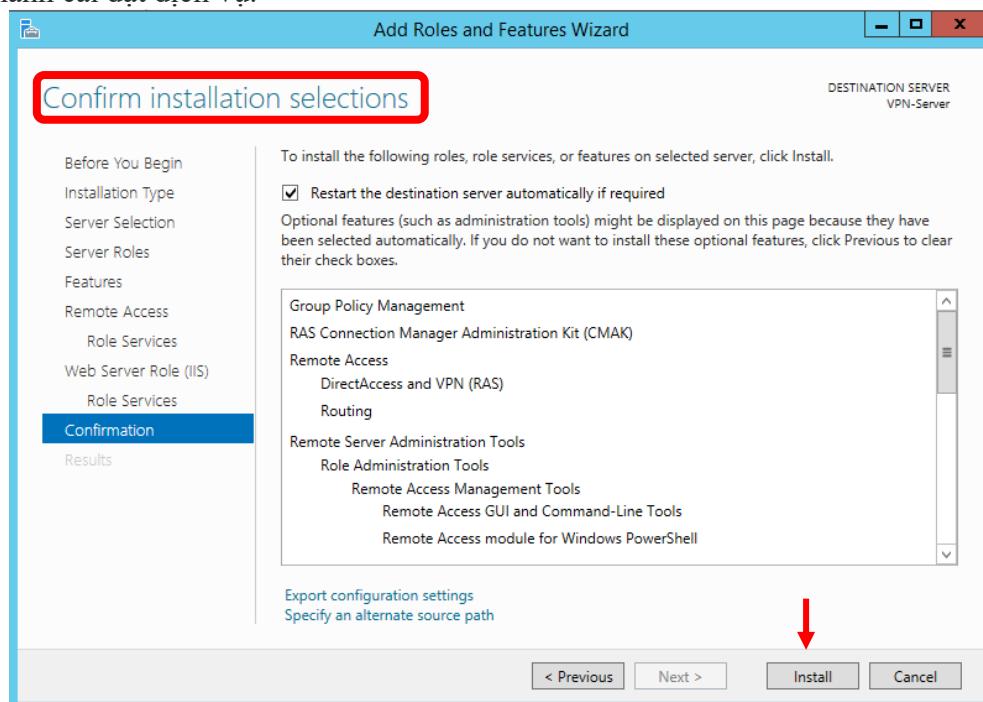
Hình 2.26: Cửa sổ Web Server Role (IIS)

- Tiếp tục chọn Next >



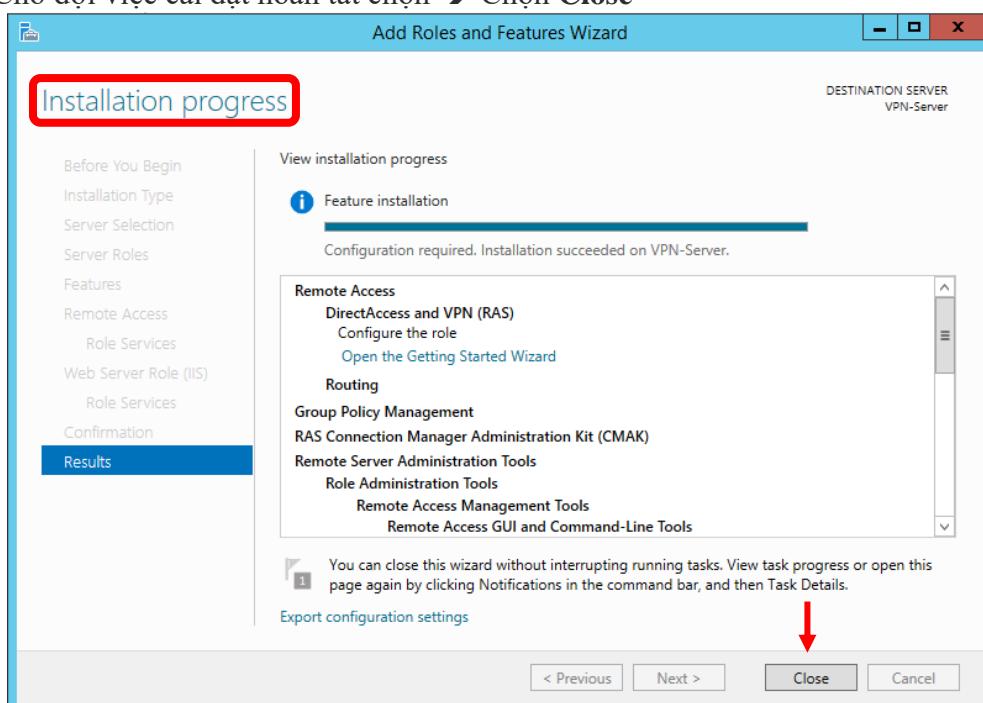
Hình 2.27: Cửa sổ Select role services

- Cuối cùng tại cửa sổ Confirm installation selections → chọn **Install** để máy chủ tiến hành cài đặt dịch vụ.



Hình 2.28: Cửa sổ Confirm installation selections

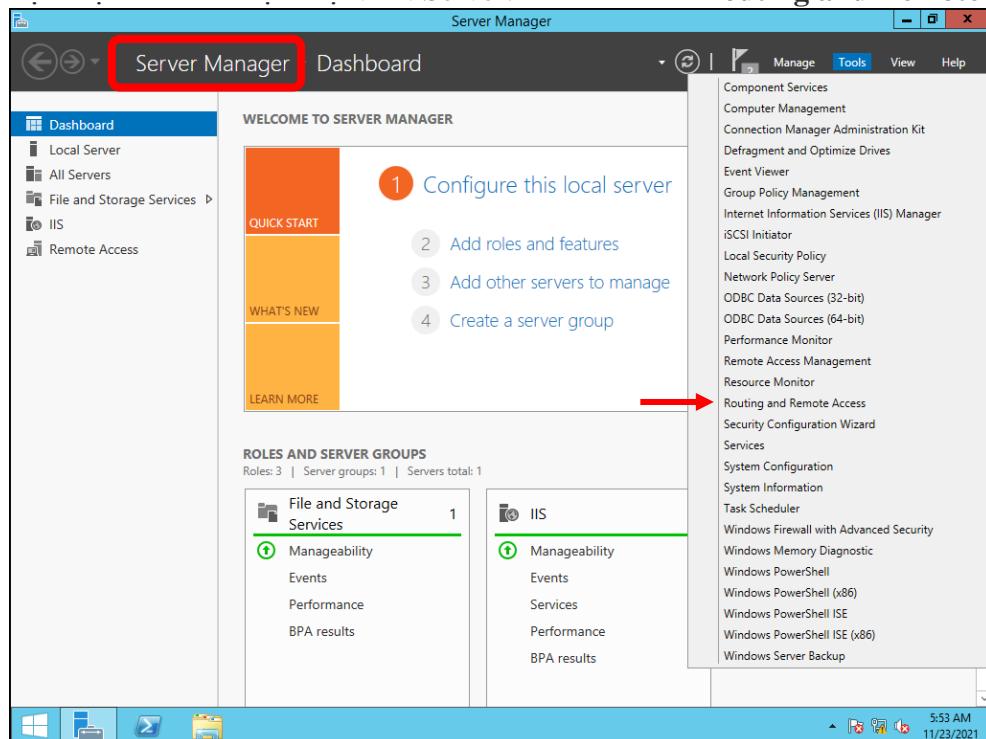
- Chờ đợi việc cài đặt hoàn tất chọn → Chọn **Close**



Hình 2.29: Cửa sổ Installation progress

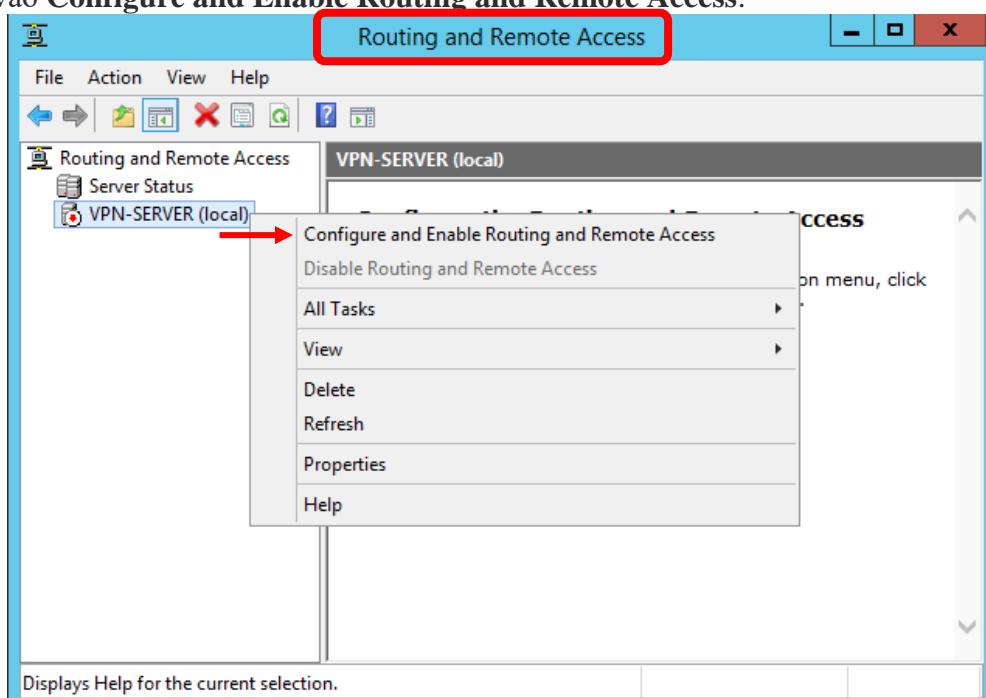
#### II.2.3.4. THỰC HIỆN CẤU HÌNH DỊCH VỤ VPN SERVER

- Thực hiện cấu hình dịch vụ VPN Server. Mở Tools → Routing and Remote Access



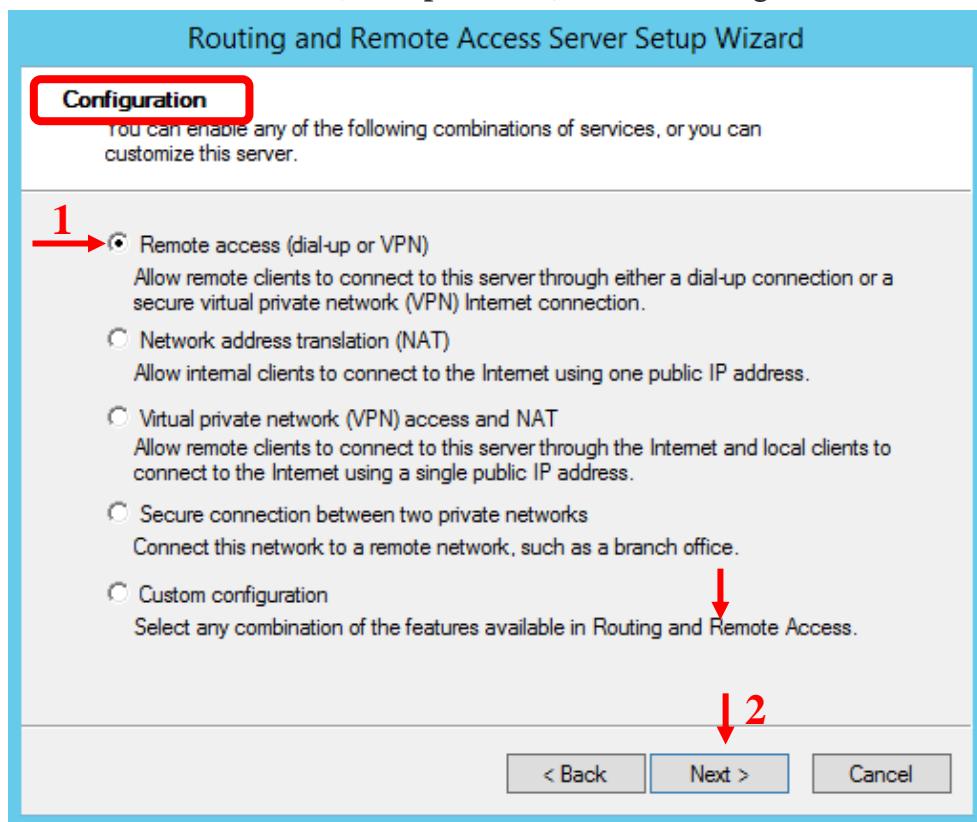
Hình 2.30: Cửa sổ Server Manager

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



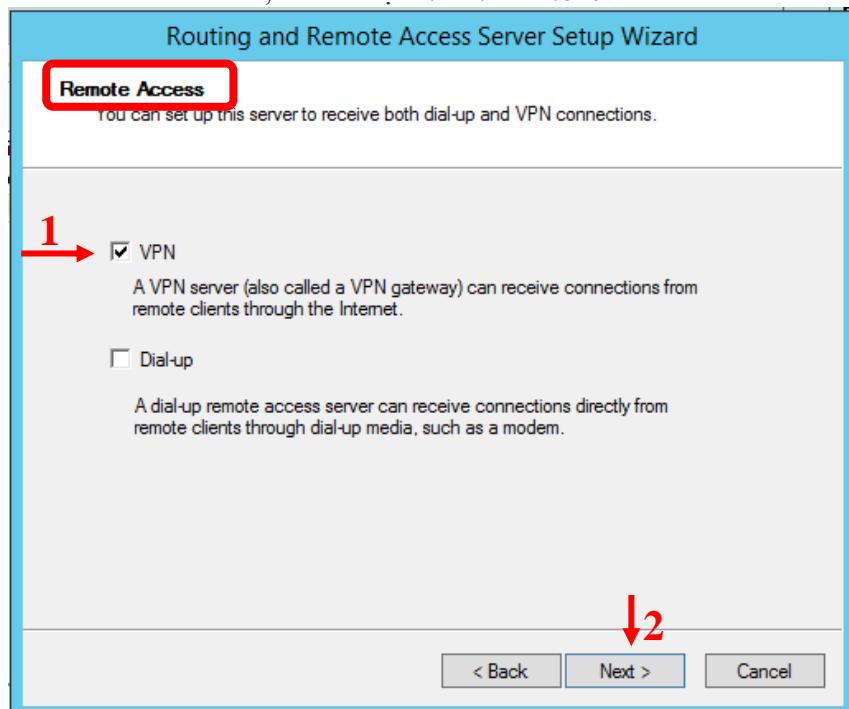
Hình 2.31: Cửa sổ Routing and Remote Access

- Click chọn **Remote access(dial-up or VPN)** ở cửa sổ configuration



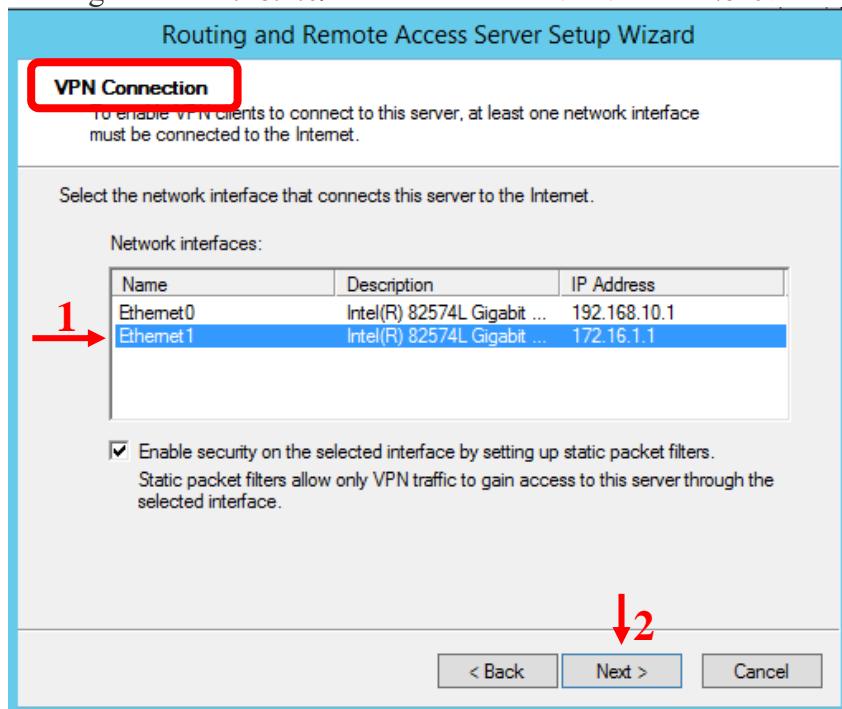
Hình 2.32: Cửa sổ Configuration

- Tại cửa sổ Remote Access, click chọn **VPN** → **Next >**



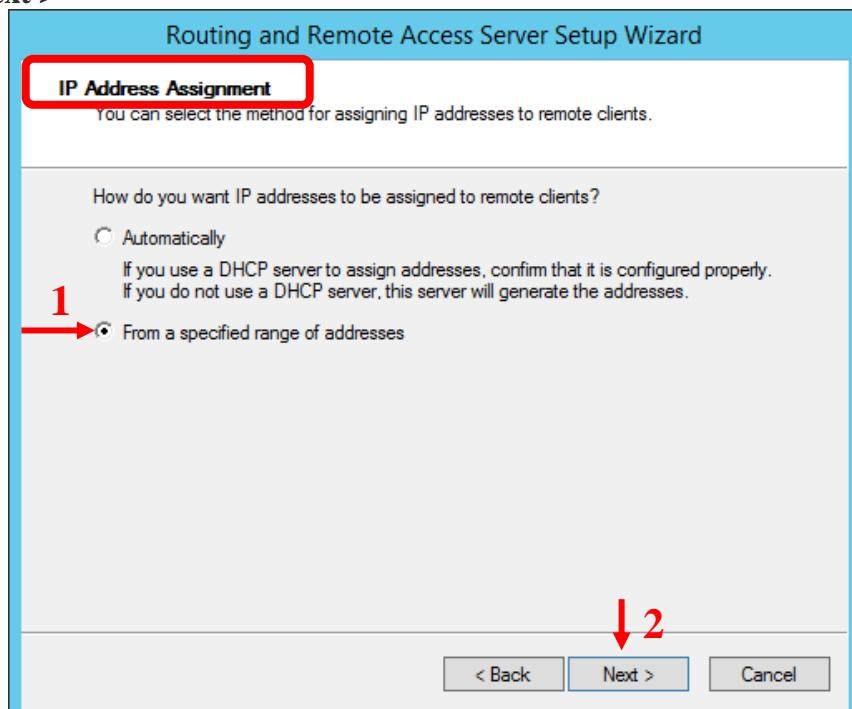
Hình 2.33: Cửa sổ Remote Access

- Ở mục **Network interface**: ta chọn **WAN(Ethernet1)** để con server này cho phép tất cả người dùng ở dải **172.16.1.0/24** có thể kết nối VPN và ấn **Next >**



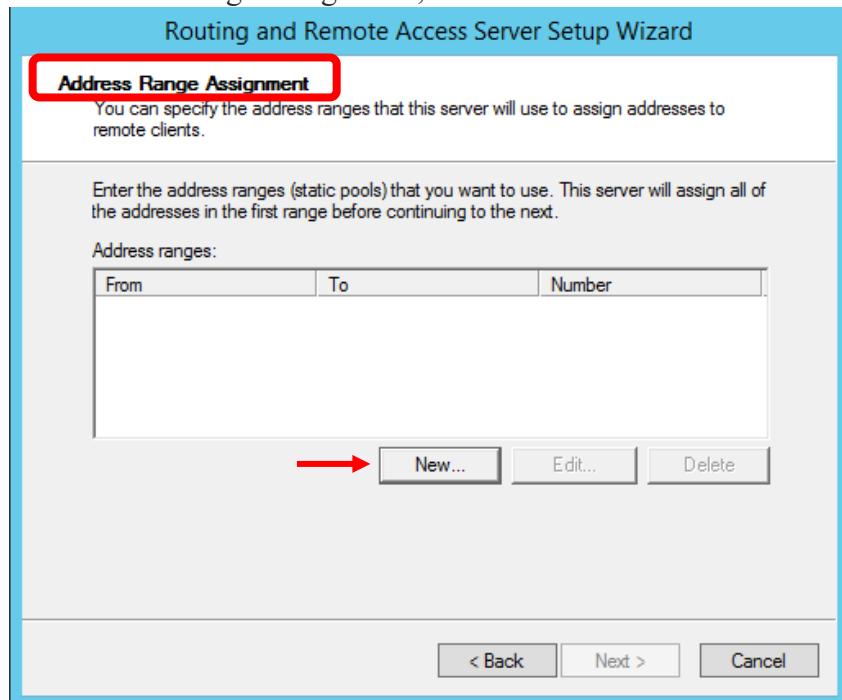
Hình 2.34: Cửa sổ VPN Connection

- Tại cửa sổ IP Address Assignment, click chọn vào **From a specified range of address** → **Next >**



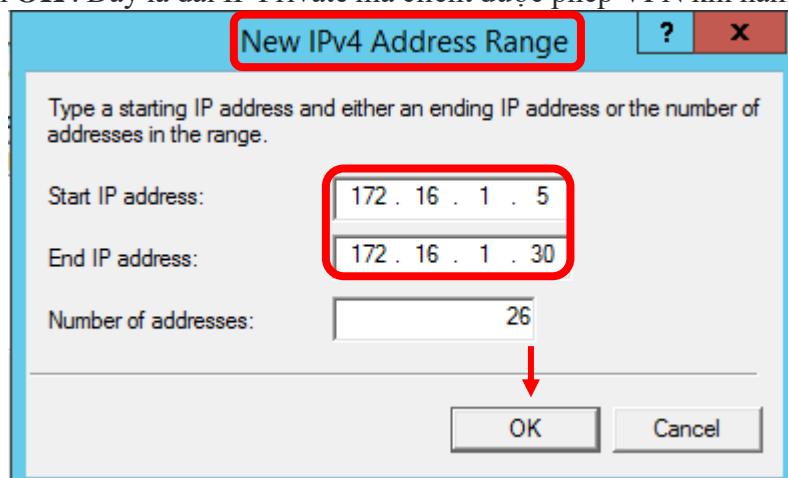
Hình 2.35: Cửa sổ IP Address Assignment

- Tại cửa sổ Address Range Assignment, click vào New...



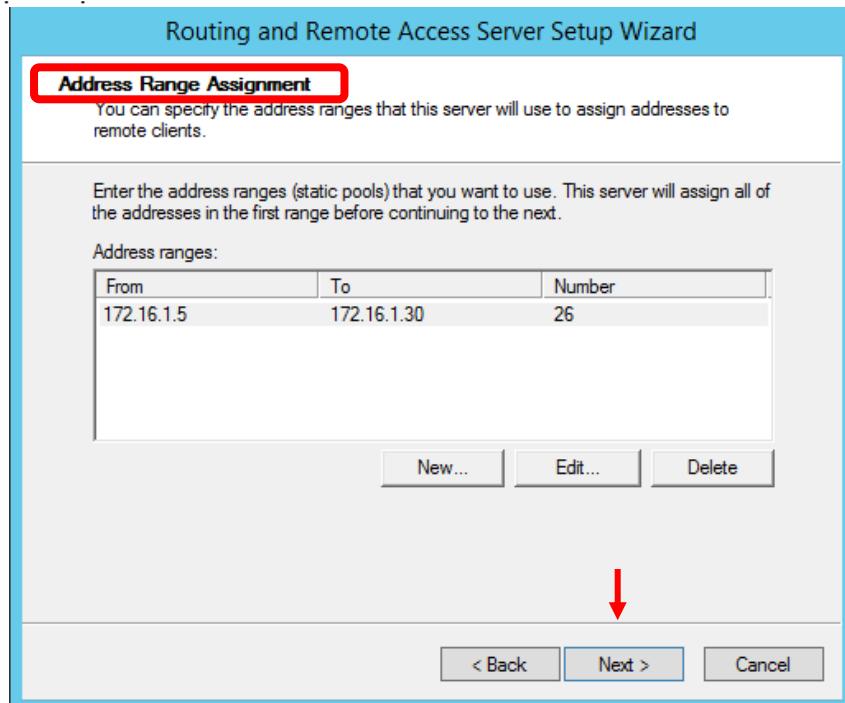
Hình 2.36: Cửa sổ Address Range Assignment

- Tại cửa sổ New Ipv4 Address Range, nhập vào dải địa chỉ IP **172.16.1.5 – 172.16.1.30**  
➔ Chọn **OK**. Đây là dải IP Private mà client được phép VPN khi nằm trong dải IP này.



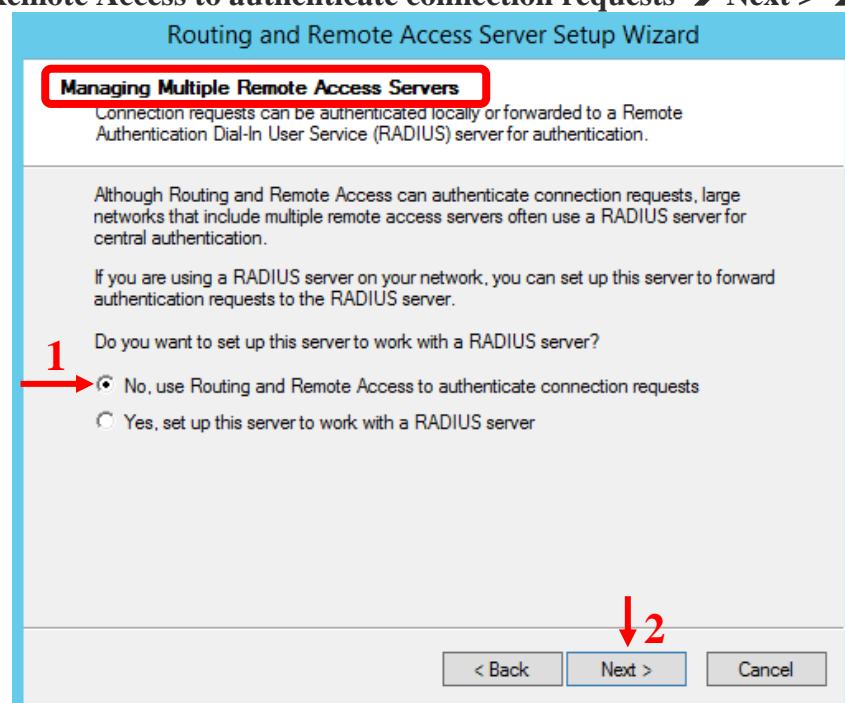
Hình 2.37: Cửa sổ New Ipv4 Address Range

- Tiếp tục Chọn Next >



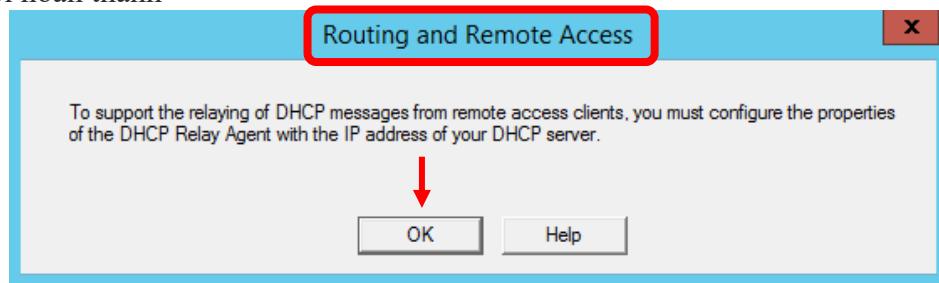
Hình 2.38: Cửa sổ Address Range Assignment

- Tại cửa sổ Managing Multiple Remote Access Servers, click chọn vào No, use Routing and Remote Access to authenticate connection requests → Next > → Finish

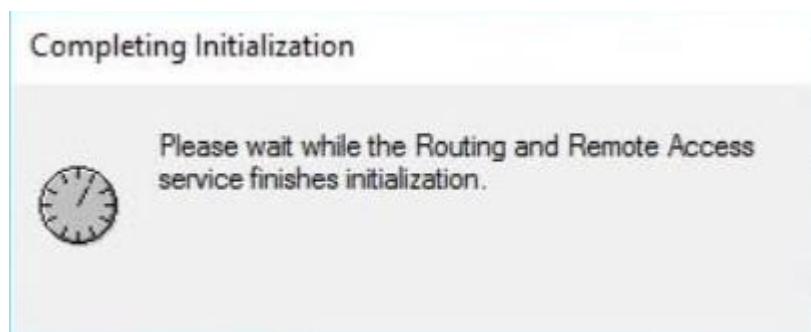


Hình 2.39: Cửa sổ Managing Multiple Remote Access Servers

- Cuối cùng Tại cửa sổ Routing and Remote Access → chọn **OK** và chờ thời gian kết nối hoàn thành



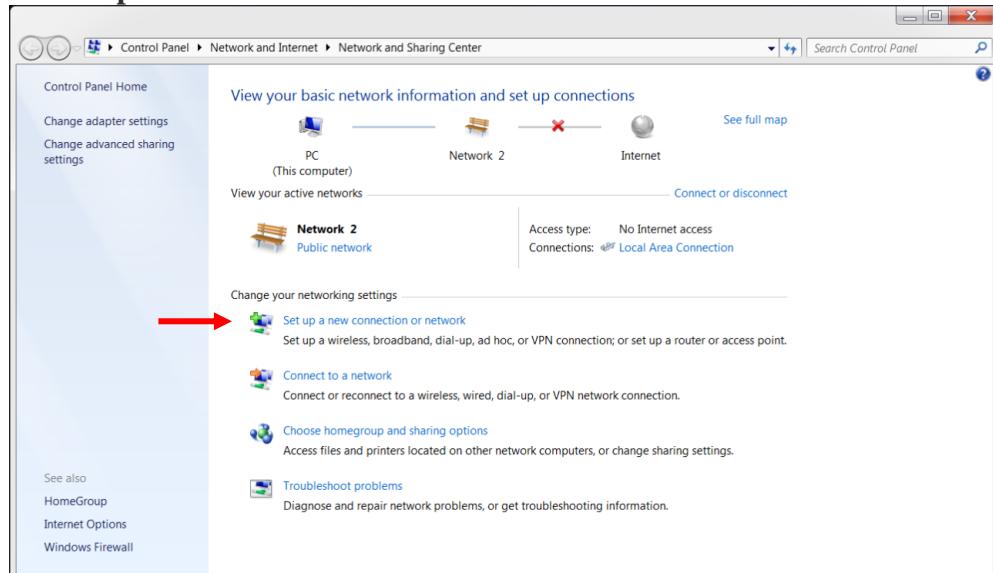
Hình 2.40: Cửa sổ Routing and Remote Access



Hình 2.41: Cửa sổ Routing and Remote Access

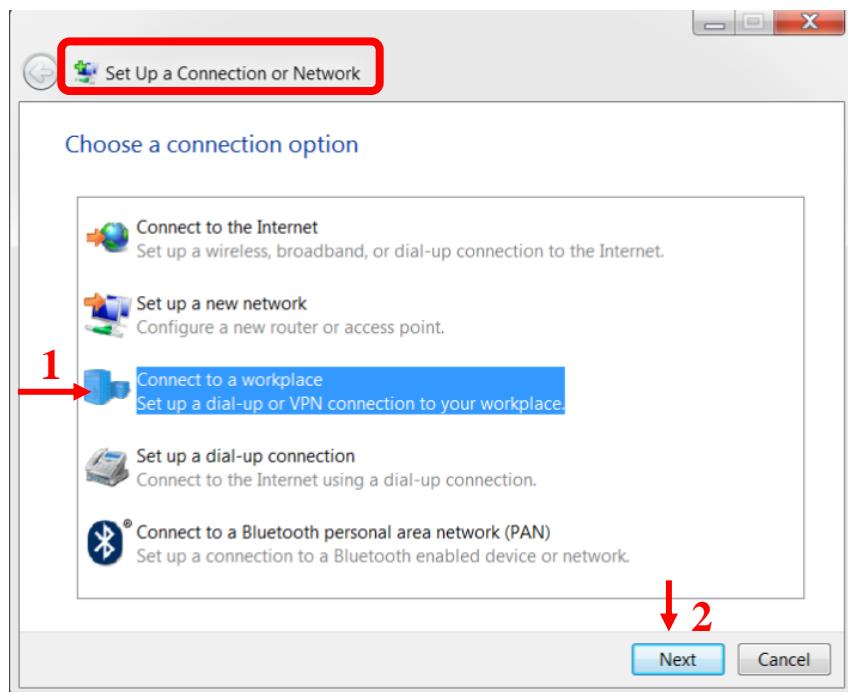
### II.2.3.5. CÀI ĐẶT VPN CONNECTION CHO CLIENT

- Chuyển sang máy **VPN\_Client** Tại cửa sổ **Network and Sharing Center**, click chọn vào **Set up an new connection or network**.



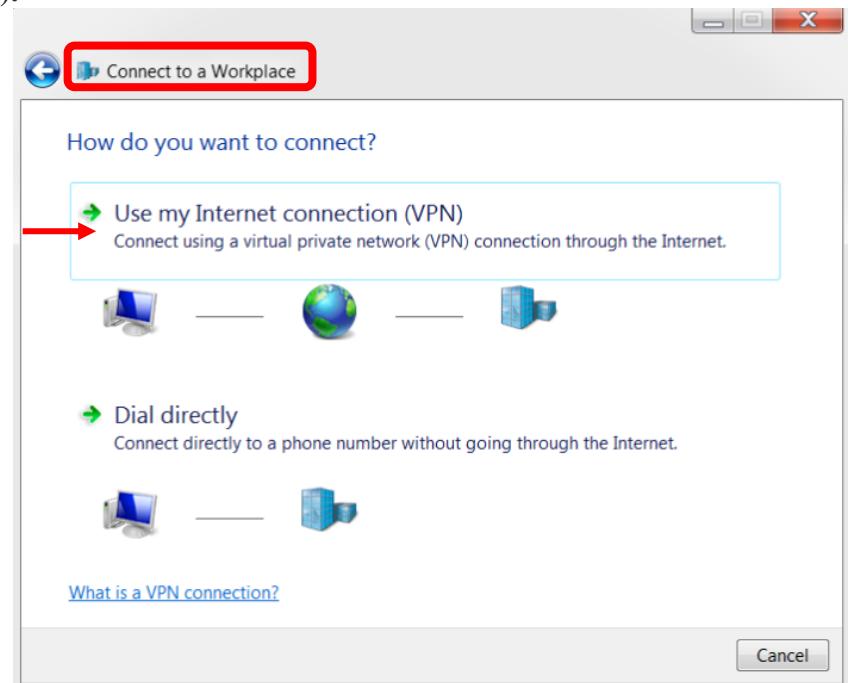
Hình 2.42: Cửa sổ Network and Sharing Center

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



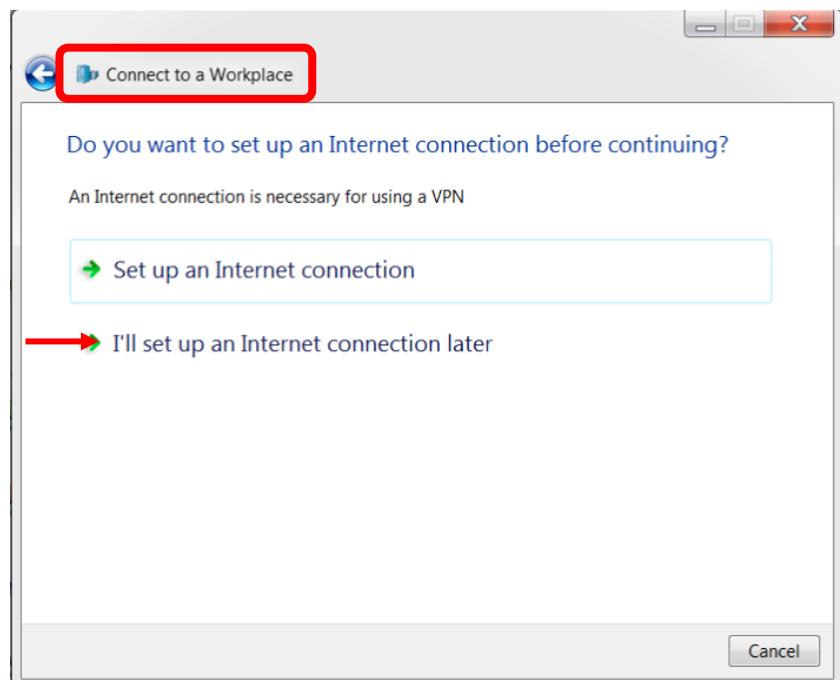
Hình 2.43: Cửa sổ Set Up a Connection or Network

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



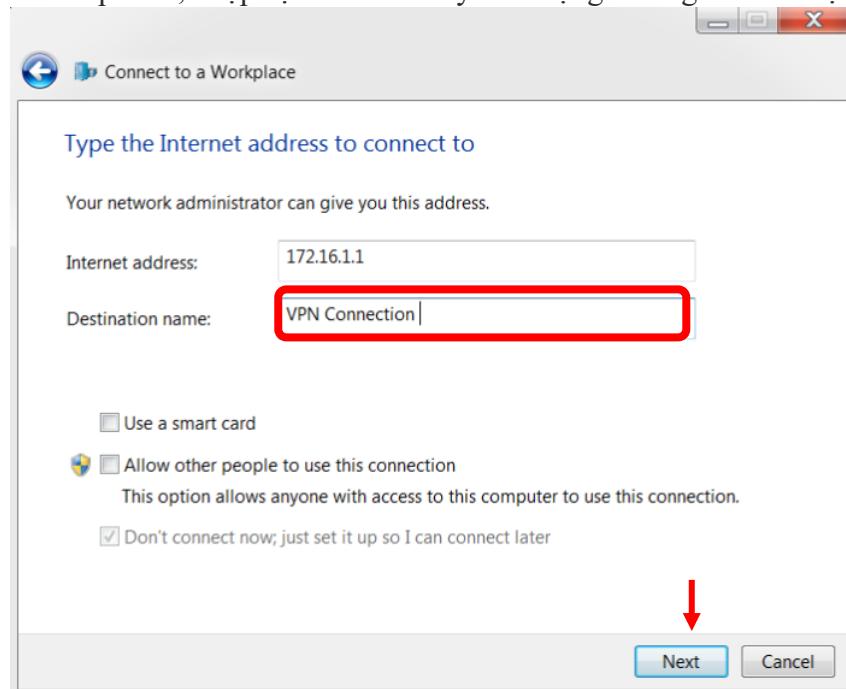
Hình 2.44: Cửa sổ Connect to a Workplace

- Tại cửa sổ tiếp theo, chọn vào **I'll set up an Internet connection later**



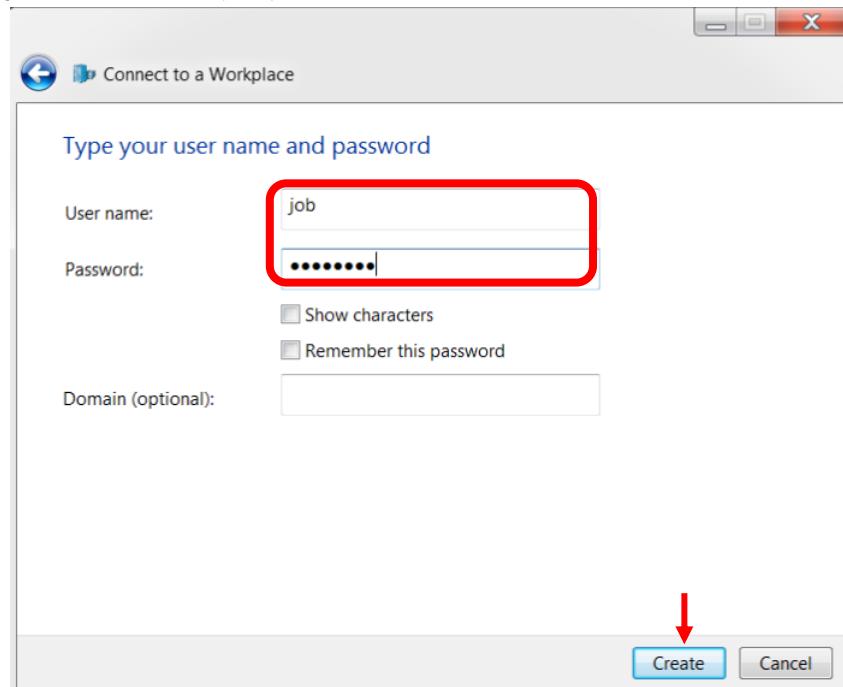
Hình 2.45: Cửa sổ Connect to a Workplace

- Tại cửa sổ tiếp theo, nhập địa chỉ Gateway của mạng bên ngoài → Chọn Next



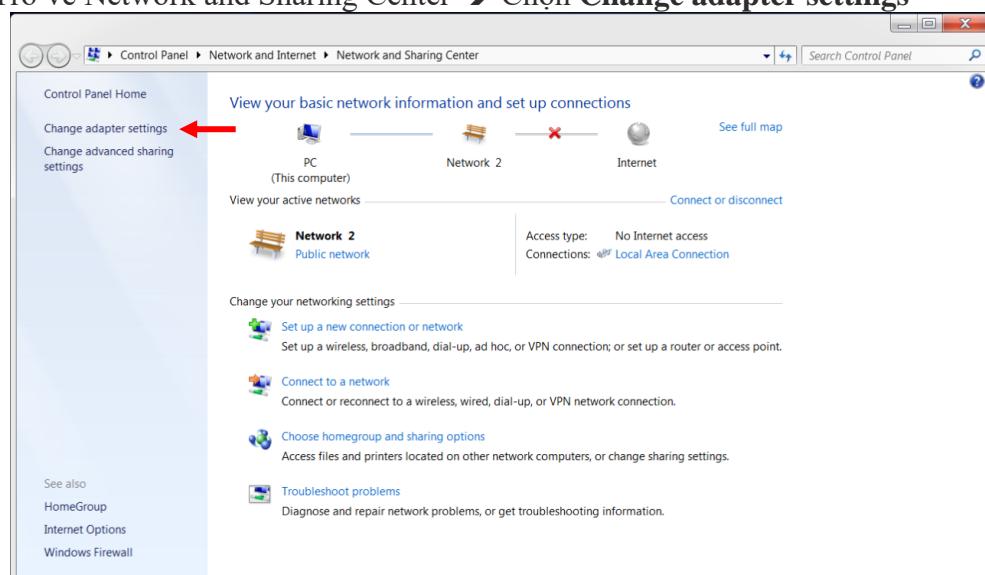
Hình 2.46: Cửa sổ Connect to a Workplace

- Nhập vào tài khoản **job** mà ta đã tạo và cấp quyền truy cập từ xa lúc nay → Chọn **Create** và chờ kết nối VPN



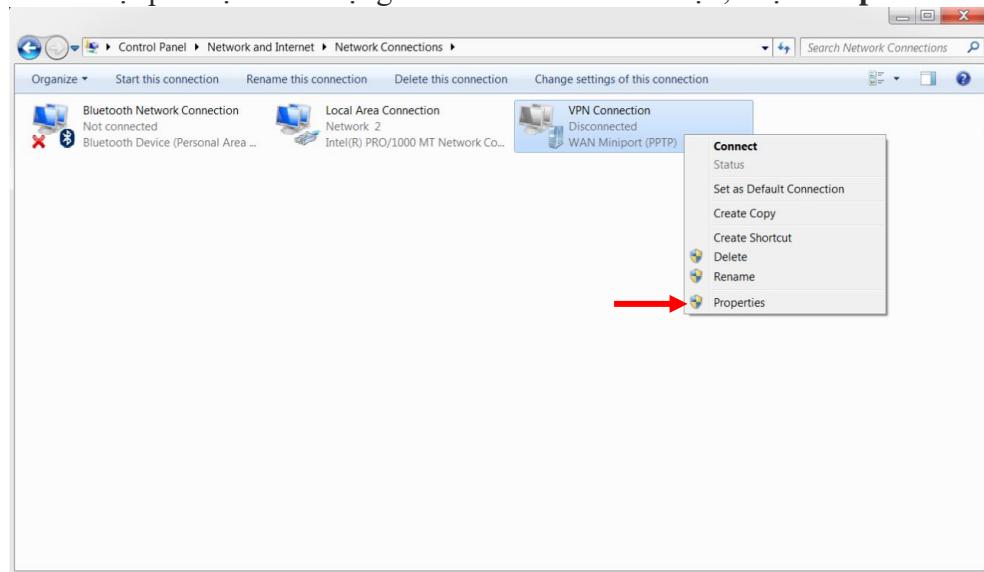
Hình 2.47: Cửa sổ Connect to a Workplace

- Trở về Network and Sharing Center → Chọn **Change adapter settings**



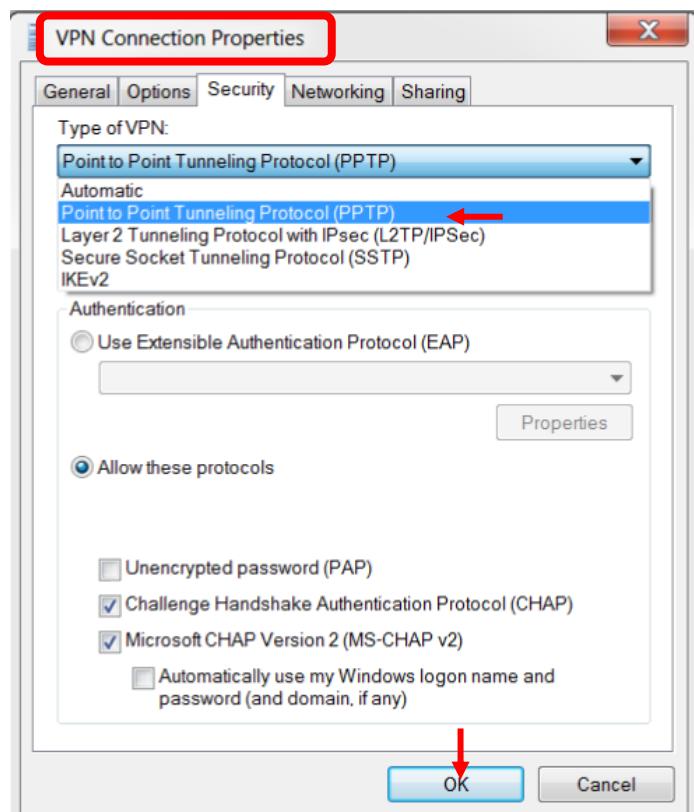
Hình 2.48: Cửa sổ Connect to a Workplace

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



**Hình 2.49: Cửa sổ Network Connections**

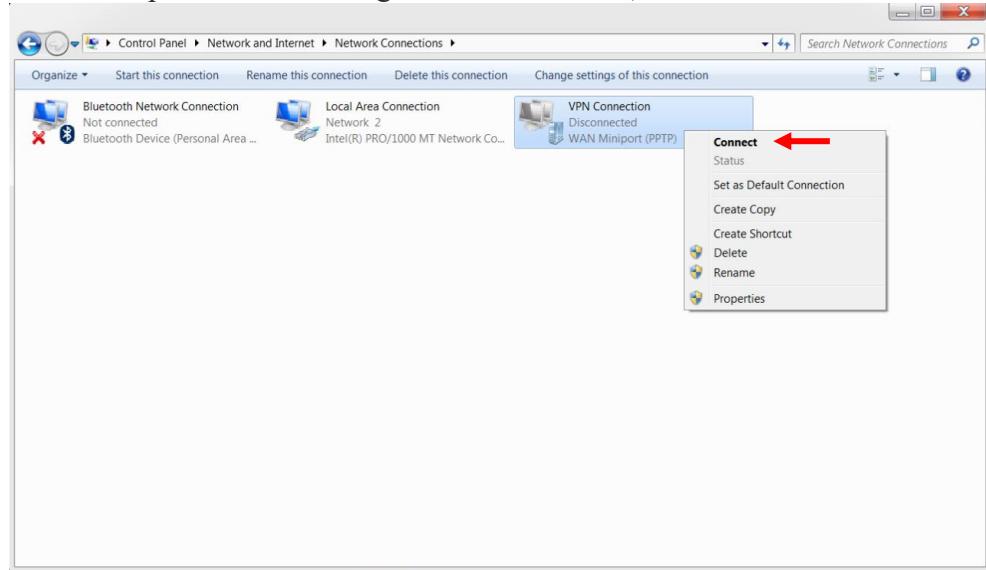
- Tại cửa sổ VPN Connection Properties, chuyển sang tab Security, tại mục Type of VPN, chọn kiểu giao thức kết nối VPN là **Point to Point Tunneling Protocol (PPTP)** → Chọn **OK**.



**Hình 2.50: Cửa sổ VPN Connection Properties**

### II.2.3.6. Kết nối và kiểm tra

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



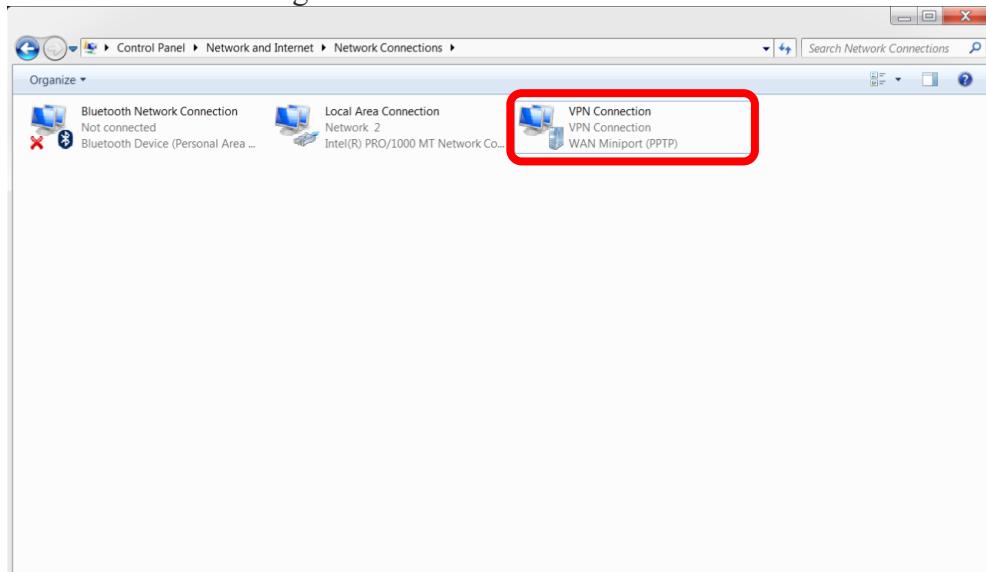
Hình 2.51: Cửa sổ Network Connections

- Nhập vào tài khoản job và mật khẩu mà ta đã tạo và cấp quyền truy cập từ xa → **Connect**



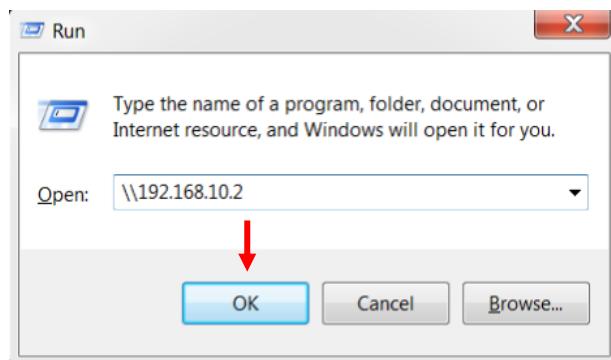
Hình 2.52: Cửa sổ Connect VPN Connection

- Kết nối VPN thành công.



**Hình 2.53: Cửa sổ Network Connections**

- Trên **VPN\_Client** mở CMD lên và gõ <\\192.168.10.2> để truy cập vào File Server và lấy tài liệu → OK



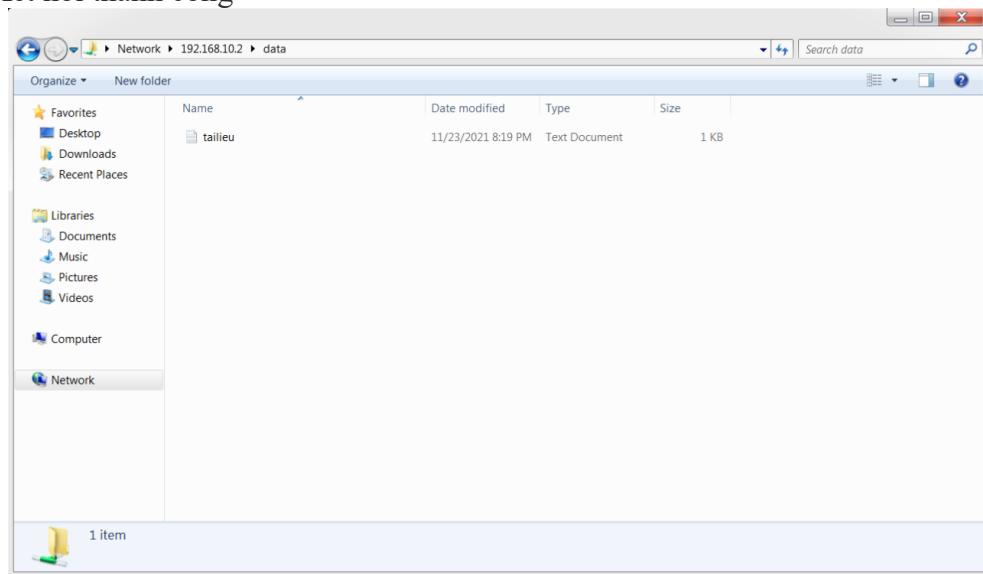
**Hình 2.54: Cửa sổ Run**

- Log in vào miền bằng tài khoản Administrator để truy cập **Folder DATA** đã tạo trên máy **DC**



**Hình 2.55: Cửa sổ Windows Security**

- Kết nối thành công



Hình 2.56: Cửa sổ folder data được kết nối từ Client sang Server

## KẾT LUẬN

Sau khi nghiên cứu và hoàn thành đề tài Terminal Services và VPN nhóm em thấy mình tự tin về thiết kế, lắp đặt hệ thống mạng doanh nghiệp nhờ việc tích lũy kiến thức – kỹ năng về TS & VPN và cũng rút ra được nhiều kinh nghiệm riêng cho mình:

Tìm hiểu những kiến thức cơ bản về mạng máy tính như mô hình mạng, giao thức mạng, các dịch vụ trên mạng, các thiết bị trong mạng LAN và WAN.

Tìm hiểu về dịch vụ **Terminal Services** và công nghệ **VPN** như các khái niệm, phân loại, các giao thức, những lợi ích, ưu và nhược điểm.

Thiết kế và cài đặt mô hình **Terminal Server** và **VPN**.

## TÀI LIỆU THAM KHẢO

- [1]. Giáo trình Mạng máy tính, Bộ môn ĐTVT – Trường CĐ KT Cao Thắng, năm 2018.
- [2]. Giáo trình Thiết kế hệ thống mạng, Bộ môn ĐTVT – Trường CĐ KT Cao Thắng, năm 2018.

The End

