Bài tập lớn môn Mạng máy tính nâng cao trường đại học mở hn năm 2023

Mạng máy tính nâng cao (Trường Đại học Mở Hà Nội)

TRƯỜNG ĐẠI HỌC MỞ HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
MÔN: MẠNG MÁY TÍNH NÂNG CAO

ĐỀ TÀI:
Tìm hiểu về giao thức IPSec trong VPN và cài đặt mô phỏng

Giảng viên hướng dẫn: ***ThS. Nguyễn Thành Huy***

Sinh viên thực hiện: Đỗ Hồng Dương

Đào Gia Bảo

Hà Nội - Năm 2024

MỤC LỤC

Trang

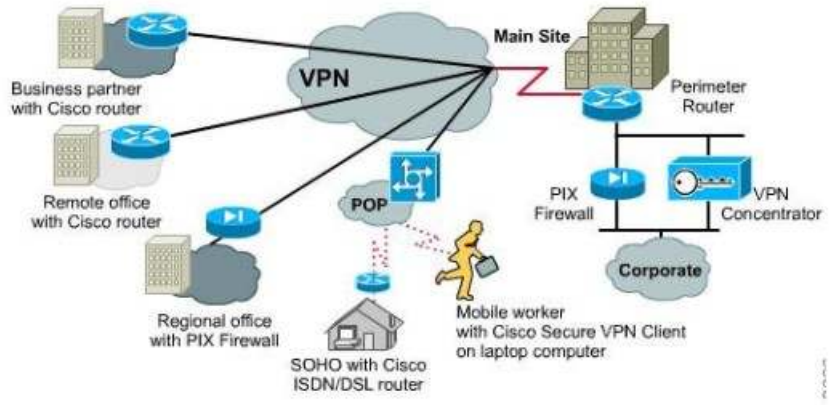
I. Tổng quan về VPN

Trong thời đại ngày nay. Internet đã phát triển mạnh về mặt mô hình cho đến công nghệ, đáp ứng các nhu cầu của người sử dụng. Internet đã được thiết kế để kết nối nhiều mạng khác nhau và cho phép thông tin chuyển đến người sử dụng một cách tự do và nhanh chóng mà không xem xét đến máy và mạng mà người sử dụng đó đang dùng Để làm được điều này người ta sử dụng một máy tính đặc biệt gọi là router để kết nối các LAN và WAN với nhau. Các máy tính kết nối vào Internet thông qua nhà cung cấp dịch vụ (ISP-Internet Service Provider), cần một giao thức chung là TCP/IP. Điều mà kỹ thuật còn tiếp tục phải giải quyết là năng lực truyền thông của các mạng viễn thông công cộng. Với Internet, những dịch vụ như giáo dục từ xa, mua hàng trực tuyến, tư vấn y tế, và rất nhiều điều khác đã trở thành hiện thực.Tuy nhiên, do Internet có phạm vi toàn cầu và không một tổ chức, chính phủ cụ thể nào quản lý nên rất khó khăn trong việc bảo mật và an toàn dữ liệu cũng như trong việc quản lý các dịch vụ. Từ đó người ta đã đưa ra một mô hình mạng mới nhằm thoả mãn những yêu cầu trên mà vẫn có thể tận dụng lại những cơ sở hạ tầng hiện có của Internet, đó chính là mô hình mạng riêng ảo (Virtual Private Network - VPN). Với mô hình mới này, người ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật, độ tin cậy vẫn đảm bảo, đồng thời có thể quản lý riêng được sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà, trên đường đi hay các văn phòng chi nhánh có thể kết nối an toàn đến máy chủ của tổ chức mình bằng cơ sở hạ tầng được cung cấp bởi mạng công cộng.[5] Nó có thể đảm bảo an toàn thông tin giữa các đại lý, người cung cấp. và các đối tác kinh doanh với nhau trong môi trường truyền thông rộng lớn. Trong nhiều trường hợp VPN cũng giống như WAN (Wide Area Network), tuy nhiên đặc tính quyết định của VPN là chúng có thể dùng mạng công cộng như Internet mà đảm bảo tính riêng tư và tiết kiệm hơn nhiều.

1. Định nghĩa VPN

VPN được hiểu đơn giản như là sự mở rộng của một mạng riêng (private network) thông qua các mạng công cộng. Về căn bản, mỗi VPN là một mạng riêng rẽ sử dụng một mạng chung (thường là internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường leased line, mỗi VPN sử dụng các kết nối ảo được dẫn đường qua Internet từ mạng riêng của các công ty tới các site hay các nhân viên từ xa. Để có thể gửi và nhận dữ liệu thông qua mạng công cộng mà vẫn bảo đảm tính an toàn và bảo mật VPN cung cấp các cơ chế mã hóa dữ liệu trên đường truyền tạo ra một đường ống bảo mật giữa nơi nhận và nơi gửi (Tunnel) giống như một kết nối point-to-point trên mạng riêng. Để có thể tạo ra một đường

ống bảo mật đó, dữ liệu phải được mã hóa hay che giấu đi chỉ cung cấp phần đầu gói dữ liệu (header) là thông tin về đường đi cho phép nó có thể đi đến đích thông qua mạng công cộng một cách nhanh chóng. Dữ liệu được mã hóa một cách cẩn thận do đó nếu các packet bị bắt lại trên đường truyền công cộng cũng không thể đọc được nội dung vì không có khóa để giải mã. Liên kết với dữ liệu được mã hóa và đóng gói được gọi là kết nối VPN. Các đường kết nối VPN thường được gọi là đường ống VPN (VPN Tunnel).



2. Lợi ích của VPN

VPN cung cấp nhiều đặc tính hơn so với những mạng truyền thống và những mạng mạng leased-line.Những lợi ích đầu tiên bao gồm:

- Chi phí thấp hơn những mạng riêng: VPN có thể giảm chi phí khi truyền tới 20-40% so với những mạng thuộc mạng leased-line và giảm việc chi phí truy cập từ xa từ 60-80%.
- Tính linh hoạt cho khả năng kinh tế trên Internet: VPN vốn đã có tính linh hoạt và có thể leo thang những kiến trúc mạng hơn là những mạng cổ điển, bằng cách đó nó có thể hoạt động kinh doanh nhanh chóng và chi phí một cách hiệu quả cho việc kết nối mở rộng. Theo cách này VPN có thể dễ dàng kết nối hoặc ngắt kết nối từ xa của những văn phòng, những vị trí ngoài quốc tế những người truyền thông, những người dùng điện thoại di động, những người hoạt động kinh doanh bên ngoài như những yêu cầu kinh doanh đã đòi hỏi.
- Đơn giản hóa những gánh nặng.
- Những cấu trúc mạng ống, vì thế giảm việc quản lý những gánh nặng: Sử dụng một giao thức Internet backbone loại trừ những PVC tĩnh hợp với kết nối hướng những giao thức như là Frame Rely và ATM.

- Tăng tình bảo mật: các dữ liệu quan trọng sẽ được che giấu đối với những người không có quyền truy cập và cho phép truy cập đối với những người dùng có quyền truy cập.
- Hỗ trợ các giao thức mạn thông dụng nhất hiện nay như TCP/IP
- Bảo mật địa chỉ IP: bởi vì thông tin được gửi đi trên VPN đã được mã hóa do đó các địa chỉ bên trong mạng riêng được che giấu và chỉ sử dụng các địa chỉ bên ngoài Internet.

3. Các thành phần cần thiết để tạo kết nối VPN

- User Authentication: cung cấp cơ chế chứng thực người dùng, chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.
- Address Management: cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên trên mạng nội bộ.
- Data Encryption: cung cấp giải pháp mã hoá dữ liệu trong quá trình truyền nhằm bảo đảm tính riêng tư và toàn vẹn dữ liệu.
- Key Management: cung cấp giải pháp quản lý các khoá dùng cho quá trình mã hoá và giải mã dữ liệu.

4. Các giao thức VPN

Các giao thức để tạo nên cơ chế đường ống bảo mật cho VPN là L2TP, Cisco GRE và IPSec.

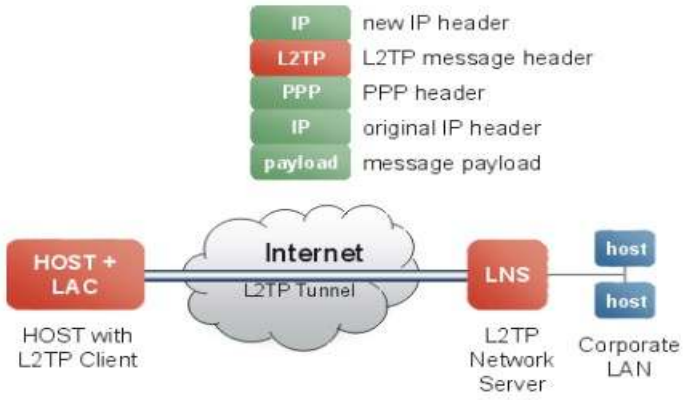
a. L2TP

- Trước khi xuất hiện chuẩn L2TP (tháng 8 năm 1999), Cisco sử dụng Layer 2 Forwarding (L2F) như là giao thức chuẩn để tạo kết nối VPN. L2TP ra đời sau với những tính năng được tích hợp từ L2F.

- L2TP là dạng kết hợp của Cisco L2F và Mircosoft Point-to-Point Tunneling Protocol (PPTP). Microsoft hỗ trợ chuẩn PPTP và L2TP trong các phiên bản WindowNT và 2000

- L2TP được sử dụng để tạo kết nối độc lập, đa giao thức cho mạng riêng ảo quay số (Virtual Private Dail-up Network). L2TP cho phép người dùng có thể kết nối thông qua các chính sách bảo mật của công ty (security policies) để tạo VPN hay VPDN như là sự mở rộng của mạng nội bộ công ty.

- L2TP không cung cấp mã hóa.

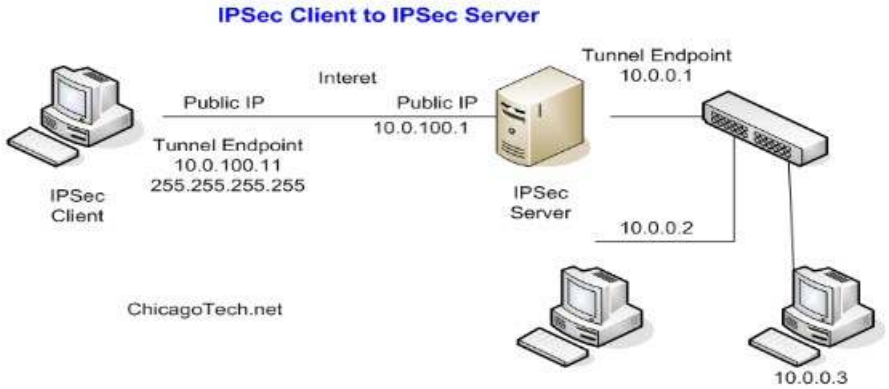


- L2TP là sự kết hợp của PPP(giao thức Point-to-Point) với giao thức L2F (Layer 2 Forwarding) của Cisco do đó rất hiệu quả trong kết nối mạng dial, ADSL, và các mạng truy cập từ xa khác. Giao thức mở rộng này sử dụng PPP để cho phép truy cập VPN bởi những người sử dụng từ xa.

b. GRE

- 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.

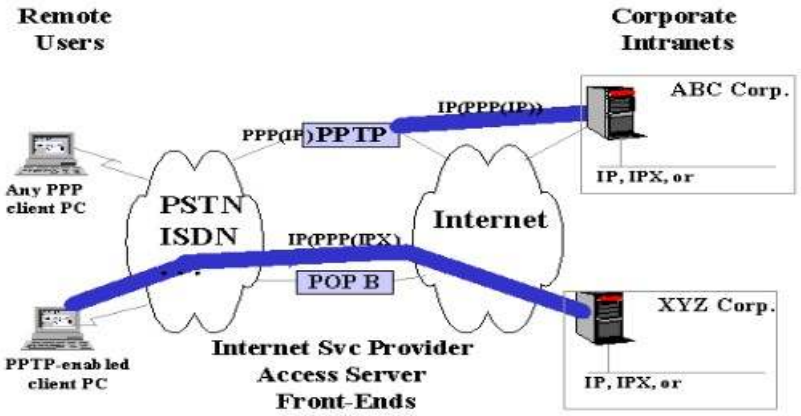
c. IPSec



- IPSec là sự lựa chọn cho việc bảo mật trên VPN. IPSec là một khung bao gồm bảo mật dữ liệu (data confidentiality), tính toàn vẹn của dữ liệu (integrity) và việc chứng thực dữ liệu.
- IPSec cung cấp dịch vụ bảo mật sử dụng KDE cho phép thỏa thuận các giao thức và thuật toan trên nền chính sách cục bộ (group policy) và sinh ra các khóa bảo mã hóa và chứng thực được sử dụng trong IPSec.

d. Point to Point Tunneling Protocol (PPTP):

- Được sử dụng trên các máy client chạy HĐH Microsoft for NT4.0 và Windows 95+ . Giao thức này được sử dụng để mã hóa dữ liệu lưu thông trên Mạng LAN. Giống như giao thức NETBEUI và IPX trong một packet gửi lên Internet. PPTP dựa trên chuẩn RSA RC4 và hỗ trợ bởi sự mã hóa 40-bit hoặc 128-bit.

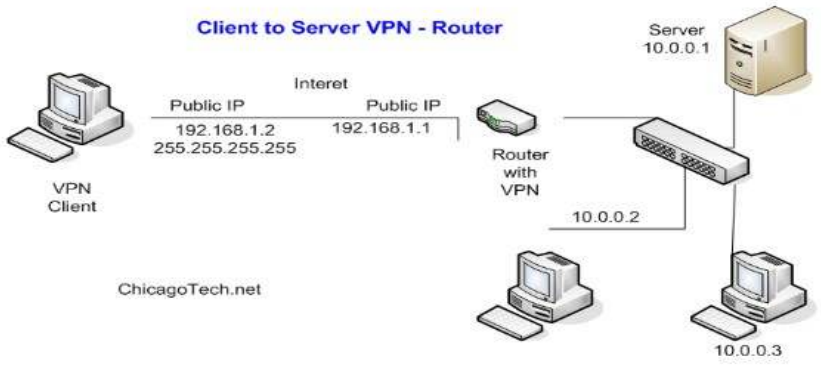


- Nó không được phát triển trên dạng kết nối LAN-to-LAN và giới hạn 255 kết nối tới 1 server chỉ có một đường hầm VPN trên một kết nối. Nó không cung cấp sự mã hóa cho các công việc lớn nhưng nó dễ cải đặt và triển khai và là một giải pháp truy cập từ xa chỉ có thể làm được trên mạng MS. Giao thức này thì được dùng tốt trong Window 2000. Layer 2 Tunneling Protocol thuộc về IPSec.

5. Thiết lập một kết nối VPN

a. Máy VPN cần kết nối (VPN client) tạo kết nốt VPN (VPN Connection) tới máy chủ cung cấp dịch vụ VPN (VPN Server) thông qua kết nối Internet.

b. Máy chủ cung cấp dịch vụ VPN trả lời kết nối tới



c. Máy chủ cung cấp dịch vụ VPN chứng thực cho kết nối và cấp phép cho kết nối

d. Bắt đầu trao đổi dữ liệu giữa máy cần kết nối VPN và mạng công ty

6. Các dạng kết nối VPN

a. Remote Access VPNs :

Remote Access VPNs 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 thường sử dụng các công nghệ WAN truyền thống để tạo lại các tunnel về mạng HO của họ.

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.

Một phần quan trọng của thiết kế này là việc thiết kế quá trình xác thực ban đầu nhằm để đảm bảo là yêu cầu được xuất phát từ một nguồn tin cậy. Thường thì giai đoạn ban đầu này dựa trên cùng một chính sách về bảo mật của công ty. Chính sách này bao gồm: qui trình (procedure), kỹ thuật, server (such as Remote Authentication Dial-In User Service [RADIUS], Terminal Access Controller Access Control System Plus [TACACS+]...).

Một số thành phần chính :

- Remote Access Server (RAS) : được đặt tại trung tâm có nhiệm vụ xác nhận và chứng nhận các yêu cầu gửi tới.
- Quay số kết nối đến trung tâm, điều này sẽ làm giảm chi phí cho một số yêu cầu ở khá xa so với trung tâm.
- Hổ trợ cho những người có nhiệm vụ cấu hình, bảo trì và quản lý RAS và hỗ trợ truy cập từ xa bởi người dùng.

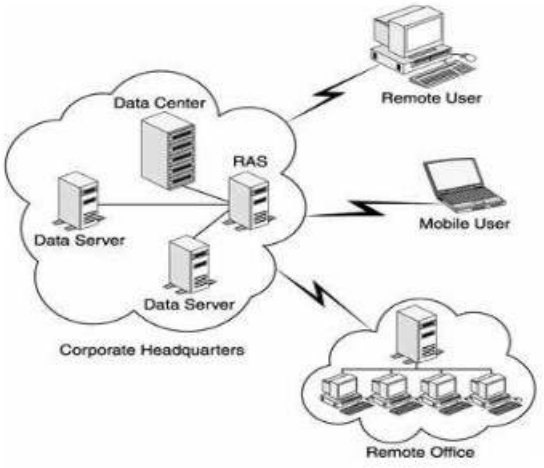


Figure 1-2: The non-VPN remote access setup.

- Bằng việc triển khai Remote Access VPNs, những người dùng từ xa hoặc các chi nhánh văn phòng chỉ cần cài đặt một kết nối cục bộ đến nhà cung cấp dịch vụ ISP hoặc ISP's POP và kết nối đến tài nguyên thông qua Internet. Thông tin Remote Access Setup được mô tả bởi hình vẽ sau :

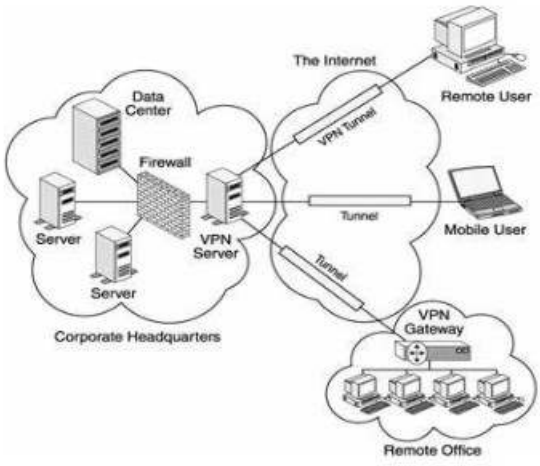


Figure 1-3: The Remote Access VPN setup

Như bạn có thể suy ra từ hình 1-3, thuận lợi chính của Remote Access VPNs : - Sự cần thiết của RAS và việc kết hợp với modem được loại trừ.

- Sự cần thiết hổ trợ cho người dung cá nhân được loại trừ bởi vì kết nối từ xa đã được tạo điều kiện thuận lợi bởi ISP

- Việc quay số từ những khoảng cách xa được loại trừ , thay vào đó, những kết nối với khoảng cách xa sẽ được thay thế bởi các kết nối cục bộ.

- Giảm giá thành chi phí cho các kết nối với khoảng cách xa.

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

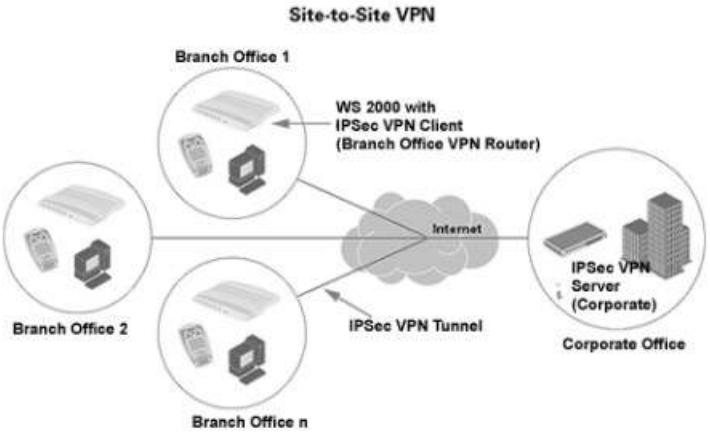
- VPNs cung cấp khả năng truy cập đến trung tâm tốt hơn bởi vì nó hỗ trợ dịch vụ truy cập ở mức độ tối thiểu nhất cho dù có sự tăng nhanh chóng các kết nối đồng thời den mang.

Ngoài những thuận lợi trên, VPNs cũng tồn tại một số bất lợi khác như :

- Remote Access VPNs cũng không bảo đảm được chất lượng phục vụ.
- Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát.
- Do độ phức tạp của thuật toán mã hoá, protocol overhead tăng đáng kể, điều này gây khó khăn cho quá trình xác nhận. Thêm vào đó, việc nén dữ liệu IP và PPP-based diễn ra vô cùng chậm chạp và tồi tệ.
- Do phải truyền dữ liệu thông qua Internet, nên khi trao đổi các dữ liệu lớn như các gói dữ liệu truyền thông, phim ảnh, âm thanh sẽ rất chậm.

b. Site To Site (Lan - To - Lan):

- Site-to-site VPN(Lan-to-Lan VPN) được áp dụng để cài đặt mạng từ một vị trí này kết nối tới mạng của một vị trí khác thông qua VPN. Trong hoàn cảnh này thì việc chứng thực ban đầu giữa các thiết bị mạng được giao cho người sử dụng. Nơi mà có một kết nối VPN được thiết lập giữa chúng. Khi đó các thiết bị này đóng vai trò như là một gateway, và đảm bảo rằng việc lưu thông đã được dự tính trước cho các site khác. Các router và Firewall tương thích với VPN, và các bộ tập trung VPN chuyên dụng đều cung cấp chức năng này.



- Lan-to-Lan VPN có thể được xem như là intranet VPN hoặc extranet VPN(xem xét về mặt chính sách quản lý). Nếu chúng ta xem xét dưới góc độ chứng thực nó có thể được xem như là một intranet VPN, ngược lại chúng được xem như là một extranet VPN. Tính chặt chẽ trong việc truy cập

giữa các site có thể được điều khiển bởi cả hai(intranet và extranet VPN) theo các site tương ứng của chúng. Giải pháp Site to site

VPN không là một remote access VPN nhưng nó được thêm vào đây vì tính chất hoàn thiện của nó.

- Sự phân biệt giữa remote access VPN và Lan to Lan VPN chỉ đơn thuần mang tính chất tượng trưng và xa hơn là nó được cung cấp cho mục đích thảo luận. Ví dụ như là các thiết bị VPN dựa trên phần cứng mới(Router cisco 3002 chẳng hạn) ở đây để phân loại được, chúng ta phải áp dụng cả hai cách, bởi vì harware-based client có thể xuất hiện nếu một thiết bị đang truy cập vào mạng. Mặc dù một mạng có thể có nhiều thiết bị VPN đang vận hành. Một ví dụ khác như là chế độ mở rộng của giải pháp Ez VPN bằng cách dùng router 806 và 17xx.

- Lan-to-Lan VPN là sự kết nối hai mạng riêng lẻ thông qua một đường hầm bảo mật. đường hầm bảo mật này có thể sử dụng các giao thức PPTP, L2TP, hoặc IPSec, mục đích của Lan-to-Lan VPN là kết nối hai mạng không có đường nối lại với nhau,

không có việc thỏa hiệp tích hợp, chứng thực, sự cẩn mật của dữ liệu. bạn có thể thiết lập một Lan-to-Lan VPN thông qua sự kết hợp của các thiết bị VPN Concentrators, Routers, and Firewalls.

- Kết nối Lan-to-Lan 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 luân chuyển thông qua internet hoặc một mạng không được tin cậy Bạn phải đảm bảo vấn 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.

1. Intranet VPNs

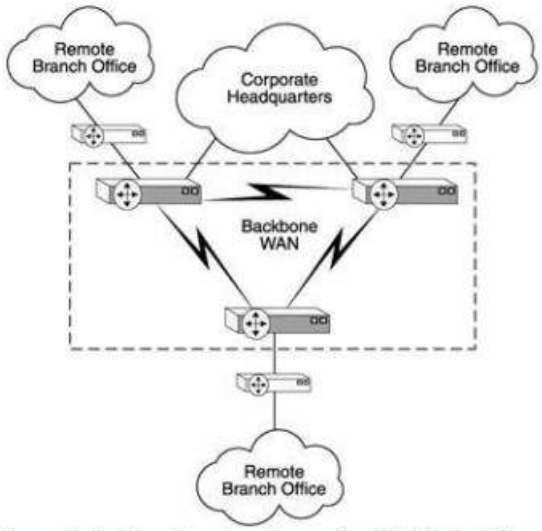
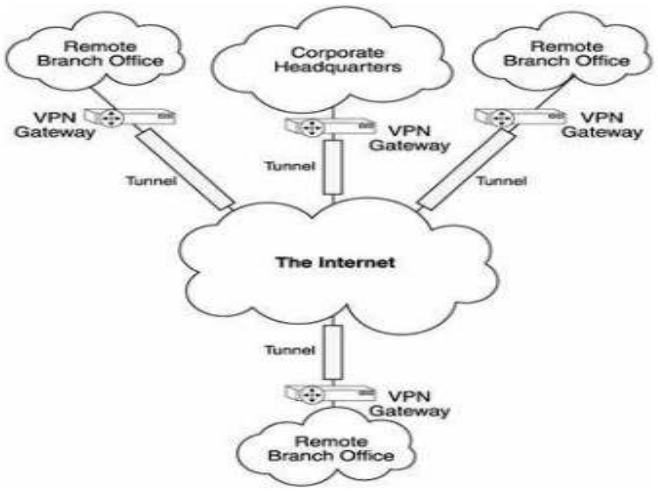


Figure 1-4: The intranet setup using WAN backbone

- Intranet VPNs được sử dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Corperate Intranet (backbone router) sử dụng campus router, xem hình bên dưới :
- Theo mô hình bên trên sẽ rất tốn chi phí do phải sử dụng 2 router để thiết lập được mạng, thêm vào đó, việc triển khai, bảo trì và quản lý mạng Intranet Backbone sẽ rất tốn kém còn tùy thuộc vào lượng lưu thông trên mạng đi trên nó và phạm vi địa lý của toàn bộ mạng Intranet.
- Để giải quyết vấn đề trên, sự tốn kém của WAN backbone được thay thế bởi các kết nối Internet với chi phí thấp, điều này có thể một lượng chi phí đáng kể của việc triển khai mạng Intranet, xem hình bên dưới :



Những thuận lợi chính của Intranet setup dựa trên VPN theo hình 1-5 :

- Hiệu quả chi phí hơn do giảm số lượng router được sử dụng theo mô hình WAN backbone

- Giảm thiểu đáng kể số lượng hỗ trợ yêu cầu người dùng cá nhân qua toàn cầu, các trạm ở một số remote site khác nhau.
- Bởi vì Internet hoạt động như một kết nối trung gian, nó dễ dàng cung cấp những kết nối mới ngang hàng.
- Kết nối nhanh hơn và tốt hơn do về bản chất kết nối đến nhà cung cấp dịch vụ, loại bỏ vấn đề về khoảng cách xa và thêm nữa giúp tổ chức giảm thiểu chi phí cho việc thực
hiện Intranet.

Những bất lợi chính kết hợp với cách giải quyết :

- Bởi vì dữ liệu vẫn còn tunnel trong suốt quá trình chia sẽ trên mạng công cộng. Internet-và những nguy cơ tấn công, như tấn công bằng từ chối dịch vụ (denial-of- service), vẫn còn là một mối đe doạ an toàn thông tin.
- Khả năng mất dữ liệu trong lúc di chuyễn thông tin cũng vẫn rất cao.
- Trong một số trường hợp, nhất là khi dữ liệu là loại high-end, như các tập tin mulltimedia, việc trao đổi dữ liệu sẽ rất chậm chạp do được truyền thông qua Internet.
- Do là kết nối dựa trên Internet, nên tính hiệu quả không liên tục, thường xuyên, và QoS cũng không được đảm bảo.

2. Extranet VPNs:

- Không giống như Intranet và Remote Access-based, Extranet không hoàn toàn cách li từ bên ngoài (outer-world), Extranet cho phép truy cập những tài nguyên mạng cần thiết của các đối tác kinh doanh, chẳng hạn như khách hàng, nhà cung cấp, đối tác những người giữ vai trò quan trọng trong tổ chức.

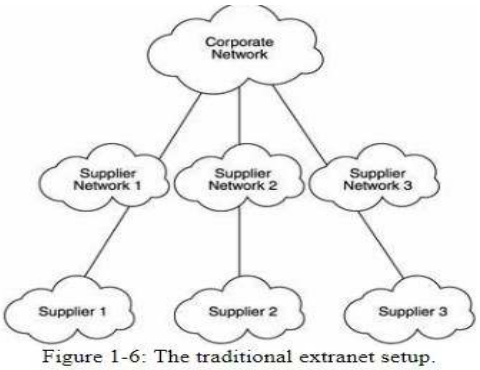


Figure 1-6: The traditional extranet setup.

- Như hình trên, mạng Extranet rất tốn kém do có nhiều đoạn mạng riêng biệt trên Intranet kết hợp lại với nhau để tạo ra một Extranet. Điều này làm cho khó triển khai và quản lý do có nhiều mạng, đồng thời cũng khó khăn

cho cá nhân làm công việc bảo trì và quản trị. Thêm nữa là mạng Extranet sẽ dễ mở rộng do điều này sẽ làm rối tung toàn bộ mạng Intranet và có thể ảnh hưởng đến các kết nối bên ngoài mạng. Sẽ có những vấn đề bạn gặp phải bất thình lình khi kết nối một Intranet vào một mạng Extranet. Triển khai và thiết kế một mạng Extranet có thể là một cơn ác mộng của các nhà thiết kế và quản trị mạng.

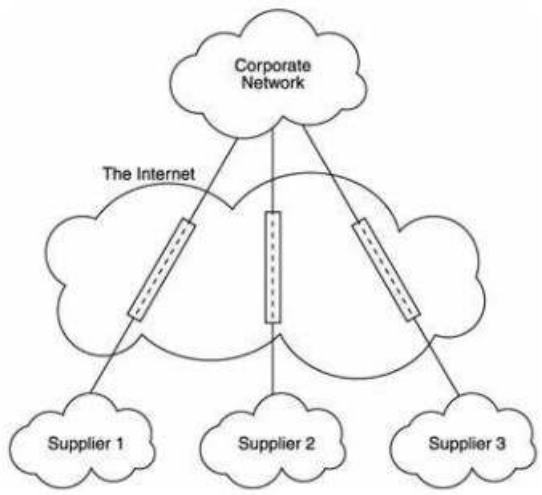


Figure 1-7: The Extranet VPN setup

Một số thuận lợi của Extranet :

- Do hoạt động trên môi trường Internet, bạn có thể lựa chọn nhà phân phối khi lựa chọn và đưa ra phương pháp giải quyết tuỳ theo nhu cầu của tổ chức.
- Bởi vì một phần Internet-connectivity được bảo trì bởi nhà cung cấp (ISP) nên cũng giảm chi phí bảo trì khi thuê nhân viên bảo trì - Dễ dàng triển khai, quản lý và chỉnh sửa thông tin.

Một số bất lợi của Extranet :

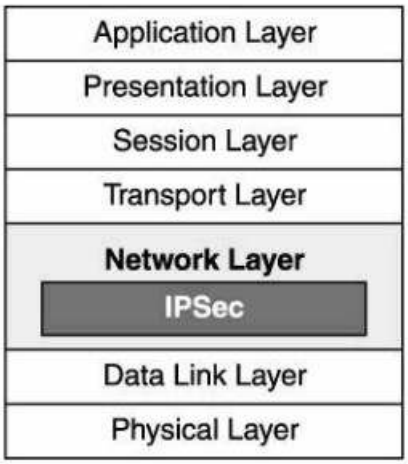
- Sự đe dọa về tính an toàn, như bị tấn công bằng từ chối dịch vụ vẫn còn tồn tại.
- Tăng thêm nguy hiểm sự xâm nhập đối với tổ chức trên Extranet.
- Do dựa trên Internet nên khi dữ liệu là các loại high-end data thì việc trao đổi diễn ra chậm chạp.
- Do dựa trên Internet, QoS(Quality of Service) cũng không được bảo đảm thường xuyên.

II. Tìm hiểu về giao thức IPSEC

1. Tổng quan về IPSEC

- Thuật ngữ IPSec là một từ viết tắt của thuật Internet Protocol Security. Nó có quan hệ tới một số bộ giao thức (AH, ESP, FIP-140-1, và một số chuẩn khác) được phát triển bởi Internet Engineering Task Force (IETF). Mục đích

chính của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI như hình dưới:



- Mọi giao tiếp trong một mạng trên cơ sở IP đều dựa trên các giao thức IP. Do đó, khi một cơ chế bảo mật cao được tích hợp với giao thức IP, toàn bộ mạng được bảo mật bởi vì các giao tiếp đều đi qua tầng 3. (Đó là lý do tại sao IPSec được phát triển ở giao thức tầng 3 thay vì tầng 2).
- IPSec VPN dùng các dịch vụ được định nghĩa trong IPSec để đảm bảo tính toàn vẹn dữ liệu, tính nhất quán, tính bí mật và xác thực của truyền dữ liệu trên một hạ tầng mạng công cộng.
- Ngoài ra,với IPSec tất cả các ứng dụng đang chạy ở tầng ứng dụng của mô hình OSI đều độc lập trên tầng 3 khi định tuyến dữ liệu từ nguồn đến đích. Bởi vì IPSec được tích hợp chặt chẽ với IP, nên những ứng dụng có thể dùng các dịch vụ kế thừa tính năng bảo mật mà không cần phải có sự thay đổi lớn lao nào. Cũng giống IP, IPSec trong suốt với người dùng cuối, là người mà không cần quan tâm đến cơ chế bảo mật mở rộng liên tục đằng sau một chuỗi các hoạt động.

❖ **Ưu điểm của IPsec:**
- Bảo mật cao: Cung cấp tính bảo mật mạnh mẽ cho dữ liệu được truyền qua mạng.
- Linh hoạt: Hỗ trợ nhiều thuật toán mã hóa và xác thực.
- Hoạt động ở lớp mạng: IPsec hoạt động ở lớp mạng, cho phép nó bảo mật cho mọi giao thức mạng được sử dụng.

❖ **Nhược điểm của IPsec:**
- Phức tạp: IPsec là một giao thức phức tạp, đòi hỏi kiến thức chuyên môn để thiết lập và quản lý.
- Tốc độ: IPsec có thể làm giảm tốc độ kết nối do quá trình mã hóa và giải mã dữ liệu.

2. Các thành phần chi tiết của IPSEC

Giao thức IPSec bao gồm các thành phần sau:

- Security Associations (SA): Là các cơ chế định danh và xác thực cho các kết nối được bảo mật trong IPSec. SA bao gồm thông tin về cơ chế mã hóa, thuật toán xác thực, địa chỉ IP của người gửi và người nhận.
- Authentication Header (AH): Là một phần của giao thức IPSec, được sử dụng để cung cấp xác thực và tính toàn vẹn dữ liệu. AH sử dụng thuật toán băm để tạo mã xác thực cho gói tin, đảm bảo rằng gói tin không bị sửa đổi trên đường truyền.
- Encapsulating Security Payload (ESP): ESP đóng vai trò cung cấp tính toàn vẹn, xác thực và bảo mật cho dữ liệu được truyền trong mạng. Bằng cách sử dụng thuật toán để mã hóa dữ liệu trong gói tin, đảm bảo rằng thông tin chỉ được giải mã bởi duy nhất người nhận chính xác.
- Internet Key Exchange (IKE): IKE có vai trò thiết lập các SA giữa hai điểm cuối trong mạng. IKE sử dụng các giao thức mã hóa khác nhau để bảo vệ các thông tin định danh và bảo mật trong quá trình thiết lập kết nối IPSec.
- Key Management: Là quá trình quản lý và phân phối các khóa mã hóa và xác thực cho các kết nối IPSec. Các khóa này được sử dụng để tạo SA và bảo vệ các thông tin nhạy cảm được truyền trong mạng.

3. Hoạt động của IPSEC

Hoạt động của IPsec:

- Xác lập kết nối an toàn: IPsec sử dụng các giao thức ISAKMP (Internet Security Association and Key Management Protocol) và IKE (Internet Key Exchange) để xác lập kết nối an toàn giữa các thiết bị.
- Tạo SA (Security Association): ISAKMP và IKE trao đổi thông tin bảo mật và tạo ra một SA (Security Association) cho mỗi kết nối. SA xác định các thông số bảo mật, bao gồm thuật toán mã hóa, thuật toán xác thực và khóa bí mật.
- Mã hóa và xác thực dữ liệu: Sau khi SA được thiết lập, dữ liệu được mã hóa và xác thực trước khi truyền.
- Giải mã và xác minh dữ liệu: Thiết bị nhận dữ liệu sẽ giải mã và xác minh dữ liệu dựa trên SA.

4. Chế độ hoạt động của IPSEC

a. Chế độ đường hầm (Tunnel mode):

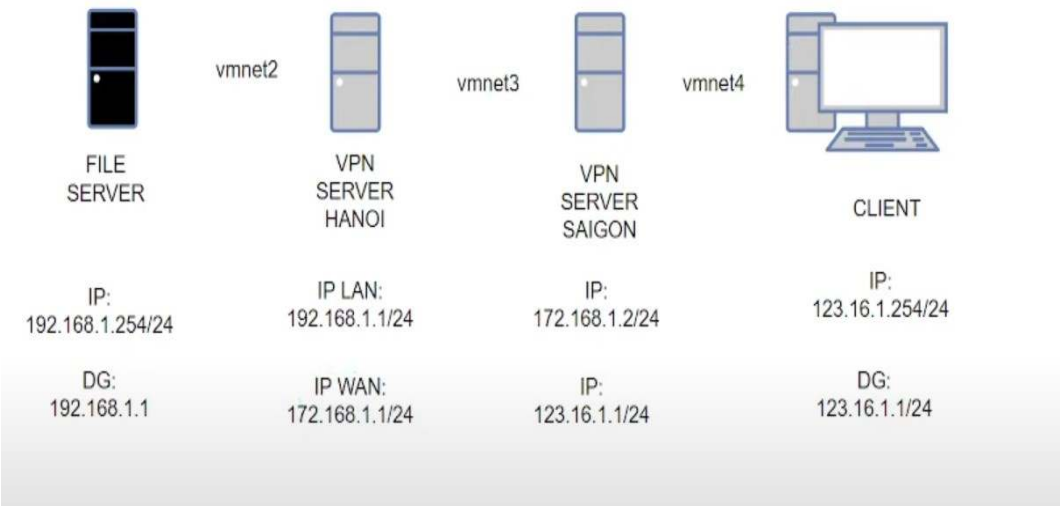
- Hoạt động: Trong chế độ đường hầm, toàn bộ gói tin IP được mã hóa, bao gồm cả tiêu đề IP và dữ liệu. IPsec tạo ra một đường hầm ảo giữa hai điểm kết nối, bao bọc gói tin gốc trong một gói tin IP mới được mã hóa.
- Ứng dụng: Chế độ đường hầm được sử dụng phổ biến cho các kết nối VPN giữa hai mạng, ví dụ như kết nối VPN giữa trụ sở chính và chi nhánh của một công ty.
- Ưu điểm: Cung cấp bảo mật cao hơn cho toàn bộ gói tin IP, giúp bảo vệ thông tin trong suốt hành trình truyền dẫn.
- Nhược điểm: Tốc độ có thể chậm hơn chế độ giao vận do phải mã hóa toàn bộ gói tin.

b. Chế độ giao vận (Transport mode):

- Hoạt động: Trong chế độ giao vận, chỉ dữ liệu được mã hóa, tiêu đề IP vẫn được giữ nguyên. IPsec thêm một tiêu đề bảo mật vào gói tin, cung cấp tính xác thực và mã hóa cho dữ liệu.
- Ứng dụng: Chế độ giao vận được sử dụng để bảo mật kết nối giữa hai thiết bị trên cùng một mạng, ví dụ như kết nối an toàn giữa hai máy tính trên mạng nội bộ của một công ty.
- Ưu điểm: Tốc độ nhanh hơn chế độ đường hầm do chỉ mã hóa dữ liệu, không mã hóa tiêu đề IP.
- Nhược điểm: Bảo mật thấp hơn chế độ đường hầm do tiêu đề IP vẫn được giữ nguyên, có thể bị lộ thông tin về nguồn gốc và đích đến của gói tin.

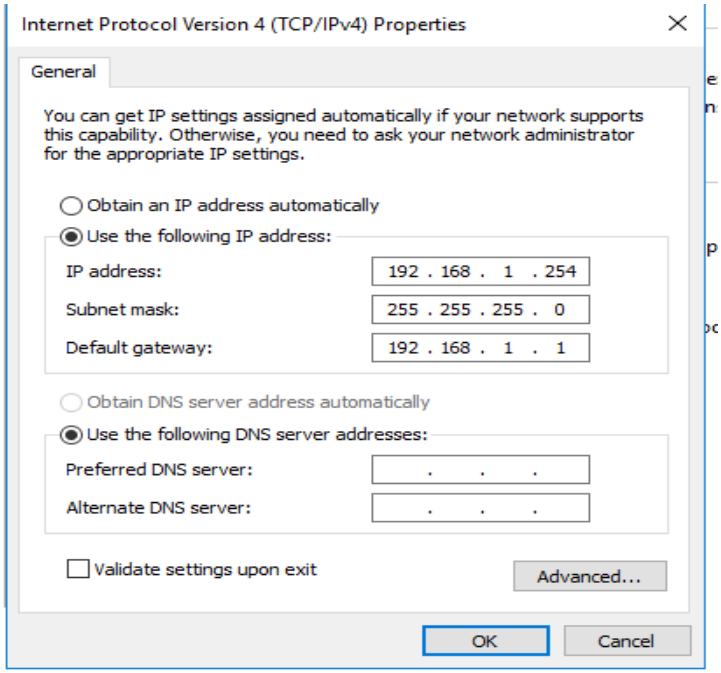
III. Demo Thiết lập hệ thống VPN Site – Site với giao thức kết nối L2TP IPSec VPN VMWARE

1. Mô hình:

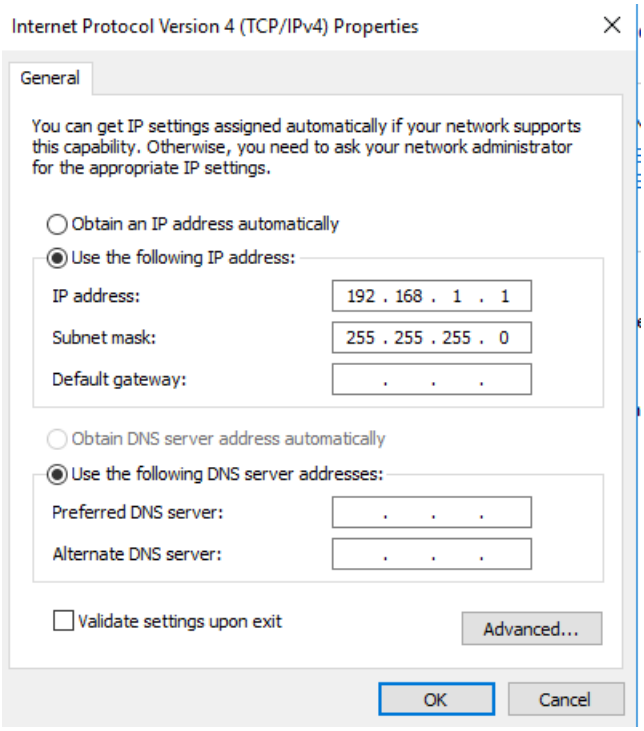


2. Các bước triển khai

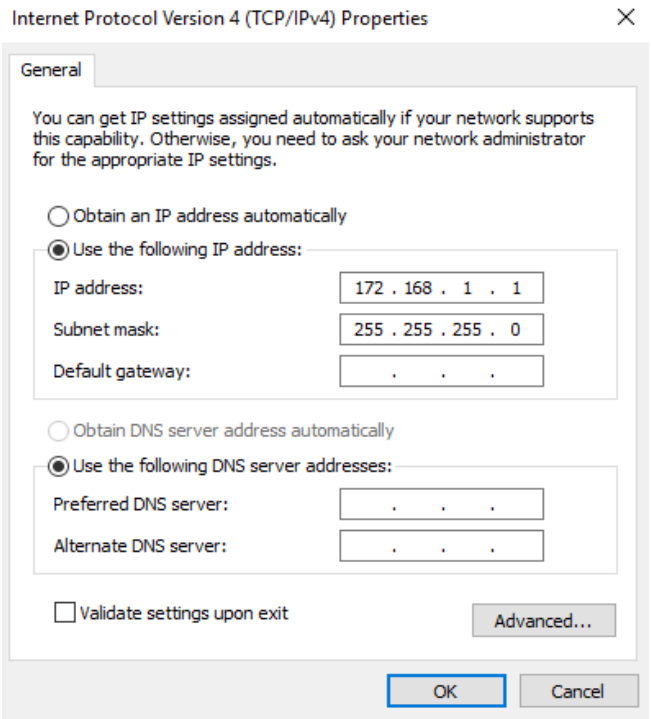
- **Bước 1: Đầu tiên Tắt Tường lửa tất cả các máy**
- **Bước 2: Cấu Hình cho máy FILE SERVER**
  - **Đặt ip cho máy File server**
  - **Card Mạng Vmnet 2 :**
  - IP Adress 192.168.1.254/24
  - Default gateway 192.168.1.1



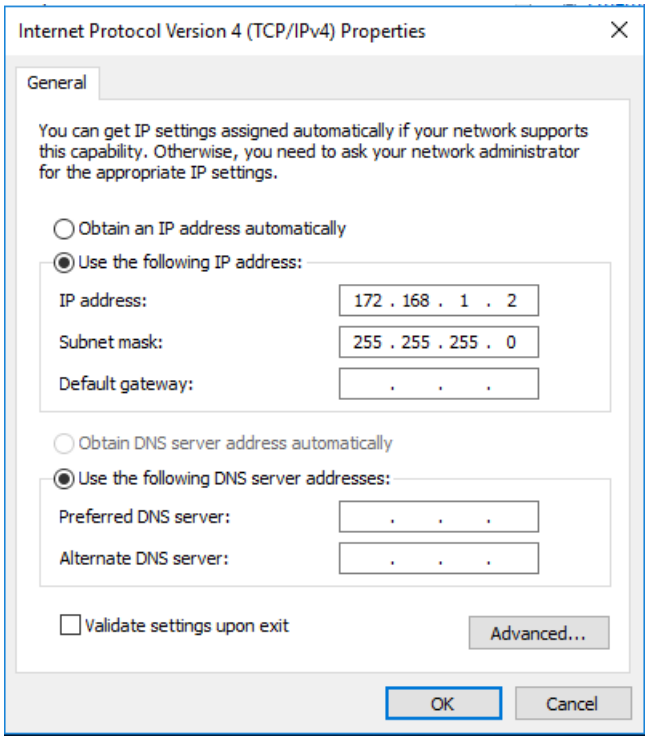
- **Cấu Hình cho máy VPN HANOI: Gồm 2 Card Mạng VMnet 2 và VMnet 3**
- Card Mạng LAN Vmnet2
- IP adress 192.168.1.1/24



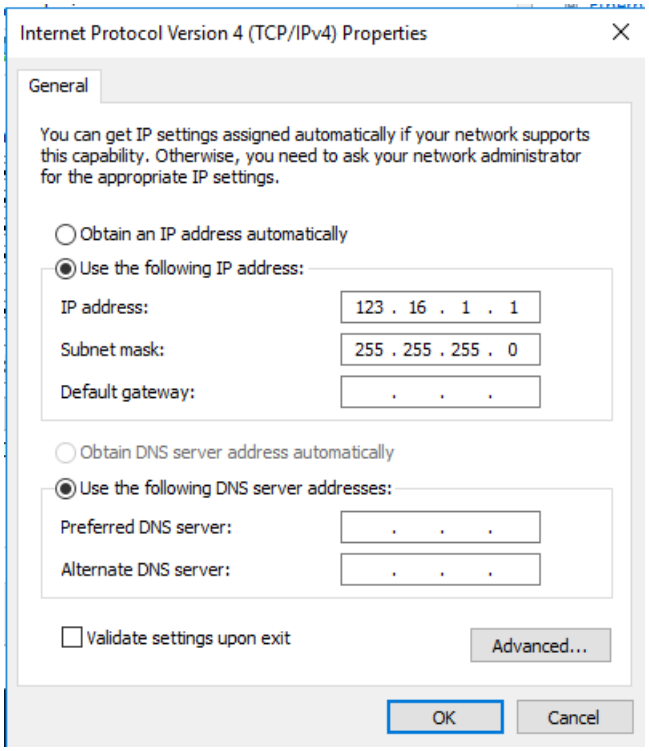
- Card Mạng Vmnet3
- IPadress 172.168.1.1/24



- **Cấu hình cho máy VNP HCM**
- **Gồm 2 card: Card mạng Vmnet3 và Vmnet 4**
  Card Mạng Vmnet 3
  IP adress = 172.168.1.2/24



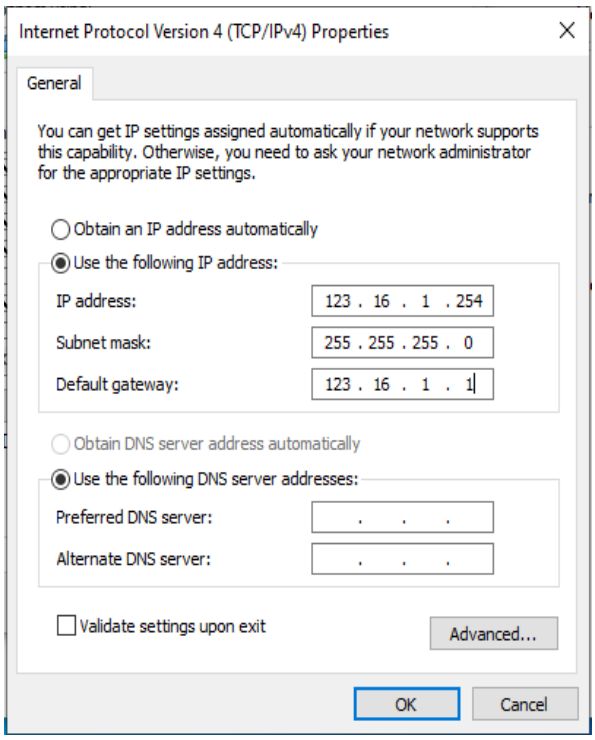
- Card Mạng Vmnet 4
- IP adress = 123.16.1.1/24



- **Cấu hình cho máy client**
- **Card Mạng Vmnet 4**

  IP adress = 123.16.1.254/24

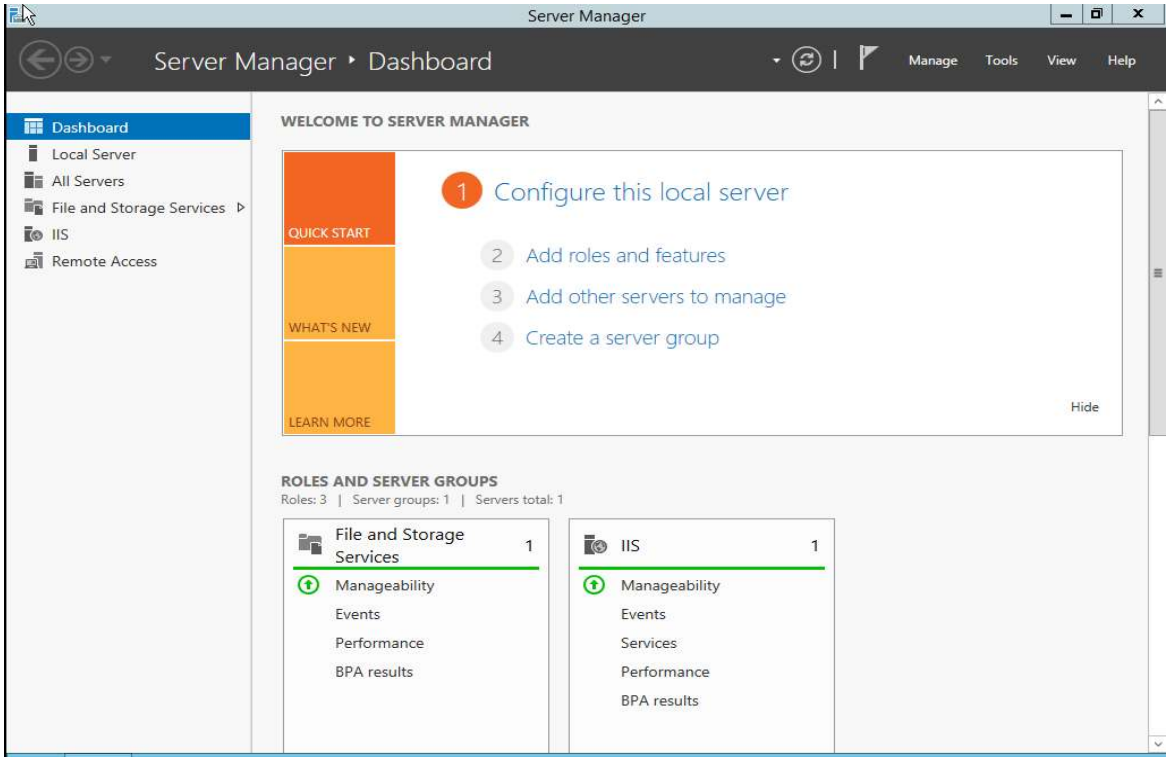
  Default gateway 123.16.1.1



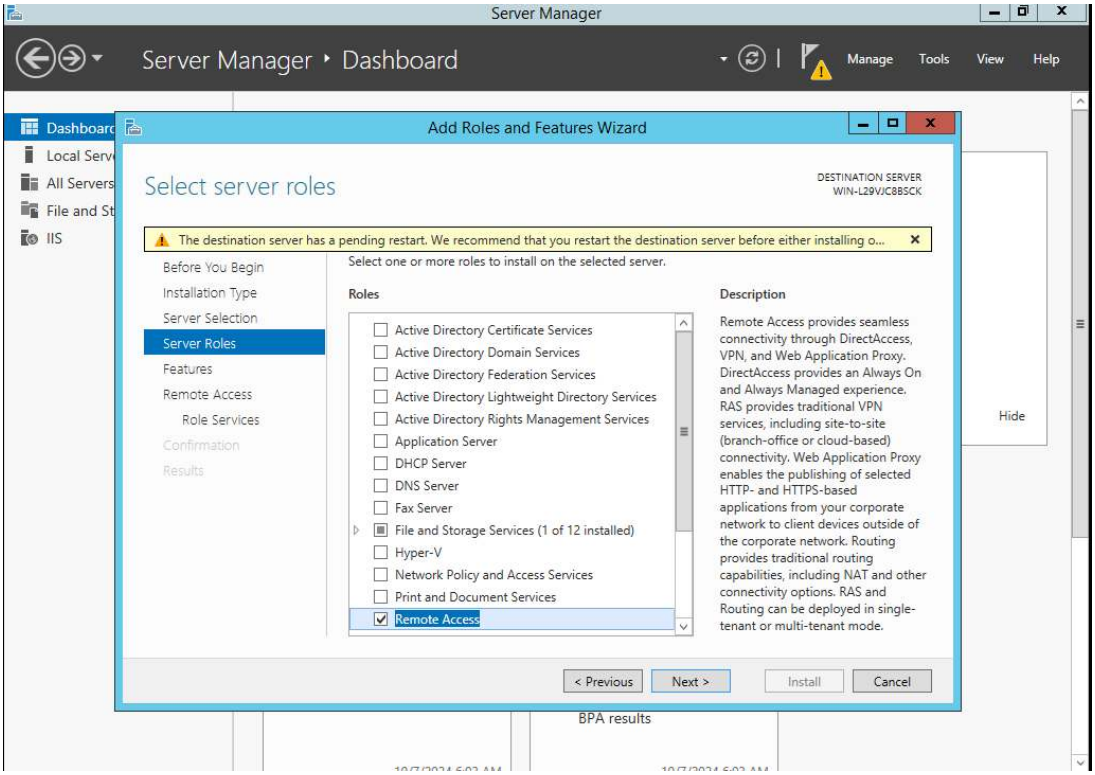
Bước 3: Cài Đặt Remote Acess

Cài đặt ở 2 máy VPN HANOI

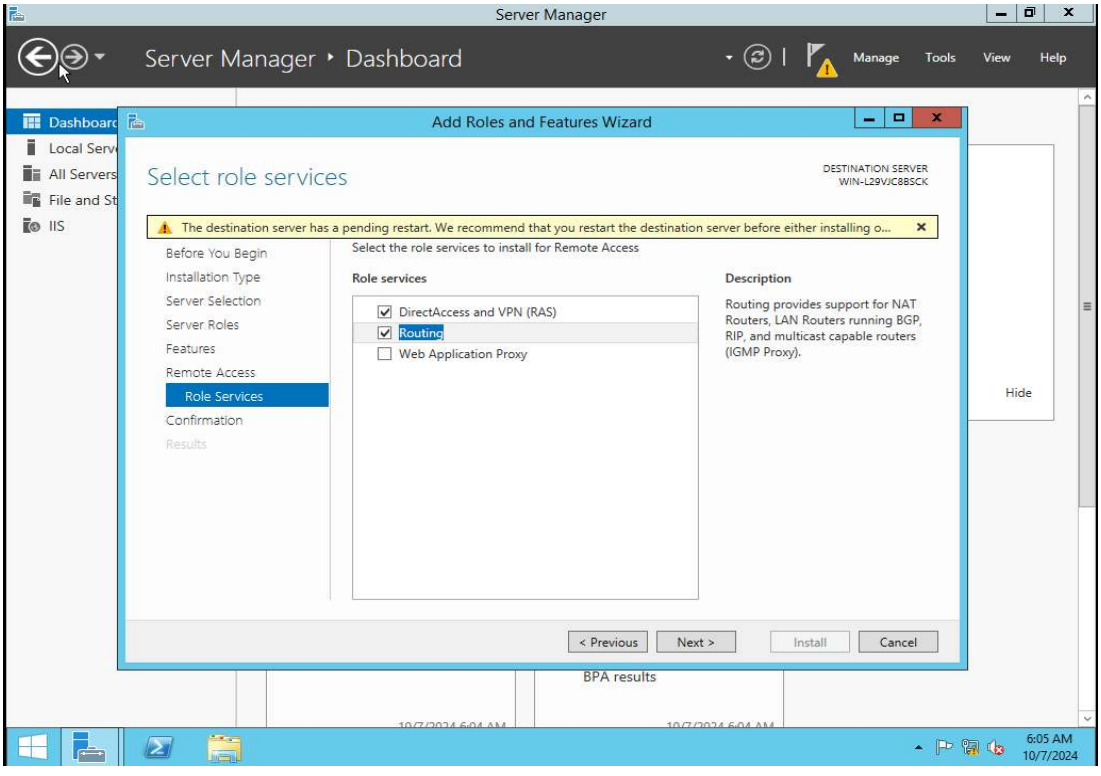
Chọn vào Add roles and feature



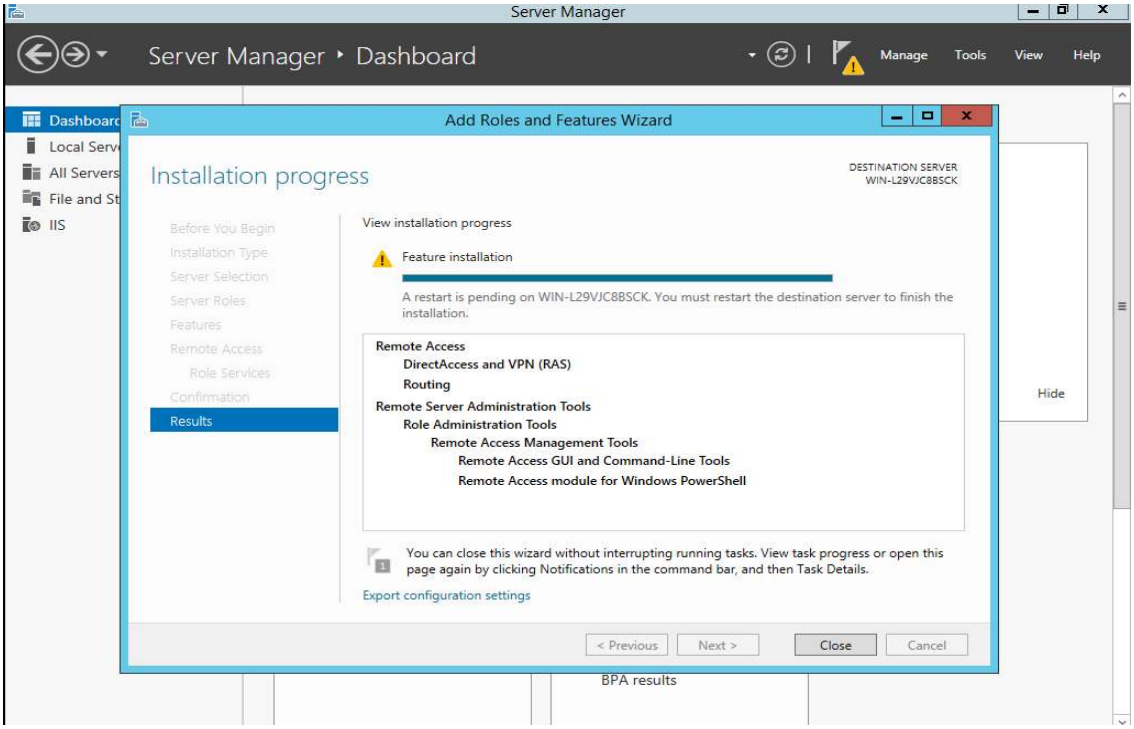
- **Tiếp tục nhấn next đến hộp thoại Select server roles thì chọn vào Remote Acess sau đó nhấn next tiếp**



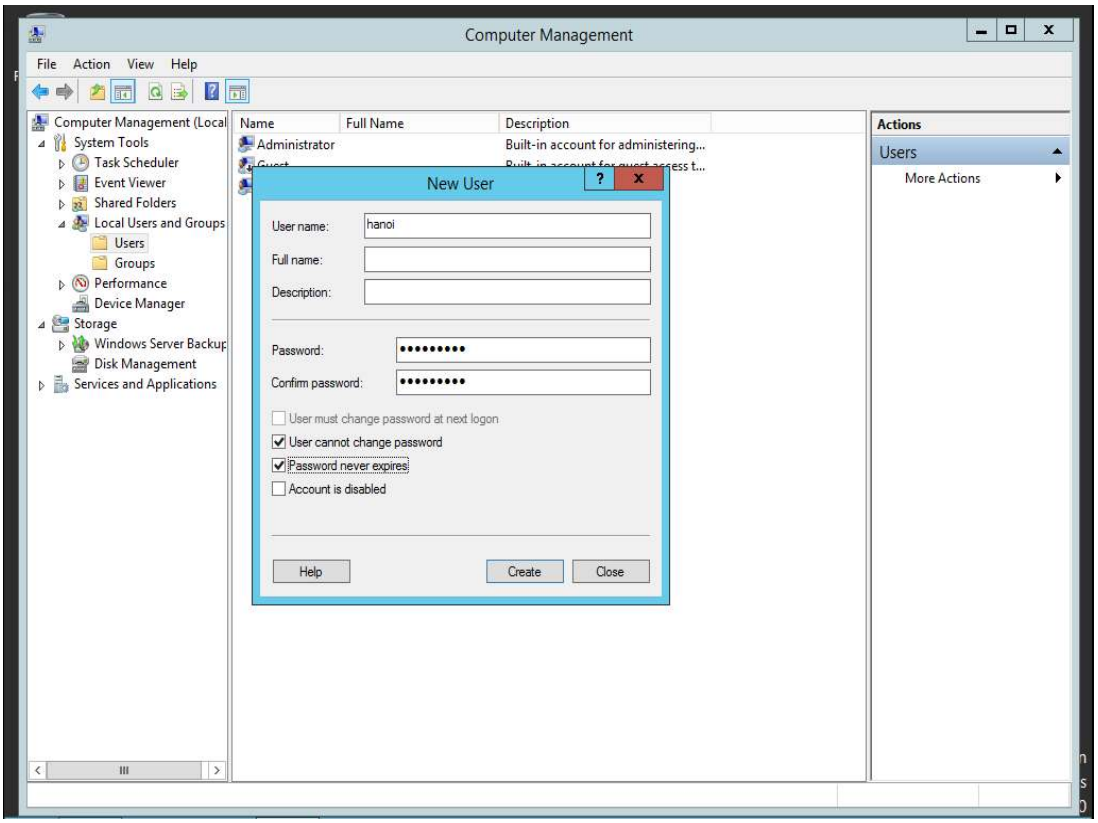
- **Đến hộp thoại role services chọn vào DirectAcess and VPN(RAS) và Routing**



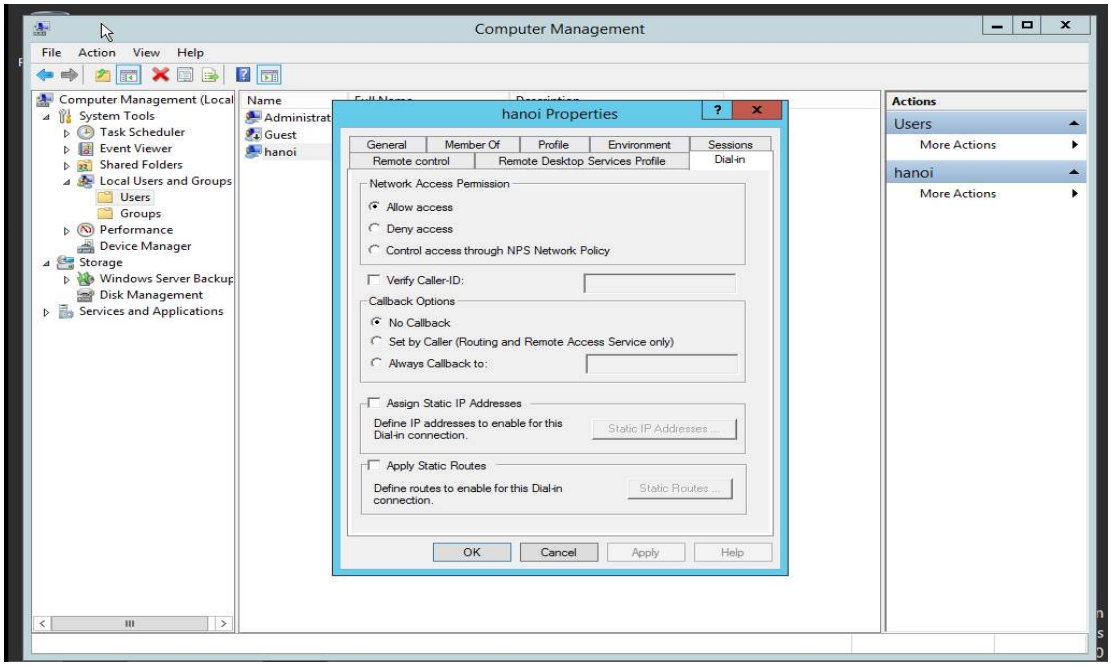
- **sau đó nhấn next và install**



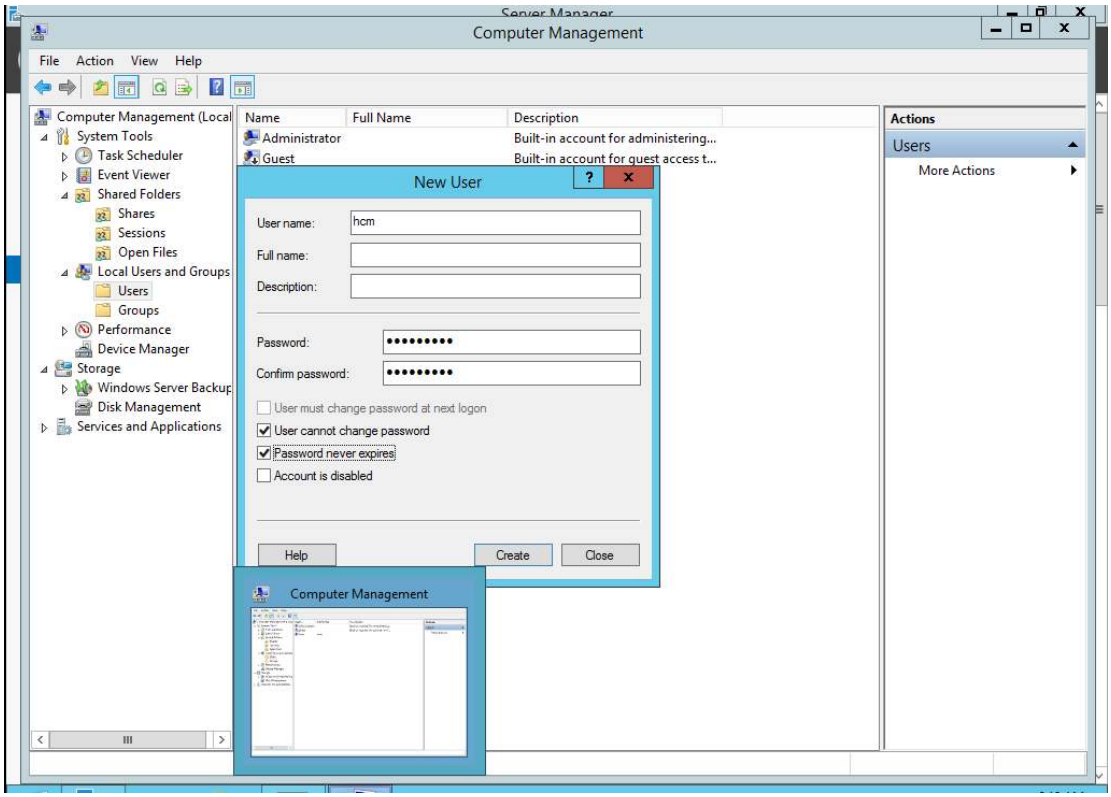
- **Tiến hành cài user cho máy VPN hanoi**
- **Tool->Computer Management->**
- **Trong hộp thoại Computer Management chọn local Users and**
- **Groups→ Users → Tạo 1 user mới có tên là hanoi**



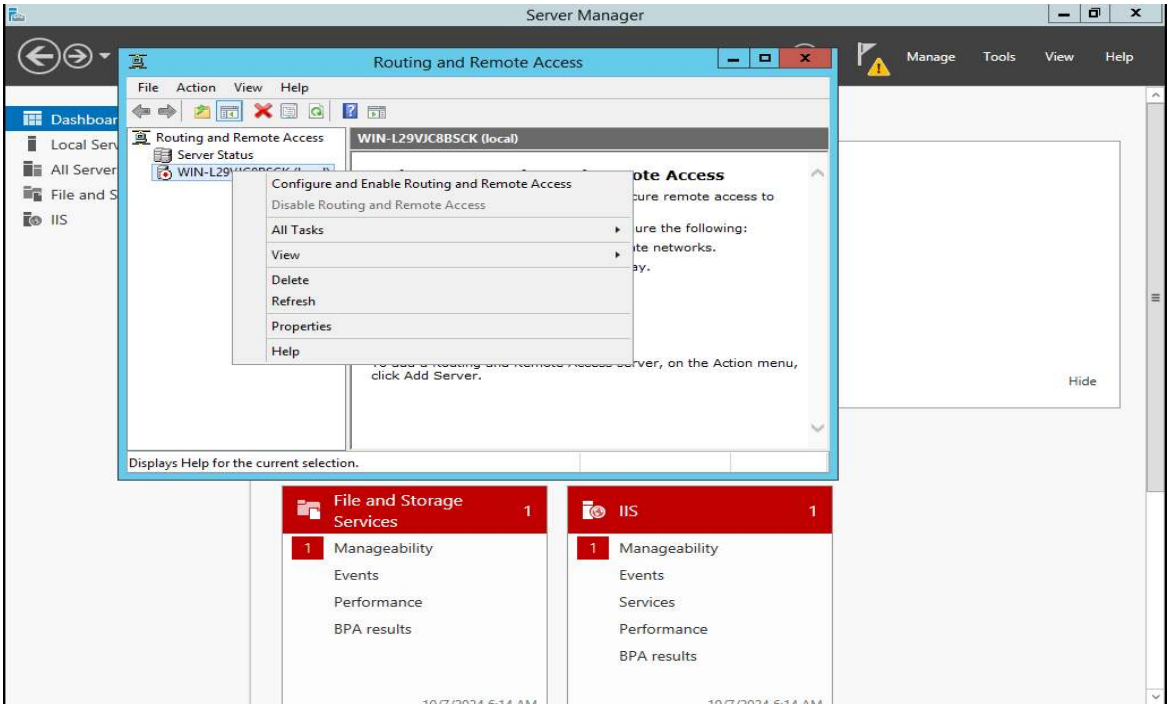
- **Trong hộp thoại Properties chọn vào Dial-in → Allow access để có thể truy cập từ xa → sau đó nhấn Apply để lưu lại**



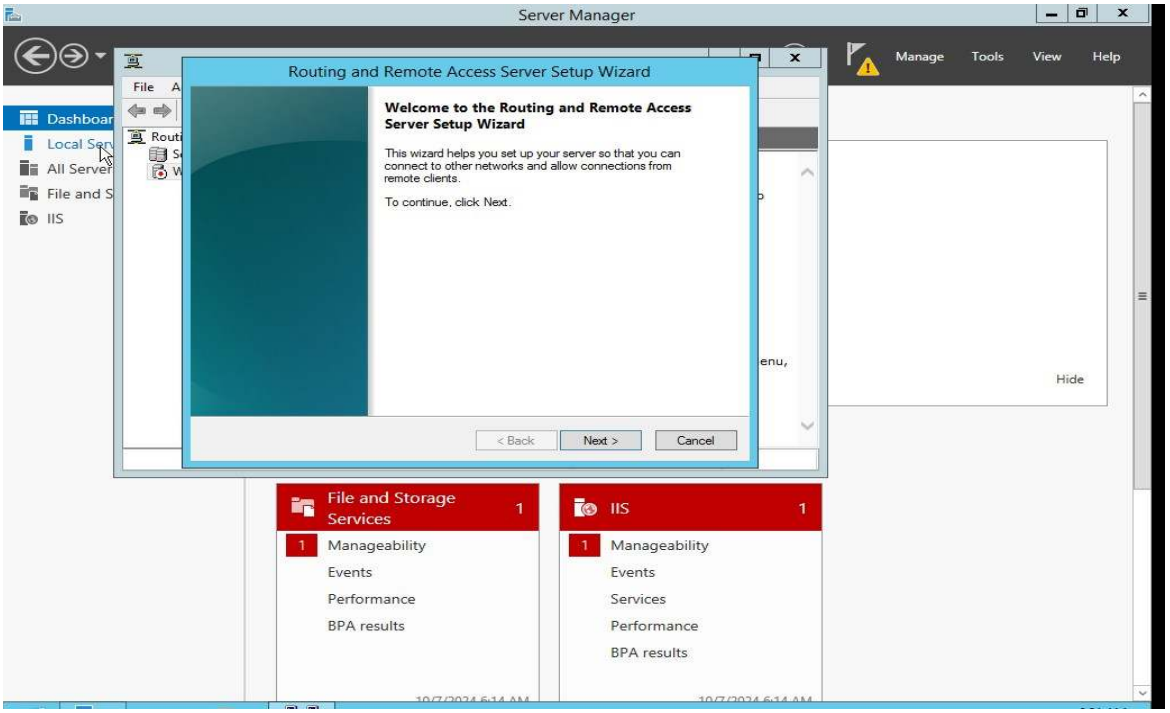
- **Tiến hành cài user cho máy VPN HCM**
- **Trong hộp thoại ComputerManagement →local Users and Groups → Users →tạo user mới có tên hcm**
- **Trong hộp Thoại hcm Properties → Dial-in →Allow access để có thể truy cập từ xa → sau đó nhấn Apply để lưu lại**



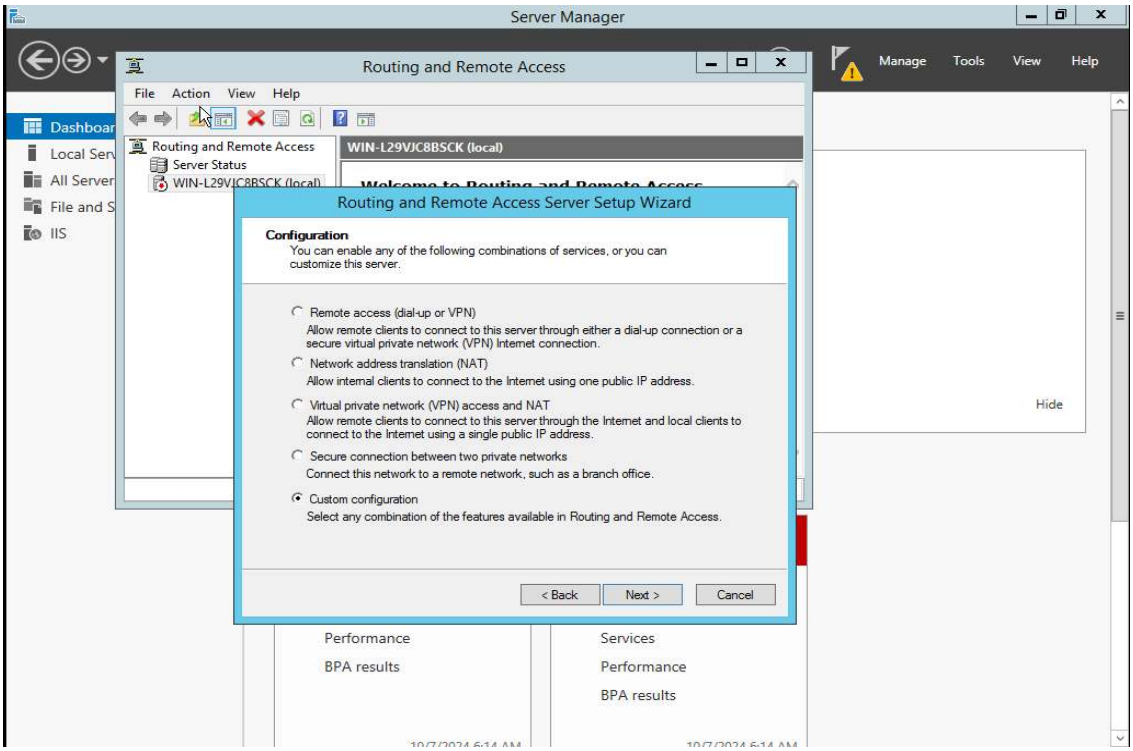
- **Quay về máy VPN HANOI**
- **Vào Tool→ Routing and Remote Access→ Xuất hiện hộp thoại chuột phải vào tên Server (VPNHANOI) →Configure and Enable Routing and Remote Acess**



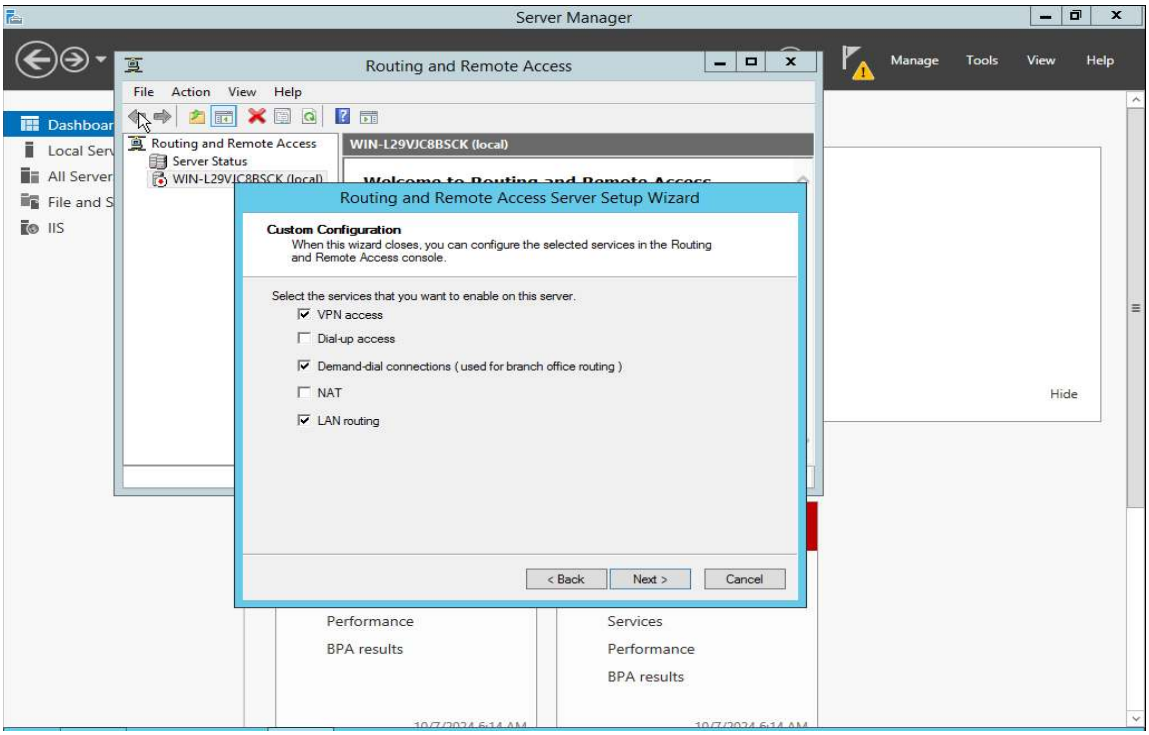
- **Xuất hiện hộp thoại Routing and Remote Acess Server Setup Wizard →Next**



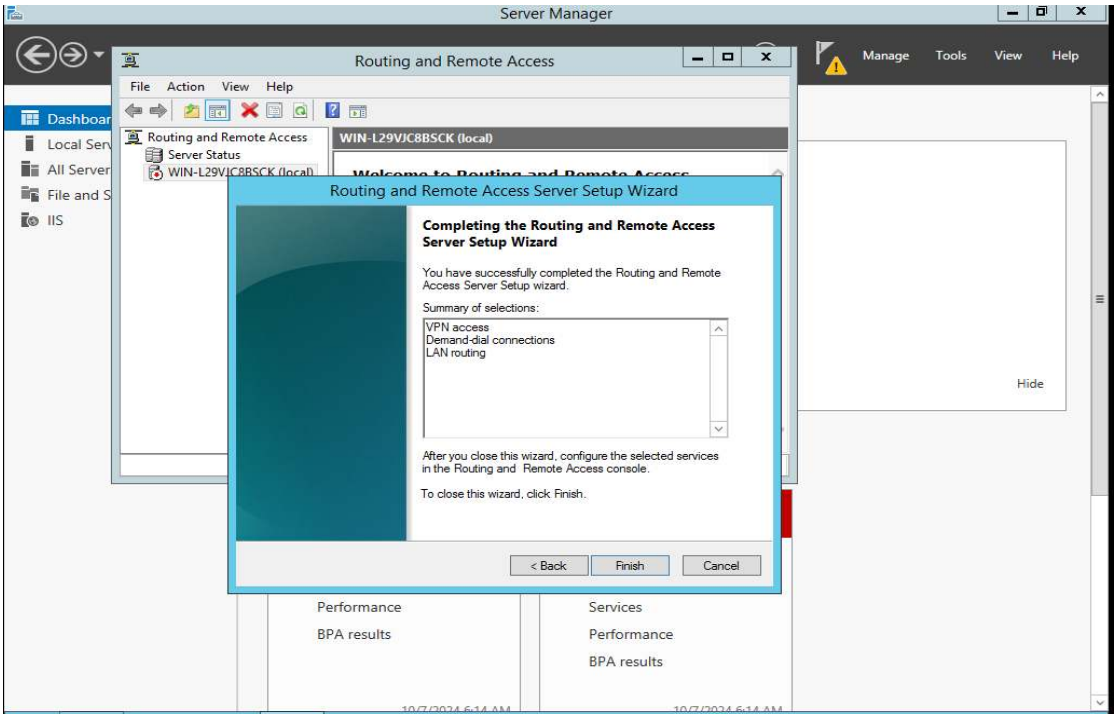
- **Chọn vào Custom configuration →Next**



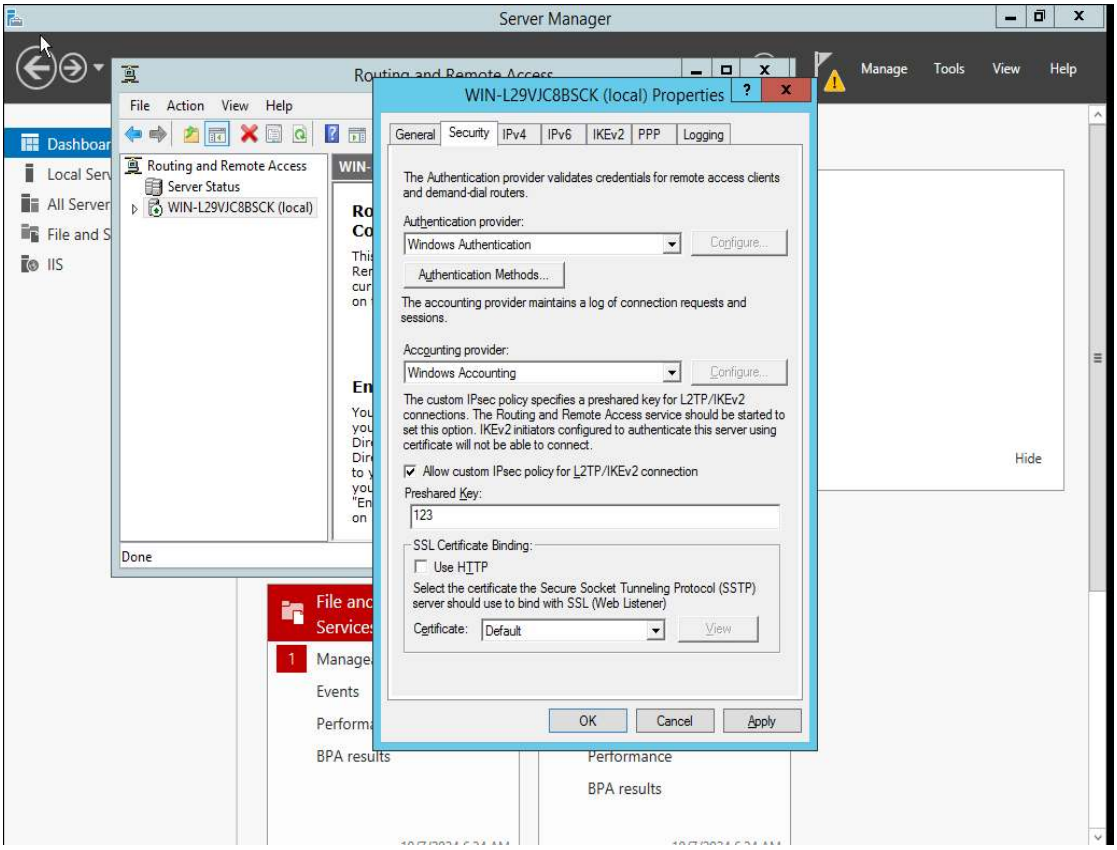
- **Ở Custom Configuration, Chọn VPN access, Demand-dial connections(used for branch office routing), LAN routing**



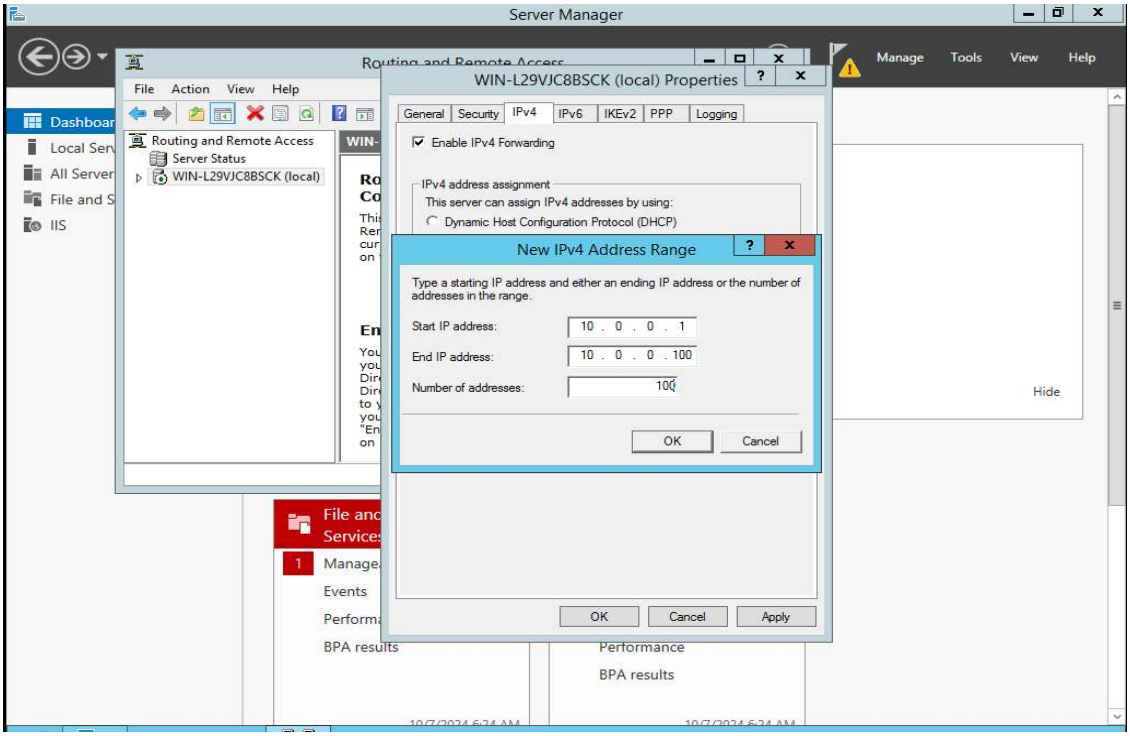
- **Tiếp tục nhấn →Next→Finish→ Start service**



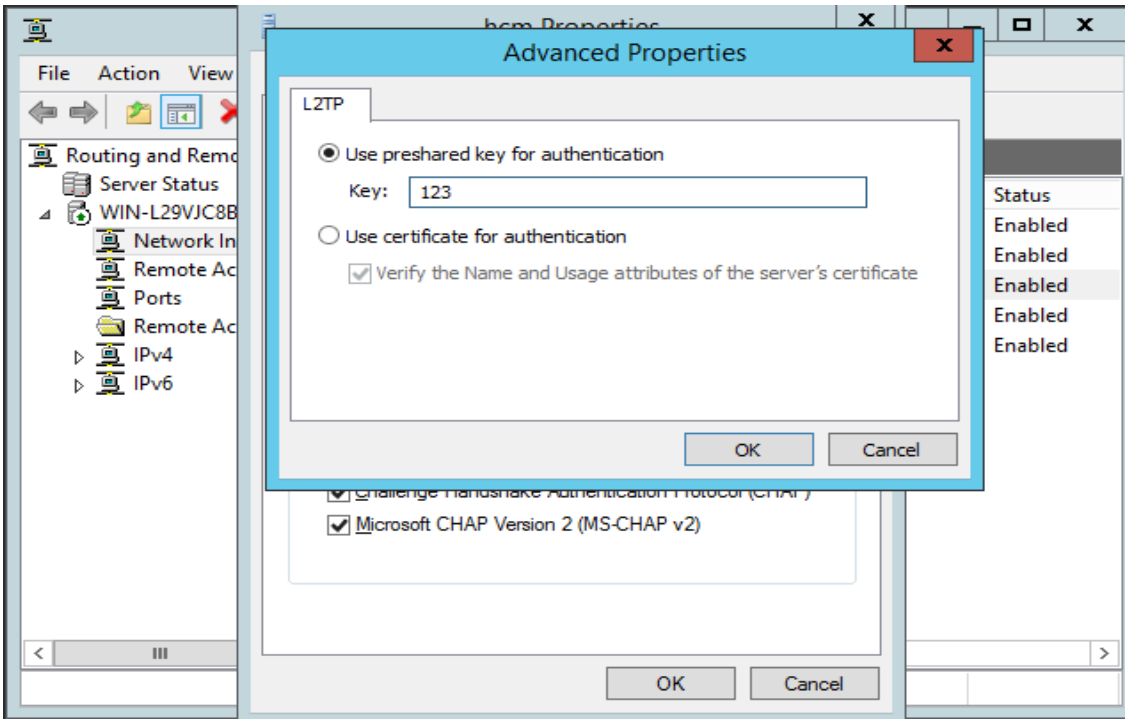
- **Máy VPN HCM làm tương tự**
- **Quay về máy VPN HANOI, trong hộp thoại WIN-L29VJC8BSCK(local) Properties →Security→ chọn Allow custom Ipsec policy for L2TP/IKEv2 connection→ Đặt Preshared Key là 123→ Apply để lưu lại**



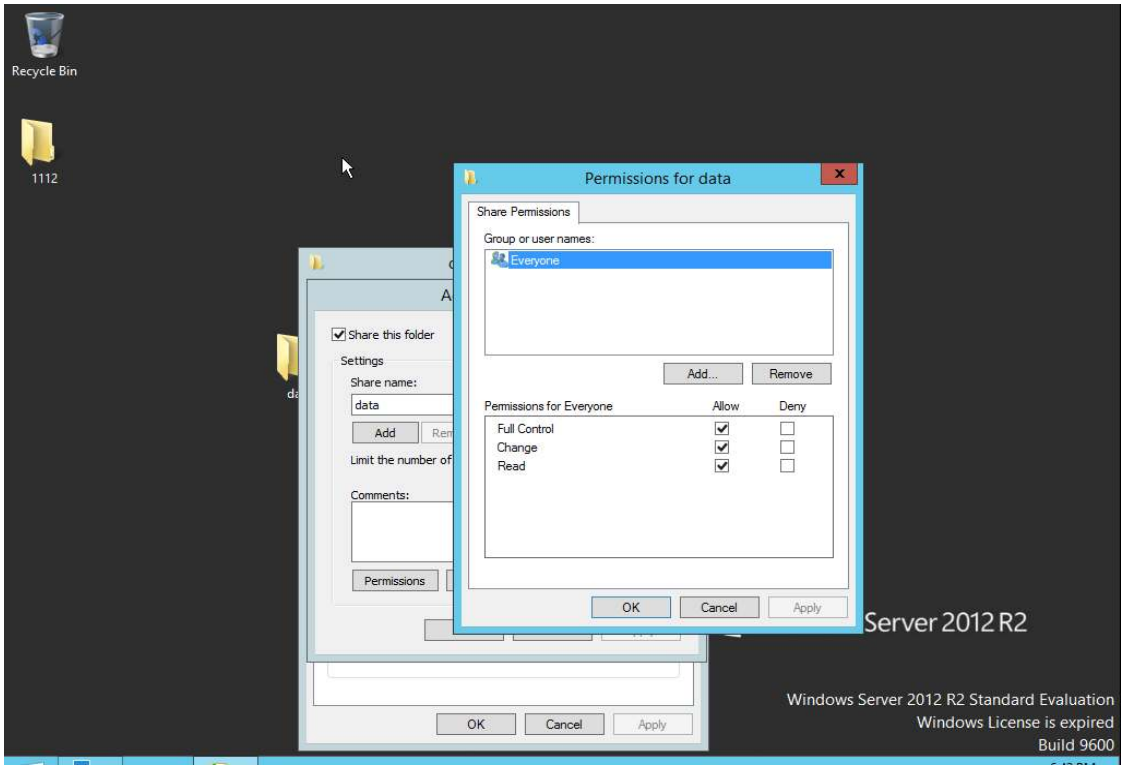
- **Trong Tag IPV4, chọn Static address pool→Add→ Start IP address là 10.0.0.1, End IP address 10.0.0.100→ OK→ Apply**



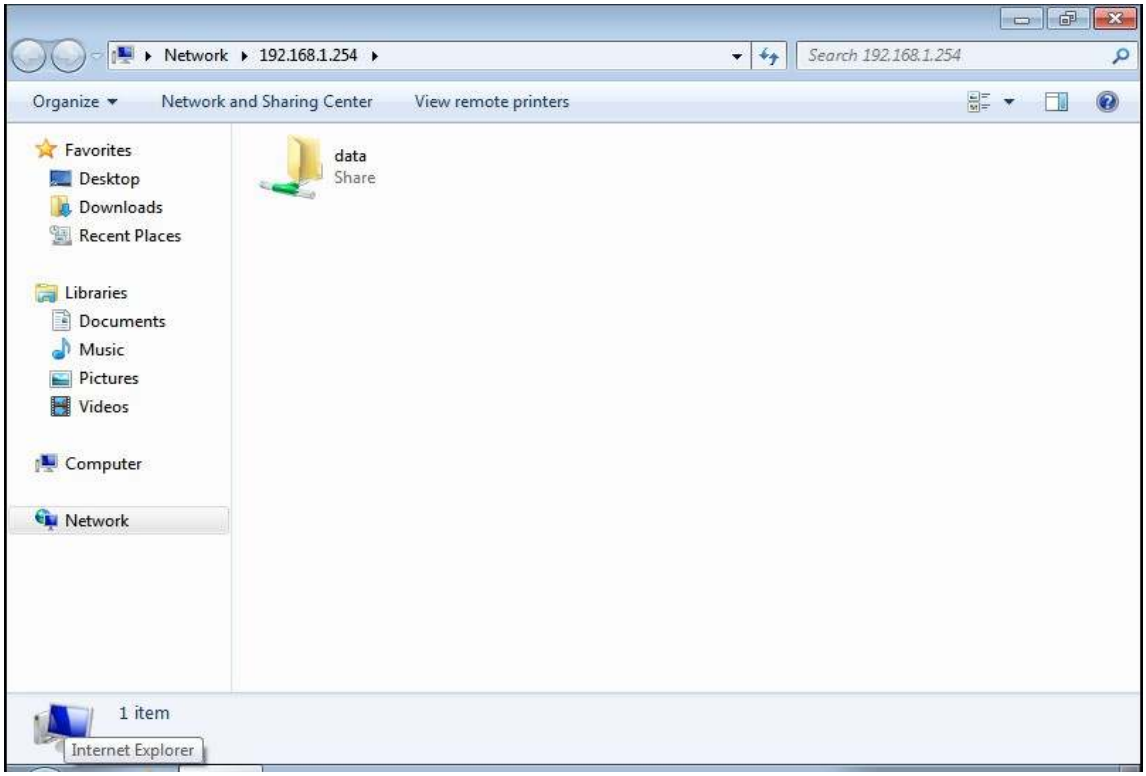
- **Máy VPN HCM làm tương tự**
- **Quay về Máy VPN HANOI, trong hộp thoại hcm(local) properties → sercurity →Advanced Settings →Use preshared key for authentication và nhập password:123 → OK**
- **Tại hộp thoại Routing and Remove access, chuột phải vào saigon và chọn properties → Connect và sang máy VPNHANOI là tương tự**



- **Sau khi đã connect xong quay về Máy FILE SEVER, tại màn hình chính tạo file DATA → chuột phải chọn Properties →Sharing →Advanced sharing →Share this folder → permission →chọn everyone →Apply →OK**



- **Chuyển sang máy client bấm windows+R → gõ \\192.168.1.254, tại đây đã xuất hiện file DATA**



TÀI LIỆU THAM KHẢO

[1] COMPUTER NETWORKS, ANDREW S. TANENBAUM, DAVID J. WETHERALL FIFTH EDITION 2011
[2] COMPUTER NETWORKING A TOP-DOWN APPROACH, Kurose, Keith Ross, 2017
[3] Bài viết của Microsoft: https://docs.microsoft.com/en-us/windows-server/networking/technologies/ipsec/ipsec-overview
[4] RFC 4301 - Security Architecture for the Internet Protocol: https://tools.ietf.org/html/rfc4301
[5] RFC 4303 - IP Encapsulating Security Payload (ESP): https://tools.ietf.org/html/rfc4303