****

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

🙣🕮🙡

**ĐỒ ÁN**

**MÔN:BẢO MẬT THÔNG TIN**

**TÊN ĐỀ TÀI: HỆ THỐNG IPSEC VPN**

Sinh viên thực hiện

1.Nguyễn Công Mạnh - 1911062046

2.Lê Viết Khả Thi - 1911065668

GVHD: ThS. Dương Minh Chiến

TP.Hồ Chí Minh – tháng 8 năm 2021

# NHẬN XÉT – ĐÁNH GIÁ

1. Hình thức trình bày

1. Nội dung

Điểm: Hình thức (20%) Nội dung (80%) Tổng kết:

Ngày Tháng Năm 2021

Giảng viên

ThS. Dương Minh Chiến

# LỜI MỞ ĐẦU

Trong giai đoạn Internet phát triển bùng nổ với tốc độ chóng mặt trên toàn thế giới kéo theo sự phát triển nhanh tróng của công nghệ thông tin. Sự phát triển của công nghệ thông tin đã đem lại những thành tựu to lớn trong việc phát triển đất nước. Việc sử dụng phần mềm ứng dụng trong đời sống không còn xa lạ với chúng ta. Những chương trình phần mềm ứng dụng bảo mật ngày càng nhiều, rất nhiều công việc thủ công đã được xử lý bằng các phần mềm chuyên dụng giảm đáng kể nhiều thời gian, công sức, nâng cao chất lượng bảo mật các hệ thống. Phần mềm bảo mật đóng vai trò rất quan trọng trong lĩnh vực bảo vệ các hệ thống server, mạng máy tính nó là công cụ hỗ trợ đắc lực và hầu như không thể thiếu.

Để có thể xây dựng được những phần mềm ứng dụng ta cần phải biết phân tích hệ thống bảo mật một cách cụ thể: những đặc điểm trong hệ thống bảo mật, ưu – nhược điểm của hệ thống. Chương trình hệ thống bảo mật IPSEC là một chương trình được xây dựng nhằm đáp ứng việc xác thực, toàn vẹn và xây dựng đường hầm cho phép nhiều loại lưu lượng được chạy qua. Trong quá trình học tập và tim hiểu chúng em được giao đề tài: “Hệ thống bảo mật IPSEC”.

Dưới sự hướng dẫn tận tình của thầy ThS. Dương Minh Chiến chúng em đã tìm hiểu và hoàn thành được bài giao. Tuy nhiên với lượng kiến thức có hạn bài làm của chúng em còn nhiều thiếu sót. Mong các thầy (cô) góp ý để bài làm của chúng em được hoàn thiện hơn.  
**Chúng em xin chân thành cảm ơn!**

## **CHƯƠNG 1. TỔNG QUAN**

## Tổng quan

Tổng quan :

Trong thập kỉ 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 cá hoạt động thương mại với quy mô lớn nhỏ khác nhau…

Ban đầu, các tổ chức cơ quan sử dụng Internet để giới thiệu các sản phẩm và dịch vụ bằng các website của mình. Cùng với thời gian, nó sẽ phát triển thành thương mại điện tử, mọi hoạt động kinh doanh, các giao dịch được thực hiện qua mạng Internet.

Bài toán đặt ra là làm thế nào để bảo mật an toàn cho các dữ liệu trong quá trình truyền qua mạng? Làm thế nào để có thể bảo vệ chống lại các cuộc tấn công trong quá trình truyền tải các dữ liệu đó? Sau đây chúng ta sẽ đi tìm hiểu về bảo mật các dữ liệu qua mạng bằng việc sử dụng IPSec

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 để này, một giải pháp đưa ra là mạng riêng ảo VPNs kết hợp với giao thức bảo mật Ipsec. Chính điều này là động lực cho sự phát triển mạng mẽ của VPNs như ngày nay

Lịch sử:

Khi Internet Protocol được phát triển vào đầu những năm 80, tính bảo mật không nằm ở vị trí được ưu tiên cao. Tuy nhiên, khi con số người dùng Internet tiếp tục phát triển, nhu cầu bảo mật cao cũng vì thế mà ngày càng tăng.

Để xử lý nhu cầu này, Cơ quan An ninh Quốc gia đã tài trợ cho sự đi lên của các giao thức bảo mật vào giữa những năm 80, trong chương trình Secure Data Network Systems (Hệ thống mạng dữ liệu bảo mật). Điều này dẫn đến sự phát triển của Security Protocol (Giao thức bảo mật) ở Layer 3 và cuối cùng là Network Layer Security Protocol. Nhiều kỹ sư đã làm việc trong dự án này trong suốt những năm 90 và IPSec đã phát triển nhờ những nỗ lực này. IPSec hiện là một tiêu chuẩn mã nguồn mở và là phần nào của IPv4

## 1.2 Nhiệm vụ

Cho phép xác thực 2 chiều, trước và trong quá trình truyền tải dữ liệu

Mã hóa đường truyền giữa 2 máy tính khi được gửi qua 1 mạng

Bảo vệ gói dữ liệu IP và phòng ngự các cuộc tấn công mạng không bảo mật

IPsec bảo vệ các lưu lượng mạng bằng việc sử dụng mã hóa và đánh dấu dữ liệu

Ipsec cho phép định nghĩa ra các loại lưu lượng mà Ipsec sẽ kiểm tra và cách các lưu lượng đó sẽ được bảo mật và mã hóa như thế nào

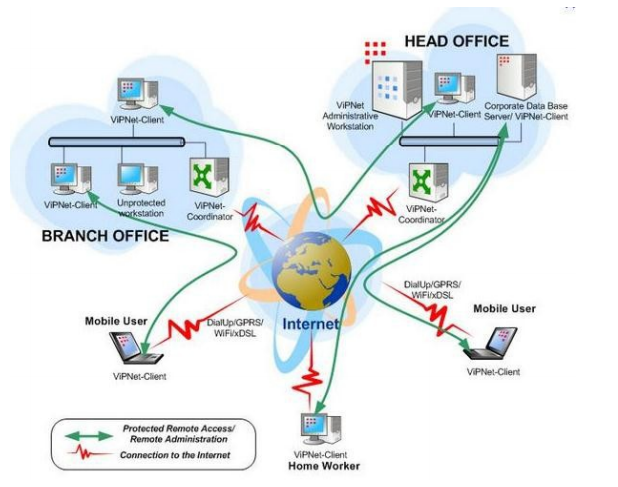
## 1.3 Cấu trúc

Sử dụng các giao thức cung cấp mật mã nhằm bảo mật gói tin trong quá trình truyền: IPsec được triển khai sử dụng các giao thức cung cấp mật mã (cryptographic protocols) nhằm bảo mật gói tin trong quá trình truyền, phương thức xác thực và thiết lập các thông số mã hoá. Cung cấp phương thức xác thực: Xây dựng IPsec sử dụng khái niệm về bảo mật trên nền tảng IP. Một sự kết hợp bảo mật rất đơn giản khi kết hợp các thuật toán và các thông số (ví như các khoá – keys) là nền tảng trong việc mã hoá và xác thực trong một chiều. Tuy nhiên trong các giao tiếp hai chiều, các giao thức bảo mật sẽ làm việc với nhau và đáp ứng quá trình giao tiếp.

Thực tế lựa chọn các thuật toán mã hoá và xác thực lại phụ thuộc vào người quản trị IPsec bởi IPsec bao gồm một nhóm các giao thức bảo mật đáp ứng mã hoá và xác thực cho mỗi gói tin IP. Thiết lập các thông số mã hóa:

• Trong các bước thực hiện phải quyết định cái gì cần bảo vệ và cung cấp cho một gói tin đi ra ngoài, IPsec sử dụng các thông số Security Parameter Index (SPI), mỗi quá trình đánh thứ tự và lưu trong dữ liệu bao gồm Security Association Database (SADB), theo suốt chiều dài của địa chỉ đích trong header của gói tin, cùng với sự nhận dạng duy nhất của một thoả hiệp bảo mật (security association) cho mỗi gói tin. Một quá trình tương tự cũng được làm với gói tin đi vào, nơi IPsec thực hiện quá trình giải mã và kiểm tra các khoá từ SADB.

• Cho các gói multicast, một thoả hiệp bảo mật sẽ cung cấp cho một group, và thực hiện cho toàn bộ các receiver trong group đó. Có thể có hơn một thoả hiệp bảo mật cho một group, bằng cách sử dụng các SPI khác nhau, tuy nhiên nó cũng cho phép thực hiện nhiều mức độ bảo mật cho một group. Mỗi người gửi có thể có nhiều thoả hiệp bảo mật, cho phép xác thực, trong khi người nhận chỉ biết được các keys được gửi đi trong dữ liêu. Chú ý các chuẩn không miêu tả làm thế nào để các thoả hiệp và lựa chọn việc nhân bản từ group tới các cá nhân



## **CHƯƠNG 2. CƠ SỞ LÝ THUYẾT**

## 2.1 Giới thiệu về giao thức/ứng dụng

**Ipsec là gì?**

IPsec đã nổi lên như một công cụ kiểm soát bảo mật lớp mạng được sử dụng phổ biến nhất để bảo vệ thông tin liên lạc. IPsec là một khuôn khổ các tiêu chuẩn mở để đảm bảo thông tin liên lạc riêng tư qua mạng IP. Giao thức Internet Key Exchange (IKE) được sử dụng để thương lượng IPsec một cách an toàn tham số và khóa mã hóa.

Nhóm Công tác IPsec tại Lực lượng Đặc nhiệm Kỹ thuật Internet (IETF) chịu trách nhiệm về duy trì và xuất bản các tiêu chuẩn cho IKE và IPsec. Tài liệu do IETF sản xuất

Nhóm làm việc được xác định theo hai loại: Yêu cầu nhận xét (RFC), được hoàn thành thông số kỹ thuật và Thư nháp trên Internet, là những tài liệu đang hoạt động có thể trở thành RFC. IKEv2 được quy định trong [23]. Tải trọng bảo mật đóng gói (ESP), giao thức bảo mật IPsec cốt lõi, được quy định trong [24]. Hướng dẫn sử dụng và triển khai thuật toán được chỉ định trong [25] cho IKEv2 và [26] cho IPsec. Các phần mở rộng khác nhau cho IKEv2 có thông số kỹ thuật RFC riêng. Các giao thức IKE và IPsec bắt nguồn từ IETF gần ba thập kỷ trước. Một số lịch sử của họ, chẳng hạn như sự khác biệt giữa IPsec-v2 và IPsec-v3

Tùy thuộc vào cách IPsec được triển khai và cấu hình, nó có thể cung cấp bất kỳ sự kết hợp nào của các loại bảo vệ sau:

* Bảo mật: IPsec đảm bảo rằng dữ liệu không thể bị phát hiện bởi các bên trái phép. Điều này được thực hiện bằng cách mã hóa và giải mã dữ liệu bằng thuật toán mật mã và khóa bí mật — giá trị chỉ được biết đối với hai bên trao đổi dữ liệu. Dữ liệu có thể chỉ được giải mã bởi người có khóa bí mật. Mặc dù có thể sử dụng Ipsec không có mã hóa, nó không được khuyến khích.
* Toàn vẹn: IPsec xác định xem dữ liệu đã bị thay đổi (cố ý hay vô ý) trong quá trình vận chuyển. Tính toàn vẹn của dữ liệu có thể được đảm bảo bằng cách tạo một thông báo giá trị mã xác thực (MAC), là một tổng kiểm tra mật mã (băm) của dữ liệu được tạo bằng khóa bí mật được hai bên đồng ý (khác với khóa bí mật mã hóa). Nếudữ liệu bị thay đổi, xác minh của MAC sẽ không thành công.
* Tính bảo mật và tính toàn vẹn. Cả hai loại séc có thể được kết hợp thành một mã hóa xác thực với thuật toán dữ liệu liên kết (AEAD). Điều này kết hợp mã hóa đối xứng và tổng kiểm tra mật mã vào một quá trình sử dụng một bí mật duy nhất thay vì hai chìa khóa riêng biệt. Cả hai bên vẫn cần có cùng một khóa bí mật và sử dụng cùng một dữ liệu được liên kết.
* Xác thực ngang hàng. Mỗi điểm cuối IPsec xác nhận danh tính của IPsec khác điểm cuối mà nó muốn giao tiếp, đảm bảo rằng lưu lượng mạng và dữ liệu chỉ được truyền đến điểm cuối mong đợi và được ủy quyền
* Bảo vệ phát lại. Dữ liệu giống nhau sẽ không được chấp nhận nhiều lần và dữ liệu không chấp nhận hoàn toàn không theo thứ tự. Điều này ngăn những kẻ tấn công sao chép và truyền lại dữ liệu được mã hóa IPsec hợp lệ cho các mục đích xấu. IPsec (như UDP) không đảm bảo rằng dữ liệu được gửi theo thứ tự chính xác mà dữ liệu đã được gửi. Người nhận có một phát lại cửa sổ nơi nó sẽ lưu trữ các tin nhắn đã nhận không theo thứ tự trước khi giải mã và gửi các thông báo này đến hệ điều hành theo đúng thứ tự.
* Bảo vệ Phân tích Lưu lượng. Khi chế độ đường hầm của IPsec được sử dụng để giám sát lưu lượng mạng không biết bên nào đang giao tiếp, làm thế nào thường xuyên xảy ra liên lạc, hoặc bao nhiêu dữ liệu đang được trao đổi. Trong khi số lượng và kích thước của các gói được mã hóa đang được trao đổi có thể được đếm, lưu lượng khả năng bảo mật luồng (TFC) của ESP có thể đệm tất cả các gói vào một độ dài duy nhất (thường là đơn vị truyền tối đa [MTU]) và các gói giả có thể được gửi tới tiếp tục làm xáo trộn thời gian của giao tiếp thực tế kiểm soát truy cập. Các điểm cuối IPsec có thể thực hiện lọc để đảm bảo rằng chỉ được ủy quyền người dùng IPsec có thể truy cập các tài nguyên mạng cụ thể. Điểm cuối IPsec cũng có thể cho phép hoặc chặn một số loại lưu lượng mạng, chẳng hạn như cho phép máy chủ web truy cập nhưng từ chối chia sẻ file. Đây được gọi là IPsec dựa trên chính sách. IPsec dựa trên định tuyến chấp nhận tất cả lưu lượng truy cập tại lớp chính sách IPsec, nhưng cả hai điểm cuối đều lọc lưu lượng truy cập hợp lệ bằng cách đặt các tuyến đường thành giao diện IPsec cụ thể. Nói cách khác, bảng định tuyến hoạt động như bộ lọc chính sách. IPsec dựa trên chính sách an toàn hơn IPsec dựa trên định tuyến, vì tính bảo mật của chính sách hoạt động độc lập với bảo mật của điểm cuối từ xa. IPsec dựa trên chính sách không dễ bị thay đổi bảng định tuyến ngẫu nhiên hoặc độc hại và nó ngăn chặn rò rỉ các gói đến mạng cục bộ, vì các gói cục bộ không sử dụng bảng định tuyến. Dựa trên Ipsec kiểm soát truy cập hoạt động độc lập với các cơ chế kiểm soát truy cập khác, chẳng hạn như dịch vụ tường lửa hoặc các cơ chế kiểm soát truy cập bắt buộc khác.
* Bảo mật Chuyển tiếp Hoàn hảo (PFS). Điểm cuối IPsec tạo khóa phiên được thay đổi thường xuyên, thường một lần một giờ. Sau đó, các điểm cuối xóa các khóa phiên cũ từ bộ nhớ dễ bay hơi và không có thực thể nào còn lại bản sao của các giải mã riêng tư này chìa khóa. Vì các khóa hết hạn không được lưu nên mọi lưu lượng được mã hóa được giám sát và lưu trữ đều không thể được giải mã sau đó bằng cách thỏa hiệp điểm cuối IPsec và lấy khóa mã hóa / giải mã thuộc các phiên IPsec trước đây. Thông thường, các khóa mới được tạo dựa trên bí mật được chia sẻ đã tạo của khóa gốc trao đổi khóa bằng cách sử dụng chức năng dẫn xuất khóa (KDF). Để đảm bảo rằng vật liệu quan trọng mới không có mối quan hệ nào với việc trao đổi khóa cũ, các khóa phiên mới có thể, tùy chọn, được được tạo bằng cách thực hiện trao đổi khóa Diffie-Hellman (DH) mới thay vì sử dụng lại bí mật được chia sẻ của trao đổi khóa cũ được tạo để tạo khóa phiên mới. Phương pháp này của sử dụng trao đổi khóa mới cung cấp bí mật chuyển tiếp hoàn hảo (PFS). Khi tài nguyên cho phép, PFS nên được sử dụng.
* Tính di động. Địa chỉ IP bên ngoài của một điểm cuối có thể thay đổi mà không gây ra gián đoạn vào luồng dữ liệu được mã hóa. Vì ứng dụng đang giao tiếp bằng cách sử dụng bên trong (được mã hóa) địa chỉ IP, không quan trọng là địa chỉ IP bên ngoài thay đổi. Điều này cho phép một thiết bị để chuyển từ WiFi sang Ethernet sang dữ liệu di động mà không bị gián đoạn ứng dụng.

Ứng dụng :

* Bảo vệ kết nối từ các mạng chi nhánh đến mạng trung tâm thông qua Internet.
* Bảo vệ kết nối truy cập từ xa (Remote Access).
* Thiết lập các kết nối Intranet và Extranet .
* Nâng cao tính bảo mật của các giao dịch thương mại điện tử

## 2.2 Nhu cầu ứng dụng IPSEC

Giao thức TCP/IP đóng 1 vai trò rất quan trọng trong các hệ thống hiện nay. Về nguyên tắc, có nhiều tùy chọn khác nhau về giao thức để triển khai các hệ thống như TCP/IP, TPX/SPX, NetBEUI, Apple Talk,… Tuy nhiên TCP/IP là sự lựa chọn gần như bắt buộc do giao thức này được sử dụng làm giao thức nền tảng của mạng Internet

Vào thời điểm thiết kế giao thức này, vấn đề bảo mật thông tin chưa thật sự được quan tâm, do đó các giao thức trong bộ TCP/IP hầu như không được trang bị bất cứ giao thức nào. Cấu trúc gói dữ liệu(IP,TCP,UDP và cả các giao thức ứng dụng) được mô tả công khai, bắt được gói IP trên mạng, ai cũng có thể phân tích gói để đọc phần dữ liệu chứa bên trong, đó là chưa kể hiện nay, các công cụ bắt và phan tích gói được sử xây dựng với tính năng mạnh và phát hành rộng rãi. Việc bổ sung các cơ chế bảo mật vào mô hình TCP/IP, bắt đầu từ giao thức IP là 1 nhu cầu cấp bách. IP security(IP sec) là 1 giao thức được chuẩn hóa bởi IETF từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hóa và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, Ipsec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đản bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thieeys bị mạng Ipsec cung cấp 1 cơ cấu bảo mật ở tầng 3( Network Layer) của mô hình OSI

Ipsec được thiết kế như phần mở rộng của giao thức IP, được thực hiện thông nhất trong cả 2 phiên bản Ipv4 và Ipv6. Đối với Ipv4, việc áp dụng Ipsec là 1 tùy chọn, nhưng đối với Ipv6, giao thức này được triển khai bắt buộc

## 2.3 Lịch sử phát triển

Sự xuất hiện mạng chuyên dùng ảo, còn gọi là mạng riêng ảo (VPN), bắt nguồn từ yêu cầu của khách hàng (client), mong muốn có thể kết nối một cách có hiệu quả với các tổng đài thuê bao (PBX) lại với nhau thông qua mạng diện rộng (WAN). Trước kia, hệ thống điện thoại nhóm hoặc là mạng cục bộ (LAN) trước kia sử dụng các đường thuê riêng cho việc tổ chức mạng chuyên dùng để thực hiện việc thông tin với nhau. Các mốc đánh dấu sự phát triển của VPN: - Năm 1975, Franch Telecom đưa ra dịch vụ Colisee, cung cấp dịch vụ dây chuyên dùng cho các khách hàng lớn. Colisee có thể cung cấp phương thức gọi số chuyên dùng cho khách hàng. Dịch vụ này căn cứ vào lượng dịch vụ mà đưa ra cước phí và nhiều tính năng quản lý khác. - Năm 1985, Sprint đưa ra VPN, AT&T đưa ra dịch vụ VPN có tên riêng là mạng được định nghĩa bằng phần mềm SDN. - Năm 1986, Sprint đưa ra Vnet, Telefonica Tây Ban Nha đưa ra Ibercom. - Năm 1988, nổ ra đại chiến cước phí dịch vụ VPN ở Mỹ, làm cho một số xí nghiệp vừa và nhỏ chịu nổi cước phí sử dụng VPN và có thể tiết kiệm gần 30% chi phí, đã kích thích sự phát triển nhanh chóng dịch vụ này tại Mỹ. - Năm 1989, AT&T đưa ra dịch vụ quốc tế IVPN là GSDN. - Năm 1990, MCI và Sprint đưa ra dịch vụ VPN quốc tế VPN; Telstra của Ôxtrây-li-a đưa ra dich vụ VPN rong nước đầu tiên ở khu vục châu Á – Thái Bình Dương. - Năm 1992, Viễn thông Hà Lan và Telia Thuỵ Điển thành lập công ty hợp tác đầu tư Unisource, cung cấp dịch vụ VPN. - Năm 1993, AT&T, KDD và viễn thông Singapo tuyên bố thành lập Liên minh toàn cầu Worldparners, cung cấp hàng loạt dịch vụ quốc tế, trong đó có dịch vụ VPN. - Năm 1994, BT và MCI thành lập công ty hợp tác đầu tư Concert, cung cấp dịch vụ VPN, dịch vụ chuyển tiếp khung (Frame relay)… Năm 1995, ITU-T đưa ra khuyến nghị F-16 về dịch vụ VPN toàn cầu (GVPNS). - Năm 1996, Sprint và viễn thông Đức (Deustch Telecom), Viễn thông Pháp (French Telecom) kết thành liên minh Global One. - Năm 1997 có thể coi là một năm rực rỡ đối với công nghệ VPN, công nghệ này có mặt trên khắp các tạp chí khoa học công nghệ, các cuộc hội thảo… Các mạng VPN xây dựng trên cơ sở hạ tầng mạng Internet công cộng đã mang lại một khả năng mới, một cái nhìn mới cho VPN. Công nghệ VPN là giải pháp thông tin tối ưu cho các công ty, tổ chức có nhiều văn phòng, chi nhánh lựa chọn. Ngày nay, với sự phát triển của công nghệ, cơ sở hạ tầng mạng IP (Internet) ngày một hoàn thiện đã làm cho khả năng của VPN ngày một hoàn thiện

## 2.4 Công nghệ áp dụng

(Hiệp hội Bảo mật Internet và Giao thức Quản lý Khóa (ISAKMP)) - Quản lý các khóa và trình xác thực của các kết nối an toàn.

* RFC 2409 (Internet Key Exchange (IKE)) - Trao đổi khóa.
* RFC 2410 (Thuật toán mã hóa NULL và việc sử dụng nó với IPsec) - Thuật toán mã hóa 0 và việc sử dụng nó.
* RFC 2411 (Lộ trình tài liệu bảo mật IP) - Phát triển thêm tiêu chuẩn.
* RFC 2412 (Giao thức xác định khóa OAKLEY) - Kiểm tra sự tuân thủ chính.

IPsec sử dụng các giao thức sau để thực hiện các chức năng khác nhau:

* Authentication Header (AH) cung cấp tính toàn vẹn của kết nối ảo (dữ liệu được truyền), xác thực nguồn thông tin và một chức năng bổ sung để ngăn truyền lại gói tin
* Internet Protocol Encapsulating Security Payload (ESP) có thể cung cấp tính bảo mật (mã hóa) thông tin được truyền đi, hạn chế luồng lưu lượng bí mật. Ngoài ra, nó có thể cung cấp tính toàn vẹn của kết nối ảo (dữ liệu được truyền), xác thực nguồn thông tin và chức năng bổ sung ngăn truyền lại các gói (Bất cứ khi nào sử dụng ESP, bắt buộc phải sử dụng một hoặc một bộ dịch vụ bảo mật khác)
* Security association (SA) cung cấp một loạt các thuật toán và dữ liệu cung cấp các tham số cần thiết để AH và / hoặc ESP hoạt động. Hiệp hội Bảo mật Internet và Giao thức Quản lý Khóa (ISAKMP) cung cấp một khuôn khổ để xác thực và trao đổi khóa, xác thực khóa.

Vì các kết nối ảo an toàn (SA) là đơn giản nên cần ít nhất hai SA để thiết lập liên kết song công. Ngoài ra, mỗi giao thức (ESP / AH) phải có SA riêng cho mỗi hướng, nghĩa là, gói AH + ESP yêu cầu bốn SA. Tất cả dữ liệu này được đặt trong SADB.

* AH: Thuật toán xác thực.
* AH: khóa bí mật để xác thực
* ESP: thuật toán mã hóa.
* ESP: khóa mã hóa bí mật.
* ESP: sử dụng xác thực (có / không).
* Tùy chọn trao đổi chìa khóa
* Hạn chế định tuyến
* Chính sách lọc IP

## 2.5 Các giao thức tương đương

SA(Security Associations): Là 1 khái niệm cơ bản trong bộ giao thức IPSec.SA là 1 kết nối luận lý theo phương hướng duy nhất giữa 2 thực thể sử dụng các dịch vụ IPSec.SA gồm có 3 trường:



* SPI( Security Parameter Index): Là 1 trường 32 bits dùng nhận dạng các giao thức bảo mật, được định nghĩa bởi các trường Security protocol trong bộ IPSec đang dùng, SPI như là phần đầu của giao thức bảo mật và thường chọn chọn bởi hệ thống đích trong suốt quá trình thỏa thuận của SA
* Destination IP address: Địa chỉ IP của nút đích. Cơ chế quản lý của SA chỉ được định nghĩa cho hệ thống unicasst mặc dù nó có thể là thệ thống boardcast, unicast hay multicast
* Security protocol: Mô tả giao thức bảo mật Ipsec là AH hoặc ESP.SA trong Ipsec được triển khai theo 2 chế độ : Transport mode và tunnel mode

## 2.6 Các Mô hình giao thức tương đương

Ipsec cung cấp tính năng mã hóa và xác thực mạnh cho lưu lượng IP và cũng cung cấp tính năng trao đổi và làm tươi khóa dựa trên chứng chỉ nhờ sử dụng IKE. Để đi đến kết luận 1 cách thận trọng, ta phải để xuất rằng những tính năng này là cần thiết giống như tính năng mà SSL và TLS cung cấp. Trong phần này chúng ta lưu ý dến sự giống nhàu và khác nhau cơ bản giữa IPSec / SSl và giải thích những phạm vi nào sử dụng cả 2 giao thức

**Điểm giống giữa IPSec và SSL:**

* IPSec và SSL cung cấp xác thực Client và Server
* IPSec và SSL cung cấp tính năng đảm bảo an toàn và xác thực đối với dữ liệu thậm chí trên các mức khác nhau của chồng giao thức
* IPSec và SSL có thể dùng các thuật toán mật mã mạnh cho việc mã hóa và các hàm băm, có thể sử dụng xác thực dựa trên chứng chỉ
* IPSec và SSL cung cấp tính năng sinh khóa và làm tươi khóa mà không phải truyền bất cứ khóa nào dưới dạng rõ hay ngoại tuyến

**Điểm khác giữa IPSec và SSL:**

* SSL được thực thi như 1 API giữa tâng ứng dụng và tầng vận tải, IPSec được thực thi như 1 khung làm việc tại tầng liên mạng
* SSL cung cấp tính năng bảo mật từ ứng dụng - tới - ứng dụng. VD: giữa WebBrowser và WebServer. IPSec cung cấp tính năng bảo mật từ thiết bị tới thiết bị
* SSL không bảo vệ lưu lượng UDP: IPSec thì có hầm. Điều này có thể là 1 vấn đề lúc lưu lượng cần được xem xét bằng cách kiểm tra nội dung và quét virus trước khi nó được phân phối thành công đến đích, IPSec có thể hoạt động theo 2 cách, điểm đầu tới điểm cuối và như 1 đường hầm
* SSL có thể vượt qua NAT hoặc SOCKS, chúng dùng để che dấu cấu trúc địa chỉ bên trong hoặc tránh sự xung đột địa chỉ IP riêng: IPSec trong chế độ vận tải( end-to-end) không thể sử dụng NAT nhưng nó có thể dùng 1 đường hầm IPSec để đạt được mục tiêu tương tự và thậm chí bảo mật hơn NAT vì đường hầm cũng có thể được mã hóa
* Các ứng dụng cần phải sử đổi để sử dụng SSL. Điều này có thể là 1 vấn đề lúc ta không truy cập được mã nguồn của ứng dụng hoặc không có thời gian hay kinh nghiệm để thay đổi mã nguồn của ứng dụng. IPSec hoàn toàn trong suốt với các ứng dụng. Thông thường SSL là tốt lúc ta chỉ có ứng dụng được bảo vệ và nó đã sẵn có trong 1 phiên bản SSL-aware. Đây là trường hợp có 1 ứng dụng chuản da dạng, không chỉ với WebBrowser và WebServer. Ngoài ra, nếu có tùy chọn của việc thực thi khái niệm 3-tier bằng cách tận dụng các cổng ứng dụng Web tại vành đai của mạng, SSL là 1 sự lựa chọn tốt. Nếu có 1 số lượng lớn các ứng dụng để bảo đảm an toàn có thể phải chọn giải pháp tốt hơn cho mạng. Trong trường hợp này, IPSec là sự lựa chọn tốt hơn. Trừ khi tự ta phát triển các ứng dụng. IPSec mềm dẻo hơn SSL để thực thi 1 chính sách bảo mật yêu cầu nhiều mức khác nhau và sự kết hợp của xác thực, mã hóa và đường hầm

## 2.7 Ưu điểm và Nhược điểm của IPSEC

**Ưu điểm:**

Khi Ipsec được triển khai trên bức tường lửa hoặc bộ định tuyến của 1 mạng riêng thì tính năng an toàn của Ipsec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan tới bảo mật

Ipsec được thực hiển bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi Ipsec được triển khai

Ipsec có thể được cấu hình để hoạt động 1 cách trong suốt đói với các ứng dụng đầu cuối, điều này giúp che dấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua Internet

**Nhược điểm:**

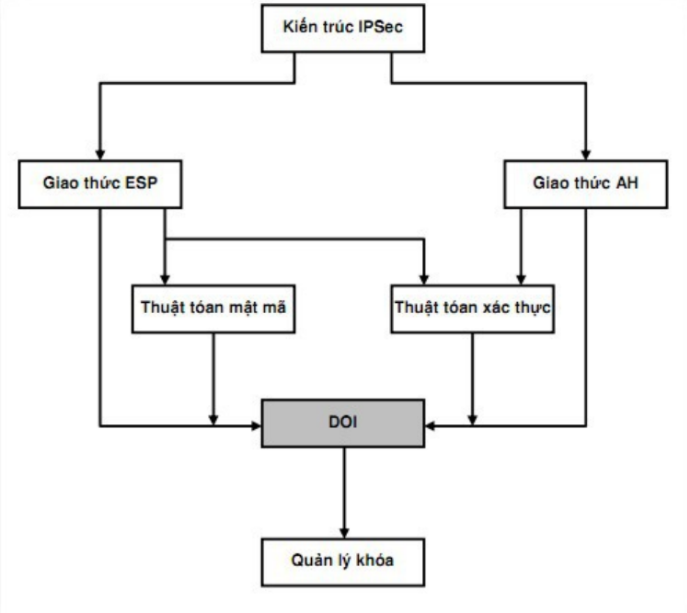
Tất cả các gói được xử lý theo Ipsec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén các dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa

Ipsec được thiết kế chỉ để hỗ trợ bảo mật thông tin cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác

Việc tính toán nhiều giải thuật phức tạp trong Ipsec vẫn còn là 1 vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu

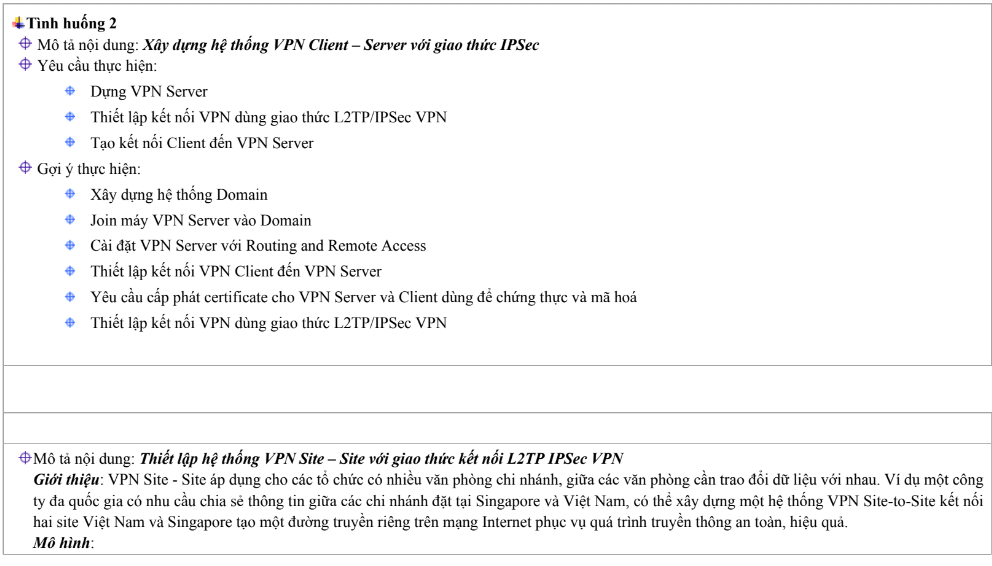
Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế với chính phủ 1 số quốc gia

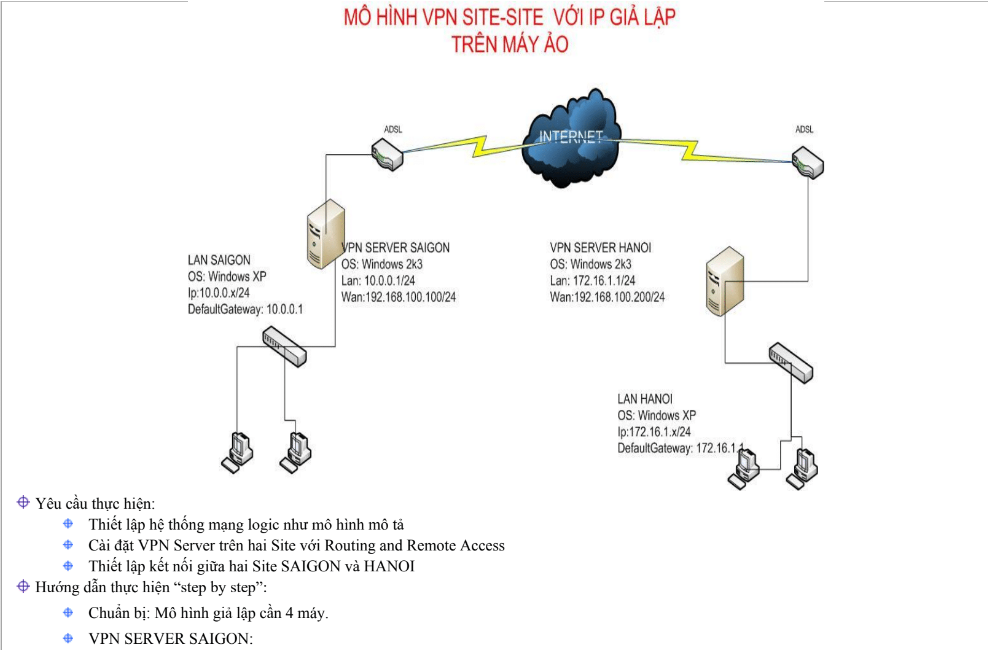
## 2.8 Kiến trúc xử lý tổng quát

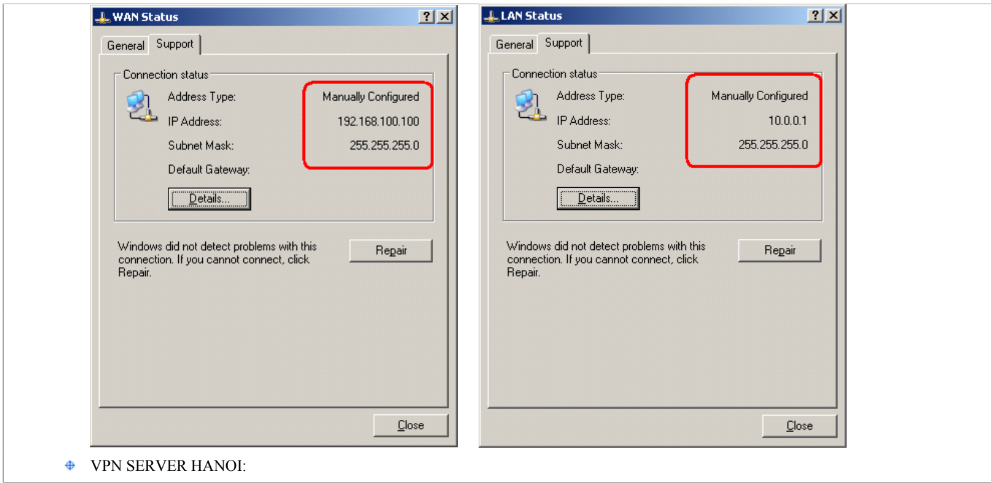


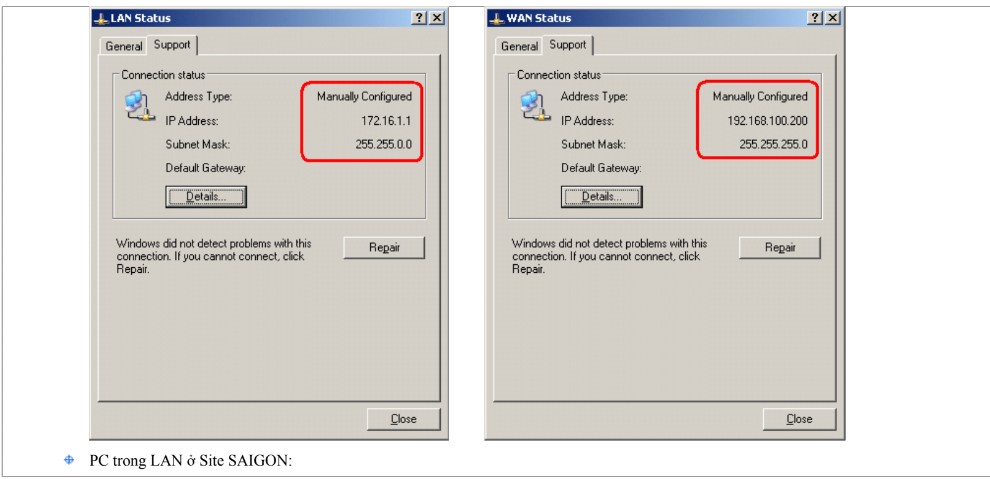
## 2.8.1 Các quá trình xử lý

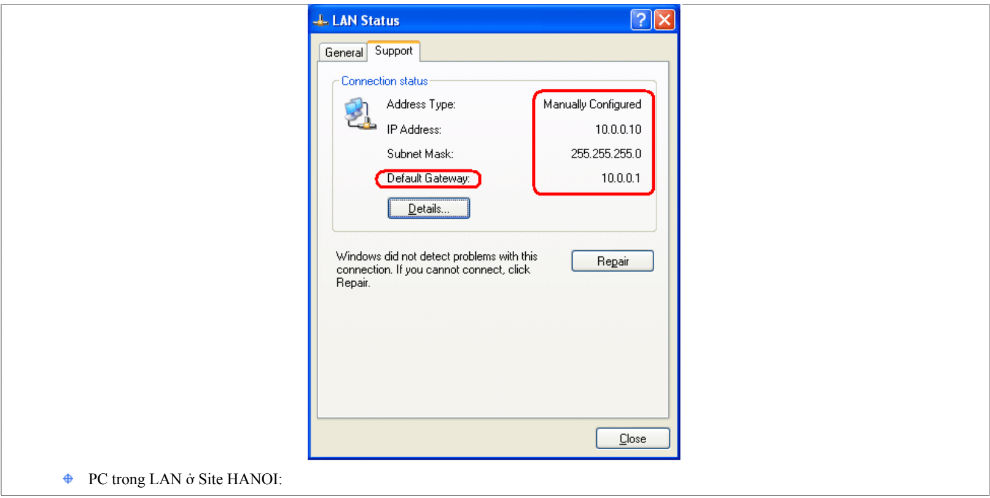
Tình huống demo



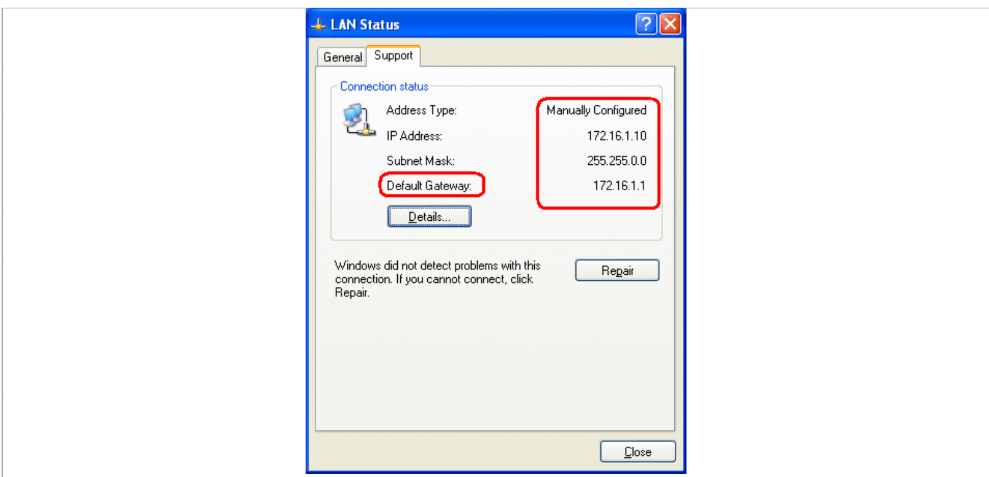


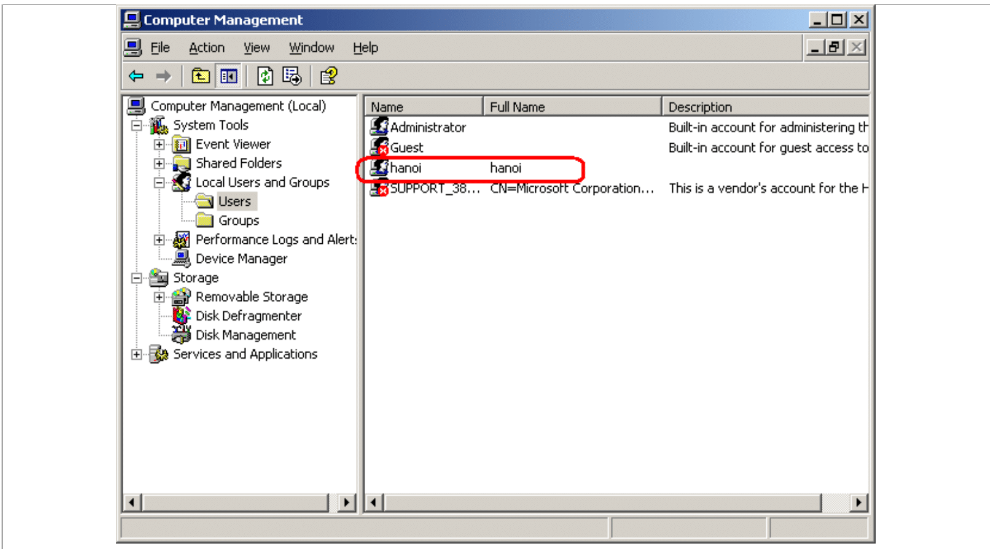


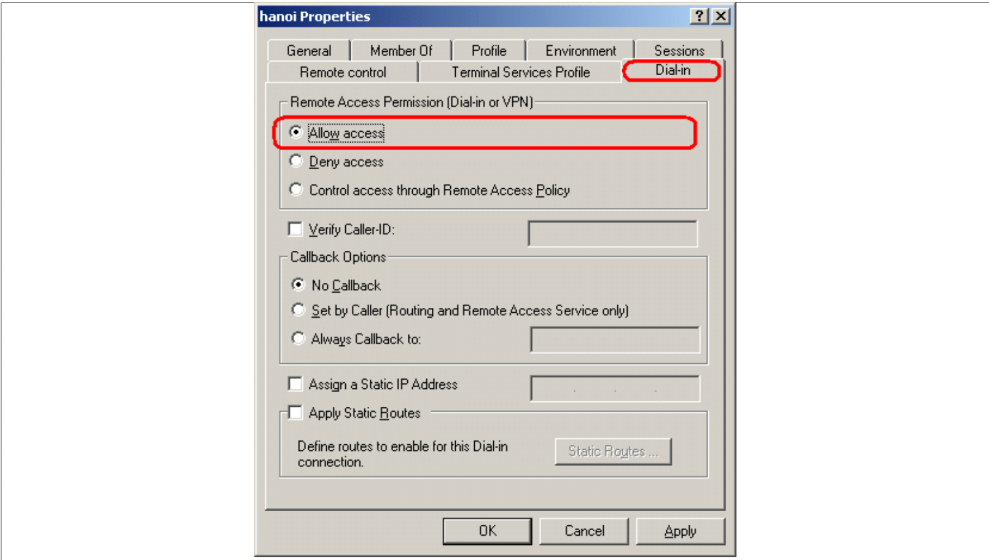


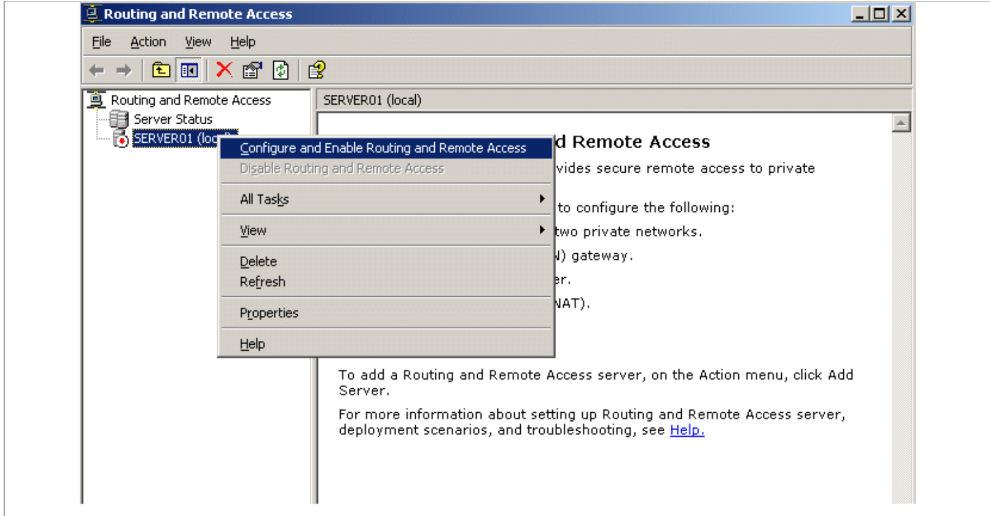


\*

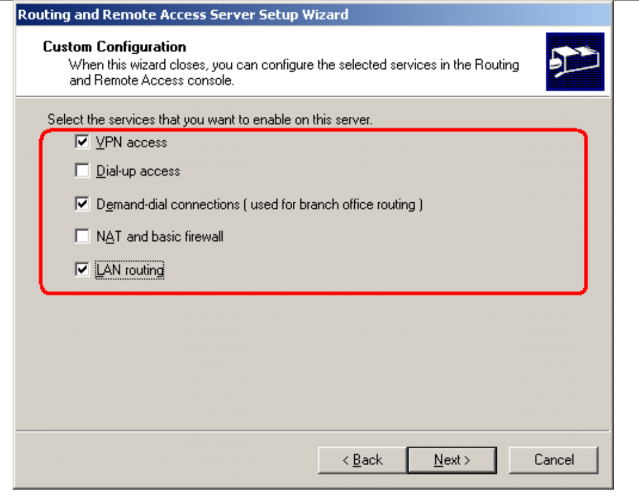
****

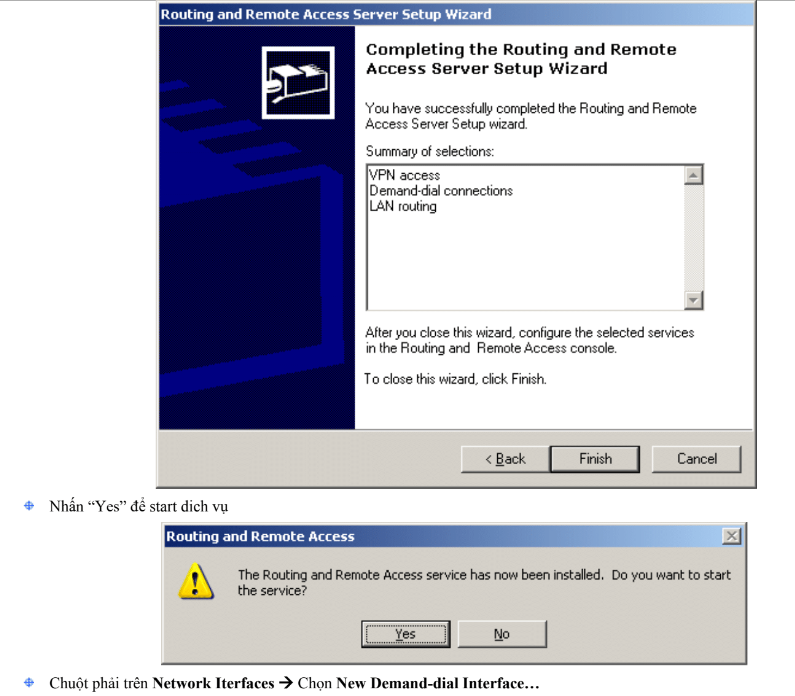
****

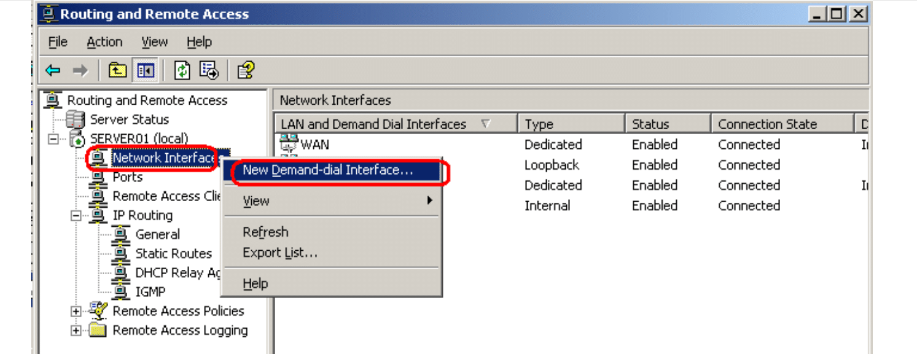
****

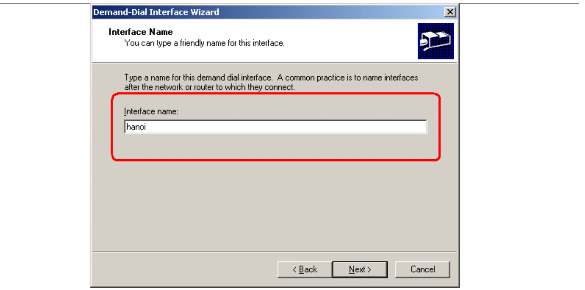
****

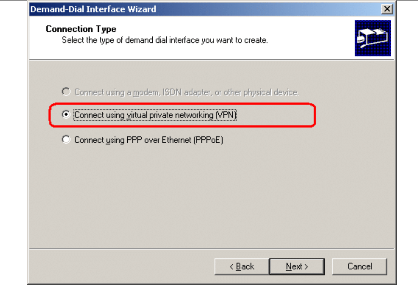
****

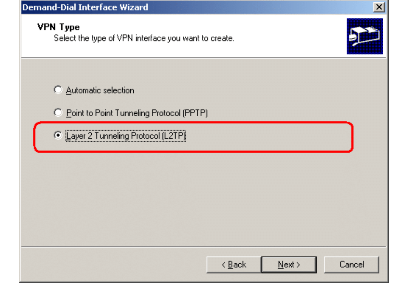
****

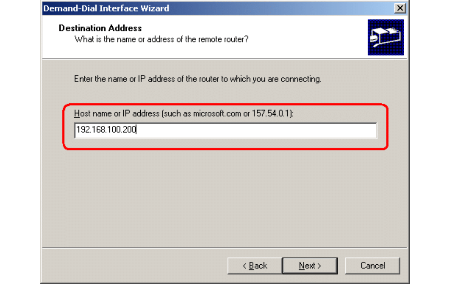
****

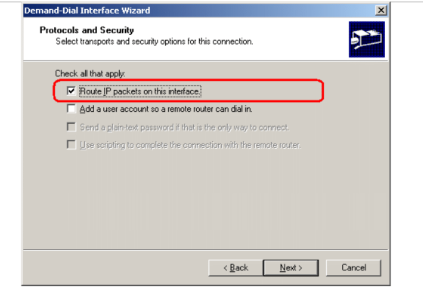
****

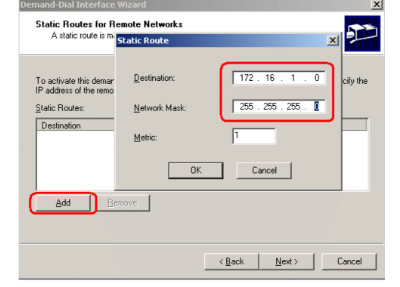
****

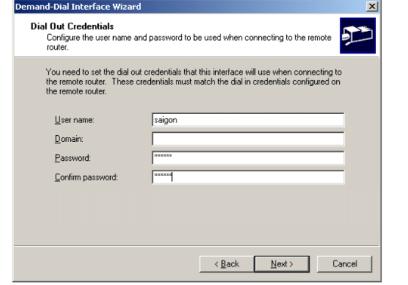
****

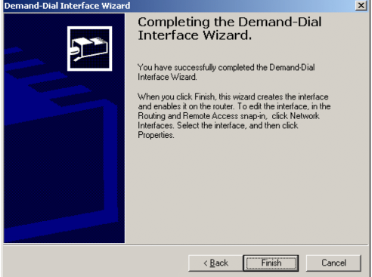
****

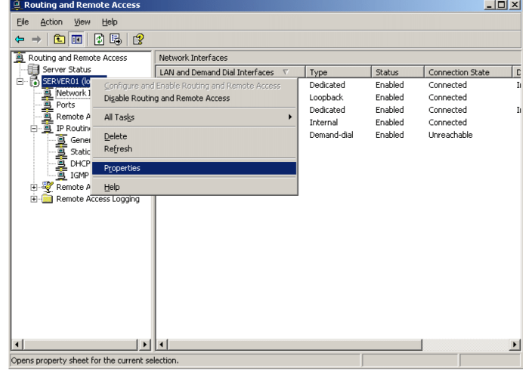
****

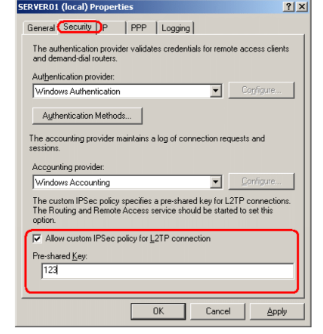
****

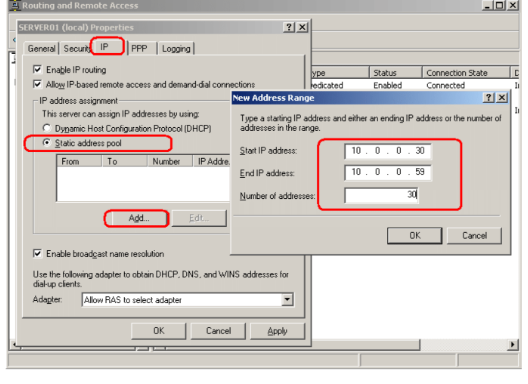
****

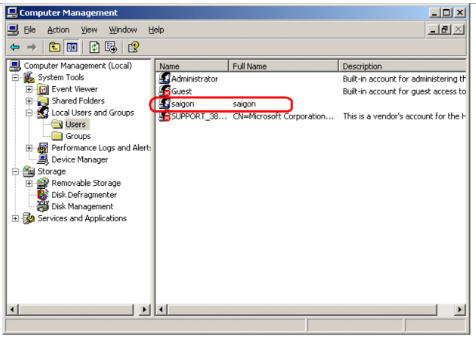
****

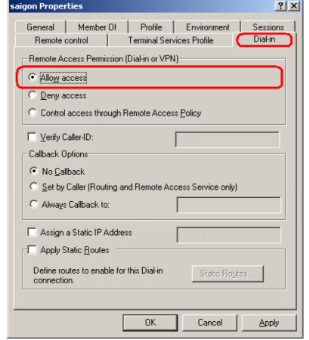
****

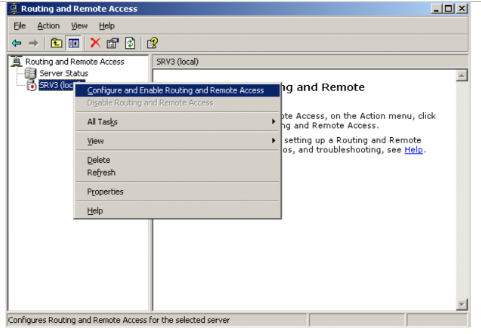
****

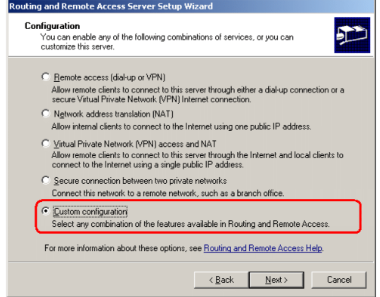
****

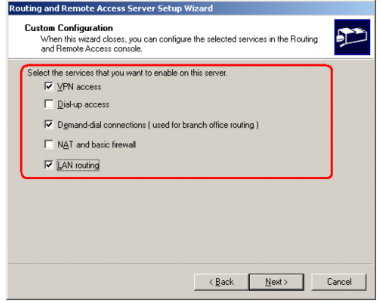


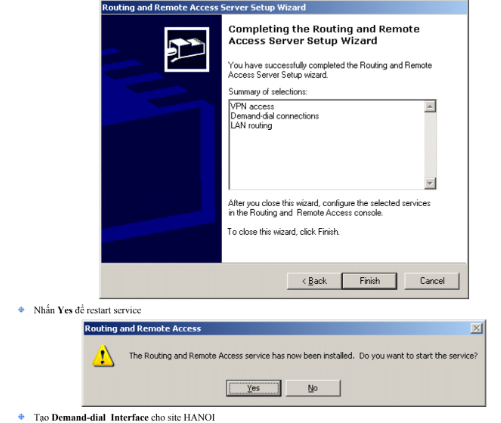


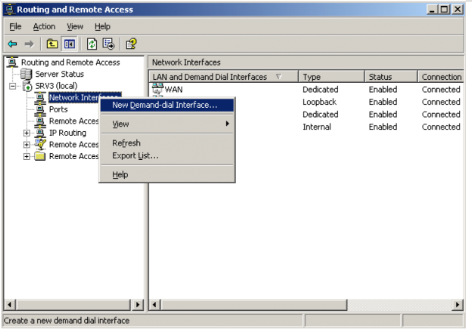


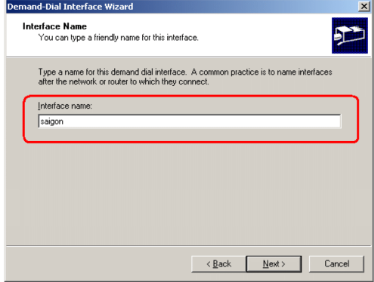


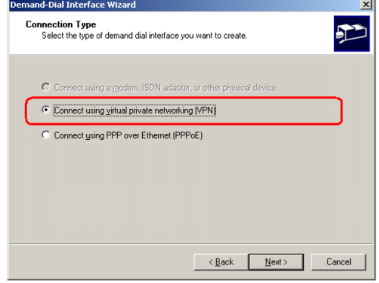


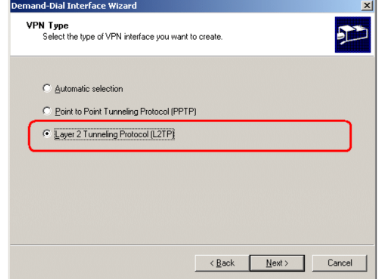


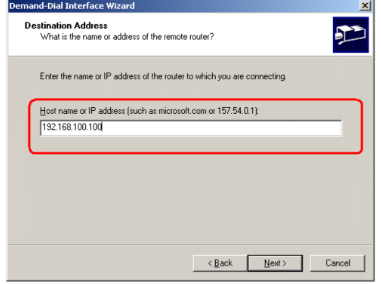


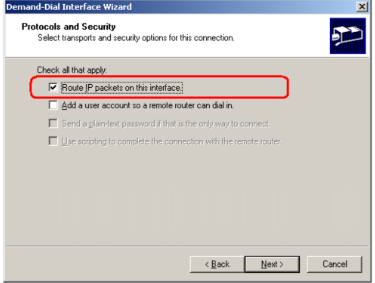


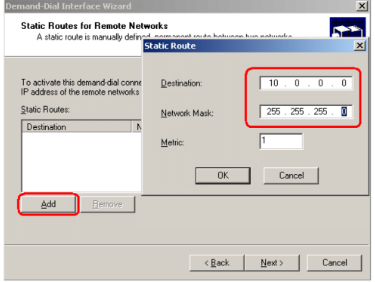


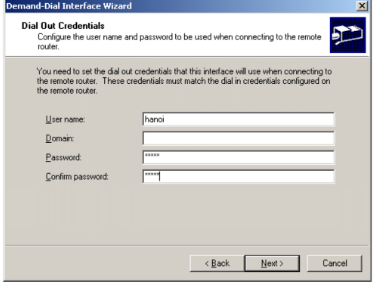


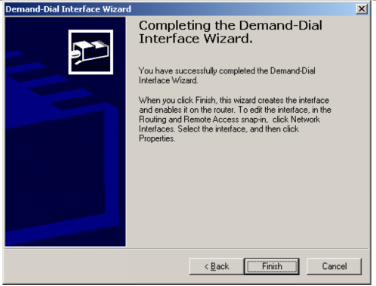


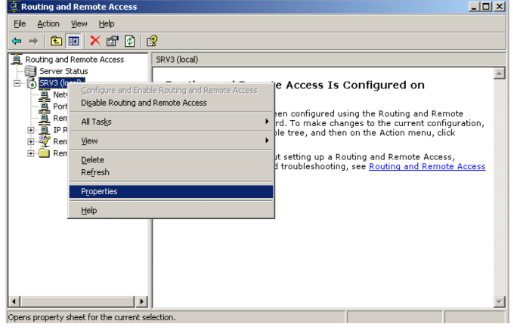


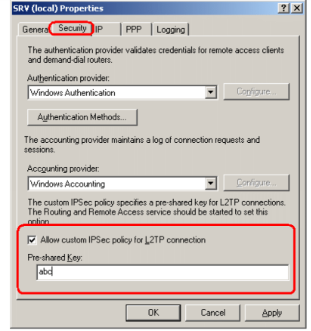


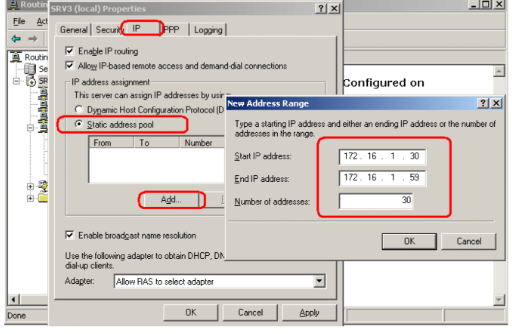


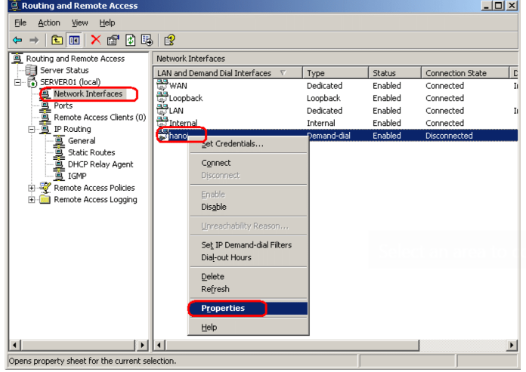


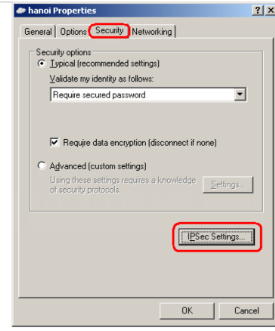


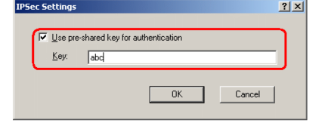


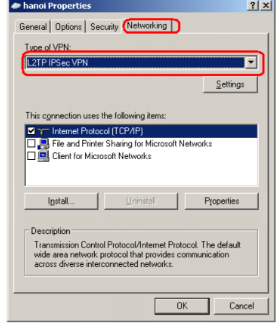


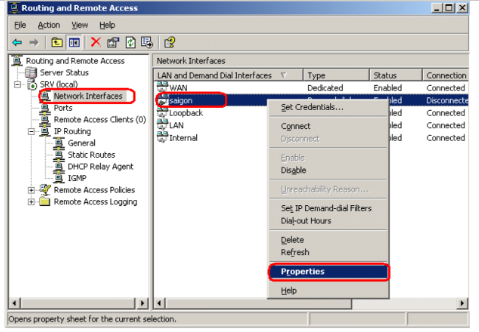


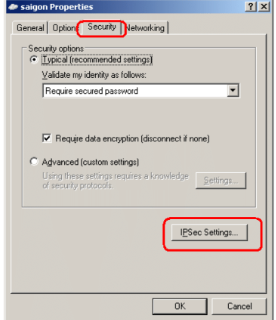


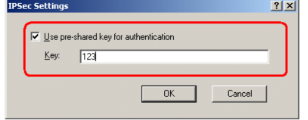


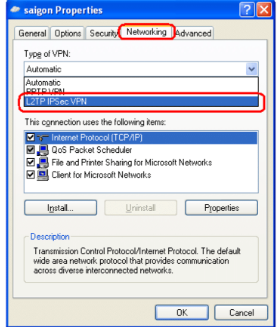


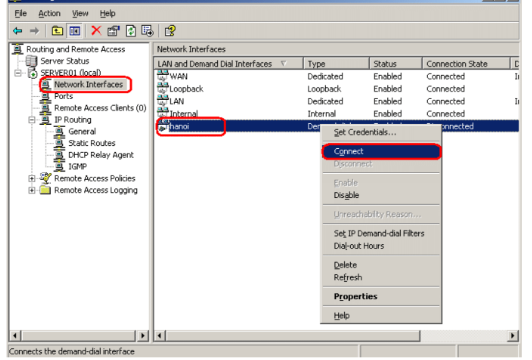


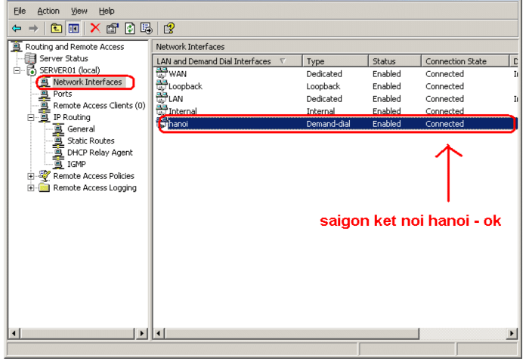


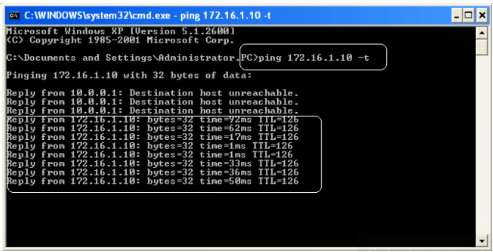


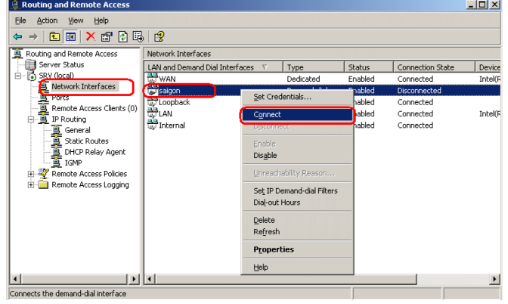


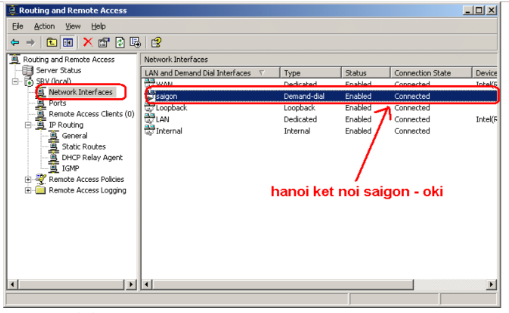




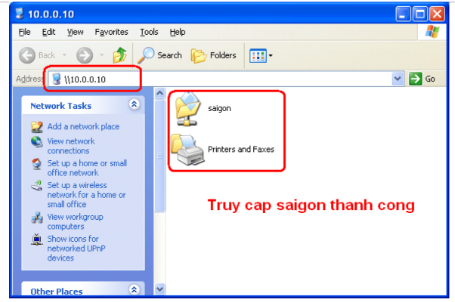












## 2.8.2 Ý nghĩa của từng quá trình

\***B1:** Login administrator trên VPN SERVER SAIGON

Tạo user cho site HANOI kết nối

Nhấp phải chuột trên user HANOI->properties->Tab Dial-in->check Allow access

Mở routing and Remote Access -> chuột phải tên server chọn Configure and Enable Routing and Remote Access chọn properties

Chọn “Custom Configuration”

Check vào 3 mục: VPN access, Demand-dial connections, LAN routing

Chọn Finish để hoàn tất

Nhấn “yes” để start dịch vụ

Chuột phải trên Network Interfaces->Chọn new Demand-dial Interface

Trong mục Interface name, ghi “hanoi”

Chọn” Connect using virtual private networking(VPN)”

Chọn Layer 2 Tunneling Protocol(L2TP)

Nhập IP card WAN của VPN SERVER HANOI

Chọn Route Ippackets on this Interface

Nhấn Add->Nhập lớp mạng nội bộ của HANOI

Nhập user và password mà site HANOI đã tạo cho site SAIGON

Chọn Finish để hoàn tất

Chuột phải VPN Server ở site SAIGON chọn properties

Tab Security -> Check “Allow custom IPSec”

Tab IP-> check vào”Static address pool” -> Nhấn “add”-> Nhập vòng IP ”saigon” sẽ cấp khi “hanoi” connect

**B2:** Login Administrator trên VPN SERVER HANOI

Các bước tương tự như trên VPN SERVER SAIGON, chỉ khác khi nhập IP

Tạo user saigon

Cấp quyền Allow access cho user saigon

Mở routing and Remote access

Chọn Custom Configuration

Chọn VPN access, Demand-dial connection, LAN routing

Chọn Finish để hoàn tất

Nhấn yes để restart service

Tạo Demand dial Interface cho site HANOI

Đặt interface Name là saigon cho phép site SAIGON kết nối đến

Chọn Connecting using virtual private netwworking(VPN)

Chọn giao thức kết nối VPN là Layer 2 Tunneling Protocol(L2TP)

Nhập WAN IP của site Saigon

Để mặc định Route IP packets on this Interface

Add range số IP LAN bên site SAIGON nếu không có sử dụng DHCP

Nhập đúng Username và password mà site SAIGON đã tạo ra cho phép site HANOI kết nối đến

Chọn Finish để hoàn tất

Nhấp phải chuột trên tên VPN Server ở site HANOI chọn properties

Chọn tab security -> Nhập Preshare-Key

Tab IP -> Check vào”Static address pool” -> Nhấn “Add” -> Nhập vòng IP ”hanoi” sẽ cấp khi “saigon” connect

**B3** : Nhập key L2TP cho 2 máy VPN server

VPN server SAIGON

Nhập phải chuột trên biểu tượng “hanoi” Network Interface chọn Properties

Trong tab Security chọn Ipsec settings

Nhập preshare key của site HANOI vì ta đang đứng ở site SAIGON

Trong tab Networking chọn Type of VPN là: L2TP IPSec VPN

VPN Server HANOI

Nhấp phải chuột trên “saigon” Netwoking Interface chọn Properties

Trong tab Security chọn IPSec Settings

Nhập preshare key mã site SAIGON đã tạo vì ta đang dùng ở SITE HANOI kết nối vào site SAIGON

Trong tab Networking chọn L2TP IPSec VPN cho Type of VPN

**B4:** Connect và test

## **CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM**

## 3.1 Mục tiêu của mô hình ứng dụng

Tạo 1 đường hầm truyền dữ liệu từ HANOI đến SAIGON

Sau đó ping từ HANOI đến SAIGON và ngược lại

## 3.2 Mô hình ứng dụng

IPSec trên VMwareworkstation

## 3.3 Yêu cầu thực hiện

## 3.4 Các công cụ cần thiết để thực hiện mô hình

VMwareworkstation

## 3.5 Các bước triển khai

Nằm trên chương 2

## **CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN CỦA ĐỒ ÁN**

## 4.1 Kết luận

Tới đây thì cũng đã hiểu sâu hơn về IPsec, khái niệm của bộ giao thức này, ưu nhược và tầm quan trọng cùng với cách hoạt động của nó. Hy vọng qua bài viết này bạn có thể có thêm nhiều kiến thức bổ ích và biết cách ứng dụng IPSec vào thực tế

## 4.2 Hướng phát triển