**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HCM**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**BÀI TẬP LỚN/ BÀI TẬP DỰ ÁN HỌC PHẦN:**

**AN NINH HẠ TẦNG MẠNG**

**TÊN ĐỀ TÀI 6-7 :**

**SITE-TO-SITE VPN**

**REMOTE ACCESS VPN**

**NHÓM :5**

**Thành phố Hồ Chí Minh, tháng 4 năm 2022**

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HỒ CHÍ MINH**

**KHOA: CÔNG NGHỆ THÔNG TIN**

-----o0o----

****

**TÊN ĐỀ TÀI :**

**SITE-TO-SITE VPN**

**REMOTE ACCESS VPN**

|  |  |
| --- | --- |
| **Nhóm: 5**  Trưởng nhóm: Trần Minh Trí  Thành viên:  1: Đặng Hoàng Duy-2033190158  2: Đinh Phạm Quốc Quyền -2033190112  3: Giáp Đức Tài -2033192280  4:Trần Minh Trí -2033190135  5: Nguyễn Thanh Tuấn - 2033190141  6 : Phạm Huy Trường - 2033190042  7 : Trần Nguyễn Vân Quỳnh - 2033192202  8 : Nguyễn Ngọc Uyên - 2033190160 | **Giảng viên hướng dẫn:**  **Bùi Duy Cương** |

**Thành phố Hồ Chí Minh, tháng 4 năm 2022**

**BẢNG ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STT | HỌ VÀ TÊN | LỚP | MÃ SỐ SV | NỘI DUNG  PHỤ TRÁCH | MỨC ĐỘ ĐÓNG GÓP | XÁC NHẬN |
| 1 | Đặng Hoàng Duy | 10DHBM2 | 2033190158 | Thực hiện làm bài lab số 6 | **14%** | Duy |
| 2 | Đinh Phạm Quốc Quyền | 10DHBM1 | 2033190112 | Thực hiện làm bài lab số 6 | **14%** | Quyền |
| 3 | Giáp Đức Tài | 10DHBM2 | 2033192280 | Thực hiện làm bài lab số 6 và quay phim bài lab số 6 | **14%** | Tài |
| 4 | Trần Minh  Trí  (Nhóm Trưởng) | 10DHBM2 | 2033190135 | Duyệt bài , làm word. Thực hiện làm 2 bài lab 6,7 và quay phim bài lab số 6 | **16%** | Trí |
| 5 | Nguyễn Thanh Tuấn | 10DHBM2 | 2033190141 | Quay phim và tham gia làm bài lab số 7 | **14%** | Tuấn |
| 6 | Phạm Huy Trường | 10DHBM2 | 2033190042 | Tham gia làm bài lab số 7 | **12%** | Trường |
| 7 | Trần Nguyễn Vân Quỳnh | 10DHBM2 | 2033192202 | Làm word và powerpoint chỉ hoàn thiện được 70% | **8%** | Quỳnh |
| 8 | Nguyễn Ngọc Uyên | 10DHBM2 | 2033190160 | Làm word và powerpoint chỉ hoàn thiện dược 70% | **8%** | Uyên |
| **Tổng cả nhóm** | | | | | **100%** | |

**CÔNG VIỆC CỦA CÁC THÀNH VIÊN TRONG NHÓM.**

**LỜI CAM ĐOAN**

Em/ chúng em xin cam đoan đề tài do cá nhân/nhóm em nghiên cứu và thực hiện.

Em/ chúng em đã kiểm tra dữ liệu theo quy định hiện hành.

Kết quả bài làm của đề tài là trung thực và không sao chép từ bất kỳ bài tập của nhóm khác.

Các tài liệu được sử dụng trong tiểu luận có nguồn gốc, xuất xứ rõ ràng.

**(Ký và ghi rõ họ tên )**

**LỜI CẢM ƠN**

Lời đầu tiên chúng em xin gửi lời cảm ơn chân thành đến quý thầy,cô giáo trong khoa Công nghệ Thông Tin trường Đại học Công nghiệp thực phẩm Tp Hồ Chí Minh đã truyền đạt kiến thức và kinh nghiệm quý báu cho chúng em trong suốt quá trình học tập và rèn luyện .

Đặc biệt chúng em xin gởi lời cảm ơn đến thầy Bùi Duy Cương , người đã trực tiếp hướng dẫn và tận tình giúp đỡ chúng em trong suốt thời gian học môn “An ninh hạ tầng mạng” cũng như trong thời gian chúng em thực hiện thực bài tập kết thúc môn học.

Mặc dù đã cố gắng trong quá trình làm bài nhưng không thể tránh khỏi những sai sót. Chúng em mong nhận được sự góp ý,nhận xét của quý thầy cô và các bạn về nội dung cũng như hình thức trình bày để bài báo cáo được hoàn thiện.

Chúng em xin chân thành cảm ơn thầy cô và các bạn đã xem.

MỤC LỤC

[**PHẦN MỞ ĐẦU** 1](#_Toc101958848)

[**PHẦN NỘI DUNG** 2](#_Toc101958849)

[**1.** **Tìm hiểu tổng quan về VPN** 2](#_Toc101958850)

[1.1. Định nghĩa 2](#_Toc101958851)

[1.2. Chức năng của VPN 2](#_Toc101958852)

[1.3. Các tình huống thông dụng của VPN 2](#_Toc101958853)

[1.4. Lợi ích của VPN 3](#_Toc101958854)

[**2. Site to Site VPN** 3](#_Toc101958855)

[2.1. Mô hình sơ lược về Site to Site VPN 3](#_Toc101958856)

[2.2. Ứng dụng Site to Site VPN trong thực tế 4](#_Toc101958860)

[**3.** **Remote Access VPN** 6](#_Toc101958861)

[3.1. Định nghĩa 6](#_Toc101958862)

[3.2. Ưu điểm và nhược điểm của Remote Access VPN 6](#_Toc101958867)

[4.1. Bài thực số 6 Site to Site VPN 7](#_Toc101958875)

[4.2. Bài thực hành số 7 Remote Access VPN 35](#_Toc101958876)

[TÀI LIỆU THAM KHẢO 65](#_Toc101958877)

# **PHẦN MỞ ĐẦU**

Trong thời đại công nghiệp 4.0 hiện nay, thì vai trò của Công nghệ Thông tin nói chung và Internet nói riêng ngày càng vô cùng quan trọng. Điều này kéo theo đa phần các doanh nghiệp, công ty hay các tổ chức đều phải phụ thuộc vào máy vi tính. Nhu cầu truy cập từ xa (ngoài văn phòng công ty) để làm việc cũng ngày càng phổ biến. Đó là nhu cầu rất thiết thực, giúp con người chủ động hơn trong công việc**, cho phép bạn tạo kết nối an toàn đến một mạng khác qua Internet. VPN có thể được sử dụng để truy cập các trang web bị giới hạn theo khu vực, bảo vệ hoạt động duyệt web của bạn khỏi những con mắt tò mò trên Wi-Fi công cộng…** Để đáp ứng được các nhu cầu đó VPN đã ra đời.

Để hiểu rõ hơn về các tính năng cũng như cách thức áp dụng công cụ này thì trong bài báo cáo này chúng em sẽ mang đến cái nhìn tổng quan hơn cũng như tác dụng rõ ràng và kèm đó là hướng dẫn sử dụng một cách cơ bản và dễ hiểu nhất về VPN.

Từ những lí do trên, chúng em quyết định lựa chọn đề tài cho cuối kì là “Site to Site VPN – Remote Access VPN”.

Phạm vi nghiên cứu của đề tài lần này của em/chúng em là về Remote Access VPN , Site-to-Site VPN

Phương pháp nghiên cứu đề tài của em/chúng em là tham khảo tài liệu , suy nghĩ chủ động và thực hiện được nội dung đã tham khảo và từ đó cải thiện nội dung của đề tài .

Chúng em xin chân thành cảm ơn thầy Bùi Duy Cương, người đã hướng dẫn trong quá trình thực hiện đề tài.

# **PHẦN NỘI DUNG**

1. **Tìm hiểu tổng quan về VPN**
   1. Định nghĩa

Virtual Private Network (VPN) hay còn gọi là mạng riêng ảo là một mạng dành riêng để kết nối các máy tính công ty hoặc tập đoàn với nhau thông qua mạng công cộng. Mạng riêng ảo thường được triển khai trong qua mạng Intenet. Để tạo ra kênh truyền ảo riêng trên mạng công cộng, công nghệ mạng riêng ảo sử dụng giải pháp đồng bộ hóa kết nối riêng và bảo vệ gói tin (thường là mã hóa).

* 1. Chức năng của VPN

VPN cung cấp ba chức năng chính đó là:

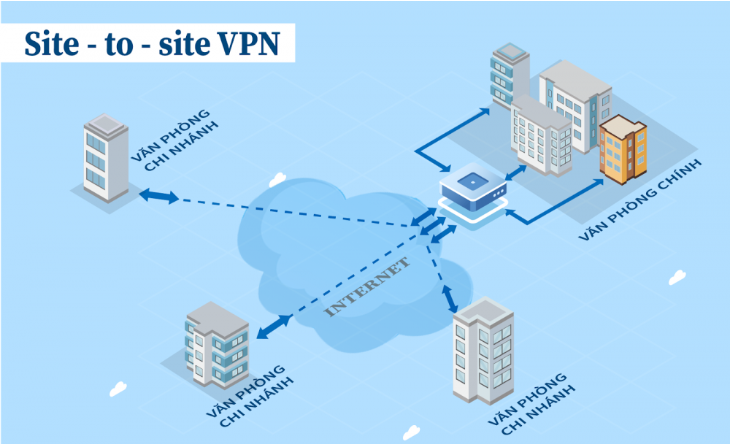
* **Tính xác thực** (Authentication): Để thiết lập một kết nối VPN thì trước hết cả hai phía phải xác thực lẫn nhau để khẳng định rằng mình đang trao đổi thông tin với người mình mong muốn chứ không phải là một người khác.
* **Tính toàn vẹn** (Integrity): Đảm bảo dữ liệu không bị thay đổi hay đảm bảo không có bất kỳ sự xáo trộn nào trong quá trình truyền dẫn.
* **Tính bảo mật** (Confidentiality): Bên gửi có thể mã hoá các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở bên thu. Như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu có lấy được thì cũng không đọc được.
  1. Các tình huống thông dụng của VPN
* Site to Site VPN: Áp dụng cho các tổ chức có nhiều văn phòng chi nhánh, giữa các văn phòng cần trao đổi dữ liệu với nhau. Ví dụ một công ty đa quốc gia có nhu cầu chia sẻ thông tin giữa các chi nhánh đặt tại Singapore và Việt Nam, có thể xây dựng một hệ thống VPN Site-to-Site kết nối hai site Việt Nam và Singapore tạo một đường truyền riêng trên mạng Internet phục vụ quá trình truyền thông an toàn, hiệu quả.
* Remote Access VPN: Đáp ứng nhu cầu truy cập dữ liệu và ứng dụng cho người dùng ở xa, bên ngoài công ty thông qua Internet. Ví dụ khi người dùng muốn truy cập vào cơ sở dữ liệu hay các file server, gửi nhận email từ các mail server nội bộ của công ty.
  1. Lợi ích của VPN
* **Tiết kiệm chi phí**: Chi phí cho VPN ít hơn rất nhiều so với các giải pháp truyền thống dựa trên đường Lease-Line như Frame Relay, ATM hay ISDN. Bởi vì VPN loại trừ được những yếu tố cần thiết cho các kết nối đường dài bằng cách thay thế chúng bởi các kết nối cục bộ tới ISP hoặc điểm đại diện của ISP.
* **Giảm được chi phí thuê nhân viên và quản trị**: Giảm được chi phí truyền thông đường dài. Tổ chức không cần thuê nhiều nhân viên mạng cao cấp.
* **Tính linh hoạt**: điểu chỉnh kiến trúc triển khai mạng và công nghệ mạng dễ dàng.
* **Khả năng mở rộng**: Do VPN được xây dựng dựa trên cơ sở hạ tầng mạng công cộng (Internet), bất cứ ở nơi nào có mạng công cộng là đều có thể triển khai VPN.
* **Giảm thiểu các hỗ trợ kỹ thuật**: Các nhà cung cấp dịch vụ có trách nhiệm vụ hỗ trợ hạ tầng mạng.
* **Bảo mật các giao dịch**: Dữ liệu truyền được bảo mật sử dụng công nghệ đường hầm sử dụng các biện pháp bảo mật như: Mã hoá, xác thực và cấp quyền để bảo đảm an toàn, tính tin cậy, tính xác thực của dữ liệu được truyền, Kết quả là VPN mang lại mức độ bảo mật cao cho việc truyền tin.
* **Sử dụng hiệu quả băng thông**: giảm lãng phí băng thông của hạ tầng mạng.
* **Giảm thiểu các yêu cầu về thiết bị**
* **Đáp ứng các nhu cầu thương mại**

**2. Site to Site VPN**

2.1. Mô hình sơ lược về Site to Site VPN

Là mô hình dùng để kết nối các hệ thống mạng ở các nơi khác nhau tạo thành mộthệ thống mạng thống nhất. Ở loại kết nối này thì việc chứng thực an đầu phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi

nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site.



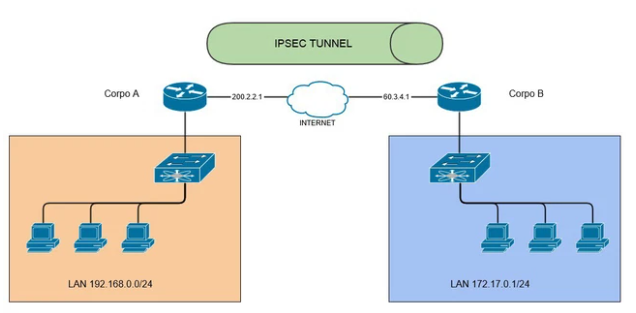
*Hình 1. Kết nối các hệ thống mạng từ các văn phòng*

2. 2. Ứng dụng Site to Site VPN trong thực tế

VPN site to site giúp giải quyết khá nhiều các bài toán thực tế, khi mà các doanh nghiệp cần đến các kết nối an toàn, bảo mật để kết nối các mạng nội bộ với nhau.

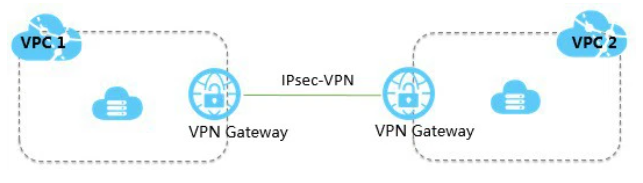
Điển hình như:

* **Kết nối mạng nội bộ của 2 hay nhiều Datacenter với nhau:** Kết nối mạng giữa các Datacenter được sử dụng rất nhiều, khi các doanh nghiệp có máy chủ chạy dịch vụ đặt tại các DC khác nhau để tăng tính dự phòng hay để làm DR (Disaster Recovery) để phòng trừ thảm họa. Khi đó, họ sẽ cần có giải pháp để kết nối mạng nội bộ giữa các DC đó với nhau, để các máy chủ tại các DC có thể giao tiếp thông qua mạng nội bộ trực tiếp với nhau thay vì thông qua internet. VPN site to site sẽ giúp giải quyết bài toán kết nối này.



*Hình 2. Mô hình VPN*

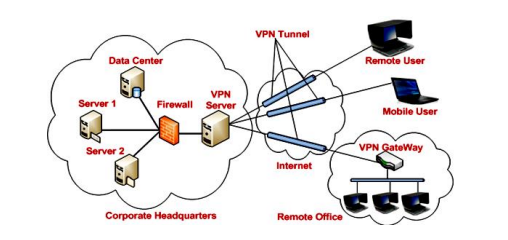
* **Kết nối mạng nội bộ giữa các trụ sở chi nhánh và trụ sở chính**: Một ứng dụng thực nữa của VPN site to site đó là việc kết nối mạng văn phòng của các trụ sở chi nhánh với nhau và với trụ sở chính để các chi nhánh có thể truy cập vào các tài nguyên dùng chung đặt tại trụ sở chính thông qua đường truyền an toàn, bảo mật thay vì internet, hay để các nhân viên tại các chi nhánh có thể trao đổi dữ liệu với nhau 1 cách dễ dàng.
* **Kết nối giữa các VPC của các Cloud Provider với nhau, trong mô hình sử dụng Multi Cloud của các doanh nghiệp:** Hiện nay việc chạy các ứng dụng trên các máy chủ ảo Cloud đã rất phổ biến. Cũng giống như việc đặt máy chủ vật lý tại nhiều Datacenter khác nhau, các doanh nghiệp có thể chạy dịch vụ trên các máy chủ ảo Cloud của nhiều các Cloud Provider khác nhau. Và từ mô hình đó cũng sẽ nảy sinh nhu cầu cần kết nối mạng nội bộ Cloud (VPC) của các Cloud Provider với nhau để trao đổi dữ liệu. VPN site to site cũng được áp dụng để giải quyết bài toán này.



*Hình 3. Kết nối giữa các VPC của các Cloud Provider với nhau*

1. **Remote Access VPN**
   1. Định nghĩa

Là một dạng Client-to-Site cho phép truy cập từ xa bất cứ lúc nào bằng thiết bị truyền thông (Laptop, điện thoại). Do nhu cầu của một tổ chức, có nhiều nhân viên cần kết nối với mạng riêng của mình khi đi làm việc ở xa hay làm việc tại nhà nên mô hình này được sinh ra.



*Hình 4. Mô hình Remote Access VPN*

3. 2. Ưu điểm và nhược điểm của Remote Access VPN
      1. Ưu điểm

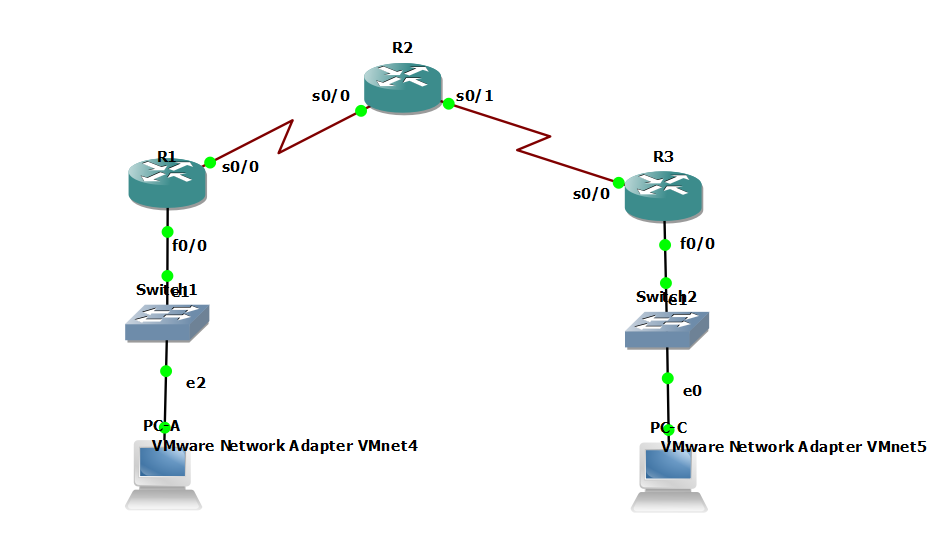
* Việc thay thế Remote Access VPN thì hệ thống không cần phần RAS và các thành phần modem liên quan mà thay vào đó là VPN server.
* Không cần sự hỗ trợ từ hệ thống do kết nố từ xa được thực hiện bởi dịch vụ cung cấp mạng ISP.
* Kết nối quay số Dial-up từ khoảng cách xa cũng được loại bỏ, thay vào đó là các kết nối cục bộ.
* Giảm giá thành chi phí khi kết nối ở khoảng cách xa.

3. 2. 2. Nhược điểm

* Chưa thực sự đảm bảo được chất lượng của dịch vụ.
* Khả năng bị mất dữ liệu cũng là khá cao, đồng thời gói tin chuyển đi có thể bị phân mảnh, mất trật tự.
* Khi thực hiện truyền gói dữ liệu thông qua mạng công cộng thì sẽ gây ra nhiều khó khăn với những gói dữ liệu lớn như là phim ảnh, âm thanh,...

1. **Triển khai thực hành VPN**
2. 1. Bài thực số 6 Site to Site VPN

Mô hình bài lab :

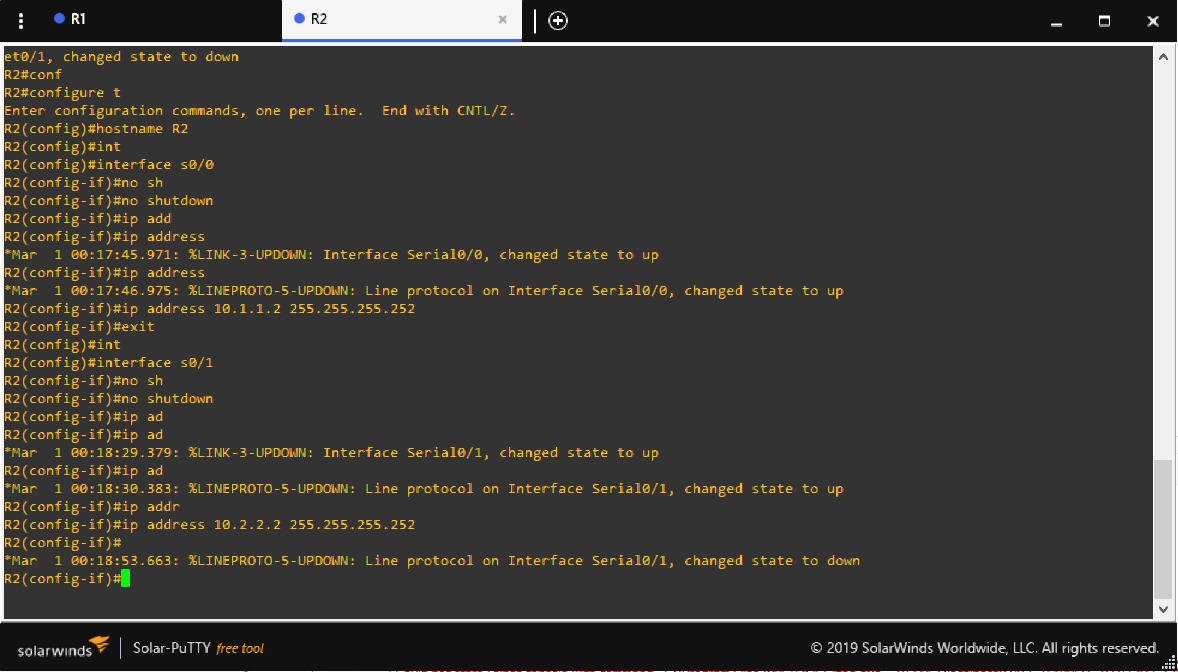


Mô tả kịch bản của bài lab : Bài lab thực hiện cấu hình Site to Site VPN để giúp cho truy cập từ xa từ site này đến site khác trên Internet bằng cách tạo ra đường đi mã hóa cho cả 2 site và sẽ được giấu đi đường đi khiến cho việc kẻ xấu cố ý truy cập vào lấy dữ liệu sẽ khá là khó khăn vì không nhìn thấy được đường đi của mình. Router R1 và Router R3 sẽ trở thành 2 cổng site chính để kết nối 2 site và Router R2 sẽ là đường đi trung gian và bị ẩn đi không thấy được đây chính là VPN mà khi di chuyển từ site R1 qua site R3 và ngược lại.Ta sẽ mã hóa đường đi bằng thuật toán AES và sử dụng khóa chia sẻ theo kiểu đối xứng dùng khóa bí mật để làm khóa chia sẻ và ta sẽ thực hiện giao thức trao đổi khóa Diffie-Hellman, giao thức chính được sử dụng để kết nối site to site trong bài này là ESP.Ta sẽ tracert từ PC-A qua PC-C ,PC-A sẽ đi qua cổng fast của R1 và đi qua cổng Se0/0 của R3 và tới địa chỉ của R3 tương tự vậy cho việc đi từ PC-C qua PC-A, ta sẽ chặn tất cả các ip không thuộc vùng dữ liệu từ R1-R3 và R3-R1 khi cấu hình 2 router này bằng Access-list quản lý khả năng truy cập và ta cũng tạo 1 crypto map để thành 1 bản đồ mã hóa cho đường đi của cả 2 site và sử dụng cổng serial để site sẽ đảm bảo tốt hơn trong việc truyền dữ liệu ổn định và 2 cổng fast làm 2 cổng tới 2 PC. Mục tiêu của bài là hoàn thành cấu hình site to site và kiểm thử xem là site to site có hoạt động hay không bằng lệnh tracert hoặc ping sau đó ta sẽ kiểm tra gói tin bằng wireshark.

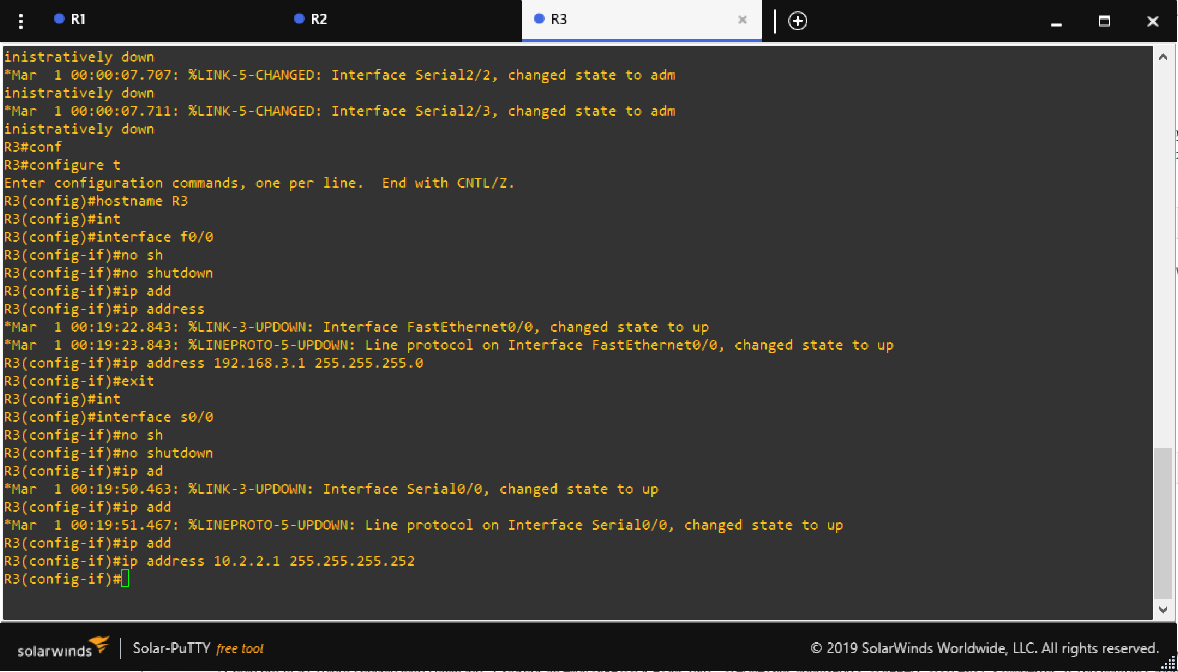
Phần 1 : Cấu hình thiết bị (router và host) cơ bản :



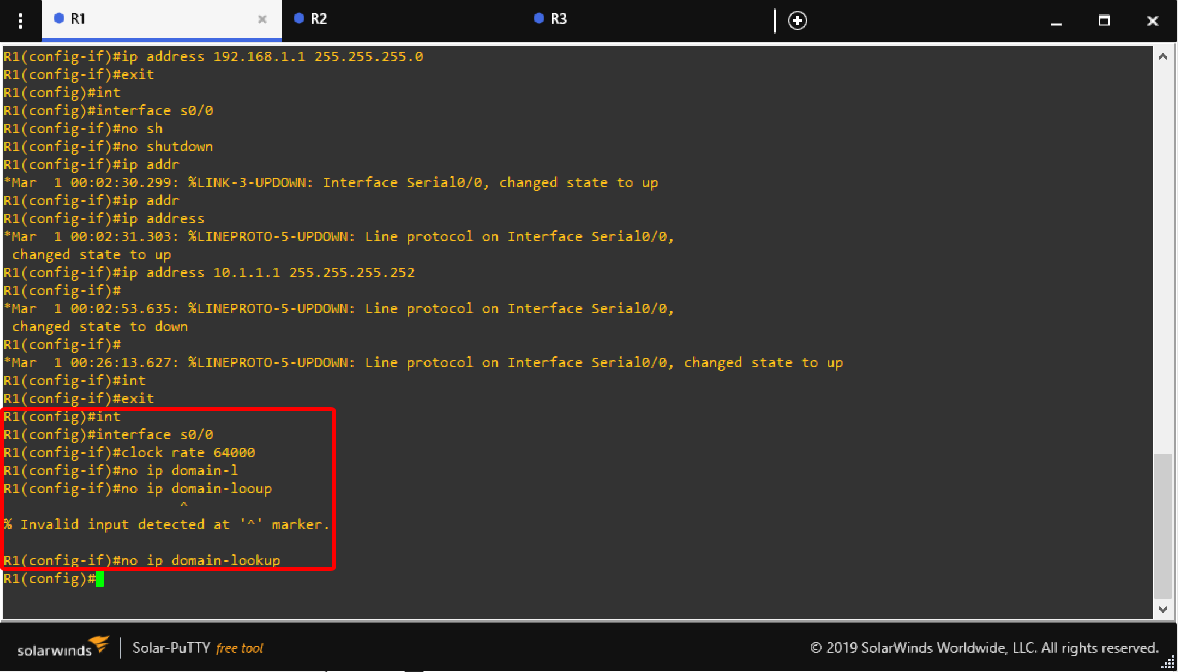
*Hình 5 : Cấu hình hostname và địa chỉ ip cho R1*



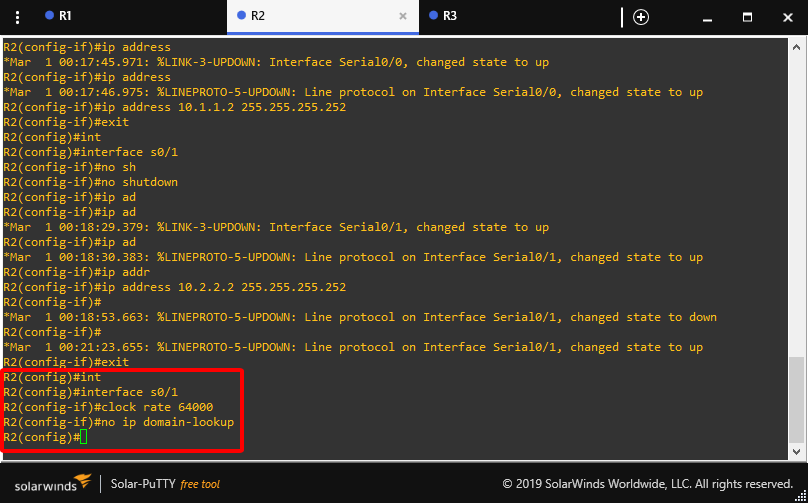
*Hình 6 : Cấu hình hostname và địa chỉ ip cho R*



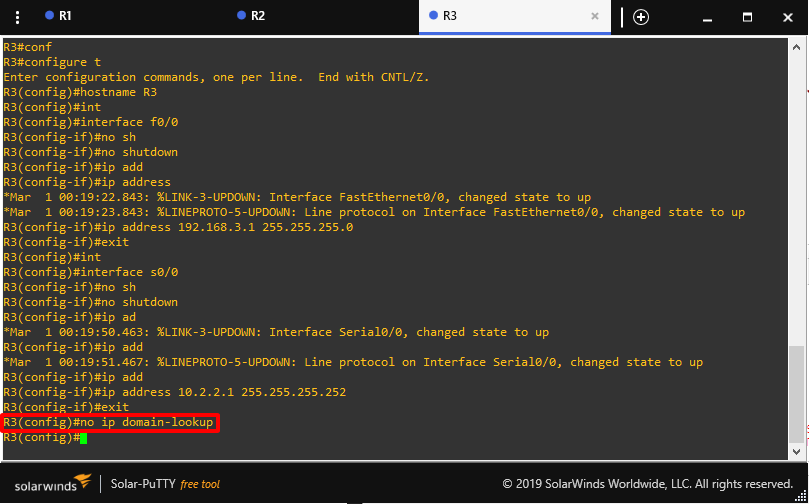
*Hình 7 : Cấu hình hostname và địa chỉ ip cho R1*



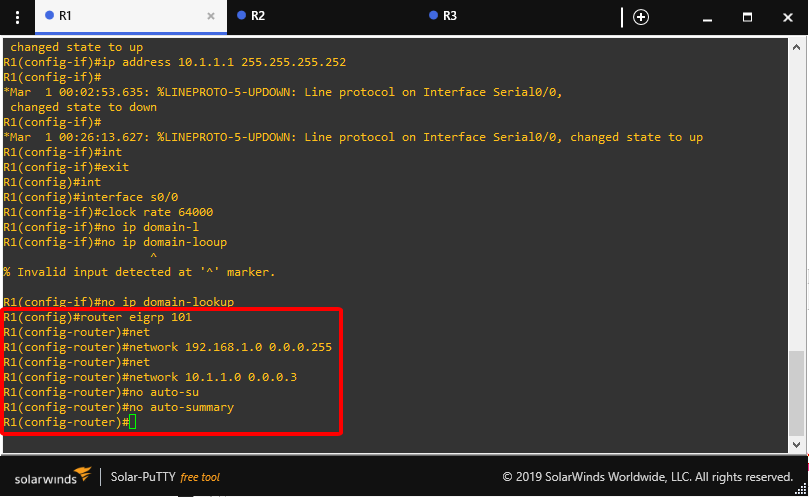
*Hình 8 : Cấu hình một xung nhịp cho cổng serial của R1 trên cổng s0/0 và vô hiệu hóa tra cứu DNS*

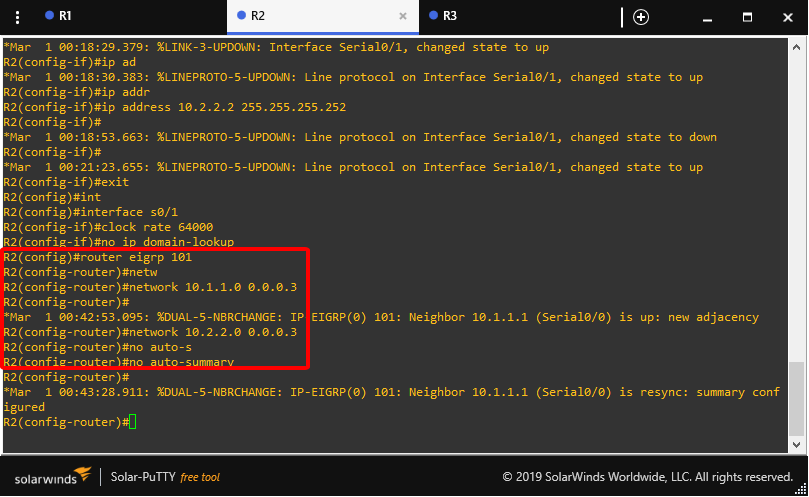


*Hình 9 : Cấu hình một xung nhịp cho cổng serial của R2 trên cổng s0/1 và vô hiệu hóa tra cứu DNS*



*Hình 10 : Vô hiệu hóa tra cứu DNS trên R3*

*Hình 11: Cấu hình giao thức định tuyến EIGRP cho R1*



*Hình 12: Cấu hình giao thức định tuyến EIGRP cho R2*

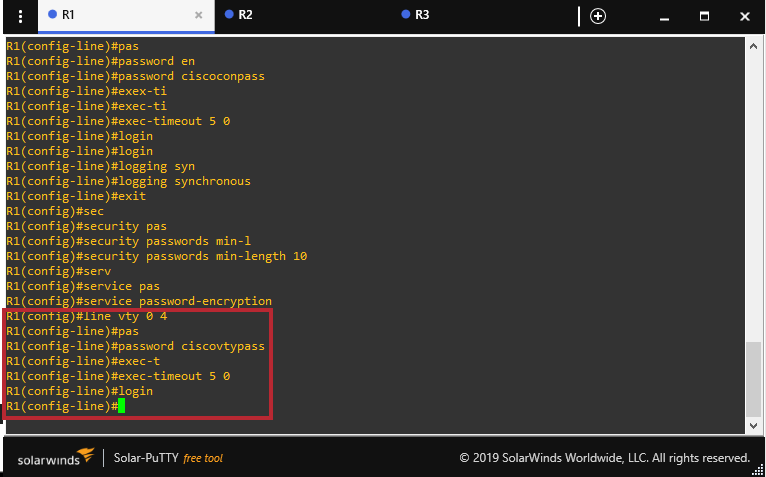
*Hình 13: Cấu hình giao thức định tuyến EIGRP cho R2*



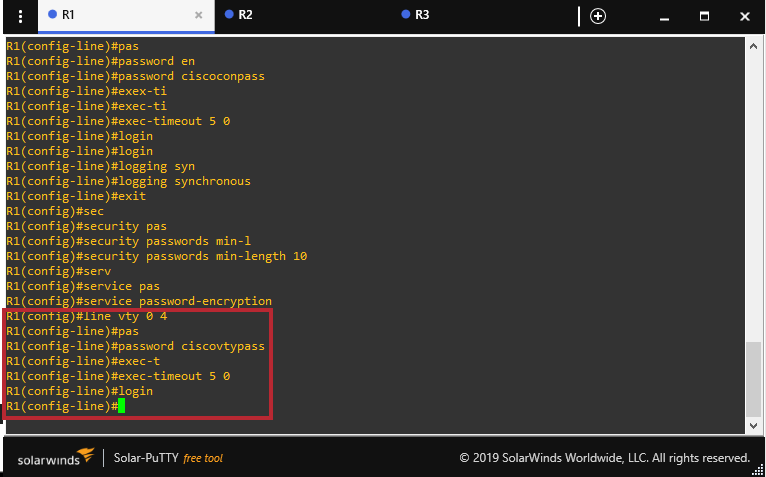
*Hình 14: Cấu hình độ dài mật khẩu và mã hóa mật khẩu cho R1*



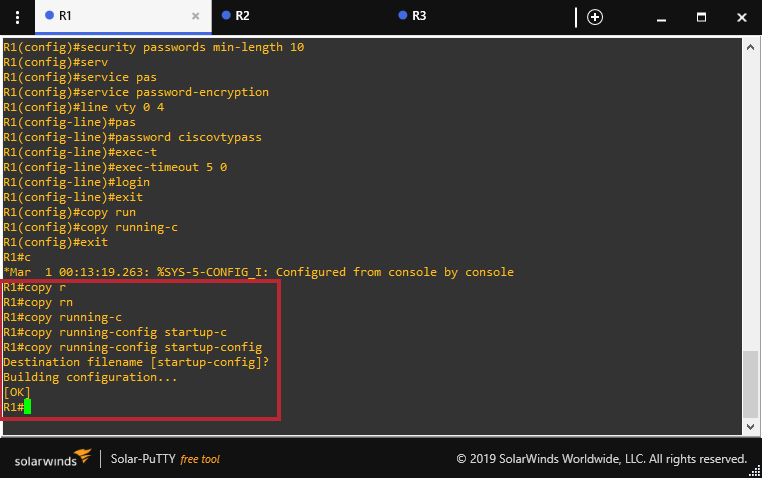
*Hình 15 : Cấu hình mật khẩu console và timeout- thời gian đăng nhập cho R1*



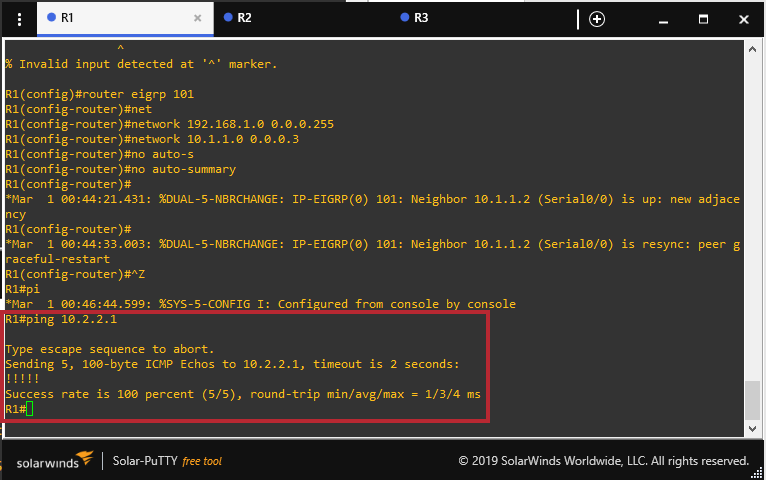
*Hình 16: Cấu hình mật khẩu trên đường vtp cho R1*



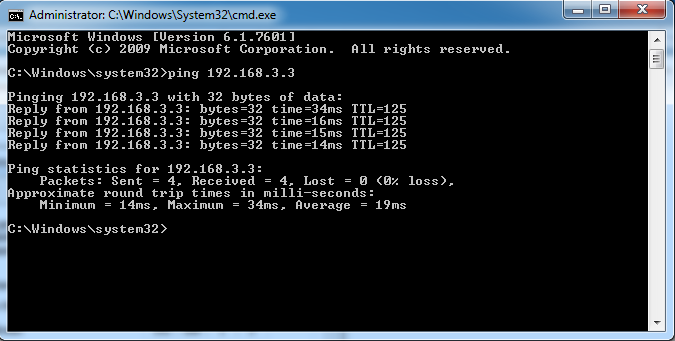
*Hình 17: Cấu hình mật khẩu trên đường vtp cho R1*



*Hình 18 :Lưu cấu hình cho R1*



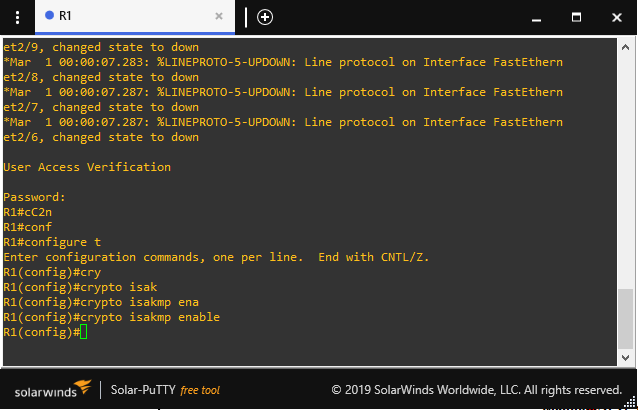
*Hình 19 : Kiểm tra kết nối từ R1 tới R3*



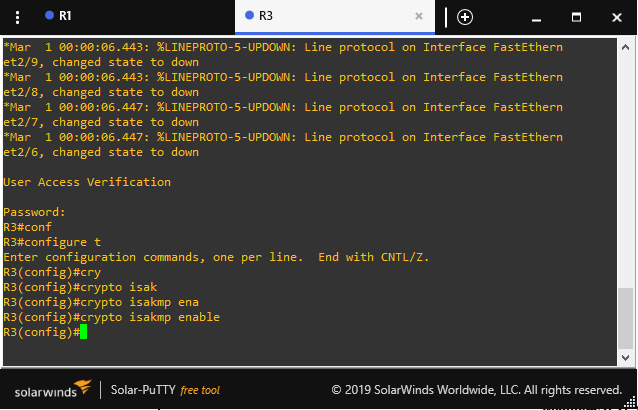
*Hình 20 : Kiểm tra kết nối từ PC-A đến PC-C*

**Phần 2: Cấu hình site-to-site VPN sử dụng Cisco IOS**

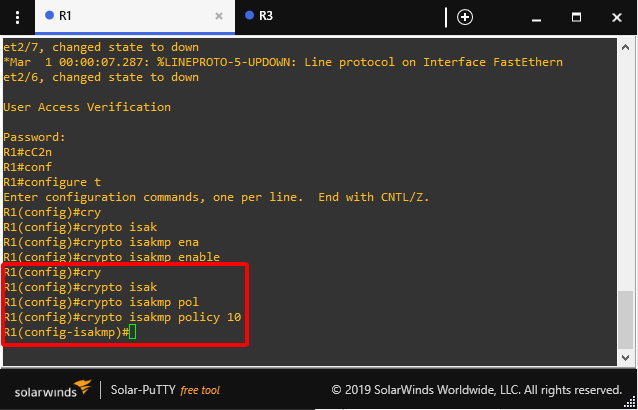
**Cấu hình IPsec VPN thiết lập trên R1 và R3**

**

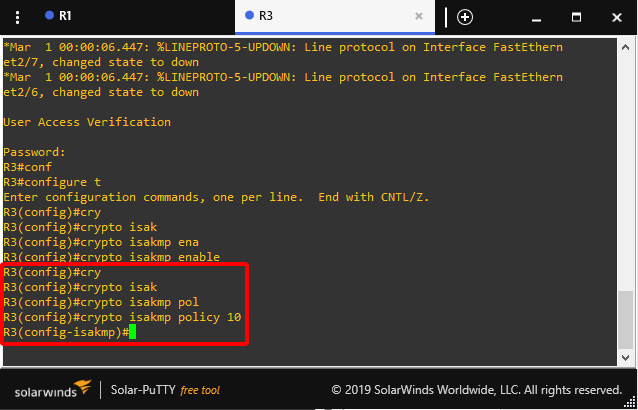
*Hình 21: Xác minh mã hóa chính sách isak cho R1*



*Hình 22 : Xác minh mã hóa chính sách isak cho R3*



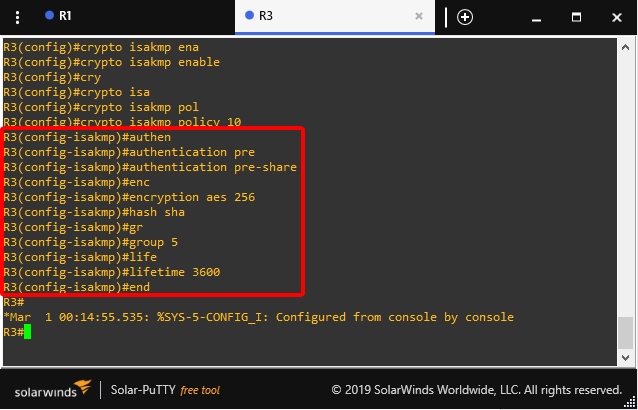
*Hình 23: Cấu hình mã hóa isakmp cho policy 10 trên R1*



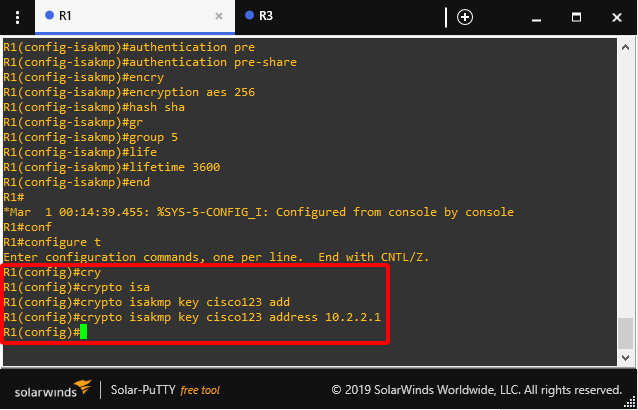
*Hình 24: Cấu hình mã hóa isakmp cho policy 10 trên R3*



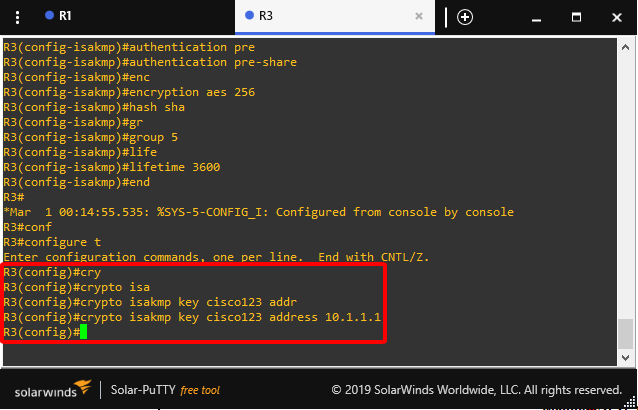
*Hình 25: Cấu hình thông số cho policy isakmp trên R1*



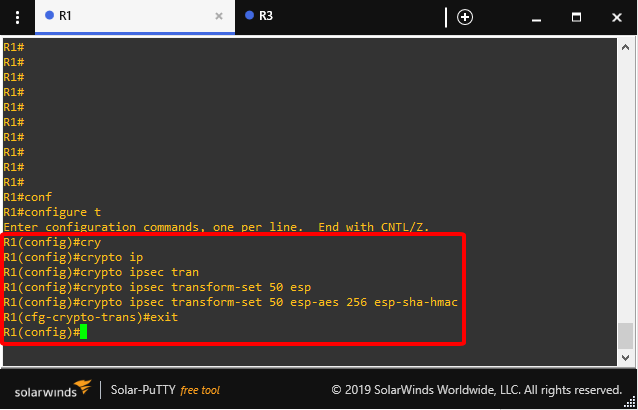
*Hình 26: Cấu hình thông số cho policy isakmp trên R3*



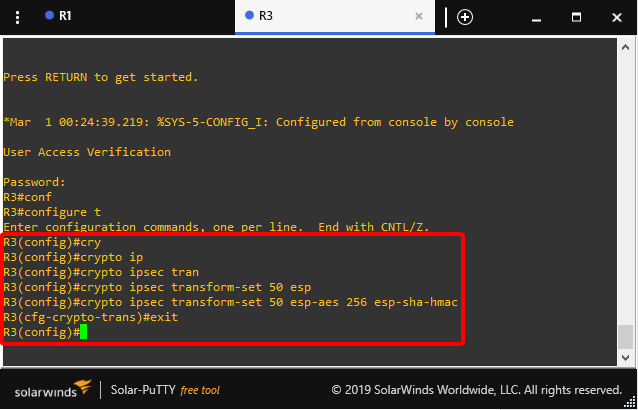
*Hình 27: Trên R1 cấu hình khóa chia sẻ trỏ đến S0/0 trên R3*



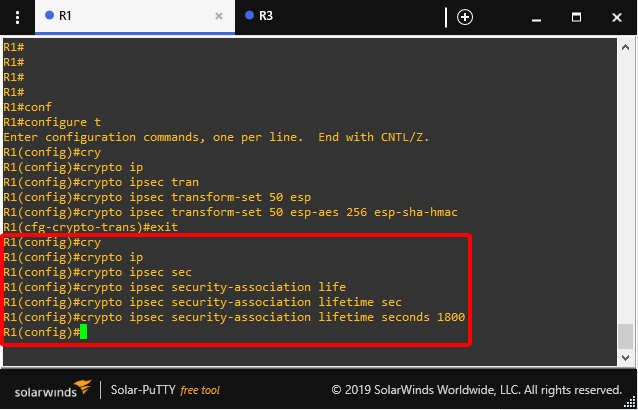
*Hình 28: Trên R3 cấu hình khóa chia sẻ trỏ đến S0/0 trên R1*



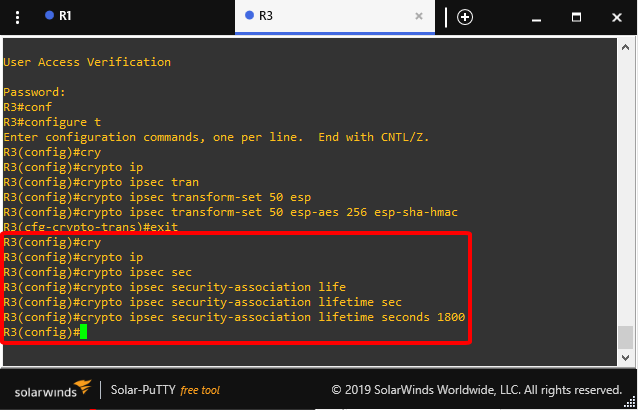
*Hình 29 : Cấu hình Ipsec transform set trên R1*



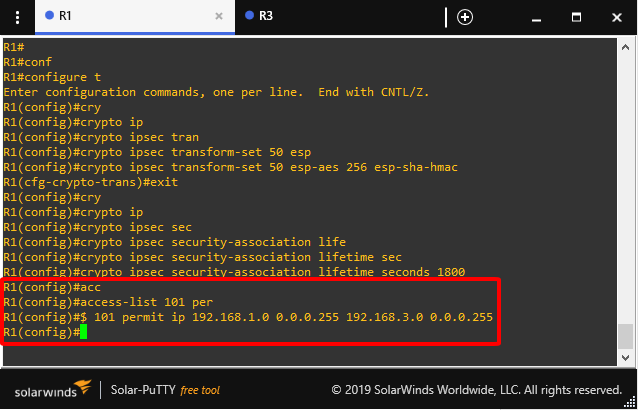
*Hình 30 : Cấu hình Ipsec transform set trên R3*



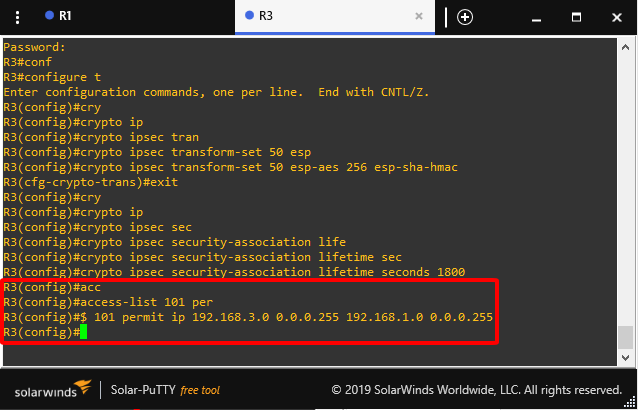
*Hình 31: Cấu hình life times trên R1*



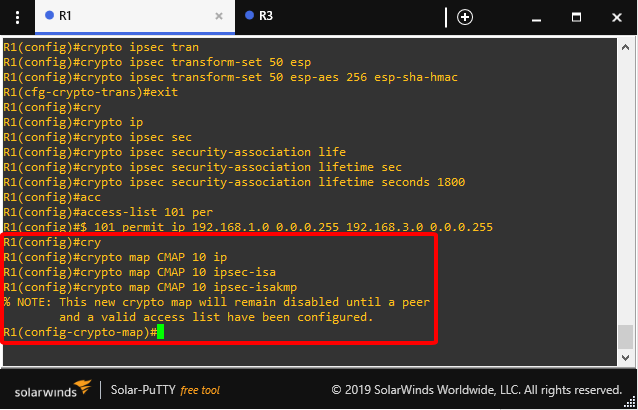
*Hình 32 : Cấu hình life times trên R3*



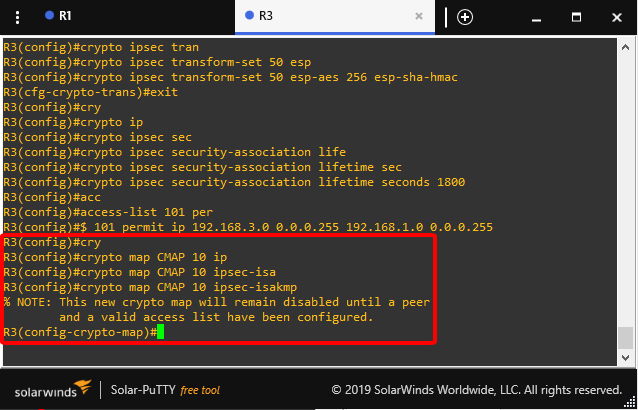
*Hình 33: Cấu hình ACL những lưu lượng quan trọng trên R1*



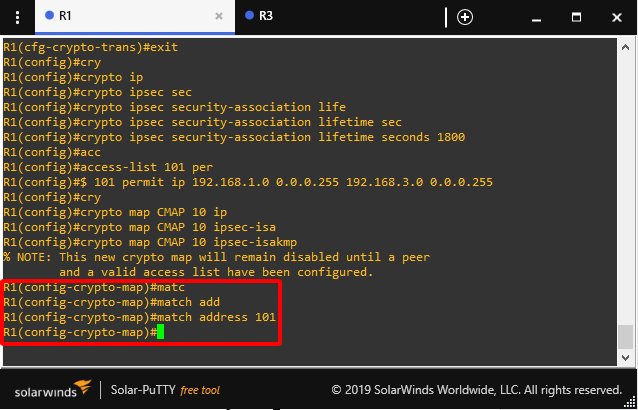
*Hình 34: Cấu hình ACL những lưu lượng quan trọng trên R3*



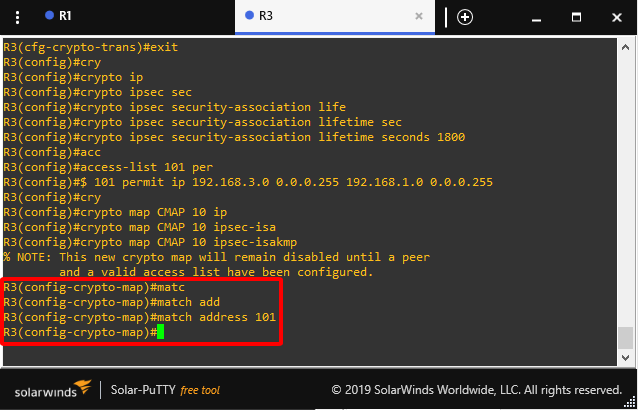
*Hình 35: Tạo một crypto map tên là CMAP và số thứ tự là 10 trên R1*



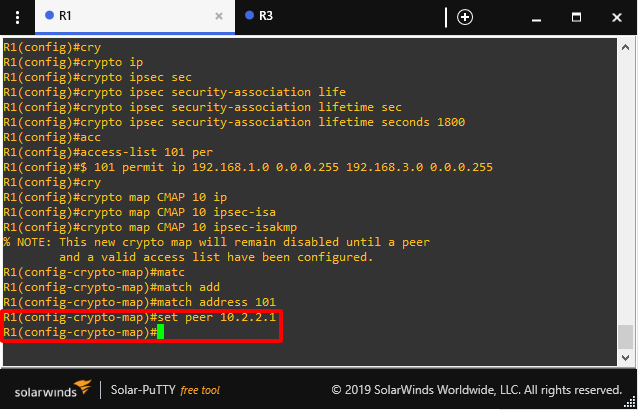
*Hình 36: Tạo một crypto map tên là CMAP và số thứ tự là 10 trên R3*



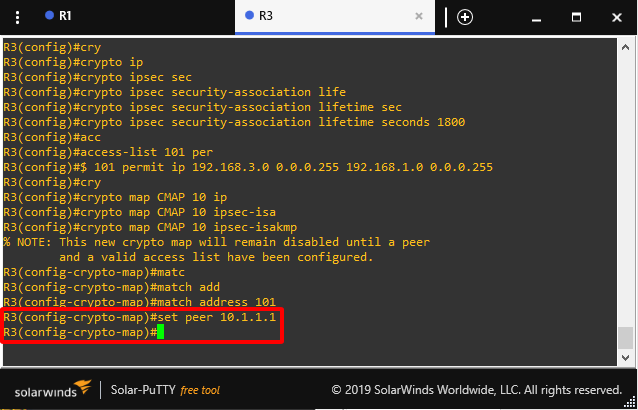
*Hình 37:Xác định danh sách ACL đã tạo cho R1*



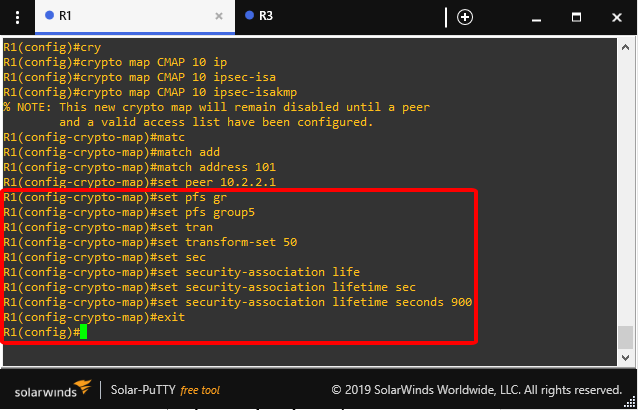
*Hình 38: Xác định danh sách ACL đã tạo cho R3*



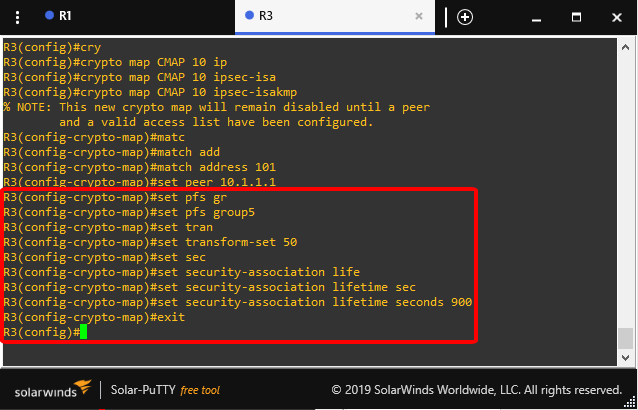
*Hình 39: Thiết lập peer ip cổng S0/0 R3 cho R1*



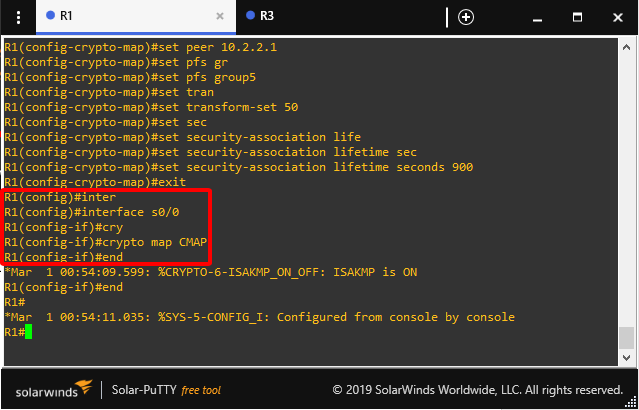
*Hình 40: Thiết lập peer ip cổng S0/0 R1 cho R3*



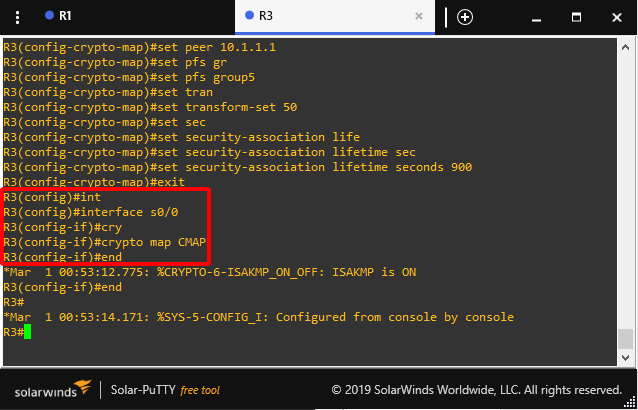
*Hình 41: Cấu hình cứng transfrom để sử dụng với peer này trên R1*



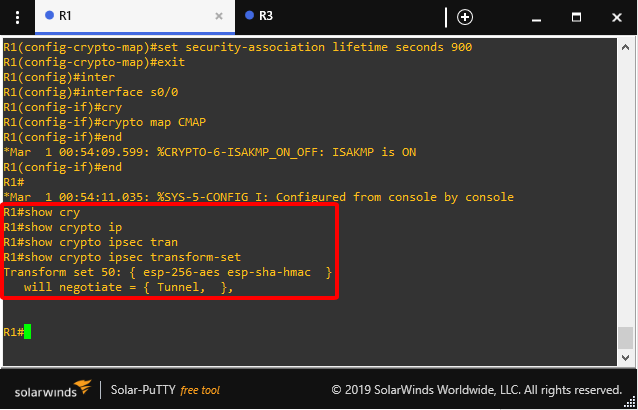
*Hình 42: Cấu hình cứng transfrom để sử dụng với peer này trên R3*



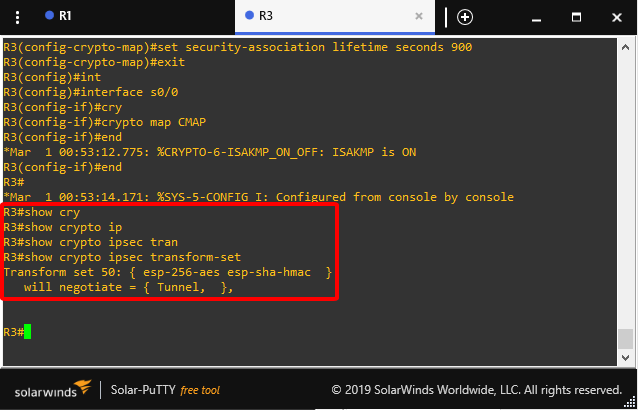
*Hình 43: Áp dụng các crypto map tới cổng S0/0 trên R1*



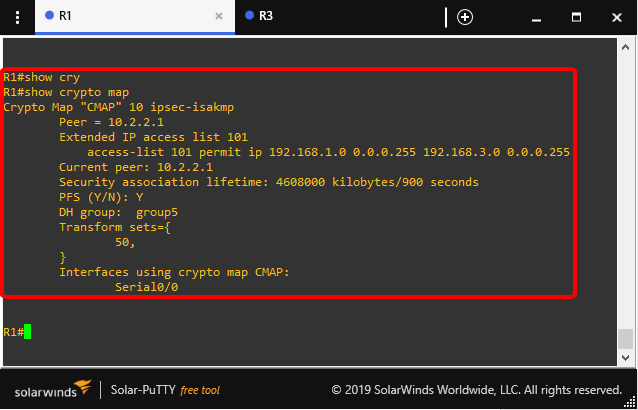
*Hình 44: Áp dụng các crypto map tới cổng S0/0 trên R3*



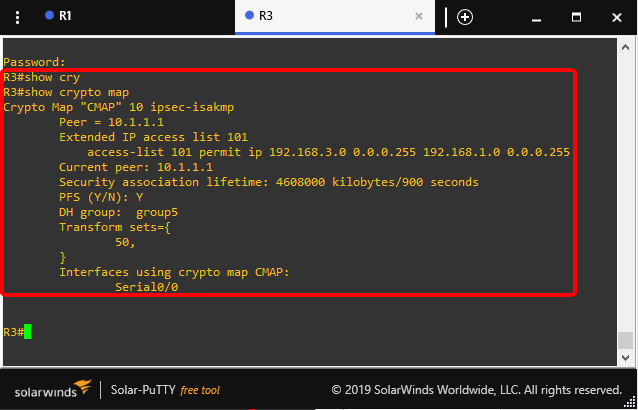
*Hình 45: Kiểm tra cấu hình ipsec trên R1*



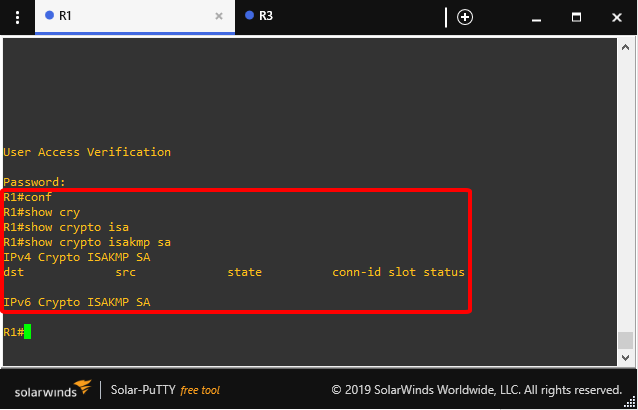
*Hình 46: Kiểm tra cấu hình ipsec trên R3*



*Hình 47: Kiểm tra các crypto trên map được áp dụng đến R1*



*Hình 48: Kiểm tra các crypto trên map được áp dụng đến R3*



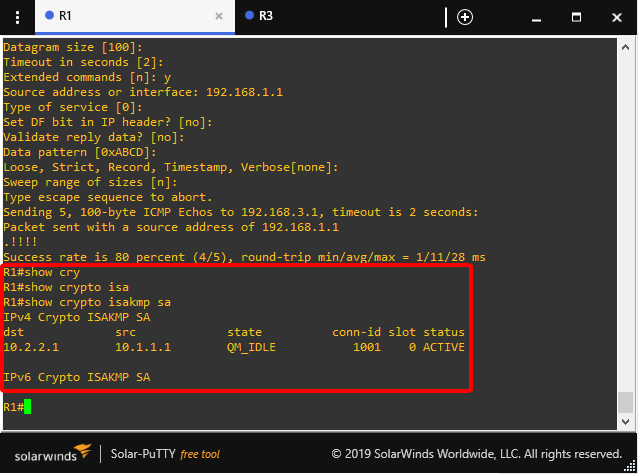
*Hình 49: Kiểm tra hoạt động của isakmp sa trên R1 khi chương có gửi lưu lượng đi*



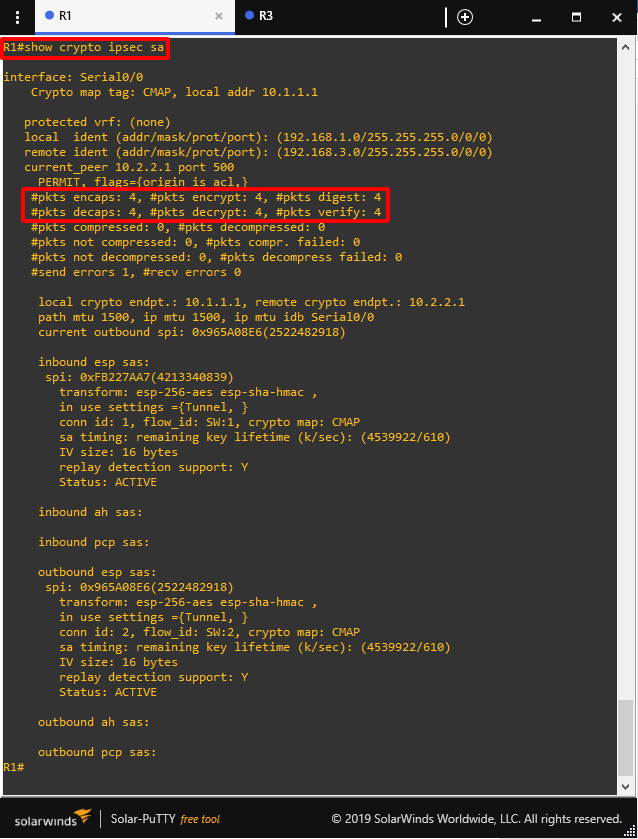
*Hình 50: Kiểm tra lưu lượng của Ipsec trên R1 khi chưa được sử dụng*



*Hình 51: Ta gửi lưu lượng từ R1 sang cổng F0/0 của R3*



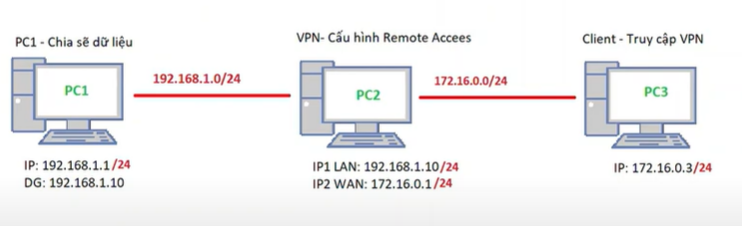
*Hình 52 :Thực kiểm tra lại lưu lượng isakmp sau khi gửi gói tin trên R1*



*Hình 53: Ta kiểm tra số gói tin được từ R1 qua R3*

* 1. Bài thực hành số 7 Remote Access VPN

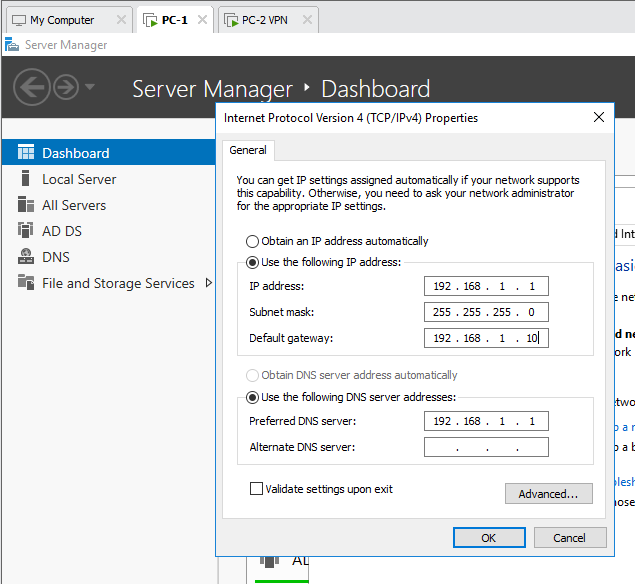
Mô hình bài lab :



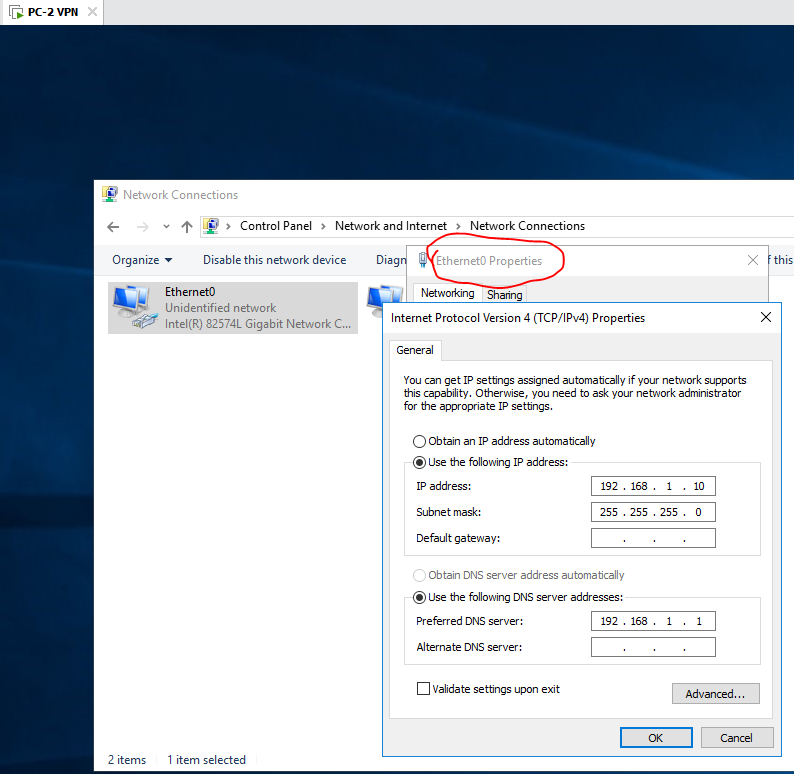
Mô tả kịch bản : Ta sẽ thực hiện cấu hình domain cho PC1 để PC2 join vào domain này từ đó PC2 sẽ tạo ra site VPN cho PC3 là máy client truy cập vào site ,sau đó PC3 sẽ dùng user đã tạo ở PC1 đăng nhập vào từ xa để lấy tài liệu – kịch bản được dựa trên một công ty chỉ có 1 trụ sở ở Hà Nội và khi người đó đi công tác ra Tp Hồ Chí Minh thì cần truy cập về máy tính của công ty lấy tài liệu thì lúc này mô hình Client to site đáp ứng điều đó PC1 – là máy tính của người này ở công ty , PC-2 là máy server của công ty là VPN site , PC-3 là máy laptop client của người này khi mang đi công tác.

Lưu ý : PC-2 sử dụng 2 card mạng , 1 card để truy cập domain qua PC-1 và 1 card để tạo site cho PC-3 kết nối

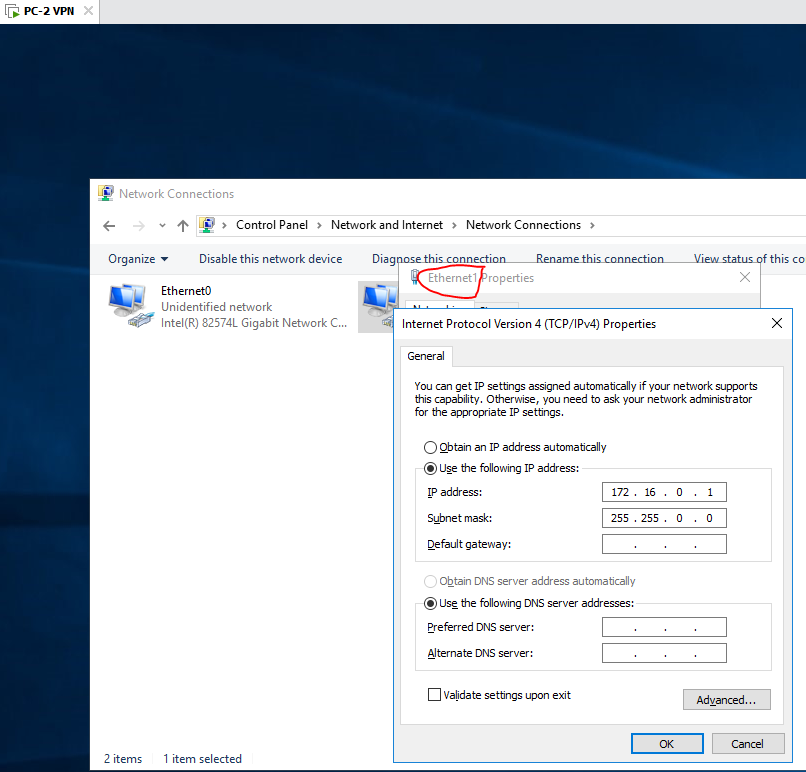
**Phần 1 : Cấu hình địa chỉ ip, kiểm tra kết nối của PC-2 và PC-1 , sau đó cho PC-2 join vào domain PC-1**



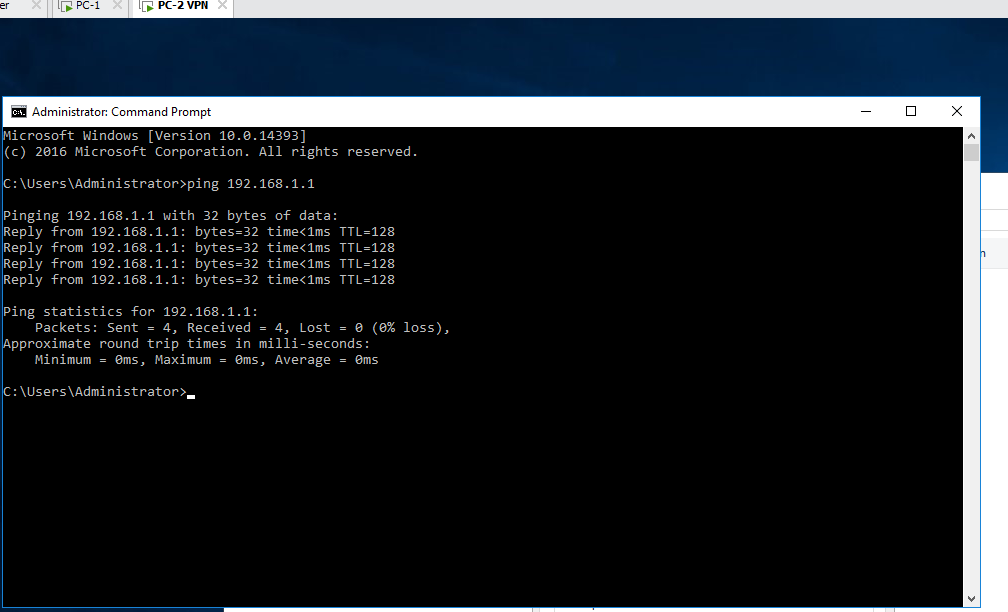
*Hình 54 : Cấu hình địa chỉ ip cho PC-1 và đặt luôn gateway tới PC-2*



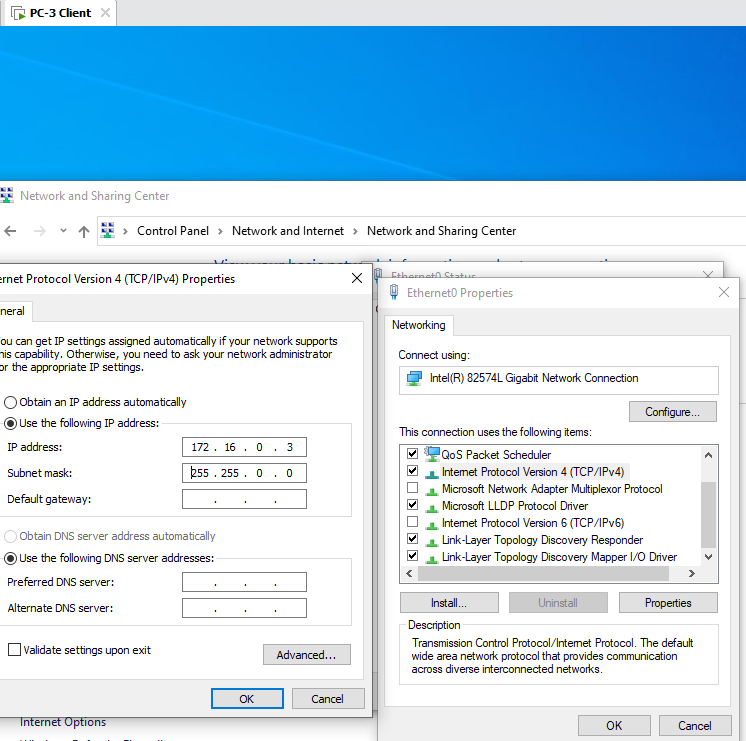
*Hình 55: Cấu hình địa chỉ ip cho card mạng đầu tiên của PC-2 trỏ tới DNS của PC-1 để truy cập vào domain trên PC-1*



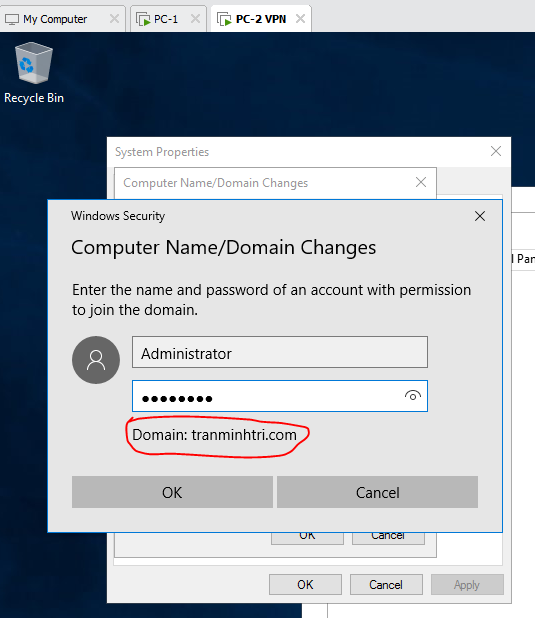
*Hình 56: Cấu hình địa chỉ ip cho card mạng thứ 2 của PC-2*



*Hình 57 : Tiến hành kiểm thử kết nối của PC-2 tới PC-1*

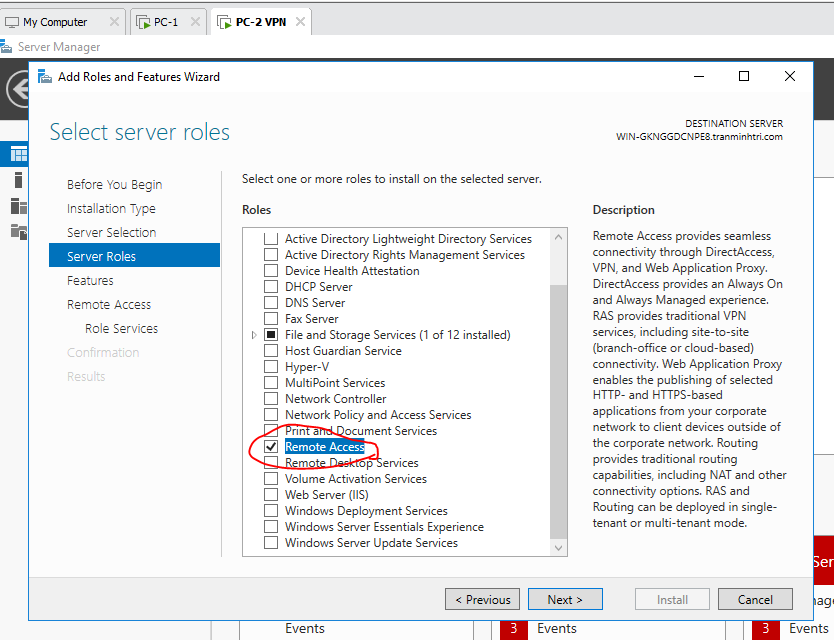


*Hình 58 : Cấu hình địa chỉ ip cho máy PC-3*

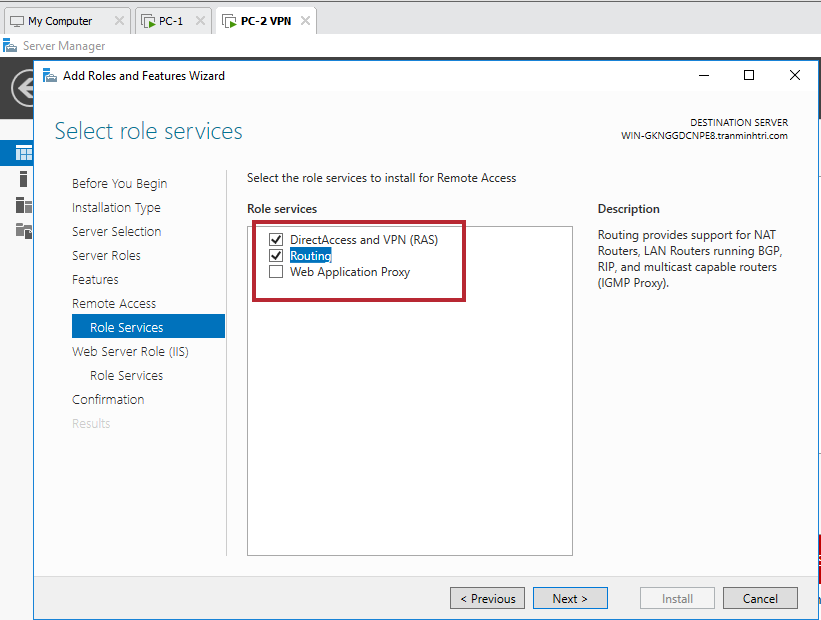


*Hình 59: Ở trên PC-2 ta truy cập vào domain đã tạo sẵn ở PC-1*

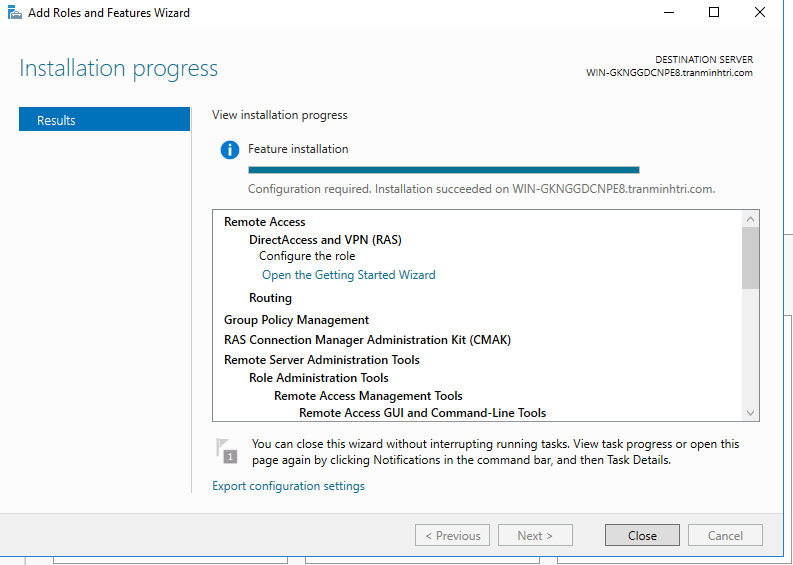
**Phần 2 : Trên PC-2 tiến hành cấu hình Remote Access VPN ( Client to site VPN)**



*Hình 60 : Chọn Roles Remote Access để tiến hành cấu hình VPN*

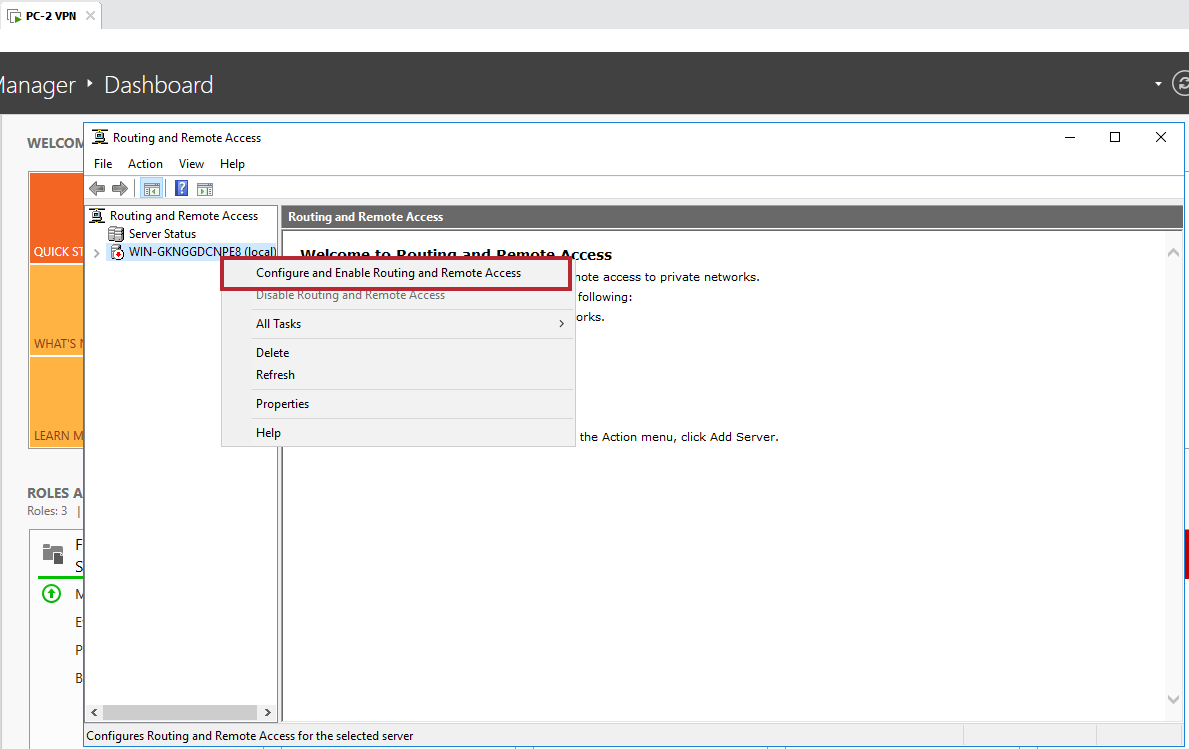
**

*Hình 61 : Ta chọn kết nối trực tiếp và VPN , chọn Routing để bổ trợ cho router tạo thành site VPN khi kết nối*

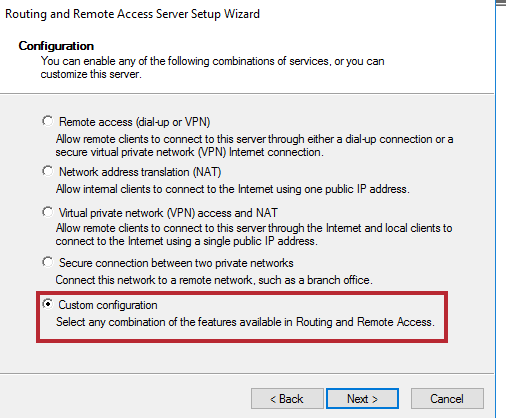


*Hình 62: Hình ảnh sau khi cài đặt xong Remote Access*

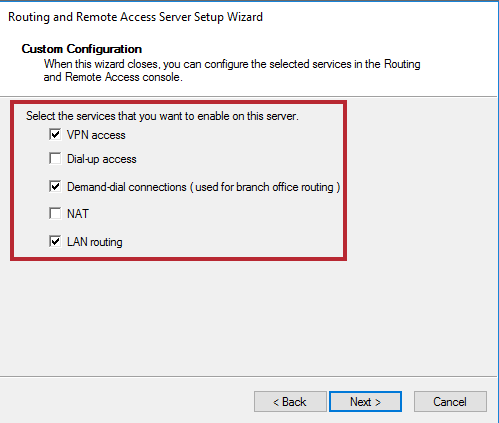
**Phần 3 : Cấu hình Remote Access VPN trên PC-2**



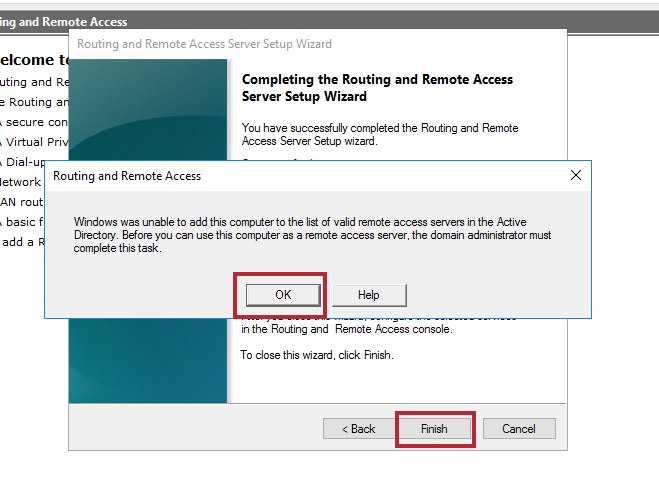
*Hình 63 : Hình ảnh ta vào phần cấu hình và kích hoạt Remote Access*



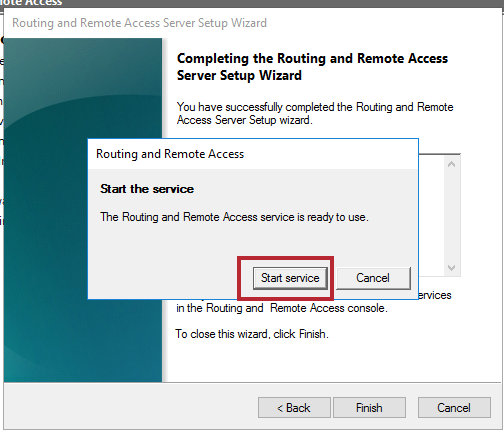
*Hình 64 : Ta chọn kiểu cấu hình custom để tùy chỉnh cho dễ*



*Hình 65: Ta sẽ chọn kiểu truy cập VPN , kết nối trực tiếp và kết nối với mạng local*

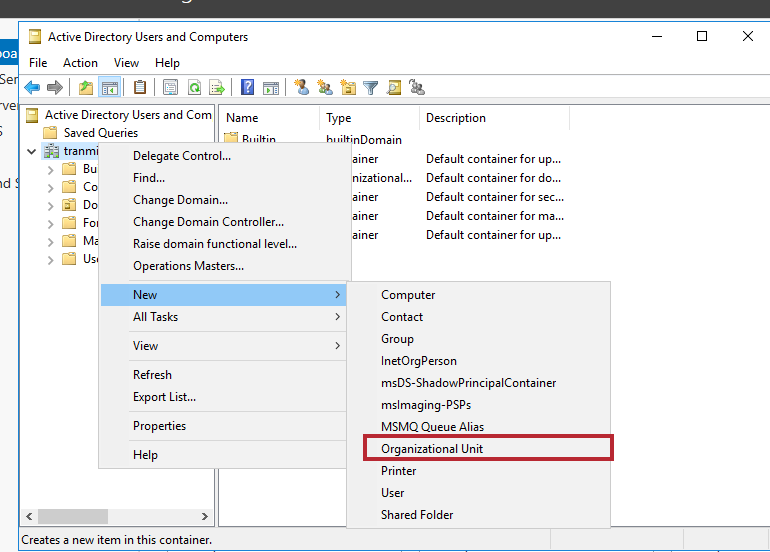


*Hình 66: Khi ta kích hoạt xong cấu hình Remote Accesss*

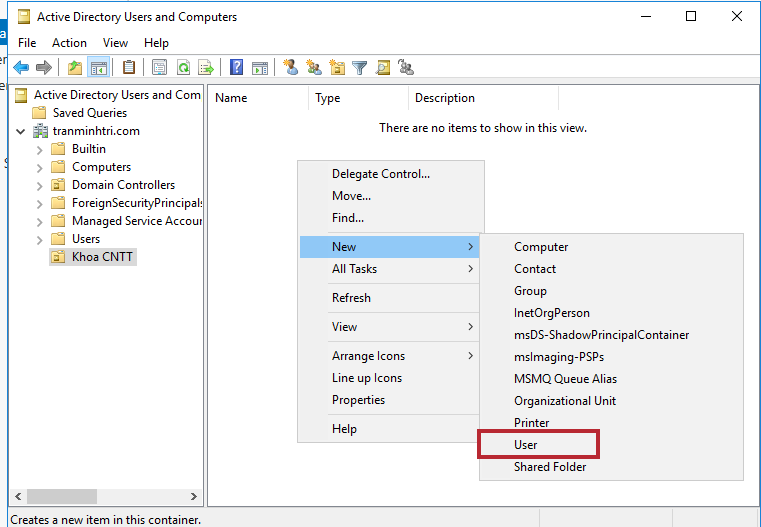


*Hình 67: Khởi chạy dịch vụ đã cấu hình*

**Phần 4: Tạo user trên PC-1 để test thử truy cập vào và cấu hình user này và quay lại PC-2 để cấu hình vùng pool truy cập**



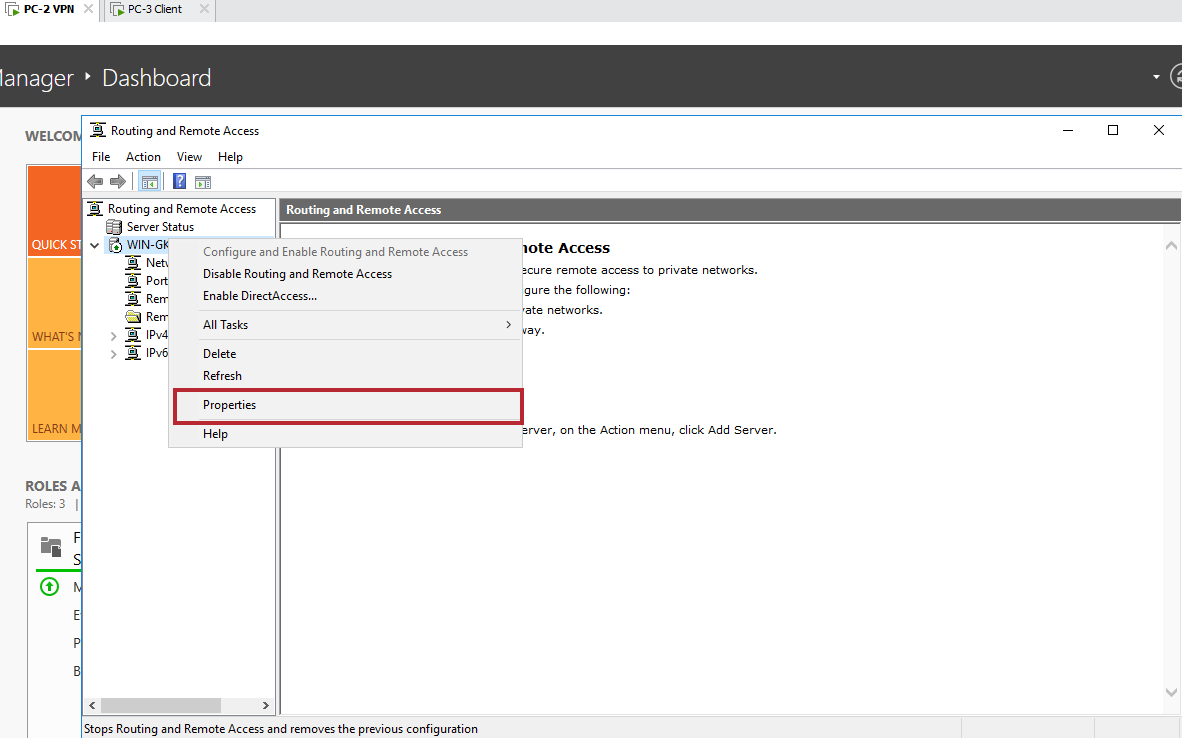
*Hình 68:Ta tiến hành tạo OU trên PC-1*



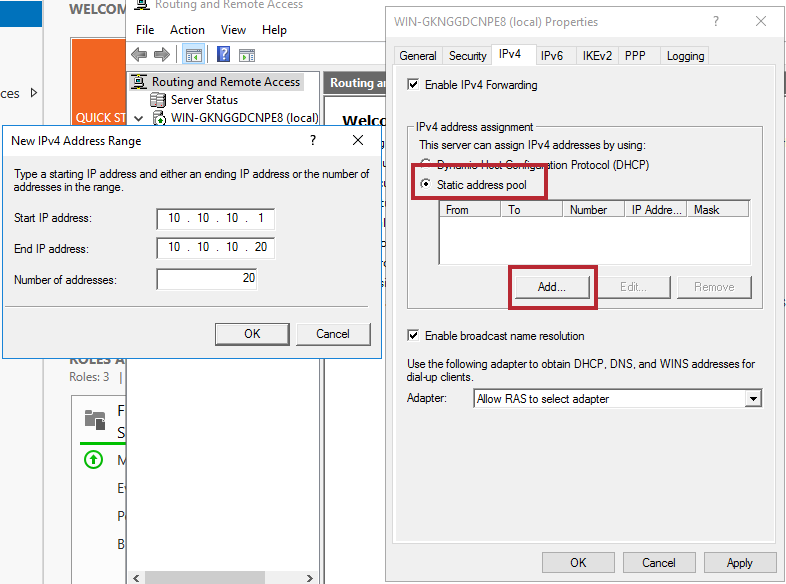
*Hình 69: Sau khi tạo xong OU là khoa CNTT ta tiến hành tạo user*



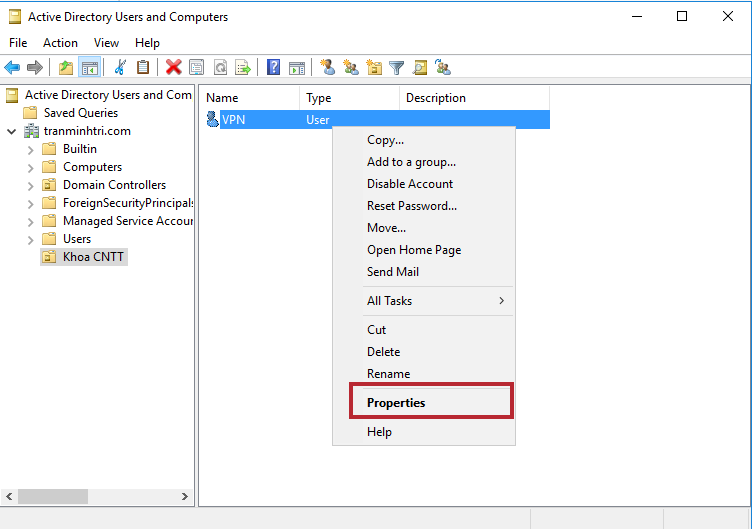
*Hình 70 : Sau khi tạo xong user VPN*



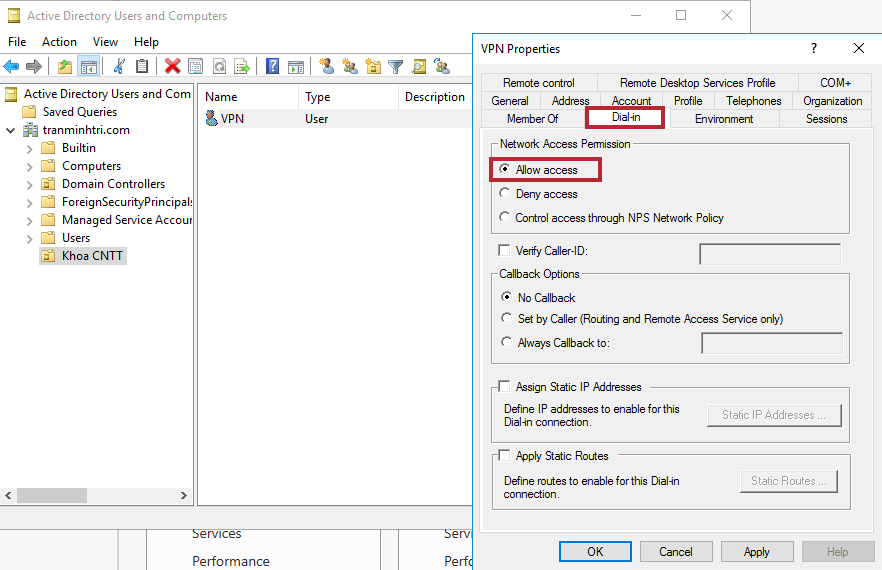
*Hình 71 : Ta quay lại PC-2 vào tool mở Routing and Remote Access rồi chọn VPN tên máy mình rồi chọn propyties để chỉnh lại 1 số thứ*



*Hình 72 : Ta chọn vùng cổng đầu và cổng cuối cho VPN site của mình và Add địa chỉ tĩnh vào trên tab Ipv4*

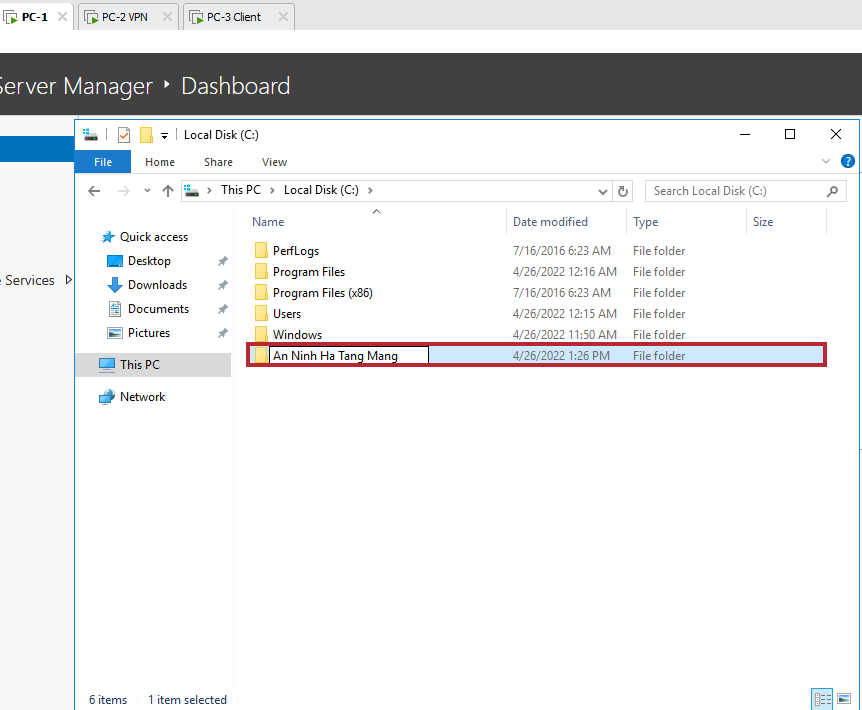
**

*Hình 73 : Ta quay lại PC-1 và cấu hình thuộc tính của nó sau khi tạo xong*

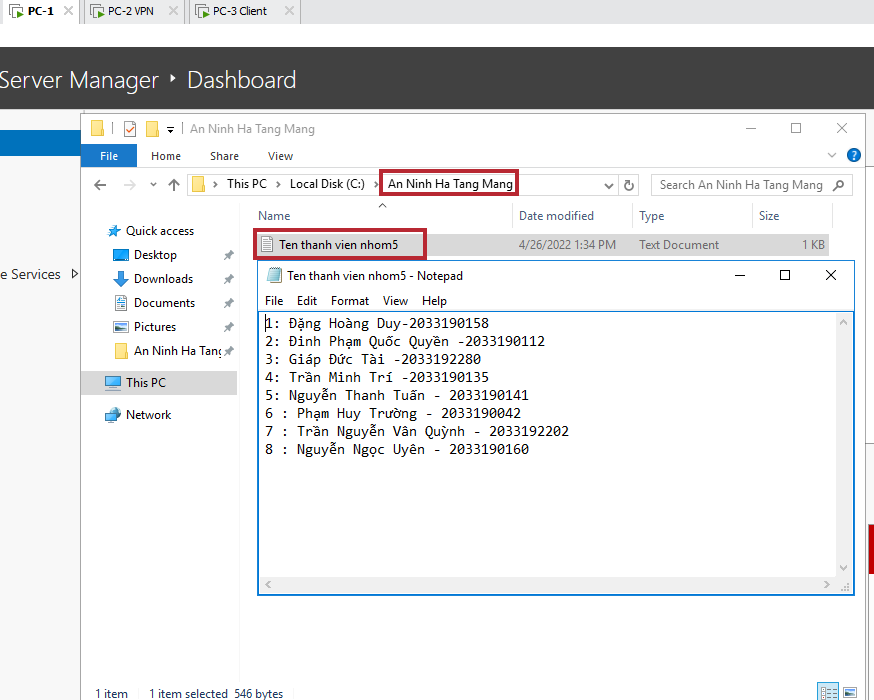


*Hình 74: Ta thay đổi cơ chế kết nối chọn cho phép kết nối*

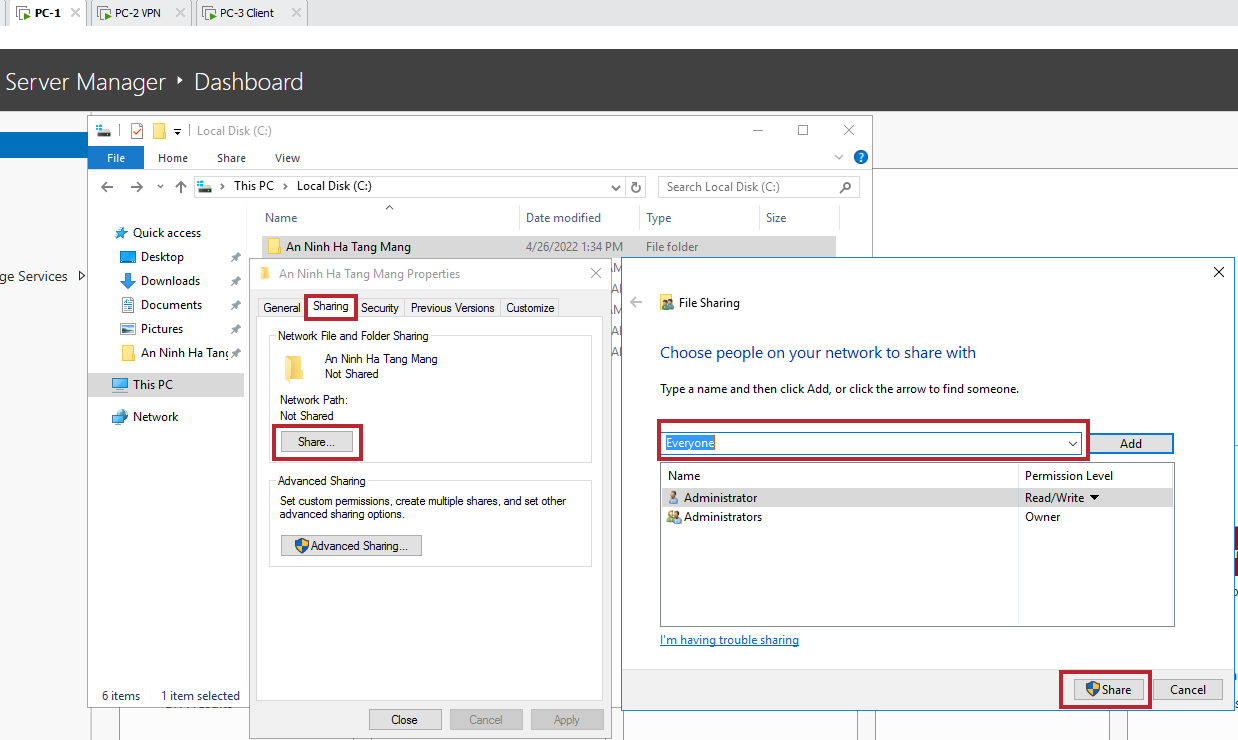
**Phần 5 : Tạo thư mục và tạo file trên PC-1 để test truy cập VPN client to site**

**

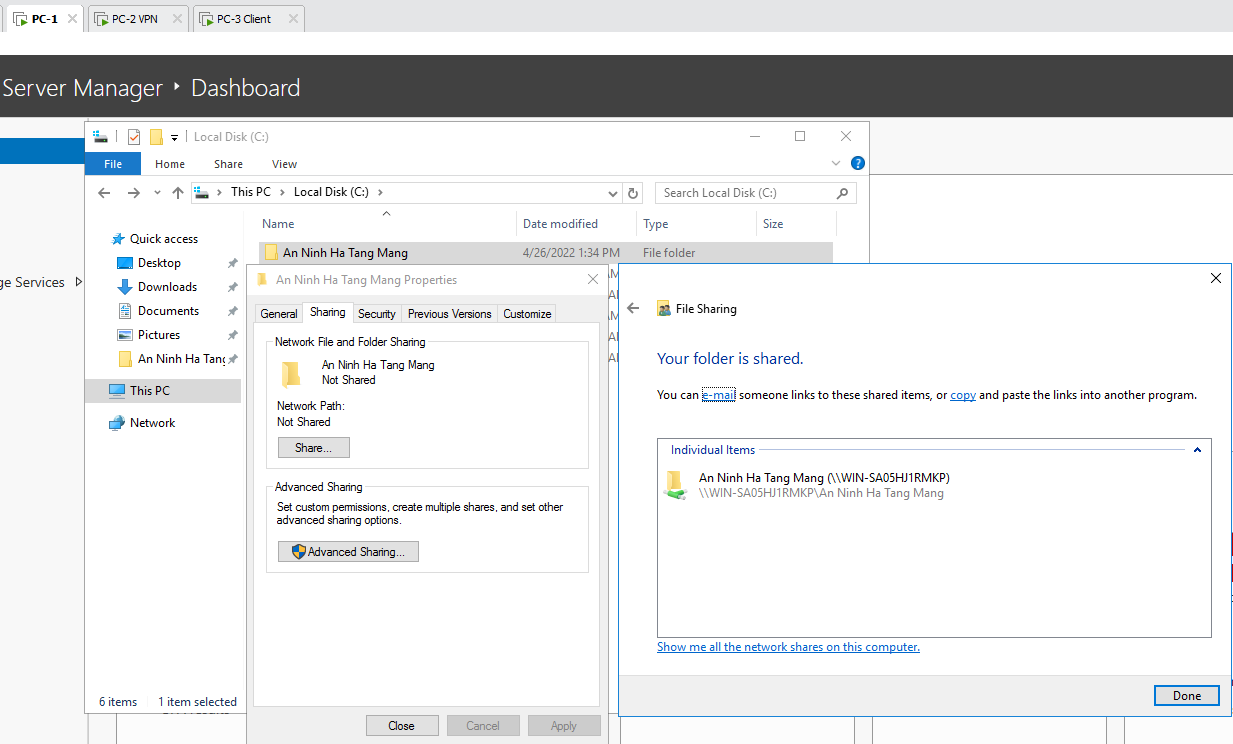
*Hình 75 : Tiến hành tạo thư mục trong ổ đĩa c*

**

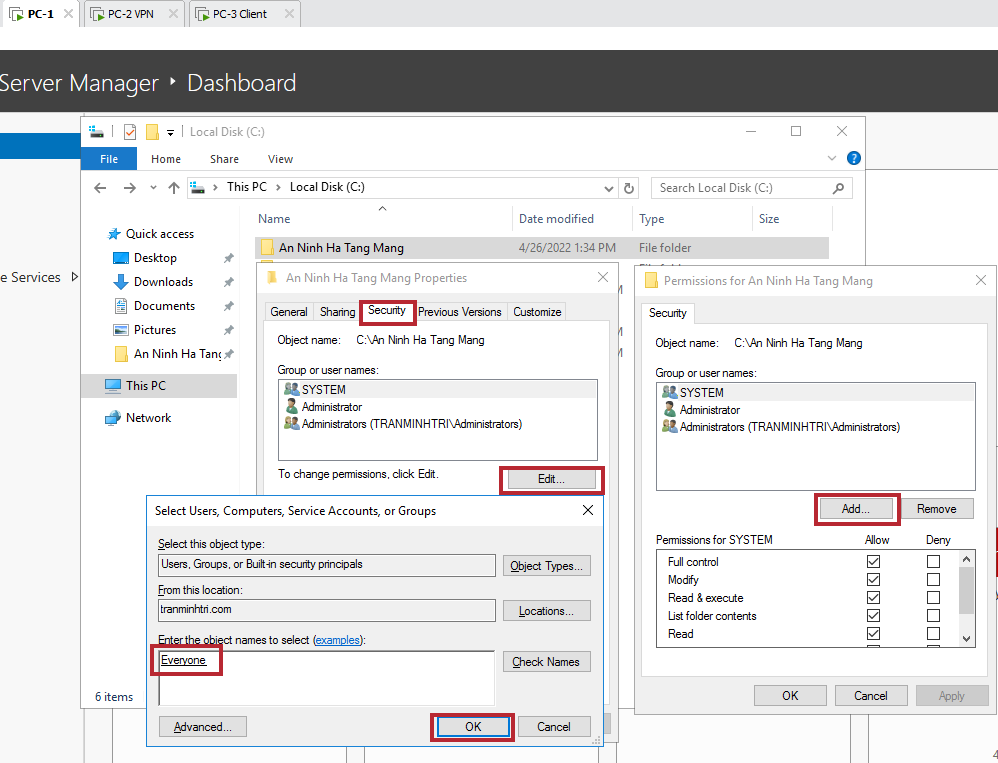
*Hình 76 : Ta tiến hành tạo file và điền 1 số dữ liệu cho file*



*Hình 77: Ta cấu hình Properties chế độ share thư mục này cho tất cả mọi người*

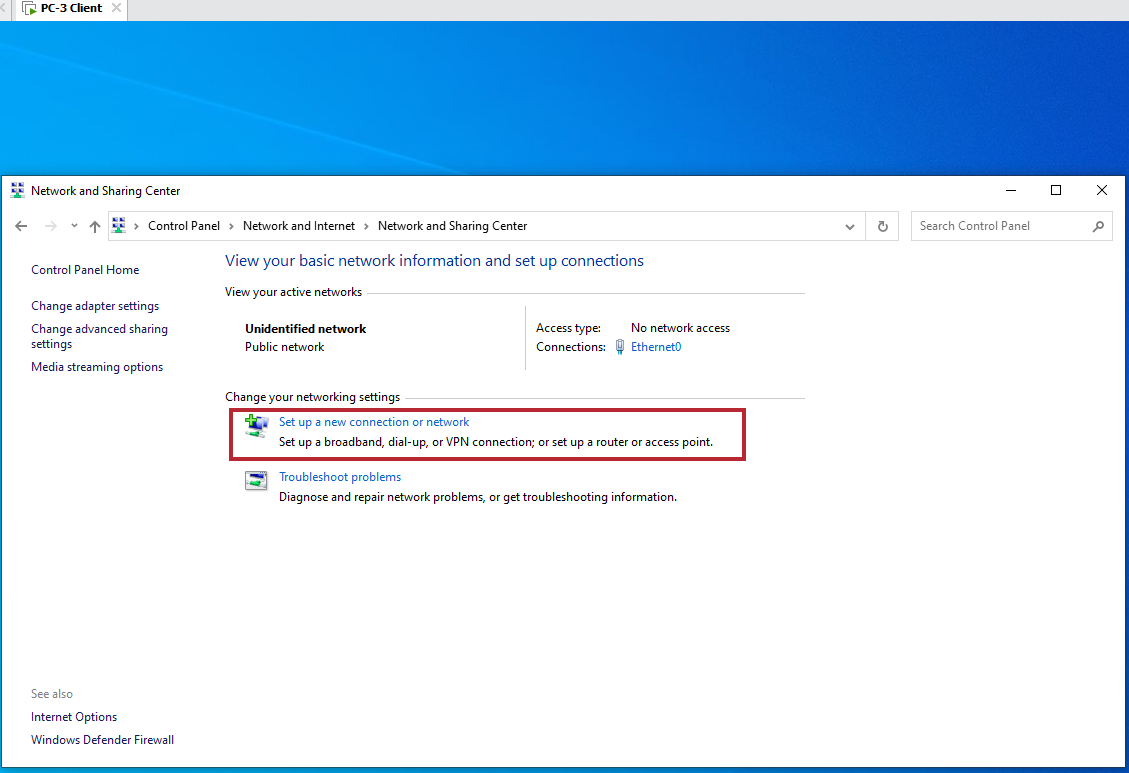


*Hình 78 :Màn hình sau khi ta share thư mục này xong*

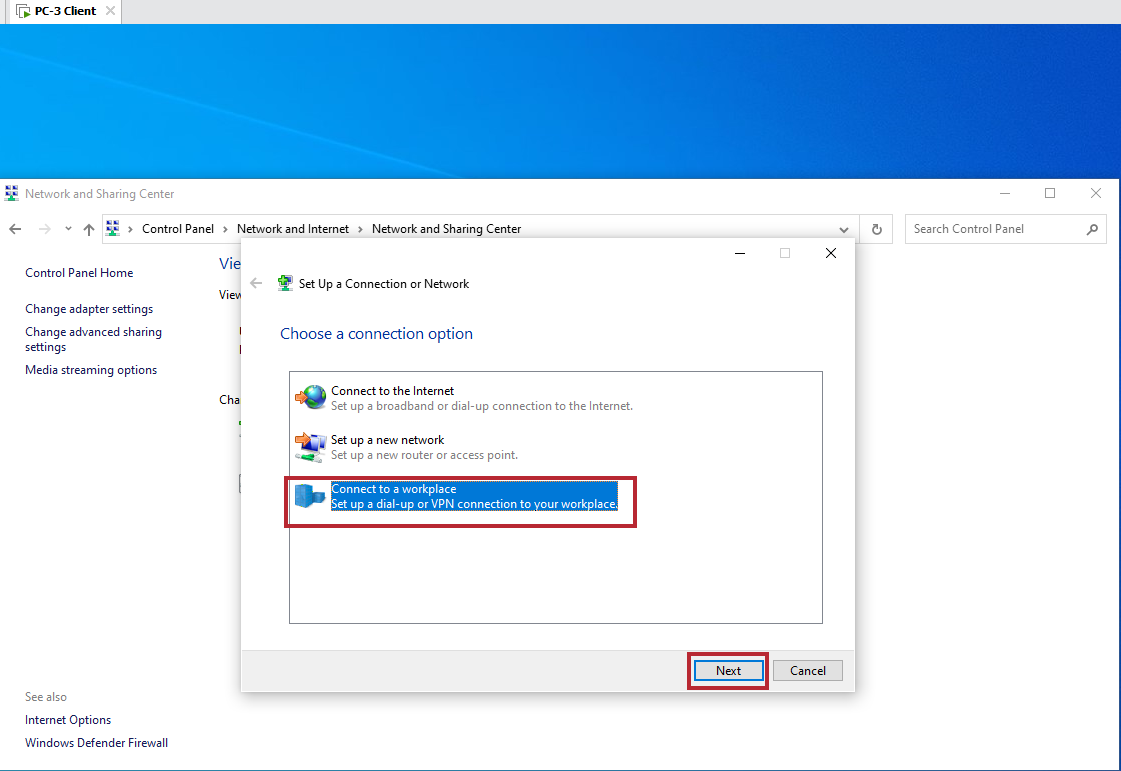


*Hình 79 : Ta cấu hình các quyền và Add vào object name Everyyone*

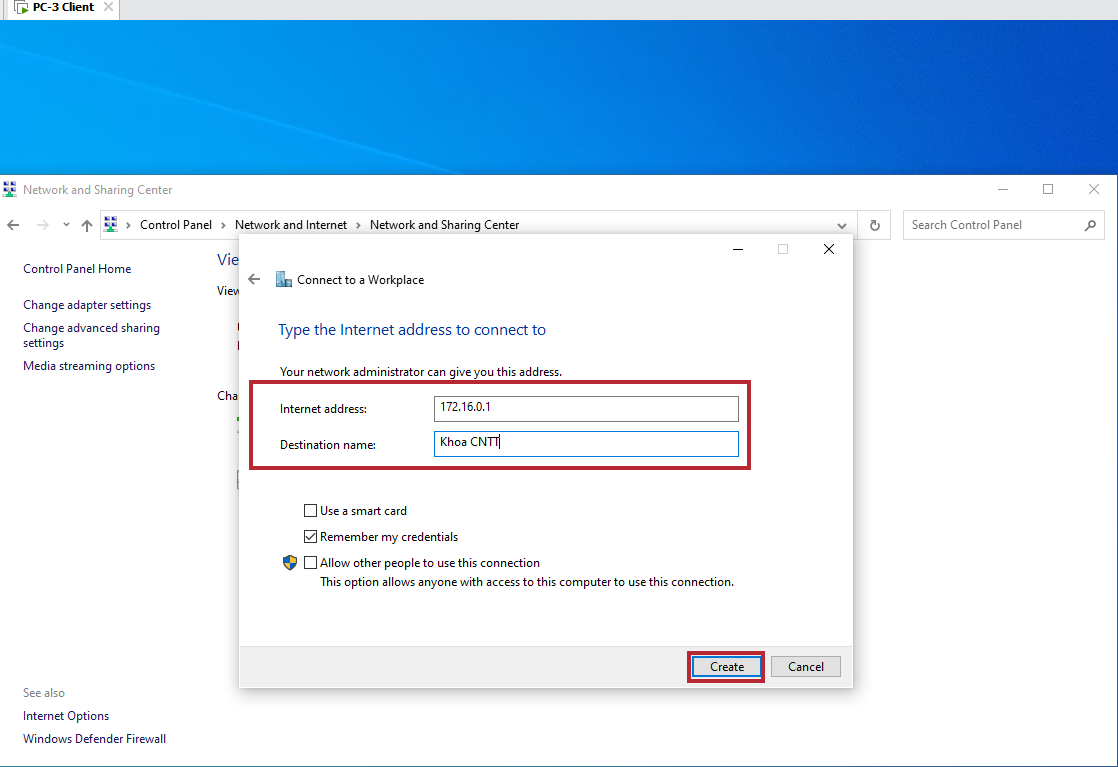
**Phần 6 : Ta vào máy PC-3 tiến hành truy cập vào VPN site và kiểm thử**

**

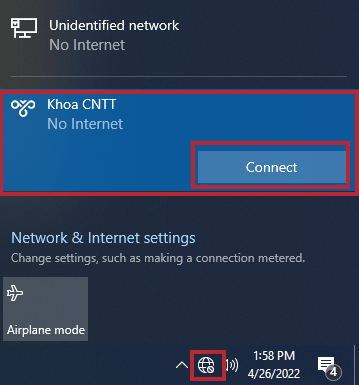
*Hình 80 : Ta vào NetWork và kết đến đia điểm VPN đã tạo*

**

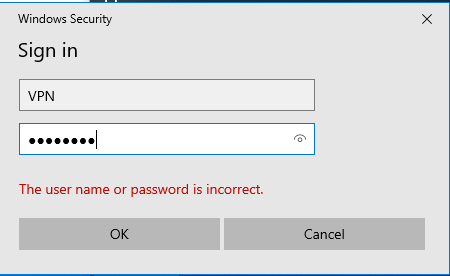
*Hình 81 : Chọn dòng kết nối đến địa điểm VPN có sẵn*



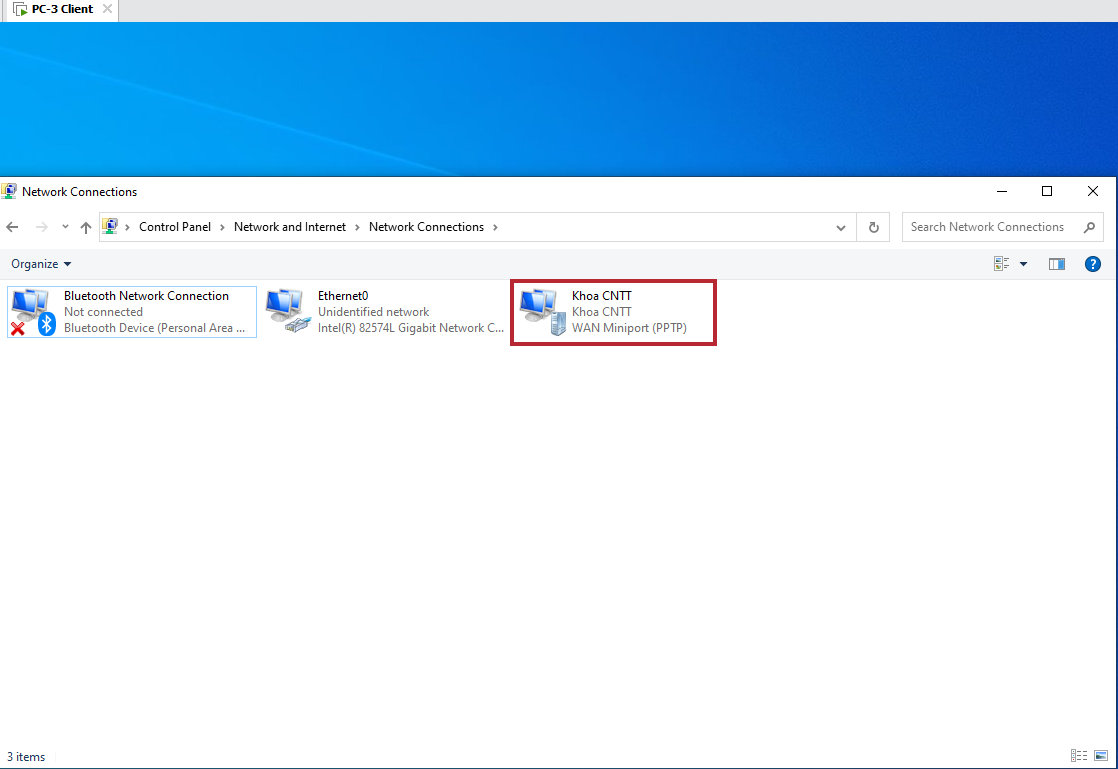
*Hình 82 : Ta trỏ để card mạng thứ 2 của PC-2 và đặt tên lại địa điểm kết nối nà*



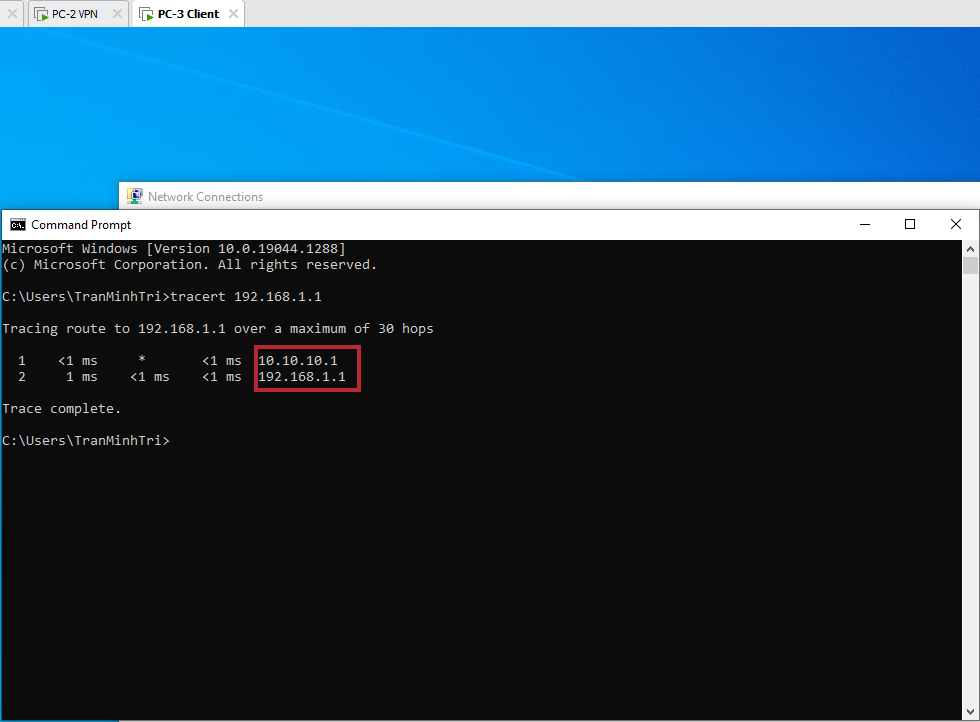
*Hình 83 : Địa điểm truy cập đã được xác nhận*



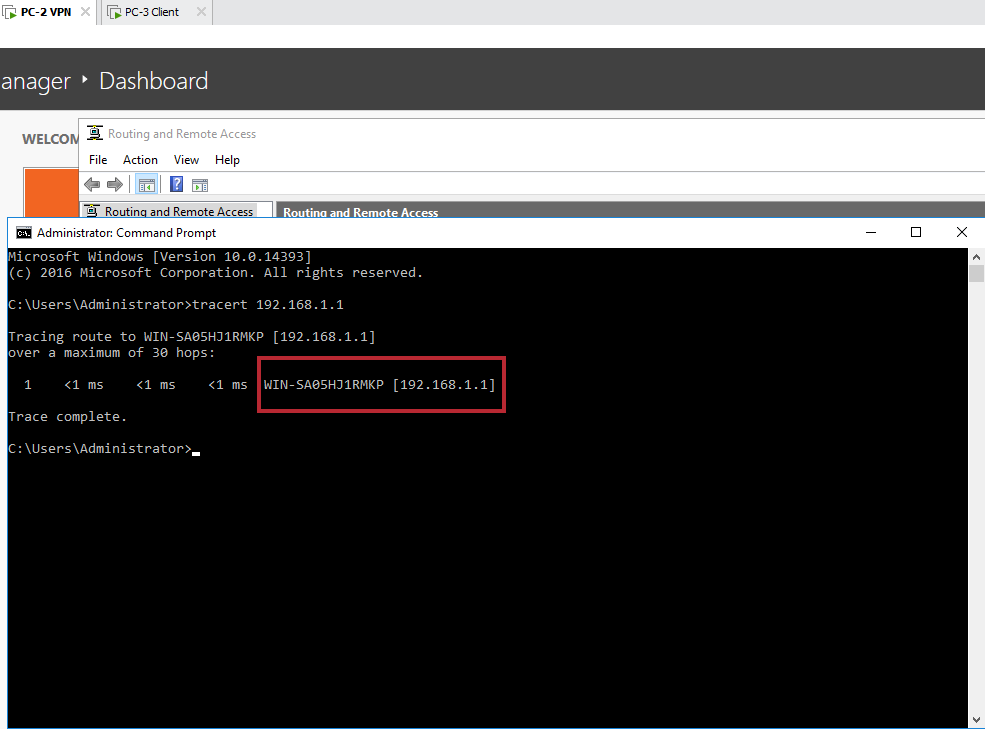
*Hình 84 : Ta điền tên tài khoản user đã tạo ở PC-1 để truy cập vào máy PC-1*



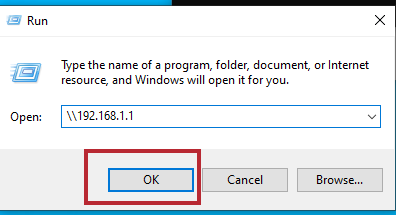
*Hình 85: Màn hình sau khi ta vào được VPN thì ta sẽ có thêm 1 card mạng nữa với tên đó*



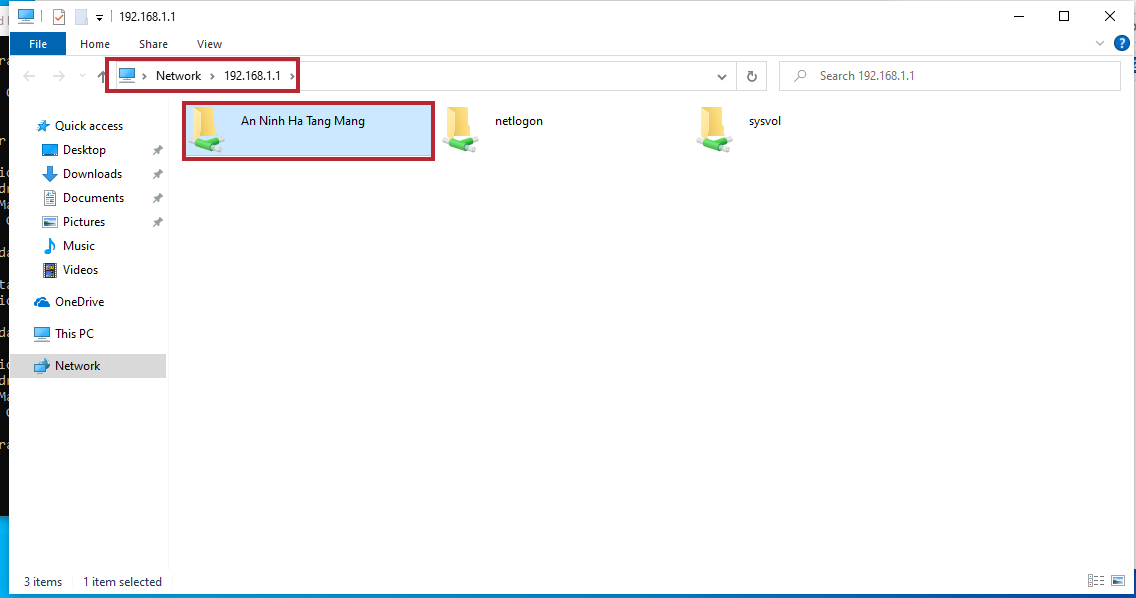
*Hình 86 : Ta tiến hành tracert thử đường đi khi PC-3 gửi dữ liệu qua PC-1 thì nó đi qua địa điểm cổng 10.10.10.1 cổng đầu ở hình 72 , rồi nó trỏ tới địa chỉ của card mạng PC-1 thì địa chỉ thật của card mạng PC-2 đã bị ẩn đi đó chính là VPN*



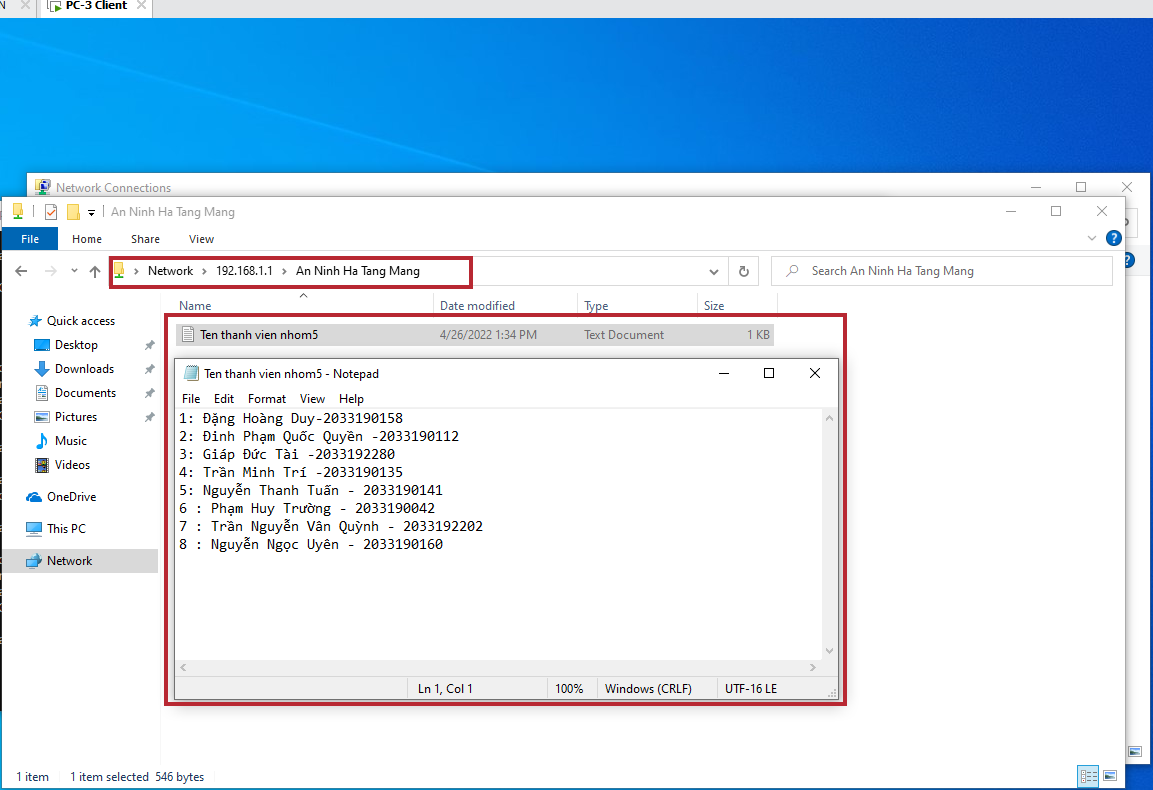
*Hình 87 : Ta tiến hành từ PC-2 tracert qua địa chỉ PC-1 thì thấy nó đi thẳng qua luôn và không thông qua card mạng PC-2 , VPN đã ẩn đi mất card mạng PC-2*



Hình 88 : Ta tiến hành kết nối tới máy PC-1 sau khi đã vào được VPN



*Hình 89 : Ta đã truy cập thành công vào và nhìn thấy thư mục được chia sẻ*

**

*Hình 90: Kiểm tra lại nội dung của file trong thư mục*

# TÀI LIỆU THAM KHẢO

[1]. TS.Văn Thiên Hoàng. (2014). *An Toàn Mạng. Truy cập 15/4/2022*, từ

<https://drive.google.com/drive/folders/1kw_05N7nVfMKJjRqaxu5tIuZdgSyouL9>

[2]. Vinh Phạm. (2019). *VPN site to site và ứng dụng trong các bài toán của doanh nghiệp. Truy cập 15/4/2022,* từ <https://bizflycloud.vn/tin-tuc/vpn-site-to-site-va-ung-dung-trong-cac-bai-toan-cua-doanh-nghiep-20190425095010051.htm>

[3]. PV. (2021). *VPN client to site là gì? Phân biệt VPN client to site và VPN site to site cụ thể. Truy cập 15/4/2022,* từ <https://thoidai.com.vn/vpn-client-to-site-la-gi-phan-biet-vpn-client-to-site-va-vpn-site-to-site-cu-the-129952.html#:~:text=VPN%20client%20to%20site%20(Remote,n%E1%BB%91i%20%C4%91%C6%B0%E1%BB%A3c%20%C4%91%E1%BA%BFn%20VPN%20server>