TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN

TỐT NGHIỆP ĐẠI HỌC

NGÀNH: KHOA HỌC MÁY TÍNH

MẠNG RIÊNG ẢO

(VIRTUAL PRIVATE NETWORK)

Nhóm sinh viên thực hiện: TRƯƠNG ĐỨC LUÂN

LÊ THỊ THANH HOA

Giảng viên hướng dẫn: **KS. NGUYỄN TRUNG PHÚ**

Cán bộ phản biện:

Lớp: **LT CĐ ĐH KHMT1 K1**

Hà Nội, 04/2009

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

LỜI NÓI ĐẦU

Cùng với sự phát triển của công nghệ thông tin, công nghệ mạng máy tính và đặc biệt là mạng Internet ngày càng phát triển đa dạng và phong phú. Các dịch vụ trên mạng Internet đã xâm nhập vào hầu hết các lĩnh vực trong đời sống xã hội. Các thông tin trao đổi trên Internet cũng đa dạng cả về nội dung và hình thức, trong đó có rất nhiều thông tin cần bảo mật cao bởi tính kinh tế, tính chính xác và tin cậy của nó.

Bên cạnh đó, những dịch vụ mạng ngày càng có giá trị, yêu cầu phải đảm bảo tính ổn định và an toàn cao. Tuy nhiên, các hình thức phá hoại mạng cũng trở nên tinh vi và phức tạp hơn, do đó đối với mỗi hệ thống, nhiệm vụ bảo mật đặt ra cho người quản trị là hết sức quan trọng và cần thiết.

Xuất phát từ những thực tế nêu trên, hiện nay trên thế giới đã xuất hiện rất nhiều công nghệ liên quan đến bảo mật hệ thống và mạng máy tính, việc nắm bắt những công nghệ này là hết sức cần thiết.

Chính vì vậy, thông qua việc nghiên cứu một cách tổng quan về bảo mật hệ thống và một công nghệ cụ thể liên quan đến bảo mật hệ thống, đó là công nghệ Mạng Riêng Ảo (VPN-Virtual Private Network) trong khoá luận này của chúng tôi có thể góp phần vào việc hiểu thêm và nắm bắt rõ về kỹ thuật VPN trong doanh nghiệp cũng như là trong nhà trường để phục vụ cho lĩnh vực học tập và nghiên cứu.

Trong quá trình xây dựng khóa luận này, chúng tôi đã nhận được rất nhiều sự giúp đỡ, góp ý, và ủng hộ của thầy cô giáo, bạn bè đồng nghiệp. Chúng tôi xin chân thành cảm ơn sự hướng dẫn nhiệt tình của thầy Nguyễn Trung Phú, là thầy giáo trực tiếp hướng dẫn khóa luận tốt nghiệp của chúng tôi, cảm ơn các thấy cô giáo trong trong khoa Công Nghệ Thông Tin đã tạo điều kiện giúp đỡ chúng tôi hoàn thành khóa luận tốt nghiệp này.

Bảo mật hệ thống và kỹ thuật VPN là một vấn đề rộng và mới đối với Việt Nam, đồng thời do kinh nghiệm và kỹ thuật còn hạn chế, nội dung tài liệu chắc chắn sẽ còn nhiều sai sót, hy vọng các thầy cùng các bạn sinh viên sẽ đóng góp nhiều ý kiến bổ sung hoàn thiện để tài liệu được chính xác và hữu ích hơn.

TÓM TẮT ĐỒ ÁN

1. Tiếng Việt

Mạng riêng ảo VPN(Virtual Private Network) 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 qua đường Internet từ mạng riêng của công ty tới các site của các nhân viên từ xa.

Một ứng dụng điển hình của VPN là cung cấp một kênh an toàn từ đầu mạng giúp cho những văn phòng chi nhánh / văn phòng ở xa hoặc những người làm việc từ xa có thể dùng Internet truy cập tài nguyên công ty một cách bảo mật và thoải mái như đang sử dụng máy tính cục bộ trong mạng công ty.

Những thiết bị ở đầu mạng hỗ trợ cho mạng riêng ảo là switch, router và firewall. Những thiết bị này có thể được quản trị bởi công ty hoặc các nhà cung cấp dịch vụ như ISP.

Ưu điểm

Bảo mật: VPN mã hóa tất cả dữ liệu trên đường hầm.

Tiết kiệm chi phí: Sự xuất hiện của VPN đã làm cho những cuộc quay số đường dài tốn kém hay đường dây thuê bao không còn cần thiết nữa đối với những tổ chức sử dụng VPN "đóng gói" dữ liệu 1 cách an toàn qua mạng Internet. Những tổ chức có văn phòng chi nhánh hay những người làm việc từ xa có thể truy cập dữ liệu của văn phòng công ty chính từ bất kỳ địa điểm nào trên thế giới mà không phải tốn kém nhiều bằng cách kết nối vào mạng Internet thông qua nhà cung cấp dịch vụ địa phương.

2. English:

VPN (Virtual Private Network) is a private Network using public Network(Internet) in order to connect to other site together (individual Network) or many people remote access.

VPN will replace expert actual connecting such as: Leased Line, each VPN will use virtual connecting over In ternet from company Network to employee site.

One Application of VPN is that provide a safety channel in the beginning of Network to help the child office or remote office or remote people can use Internet access to company properties properly way and comfortable that is the same using computer as inside company.

VPN require some equipments such as: Firewall, Switch, Router. This equipments are controlled by company or ISP.

Advandtage:

Encryptation: VPN encrypt all data on VPN tunnel.

Cost down: VPN appear is mean that replace on Leased Line and Dial up they are expensive when VPN appear many company don’t need Leased Line and Dial up instead of they use packing VPN. Data is safety in the Internet, the company have remote office or remote people can access Company’s data in everywhere which don’t need to use the local sevices.

MỤC LỤC

CÁC CỤM TỪ VIẾT TẮT

ACL: Access Control List

ATM: Asynchronous Transfer Mode (Chế độ truyền không đồng bộ)

AH: Authentication Header

ESP: Encapsulation Security Payload

GRE: Generic Routing Protocol

ISP: Internet Service Provides (Nhà cung cấp dịch vụ Internet)

IP: Internet Protocol (Giao thức Internet)

IPSec: IP Security

IETF: Internet Engineering Task Force

IPX: Internetwork Packet Exchange

ICMP: Internet Control Message protocol

IPMG: Internet Group Management Protocol

ISAKMP: Internet Security Association and Key Management Protocol

IKE: Internet Key Exchange

TCP/IP: Transfer Control Protocol/Internet Protocol

NAS: Network Access Server (Máy chủ truy cập mạng)

LAC: L2TP Access Concentrator

LNS: L2TP Network Server

LAN: Local area network (Mạng cục bộ)

L2TP: Layer 2 Tunneling Protocol

L2F: Layer 2 Forwarding

OC3: optical carrier-3 (Đường truyền cap quang)

OSI: Open Systems Interconnection (Mô hình liên kết các hệ thống mở)

PPP: Point To Point Protocol (Giao thức điểm nối điểm)

PAP: Password Authentication Protocol (Giao thức xác thực mật mã)

POP: Post Office Protocol (Giao thức bưu điện)

PPTP: Point To Point Tunneling Protocol (Dịch vụ quay số ảo)

PVC: Permanent Virtual Circuit (Mạch ảo cố định)

QoS: Quanlity of Service (Chất lượng phục vụ)

SA: Security Association

SPD: Security Policy Database

SPI: Security Parameter Index

SAD: Security Association Database

RAS: Remote Access Server

UDP: User DataGram Protocol

VPN: Virtual Private Network (Mạng riêng ảo)

WAN: Wide Are Network (Mạng Wan)

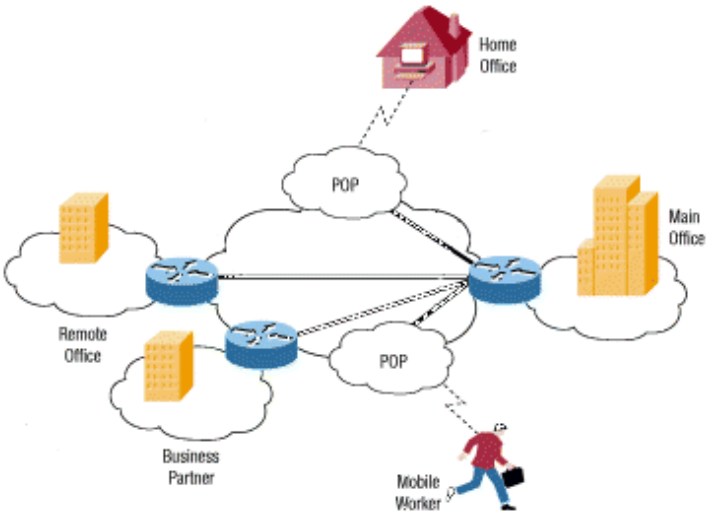
CHƯƠNG I: TỔNG QUAN VỀ VPN

1.1. Định nghĩa, chức năng, và ưu điểm của VPN

1.1.1 Khái niệm cơ bản về VPN

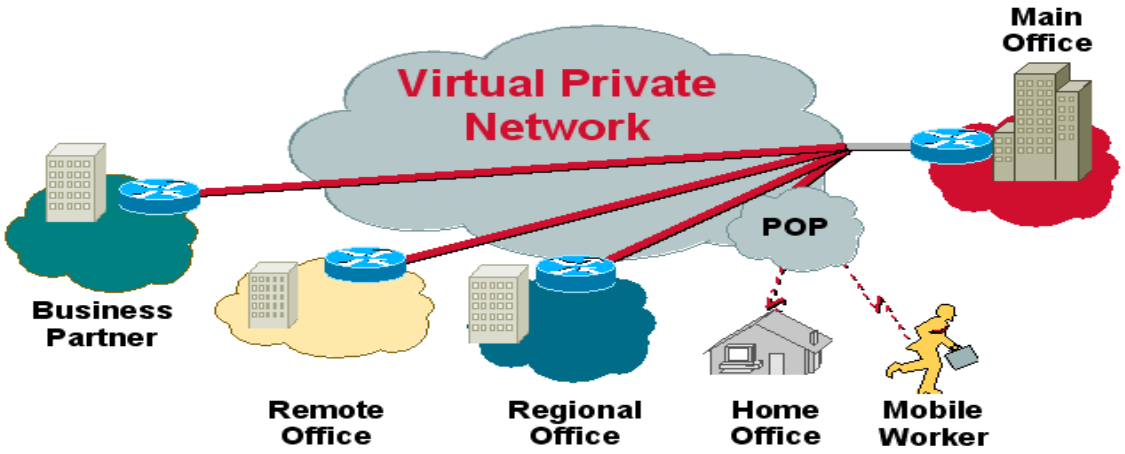
Phương án truyền thông nhanh, an toàn và tin cậy đang trở thành mối quan tâm của nhiều doanh nghiệp, đặc biệt là các doanh nghiệp có các địa điểm phân tán về mặt địa lý. Nếu như trước đây giải pháp thông thường là thuê các đường truyền riêng (leased lines) để duy trì mạng WAN (Wide Are Network). Các đường truyền này giới hạn từ ISDN (128 Kbps) đến đường cáp quang OC3 (optical carrier-3, 155Mbps). Mỗi mạng WAN đều có các điểm thuận lợi trên một mạng công cộng như Internet trong độ tin cậy, hiệu năng và tính an toàn, bảo mật. Nhưng để bảo trì một mạng WAN, đặc biệt khi sử dụng các đường truyền riêng, có thể trở nên quá đắt khi doanh nghiệp muốn mở rộng các chi nhánh.

Khi tính phổ biến của Internet gia tăng, các doanh nghiệp đầu tư vào nó như một phương tiện quảng bá và mở rộng các mạng mà họ sở hữu. Ban đầu, là các mạng nội bộ (Intranet) mà các site được bảo mật bằng mật khẩu được thiết kế cho việc sử dụng chỉ bởi các thành viên trong công ty.



Hình 1.1 Mô hình VPN cơ bản

Về căn bản, mỗi VPN(virtual private network) 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 qua đường Internet từ mạng riêng của công ty tới các site của các nhân viên từ xa.



Hình 1.2 Mô hình mạng VPN

Những thiết bị ở đầu mạng hỗ trợ cho mạng riêng ảo là switch, router và firewall. Những thiết bị này có thể được quản trị bởi công ty hoặc các nhà cung cấp dịch vụ như ISP.

VPN được gọi là mạng ảo vì đây là một cách thiết lập một mạng riêng qua một mạng công cộng sử dụng các kết nối tạm thời. Những kết nối bảo mật được thiết lập giữa 2 host , giữa host và mạng hoặc giữa hai mạng với nhau

Một VPN có thể được xây dựng bằng cách sử dụng "Đường hầm" và "Mã hoá". VPN có thể xuất hiện ở bất cứ lớp nào trong mô hình OSI. VPN là sự cải tiến cơ sở hạ tầng mạng WAN mà làm thay đổi hay làm tăng thêm tính chất của các mạng cục bộ.

1.1.2. Chức năng của VPN

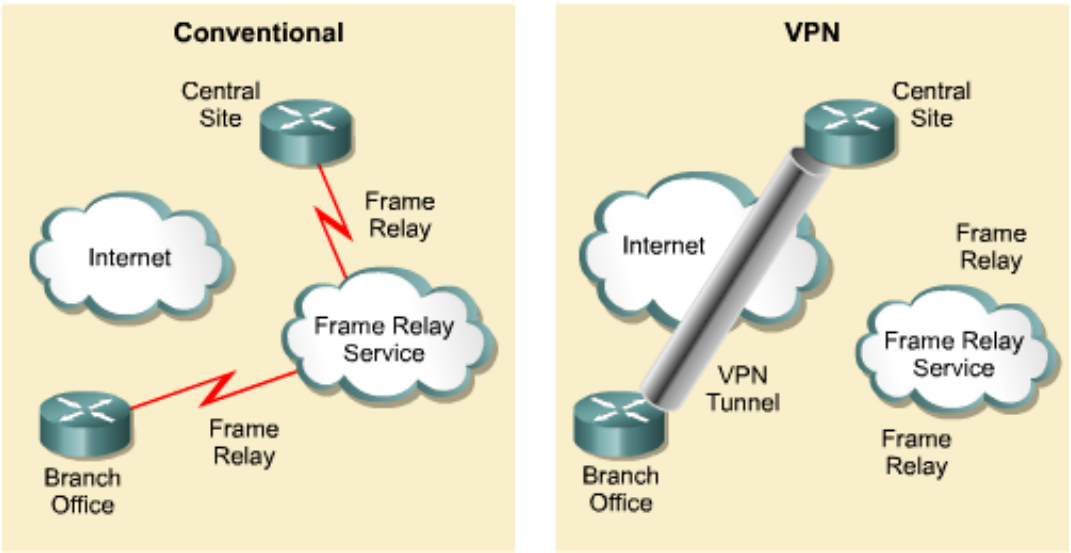
VPN cung cấp ba chức năng chính:

- *Sự tin cậy (Confidentiality):* Người gửi có thể mã hoá các gói dữ liệu trước khi truyền chúng ngang qua mạng. Bằng cách làm như vậy, không một ai có thể truy cập thông tin mà không được cho phép. Và nếu có lấy được thì cũng không đọc được.
- *Tính toàn vẹn dữ liệu (Data Integrity):* người nhận có thể kiểm tra rằng dữ liệu đã được truyền qua mạng Internet mà không có sự thay đổi nào.
- *Xác thực nguồn gốc (Origin Authentication):* Người nhận có thể xác thực nguồn gốc của gói dữ liệu, đảm bảo và công nhận nguồn thông tin.

1.1.3. Ưu điểm

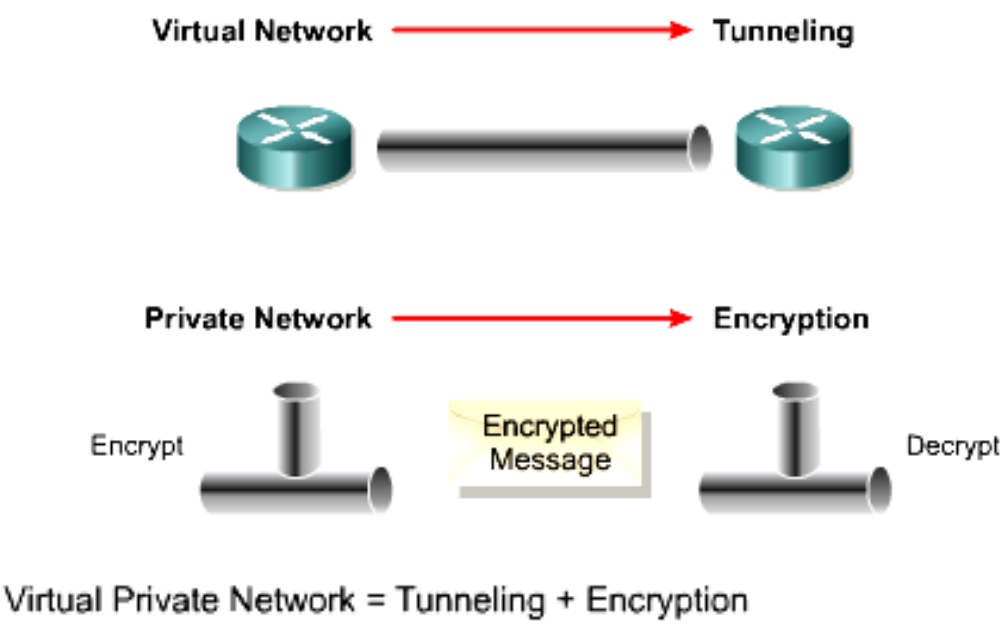
VPN có nhiều ưu điểm hơn so với các mạng leased-line truyền thống. Nó bao gồm:

- *VPN làm giảm chi phí hơn so với mạng cục bộ*. Tổng giá thành của việc sở hữu một mạng VPN sẽ được thu nhỏ, do chỉ phải trả ít hơn cho việc thuê băng thông đường truyền, các thiết bị mạng đường trục, và hoạt động của hệ thống. Giá thành cho việc kết nối LAN-to-LAN giảm từ 20-30% so với việc sử dụng đường Leased-line truyền thống. Còn đối với việc truy cập từ xa thì giảm tới từ 60-80%.
- *VPN tạo ra tính mềm dẻo cho khả năng quản lý Internet*. Các VPN đã kết thừa phát huy hơn nữa tính mềm dẻo và khả năng mở rộng kiến trúc mạng hơn là các mạng WAN truyền thống. Điều này giúp các doanh nghiệp có thể nhanh chóng và hiệu quả kinh tế cho việc mở rộng hay huỷ bỏ kết nối của các trụ sở ở xa, các người sử dụng di động…, và mở rộng các đối tác kinh doanh khi có nhu cầu.
- *VPN làm đơn giản hoá cho việc quản lý các công việc so với việc sở hữu và vận hành một mạng cục bộ*. Các doanh nghiệp có thể cho phép sử dụng một vài hay tất cả các dịch vụ của mạng WAN, giúp các doanh nghiệp có thể tập chung vào các đối tượng kinh doanh chính, thay vì quản lý một mạng WAN hay mạng quay số từ xa.
- *VPN cung cấp các kiểu mạng đường hầm và làm giả thiểu các công việc quản lý.* Một Backbone IP sẽ loại bỏ các PVC (Permanent Virtual Circuit) cố định tương ứng với các giao thức kết nối như là Frame Relay và ATM. Điều này tạo ra một kiểu mạng lưới hoàn chỉnh trong khi giảm được độ phức tạp và giá thành.



Hình 1.3 Ưu điểm của VPN so với mạng truyền thống

Một mạng VPN có được những ưu điểm của mạng cục bộ trên cơ sở hạ tầng của mạng IP công cộng**.** Các ưu điểm này bao gồm tính bảo mật và sử dụng đa giao thức.



Hình 1.4 Các ưu điểm của VPN

Một mạng ảo được tạo ra nhờ các giao thức đường hầm trên một kết nối IP chuẩn. GRE (Generic Routing Protocol), L2TP (Layer 2 Tunneling Protocol) và IPSec là ba phương thức đường hầm.

Một mạng cục bộ là một mạng mà đảm bảo độ tin cậy, tính toàn vẹn và xác thực, gọi tắt là CIA. Mã hoá dữ liệu và sử dụng giao thức IPSec giúp giữ liệu có thể chung chuyển trên Web với các tính chất CIA tương tự như là một mạng cục bộ.

1.1.4. Các yêu cầu cơ bản đối với một giải pháp VPN

Có 4 yêu cầu cần đạt được khi xây dựng mạng riêng ảo.

- ***Tính tương thích (compatibility)***

Mỗi công ty, mỗi doanh nghiệp đều được xây dựng các hệ thống mạng nội bộ và diện rộng của mình dựa trên các thủ tục khác nhau và không tuân theo một chuẩn nhất định của nhà cung cấp dịch vụ. Rất nhiều các hệ thống mạng không sử dụng các chuẩn TCP/IP vì vậykhông thể kết nối trực tiếp với Internet. Để có thể sử dụng được IP VPN tất cả các hệ thống mạng riêng đều phải được chuyển sang một hệ thống địa chỉ theo chuẩn sử dụng trong internet cũng như bổ sung các tính năng về tạo kênh kết nối ảo, cài đặt cổng kết nối internet có chức năng trong việc chuyển đổi các thủ tục khác nhau sang chuẩn IP. 77% số lượng khách hàng được hỏi yêu cầu khi chọn một nhà cung cấp dịch vụ IP VPN phải tương thích với các thiết bị hiện có của họ.

- ***Tính bảo mật (security)***

Tính bảo mật cho khách hàng là một yếu tố quan trọng nhất đối với một giải pháp VPN. Người sử dụng cần được đảm bảo các dữ liệu thông qua mạng VPN đạt

được mức độ an toàn giống như trong một hệ thống mạng dùng riêng do họ tự xây dựng và quản lý.

Việc cung cấp tính năng bảo đảm an toàn cần đảm bảo hai mục tiêu sau:
- Cung cấp tính năng an toàn thích hợp bao gồm: cung cấp mật khẩu cho người sử dụng trong mạng và mã hoá dữ liệu khi truyền.

- Đơn giản trong việc duy trì quản lý, sử dụng. Đòi hỏi thuận tiện và đơn giản cho người sử dụng cũng như nhà quản trị mạng trong việc cài đặt cũng như quản trị hệ thống.

- ***Tính khả dụng (Availability):***

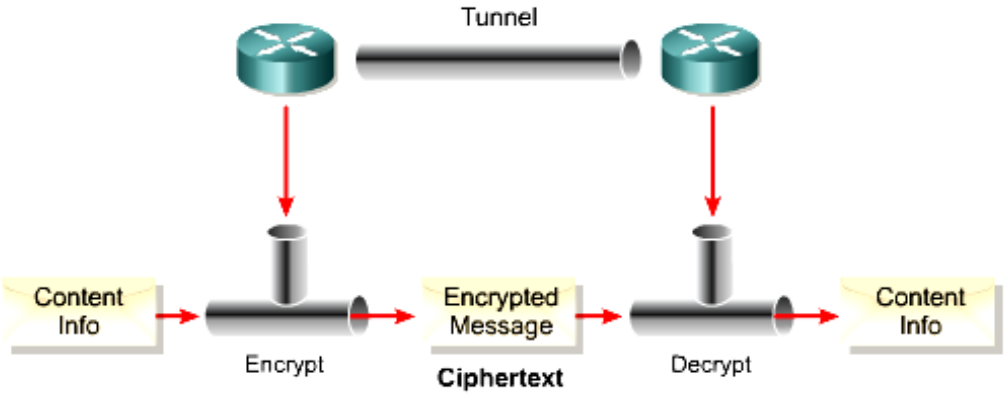
Một giải pháp VPN cần thiết phải cung cấp được tính bảo đảm về chất lượng, hiệu suất sử dụng dịch vụ cũng như dung lượng truyền.

- ***Tiêu chuẩn về chất lượng dịch vụ (QoS):***

Tiêu chuẩn đánh giá của một mạng lưới có khả năng đảm bảo chất lượng dịch vụ cung cấp đầu cuối đến đầu cuối. QoS liên quan đến khả năng đảm bảo độ trễ dịch vụ trong một phạm vi nhất định hoặc liên quan đến cả hai vấn đề trên

1.2. Đường hầm và mã hóa

Chức năng chính của VPN đó là cung cấp sự bảo mật bằng cách mã hoá qua một đường hầm.



Hình 1.5 Đường hầm VPN

❖ *Đường hầm* (*Tunnel*) cung cấp các kết nối logic, điểm tới điểm qua mạng IP không hướng kết nối. Điều này giúp cho việc sử dụng các ưu điểm các tính năng bảo mật. Các giải pháp đường hầm cho VPN là sử dụng sự mã hoá để bảo vệ dữ liệu không bị xem trộm bởi bất cứ những ai không được phép và để thực hiện đóng gói đa giao thức nếu cần thiết. Mã hoá được sử dụng để tạo kết nối đường hầm để dữ liệu chỉ có thể được đọc bởi người nhận và người gửi.

❖ *Mã hoá(Encryption)* chắc chắn rằng bản tin không bị đọc bởi bất kỳ ai nhưng có thể đọc được bởi người nhận. Khi mà càng có nhiều thông tin lưu thông trên mạng thì sự cần thiết đối với việc mã hoá thông tin càng trở nên quan trọng. Mã hoá sẽ biến đổi nội dung thông tin thành trong một văn bản mật mã mà là vô nghĩa trong dạng mật mã của nó. Chức năng giải mã để khôi phục văn bản mật mã thành nội dung thông tin có thể dùng được cho người nhận.

CHƯƠNG II: CÁC KIỂU VPN

VPNs nhằm hướng vào 3 yêu cầu cơ bản sau đây :

- Có thể truy cập bất cứ lúc nào bằng điều khiển từ xa, bằng điện thoại cầm tay, và việc liên lạc giữa các nhân viên của một tổ chức tới các tài nguyên mạng.
- Nối kết thông tin liên lạc giữa các chi nhánh văn phòng từ xa.
- Được điều khiển truy nhập tài nguyên mạng khi cần thiết của khách hàng, nhà cung cấp và những đối tượng quan trọng của công ty nhằm hợp tác kinh doanh.

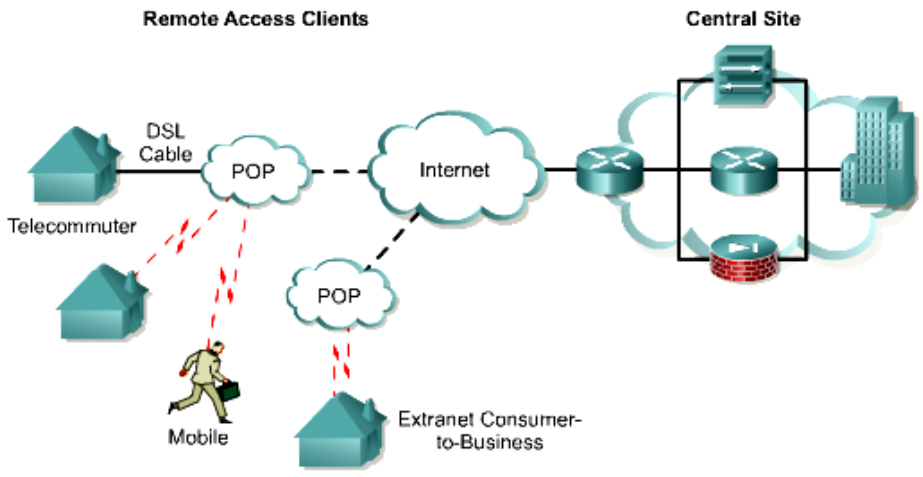
Dựa trên những nhu cầu cơ bản trên, ngày nay VPNs đã phát triển và phân chia ra làm 3 phân loại chính sau :

- Remote Access VPNs.
- Intranet VPNs.
- Extranet VPNs.

2.1 Các VPN truy cập (Remote Access VPNs)

Giống như gợi ý của tên gọi, 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. Đặc biệt là những người dùng thường xuyên di chuyển hoặc các chi nhánh văn phòng nhỏ mà không có kết nối thường xuyên đến mạng Intranet hợp tác.

Các truy cập VPN thường yêu cầu một vài kiểu phần mềm client chạy trên máy tính của người sử dụng. Kiểu VPN này thường được gọi là VPN truy cập từ xa.



Hình 2.1 Mô hình mạng VPN truy cập

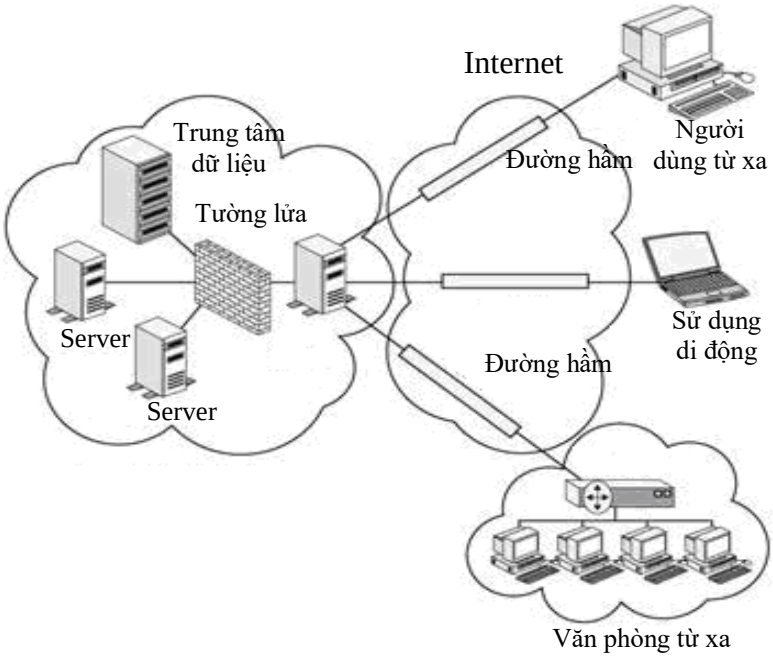
Một số thành phần chính :

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.

Hỗ 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.

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.



Hình 2.2: Cài đặt Remote Access VPN

Thuận lợi chính của Remote Access VPNs :

✓ Sự cần thiết của RAS và việc kết hợp với modem được loại trừ.

✓ Sự cần thiết hỗ 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 đến mạng.

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.

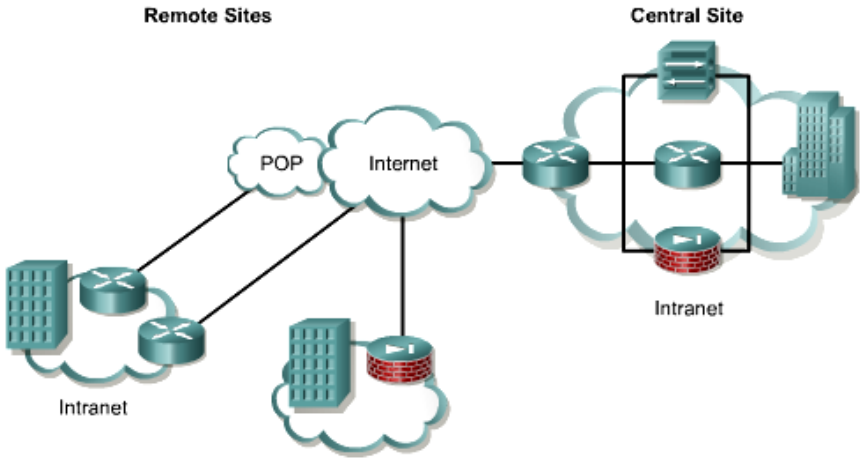
✓Do phải truyền dữ liệu thông qua Internet, nên khi trao đổi các dữ liệu lớn như các gói dữ liệu truyền thông, phim ảnh, âm thanh sẽ rất chậm.

2.2. Các VPN nội bộ (Intranet VPNs):

Intranet VPNs được sử dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Corporate Intranet (backbone router) sử dụng campus router. Theo mô hình này 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 giảm một lượng chi phí đáng kể của việc triển khai mạng Intranet.

Intranet VPNs là một VPN nội bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Điều này cho phép tất cả các địa điểm có thể truy cập các nguồn dữ liệu được phép trong toàn bộ mạng của công ty. Các VPN nội bộ liên kết trụ sở chính, các văn phòng, và các văn phòng chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối mà luôn luôn được mã hoá. Kiểu VPN này thường được cấu hình như là một VPN Site-to-Site.



Hình 2.3 Mô hình mạng VPN nội bộ

Những thuận lợi chính của Intranet setup dựa trên VPN:

✓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.

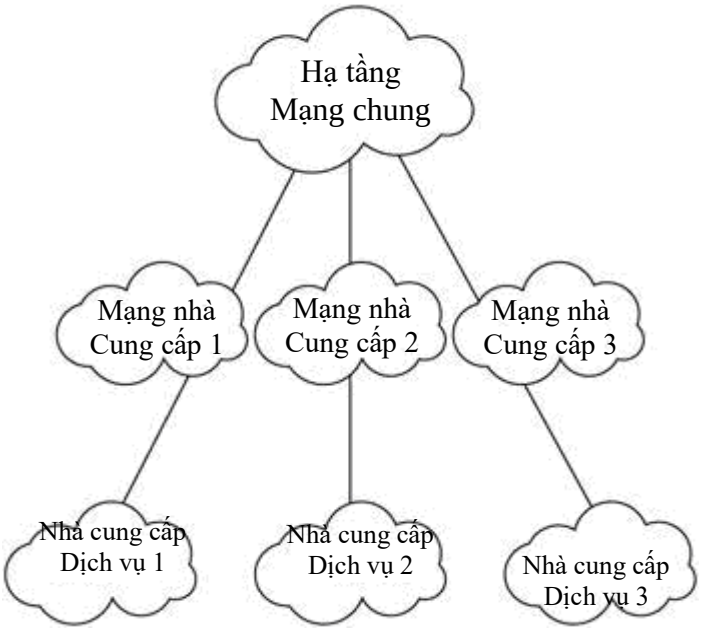
✓Trong một số trường hợp, nhất là khi dữ liệu là loại high-end, như các tập tin mulltimedia, việc trao đổi dữ liệu sẽ rất chậm chạp do được truyền thông qua Internet.

✓Do là kết nối dựa trên Internet, nên tính hiệu quả không liên tục, thường xuyên, và QoS cũng không được đảm bảo.

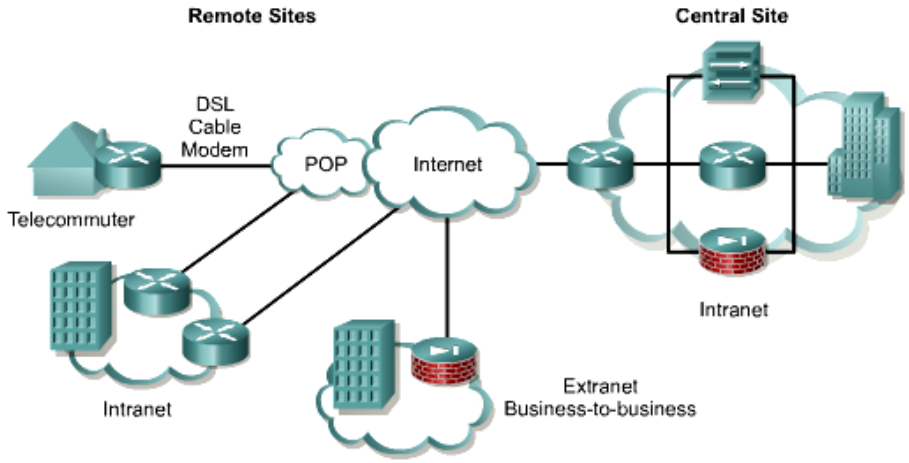
2.3. Các VPN mở rộng (Extranet VPNs):

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.

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 khó 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.



Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp, và các đối tác qua một cơ sở hạ tầng công cộng sử dụng các kết nối mà luôn luôn được bảo mật. Kiểu VPN này thường được cấu hình như là một VPN Site-to-Site. Sự khác nhau giữa một VPN nội bộ và một VPN mở rộng đó là sự truy cập mạng mà được công nhận ở một trong hai đầu cuối của VPN. Hình dưới đây minh hoạ một VPN mở rộng.



Hình 2.5 Mô hình mạng VPN mở rộng

Một số thuận lợi của Extranet :

✓ Do hoạt động trên môi trường Internet, chúng ta 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.

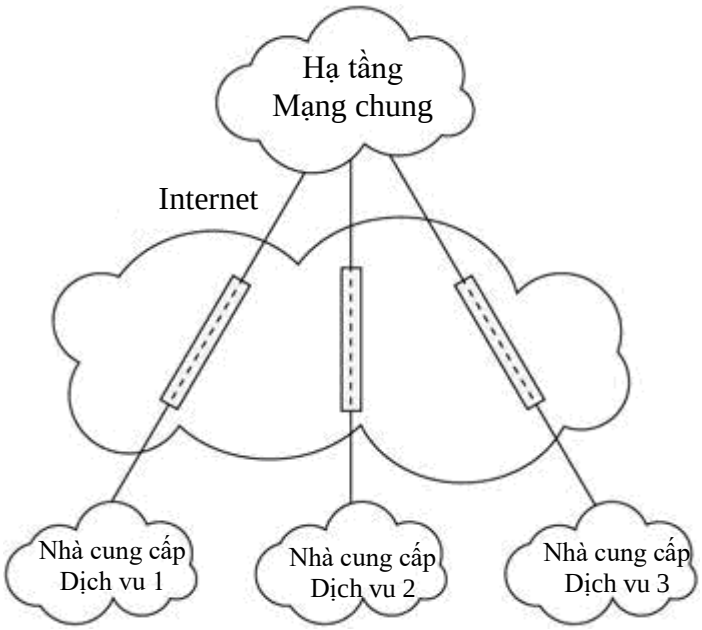
Một số bất lợi của Extranet :

✓ Sự đe dọa về tính an toàn, như bị tấn công bằng từ chối dịch vụ vẫn còn tồn tại.

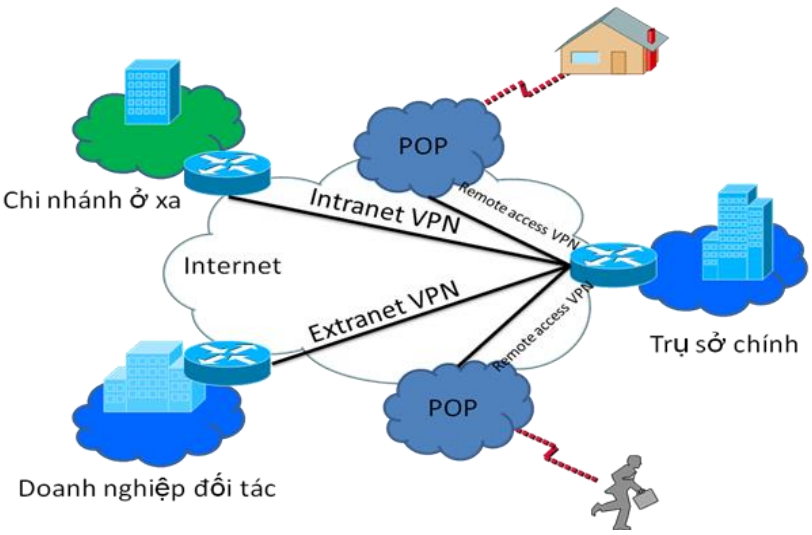
✓ Tăng thêm nguy hiểm sự xâm nhập đối với tổ chức trên Extranet.

✓ 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 cũng không được bảo đảm thường xuyên.



Hình 2.6: Thiết lập Extranet VPN



Hình 2.7 Ba loại mạng riêng ảo

CHƯƠNG III: GIAO THỨC ĐƯỜNG HẦM VPN

Giao thức đường hầm là một nền tảng trong VPN. Giao thức đường hầm đóng vai trò quan trọng trong việc thực hiện đóng gói và vận chuyển gói tin để truyền trên đường mạng công cộng. Có ba giao thức đường hầm cơ bản và được sử dụng nhiều trong thực tế và đang được sử dụng hiện nay là giao thức tầng hầm chuyển tiếp lớp 2 L2F, Giao thức đường hầm điểm tới điểm (PPTP), giao thức tầng hầm lớp 2 Layer. Trong chương này sẽ đi sâu hơn và cụ thể hơn các giao thức đường hầm nói trên. Nó liên quan đến việc thực hiện IP-VPN trên mạng công cộng.

Nội dung chương này bao gồm:

- Giới thiệu các giao thức đường hầm
- Giao thức đường hầm điểm tới điểm
- Giao thức chuyển tiếp lớp 2
- Giao thức đường hầm lớp 2
- GRE
- IPSEC

3.1 Giới thiệu các giao thức đường hầm

Có rất nhiều giao thức đường hầm khác nhau trong công nghệ VPN, và việc sử dụng các giao thức nào lên quan đến các phương pháp xác thực và mật mã đi kèm. Một số giao thức đường hầm phổ biến hiện nay là:

- Giao thức tầng hầm chuyển tiếp lớp 2 (L2F).
- Giao thức đường hầm điểm tới điểm (PPTP).
- Giao thức tầng hầm lớp 2 (L2TP).
- GRE
- IPSEC

Hai giao thức L2F và PPTP đều được kế thừa và phát triển dựa trên giao thức PPP (Point to Point Protocol). Có thể nói PPP là một giao thức cơ bản và được sử dụng nối tiếp lớp 2, Có thể sử dụng để chuyển gói tin dữ liệu qua các mạng IP và hỗ trợ đa giao thức lớp trên. Giao thức L2F được hãng Cisco nghiên cứu và phát triển độc quyền, còn PPTP được nhiều công ty cùng nhau hợp tác nghiên cứu và phát triển. Dựa vào hai giao thức trên được tổ chức kĩ thuật Internet (IETF) đã phát triển giao thức đường hầm L2TP. Và hiện nay các giao thức PPTP và L2TP được sử dụng phổ biến hơn L2F. Trong các giao thức đường hầm nói trên, giao thức IPSec là một trong nhưng giải pháp tối ưu về mặt an toàn dữ liệu của gói tin. Nó được sử dụng các phương pháp xác thực và mật mã tương đối cao. IPSec được mang tính linh động hơn, không bị ràng buộc bởi các thuật toán xác thực hay mật mã nào cả.

3.2 Giao thức đường hầm điểm tới điểm (PPTP).

Giao thức này được nghiên cứu và phát triển bởi công ty chuyên về thiết bị công nghệ viễn thông. Trên cơ sở của giao thức này là tách các chức năng chung và riêng của việc truy nhập từ xa, dự trên cơ sở hạ tầng Internet có sẵn để tạo kết nối đường hầm giữa người dùng và mạng riêng ảo. Người dùng ở xa có thể dùng phương pháp quay số tới các nhà cung cấp dịch vụ Internet để có thể tạo đường hầm riêng để kết nối tới truy nhập tới mạng riêng ảo của người dùng đó. Giao thức PPTP được xây dựng dựa trên nền tảng của PPP, nó có thể cung cấp khả năng truy nhập tạo đường hầm thông qua Internet đến các site đích. PPTP sử dụng giao thức đóng gói tin định tuyến chung GRE được mô tả để đóng lại và tách gói PPP. Giao thức này cho phép PPTP linh hoạt trong xử lý các giao thức khác.

3.2.1 Nguyên tắc hoạt động của PPTP

PPP là giao thức truy nhập vào Internet và các mạng IP phổ biến hiện nay. Nó làm việc ở lớp liên kết dữ liệu trong mô hình OSI, PPP bao gồm các phương thức đóng gói, tách gói IP, là truyền đi trên chỗ kết nối điểm tới điểm từ máy này sang máy khác.

PPTP đóng các gói tin và khung dữ liệu của giao thức PPP vào các gói tin IP để truyền qua mạng IP. PPTP dùng kết nối TCP để khởi tạo và duy trì, kết thức đường hầm và dùng một gói định tuyến chung GRE để đóng gói các khung PPP. Phần tải của khung PPP có thể được mã hoá và nén lại.

PPTP sử dụng PPP để thực hiện các chức năng thiết lập và kết thức kết nối vật lý, xác định người dùng, và tạo các gói dữ liệu PPP.

PPTP có thể tồn tại một mạng IP giữa PPTP khách và PPTP chủ của mạng. PPTP khách có thể được đấu nối trực tiếp tới máy chủ thông qua truy nhập mạng NAS để thiết lập kết nối IP. Khi kết nối được thực hiện có nghĩa là người dùng đã được xác nhận. Đó là giai đoạn tuy chọn trong PPP, tuy nhiên nó luôn luôn được cung cấp bởi ISP. Việc xác thực trong quá trình thiết lập kết nối dựa trên PPTP sử dụng các cơ chế xác thực của kết nối PPP. Một số cơ chế xác thực được sử dụng là:

- Giao thức xác thực mở rộng EAP.
- Giao thức xác thực có thử thách bắt tay CHAP.
- Giao thức xác định mật khẩu PAP.

Giao thức PAP hoạt động trên nguyên tắc mật khẩu được gửi qua kết nối dưới dạng văn bản đơn giản và không có bảo mật. CHAP là giao thức các thức mạnh hơn, sử dụng phương pháp bắt tay ba chiều để hoạt động, và chống lại các tấn công quay lại bằng cách sử dụng các giá trị bí mật duy nhất và không thể đoán và giải được. PPTP cũng được các nhà phát triển công nghệ đua vào việc mật mã và nén phần tải tin của PPP. Để mật mã phần tải tin PPP có thể sử dụng phương thức mã hoá điểm tới điểm MPPE. MPPE chỉ cung cấp mật mã trong lúc truyền dữ liệu trên đường truyền không cung cấp mật mã tại các thiết bị đầu cuối tới đầu cuối. Nếu cần

sử dụng mật mã đầu cuối đến đầu cuối thì có thể dùng giao thức IPSec để bảo mật lưu lượng IP giữa các đầu cuối sau khi đường hầm PPTP được thiết lập.

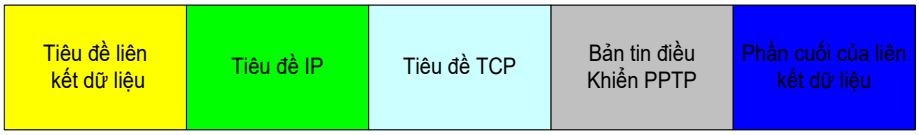
Khi PPP được thiết lập kết nối, PPTP sử dụng quy luật đóng gói của PPP để đóng gói các gói truyền trong đường hầm. Để có thể dự trên những ưu điểm của kết nối tạo bởi PPP, PPTP định nghĩa hai loại gói là điều khiển và dữ liệu, sau đó gán chúng vào hai kênh riêng là kênh điều khiển và kênh dữ liệu. PPTP tách các kênh điều khiển và kênh dữ liệu thành những luồng điều khiển với giao thức điều khiển truyền dữ liệu TCP và luồng dữ liệu với giao thức IP. Kết nối TCP tạo ra giữa các máy khách và máy chủ được sử dụng để truyền thông báo điều khiển.

Các gói dữ liệu là dữ liệu thông thường của người dùng. Các gói điều khiển được đua vào theo một chu kì để lấy thông tin và trạng thái kết nối và quản lý báo hiệu giữa ứng máy khách PPTP và máy chủ PPTP. Các gói điều khiển cũng được dùng để gửi các thông tin quản lý thiết bị, thông tin cấu hình giữa hai đầu đường hầm.

Kênh điều khiển được yêu cầu cho việc thiết lập một đường hầm giữa các máy khách và máy chủ PPTP. Máy chủ PPTP là một Server có sử dụng giao thức PPTP với một giao diện được nối với Internet và một giao diện khác nối với Intranet, còn phần mềm client có thể nằm ở máy người dùng từ xa hoặc tại các máy chủ ISP.

3.2.2 Nguyên tắc kết nối điều khiển đường hầm theo giao thức PPTP

Kết nối điều khiển PPTP là kết nối giữa địa chỉ IP của máy khách PPTP và địa chỉ máy chủ. Kết nối điều khiển PPTP mang theo các gói tin điều khiển và quản lý được sử dụng để duy trì đường hầm PPTP. Các bản tin này bao gồm PPTP yêu cầu phản hồi và PPTP đáp lại phải hồi định kì để phát hiện các lỗi kết nối giữa các máy trạm và máy chủ PPTP. Các gói tin của kết nối điều khiển PPTP bao gồm tiêu đề IP, tiêu đề TCP và bản tin điều khiển PPTP và tiêu đề, phần cuối của lớp liên kết dữ liệu.



Hình 3.1: Gói dữ liệu kết nối điều khiển PPTP

3.2.3 Nguyên lý đóng gói dữ liệu đường hầm PPTP

Đóng gói khung PPP và gói định tuyến chung GRE

Dữ liệu đường hầm PPTP được đóng gói thông qua các mức được mô tả theo mô hình.

Hình 3.2: Mô hình đóng gói dữ liệu đường hầm PPTP

Phần tải của khung PPP ban đầu được mã hoá và đóng gói với tiêu đề PPP để tạo ra khung PPP. Khung PPP sau đó được đóng gói với phần tiêu đề của phiên bản giao thức GRE sửa đổi.

GRE là giao thức đóng gói chung, cung cấp cơ chế đóng gói dữ liệu để định tuyến qua mạng IP. Đối với PPTP, phần tiêu đề của GRE được sửa đổi một số điểm đó là. Một trường xác nhận dài 32 bits được thêm vào. Một bits xác nhận được sử dụng để chỉ định sự có mặt của trường xác nhận 32 bits. trường Key được thay thế bằng trường độ dài Payload 16 bits và trường chỉ số cuộc gọi 16 bits. Trường chỉ số cuộc gọi được thiết lập bởi máy trạm PPTP trong quá trình khởi tạo đường hầm.

Đóng gói IP

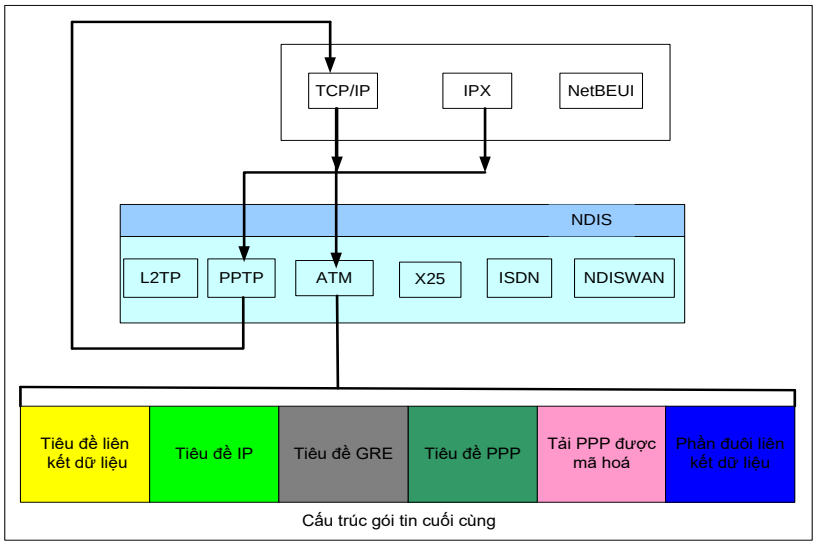
Trong khi truyền tải phần tải PPP và các tiêu đề GRE sau đó được đóng gói với một tiêu đề IP chứa các thông tin địa chỉ nguồn và đích thích hợp cho máy trạm và máy chủ PPTP.

Đóng gói lớp liên kết dữ liệu

Để có thể truyền qua mạng LAN hay WAN thì gói tin IP cuối cùng sẽ được đóng gói với một tiêu đề và phần cuối của lớp liên kết dữ liệu ở giao diện vật lý đầu ra. Như trong mạng LAN thì nếu gói tin IP được gửi qua giao diện Ethernet, nó sẽ được gói với phần tiêu đề và đuôi Ethernet. Nếu gói tin IP được gửi qua đường truyền WAN điểm tới điểm nó sẽ được đóng gói với phần tiêu đề và đuôi của giao thức PPP.

Sơ đồ đóng gói trong giao thức PPTP

Quá trình đóng gói PPTP từ một máy trạm qua kết nối truy nhập VPN từ xa sử dụng modem được mô phỏng theo hình dưới đây.



Hình 3.9: Sơ đồ đóng gói PPTP

- Các gói tin IP, IPX, hoặc khung NetBEUI được đưa tới giao diện ảo đại diện cho kết nối VPN bằng các giao thức tương ứng sử dụng đặc tả giao diện thiết bị mạng NDIS.
- NDIS đưa gói tin dữ liệu tới NDISWAN, nơi thực hiện việc mã hoá và nén dữ liệu, cũng như cung cấp tiêu đề PPP phần tiêu đề PPP này chỉ gồm trường mã số giao thức PPP không có trường Flags và trường chuỗi kiểm tra khung (FCS). Giả định trường địa chỉ và điều khiển được thoả thuận ở giao thức điều khiển đường truyền (LCP) trong quá trình kết nối PPP.
- NDISWAN gửi dữ liệu tới giao thức PPTP, nơi đóng gói khung PPP với phần tiêu đề GRE. Trong tiêu đề GRE, trường chỉ số cuộc gọi được đặt giá trị thích hợp xác định đường hầm.
- Giao thức PPTP sau đó sẽ gửi gói tin vừa tạo ra tới TCP/IP.
- TCP/IP đóng gói dữ liệu đường hầm PPTP với phần tiêu đề IP sau đó gửi kết quả tới giao diện đại diện cho kết nối quay số tới ISP cục bộ NDIS.
- NDIS gửi gói tin tới NDISWAN, cung cấp các tiêu đề và đuôi PPP.
- NDISWAN gửi khung PPP kết quả tới cổng WAN tương ứng đại diện cho phần cứng quay số.

3.2.4 Nguyên tắc thực hiện gói tin dữ liệu tại đầu cuối đường hầm PPTP

Khi nhận được được dữ liệu đường hầm PPTP, máy trạm và máy chủ PPTP, sẽ thực hiện các bước sau.

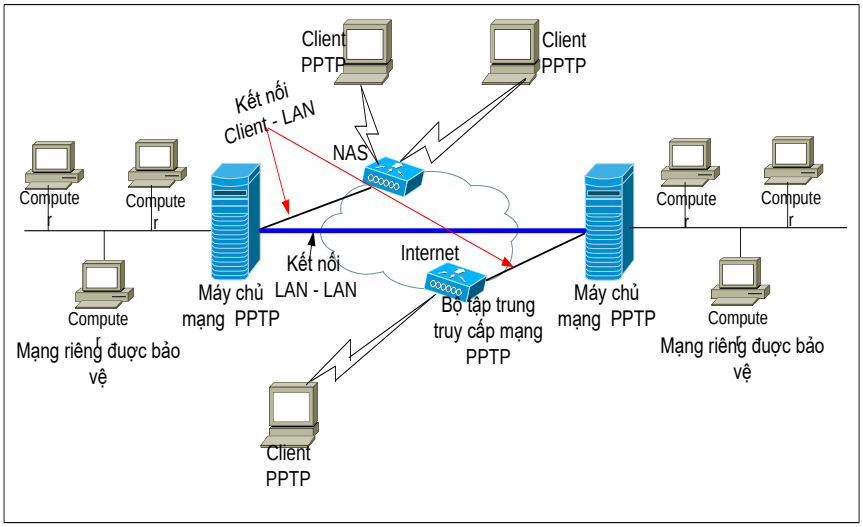
- Xử lý và loại bỏ gói phần tiêu đề và đuôi của lớp liên kết dữ liệu hay gói tin.
- Xử lý và loại bỏ tiêu đề IP.
- Xử lý và loại bỏ tiêu đề GRE và PPP.
- Giải mã hoặc nén phần tải tin PPP.

- Xử lý phần tải tin để nhận hoặc chuyển tiếp.

3.2.5 Triển khai VPN dự trên PPTP

Khi triển khai VPN dự trên giao thức PPTP yêu cầu hệ thống tối thiểu phải có các thành phần thiết bị như chỉ ra ở hình trên nó bao gồm.

- Một máy chủ truy nhập mạng dùng cho phương thức quay số truy nhập bảo mật VPN.
- Một máy chủ PPTP.
- Máy trạm PPTP với phần mềm client cần thiết.



Hình 3.3: Các thành phần hệ thống cung cấp VPN dựa trên PPTP

Máy chủ PPTP

Máy chủ PPTP có hai chức năng chính, đóng vai trò là điểm kết nối của đường hầm PPTP và chuyển các gói tin đến từng đường hầm mạng LAN riêng. Máy chủ PPTP chuyển các gói tin đến máy đích bằng cách xử lý gói tin PPTP để có thể được địa chỉ mạng của máy đích. Máy chủ PPTP cũng có khả năng lọc gói, bằng cách sử dụng cơ chế lọc gói PPTP máy chủ có thể ngăn cấm, chỉ có thể cho phép truy nhập vào Internet, mạng riêng hay truy nhập cả hai.

Thiết lập máy chủ PPTP tại site mạng có thể hạn chế nếu như máy chủ PPTP nằm sau tường lửa. PPTP được thiết kế sao cho chỉ có một cổng TCP 1723 được sử dụng để chuyển dữ liệu đi. Nhược điểm của cấu hình cổng này có thể làm cho bức tường lửa dễ bị tấn công. Nếu như bức tường được cấu hình để lọc gói tin thì cần phải thiết lập nó cho phép GRE đi qua.

Một thiết bị khác được đua ra năm 1998 do hãng 3Com có chức năng tương tự như máy chủ PPTP gọi là chuyển mạch đường hầm. Mục đích của chuyển mạch đường hầm là mở rộng đường hầm từ một mạng đến một mạng khác, trải rộng đường hầm từ mạng của ISP đến mạng riêng. Chuyển mạch đường hầm có thể được sử dụng tại bức tường lửa làm tăng khả năng quản lý truy nhập từ xa vào tài nguyên

của mạng nội bộ. Nó có thể kiểm tra các gói tin đến và đi, giao thức của các khung PPP hoặc tên của người dùng từ xa.

Phần mềm Client PPTP

Các thiết bị của ISP đã hỗ trợ PPTP thì không cần phần cứng hay phần mềm bổ sung nào cho các máy trạm, chỉ cần một kết nối PPP chuẩn. Nếu như các thiết bị của ISP không hỗ trợ PPTP thì một phần mềm ứng dụng Client vẫn có thể tạo liên kết nối bảo mật bằng các đầu tiên quay số kết nối tới ISP bằng PPP, sau đó quay số một lần nữa thông qua cổng PPTP ảo được thiết lập ở máy trạm.

Máy chủ truy nhập mạng

Máy chủ truy nhập mạng Network Access Server (NAS) còn có tên gọi là máy chủ truy nhập từ xa hay bộ tập trung truy nhập. NAS cung cấp khả năng truy nhập đường dây dựa trên phần mềm, có khả năng tính cước và có khả năng chịu đừng lỗi tại ISP, POP. NAS của ISP được thiết kế cho phép một số lượng lớn người dùng có thể quay số truy nhập vào cùng một lúc. Nếu một ISP cung cấp dịch vụ PPTP thì cần phải cài một NAS cho phép PPTP để hỗ trợ các client chạy trên các hệ điều hành khác nhau. Trong trường hợp này máy chủ ISP đóng vai trò như một client PPTP kết nối với máy chủ PPTP tại mạng riêng và máy chủ ISP trở thành một điểm cuối của đường hầm, điểm cuối còn lại máy chủ tại đầu mạng riêng

3.2.6 Một số ưu nhược điểm và khả năng ứng dụng của PPTP

Ưu điểm của PPTP là được thiết kế để hoạt động ở lớp 2 trong khi IPSec chạy ở lớp 3 của mô hình OSI. Việc hỗ trợ truyền dữ liệu ở lớp 2, PPTP có thể lan truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói tin IP trong đường hầm.

PPTP là một giải pháp tạm thời vì hầu hết các nhà cung cấp dịch vụ đều có kế hoạch thay đổi PPTP bằng L2TP khi giao thức này đã được mã hoá. PPTP thích hợp cho việc quay số truy nhập với số lượng người dùng giới hạn hơn là VPN kết nối LAN-LAN. Một vấn đề của PPTP là xử lý xác thực người thông qua hệ điều hành. Máy chủ PPTP cũng quá tải với một số lượng người dùng quay số truy nhập hay một lưu lượng lớn dữ liệu truyền qua, điều này là một yêu cầu của kết nối LAN-LAN. Khi sử dụng VPN dựa trên PPTP mà có hỗ trợ thiết bị ISP một số quyền quản lý phải chia sẽ cho ISP. Tính bảo mật của PPTP không mạng bằng IPSec. Nhưng quản lý bảo mật trong PPTP lại đơn giản hơn.

Khó khăn lớn nhất gắn kèm với PPTP là cơ chế yếu kém về bảo mật do nó dùng mã hóa đồng bộ trong khóa được xuất phát từ việc nó sử dụng mã hóa đối xứng là cách tạo ra khóa từ mật khẩu của người dùng. Điều này càng nguy hiểm hơn vì mật khẩu thường gửi dưới dạng phơi bày hoàn toàn trong quá trình xác nhận. Giao thức tạo đường hầm kế tiếp (L2F) được phát triển nhằm cải thiện bảo mật với mục đích này.

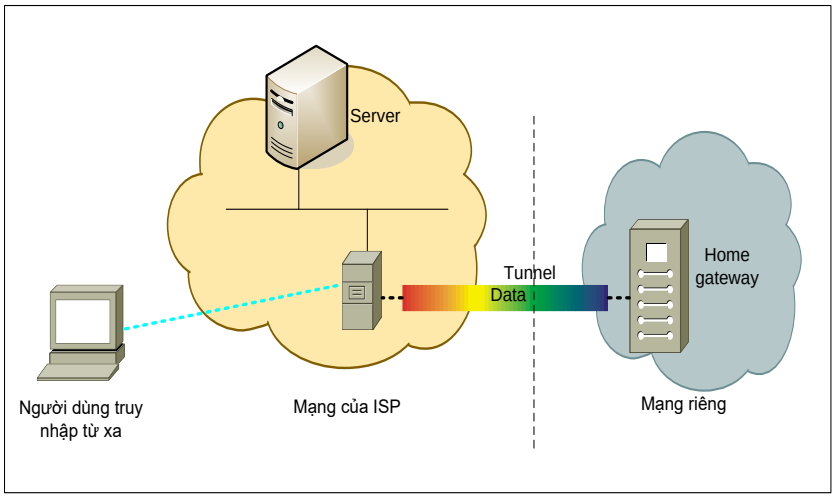
3.3 Giao thức chuyển tiếp lớp 2 (L2F)

Giao thức L2F được nghiên cứu và phát triển sớm nhất và là một trong những phương pháp truyền thống để cho người sử dụng ở truy nhập từ xa vào mang các doanh nghiệp thông qua thiết bị. L2F cung cấp các giải cho dịch vụ quay số ảo bằng thiết bị một đường hầm bảo mật thông qua cơ sở hạ tầng công cộng như Internet. Nó cho phép đóng gói các gói tin PPP trong khuôn dạng L2F và định đường hầm ở lớp liên kết dữ liệu.

3.3.1 Nguyên tắc hoạt động của L2F

Giao thức chuyển tiếp L2F đóng gói những gói tin lớp 2, sau đó trong truyền chúng đi qua mạng. Hệ thống sử dụng L2F gồm các thành phần sau.

- Máy trạm truy nhập mạng NAS: hướng lưu lượng đến và đi giữa các máy khách ở xa và Home Gateway. Một hệ thống ERX có thể hoạt động như NAS.
- Đường hầm: định hướng đường đi giữa NAS và Home Gateway. Một đường hầm gồm một số kết nối.
- Kết nối: Là một kết nối PPP trong đường hầm. Trong LCP, một kết nối L2F được xem như một phiên.
- Điểm đích: Là điểm kết thúc ở đâu xa của đường hầm. Trong trường hợp này thì Home Gateway là đích.



Hình 3.4: Hệ thống sử dụng L2F

Quá trình hoạt động của giao thức đường hầm chuyển tiếp là một quá trình tương đối phức tạp. Một người sử dụng ở xa quay số tới hệ thống NAS và khởi đầu một kết nối PPP tới ISP. Với hệ thống NAS và máy trạm có thể trao đổi các gói giao thức điều khiển liên kết. NAS sử dụng cơ sở dữ liệu cục bộ liên quan tới điểm tên miền để quyết định xem người sử dụng có hay không yêu cầu dịch vụ L2F.

Nếu người sử dụng yêu cầu L2F thì quá trình tiếp tục, NAS thu nhận địa chỉ của Gateway đích. Một đường hầm được thiết lập từ NAS tới Gateway đích nếu giữa chúng có chưa có đường hầm nào. Sự thành lập đường hầm bao gồm giai đoạn

xác thực từ ISP tới Gateway đích để chống lại tấn công bởi những kẻ thứ ba. Một kết nối PPP mới được tạo ra trong đường hầm, điều này có tác động kéo dài phiên PPP mới được tạo ra người sử dụng ở xa tới Home Gateway. Kết nối này được thiết lập theo một quy trình như sau. Home Gateway tiếp nhận các lựa chọn và tất cả thông tin xác thực PAP/CHAP như thoả thuận bởi đầu cuối người sử dụng và NAS. Home Gateway chấp nhận kết nối hay thoả thuận lại LCP và xác thực lại người sử dụng. Khi NAS tiếp nhận lưu lượng dữ liệu từ người sử dụng, nó đóng gói lưu lượng vào trong các khung L2F và hướng chúng vào trong đường hầm. Tại Home Gateway khung được tách bỏ và dữ liệu đóng gói được hướng tới mạng một doanh nghiệp hay người dùng.

Khi hệ thống đã thiết lập điểm đích đường hầm và những phiên kết nối, ta phải điều khiển và quản lý lưu lượng L2F bằng cách. Ngăn cản tạo những đích đến, đường hầm và các phiên mới. Đóng và mở lại tất cả hay chọn lựa những điểm đích, đường hầm và phiên, có khả năng kiểm tra tổng UDP. Thiết lập thời gian rỗi cho hệ thống và lưu giữ cơ sở dữ liệu vào các đường hầm kết nối.

3.3.2 Những ưu điểm và nhược điểm của L2F

Mặc dù L2F yêu cầu mở rộng xử lý với các LCP và phương pháp tùy chọn khác nhau, nó được dùng rộng rãi hơn so với PPTP bởi vì nó là một giải pháp chuyển hướng khung ở cấp thấp. Nó cũng cung cấp một nền tảng giải pháp VPN tốt hơn PPTP đối với mạng doanh nghiệp.

Những thuận lợi chính của việc triển khai giải pháp L2F bao gồm:

- Nâng cao bảo mật cho quá trình giao dịch.
- Có nền tảng độc lập.
- Không cần những sự lắp đặt đặc biệt với ISP.
- Hỗ trợ một phạm vi rộng rãi các công nghệ mạng như ATM, IPX, NetBEUI, và Frame Relay

Những khó khăn của việc triển khai L2F bao gồm:

- L2F yêu cầu cấu hình và hỗ trợ lớn.
- Thực hiện L2F dựa trên ISP. Nếu trên ISP không hỗ trợ L2F thì không thể triển khai L2F được.

3.4. Giao thức đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol)

3.4.1. Giới thiệu

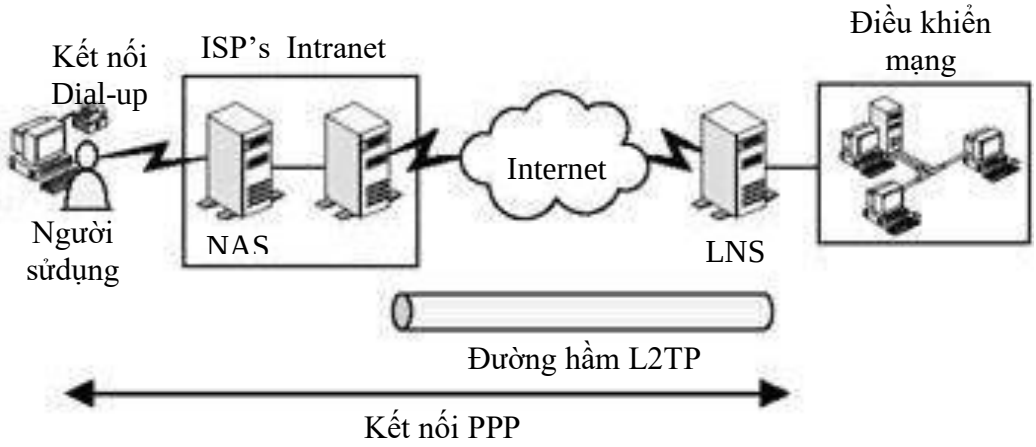
IETF đã kết hợp hai giao thức PPTP và L2F và phát triển thành L2TP. Nó kết hợp những đặc điểm tốt nhất của PPTP và L2F. Vì vậy, L2TP cung cấp tính linh động, có thể thay đổi, và hiệu quả chi phí cho giải pháp truy cập từ xa của L2F và khả năng kết nối điểm điểm nhanh của PPTP.

Do đó L2TP là sự trộn lẫn cả hai đặc tính của PPTP và L2F, bao gồm:

- L2TP hỗ trợ đa giao thức và đa công nghệ mạng, như IP, ATM, FR, và PPP.
- L2TP không yêu cầu việc triển khai thêm bất cứ phần mềm nào, như điều khiển và hệ điều hành hỗ trợ. Do đó, cả người dùng và mạng riêng Intranet cũng không cần triển khai thêm các phần mềm chuyên biệt.
- L2TP cho phép người dùng từ xa truy cập vào mạng từ xa thông qua mạng công cộng với một địa chỉ IP chưa đăng ký (hoặc riêng tư).

Quá trình xác nhận và chứng thực của L2TP được thực hiện bởi cổng mạng máy chủ. Do đó, ISP không cần giữ dữ liệu xác nhận hoặc quyền truy cập của người dùng từ xa. Hơn nữa, mạng riêng intranet có thể định nghĩa những chính sách truy cập riêng cho chính bản thân. Điều này làm qui trình xử lý của việc thiết lập đường hầm nhanh hơn so với giao thức tạo hầm trước đây.

Điểm chính của L2TP tunnels là L2TP thiếp lập đường hầm PPP không giống như PPTP, không kết thúc ở gần vùng của ISP. Thay vào đó, những đường hầm mở rộng đến cổng của mạng máy chủ (hoặc đích), như hình 3.23, những yêu cầu của đường hầm L2TP có thể khởi tạo bởi người dùng từ xa hoặc bởi cổng của ISP.



Hình 3.5: Đường hầm L2TP

Khi PPP frames được gửi thông qua L2TP đường hầm, chúng được đóng gói như những thông điệp User Datagram Protocol (UDP). L2TP dùng những thông điệp UDP này cho việc tạo hầm dữ liệu cũng như duy trì đường hầm. Ngoài ra, đường hầm dữ liệu và đường hầm duy trì gói tin, không giống những giao thức tạo hầm trước, cả hai có cùng cấu trúc gói dữ liệu.

3.4.2. Các thành phần của L2TP

Quá trình giao dịch L2TP đảm nhiệm 3 thành phần cơ bản, một Network Access Server (NAS), một L2TP Access Concentrator (LAC), và một L2TP Network Server (LNS).

Network Access Server (NAS)

L2TP NASs là thiết bị truy cập điểm-điểm cung cấp dựa trên yêu cầu kết nối Internet đến người dùng từ xa, là những người quay số (thông qua PSTN hoặc ISDN) sử dụng kết nối PPP. NASs phản hồi lại xác nhận người dùng từ xa ở nhà cung cấp ISP cuối và xác định nếu có yêu cầu kết nối ảo. Giống như PPTP NASs, L2TP NASs được đặt tại ISP site và hành động như client trong qui trình thiết lập L2TP tunnel. NASs có thể hồi đáp và hỗ trợ nhiều yêu cầu kết nối đồng thời và có thể hỗ trợ một phạm vi rộng các client

Bộ tập kết truy cập L2TP

Vai trò của LACs trong công nghệ tạo hầm L2TP thiết lập một đường hầm thông qua một mạng công cộng (như PSTN, ISDN, hoặc Internet) đến LNS ở tại điểm cuối mạng chủ. LACs phục vụ như điểm kết thúc của môi trường vật lý giữa client và LNS của mạng chủ.

L2TP Network Server

LNSs được đặt tại cuối mạng chủ. Do đó, chúng dùng để kết thúc kết nối L2TP ở cuối mạng chủ theo cùng cách kết thúc đường hầm từ client của LACs. Khi một LNS nhận một yêu cầu cho một kết nối ảo từ một LAC, nó thiết lập đường hầm và xác nhận người dùng, là người khởi tạo yêu cầu kết nối. Nếu LNS chấp nhận yêu cầu kết nối, nó tạo giao diện ảo.

3.4.3. Qui trình xử lý L2TP

Khi một người dùng từ xa cần thiết lập một L2TP tunnel thông qua Internet hoặc mạng chung khác, theo các bước tuần tự sau đây:

(1) Người dùng từ xa gửi yêu cầu kết nối đến ISP's NAS gần nhất của nó, và bắt đầu khởi tạo một kết nối PPP với nhà ISP cuối.

(2) NAS chấp nhận yêu cầu kết nối sau khi xác nhận người dùng cuối. NAS dùng phương pháp xác nhận PPP, như PAP, CHAP, SPAP, và EAP cho mục đích này.

(3) Sau đó NAS kích hoạt LAC, nhằm thu nhập thông tin cùng với LNS của mạng đích.

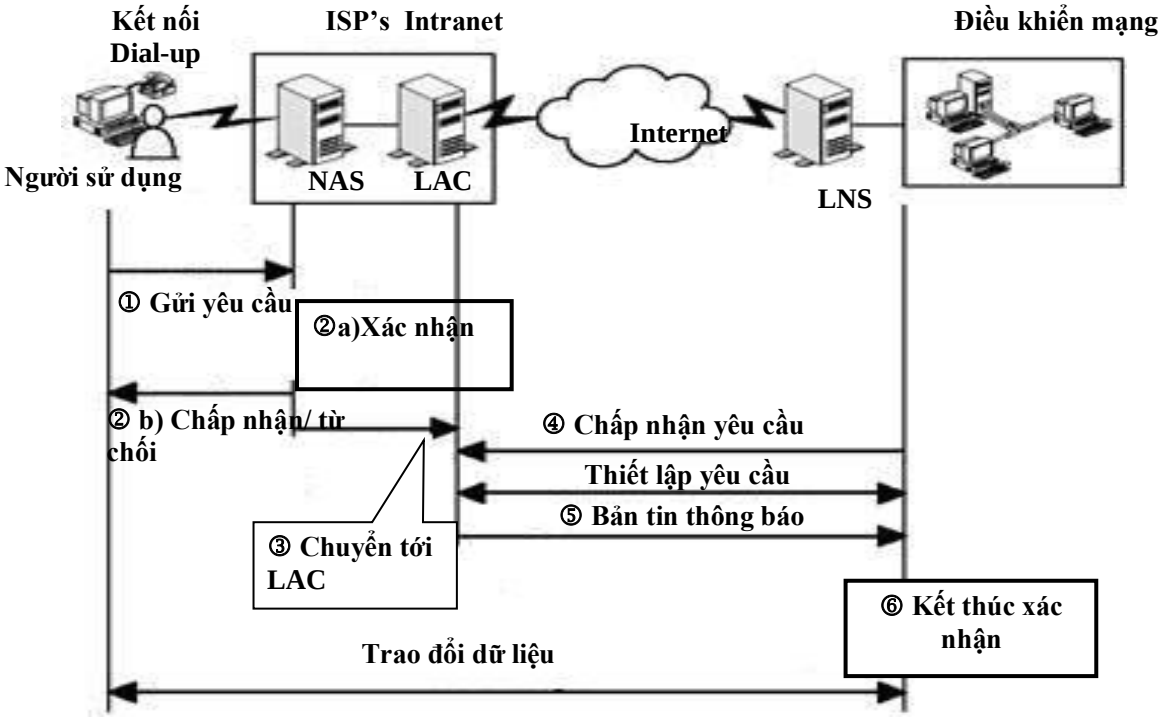
(4) Kế tiếp, LAC thiết lập một đường hầm LAC-LNS thông qua mạng trung gian giữa hai đầu cuối. Đường hầm trung gian có thể là ATM, Frame Relay, hoặc IP/UDP.

(5) Sau khi đường hầm đã được thiết lập thành công, LAC chỉ định một Call ID (CID) đến kết nối và gửi một thông điệp thông báo đến LNS. Thông báo xác định này chứa thông tin có thể được dùng để xác nhận người dùng. Thông điệp cũng mang theo LCP options dùng để thoả thuận giữa người dùng và LAC.

(6) LNS dùng thông tin đã nhận được từ thông điệp thông báo để xác nhận người dùng cuối. Nếu người dùng được xác nhận thành công và LNS chấp

nhận yêu cầu đường hầm, một giao diện PPP ảo (L2TP tunnel) được thiết lập cùng với sự giúp đỡ của LCP options nhận được trong thông điệp thông báo.

(7) Sau đó người dùng từ xa và LNS bắt đầu trao đổi dữ liệu thông qua đường hầm.



Hình 3.6: Mô tả qui trình thiết lập L2TP tunnel

L2TP, giống PPTP và L2F, hỗ trợ hai chế độ hoạt động L2TP, bao gồm:

Chế độ gọi đến. Trong chế độ này, yêu cầu kết nối được khởi tạo bởi người dùng từ xa.

Chế độ gọi đi. Trong chế độ này, yêu cầu kết nối được khởi tạo bởi LNS. Do đó, LNS chỉ dẫn LAC lập một cuộc gọi đến người dùng từ xa. Sau khi LAC thiết lập cuộc gọi, người dùng từ xa và LNS có thể trao đổi những gói dữ liệu đã qua đường hầm.

3.4.4 Dữ liệu đường hầm L2TP

Tương tự PPTP tunneled packets, L2TP đóng gói dữ liệu trải qua nhiều tầng đóng gói. Sau đây là một số giai đoạn đóng gói của L2TP data tunneling:

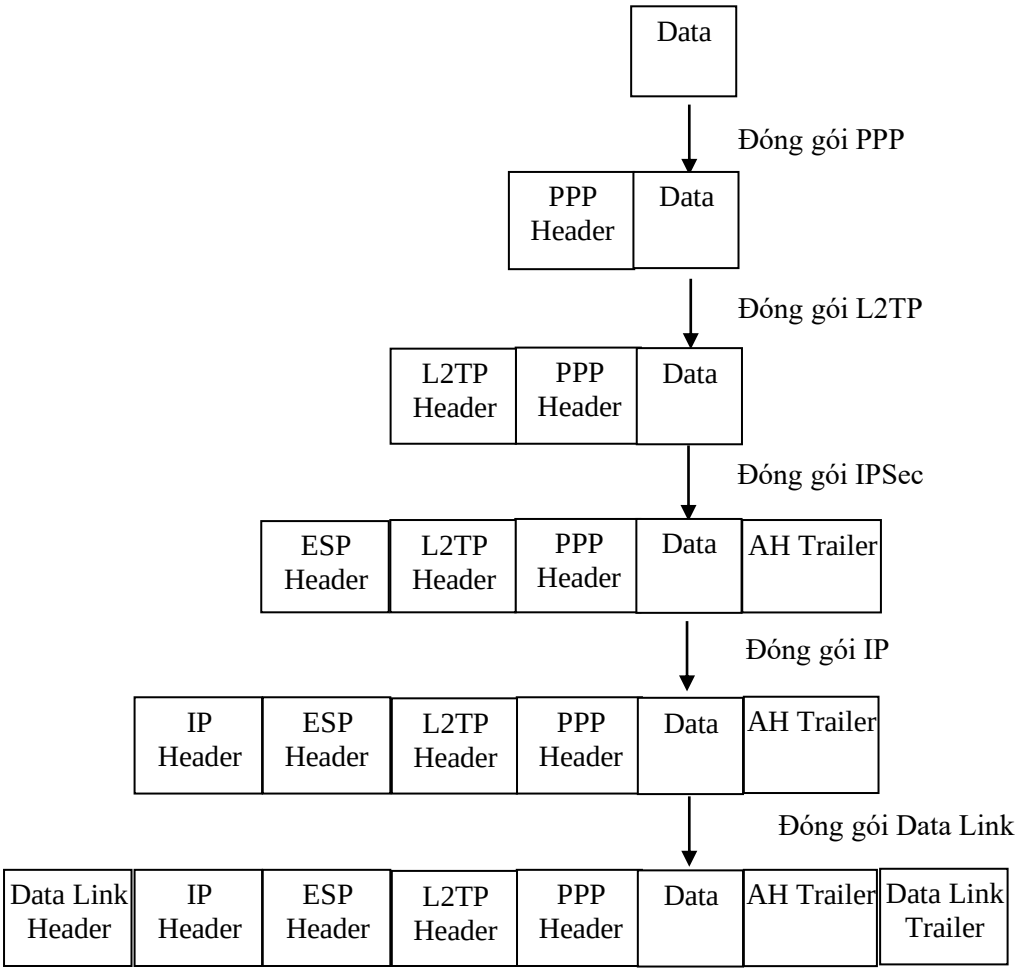
PPP đóng gói dữ liệu không giống phương thức đóng gói của PPTP, dữ liệu không được mã hóa trước khi đóng gói. Chỉ PPP header được thêm vào dữ liệu payload gốc.

L2TP đóng gói khung của PPP. Sau khi original payload được đóng gói bên trong một PPP packet, một L2TP header được thêm vào nó.

UDP Encapsulation of L2TP frames. Kế tiếp, gói dữ liệu đóng gói L2TP được đóng gói thêm nữa bên trong một UDP frame. Hay nói cách khác, một UDP header được thêm vào L2TP frame đã đóng gói. Cổng nguồn và đích bên trong UDP header được thiết lập đến 1710 theo chỉ định.

IPSec Encapsulation of UDP datagrams. Sau khi L2TP frame trở thành UDP đã được đóng gói, UDP frame này được mã hoá và một phần đầu IPSec ESP được thêm vào nó. Một phần đuôi IPSec AH cũng được chèn vào gói dữ liệu đã được mã hóa và đóng gói.

IP Encapsulation of IPSec-encapsulated datagrams. Kế tiếp, phần đầu IP cuối cùng được thêm vào gói dữ liệu IPSec đã được đóng gói. Phần đầu IP chứa đựng địa chỉ IP của L2TP server (LNS) và người dùng từ xa.

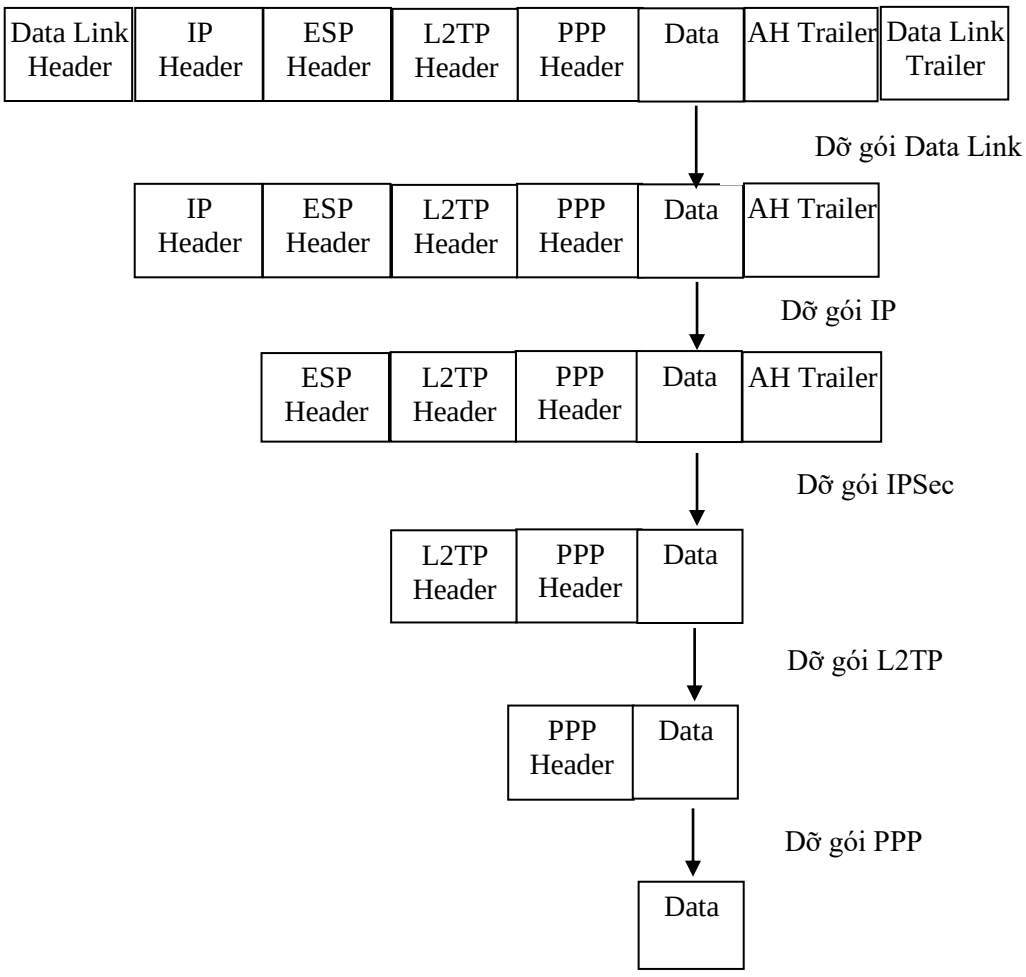


Hình 3.7: Quá trình hoàn tất của dữ liệu qua đường hầm

Đóng gói tầng Data Link. Phần đầu và phần cuối tầng Data Link cuối cùng được thêm vào gói dữ liệu IP xuất phát từ quá trình đóng gói IP cuối cùng. Phần đầu và phần cuối của tầng Data Link giúp gói dữ liệu đi đến nút đích. Nếu nút đích là nội bộ, phần đầu và phần cuối tầng Data Link được dựa trên công nghệ LAN (ví dụ, chúng có thể là mạng Ethernet). Ở một khía cạnh khác, nếu gói dữ liệu là phương

tiện cho một vị trí từ xa, phần đầu và phần cuối PPP được thêm vào gói dữ liệu L2TP đã đóng gói.

Qui trình xử lý de-tunneling những gói dữ liệu L2TP đã tunnel thì ngược lại với qui trình đường hầm. Khi một thành phần L2TP (LNS hoặc người dùng cuối) nhận được L2TP tunneled packet, trước tiên nó xử lý gói dữ liệu bằng cách gỡ bỏ Data Link layer header and trailer. Kế tiếp, gói dữ liệu được xử lý sâu hơn và phần IP header được gỡ bỏ. Gói dữ liệu sau đó được xác nhận bằng việc sử dụng thông tin mang theo bên trong phần IPSec ESP header và AH trailer. Phần IPSec ESP header cũng được dùng để giải mã và mã hóa thông tin. Kế tiếp, phần UDP header được xử lý rồi loại ra. Phần Tunnel ID và phần Call ID trong phần L2TP header dùng để nhận dạng phần L2TP tunnel và phiên làm việc. Cuối cùng, phần PPP header được xử lý và được gỡ bỏ và phần PPP payload được chuyển hướng đến protocol driver thích hợp cho qui trình xử lý.

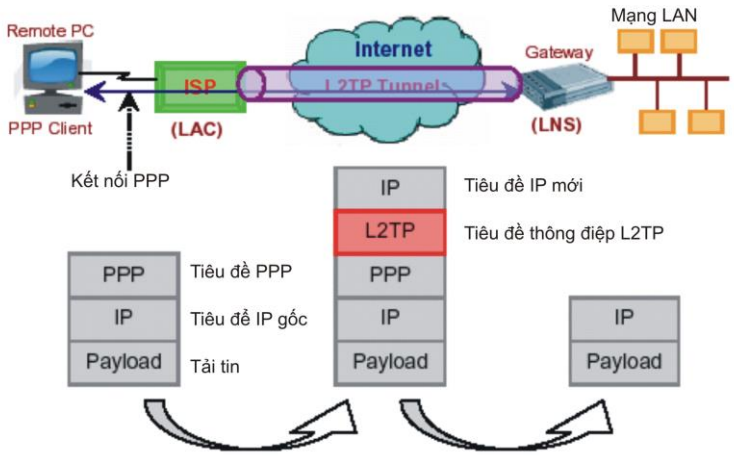


Hình 3.8: Mô tả qui trình xử lý de-tunneling gói dữ liệu L2TP

3.4.5. Chế độ đường hầm L2TP

L2TP hỗ trợ 2 chế độ - chế độ đường hầm bắt buộc và chế độ đường hầm tự nguyện. Những đường hầm này giữ một vai trò quan trọng trong bảo mật giao dịch dữ liệu từ điểm cuối đến điểm khác.

Trong *chế độ đường hầm bắt buộc*, khung PPP từ PC ở xa được tạo đường hầm trong suốt tới mạng LAN. Điều này có nghĩa là Client ở xa không điều khiển đường hầm và nó sẽ xuất hiện như nó được kết nối chính xác tới mạng công ty thông qua một kết nối PPP. Phần mềm L2TP sẽ thêm L2TP header vào mỗi khung PPP cái mà được tạo đường hầm. Header này được sử dụng ở một điểm cuối khác của đường hầm, nơi mà gói tin L2TP có nhiều thành phần.



Hình 3.9. Chế độ đường hầm bắt buộc L2TP.

Các bước thiết lập L2TP đường hầm bắt buộc được mô tả trong hình 3.28 theo các bước sau:

(1) Người dùng từ xa yêu cầu một kết nối PPP từ NAS được đặt tại ISP site.

(2) NAS xác nhận người dùng. Qui trình xác nhận này cũng giúp NAS biết được cách thức người dùng yêu cầu kết nối.

(3) Nếu NAS tự do chấp nhận yêu cầu kết nối, một kết nối PPP được thiết lập giữa ISP và người dùng từ xa.

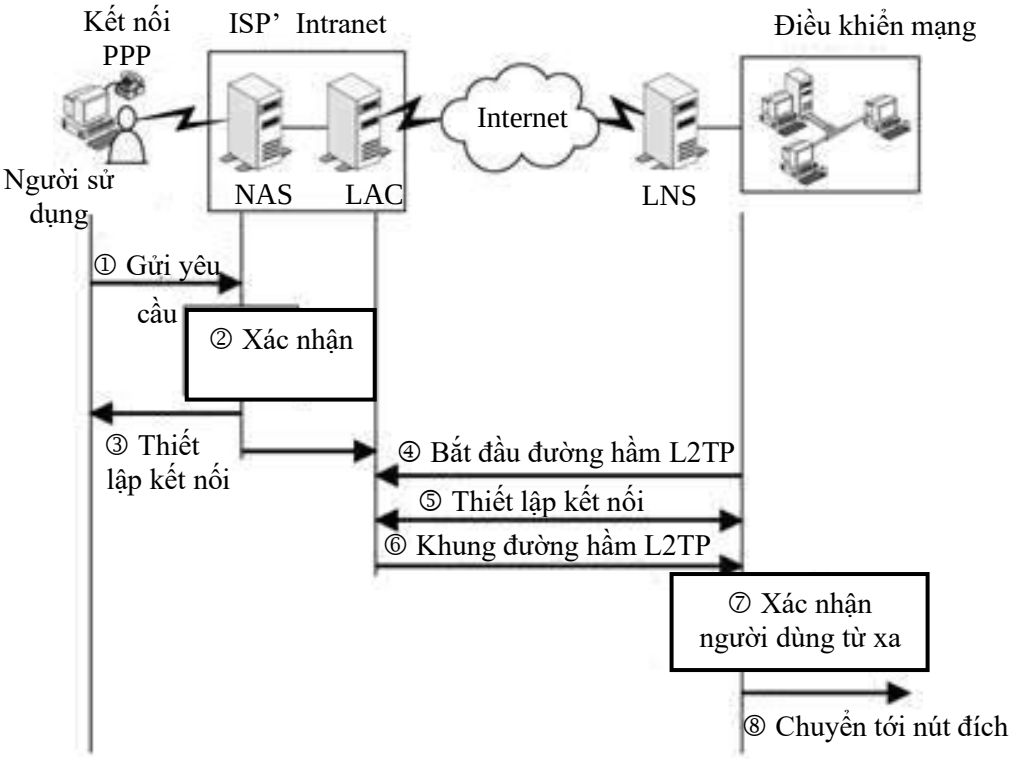
(4) LAC khởi tạo một L2TP tunnel đến một LNS ở mạng chủ cuối.

(5) Nếu kết nối được chấp nhận bởi LNS, PPP frames trải qua quá trình L2TP tunneling. Những L2TP-tunneled frames này sau đó được chuyển đến LNS thông qua L2TP tunnel.

(6) LNS chấp nhận những frame này và phục hồi lại PPP frame gốc.

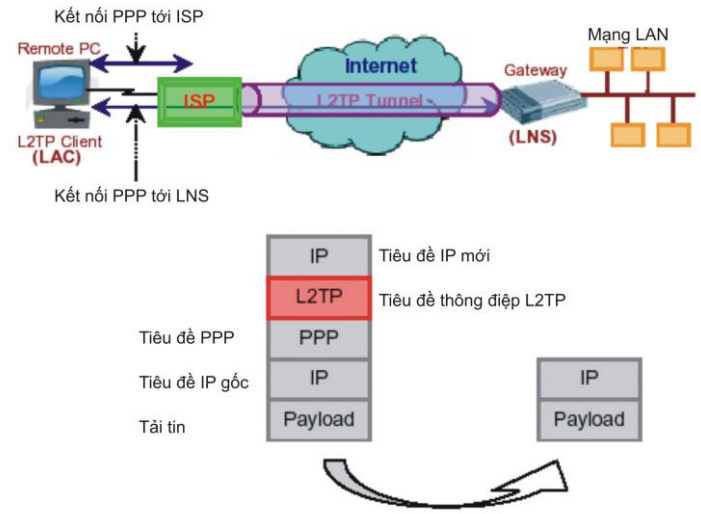
(7) Cuối cùng, LNS xác nhận người dùng và nhận các gói dữ liệu. Nếu người dùng được xác nhận hợp lệ, một địa chỉ IP thích hợp được ánh xạ đến frame

(8) Sau đó frame này được chuyển đến nút đích trong mạng intranet.



Hình 3.10. Thiết lập một đường hầm bắt buộc

Chế độ đường hầm tự nguyện có Client ở xa khi gắn liên chức năng LAC và nó có thể điều khiển đường hầm. Từ khi giao thức L2TP hoạt động theo một cách y hệt như khi sử dụng đường hầm bắt buộc, LNS sẽ không thấy sự khác biệt giữa hai chế độ.



Hình 3.11 Chế độ đường hầm tự nguyện L2TP.

Thuận lợi lớn nhất của đường hầm tự nguyện L2TP là cho phép người dùng từ xa kết nối vào internet và thiết lập nhiều phiên làm việc VPN đồng thời. Tuy nhiên, để ứng dụng hiệu quả này, người dùng từ xa phải được gán nhiều địa chỉ IP. Một trong những địa chỉ IP được dùng cho kết nối PPP đến ISP và một được dùng

để hỗ trợ cho mỗi L2TP tunnel riêng biệt. Nhưng lợi ích này cũng là một bất lợi cho người dùng từ xa và do đó, mạng chủ có thể bị tổn hại bởi các cuộc tấn công.

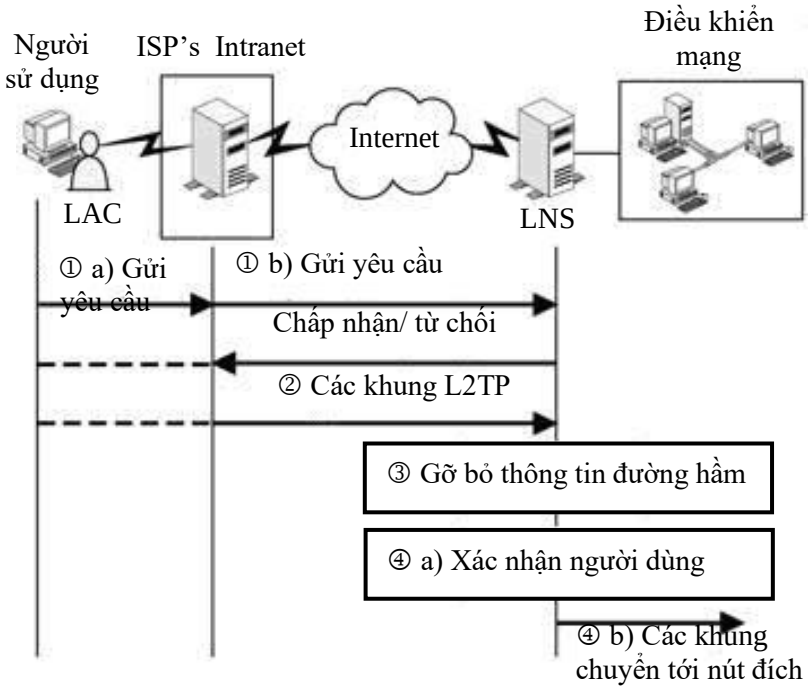
Việc thiết lập một voluntary L2TP tunnel thì đơn giản hơn việc thiết lập một đường hầm bắt buộc bởi vì người dùng từ xa đảm nhiệm việc thiết lập lại kết nối PPP đến điểm ISP cuối. Các bước thiết lập đường hầm tự nguyện L2TP gồm :

(1) LAC (trong trường hợp này là người dùng từ xa) phát ra một yêu cầu cho một đường hầm tự nguyện L2TP đến LNS.

(2) Nếu yêu cầu đường hầm được LNS chấp nhận, LAC tạo hầm các PPP frame cho mỗi sự chỉ rõ L2TP và chuyển hướng những frame này thông qua đường hầm.

(3) LNS chấp nhận những khung đường hầm, lưu chuyển thông tin tạo hầm, và xử lý các khung.

(4) Cuối cùng, LNS xác nhận người dùng và nếu người dùng được xác nhận thành công, chuyển hướng các frame đến nút cuối trong mạng Intranet.



Hình 3.12: Thiết lập L2TP đường hầm tự nguyện.

3.4.6. Những thuận lợi và bất lợi của L2TP

Thuận lợi chính của L2TP được liệt kê theo danh sách dưới đây:

- L2TP là một giải pháp chung. Hay nói cách khác nó là một nền tảng độc lập. Nó cũng hỗ trợ nhiều công nghệ mạng khác nhau. Ngoài ra, nó còn hỗ trợ giao dịch qua kết nối WAN non-IP mà không cần một IP.

- L2TP tunneling trong suốt đối với ISP giống như người dùng từ xa. Do đó, không đòi hỏi bất kỳ cấu hình nào ở phía người dùng hay ở ISP.

- L2TP cho phép một tổ chức điều khiển việc xác nhận người dùng thay vì ISP phải làm điều này.
- L2TP cung cấp chức năng điều khiển cấp thấp có thể giảm các gói dữ liệu xuống tùy ý nếu đường hầm quá tải. Điều này làm cho qua trình giao dịch bằng L2TP nhanh hơn so với quá trình giao dịch bằng L2F.
- L2TP cho phép người dùng từ xa chưa đăng ký (hoặc riêng tư) địa chỉ IP truy cập vào mạng từ xa thông qua một mạng công cộng.
- L2TP nâng cao tính bảo mật do sử dụng IPSec-based payload encryption trong suốt qua trình tạo hầm, và khả năng triển khai xác nhận IPSec trên từng gói dữ liệu.

Ngoài ra việc triển khai L2TP cũng gặp một số bất lợi sau:

- L2TP chậm hơn so với PPTP hay L2F bởi vì nó dùng IPSec để xác nhận mỗi gói dữ liệu nhận được.
- Mặc dù PPTP được lưu chuyển như một giai pháp VPN dựng sẵn, một Routing and Remote Access Server (RRAS) cần có những cấu hình mở rộng.

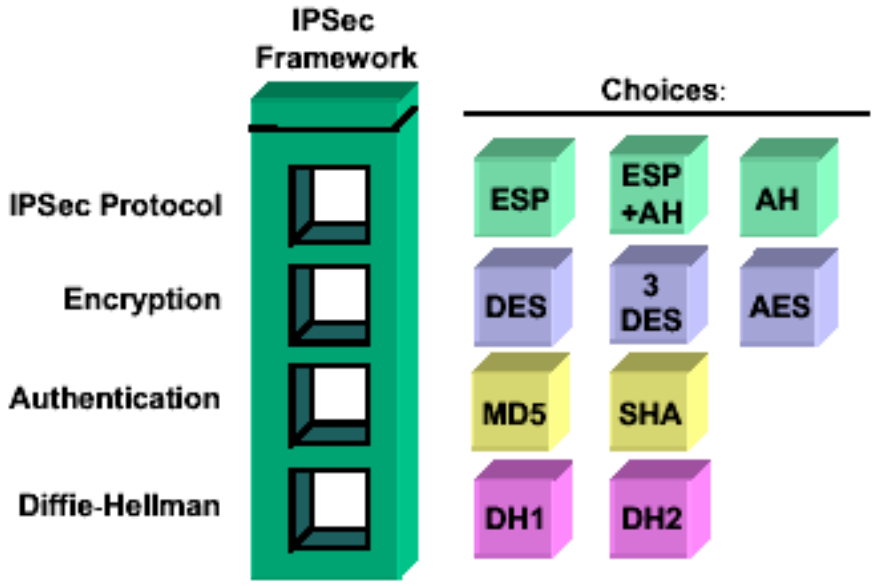
3.5. GRE (Generic Routing Encapsulution)

- Giao thức mang đa giao thức này đóng gói IP, CLNP, và bất kỳ các gói dữ liệu giao thức khác vào bên trong các đường hầm IP.
- Với giao thức tạo đường hầm GRE, một Router ở mỗi điểm sẽ đóng gói các gói dữ liệu của một giao thức cụ thể vào trong một tiêu đề IP, tạo ra một đường kết nối ảo điểm-điểm tới các Router ở các điểm khác trong một đám mây mạng IP, mà ở đó tiêu đề IP sẽ được gỡ bỏ.
- Bằng cách kết nối các mạng con đa giao thức trong một môi trường Backbone đơn giao thức, đường hầm IP cho phép mở rộng mạng qua một môi trường xương sống đơn giao thức. Tạo đường hầm GRE cho phép các giao thức desktop có thể tận dụng được các ưu điểm của khả năng chọn tuyến cao của IP.
- GRE không cung cấp sự mã hoá và có thể được giám sát bằng một công cụ phân tích giao thức.

3.6 Giao thức bảo mật IP (IP Security Protocol)

3.6.1. Giới thiệu

IPSec không phải là một giao thức. Nó là một khung của các tập giao thức chuẩn mở được thiết kế để cung cấp sự xác thực dữ liệu, tính toàn vẹn dữ liệu, và sự tin cậy dữ liệu.



Hình 3.13 Sơ đồ khung IPSec

IPSec chạy ở lớp 3 và sử dụng IKE để thiết lập SA giữa các đối tượng ngang hàng. Dưới đây là các đối tượng cần được thiết lập như là một phần của sự thiết lập SA.

- Thuật toán mã hoá.
- Thuật toán băm (Hash).
- Phương thức xác thực.
- Nhóm Diffie-Hellman.

Chức năng của IPSec là để thiết lập sự bảo mật tương ứng giữa hai đối tượng ngang hàng. Sự bảo mật này xác định khoá, các giao thức, và các thuật toán được sử dụng giữa các đối tượng ngang hàng. Các SA IPSec có thể chỉ được thiết lập như là vô hướng.

Sau khi gói tin được chuyển tới tầng mạng thì gói tin IP không gắn liền với bảo mật. Bởi vậy, không cam đoan rằng IP datagram nhận được là:

- Từ người gửi yêu cầu.

- Dữ liệu gốc từ người gửi.

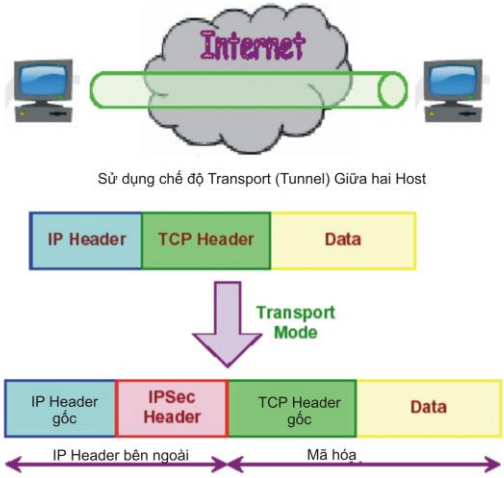
- Không bị kiểm tra bởi bên thứ 3 trong khi gói tin đang được gửi từ nguồn tới đích.

IPSec là một phương pháp để bảo vệ IP datagram. IPSec bảo vệ IP datagram bằng cách định nghĩa một phương pháp định rõ lưu lượng để bảo vệ, cách lưu lượng đó được bảo vệ và lưu lượng đó được gửi tới ai. IPSec có thể bảo vệ gói tin giữa các host, giữa cổng an ninh mạng, hoặc giữa các host và cổng an ninh. IPSec cũng thực hiện đóng gói dữ liệu và xử lý các thông tin để thiết lập, duy trì, và hủy bỏ đường hầm khi không dùng đến nữa. Các gói tin truyền trong đường hầm có khuôn dạng

giống như các gói tin bình thường khác và không làm thay đổi các thiết bị, kiến trúc cũng như các ứng dụng hiện có trên mạng trung gian, qua đó cho phép giảm đáng kể chi phí để triển khai và quản lý.

Nó là tập hợp các giao thức được phát triển bởi IETF để hỗ trợ sự thay đổi bảo mật của gói tin ở tầng IP qua mạng vật lý. IPSec được phát triển rộng rãi để thực hiện VPN. IPSec hỗ trợ hai chế độ mã hóa: transport và tunnel

Chế độ transport chỉ mã hóa phần payload của mỗi gói tin, nhưng bỏ đi phần header không sờ đến. Ở bên nhận, thiết bị IPSec_compliant sẽ giải mã từng gói tin.

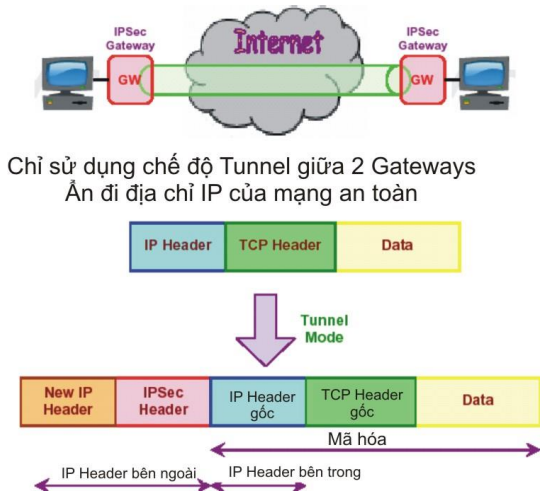


Hình 3.14 Chế độ Transport

Mode transport bảo vệ phần tải tin của gói dữ liệu, các giao thức ở lớp cao hơn, nhưng vận chuyển địa chỉ IP nguồn ở dạng "clear". Địa chỉ IP nguồn được sử dụng để định tuyến các gói dữ liệu qua mạng Internet. Mode transport ESP được sử dụng giữa hai máy, khi địa chỉ đích cuối cùng là địa chỉ máy của chính bản thân nó. Mode transport cung cấp tính bảo mật chỉ cho các giao thức lớp cao hơn.

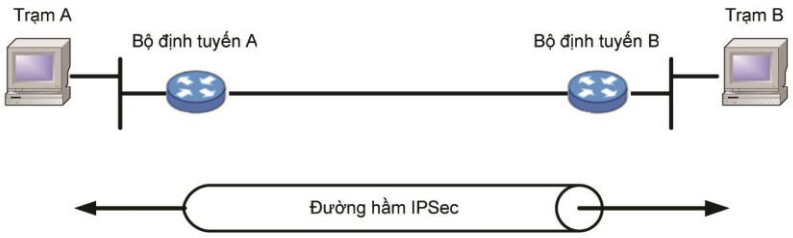
Nhược điểm của chế độ này là nó cho phép các thiết bị trong mạng nhìn thấy địa chỉ nguồn và đích của gói tin và có thể thực hiện một số xử lý (như phân tích lưu lượng) dựa trên các thông tin của tiêu đề IP. Tuy nhiên, nếu dữ liệu được mã hóa bởi ESP thì sẽ không biết được thông tin cụ thể bên trong gói tin IP là gì. Theo IETF thì chế độ truyền tải chỉ có thể được sử dụng khi hai hệ thống đầu cuối IP-VPN có thực hiện IPSec.

Chế độ tunnel mã hóa cả phần header và payload để cung cấp sự thay đổi bảo mật nhiều hơn của gói tin. Ở bên nhận, thiết bị IPSec_compliant sẽ giải mã từng gói tin. Một trong nhiều giao thức phổ biến được sử dụng để xây dựng VPN là chế độ đường hầm IPSec.

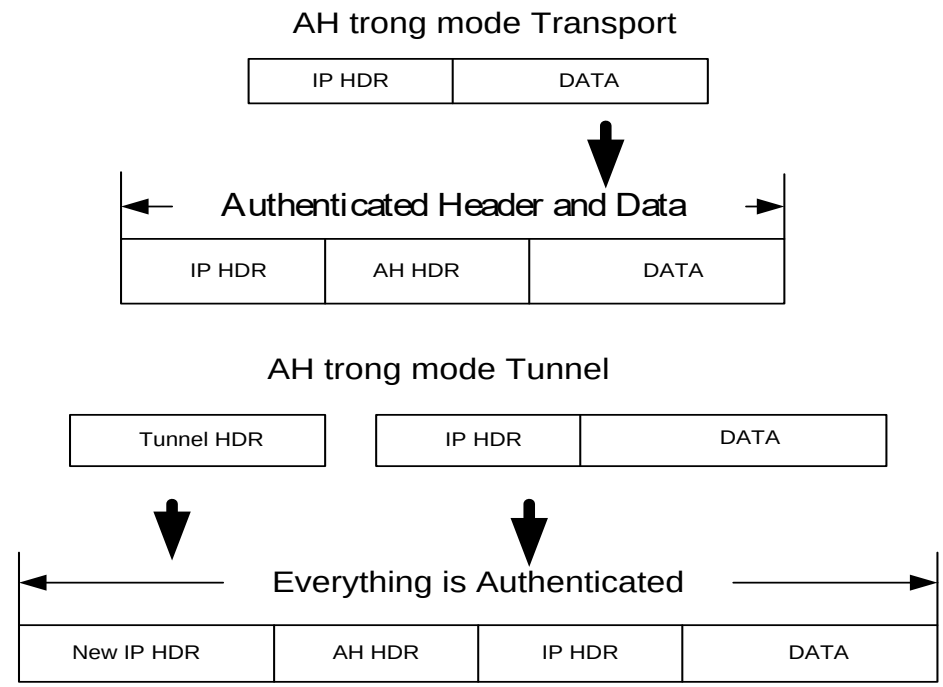


Hình 3.15 Chế độ tunnel

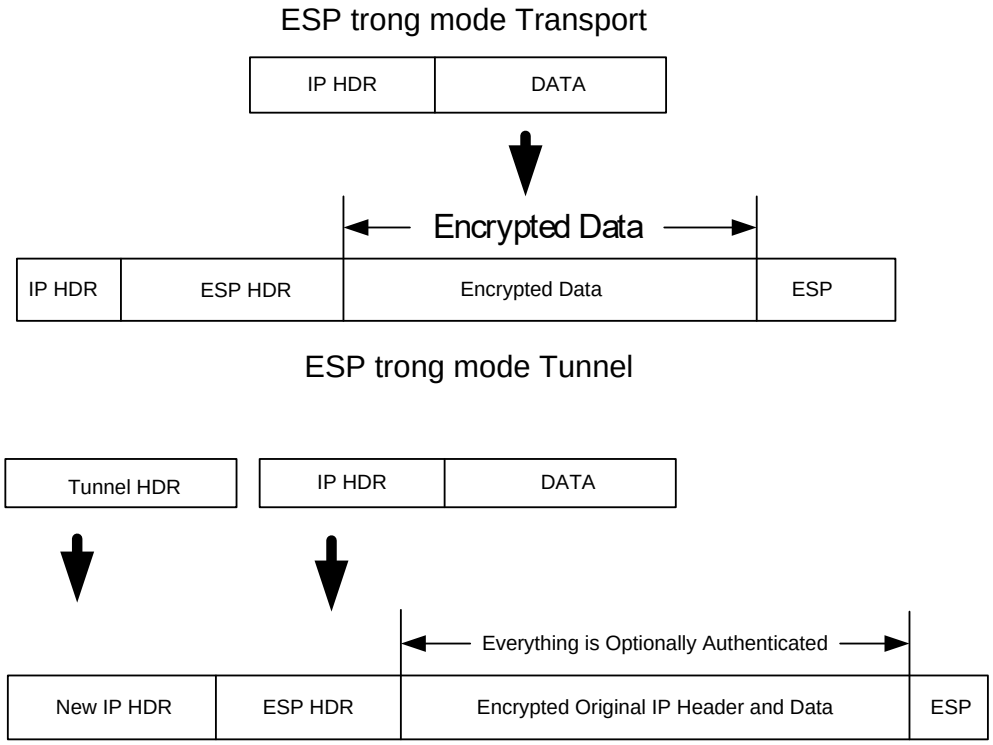
Chế độ này cho phép các thiết bị mạng như bộ định tuyến thực hiện xử lý IPSec thay cho các trạm cuối (host). Trong ví dụ trên hình 3.9, bộ định tuyến A xử lý các gói từ trạm A, gửi chúng vào đường hầm. Bộ định tuyến B xử lý các gói nhận được trong đường hầm, đưa về dạng ban đầu và chuyển chúng tới trạm B. Như vậy, các trạm cuối không cần thay đổi mà vẫn có được tính an ninh dữ liệu của IPSec. Ngoài ra, nếu sử dụng chế độ đường hầm, các thiết bị trung gian trong mạng sẽ chỉ nhìn thấy được các địa chỉ hai điểm cuối của đường hầm (ở đây là các bộ định tuyến A và B). Khi sử dụng chế độ đường hầm, các đầu cuối của IPSec-VPN không cần phải thay đổi ứng dụng hay hệ điều hành.



Hình 3.16: Thiết bị mạng thực hiện trong IPSec trong chế độ đường hầm



Hình 3.17 AH trong mode Tunnel và transport



Hình 3.18. ESP trong mode Tunnel và transport

IPSec được phát triển cho lí do bảo mật bao gồm tính toàn vẹn không kết nối, xác thực dữ liệu gốc, anti_replay, và mã hóa. IETF định nghĩa theo chức năng của IPSec.

- *Tính xác thực*: Mọi người đều biết là dữ liệu nhận được giống với dữ liệu được gửi và người gửi yêu cầu là người gửi hiện tại.

- *Tính toàn vẹn*: Đảm bảo rằng dữ liệu được truyền từ nguồn tới đích mà không bị thay đổi hay có bất kỳ sự xáo trộn nào.
- *Tính bảo mật:* Người gửi có thể mã hóa các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu lấy được cũng không đọc được.
- *Mã hóa*: Một cơ cấu cơ bản được sử dụng để cung cấp tính bảo mật.
- *Phân tích lưu lượng*: Phân tích luồng lưu lượng mạng cho mục đích khấu trừ thông tin hữu ích cho kẻ thù. Ví dụ như thông tin thường xuyên được truyền, định danh của các bên đối thoại, kích cỡ gói tin, định danh luồng sử dụng, vv..
- *SPI*: Viết tắt của chỉ số tham số an toàn (security parameter index), nó là chỉ số không có kết cấu rõ ràng, được sử dụng trong liên kết với địa chỉ đích để định danh liên kết an toàn tham gia.

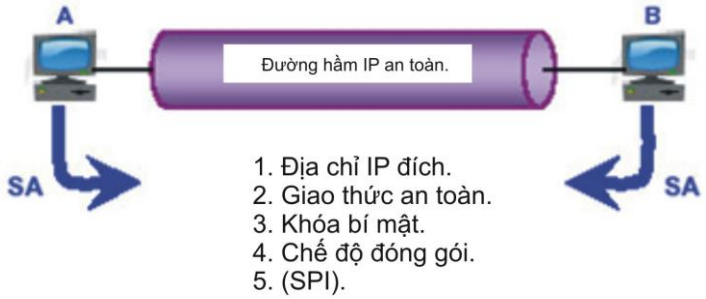
Phương pháp bảo vệ IP datagram bằng cách sử dụng một trong các giao thức IPSec, Encapsulate Security Payload (ESP) hoặc Authentication Header (AH). AH cung cấp chứng cứ gốc của gói tin nhận, toàn vẹn dữ liệu, và bảo vệ anti_replay. ESP cung cấp cái mà AH cung cấp cộng với tính bảo mật dữ liệu tùy ý. Nền tảng bảo mật được cung cấp bởi AH hoặc ESP phụ thuộc vào thuật toán mã hóa áp dụng trên chúng.

Dịch vụ bảo mật mà IPSec cung cấp yêu cầu khóa chia sẻ để thực hiện tính xác thực và bảo mật. Giao thức khóa chia sẻ là Internet Key Exchange (IKE), là một phương pháp chuẩn của xác thực IPSec, dịch vụ thương lượng bảo mật, và phát sinh khóa chia sẻ.

3.6.2 Liên kết an toàn

Một liên kết an toàn SA là một liên kết đơn hình, mà các dịch vụ bảo mật cho phép truyền tải nó. Một SA chính là một sự thỏa thuận giữa hai đầu kết nối cùng cấp chẳng hạn như giao thức IPSec. Hai giao thức AH và ESP đều sử dụng SA, và nó là chức năng chính của giao thức trao đổi khóa IKE. Vì SA là liên kết đơn hình (có nghĩa là chúng chỉ liên kết theo một hướng duy nhất) cho nên các SA tách biệt được yêu cầu cho các lưu lượng gửi và nhận. Các gói SA được sử dụng để mô tả một tập hợp các SA mà được áp dụng cho các gói dữ liệu gốc được đưa ra bởi các host. Các SA được thỏa thuận giữa các kết nối cùng cấp thông qua giao thức quản lý khóa chẳng hạn như IKE. Khi thỏa thuận của một SA hoàn thành, cả hai mạng cùng cấp đó lưu các tham số SA trong cơ sở dữ liệu liên kết an toàn (SAD) của chúng. Một trong các tham số của SA là khoảng thời gian sống (life time) của nó. Khi khoảng thời gian tồn tại của một SA hết hạn, thì SA này sẽ được thay thế bởi một SA mới hoặc bị hủy bỏ. Khi một SA bị hủy bỏ, chỉ mục của nó sẽ được xóa bỏ khỏi SAD. Các SA được nhận dạng duy nhất bởi một bộ ba chứa chỉ số của tham

số liên kết an toàn SPI, một địa chỉ IP đích, và một giao thức cụ thể (AH hoặc ESP). SPI được sử dụng kết hợp với địa chỉ IP đích và số giao thức để tra cứu trong cơ sở dữ liệu để biết được thuật toán và các thông số liên quan.



Hình 3.19 Liên kết an toàn

Chính sách

Chính sách IPSec được duy trì trong SPD. Mỗi cổng vào của SPD định nghĩa lưu lượng được bảo vệ, cách để bảo vệ nó và sự bảo vệ được chia sẻ với ai. Với mỗi gói tin đi vào và rời khỏi hàng đợi IP, SPD phải được tra cứu.

Một cổng vào SPD phải định nghĩa một trong ba hoạt động:

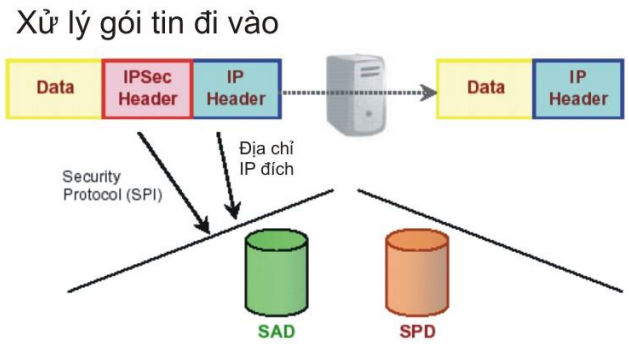
- Discard: không để gói tin này vào hoặc ra.
- Bypass: không áp dụng dịch vụ bảo mật cho gói tin đi ra và không đòi hỏi bảo mật trên gói tin đi vào.
- Protect: áo dụng dịch vụ bảo mật trên gói tin đi ra và yêu cầu gói tin đi vào có áp dụng dịch vụ bảo mật.

Lưu lượng IP được tạo ra thành chính sách IPSec bởi người chọn lựa. Người lựa chọn IPSec là: địa chỉ IP đích, địa chỉ IP nguồn, tên hệ thống, giao thức tầng trên, cổng nguồn và cổng đích và độ nhạy của dữ liệu.

SPD ghi vào định nghĩa hoạt động "bảo vệ" sẽ được chỉ rõ trên SA mà định danh trạng thái sử dụng để bảo vệ gói tin. Nếu một cổng vào SPD không được chỉ định rõ trong bất kỳ SA nào trong cơ sở dữ liệu SA (SAD), SA này sẽ phải được tạo trước khi bất kỳ lưu lượng nào có thể đi qua. Nếu luật được áp dụng tới lưu lượng đi vào và SA không tồn tại trong SAD, gói tin sẽ bị bỏ đi. Nếu nó được áp dụng cho lưu lượng đi ra, SA có thể được tạo khi sử dụng IKE.

Kiến trúc IPSec định nghĩa sự tương tác của SAD và SPD với chức năng xử lý IPSec như đóng gói và dỡ gói, mã hóa và giải mã, bảo vệ tính toàn vẹn và xác minh tính toàn vẹn. Nó cũng định nghĩa cách thực thi IPSec khác nhau có thể tồn tại.

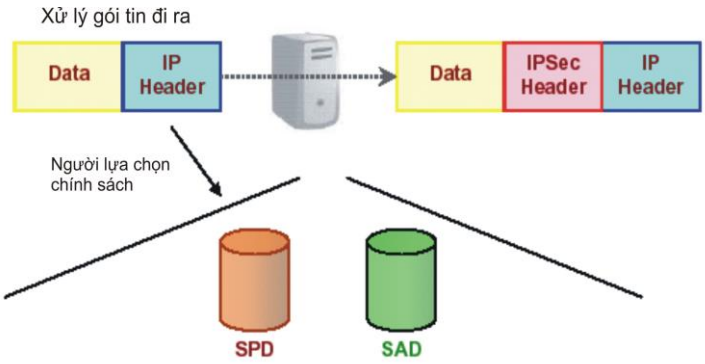
Khi nhận được gói tin vào máy tính thì đầu tiên máy tính đó tham khảo cơ sở dữ liệu về chính sách. Trong trường hợp cần xử lý thì xử lý header, tham khảo cơ sở dữ liệu, tìm đến SA tương ứng.



Hình 3.20. Chính sách IPSec: xử lý gói tin đầu vào

Khi gói tin ra từ một máy thì cũng phải tham khảo cơ sở dữ liệu chính sách. Có thể xảy ra 3 trường hợp:

- Cấm hoàn toàn, gói tin không được phép truyền qua.
- Được truyền qua nhưng không có mã hóa và xác thực.
- Có SA tương ứng



Hình 3.21. Chính sách IPSec: xử lý gói tin đầu ra.

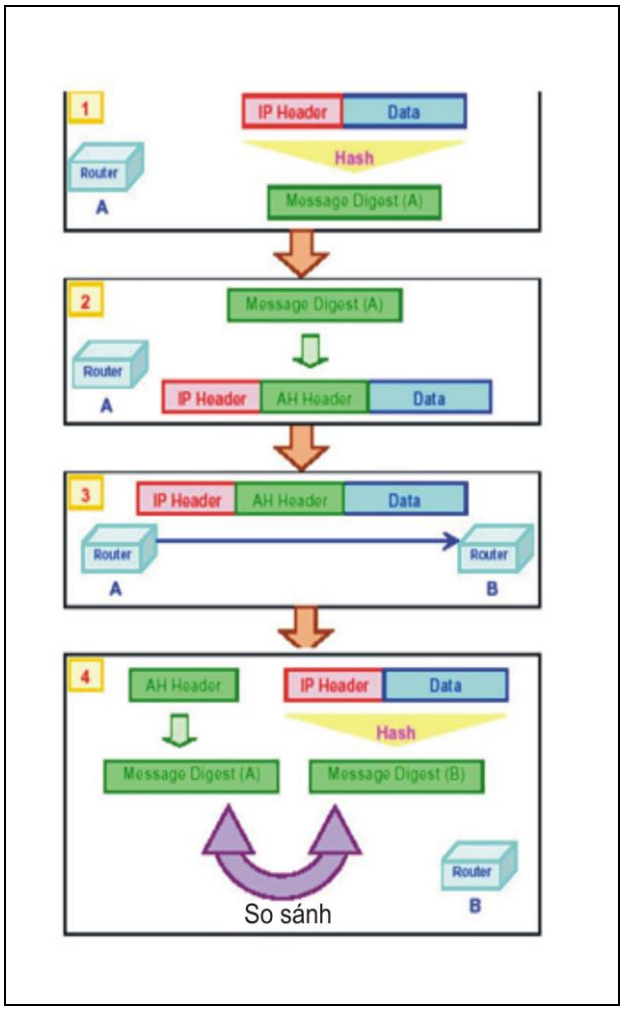
3.6.3 Giao thức xác thực tiêu đề AH

Authentication Header (AH) là một giao thức khóa trong kiến trúc IPSec. Nó cung cấp tính xác thực và tính toàn vẹn cho IP datagram.

Nó có thể hoàn thành việc này bằng cách áp dụng "*Hàm băm khóa một chiều*" cho datagram để tạo tin nhắn giản lược. Khi người nhận thực hiện giống chức năng băm một chiều trên datagram và thực hiện so sánh với giá trị của bản tin giản lược mà người gửi đã cung cấp, anh ấy sẽ phát hiện ra một phần của datagram bị thay đổi trong suốt quá trình quá độ nếu bất kỳ trường gốc nào bị thay đổi. Theo cách này, tính xác thực và toàn vẹn của tin nhắn có thể được đảm bảo khi sử dụng một mã bí mật giữa hai hệ thống bởi hàm băm một chiều.

AH cũng có thể ép buộc bảo vệ anti_replay (chống phát lại) bằng cách yêu cầu host nhận đặt bit replay trong header để chỉ ra rằng gói tin đã được nhìn thấy. Mặc dù không có bảo vệ này, kẻ tấn công có thể gửi lại gói tin tương tự nhiều hơn một lần.

Chức năng AH được áp dụng cho toàn bộ datagram trừ bất kỳ trường IP header nào thay đổi từ trạng thái này sang trạng thái khác. AH không cung cấp mã hóa và bởi vậy không cung cấp tính bảo mật và tính riêng tư.



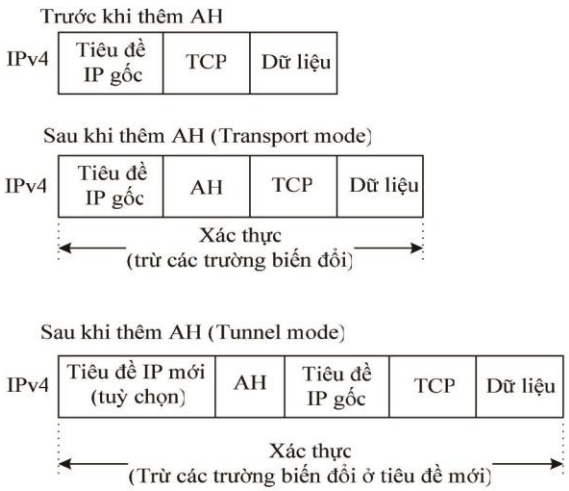
Hình 3.22. Xác thực tiêu đề.

Các bước hoạt động của AH:

Bước	Hoạt động
1	Toàn bộ gói tin IP (bao gồm header và data payload) được thực hiện qua một hàm băm một chiều.
2	Mã băm (tin nhắn giản lược) được sử dụng để xây dựng AH header mới, tiêu đề này được gắn thêm vào gói tin gốc.

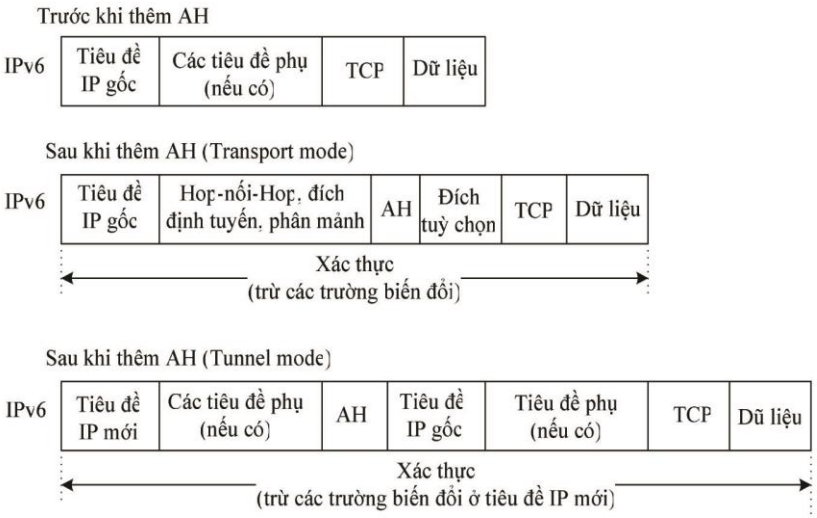
3	Gói tin mới được truyền tới IPSec router ở đích.
4	Router khác ở đích thực hiện băm IP header và data payload, kết quả thu được một mã băm. Sau đó, nó so sánh với mã băm được truyền từ AH header. Hai hàm băm phải giống nhau. Nếu chúng khác nhau, bên thu lập tức phát hiện tính không toàn vẹn của dữ liệu.

Việc xử lý AH phụ thuộc vào chế độ hoạt động của IPSec và phiên bản sử dụng của giao thức IP. Khuôn dạng của gói tin IPv4 trước và sau khi xử lý AH trong hai chế độ truyền tải và đường hầm được thể hiện trên hình:



Hình 3.23: Khuôn dạng gói tin IPv4 trước và sau khi xử lý AH

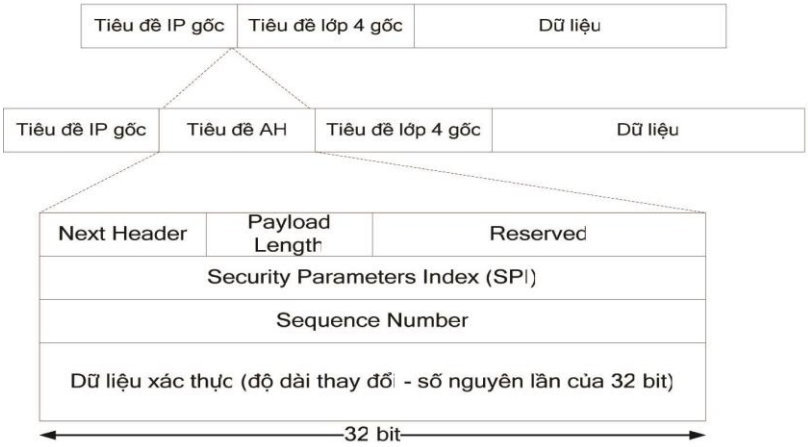
Khuôn dạng của gói tin IPv6 trước và sau khi xử lý AH được thể hiện trên hình:



Hình 3.24: Khuôn dạng gói tin IPv6 trước và sau khi xử lý AH

Cấu trúc gói tin AH

Các thiết bị sử dụng AH sẽ chèn một tiêu đề vào giữa lưu lượng cần quan tâm của gói IP, ở giữa phần tiêu đề IP và tiêu đề lớp 4. Bởi AH được liên kết với IPSec, IP-VPN có thể định dạng để chọn lưu lượng nào cần được bảo vệ và lưu lượng nào không cần phải sử dụng giải pháp an toàn giữa các bên. Ví dụ như có thể chọn để xử lý an toàn lưu lượng email nhưng không cần đối với các dịch vụ web. Quá trình xử lý chèn tiêu đề AH được minh họa trên hình 3.25



Hình 3.25: Cấu trúc tiêu đề AH cho gói IPSec.

Ý nghĩa của các trường trong tiêu đề AH như sau:

- *Next Header (tiêu đề tiếp theo).* Có độ dài 8 bit để nhận dạng loại dữ liệu của phần tải tin theo sau AH.

- *Payload Length (độ dài tải tin).* Có độ dài 8 bit và chứa độ dài của tiêu đề AH được biểu diễn trong các từ 32 bit, trừ đi 2. Ví dụ, trong trường hợp của thuật toán toàn vẹn mang lại một giá trị xác minh 96 bit (3 x 32 bit), cộng với 3 từ 32 bit cố định thì trường độ dài này có giá trị là 4. Với Ipv6, tổng độ dài của tiêu đề phải là bội của các khối 8 bit.

- *Reserved (dự trữ).* Trường 16 bit này dự trữ cho ứng dụng trong tương lai. Giá trị của trường này có thể đặt bằng 0 và có tham gia trong việc tính dữ liệu xác thực.

- *Security Parameters Index (SPI-chỉ số thông số an ninh).* Trường này có độ dài 32 bit, cùng với địa chỉ IP đích và giao thức an ninh ESP cho phép nhận dạng duy nhất SA cho gói dữ liệu. Các giá trị SPI từ 1 đến 255 được dành riêng để sử dụng trong tương lai. SPI là trường bắt buộc và thường được lựa chọn bởi phía thu khi thiết lập SA. Giá trị SPI bằng 0 được sử dụng cục bộ và có thể dùng để chỉ ra rằng chưa có SA nào tồn tại.

- *Sequence Number (số thứ tự).* Đây là trường 32 bit không dấu chứa một giá trị mà khi mỗi gói được gửi đi thì tăng một đơn vị. Trường này là bắt buộc và luôn được đưa vào bởi bên gửi ngay cả khi bên nhận không sử dụng dịch vụ chống phát lại. Bộ đếm bên gửi và bên nhận được khởi tạo ban đầu là 0, gói đầu tiên có số thứ tự là 1. Nếu dịch vụ chống phát lại được sử dụng thì chỉ số này không thể lặp lại.

Khi đó, để tránh trường hợp bộ đếm bị tràn và lặp lại các số thứ tự, sẽ có yêu cầu kết thúc phiên truyền thông và một SA mới được thiết lập trước khi truyền gói thứ 2 của SA hiện hành.

- *Authentication Data (dữ liệu xác thực).* Còn được gọi là giá trị kiểm tra tính toàn vẹn ICV (Integrity Check Value), có độ dài thay đổi và bằng số nguyên lần của 32 bit đối với IPv4 hay 64 bit đối với IPv6. Nó có thể chứa đệm để lấp đầy cho đủ là bội số của các khối bit như trên. ICV được tính toán sử dụng thuật toán xác thực, bao gồm mã xác thực bản tin (MAC-Message Authentication Code). MAC đơn giản có thể là thuật toán mã hóa MD5 hoặc SHA-1. Các khóa dùng cho mã hóa AH là khóa xác thực bí mật được chia sẻ giữa các đối tượng tryền thông, có thể là một số ngẫu nhiên, không thể đoán trước được. Tính toán ICV được thực hiện đối với gói tin mới đưa vào. Bất kì trường nào có thể biến đổi của tiêu đề IP đều được cài đặt bằng 0, dữ liệu lớp trên được giả sử là không biến đổi. Mỗi bên đầu cuối VPN sẽ tính toán giá trị ICV này một cách độc lập. Nếu ICV tính toán được ở phía thu và ICV do phía phát truyền đến so sánh với nhau mà không phù hợp thì gói tin bị loại bỏ. Bằng cách như vậy sẽ bảo đảm rằng gói tin không bị giả mạo.

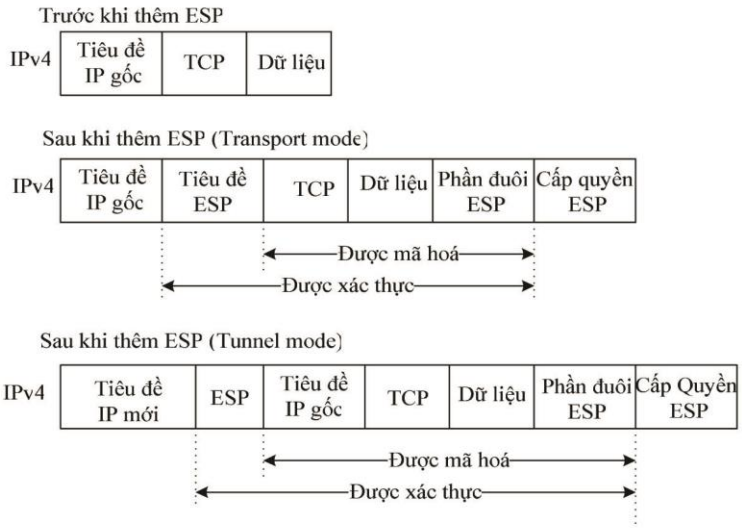
3.6.4. Giao thức đóng gói tải tin an toàn ESP.

Encapsulation Security Payload (ESP) là một giao thức khóa trong IPSec, nó cung cấp *tính toàn vẹn* và *bảo mật (mã hóa)* cho IP datagram. ESP cũng có thể được sử dụng để mã hóa toàn bộ IP datagram hoặc phân đoạn tầng vận chuyển (ví dụ TCP, UDP, ICMP, IGMP). Có hai chế độ mà ESP có thể thực hiện: chế độ tunnel và chế độ transport.

Trong *chế độ tunnel ESP*, IP datagram gốc được đưa vào phần mã hóa của ESP và toàn bộ khung ESP được đặt vào trong một datagram có tiêu đề IP chưa mã hóa. Phần chưa mã hóa của datagram cuối cùng có chứa thông tin định tuyến cho đường hầm IP. Chế độ tunnel là cơ bản nhất được sử dụng giữa hai gateway hoặc từ trạm cuối tới một gateway.

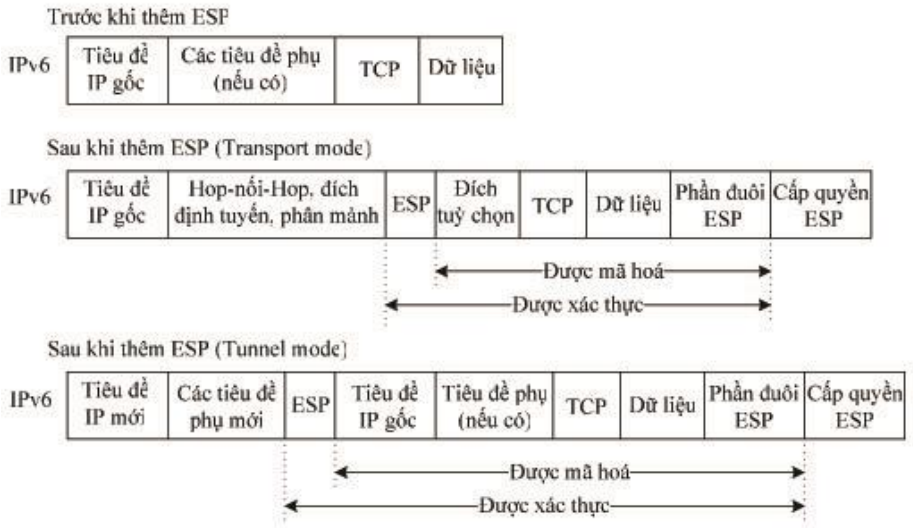
Chế độ transport ESP mã hóa giao thức tầng vận chuyển và chèn vào một tiêu đề ESP ngay trước tiêu đề giao thức mã hóa. IP datagram mới không được phát sinh và chế độ này giữ gìn băng thông. Chế độ transport được sử dụng giữa hai trạm cuối hoặc giữa trạm cuối và một cổng an ninh nếu cổng an ninh được coi như một host (ví dụ như telnet từ một máy tính tới một cổng an ninh).

Việc xử lý ESP phụ thuộc vào chế độ hoạt động của IPSec và phiên bản sử dụng của giao thức IP. Khuôn dạng của gói tin IPv4 trước và sau khi xử lý ESP trong hai chế độ truyền tải và đường hầm được thể hiện ở hình 3.17.



Hình 3.26: Khuôn dạng gói tin IPv4 trước và sau khi xử lý ESP

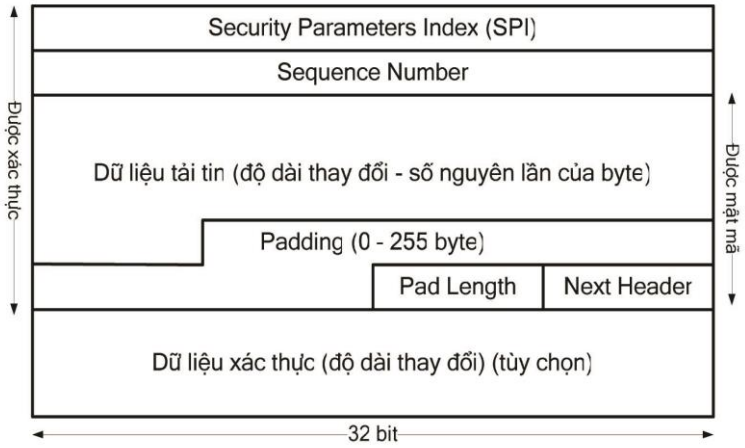
Khuôn dạng của gói tin IPv6 trước và sau khi xử lý ESP được thể hiện trên hình 3.27



Hình 3.27: Khuôn dạng gói tin IPv6 trước và sau khi xử lý ESP

Cấu trúc gói tin ESP

Cấu trúc gói tin ESP được thể hiện trên hình 3.19. Các trường trong gói tin ESP có thể là bắt buộc hay tùy chọn. Những trường bắt buộc luôn có mặt trong tất cả các gói ESP. Việc lựa chọn một trường tùy chọn được định nghĩa trong quá trình thiết lập liên kết an ninh. Như vậy, khuôn dạng ESP đối với một SA là cố định trong khoảng thời gian tồn tại của SA đó.



Hình 3.28: Khuôn dạng gói ESP.

Sau đây là ý nghĩa của các trường trong cấu trúc gói tin ESP.

- *SPI (chỉ số thông số an ninh).* Là một số bất kỳ 32 bit, cùng với địa chỉ IP đích và giao thức an ninh ESP cho phép nhận dạng duy nhất SA cho gói dữ liệu. Các giá trị SPI từ 0 đến 255 được dành riêng để sử dụng trong tương lai. SPI là trường bắt buộc và thường được lựa chọn bởi phía thu khi thiết lập SA.
- *Sequence Number (số thứ tự).* Tương tự như trường số thứ tự của AH.
- *Payload Data (dữ liệu tải tin).* Đây là trương bắt buộc, bao gồm một số lượng biến đổi các byte dữ liệu gố hoặc một phần dữ liệu yêu cầu bảo mật đã được mô tả trong trường Next Header. Trường này được mã hóa cùng với thuật toán mã hóa đã lựa chọn trong suốt quá trình thiết lập SA. Nếu thuật toán yêu cầu các vectơ khởi tạo thì nó cũng được bao gồm ở đây. Thuật toán thường được dùng để mã hóa ESP là DES-CBC. Đôi khi các thuật toán khác cũng được hỗ trợ như 3DES hay CDMF.
- *Padding (đệm).* Có nhiều nguyên nhân dẫn đến sự có mặt của trường đệm như:

✓ Nếu thuật toán mật mã sử dụng yêu cầu bản rõ (Clear-text) phải là số nguyên lần các khối byte (ví dụ trường mã khối) thì trường đệm được sử dụng để điền đầy vào phần bản rõ này (bao gồm Payload Data, Pad Length, Next Header và Padding) sao cho đạt tới kích thước theo yêu cầu.

✓ Trường đệm cũng cần thiết để đảm bảo phần dữ liệu mật mã (Cipher-text) sẽ kết thúc ở biên giới số nguyên lần của 4 byte nhằm phân biệt rỗ ràng với trường dữ liệu xác thực (Authentication Data).

✓ Ngoài ra, trường đệm còn có thể sử dụng để che dấu độ dài thực của tải tin, tuy nhiên mục đích này cần phải được cân nhắc vì nó ảnh hưởng tới băng thông truyền dẫn.

- *Pad length (độ dài đệm)*. Trường này xác định số byte đệm được thêm vào. Pad length là trường bắt buộc với các giá trị phù hợp nằm trong khoảng từ 0 đến 255 byte.

- *Next Header (tiêu đề tiếp theo)*. Next Header là trường bắt buộc và có độ dài 8 bit. Nó xác định kiểu dữ liệu chứa trong phần tải tin, ví dụ một tiêu đề mở rộng (Extension Header) trong Ipv6 hoặc nhận dạng của một giao thức lớp trên khác. Giá trị của trường này được lựa chọn từ tập các giá trị IP Protocol Nember định nghĩa bởi IANA.

- *Authentication Data (dữ liệu xác thực)* . Trường này có độ dài biến đổi, chứa một giá trị kiểm tra tính toàn vẹn ICV tính trên dữ liệu của toàn bộ gói ESP trừ trường Authentication Data. Độ dài của trường này phụ thuộc vào thuật toán xác thực được sử dụng. Trường này là tùy chọn và chỉ được thêm vào nếu dịch vụ xác thực được lựa chọn cho SA đang xét. Thuật toán xác thực phải chỉ ra độ dài ICV, các bước xử lý cũng như các luật so sánh cần thực hiện để kiểm tra tính toàn vẹn của gói tin.

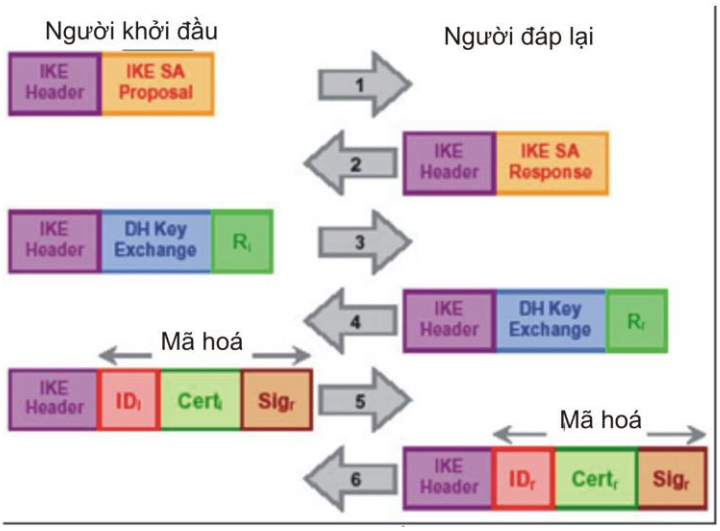
3.6.5. Giao thức trao đổi khóa

Tất cả giao thức trao đổi khóa IPSec đều dựa trên Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP tạo và quản lý liên kết an toàn. Qúa trình này đầu tiên yêu cầu hệ thống IPSec tự xác thực với nhau và thiết lập ISAKMP khóa chia sẻ.

Oakley Key Exchange Protocol sử dụng thuật toán trao đổi khóa Diffie_Hellman để thuận tiện trao đổi mã hóa bí mật.

Internet Key Exchange (IKE) là sự kết hợp của ISAKMP và giao thức trao đổi khóa Oakley.

IKE sử dụng hai "pha" của thương lượng. *Pha một* bắt đầu xác thực liên kết an toàn giữa hai server ISAKMP, được gọi là Liên kết an toàn IKE. Trong pha một có hai chế độ hoạt động: Main Mode (chế độ chính) và Aggressive Mode (chế độ linh hoạt). Điều này bảo đảm tính hợp pháp và riêng tư của việc thương lượng liên kết an toàn. Mỗi khi liên kết được thiết lập giữa các server ISAKMP, cộng thêm liên kết an toàn được tạo và phân bổ theo cách nào đó. Sự thỏa thuận khóa Diffie-Hellman luôn được sử dụng trong pha này.



Hình 3.29 IKE pha 1- Main Mode.

IKE Main Mode bao gồm 6 tin nhắn được trao đổi giữa người khởi đầu và người nhận cốt để thiết lập một liên kết an toàn IKE. Giao thức IKE sử dụng UDP cổng 500.

1. Người khởi đầu gửi lời đề nghị IKE SA lập danh sách tất cả phương pháp hỗ trợ xác thực, nhóm Diffie-Hellman, lựa chọn mã hóa, và thuật toán băm, và muốn trong suốt thời gian SA tồn tại.

2. Người nhận trả lời với câu trả lời IKE SA chỉ ra phương pháp xác thực ưu tiên hơn, nhóm Diffie-Hellman, mã hóa và thuật toán băm, chấp nhận thời gian SA tồn tại.

Nếu hai bên có thể thương lượng thành công tập hợp các phương pháp cơ bản, giao thức được tiếp tục bằng cách thiết lập kênh truyền thông được mã hóa khi sử dụng thuật toán trao đổi khóa Diffie-Hellman.

3. Người khởi đầu gửi phần mã bí mật Diffie-Hellman của anh ấy cộng thêm một giá trị ngẫu nhiên.

4. Người đáp lại làm tương tự bằng việc gửi phần mã bí mật Diffie-Hellman của anh ấy cộng với một giá trị ngẫu nhiên.

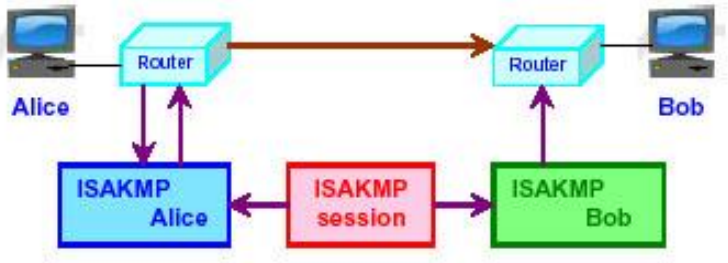
Trao đổi khóa Diffie-Hellman có thể được hoàn thành ngay bởi cả hai bên đang định hình bí mật chia sẻ cơ bản. Bí mật chia sẻ này thường phát sinh ra khóa phiên đối xứng với cái mà những tin nhắn còn lại của giao thức IKE sẽ được mã hóa.

5. Tiếp theo Người khởi đầu gửi định danh của anh ấy một cách tùy ý là một chứng chỉ liên kết định danh tới một khóa công khai. Có được điều này là bởi một hàm băm qua tất cả trường tin nhắn ra dấu bởi bí mật được chia sẻ trước hoặc khóa RSA riêng.

6. Giống như bước 5, nhưng được gửi bởi người nhận.

Nếu định danh của hai bên được xác thực thành công thì IKE SA sẽ được thiết lập.

Trong pha hai, IKE thương lượng liên kết an toàn IPSec và phát sinh nguyên liệu khóa được yêu cầu cho IPSec. Trong pha hai có hai chế độ hoạt động: Quick Mode và New Group Mode. Người gửi đưa ra một hoặc nhiều tập hợp biến đổi được sử dụng để chỉ rõ sự kết hợp cho phép của biến đổi với cài đặt tương ứng của chúng. Người gửi cũng chỉ ra luồng dữ liệu mà tập hợp biến đổi được áp dụng. Sau đó, người nhận gửi lại tập hợp từng biến đổi, chỉ ra sự đồng ý biến đổi lẫn nhau và thuật toán cho việc tham gia phiên IPSec này. Sự đồng ý Diffie-Hellman mới có thể hoàn thành trong pha hai hoặc khóa có thể được lấy từ bí mật chia sẻ của pha một.



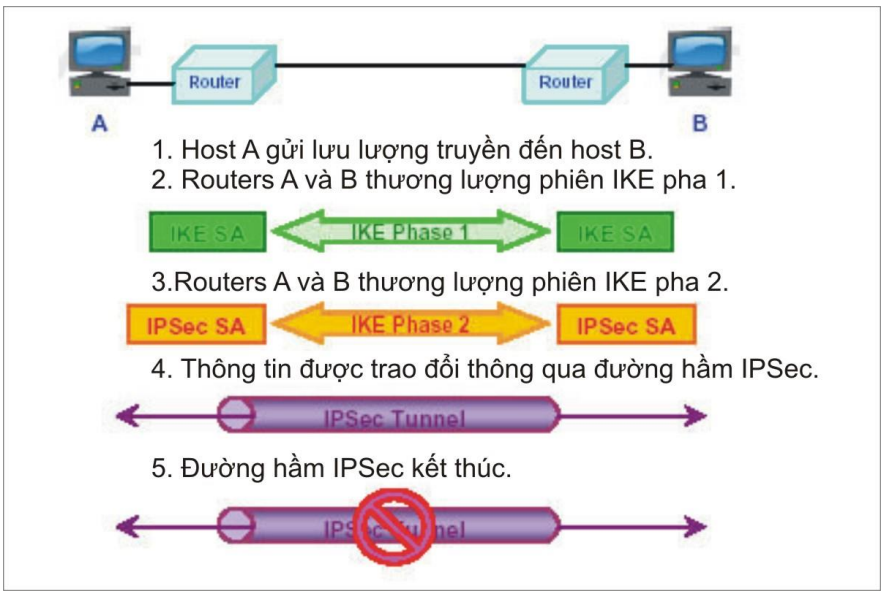
Hình 3.30 Internet Key Exchange

Như hình 3.21, ta thấy quá trình trao đổi dữ liệu giữa Bob và Alice diễn ra như sau:

1. Gói tin được truyền từ Alice đến Bob, lúc này chưa có SA nào.
2. IKE của Alice bắt đầu thương lượng với IKE của Bob.
3. Thương lượng hoàn thành. Alice và Bob bây giờ đã có IKE SA và IPSec SA.
4. Gói tin được gửi từ Alice tới Bob và được bảo vệ bởi IPSec SA.

Quá trình hoạt động của IPSec

IPSec đòi hỏi nhiều thành phần công nghệ và phương pháp mã hóa. Hoạt động của IPSec có thể được chia thành 5 bước chính:



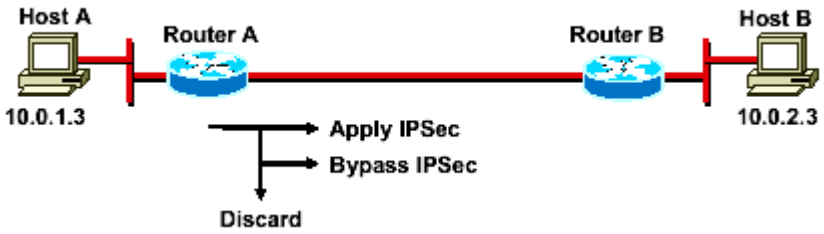
Hình 3.31 Các bước hoạt động của IPSec

Hình 3.31. Sơ đồ kết nối hai Router chạy IPSec

Mục đích chính của IPSec là để bảo vệ luồng dữ liệu mong muốn với các dịch vụ bảo mật cần thiết. Quá trình hoạt động của IPSec được chia thành năm bước:

- Xác định luồng traffic cần quan tâm: Luồng traffic được xem là cần quan tâm khi đó các thiết bị VPN công nhận rằng luồng traffic bạn muốn gửi cần bảo vệ.
- Bước 1 IKE: Giữa các đối tượng ngang hàng (peer), một tập các dịch vụ bảo mật được thoả thuận và công nhận. Tập dịch vụ bảo mật này bảo vệ tất cả các quá trình trao đổi thông tin tiếp theo giữa các peer.
- Bước 2 IKE:IKE thoả thuận các tham số SA IPSec và thiết lập "matching" các SA IPSec trong các peer. Các tham số bảo mật này được sử dụng để bảo vệ dữ liệu và các bản tin được trao đổi giữa các điểm đầu cuối. Kết quả cuối cùng của hai bước IKE là một kênh thông tin bảo mật được tạo ra giữa các peer.
- Truyền dữ liệu: Dữ liệu được truyền giữa các peer IPSec trên cơ sở các thông số bảo mật và các khoá được lưu trữ trong SA database.
- Kết thúc đường hầm "Tunnel": Kết thúc các SA IPSec qua việc xoá hay timing out.

Bước 1: xác định luồng traffic cần quan tâm

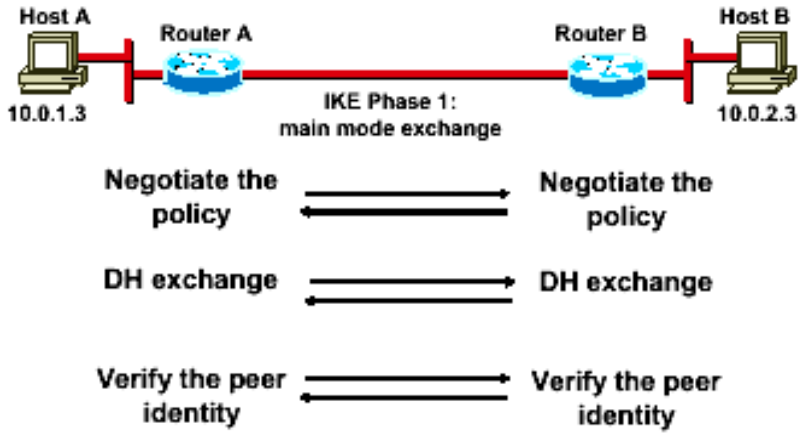


Hình 2.32 Xác định luồng traffic

Việc xác định luồng dữ liệu nào cần được bảo vệ được thực hiện như là một phần trong việc tính toán một chính sách bảo mật cho việc sử dụng của một VPN. Chính sách được sử dụng để xác định luồng traffic nào cần bảo vệ và luồng traffic nào có thể gửi ở dạng "clear text". Đối với mọi gói dữ liệu đầu vào và đầu ra, sẽ có ba lựa chọn: Dùng IPSec, cho qua IPSec, hoặc huỷ gói dữ liệu. Đối với mọi gói dữ liệu được bảo vệ bởi IPSec, người quản trị hệ thống cần chỉ rõ các dịch vụ bảo mật được sử dụng cho gói dữ liệu. Các cơ sở dữ liệu chính sách bảo mật chỉ rõ các giao thức IPSec, các mode, và các thuật toán được sử dụng cho luồng traffic. Các dịch vụ này sau đó được sử dụng cho luồng traffic dành cho mỗi Peer IPSec cụ thể. Với VPN Client, bạn sử dụng các cửa sổ thực đơn để chọn các kết nối mà bạn muốn bảo

mật bởi IPSec. Khi các luồng dữ liệu mong muốn truyền tới IPSec Client, client khởi tạo sang bước tiếp theo trong quá trình: Thoả thuận một sự trao đổi bước 1 IKE.

Bước 2: Bước 1 IKE

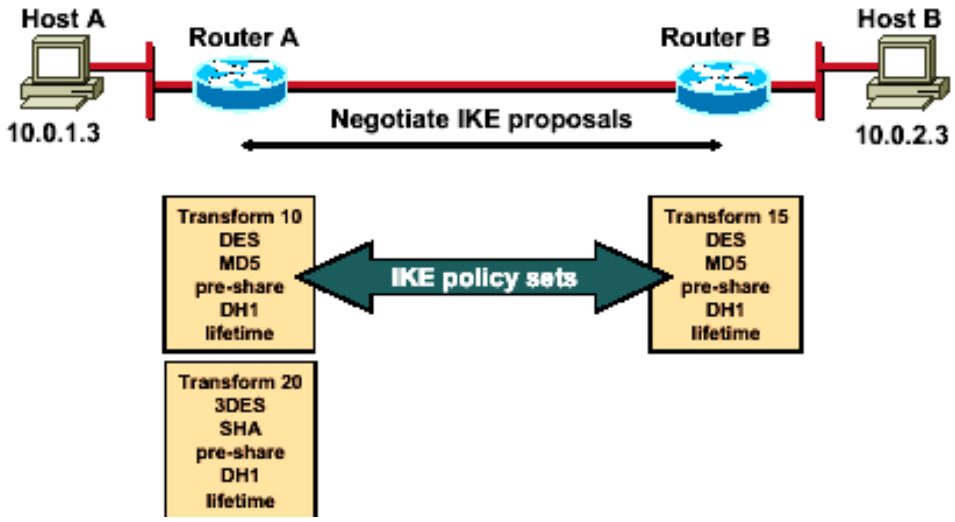


Hình 3.33. Bước một IKE

Mục đích cơ bản của bước 1 IKE là để thoả thuận các tập chính sách IKE, xác thực các đối tượng ngang hàng, và thiết lập một kênh bảo mật giữa các đối tượng ngang hàng. Bước 1 IKE xuất hiện trong hai mode: Main mode và Aggressive mode.

Main mode có ba quá trình chao đổi hai chiều giữa nơi khởi tạo và nơi nhận:

Quá trình trao đổi đầu tiên:



Hình 3.34. Quá trình trao đổi đầu tiên

Trong xuốt quá trình trao đổi đầu tiên các thuật toán và các hash được sử dụng để bảo mật sự trao đổi thông tin IKE đã được thoả thuận và đã được đồng ý giữa các đối tượng ngang hàng. Trong khi cố gắng tạo ra một kết nối bảo mật giữa máy A và máy B qua Internet, các kế hoạch bảo mật IKE được trao đổi giữa Router A và B. Các kế hoạch bảo vệ định nghĩa giao thức IPSec hiện tại đã được thoả thuận (ví dụ

ESP). Dưới mỗi kế hoạch, người khởi tạo cần phác hoạ những thuật toán nào được sử dụng trong chính sách (ví dụ DES với MD5). Ở đây không phải là thoả thuận mỗi thuật toán một cách riêng biệt, mà là các thuật toán được nhóm trong các tập, một tập chính sách IKE. Một tập chính sách mô tả thuật toán mã hoá nào, thuật toán xác thực nào, mode, và chiều dài khoá. Những kế hoạch IKE và những tập chính sách này được trao đổi trong suốt quá trình trao đổi đầu tiên trong chế độ main mode. Nếu một tập chính sách match được tìm thấy giữa hai đối tượng ngang hàng, main mode tiếp tục. Nếu không một tập chính sách match nào được tìm thấy, tunnel là torn down.

Trong ví dụ ở trong hình trên, RouterA gửi các tập chính sách IKE 10 và 20 tới RouterB. RouterB so sánh tập chính sách của nó, tập chính sách 15, với những tập chính sách nhận được từ RouterA. Trong trường hợp này, có một cái match: Đó là tập chính sách 10 của Router A match với tập chính sách 15 của Router B.

Quá trình trao đổi thứ hai

Sử dụng một sự trao đổi DH để tạo ra các khoá mật mã chia sẻ và qua quá trình này các số ngẫu nhiên gửi tới các đối tác khác, signed, và lấy lại xác thực định nghĩa của chúng. Khoá mật mã chia sẻ được sử dụng để tạo ra tất cả các khoá xác thực và mã hoá khác. Khi bước này hoàn thành, các đối tượng ngang hàng có cùng một mật mã chia sẻ nhưng các đối tượng ngang hàng không được xác thực. Quá trình này diễn ra ở bước thứ 3 của bước 1 IKE, quá trình xác thực đặc tính của đối tượng ngang hàng.

Quá trình thứ ba – xác thực đặc tính đối tượng ngang hàng:

Hình 3.35 Quá trình trao đổi thứ ba

Các phương thức xác thực đối tượng ngang hàng:

- Pre-shared keys
- RSA signatures
- RSA encrypted nonces

Bước thứ ba và cũng là bước trao đổi cuối cùng được sử dụng để xác thực các đối tượng ngang hàng ở xa. Kết quả chính của main mode là một tuyến đường trao

đổi thông tin bảo mật cho các quá trình trao đổi tiếp theo giữa các đối tượng ngang hàng được tạo ra. Có ba phương thức xác thực nguồn gốc dữ liệu:

- Các khoá pre-shared: Một giá trị khoá mật mã được nhập vào bằng tay của mỗi đối tượng ngang hàng được sử dụng đê xác thực đối tượng ngang hàng.
- Các chữ ký RSA: Sử dụng việc trao đổi các chứng nhận số để xác thực các đối tượng ngang hàng.
- RSA encryption nonces: Nonces (một số ngẫu nhiên được tạo ra bởi mỗi đối tượng ngang hàng) được mã hoá và sau đó được trao đổi giữa các đối tượng ngang hàng. Hai nonce được sử dụng trong suốt quá trình xác thực đối tượng ngang hàng.

Trong aggressive mode, các trao đổi là ít hơn với ít gói dữ liệu hơn. Mọi thứ đều được trao đổi trong quá trình trao đổi đầu tiên: Sự thoả thuận tập chính sách IKE, sự tạo ra khoá chung DH, một nonce. Trong aggressive mode nhanh hơn main mode.

Bước 3 – Bước 2 IKE

Hình 3.36. Bước 2 IKE

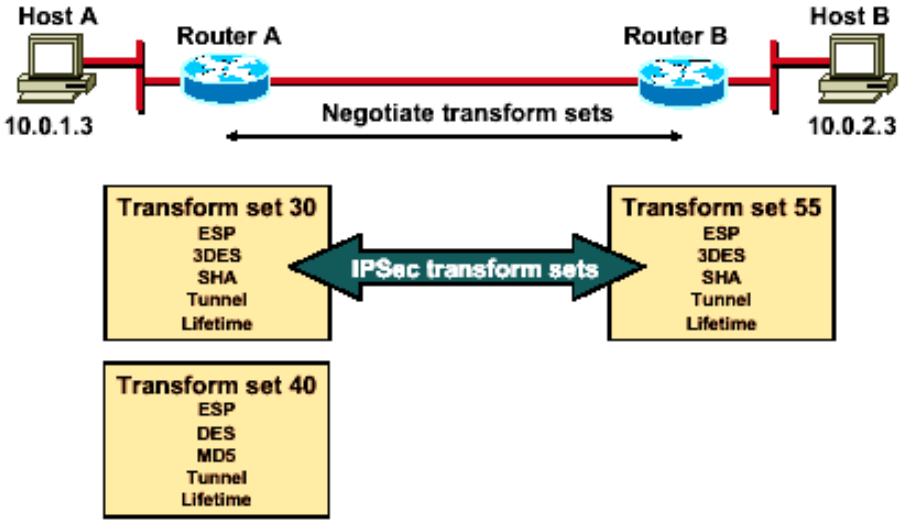
Mục đích của bước 2 IKE là để thoả thuận các thông số bảo mật IPSec được sử dụng để bảo mật đường hầm IPSec. Bước 2 IKE thực hiện các chức năng dưới đây:

- Thoả thuận các thông số bảo mật, các tập transform IPSec.
- Thiết lập các SA IPSec.
- Thoả thuận lại theo chu kỳ các SA IPSec để chắc chắn bảo mật.
- Có thể thực hiện thêm một sự trao đổi DH.

Trong bước 2 IKE chỉ có một mode, gọi là Quick mode. Quick mode xuất hiện sau khi IKE đã được thiết lập đường hầm bảo mật trong bước 1 IKE. Nó thoả thuận một transform IPSec chia sẻ, và thiết lập các SA IPSec. Quick mode trao đổi các nonce mà được sử dụng để tạo ra khoá mật mã chia sẻ mới và ngăn cản các tấn công "replay" từ việc tạo ra các SA không có thật.

Quick mode cũng được sử dụng để thoả thuận lại một SA IPSec mới khi thời gian sống của SA IPSec đã hết. Quick mode được sử dụng để nạp lại "keying material" được sử dụng để tạo ra khóa mậtmã chia sẻ trên cơ sở "keying material" lấy từ trao đổi DH trong bước 1.

Các tập Transform IPSec

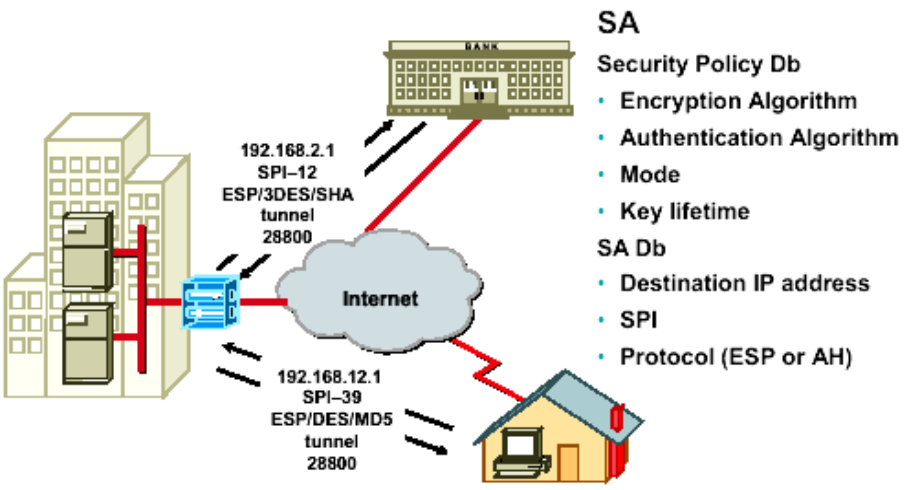


Hình 3.37. Thỏa thuận tập transform

Kết quả cuối cùng của bước 2 IKE là thiết lập một phiên IPSec bảo mật giữa các điểm đầu cuối. Trước khi điều này có thể xảy ra, mỗi cặp của các điểm đầu cuối thoả thuận mức bảo mật yêu cầu (ví dụ, các thuật toán xác thực và mã hoá cho một phiên). Không những là thoả thuận những giao thức riêng biệt, các giao thức được nhóm vào trong các tập, một tập transform IPSec. Các tập transform IPSec được trao đổi giữa các peer trong xuốt quá trình "quick mode". Nếu một "match"được tìm thấy giữa các tập, phiên thiết lập IPSec sẽ tiếp tục. Nếu ngược lại thì phiên sẽ bị huỷ bỏ.

Trong ví dụ trong hình trên, RouterA gửi các tập transform IPSec 30 và 40 đến RouterB. RouterB so sánh tập transform của nó với những cái đã nhận được từ RouterA. Trong ví dụ này, có một cái "match". Tập transform 30 của RouterA match với tập transform 55 của RouterB. Các thuật toán mã hoá và xác thực có dạng một SA.

SA (Security Association)



Hình 3.38. Các thông số của SA

Khi mà các dịch vụ bảo mật được đồng ý giữa các peer, mỗi thiết bị ngang hàng VPN đưa thông tin vào trong một SPD (Security Policy Database). Thông tin này bao gồm thuật toán xác thực, mã hoá, địa chỉ IP đích, mode truyền dẫn, thời gian sống của khoá .v.v. Những thông tin này được coi như là một SA. Một SA là một kết nối logic một chiều mà cung cấp sự bảo mật cho tất cả traffic đi qua kết nối. Bởi vì hầu hết traffic là hai chiều, do vậy phải cần hai SA: một cho đầu vào và một cho đầu ra. Thiết bị VPN gán cho SA một số thứ tự, gọi là SPI (Security Parameter Index). Khi gửi các thông số riêng biệt của SA của qua đường hầm, Gateway, hoặc Host chèn SPI vào trong tiêu đề ESP. Khi mà đối tượng ngang hàng IPSec nhận được gói dữ liệu, nó nhìn vào địa chỉ IP đích, giao thức IPSec, và SPI trong SAD (Security Association Database) của nó, và sau đó xử lý gói dư liệu theo các thuật toán được chỉ ra trong SPD.

IPSec SA là một sự tổ hợp của SAD và SPD. SAD được sử dụng để định nghĩa địa chỉ IP đích SA, giao thức IPSec, và số SPI. SPD định nghĩa các dịch vụ bảo mật được sử dụng cho SA, các thuật toán mã hoá và xác thực, mode, và thời gian sống của khoá. Ví dụ, trong kết nối từ tổng công ty đến nhà băng, chính sách bảo mật cung cấp một vài đường hầm bảo mật sử dụng 3DES, SHA, mode tunnel, và thời gian sống của khoá là 28800. Giá trị SAD là 192.168.2.1, ESD, và SPI là 12.

Bước 4 – phiên IPSec

Hình 3.39 Một phiên IPSec

Sau khi bước 2 IKE hoàn thành và quick mode được thiết lập, traffic sẽ được trao đổi giữa máy A và máy B qua một đường hầm bảo mật. Traffic mong muốn được mã hoá và giải mã theo các dịch vụ bảo mật được chỉ ra trong SA IPSec.

Bước 5 – Kết thúc đường hầm

Hình 3.40. Kết thúc một phiên IPSec

Các SA IPSec kết thúc thông qua việc xoá hay bằng timing out. Một SA có thể time out khi lượng thời gian đã được chỉ ra là hết hoặc khi số byte được chỉ ra đã qua hết đường hầm. Khi các SA kết thúc, các khoá cũng bị huỷ. Khi các SA IPSec tiếp theo cần cho một luồng, IKE thực hiện một bước 2 mới, và nếu cần thiết, một sự thoả thuận mới trong bước 1 IKE. Một sự thoả thuận thành công sẽ tạo ra các SA và các khoá mới. Các SA mới thường được thiết lập trước khi các SA đang tồn tại hết giá trị.

Năm bước được tổng kết của IPSec

Bước	Hoạt động	Miêu tả
1	Lưu lượng truyền bắt đầu quá trình IPSec	**Lưu lượng được cho rằng đang truyền khi chính sách bảo mật IPSec đã cấu hình trong các bên IPSec bắt đầu quá trình IKE.**
2	IKE pha một	**IKE xác thực các bên IPSec và thương lượng các IKE SA trong suốt pha này, thiết lập kênh an toàn cho việc thương lượng các IPSec SA trong pha hai.**
3	IKE pha hai	**IKE thương lượng tham số IPSec SA và cài đặt IPSec SA trong các bên.**
4	Truyền dữ liệu	**Dữ liệu được truyền giữa các bên IPSec dựa trên tham số IPSec và những khóa được lưu trong CSDL của SA.**

5	**Kết thúc đường hầm IPSec**	**IPSec SA kết thúc qua việc xóa hoặc hết thời gian thực hiện.**

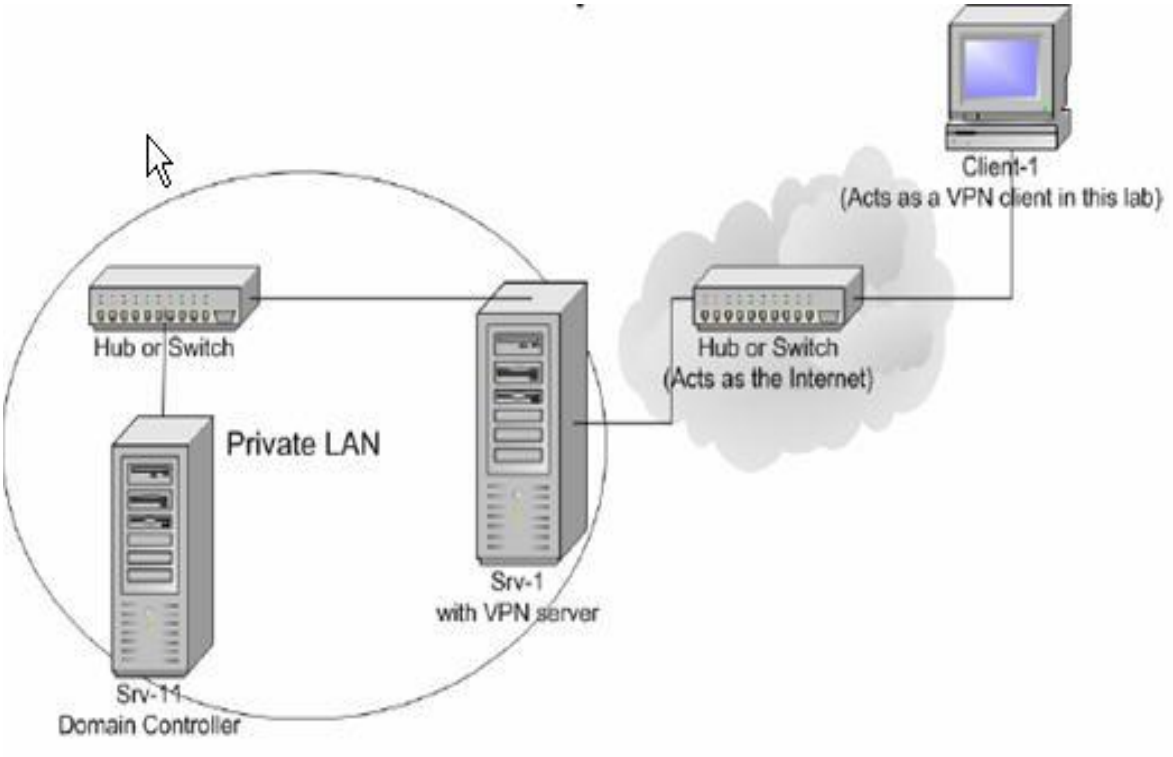
3.6.6 Những hạn chế của IPSec

Mặc dù IPSec đã sẵn sàng đưa ra các đặc tính cần thiết để đảm bảo thiết lập kết nối VPN an toàn thông qua mạng Internet, nó vẫn còn ở trong giai đoạn phát triển để hướng tới hoàn thiện. Sau đây là một số vấn đề đặt ra mà IPSec cần phải giải quyết để hỗ trợ tốt hơn cho việc thực hiện VPN:

- 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 dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IKE vẫn là công nghệ chưa thực sự khẳng định được khả năng của mình. Phương thức chuyển khóa thủ công lại không thích hợp cho mạng có số lượng lớn các đối tượng di động.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật 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 một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phầm mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

CHƯƠNG IV: THIẾT LẬP VPN

Thiết lập mô hình Client to site(Host to Network)



Hình 4.1: Mô hình Client to Site

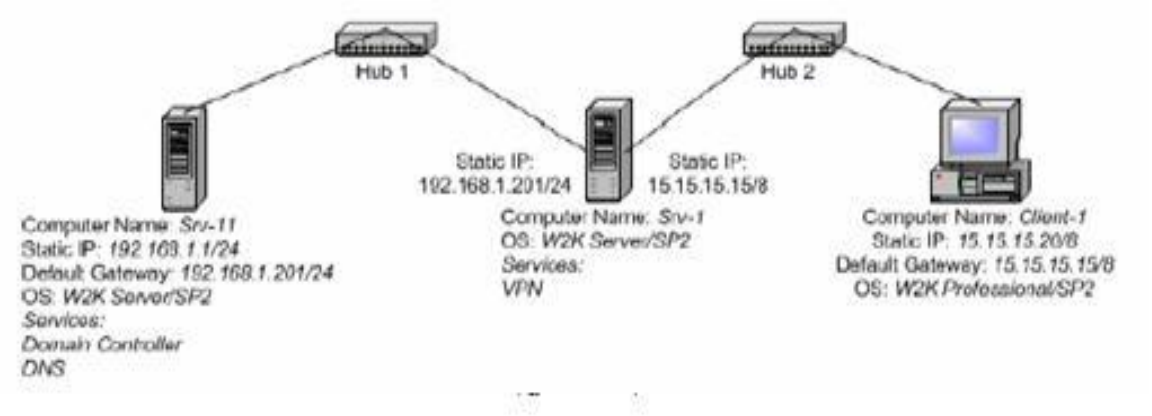
Thiết lập mô hình Client to Site như trên cho công ty Cổ phần truyền thông và máy tính Thánh Gióng

Công ty Cổ phần truyền thông và máy tính Thánh Gióng có 1 đường truyền ADSL để kết nối với internet thông qua vpn server tên là **srv-1**có 2 card mạng là:

- Public nic:15.15.15.15/8

- Private nic: 192.168.1.201/24

Để có thể quản lý tài khoản người dùng 1 cách tập trung công ty Cổ phần truyền thông và máy tính Thánh Gióng xây dựng 1 hệ thống Active Directory trên domain controler tên **srv-11** có địa chỉ IP là 192.168.1.1/24, domain name là **cvntlip.com.**



Hình 4.2: Mô hình triển khai

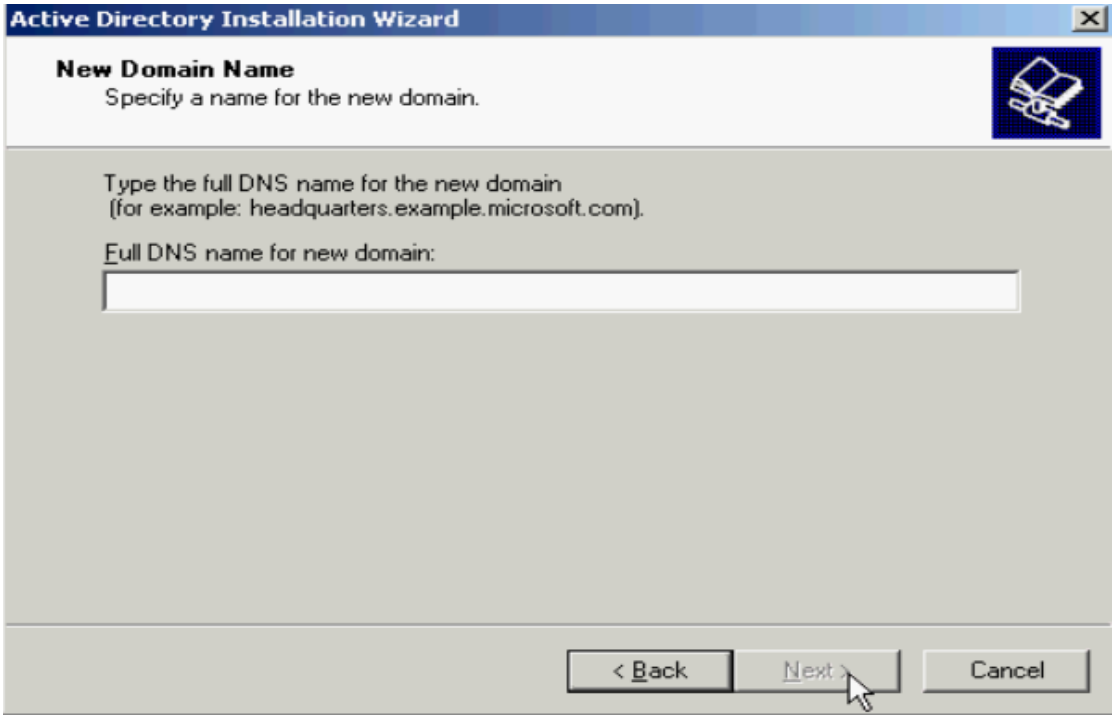
Chúng ta hãy xây dựng hệ thống **cvntlip.com** sao cho các nhân viên kinh doanh khi công tác ở xa hoặc là việc tại nhà vẫn có thể update dữ liệu lên thư mục chia sẻ Share reports trên domain controler **srv-11**

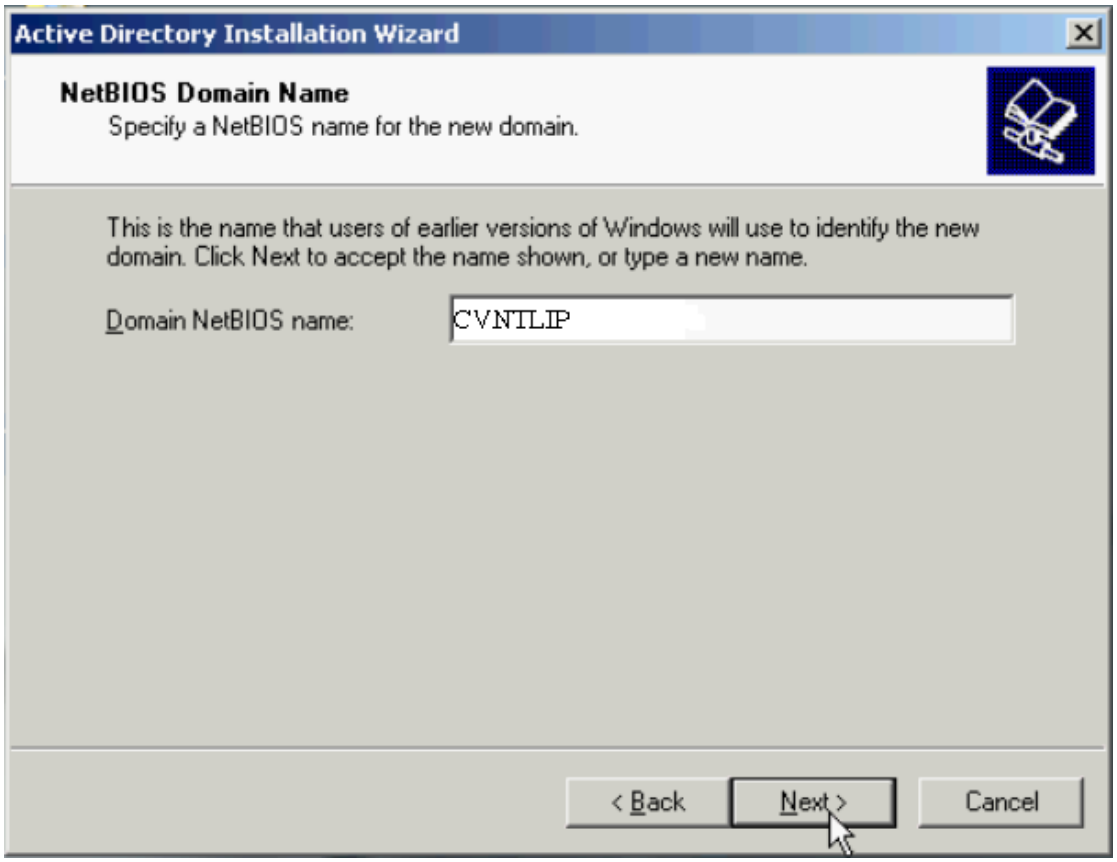
Triển khai mô hình này chúng ta có thể dựng lab với 3 máy như trên hình vẽ, trong đó *client-1 là máy tính ở bên ngoài có ip là 15.15.15.20/8*.

Bước1: Trên **srv-11** cài đặt Domain Controler bằng lệnh dcpromo với domain name cvntlip.com (chúng ta cần khai báo đúng prefered dns server là 192.168.1.1)

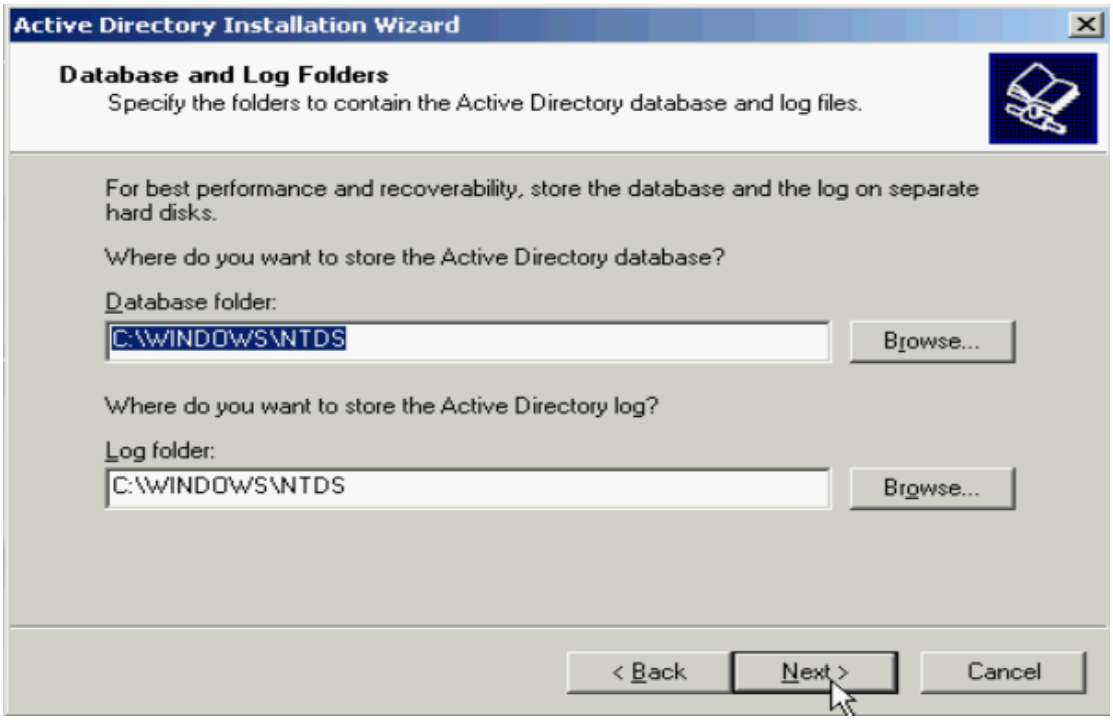
Sau đó Click Next

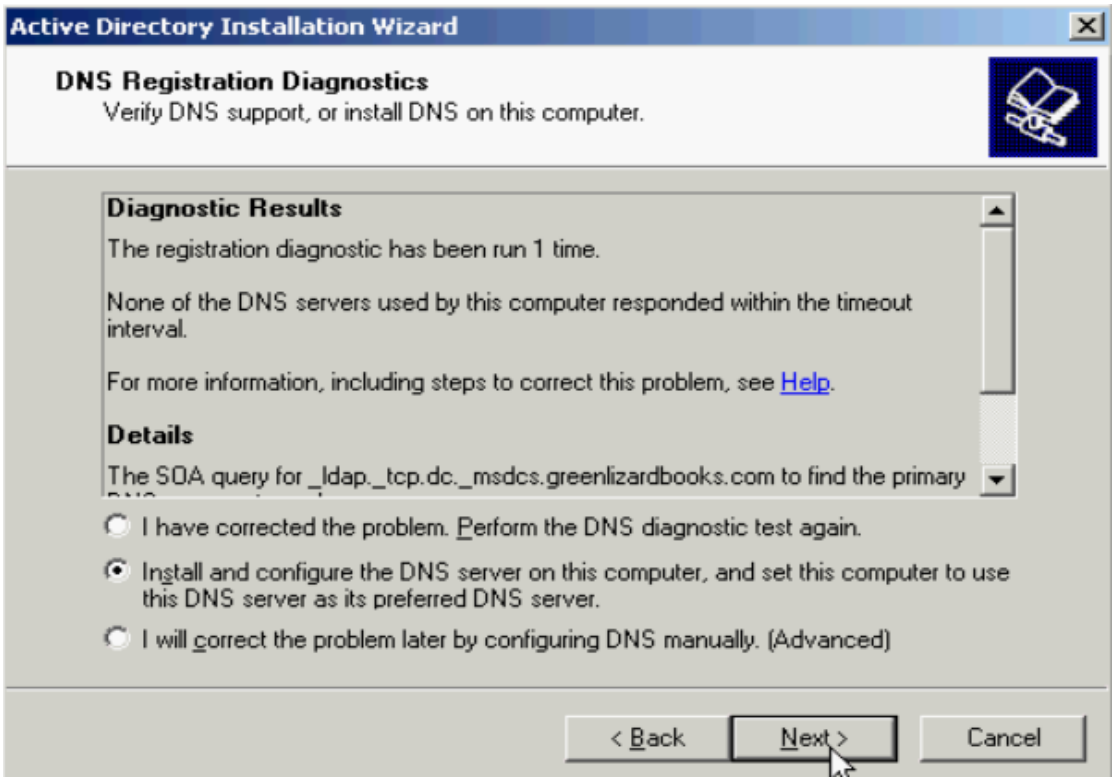
Nhập tên Domain vào: cvntlip.com

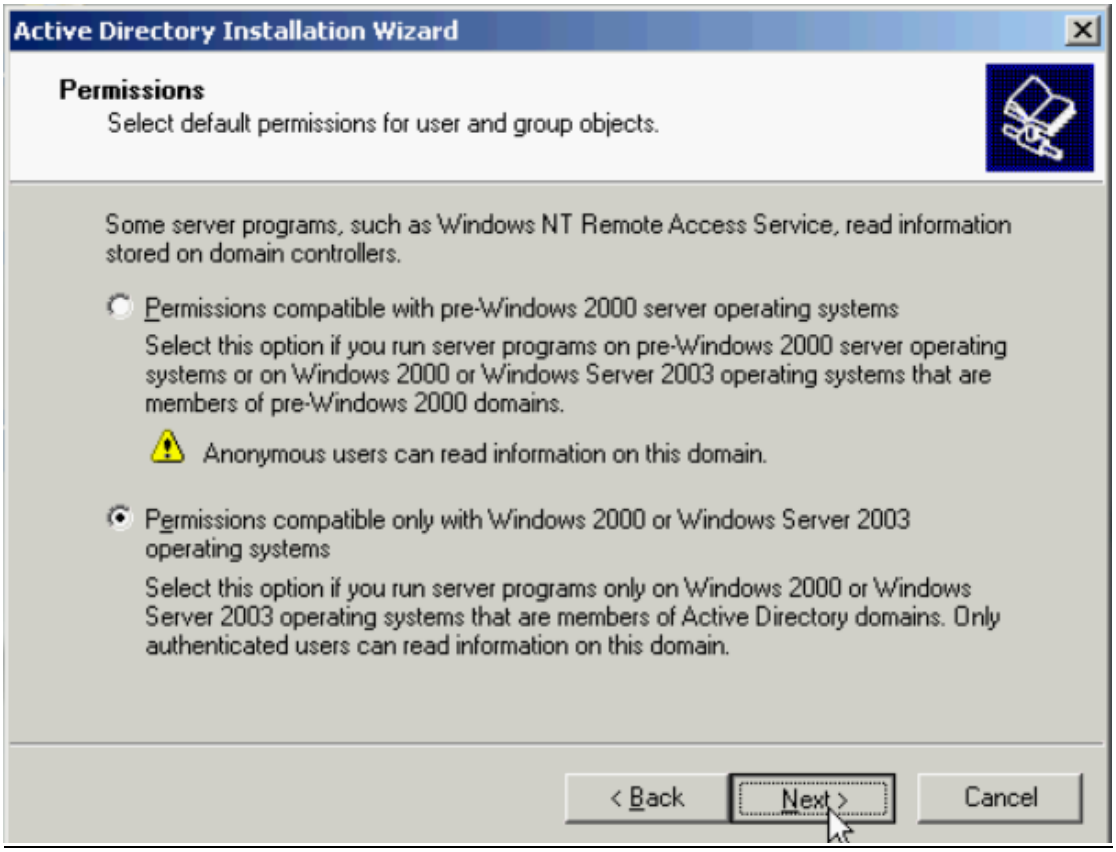




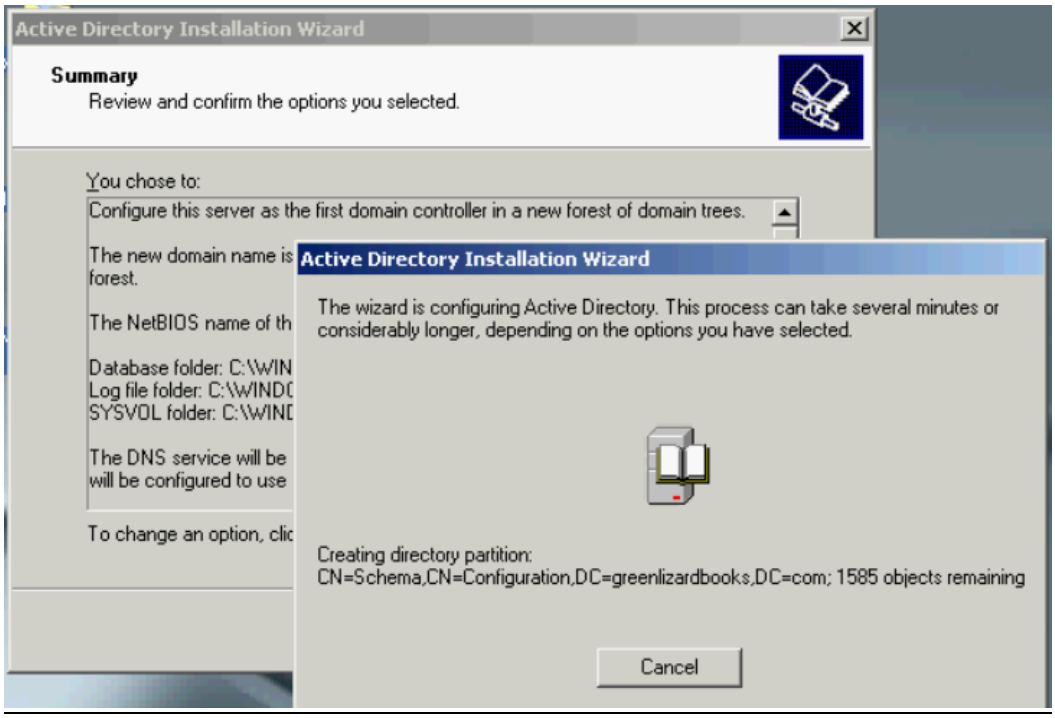
Sau đó Click Next





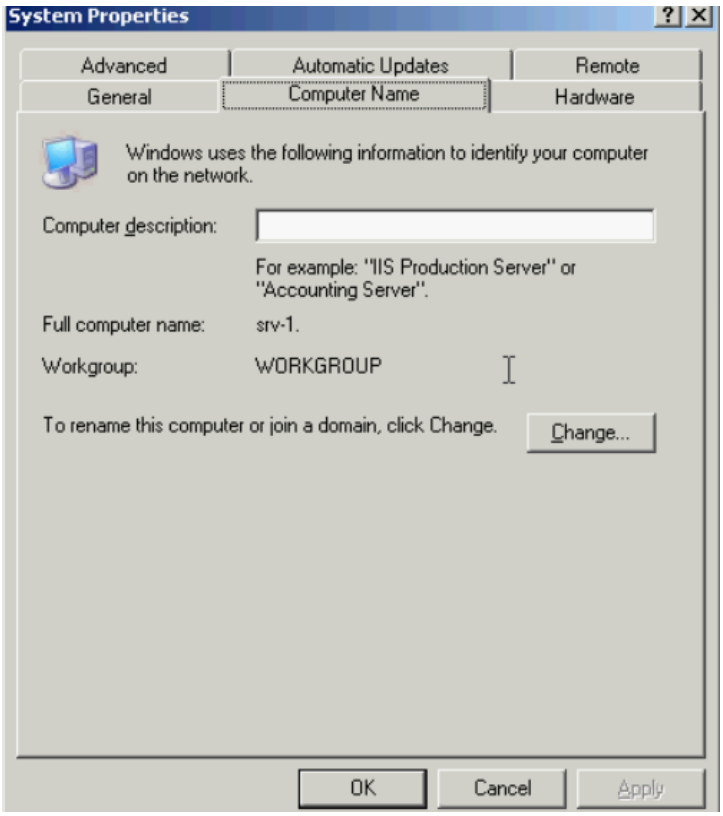


Chọn Permissions compatible only with Windows 2000 or Window Server 20003 operating systems

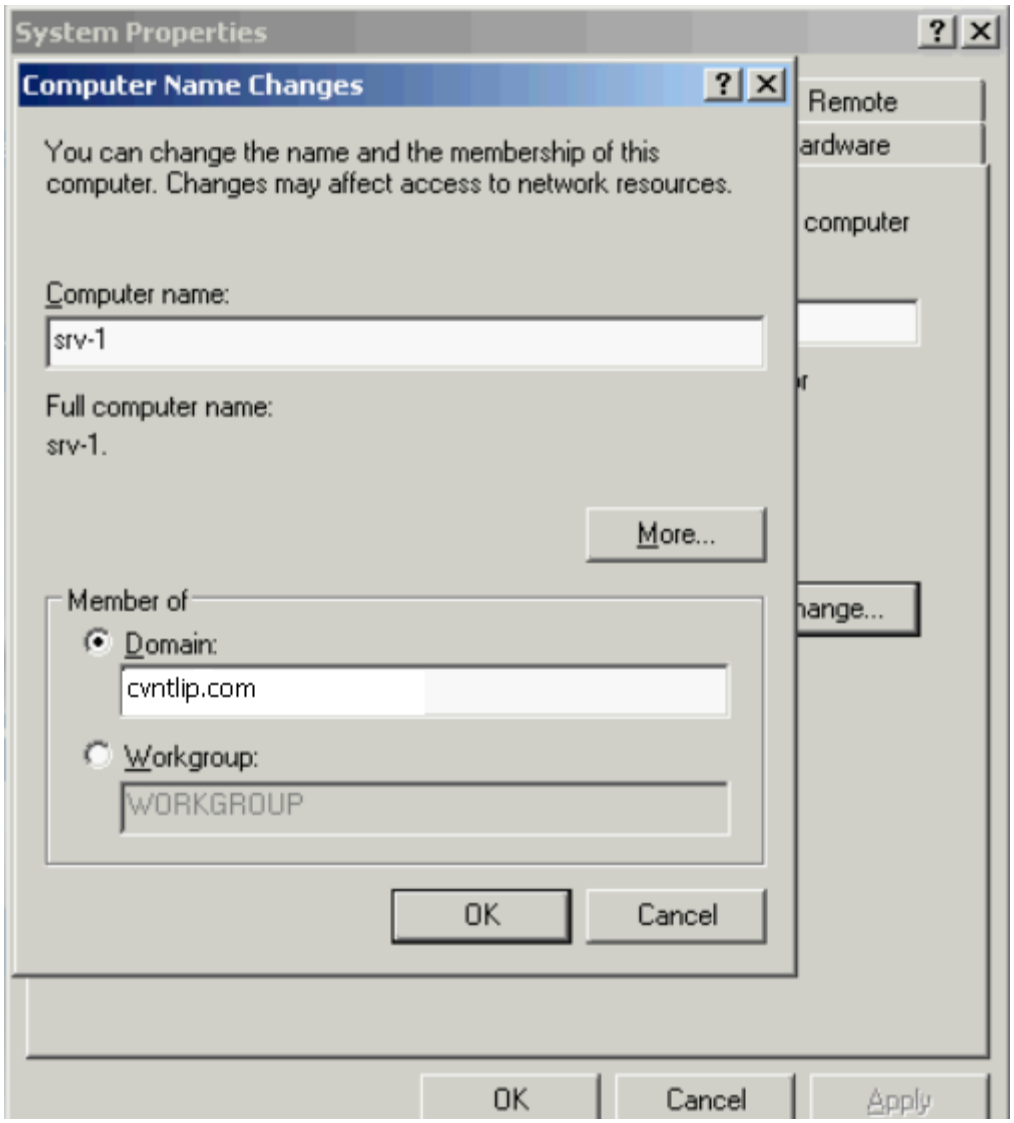


Bước 2 : Join srv1 in Domain Controller on srv11

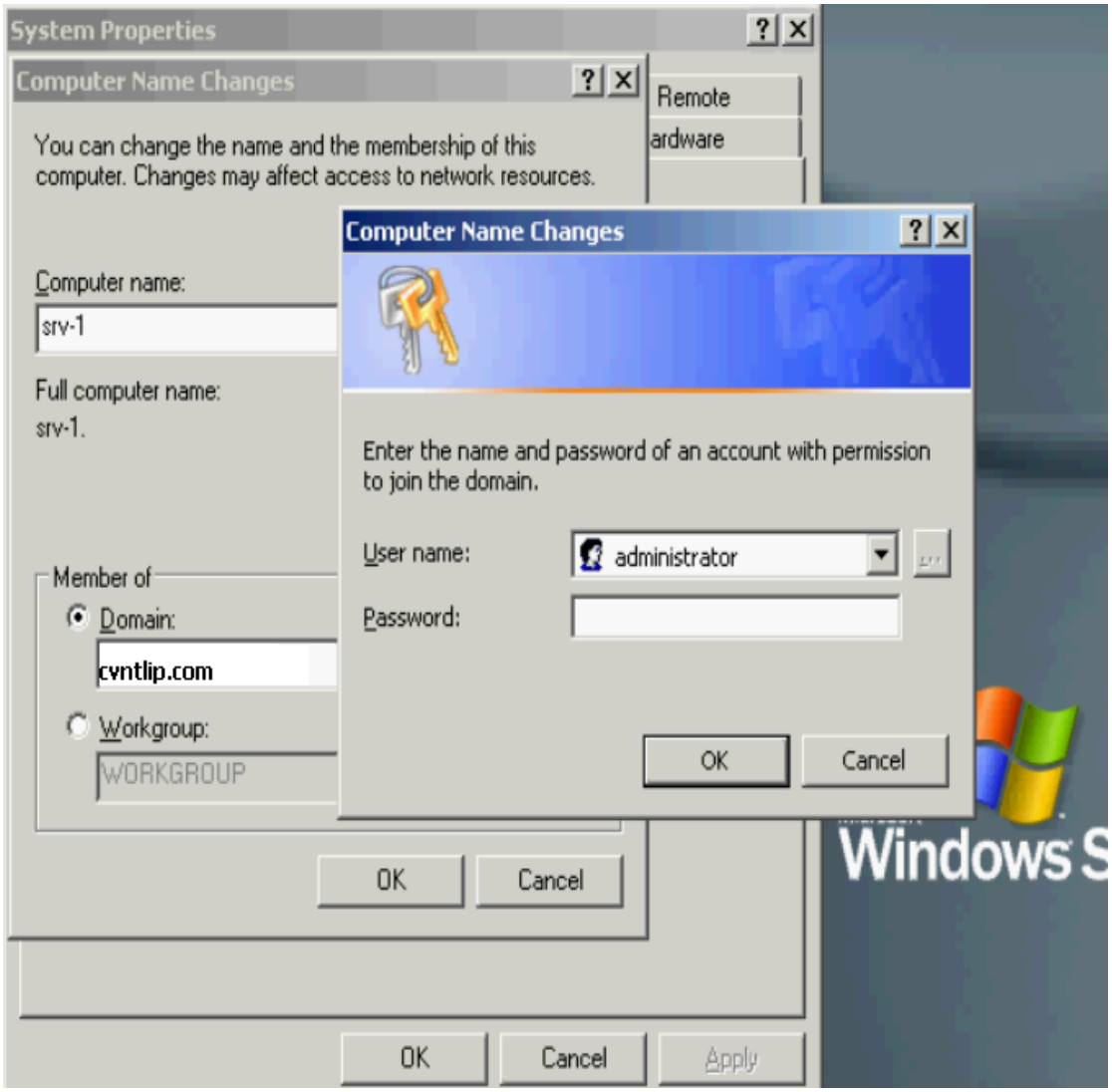
Chuột phải vào Mycomputer chọn Properties/ Computer Name/ Change/ Domain



Nhập tên Domain vào ô trống


System Properties
Computer Name Changes
You can change the name and the membership of this computer. Changes may affect access to network resources.
Computer name:
srv-1
Full computer name:
srv-1.
More...
Member of
Domain:
cvntlip.com
Workgroup:
WORKGROUP
OK
Cancel
Remote
ardware
computer
nange...
OK
Cancel
Apply

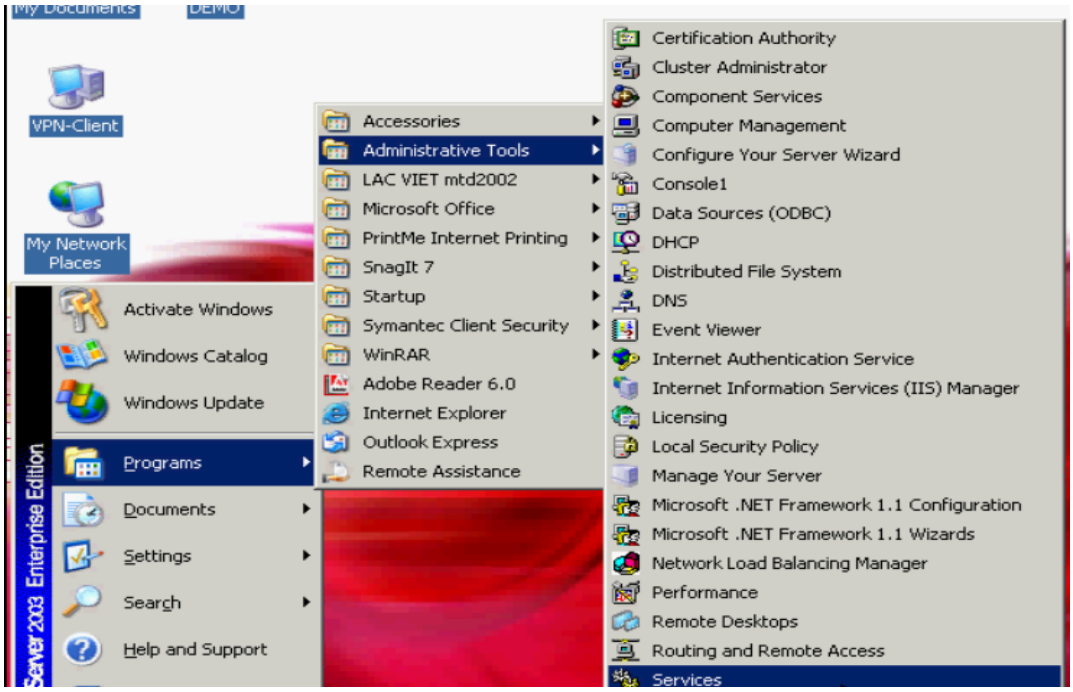
Nhập User name và Password của Administrator theo SRV11(DC)



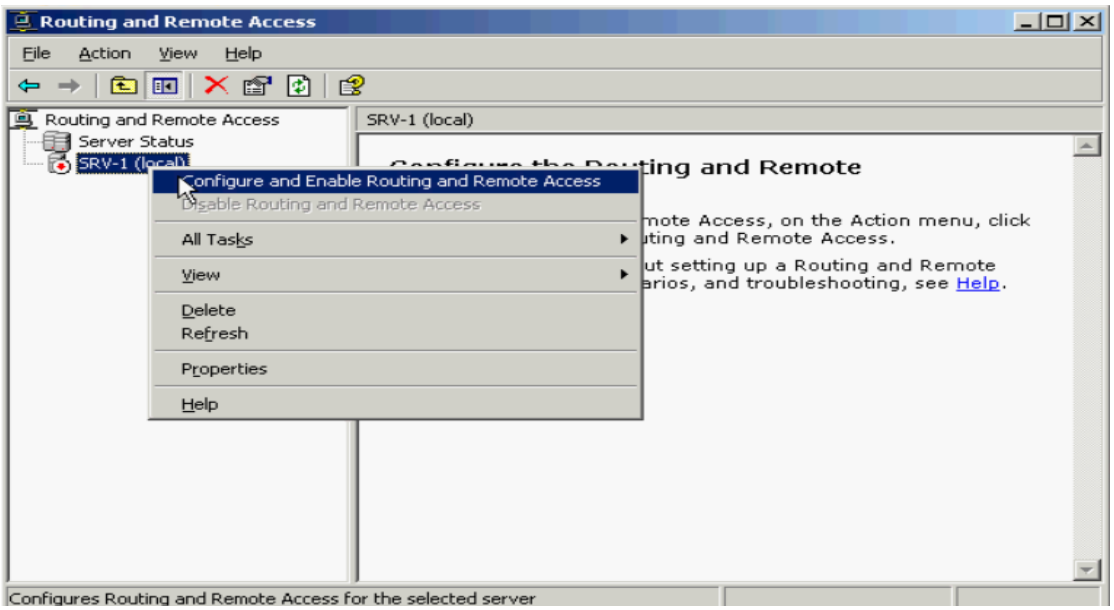
Khi kiểm tra tên máy của SRV1 là: srv1.cvntlip.com là được

Bước 3 : Cài đặt vpn server thông qua RRAS trên srv-1

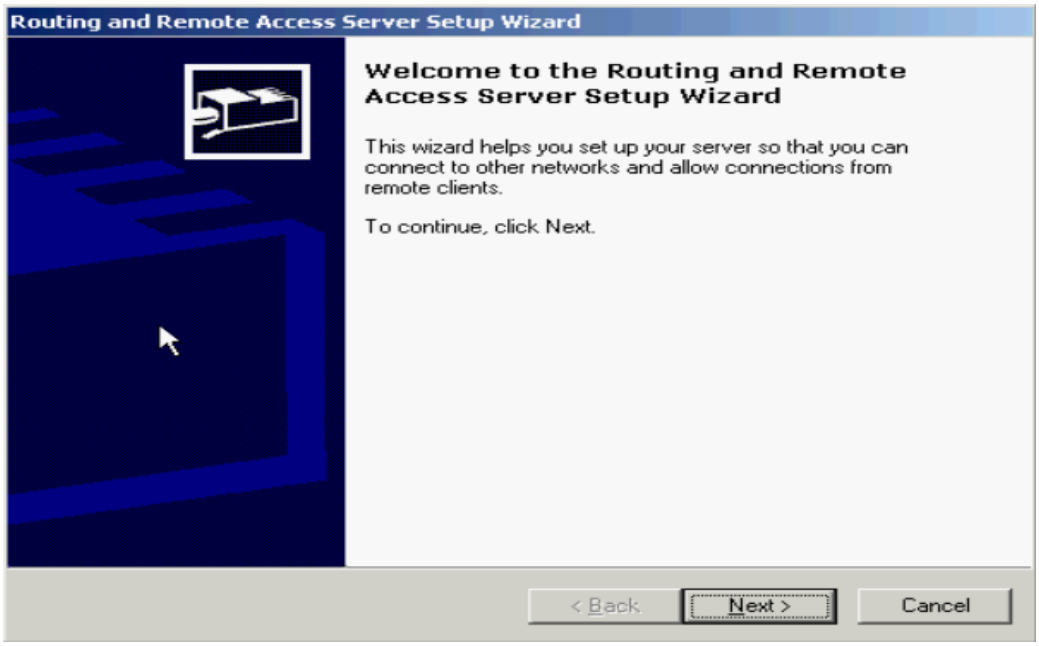
Programs/ Administrator Tools/ Routing and Remote Access



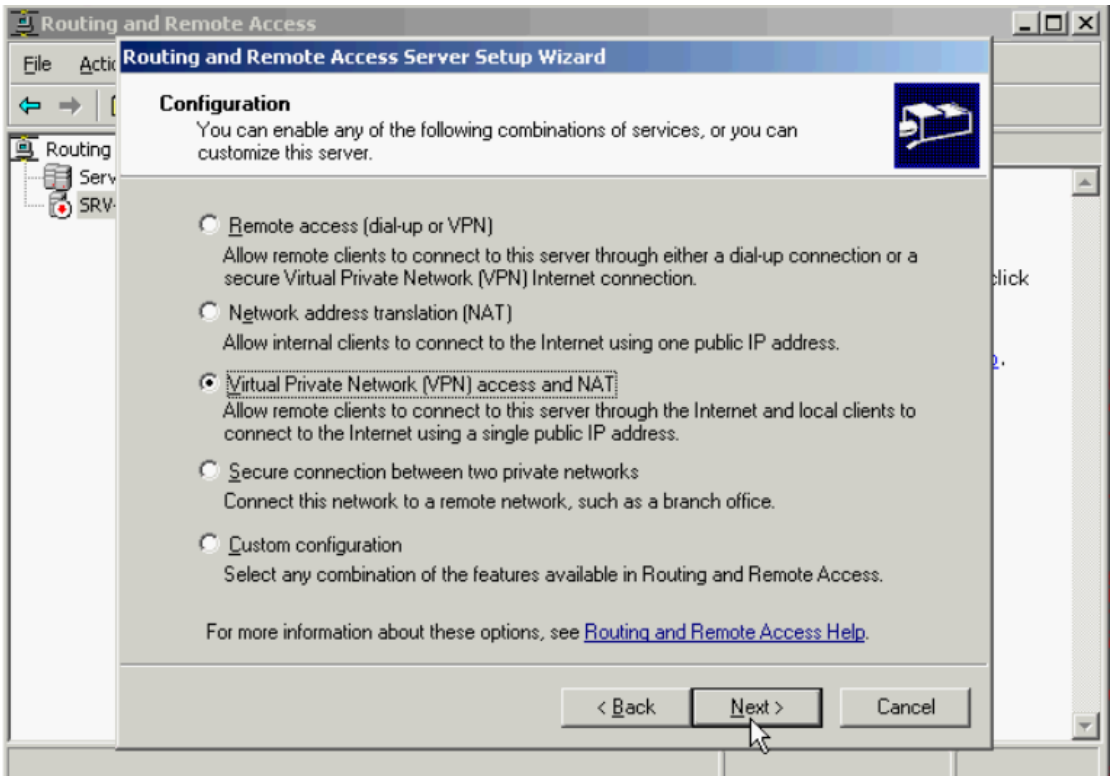
Chuột phải vào Srv1 và chọn Configure and Enable Routing and Remote



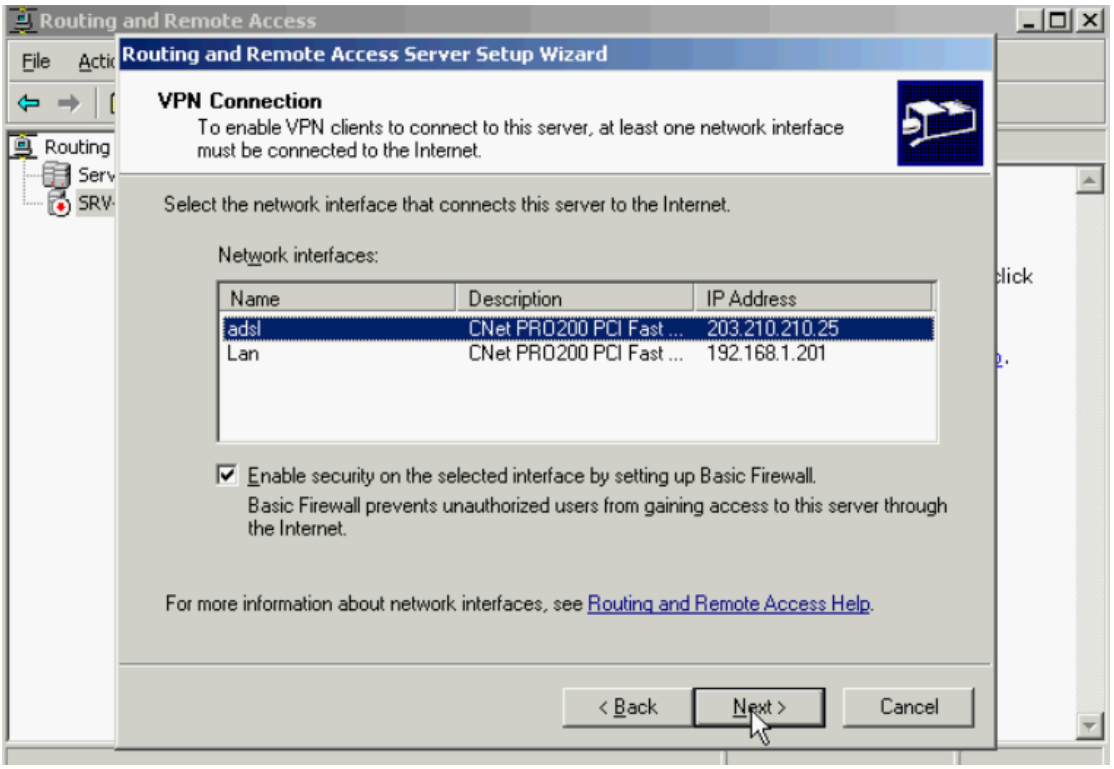
Chọn Next



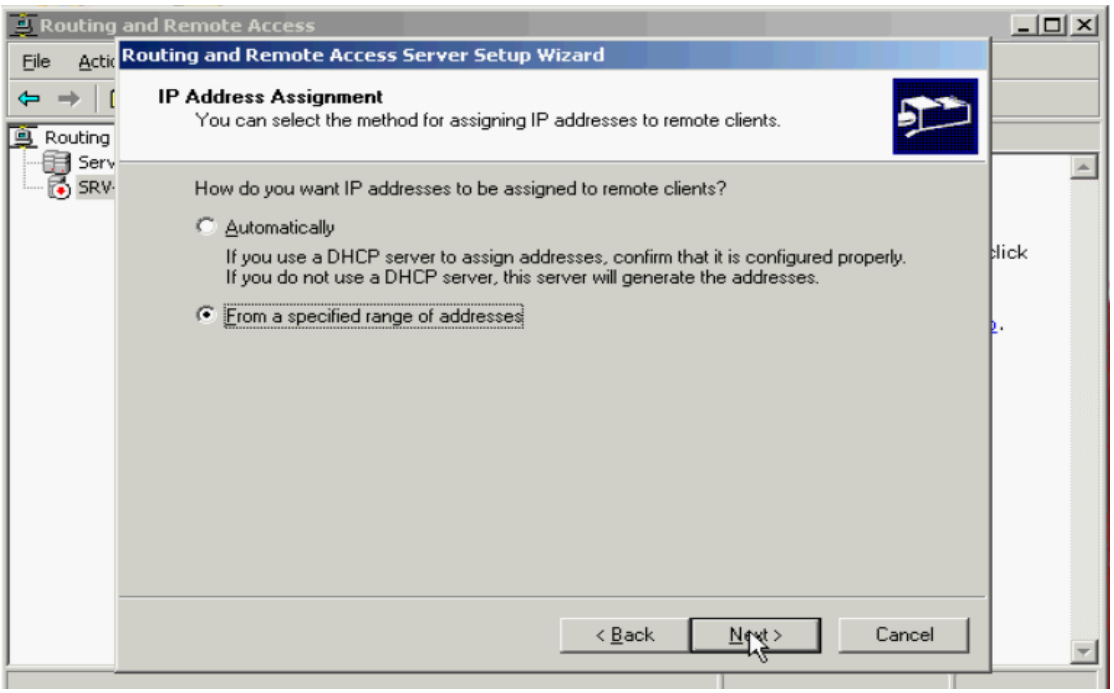
Chọn Virtual Private Network(VPN Access and NAT)



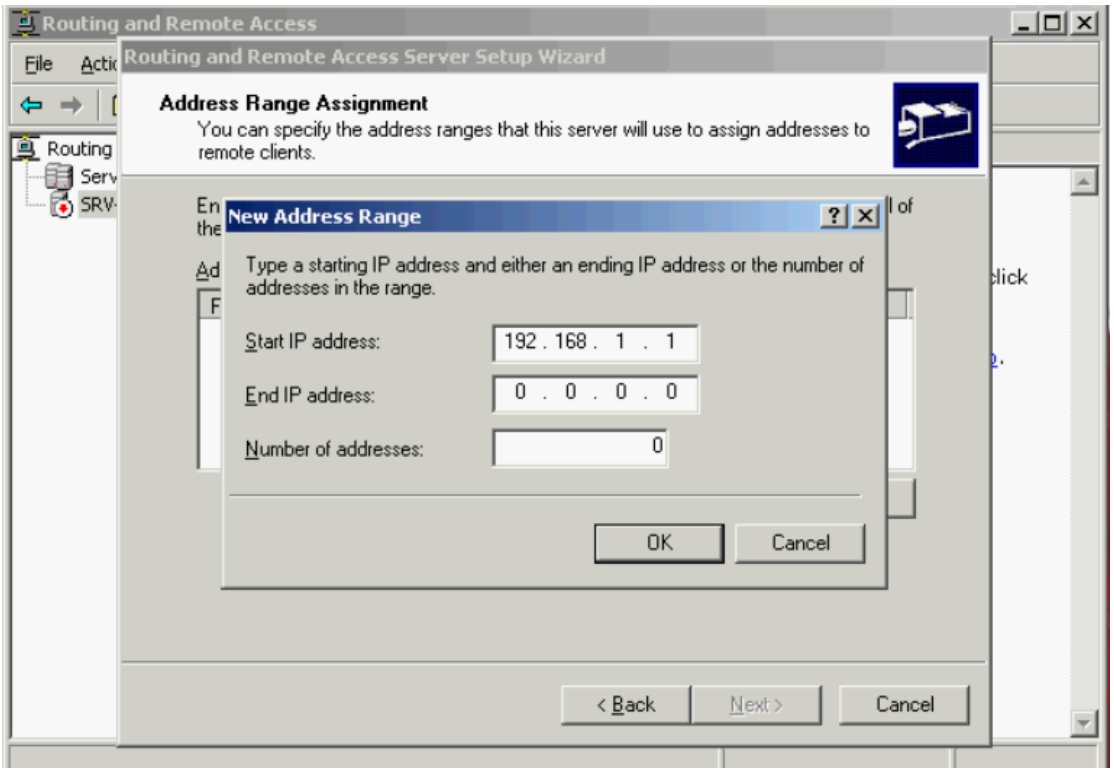
Chọn adsl theo yêu cầu của bài toán



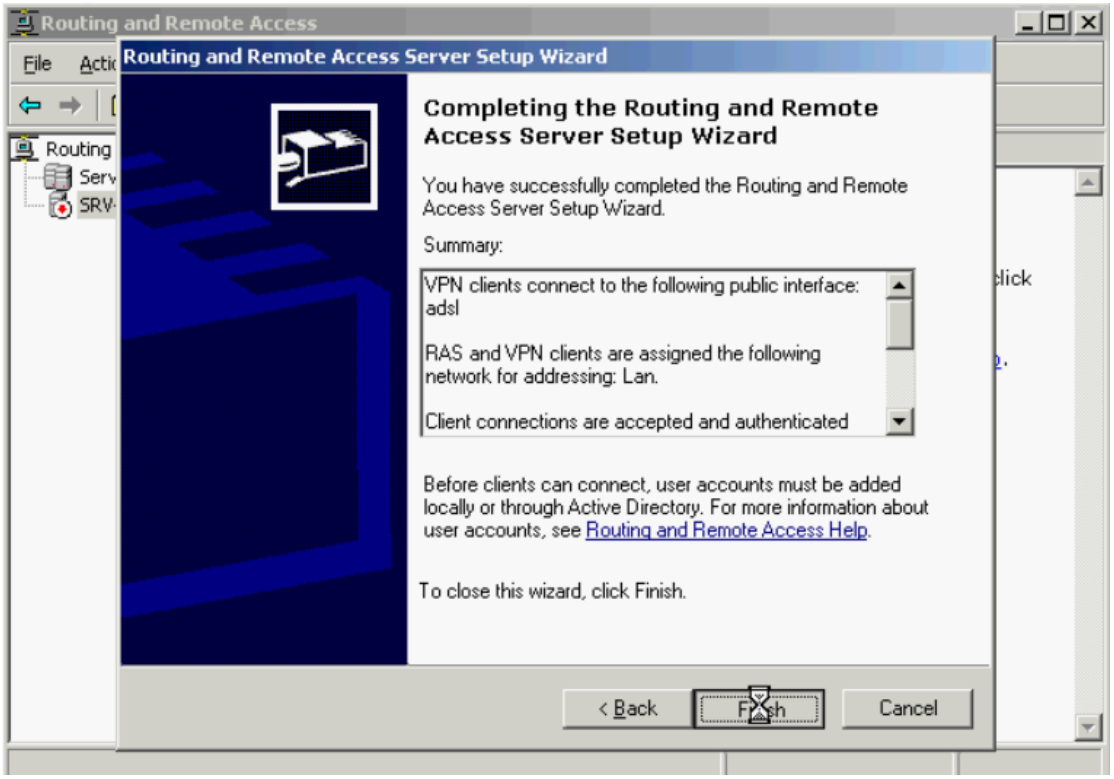
Chọn From a specifield range of addresses

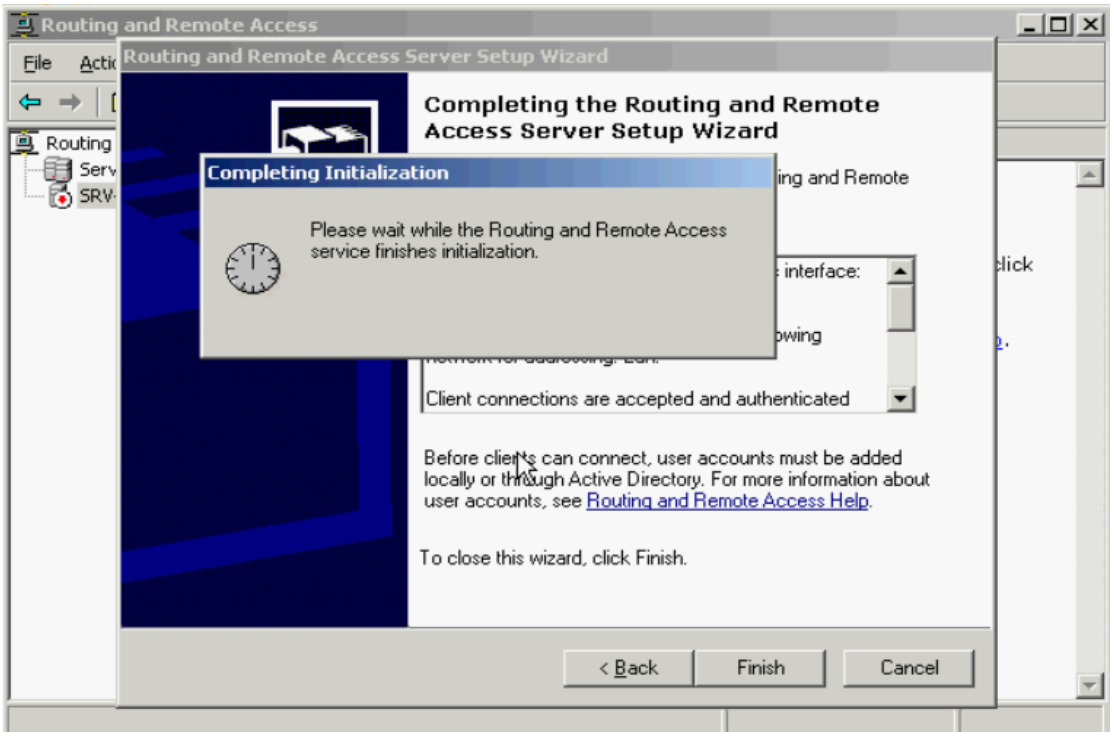


Chọn New sau đó nhập địa chỉ IP của các máy Client connect đến VPN server

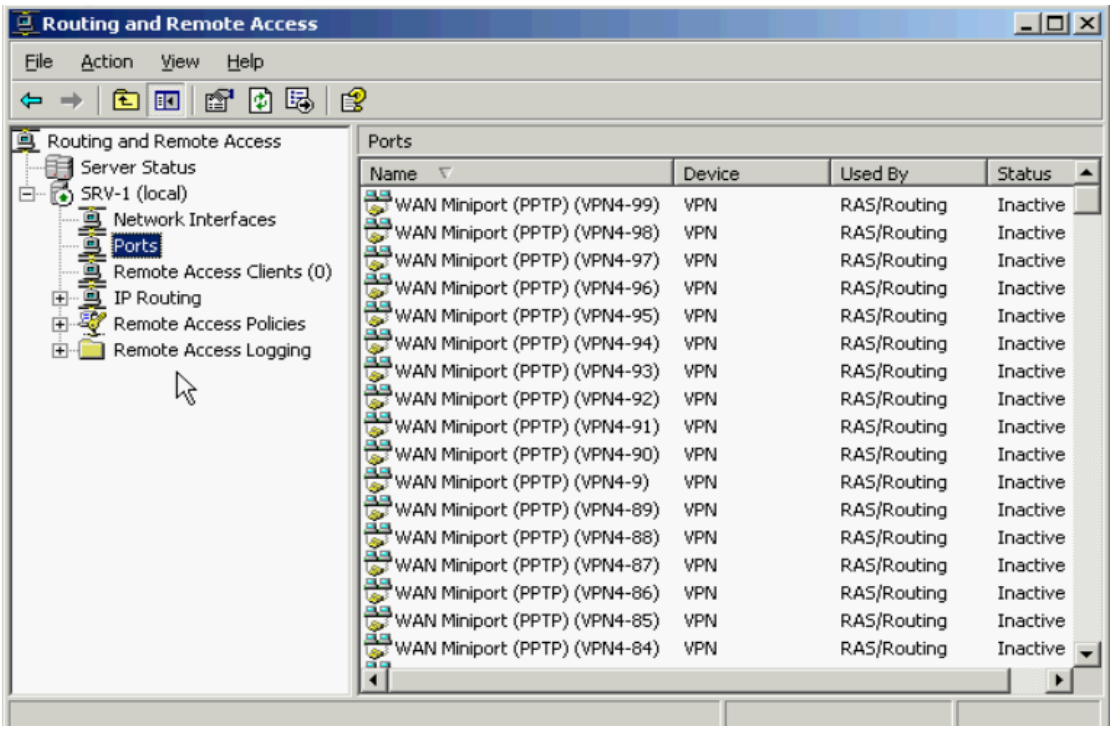


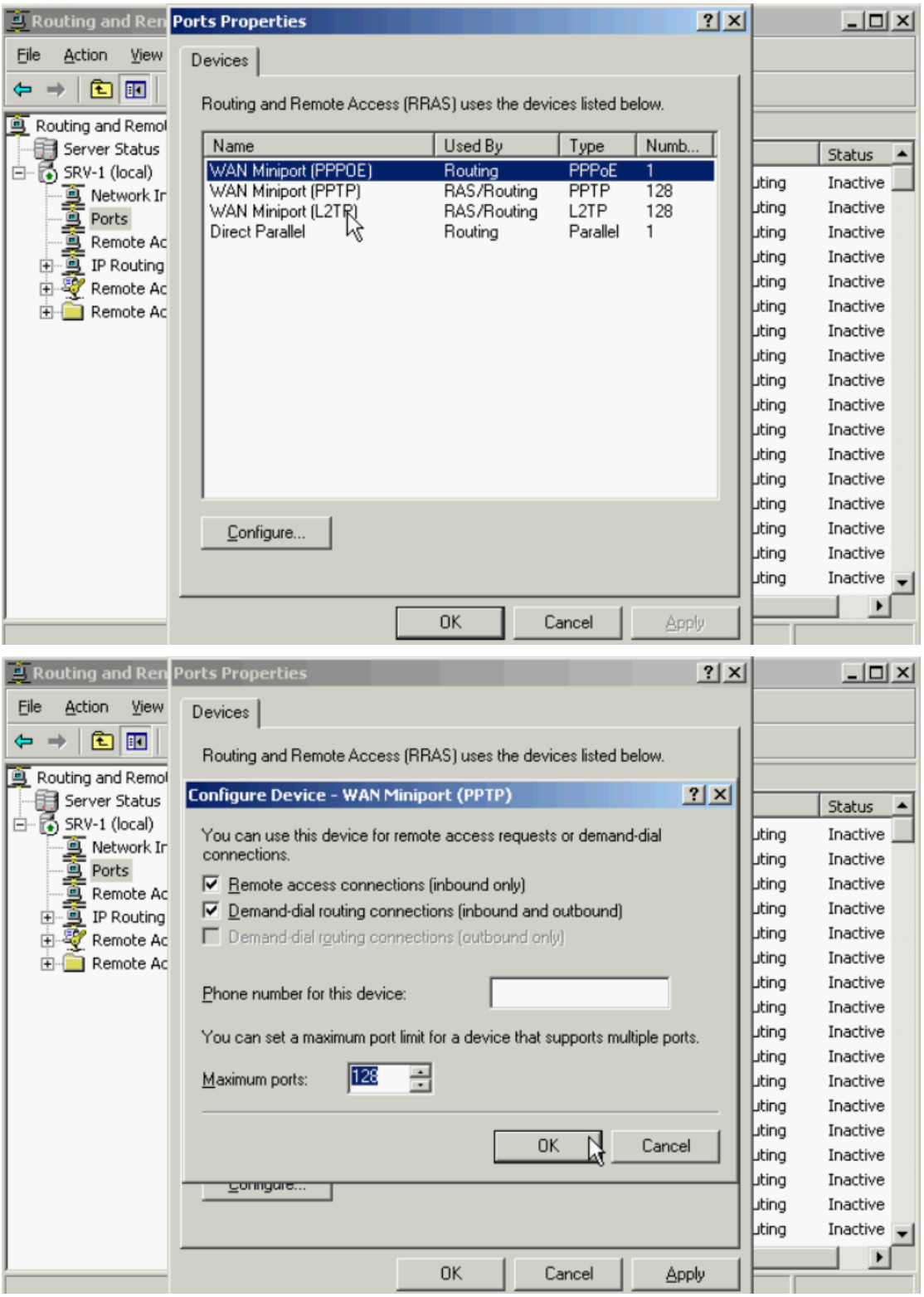
Chọn Next sau đó chọn Finish





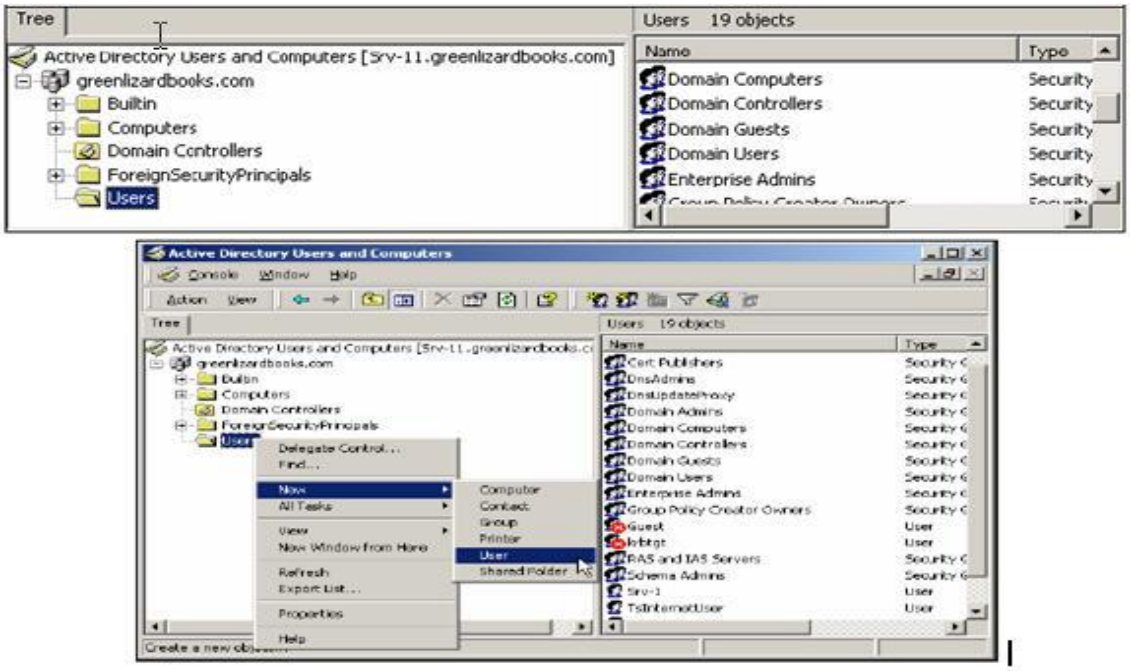
Xem thông tin của các Port/ Chuột phải vào Port



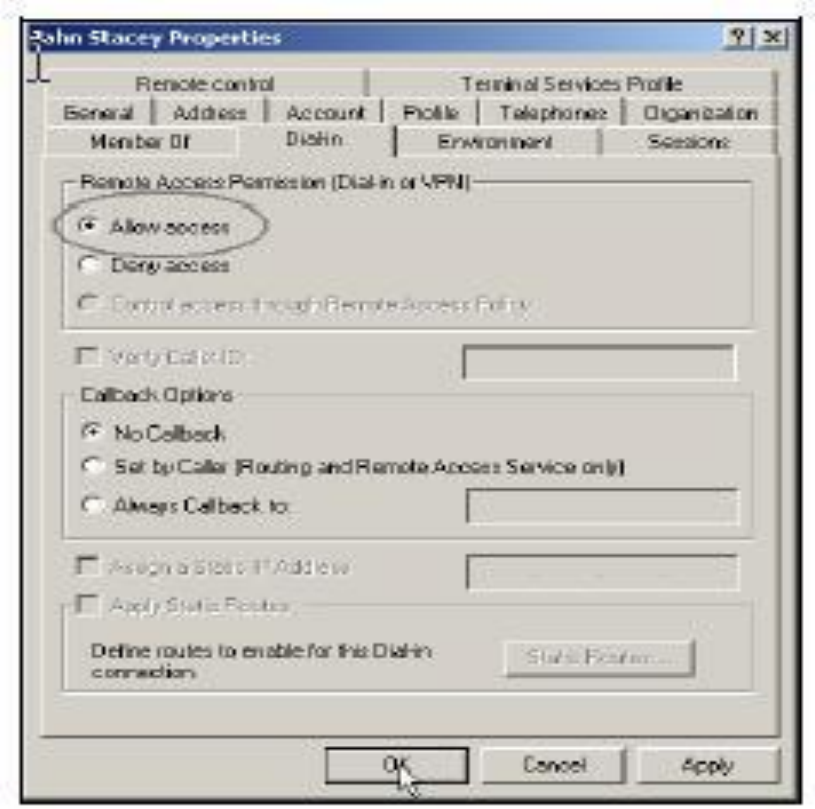


Chúng ta đã cấu hình xong vpn server trên srv-1 và xây dựng domain controler srv-11, lúc này chúng ta có thể kiểm tra kết nối vpn có thành công hay không bằng cách tạo tài khoản người dùng **v008209** trên DC cho phép Allow (dial-in) và tạo vpn client conection trên máy tính ở xa client-1 (15.15.15.20)

Vào Start/ Programs/ Administrator Tools/ Actice Directtory User and Computer tạo new user v008209

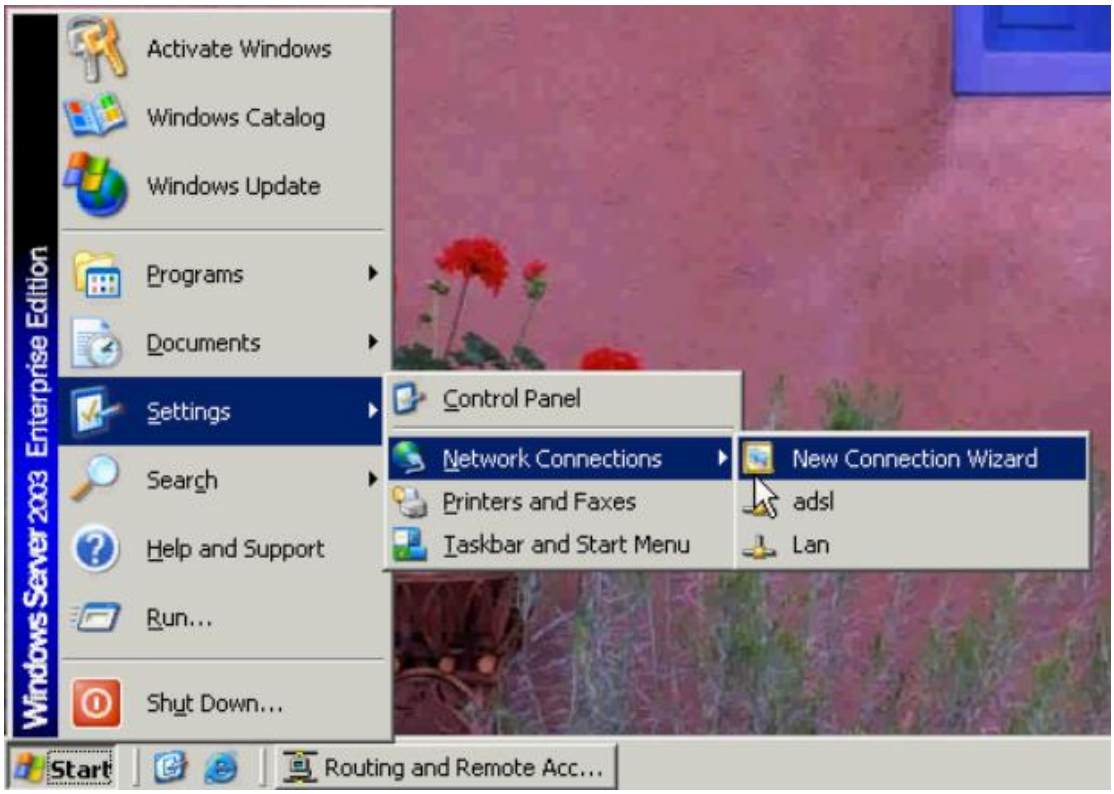


Chuột phải vào User vừa chọn và chọn Properties/ Allow access

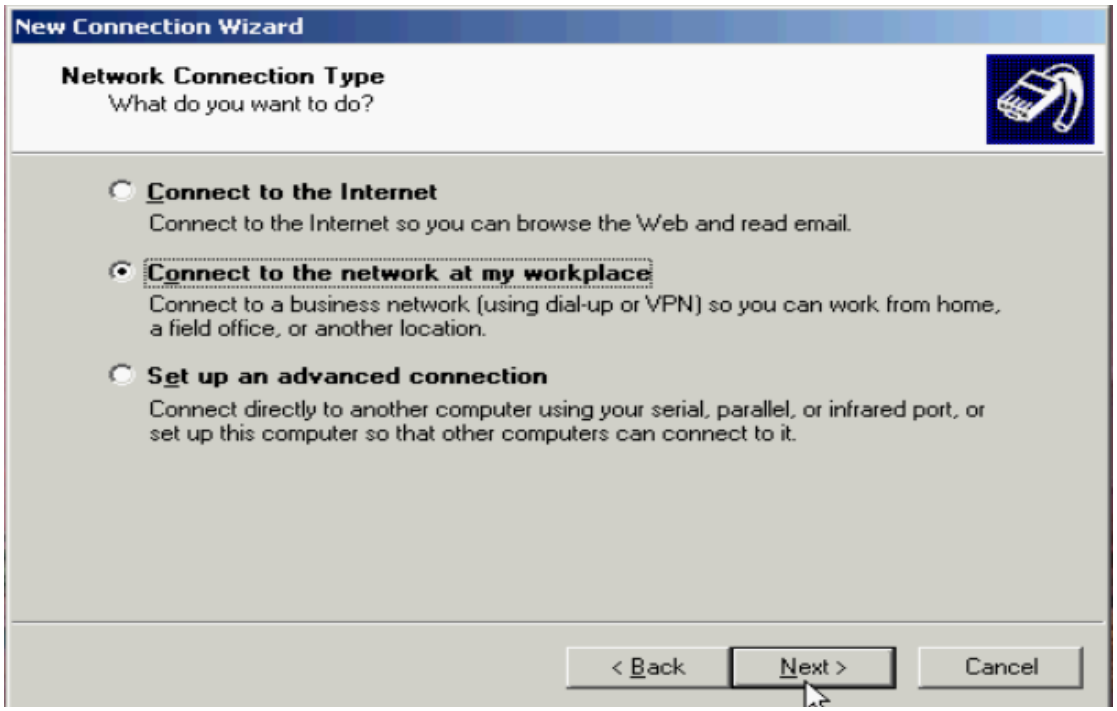


Bư ớc 4: Tạo VPN client để connect vào srv1

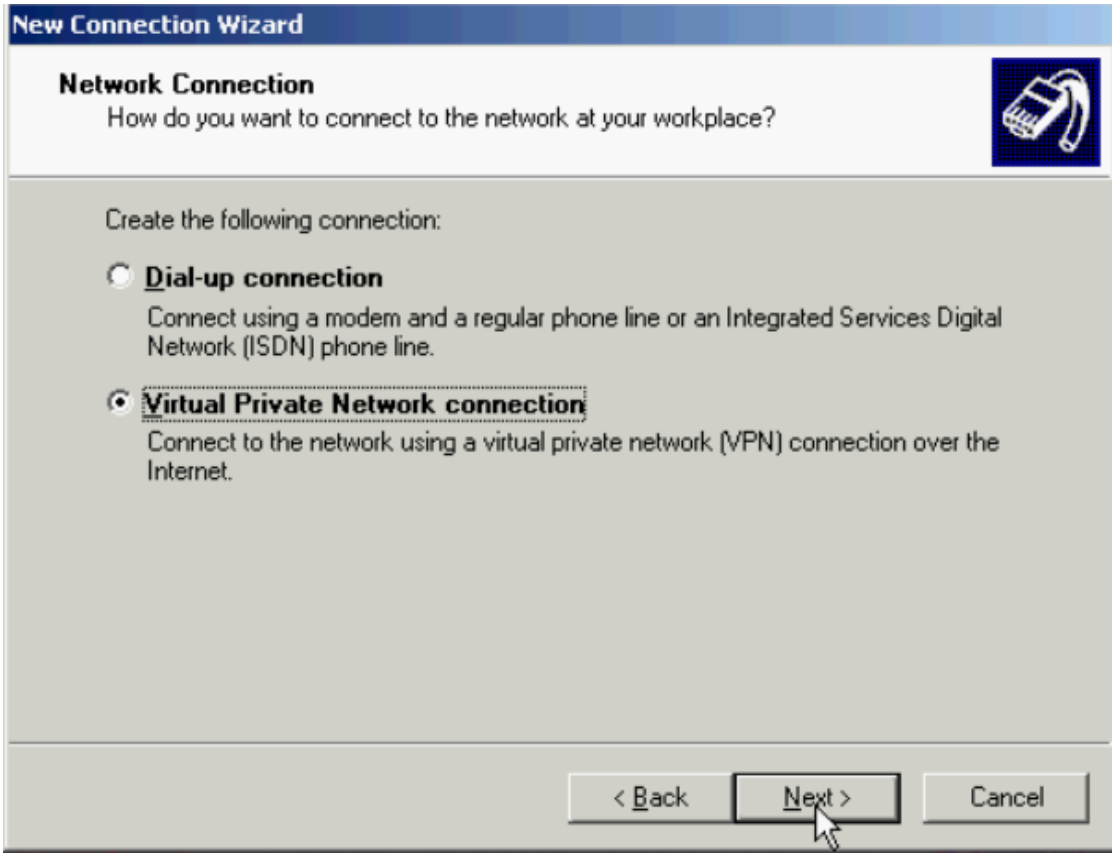
Sau đó chúng ta tạo 1 vpn client connection trên client 1 :chọn start->setting->network and dialup connection và click make new connection

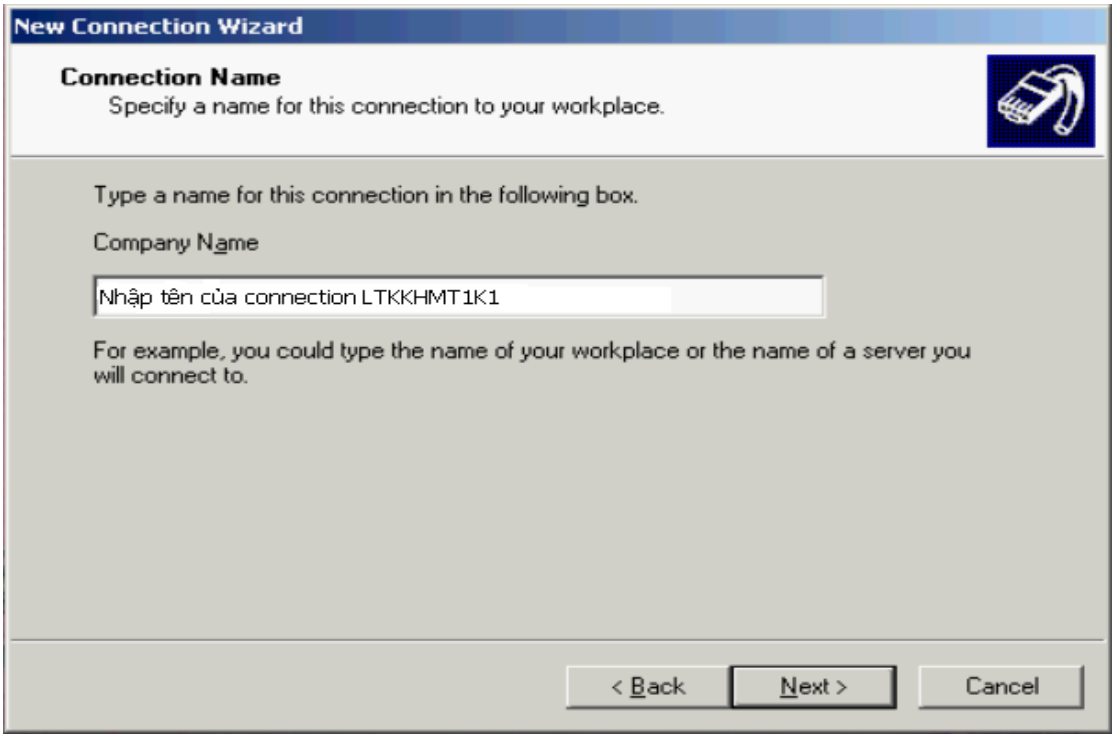


Chọn Next/ Connect to the Network at my workplace

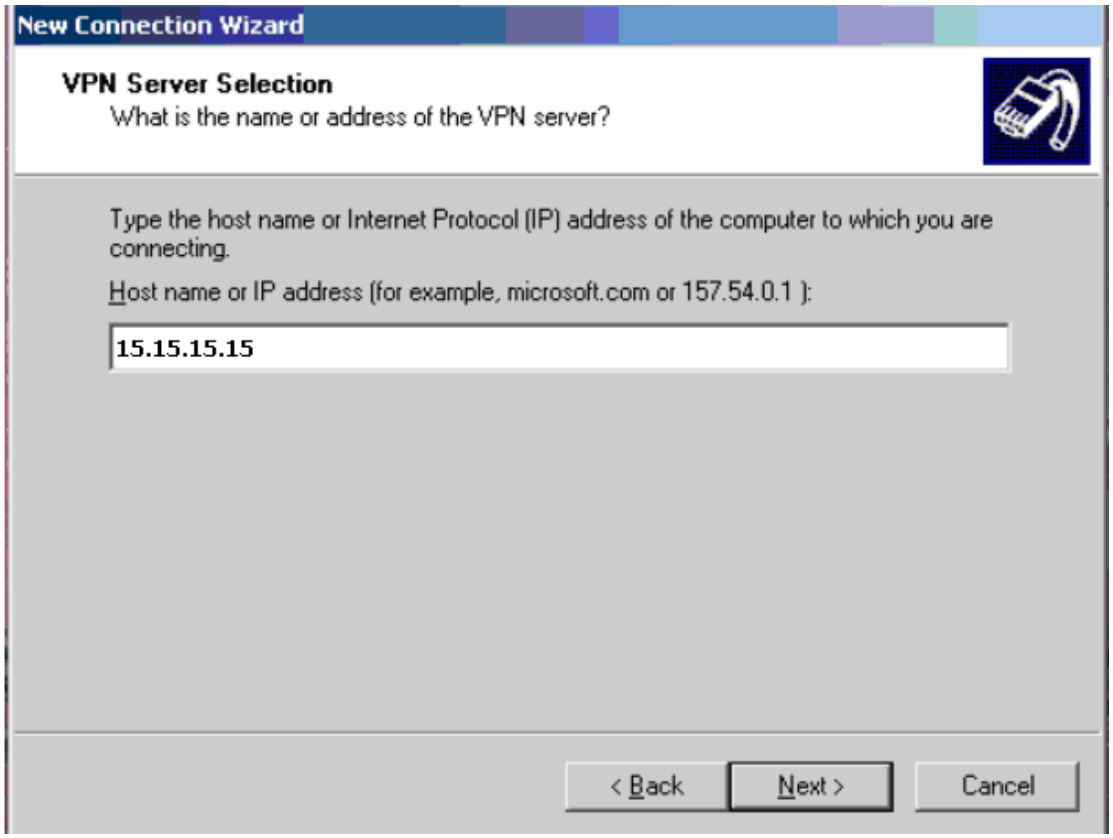


Chọn Virtual Private Network connection

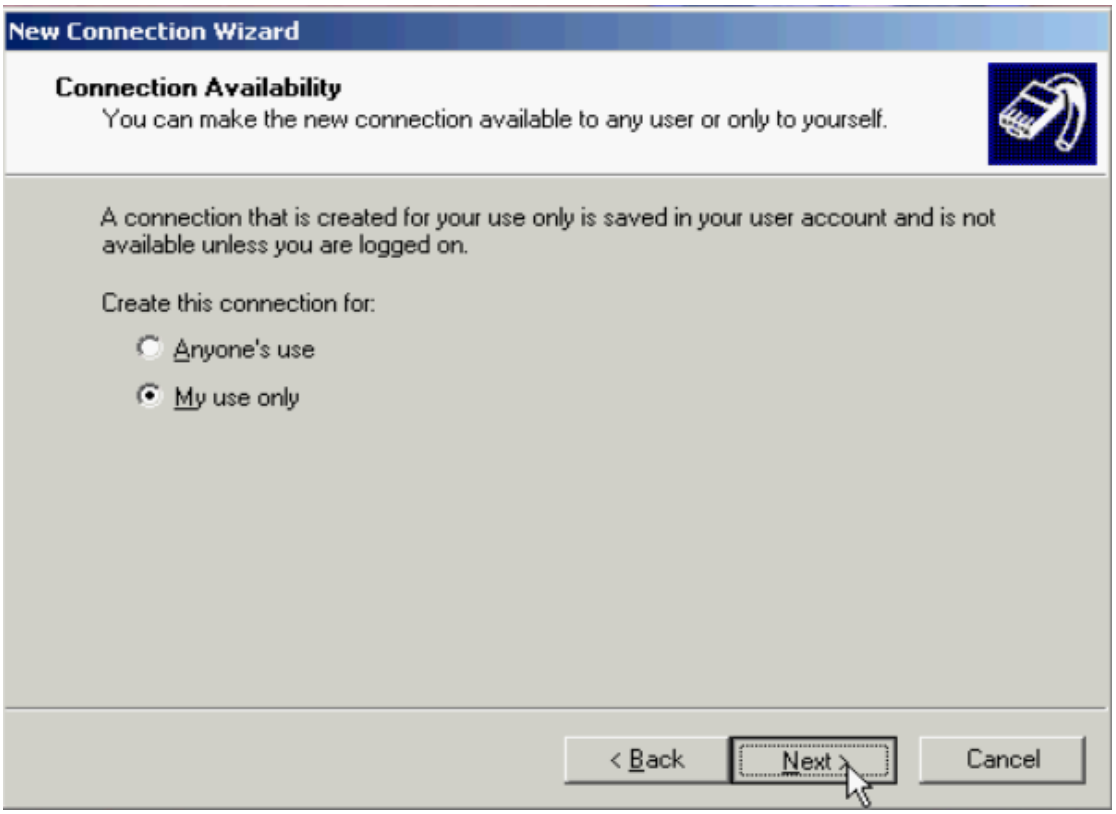




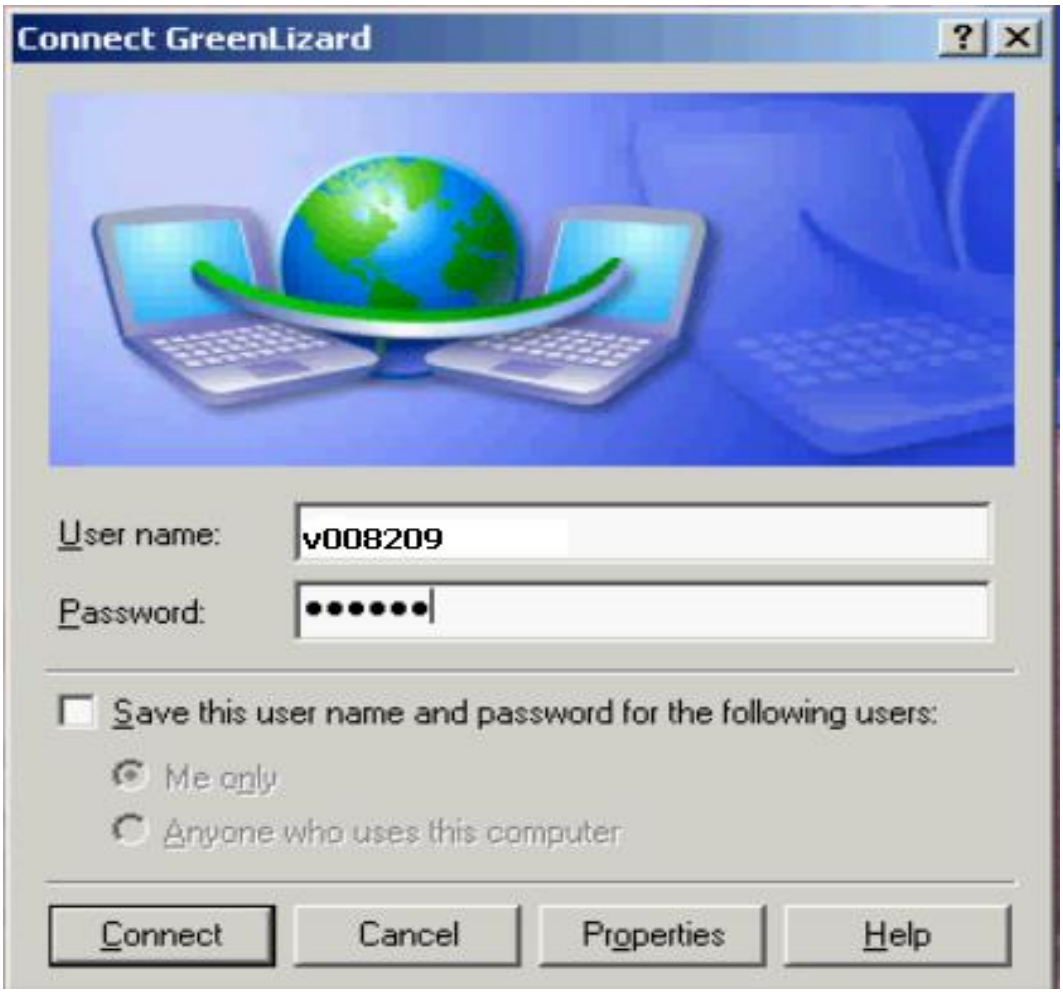
Nhập địa chỉ của Host name srv11(15.15.15.15): Đây là địa chỉ external của VPN server trong thực tế địa chỉ này được gán bởi ISP

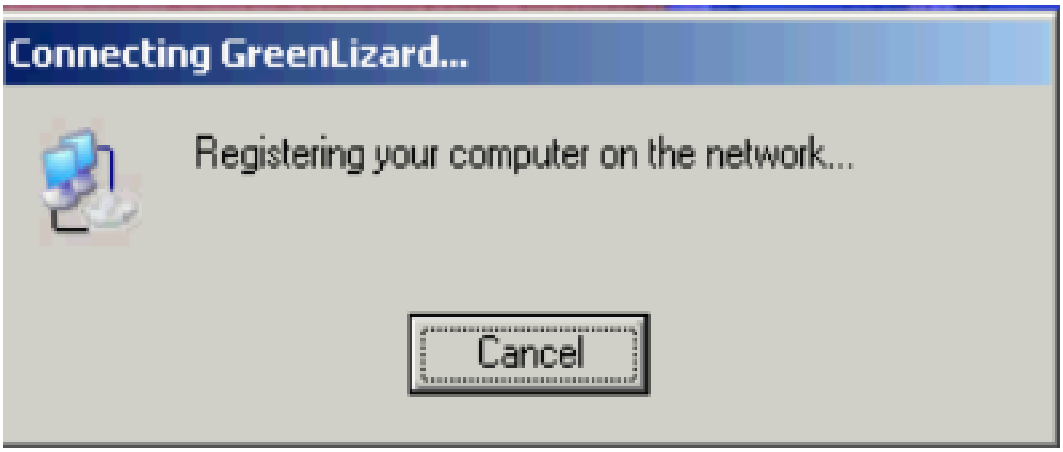


Chọn My use only và Finish

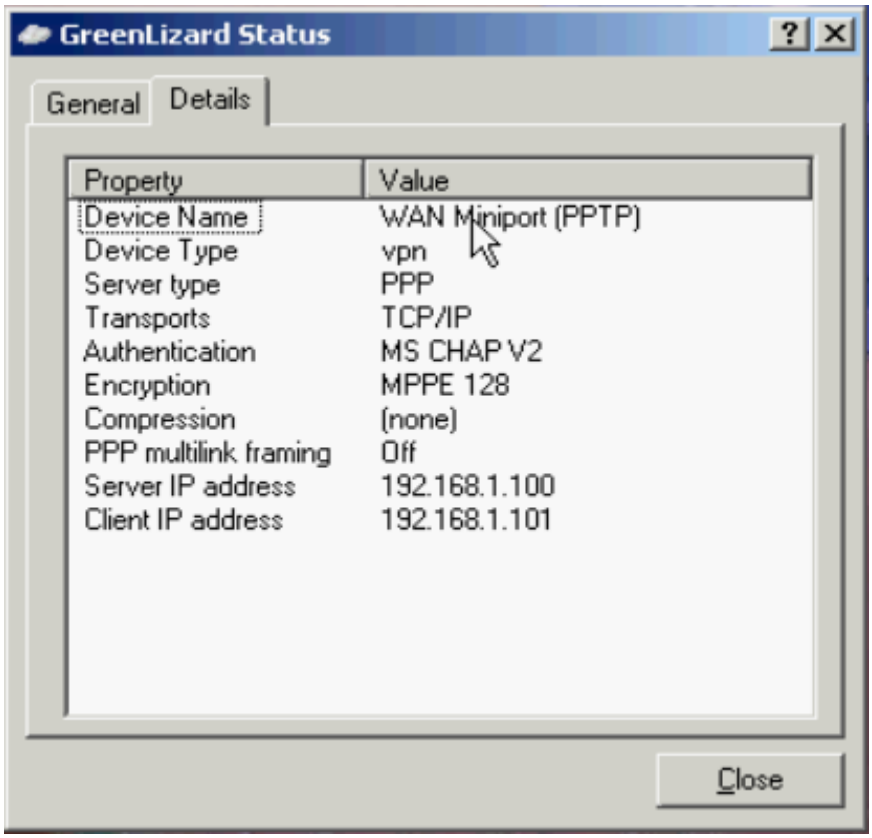


Nhập user name và password mà ta đã tạo trên DC(SRV11)





Xem thông tin của Card mạng



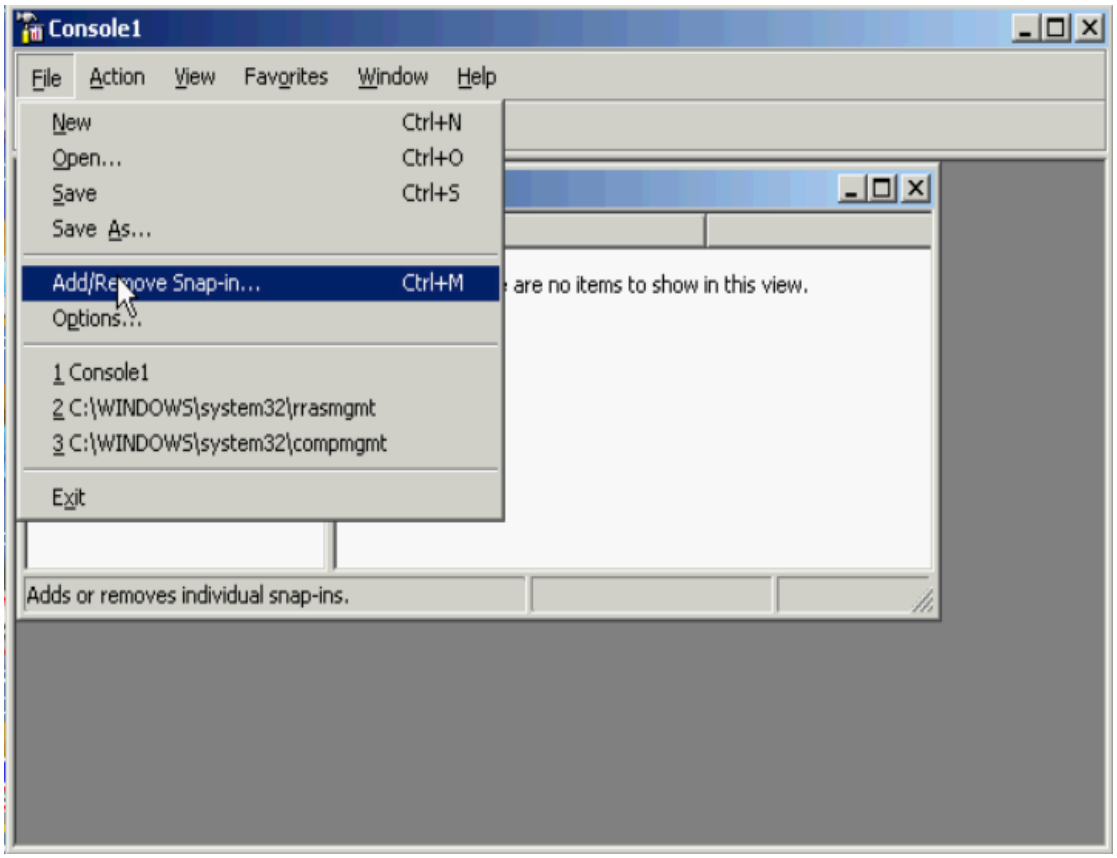
Sau đó ping đến srv11(192.168.1.1) đư ợc là thành công

Bước 5: Join Client vào Domain cvntlip.com

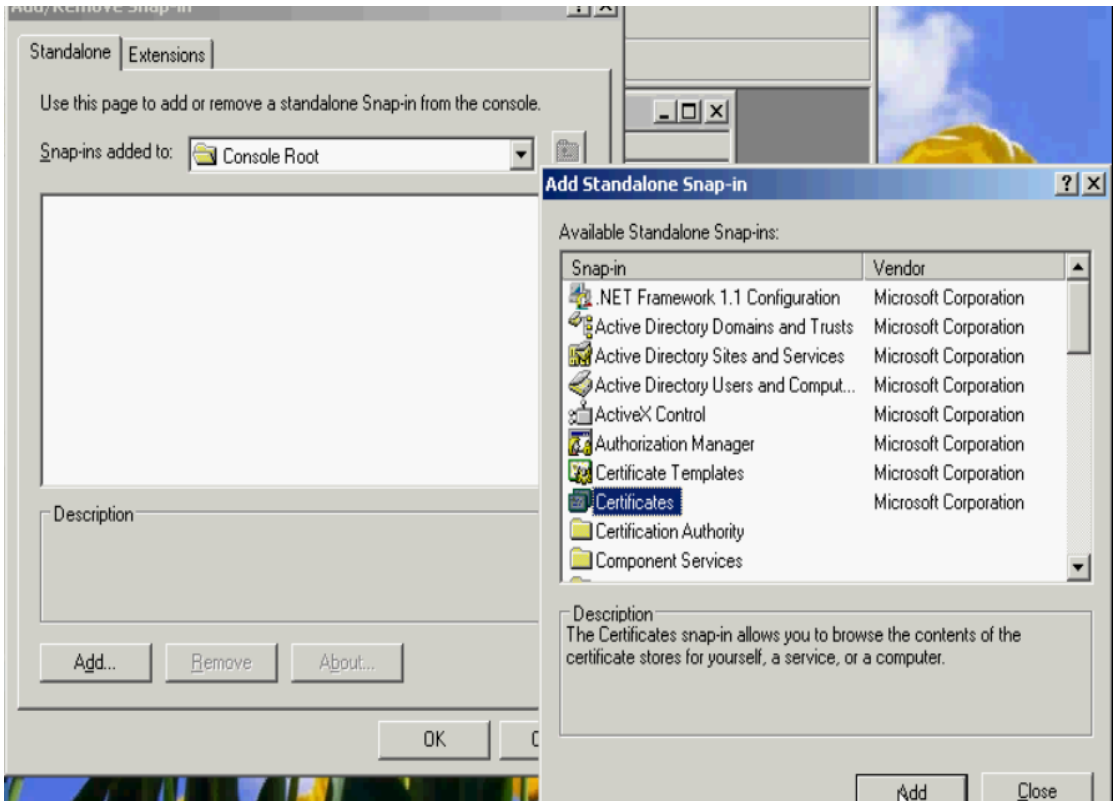
Tương tự như join Srv1 vào Domain Controller

Bước 6: Tạo một thiết lập yêu cầu giữa VPN server và Client

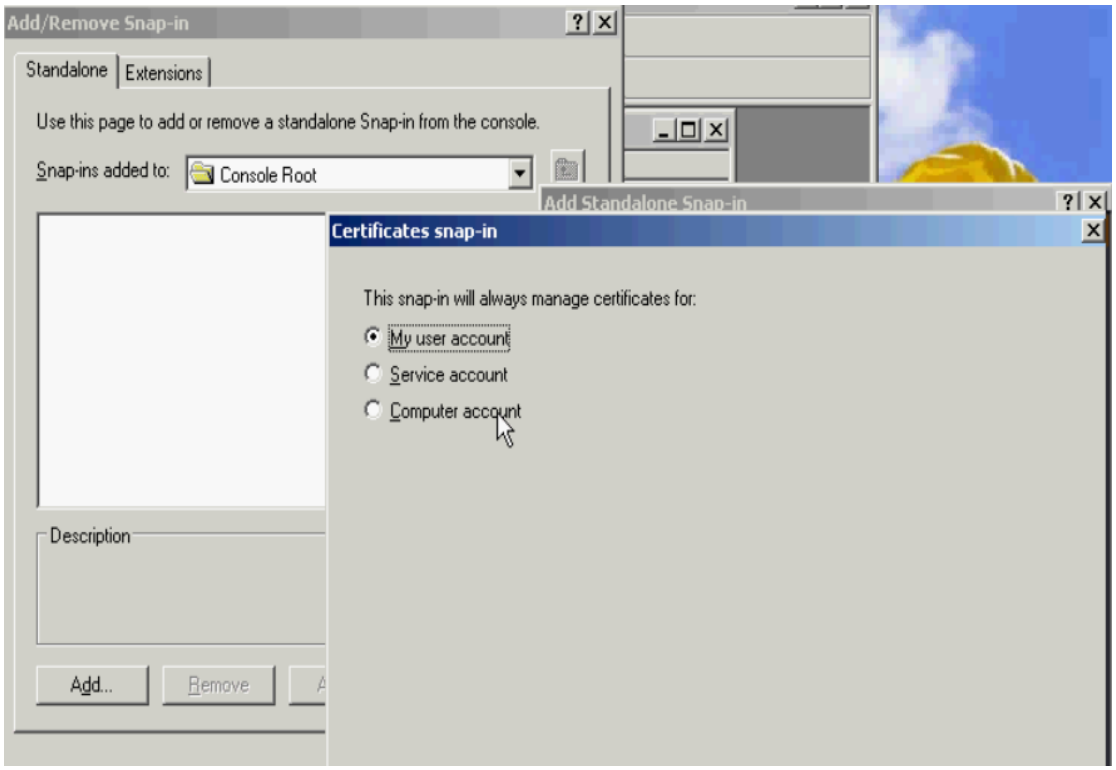
Tại cửa sổ Run/ mmc/ Enter



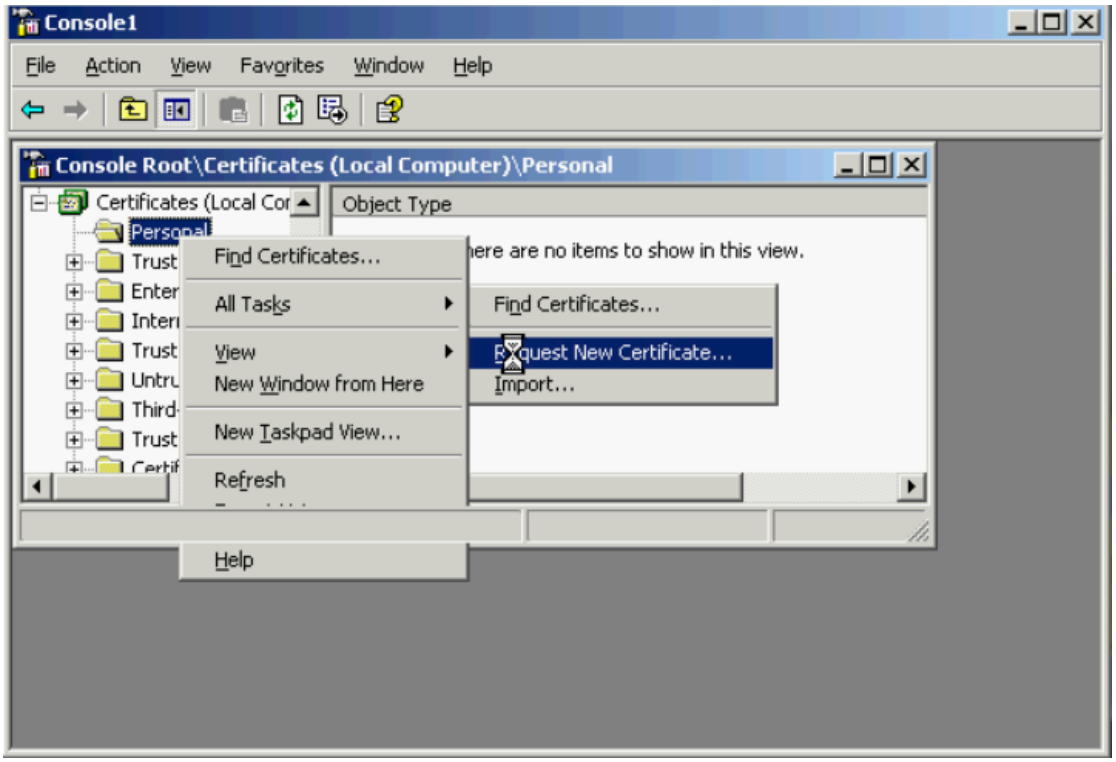
Vào Add/ Remove Snap-in…/ Add/ Cerfiticates

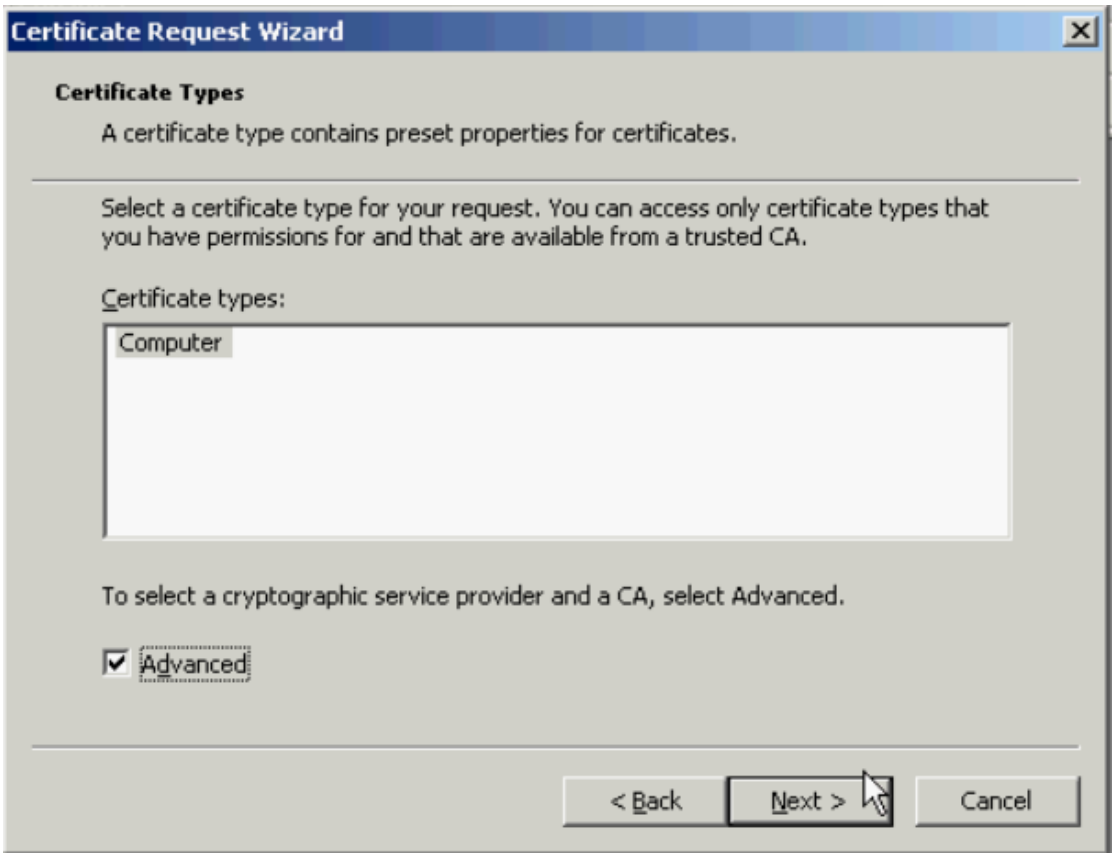


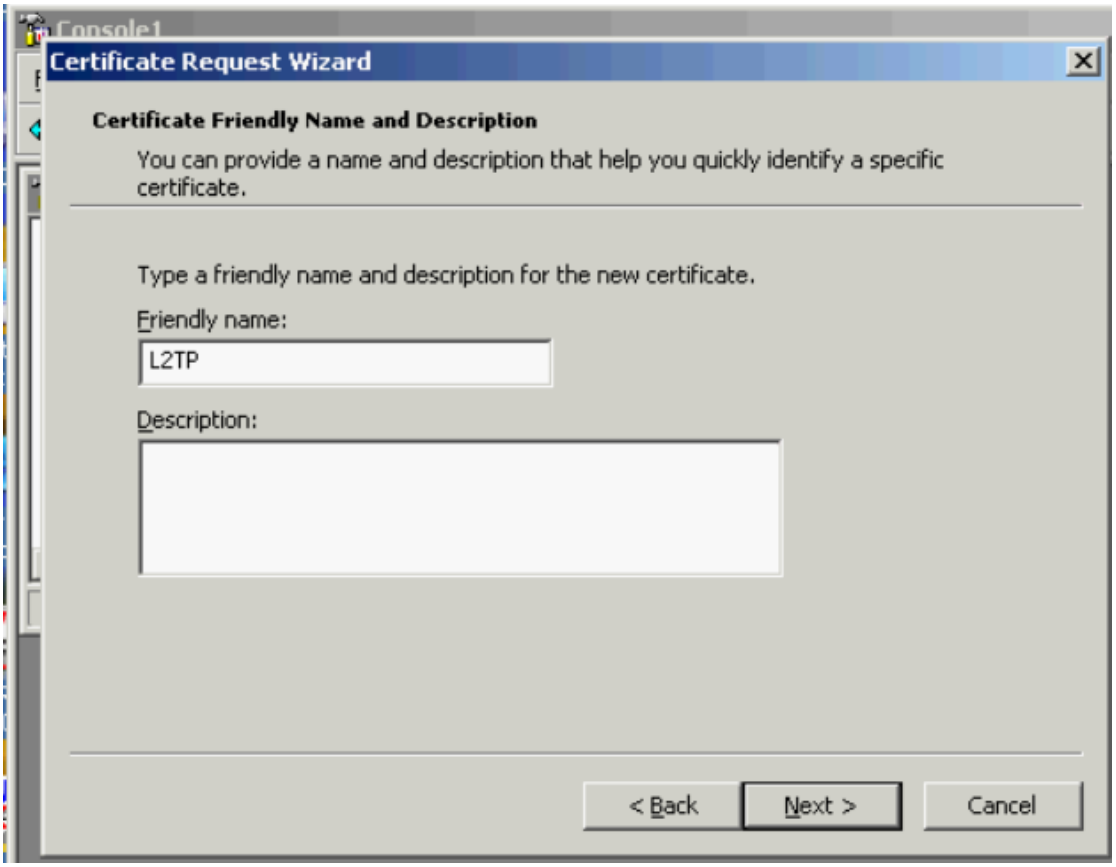
Chọn Computer account

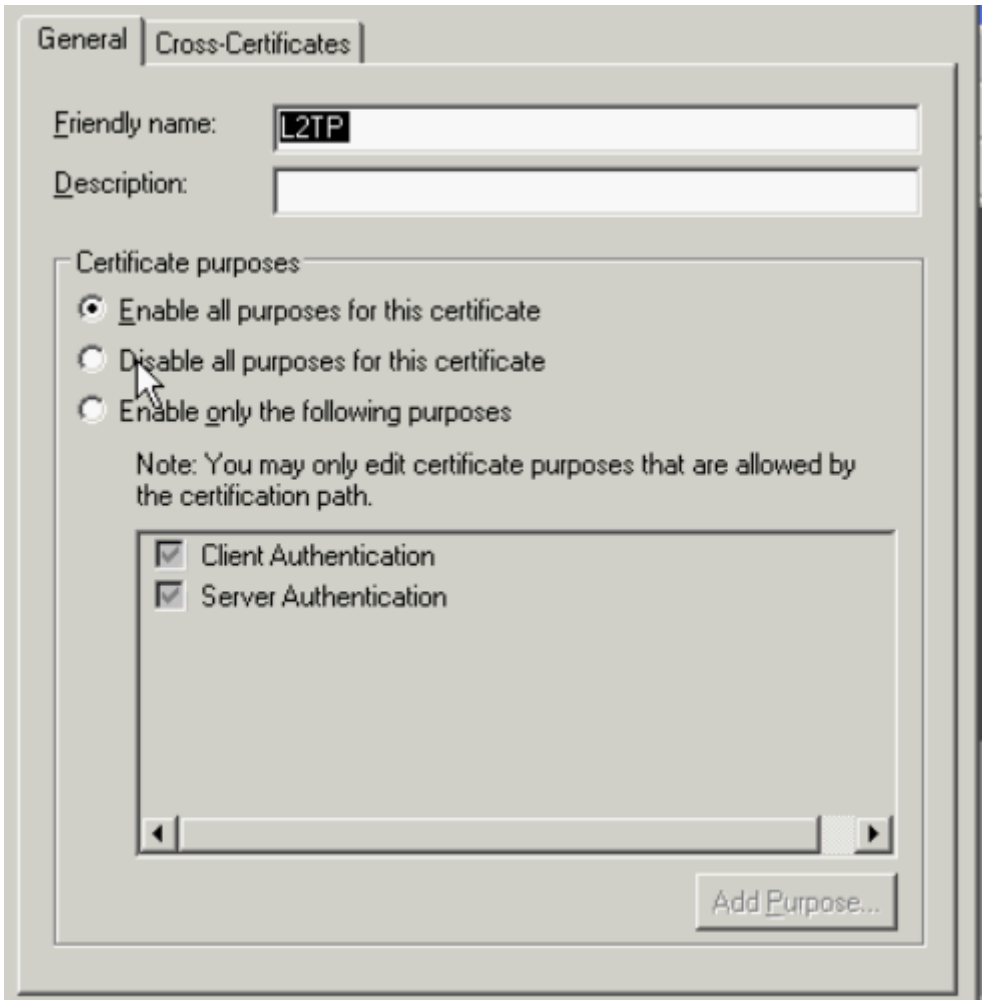


Chọn Personal/ All Tasks/ Request New Certificate…/ Next

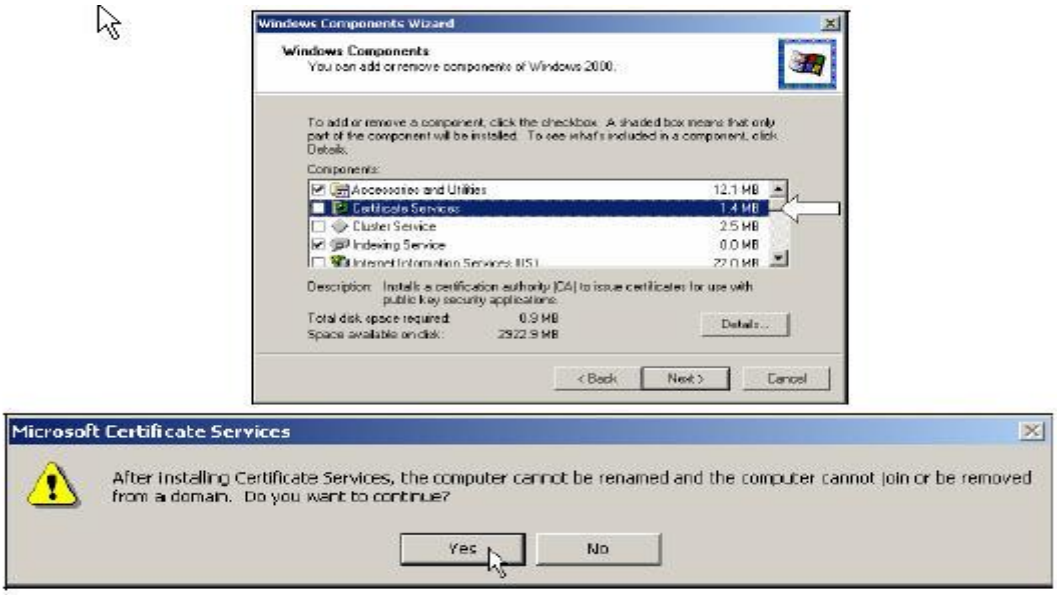


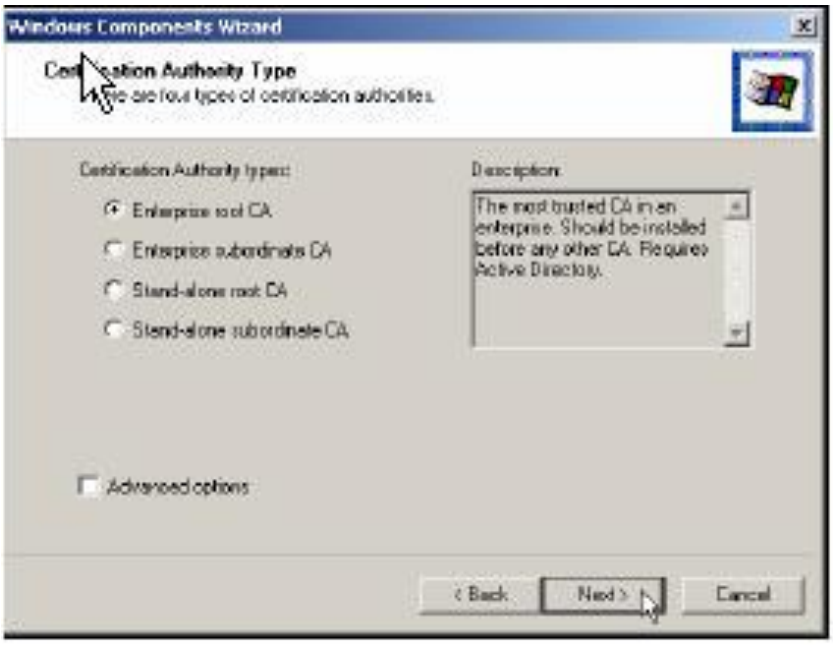

Certificate Request Wizard
Certificate Types
A certificate type contains preset properties for certificates.
Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.
Certificate types:
Computer
To select a cryptographic service provider and a CA, select Advanced.
Advanced
< Back
Next >
Cancel

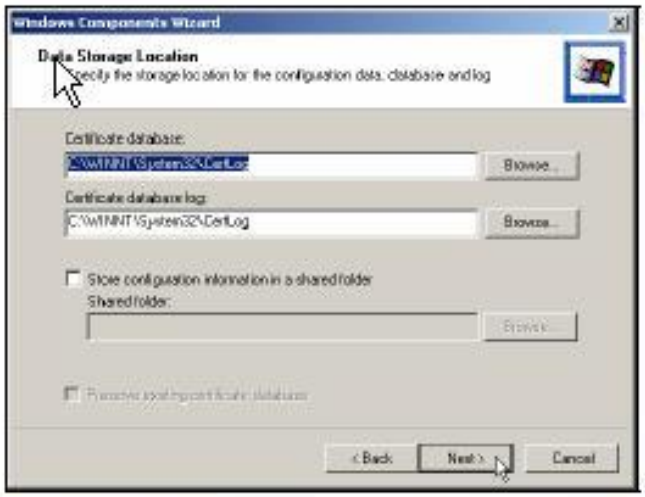

Console1
Certificate Request Wizard
Certificate Friendly Name and Description
You can provide a name and description that help you quickly identify a specific certificate.
Type a friendly name and description for the new certificate.
Friendly name:
L2TP
Description:
< Back
Next >
Cancel

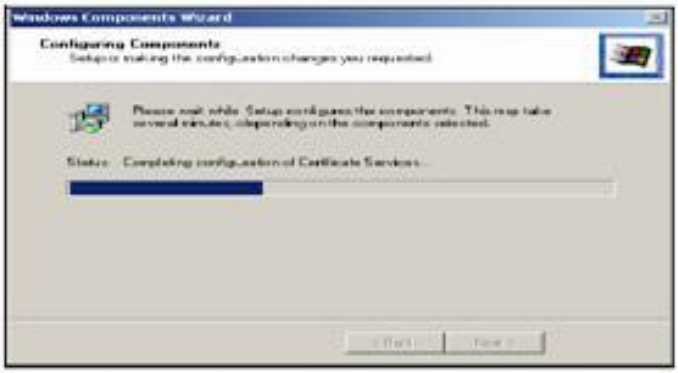


Cài đặt certificate service trên srv-11 thông qua add/remove program -> add / remove windows component, chúng ta sử dụng CA để cấp phát certificate cho domain cvntlip.com chọn chế độ cài đặt enterprise CA

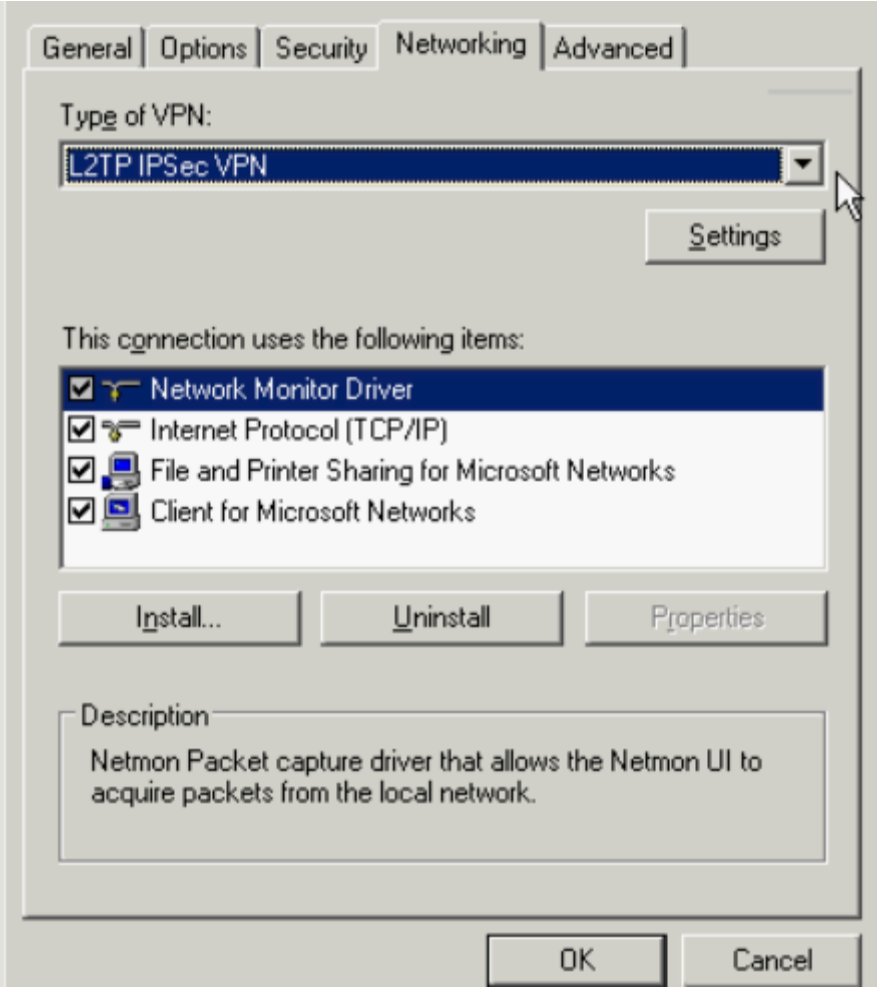


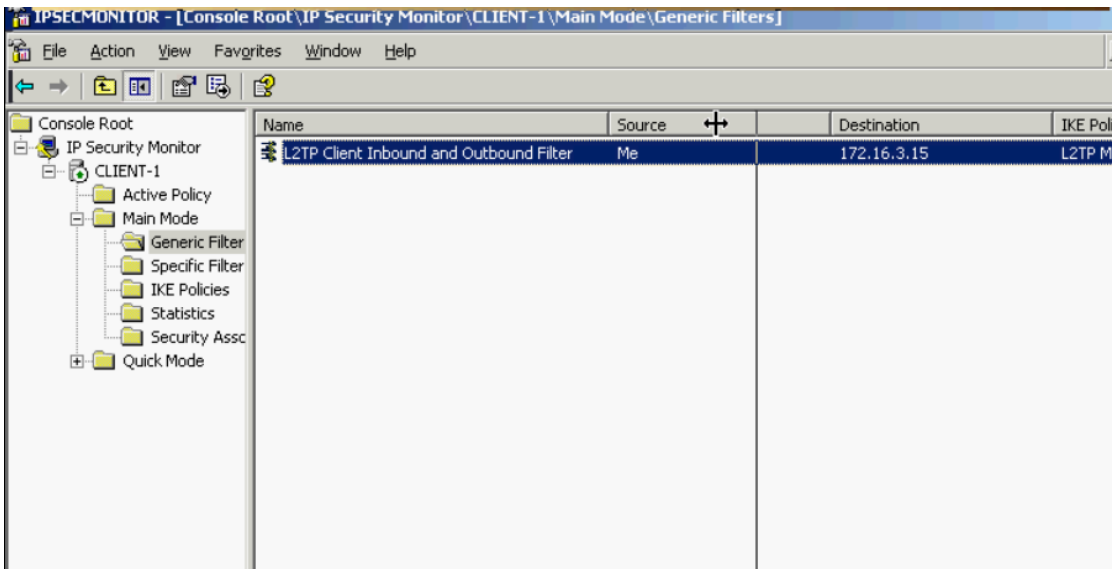


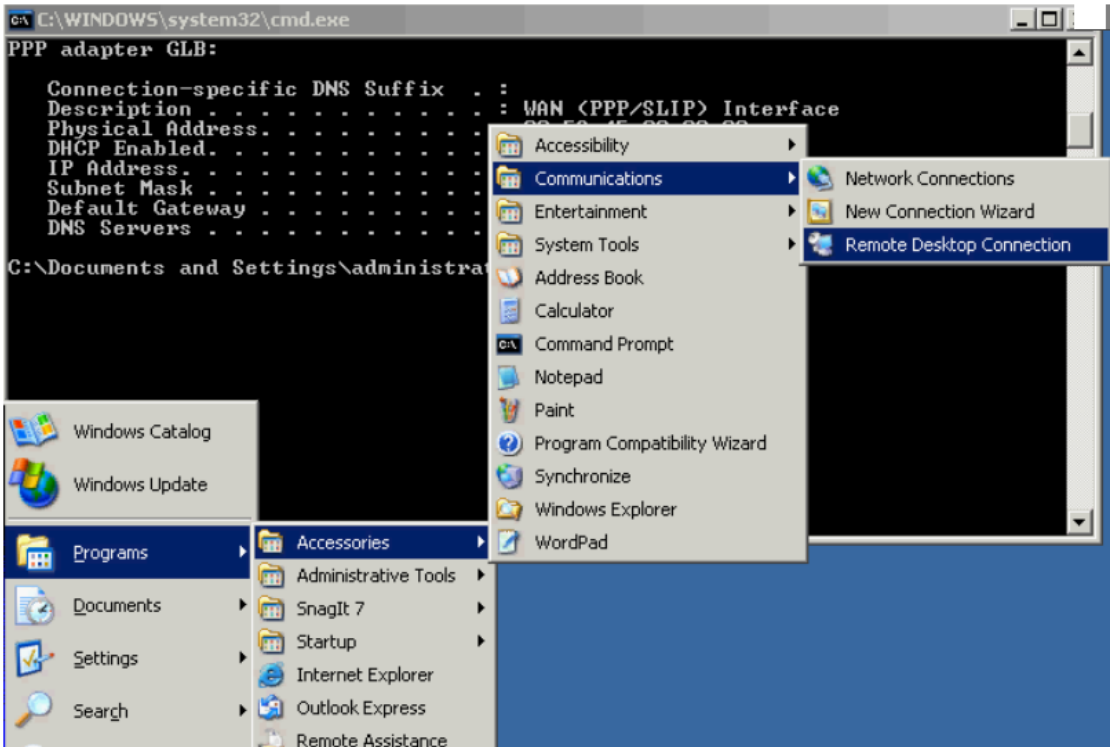


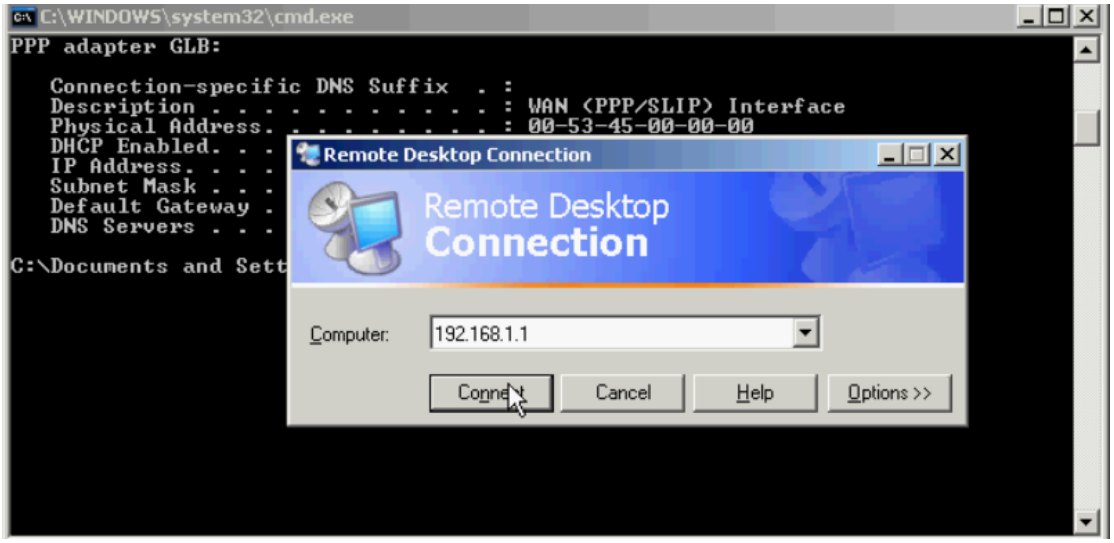


Bước 7: Thiết lập connection tới VPN server sử dụng giaô thức L2TP.

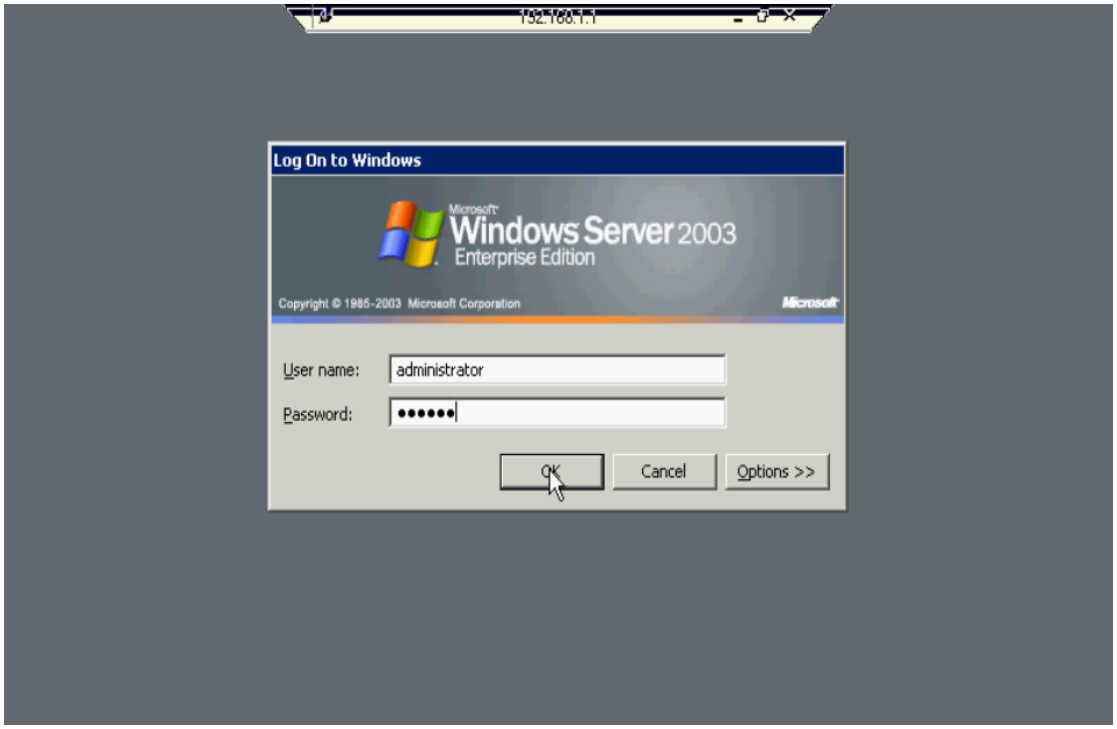

General
Options
Security
Networking
Advanced
Type of VPN:
L2TP IPSec VPN
Settings
This connection uses the following items:
Network Monitor Driver
Internet Protocol (TCP/IP)
File and Printer Sharing for Microsoft Networks
Client for Microsoft Networks
Install...
Uninstall
Properties
Description
Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network.
OK
Cancel


IPSECMONITOR - [Console Root\IP Security Monitor\CLIENT-1\Main Mode\Generic Filters]
File
Action
View
Favorites
Window
Help
Console Root
IP Security Monitor
CLIENT-1
Active Policy
Main Mode
Generic Filter
Specific Filter
IKE Policies
Statistics
Security Assc
Quick Mode
Name
Source
Destination
IKE Pol
L2TP Client Inbound and Outbound Filter
Me
172.16.3.15
L2TP M


C:\WINDOWS\system32\cmd.exe
PPP adapter GLB:
Connection-specific DNS Suffix . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . :
DHCP Enabled. . . . . :
IP Address. . . . . :
Subnet Mask . . . . . :
Default Gateway . . . . . :
DNS Servers . . . . . :
C:\Documents and Settings\administra
Windows Catalog
Windows Update
Programs
Documents
Settings
Search
Accessories
Administrative Tools
SnagIt 7
Startup
Internet Explorer
Outlook Express
Remote Assistance
Accessibility
Communications
Entertainment
System Tools
Address Book
Calculator
Command Prompt
Notepad
Paint
Program Compatibility Wizard
Synchronize
Windows Explorer
WordPad
Network Connections
New Connection Wizard
Remote Desktop Connection


C:\WINDOWS\system32\cmd.exe
PPP adapter GLB:
Connection-specific DNS Suffix . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
DHCP Enabled. . .
IP Address. . . .
Subnet Mask . . .
Default Gateway .
DNS Servers . . .
C:\Documents and Sett
Remote Desktop Connection
Remote Desktop
Connection
Computer:
192.168.1.1
Connect
Cancel
Help
Options >>

Nhập địa chỉ của Srv11(192.168.1.1)



Màn hình hiện ra như trên là thành công

CHƯƠNG V: BẢO MẬT TRONG VPN

5.1 TỔNG QUAN VỀ AN NINH MẠNG

5.1.1. An toàn mạng là gì?

Mục tiêu của việc kết nối mạng là để nhiều người sử dụng, từ những vị trí địa lý khác nhau có thể sử dụng chung tài nguyên, trao đổi thông tin với nhau. Do đặc điểm nhiều người sử dụng lại phân tán về mặt vật lý nên việc bảo vệ các tài nguyên thông tin trên mạng, tránh sự mất mát, xâm phạm là cần thiết và cấp bách. An toàn mạng có thể hiểu là cách bảo vệ, đảm bảo an toàn cho tất cả các thành phần mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên mạng được sử dụng tương ứng với một chính sách hoạt động được ấn định và chỉ với những người có thẩm quyền tương ứng.

An toàn mạng bao gồm:

- Xác định chính xác các khả năng, nguy cơ xâm phạm mạng, các sự cố rủi ro đối với thiết bị, dữ liệu trên mạng để có các giải pháp phù hợp đảm bảo an toàn mạng.
- Đánh giá nguy cơ tấn công của Hacker đến mạng, sự phát tán virus... Phải nhận thấy an toàn mạng là một trong những vấn đề cực kỳ quan trọng trong các hoạt động, giao dịch điện tử và trong việc khai thác sử dụng các tài nguyên mạng.

Một thách thức đối với an toàn mạng là xác định chính xác cấp độ an toàn cần thiết cho việc điều khiển hệ thống và các thành phần mạng. Đánh giá các nguy cơ, các lỗ hổng khiến mạng có thể bị xâm phạm thông qua cách tiếp cận có cấu trúc. Xác định những nguy cơ ăn cắp, phá hoại máy tính, thiết bị, nguy cơ virus, bọ gián điệp.., nguy cơ xoá, phá hoại CSDL, ăn cắp mật khẩu,... nguy cơ đối với sự hoạt động của hệ thống như nghẽn mạng, nhiễu điện tử...Khi đánh giá được hết những nguy cơ ảnh hưởng tới an ninh mạng thì mới có thể có được những biện pháp tốt nhất để đảm bảo an ninh mạng.

Sử dụng hiệu quả các công cụ bảo mật (ví dụ như Firewall ...) và những biện pháp, chính sách cụ thể chặt chẽ.

Về bản chất có thể phân loại các vi phạm thành hai loại vi phạm thụ động và vi phạm chủ động. Thụ động và chủ động được hiểu theo nghĩa có can thiệp vào nội dung và luồng thông tin có bị tráo đổi hay không. Vi phạm thụ động chỉ nhằm mục đích nắm bắt được thông tin. Vi phạm chủ động là thực hiện sự biến đổi, xoá bỏ hoặc thêm thông tin ngoại lai để làm sai lệch thông tin gốc nhằm mục đích phá hoại. Các hành động vi phạm thụ động thường khó có thể phát hiện nhưng có thể ngăn chặn hiệu quả. Trái lại vi phạm chủ động rất dễ phát hiện nhưng lại khó ngăn chặn.

5.1.2. Các đặc trưng kỹ thuật của an toàn mạng

1. Xác thực (Authentification): Kiểm tra tính xác thực của một thực thể giao tiếp trên mạng. Một thực thể có thể là một người sử dụng, một chương trình máy tính, hoặc một thiết bị phần cứng. Các hoạt động kiểm tra tính xác thực được đánh giá là quan trọng nhất trong các hoạt động của một phương thức bảo mật. Một hệ thống thông thường phải thực hiện kiểm tra tính xác thực của một thực thể trước khi thực thể đó thực hiện kết nối với hệ thống. Cơ chế kiểm tra tính xác thực của các phương thức bảo mật dựa vào 3 mô hình chính sau:

- Đối tượng cần kiểm tra cần phải cung cấp những thông tin trước, ví dụ như Password, hoặc mã số thông số cá nhân PIN (Personal Information Number).
- Kiểm tra dựa vào mô hình những thông tin đã có, đối tượng kiểm tra cần phải thể hiện những thông tin mà chúng sở hữu, ví dụ như Private Key, hoặc số thẻ tín dụng.
- Kiểm tra dựa vào mô hình những thông tin xác định tính duy nhất, đối tượng kiểm tra cần phải có những thông tin để định danh tính duy nhất của mình ví dụ như thông qua giọng nói, dấu vân tay, chữ ký ...

Có thể phân loại bảo mật trên VPN theo các cách sau: mật khẩu truyền thống hay mật khẩu một lần; xác thực thông qua các giao thức (PAP, CHAP, RADIUS…) hay phần cứng (các loại thẻ card: smart card, token card, PC card), nhận diện sinh trắc học (dấu vân tay, giọng nói, quét võng mạc...).

2. Tính khả dụng (Availability): Tính khả dụng là đặc tính mà thông tin trên mạng được các thực thể hợp pháp tiếp cận và sử dụng theo yêu cầu, khi cần thiết bất cứ khi nào, trong hoàn cảnh nào. Tính khả dụng nói chung dùng tỷ lệ giữa thời gian hệ thống được sử dụng bình thường với thời gian quá trình hoạt động để đánh giá. Tính khả dụng cần đáp ứng những yêu cầu sau: Nhận biết và phân biệt thực thể, khống chế tiếp cận (bao gồm cả việc khống chế tự tiếp cận và khống chế tiếp cận cưỡng bức), khống chế lưu lượng (chống tắc nghẽn..), khống chế chọn đường (cho phép chọn đường nhánh, mạch nối ổn định, tin cậy), giám sát tung tích (tất cả các sự kiện phát sinh trong hệ thống được lưu giữ để phân tích nguyên nhân, kịp thời dùng các biện pháp tương ứng).

3. Tính bảo mật (Confidentialy): Tính bảo mật là đặc tính tin tức không bị tiết lộ cho các thực thể hay quá trình không được uỷ quyền biết hoặc không để cho các đối tượng đó lợi dụng. Thông tin chỉ cho phép thực thể được uỷ quyền sử dụng. Kỹ thuật bảo mật thường là phòng ngừa dò la thu thập (làm cho đối thủ không thể dò la thu thập được thông tin), phòng ngừa bức xạ (phòng ngừa những tin tức bị bức xạ ra ngoài bằng nhiều đường khác nhau), tăng cường bảo mật thông tin (dưới sự khống chế của khoá mật mã), bảo mật vật lý (sử dụng các phương pháp vật lý để đảm bảo tin tức không bị tiết lộ).

4. Tính toàn vẹn (Integrity): Là đặc tính khi thông tin trên mạng chưa được uỷ quyền thì không thể tiến hành biến đổi được, tức là thông tin trên mạng khi đang lưu giữ hoặc trong quá trình truyền dẫn đảm bảo không bị xoá bỏ, sửa đổi, giả mạo, làm rối loạn trật tự, phát lại, xen vào một cách ngẫu nhiên hoặc cố ý và những sự phá hoại khác. Những nhân tố chủ yếu ảnh hưởng tới sự toàn vẹn thông tin trên mạng gồm: sự cố thiết bị, sai mã, bị tác động của con người, virus máy tính…

Một số phương pháp bảo đảm tính toàn vẹn thông tin trên mạng:

- Giao thức an toàn có thể kiểm tra thông tin bị sao chép, sửa đổi. Nếu phát hiện thì thông tin đó sẽ bị vô hiệu hoá.
- Phương pháp phát hiện sai và sửa sai. Phương pháp sửa sai mã hoá đơn giản nhất và thường dùng là phép kiểm tra chẵn - lẻ.
- Biện pháp kiểm tra mật mã ngăn ngừa hành vi xuyên tạc và cản trở truyền tin.
- Chữ ký điện tử: bảo đảm tính xác thực của thông tin.
- Yêu cầu cơ quan quản lý hoặc trung gian chứng minh tính chân thực của thông tin.

5. Tính khống chế (Accountlability): Là đặc tính về năng lực khống chế truyền bá và nội dung vốn có của tin tức trên mạng.

6. Tính không thể chối cãi (Nonreputation): Trong quá trình giao lưu tin tức trên mạng, xác nhận tính chân thực đồng nhất của những thực thể tham gia, tức là tất cả các thực thể tham gia không thể chối bỏ hoặc phủ nhận những thao tác và cam kết đã được thực hiện.

5.1.3. Các lỗ hổng và điểm yếu của mạng

1. Các lỗ hổng bảo mật hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền đối với người sử dụng hoặc cho phép các truy nhập không hợp pháp vào hệ thống. Các lỗ hổng tồn tại trong các dịch vụ như Sendmail, Web, Ftp ... và trong hệ điều hành mạng như trong Windows NT, Windows 95, UNIX; hoặc trong các ứng dụng. Các loại lỗ hổng bảo mật trên một hệ thống được chia như sau:

Lỗ hổng loại C: cho phép thực hiện các phương thức tấn công theo kiểu từ chối dịch vụ DoS (Dinal of Services). Mức nguy hiểm thấp, chỉ ảnh hưởng chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống, không phá hỏng dữ liệu hoặc chiếm quyền truy nhập.

Lổ hổng loại B: cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Mức độ nguy hiểm trung bình, những lỗ hổng này thường có trong các ứng dụng trên hệ thống, có thể dẫn đến lộ thông tin yêu cầu bảo mật.

Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

2. Các phương thức tấn công mạng:

Kẻ phá hoại có thể lợi dụng những lỗ hổng trên để tạo ra những lỗ hổng khác tạo thành một chuỗi những lỗ hổng mới. Để xâm nhập vào hệ thống, kẻ phá hoại sẽ tìm ra các lỗ hổng trên hệ thống, hoặc từ các chính sách bảo mật, hoặc sử dụng các công cụ dò xét (như SATAN, ISS) để đạt được quyền truy nhập. Sau khi xâm nhập, kẻ phá hoại có thể tiếp tục tìm hiểu các dịch vụ trên hệ thống, nắm bắt được các điểm yếu và thực hiện các hành động phá hoại tinh vi hơn.

5.2 MỘT SỐ PHƯƠNG THỨC TẤN CÔNG MẠNG PHỔ BIẾN

5.2.1. Scanner:

Kẻ phá hoại sử dụng chương trình Scanner tự động rà soát và có thể phát hiện ra những điểm yếu lỗ hổng về bảo mật trên một server ở xa. Scanner là một chương trình trên một trạm làm việc tại cục bộ hoặc trên một trạm ở xa.

Các chương trình Scanner có thể rà soát và phát hiện các số hiệu cổng (Port) sử dụng trong giao thức TCP/UDP của tầng vận chuyển và phát hiện những dịch vụ sử dụng trên hệ thống đó, nó ghi lại những đáp ứng (Response) của hệ thống ở xa tương ứng với các dịch vụ mà nó phát hiện ra. Dựa vào những thông tin này, những kẻ tấn công có thể tìm ra những điểm yếu trên hệ thống .

Các chương trình Scanner cung cấp thông tin về khả năng bảo mật yếu kém của một hệ thống mạng. Những thông tin này là hết sức hữu ích và cần thiết đối với người quản trị mạng, nhưng hết sức nguy hiểm khi những kẻ phá hoại có những thông tin này.

5.2.2 Bẻ khóa (Password Cracker)

Chương trình bẻ khoá Password là chương trình có khả năng giải mã một mật khẩu đã được mã hoá hoặc có thể vô hiệu hoá chức năng bảo vệ mật khẩu của một hệ thống. Hầu hết việc mã hoá các mật khẩu được tạo ra từ một phương thức mã hoá. Các chương trình mã hoá sử dụng các thuật toán mã hoá để mã hoá mật khẩu. Có thể thay thế phá khoá trên một hệ thống phân tán, đơn giản hơn so với việc phá khoá trên một Server cục bộ.

Một danh sách các từ được tạo ra và thực hiện mã hoá từng từ. Sau mỗi lần mã hoá, sẽ so sánh với mật khẩu (Password) đã mã hoá cần phá. Nếu không trùng hợp, quá trình lại quay lại. Phương thức bẻ khoá này gọi là Bruce-Force. Phương pháp này tuy không chuẩn tắc nhưng thực hiện nhanh vì dựa vào nguyên tắc khi đặt mật khẩu người sử dụng cũng thường tuân theo một số qui tắc để thuận tiện khi sử dụng.

Thông thường các chương trình phá khoá thường kết hợp một số thông tin khác trong quá trình dò mật khẩu như: thông tin trong tập tin /etc/passwd, từ điển và sử dụng các từ lặp các từ liệt kê tuần tự, chuyển đổi cách phát âm của một từ ...

Biện pháp khắc phục là cần xây dựng một chính sách bảo vệ mật khẩu đúng đắn.

5.2.3 Trojans

Một chương trình Trojans chạy không hợp lệ trên một hệ thống với vai trò như một chương trình hợp pháp. Nó thực hiện các chức năng không hợp pháp. Thông thường, Trojans có thể chạy được là do các chương trình hợp pháp đã bị thay đổi mã bằng những mã bất hợp pháp. Virus là một loại điển hình của các chương trình Trojans, vì các chương trình virus che dấu các đoạn mã trong những chương trình sử dụng hợp pháp. Khi chương trình hoạt động thì những đoạn mã ẩn sẽ thực hiện một số chức năng mà người sử dụng không biết.

Trojan có nhiều loại khác nhau. Có thể là chương trình thực hiện chức năng ẩn dấu, có thể là một tiện ích tạo chỉ mục cho file trong thư mục, hoặc một đoạn mã phá khoá, hoặc có thể là một chương trình xử lý văn bản hoặc một tiện ích mạng...

Trojan có thể lây lan trên nhiều môi trường hệ điều hành khác nhau. Đặc biệt thường lây lan qua một số dịch vụ phổ biến như Mail, FTP... hoặc qua các tiện ích, chương trình miễn phí trên mạng Internet. Hầu hết các chương trình FTP Server đang sử dụng là những phiên bản cũ, có nguy cơ tiềm tàng lây lan Trojans.

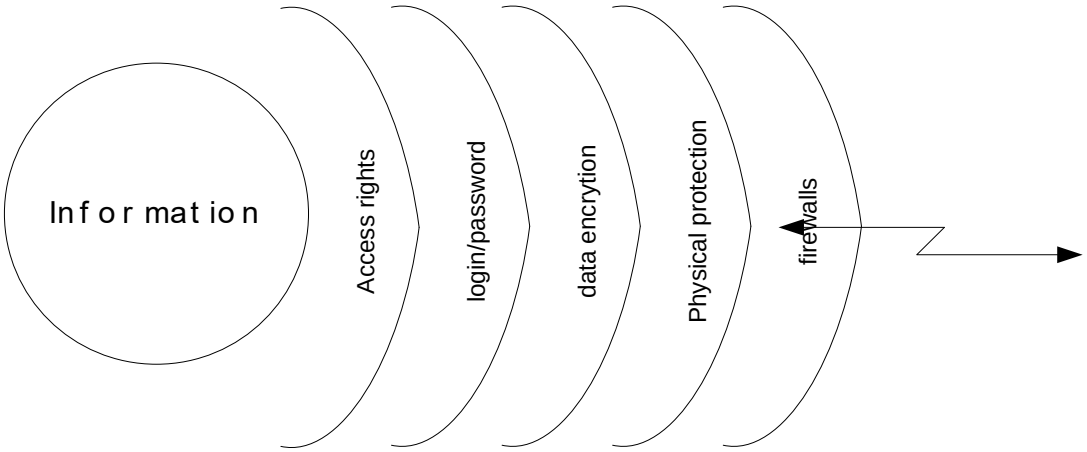
Đánh giá mức độ phá hoại của Trojans là hết sức khó khăn. Trong một số trường hợp, nó chỉ làm ảnh hưởng đến các truy nhập của người sử dụng. Nghiêm trọng hơn, nó là những kẻ tấn công lỗ hổng bảo mật mạng. Khi kẻ tấn công chiếm được quyền Root trên hệ thống, nó có thể phá huỷ toàn bộ hoặc một phần của hệ thống. Chúng sử dụng các quyền Root để thay đổi logfile, cài đặt các chương trình Trojans khác mà người quản trị không thể phát hiện được và người quản trị hệ thống đó chỉ còn cách là cài đặt lại toàn bộ hệ thống

5.2.4 Sniffer:

Sniffer theo nghĩa đen là “đánh hơi” hoặc “ngửi”. Là các công cụ (có thể là phần cứng hoặc phần mềm) “tóm tắt” các thông tin lưu chuyển trên mạng để “đánh hơi” những thông tin có giá trị trao đổi trên mạng. Hoạt động của Sniffer cũng giống như các chương trình "tóm bắt" các thông tin gõ từ bàn phím (Key Capture). Tuy nhiên các tiện ích Key Capture chỉ thực hiện trên một trạm làm việc cụ thể, Sniffer có thể bắt được các thông tin trao đổi giữa nhiều trạm làm việc với nhau. Các chương trình Sniffer hoặc các thiết bị Sniffer có thể ”ngửi” các giao thức TCP, UDP, IPX .. ở tầng mạng. Vì vậy nó có thể tóm bắt các gói tin IP Datagram và Ethernet Packet. Mặt khác, giao thức ở tầng IP được định nghĩa tường minh và cấu trúc các trường Header rõ ràng, nên việc giải mã các gói tin không khó khăn lắm.

Mục đích của các chương trình Sniffer là thiết lập chế độ dùng chung (Promiscuous) trên các Card mạng Ethernet, nơi các gói tin trao đổi và "tóm bắt" các gói tin tại đây.

5.3 Các mức bảo vệ an toàn mạng



Hình 5.1. Các lớp bảo vệ

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng đồng thời nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với các hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các máy tính, đặc biệt là trong các server của mạng

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiện nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp.
- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải có đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiệm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác tuỳ theo thời gian và không gian.
- Lớp thứ ba là sử dụng các phương pháp mã hoá (encryption). Dữ liệu được biến đổi từ dạng "đọc được" sang dạng “không đọc được" theo một thuật toán nào đó. Chúng ta sẽ xem xét các phương thức và các thuật toán mã hoá hiện được sử dụng phổ biến ở phần dưới đây.
- Lớp thứ tư là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập vật lý bất hợp pháp vào hệ thống. Thường dùng các biện pháp truyền thống

như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khoá trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống ...

➢ Lớp thứ năm: Cài đặt các hệ thống bức tường lửa (firewall), nhằm ngăn chặn các thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó.

5.4 Các kỹ thuật bảo mật trong VPN

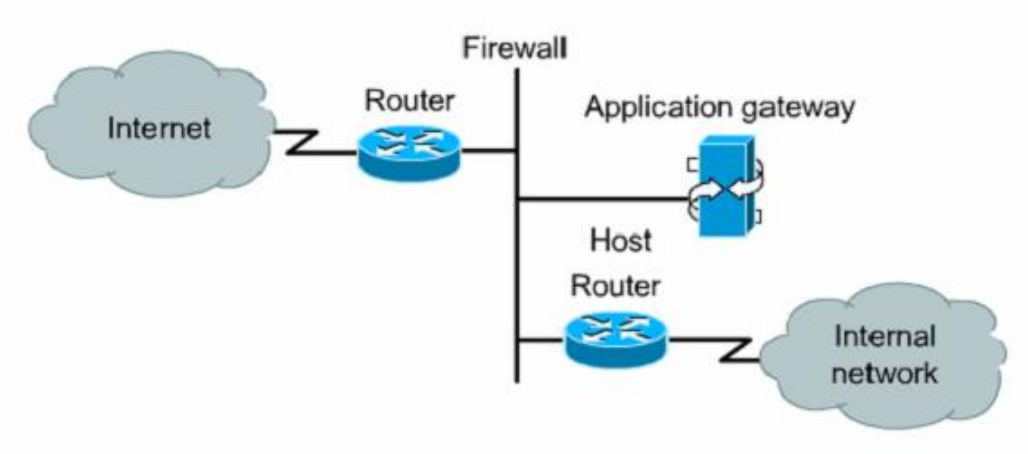
VPNs sử dụng một vài kỹ thuật để bảo vệ dữ liệu truyền qua mạng Internet . Những khái niệm quan trọng nhất là firewalls (tường lửa) , nhận thực, mã hoá và tunneling

5.4.1. Firewalls

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Cũng có thể hiểu Firewall là một cơ chế (mechanism) để bảo vệ mạng tin t-ưởng (Trusted network) khỏi các mạng không tin tưởng (Untrusted network).

Thông thường Firewall được đặt giữa mạng bên trong (Intranet) của một công ty, tổ chức, ngành hay một quốc gia, và Internet. Vai trò chính là bảo mật thông tin, ngăn chặn sự truy nhập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) tới một số địa chỉ nhất định trên Internet.

Một tường lửa Internet sử dụng các kỹ thuật ví dụ như kiểm tra địa chỉ Internet của các gói dữ liệu hoặc các cổng truy nhập mà các kết nối yêu cầu để quyết định truy nhập đó có được phép hay không



Hình 5.2. Firewall

Firewalls cung cấp hai chức năng chính cho nhà quản trị mạng. Thứ nhất là chức năng kiểm soát những gì mà người dùng từ mạng ngoài có thể nhìn thấy được và những dịch vụ nào được cho phép sử dụng ở mạng nội bộ. Thứ hai là kiểm soát những nơi nào, dịch vụ nào của Internet mà một user trong mạng nội bộ có thể được truy cập, được sử dụng.

Hầu hết các kỹ thuật tường lửa đều được thiết kết tương tự nhau là có một điểm điều khiển tập trung, do đó chỉ cần khảo sát một số biến đổi ở mức cao nhất là đủ

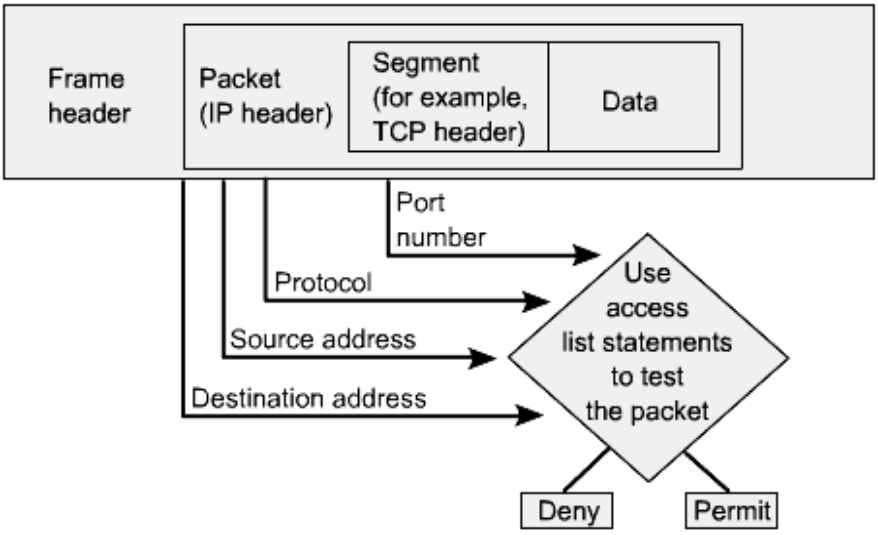
5.4.1.1. Router lọc gói dữ liệu (Packets Filtering Router)

Các router mà có nhiệm vụ lọc gói dữ liệu sẽ lựa chọn để gửi dữ liệu tới một mạng nào đó dựa vào một bảng gồm các luật đã được xác định trước. Router không quyết định dựa trên thông tin dữ liệu của gói dữ liệu mà chỉ quan tâm là gói đó đến từ đâu và đích đến của nó là gì, tức là nó chỉ quan tâm đến phần thông tin tiêu đề TCP/IP. Nếu gói đó phù hợp với một hoặc một tập hợp các luật thì router sẽ thực hiện tương ứng là cho phép đi qua hay không.

Bảng các luật ở đây chính là các danh sách điều khiển truy cập - ACL (Access Control List). Những danh sách này chỉ cho Router biết các kiểu của các gói dữ liệu nào được chấp nhận “permit” hoặc loại bỏ “deny”. Việc chấp nhận hay loại bỏ dựa trên các điều kiện được chỉ ra. Các ACL giúp quản lý lưu lượng và bảo mật truy cập tới và từ một mạng.

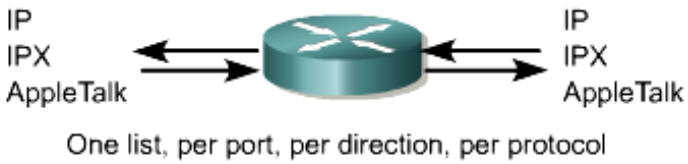
Các ACL có thể được tạo ra cho tất cả các giao thức mạng có khả năng định tuyến, như là IP, IPX. Các ACL có thể được cấu hình ở Router để điều khiển truy cập tới một mạng hay một mạng con.

Các ACL lọc lưu lượng mạng bằng cách điều khiển cho phép hay không cho phép các gói dữ liệu được chuyển đi hay chặn lại ở cổng của Router. Router kiểm tra mỗi gói dữ liệu để xác định có hay không chuyển hay huỷ nó, trên cơ sở các điều kiện được chỉ ra trong ACL. Cơ sở để cho phép hay huỷ bỏ có thể là địa chỉ IP nguồn, đích, các giao thức, số hiệu các cổng ở lớp trên.



Hình 5.3. Các thông số của ACL

Để điều khiển luồng lưu lượng trên mỗi một cổng, một ACL cần được định nghĩa cho mỗi giao thức được sử dụng trên mỗi cổng. Một ACL riêng biệt cần được tạo cho mỗi hướng, một cho một lối vào, và một cho một lối ra. Cuối cùng mọi cổng có thể có nhiều giao thức và nhiều hướng được định nghĩa. Nếu Router có hai cổng được cấu hình cho IP, IPX, và Apple Talk thì phải cần định nghĩa 12 ACL riêng biệt.



Hình 5.4. Vị trí của các ACL

Chức năng của các ACL

➢ Giới hạn lưu lượng mạng và tăng hiệu suất của mạng.

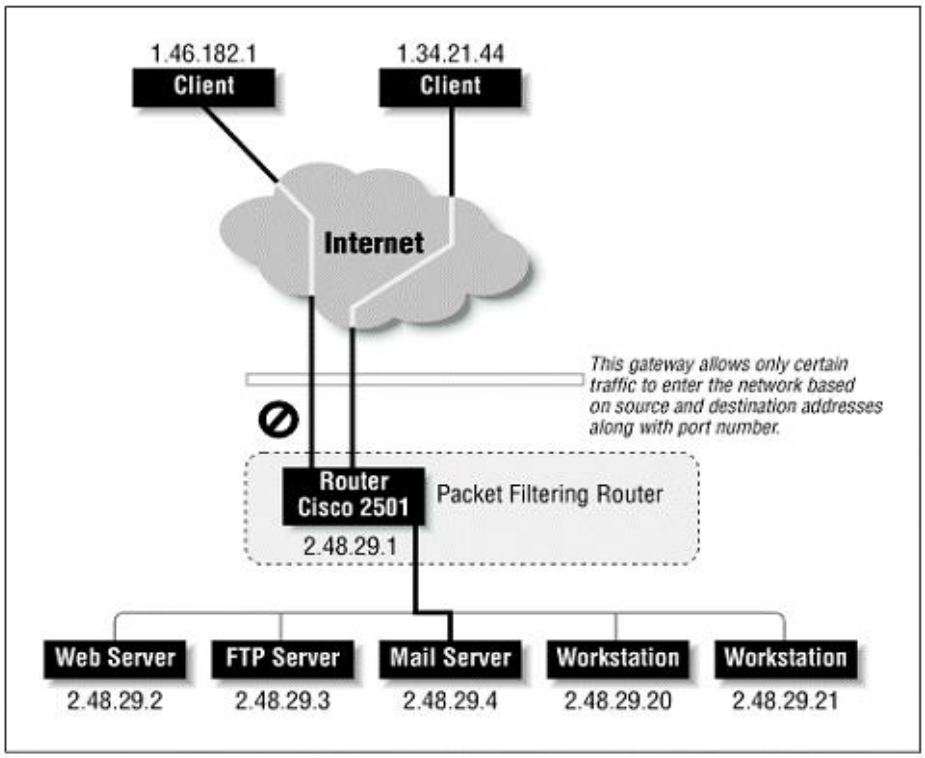
➢ Điều khiển luồng lưu lượng. Các ACL có thể loại bỏ việc trao đổi các bản tin cập nhật định tuyến nếu các bản tin này là không được yêu cầu.

➢ Cung cấp một mức cơ bản của bảo mật cho truy cập mạng. Các ACL có thể cho phép một máy truy cập đến một phần của mạng và ngăn cản các máy khác truy cập đến phần mạng đó.

➢ Quyết định các kiểu lưu lượng nào được chuyển hay bị huỷ trên các cổng của Router.

Một ví dụ như ở hình dưới đây. Nếu một router được yêu cầu cho phép tất cả các traffic từ mạng 1.34.21.0/24, nó sẽ kiểm tra tất cả các gói dữ liệu xem gói

nào có địa chỉ nguồn phù hợp với địa chỉ đó thì sẽ cho phép đi qua, còn các gói thuộc mạng khác sẽ bị huỷ bỏ.



Hình 5.5. Packet filtering Router

5.4.1.2. Bastion host

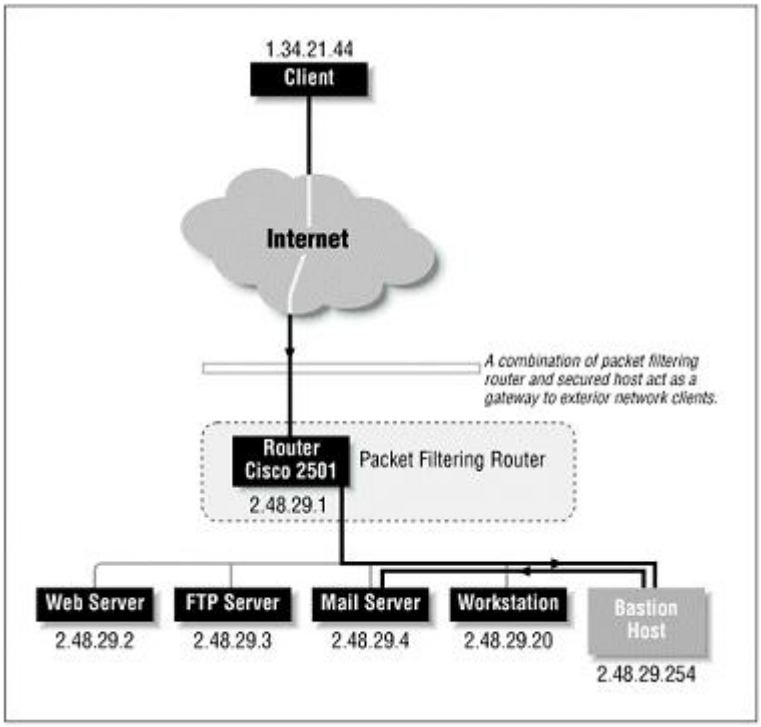
Đây là một host vừa có chức năng bảo mật lại vừa có chức năng lọc gói dữ liệu của một router, hệ điều hành và những dịch vụ quan trọng của nó được cài đặt một chương trình bảo mật chuyên dụng. Nhiệm vụ bảo mật thực hiện chủ yếu bởi router và host bảo mật được sử dụng để thực thi các luồng dữ liệu theo một trong hai chiều Bastion host thường đi cùng với router lọc bởi vì hệ thống lọc gói dữ liệu đơn giản không thể lọc các loại giao thức hay lớp ứng dụng. Việc cấu hình và bảo trì khá dễ dàng vì nhóm các traffic được gửi tới chỉ một hệ thống (mail server hay ftp server….)

Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đảm bảo sự tích hợp firewall.
Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị

tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.

Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ nh user password hay smart card.

Tuy nhiên phương pháp điều khiển tập trung này trở nên bất tiện khi sử dụng trong một mạng lớn bởi vì sẽ cần nhiều bastion host, thậm chí sẽ cần phải có hẳn một mạng bastion host ngoại vi để tránh xung đột.



Hình 5.6. Bastion host

5.4.1.3. Proxy server

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service. Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn đề

Ưu điểm

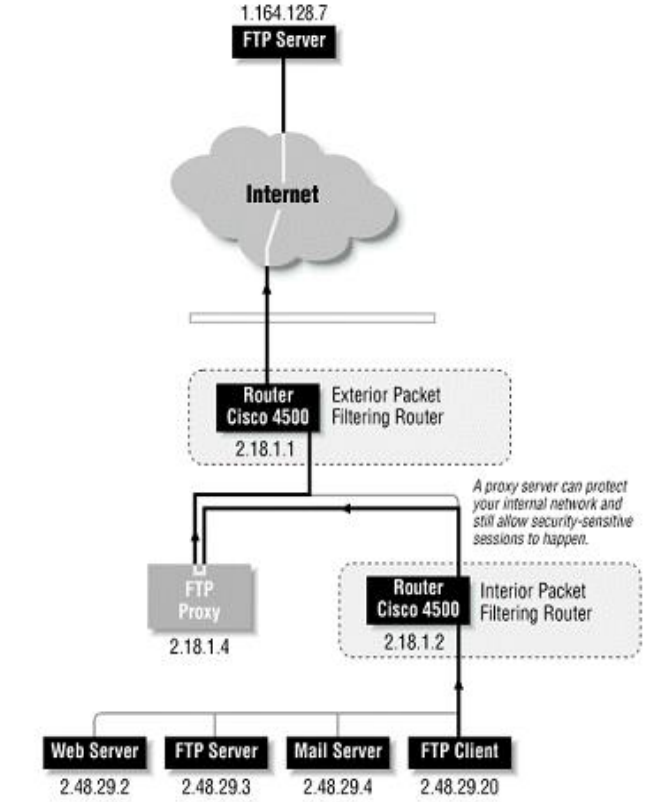
Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.

Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.

Luật lệ lọc filltering cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

Hạn chế

Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một . Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet khác.



Hình 5.7. Proxy server

5.4.2. Authentication (nhận thực)

Authentication đóng vai trò quan trọng đối với VPNs, phương pháp này đảm bảo các bên tham gia truyền tin trao đổi dữ liệu với đúng người, đúng host. Authentication cũng tương tự như "logging in" vào một hệ thống với username và password, tuy nhiên VPNs yêu cầu các phương pháp nhận thực chặt chẽ, nghiêm ngặt hơn rất nhiều để xác nhận tính hợp lệ. Hầu hết các hệ thống nhận thực VPN đều dựa trên hệ thống khoá bảo mật chung, các khoá được đưa vào thuật toán băm để tạo ra các giá trị băm. Để có quyền truy nhập thì giá trị băm của bên yêu cầu phải trùng với giá trị băm được phép tại đích. Các giá trị băm này không nhìn thấy được khi truyền qua Internet do đó việc ăn cắp password là không thể. Một số phương pháp nhận thực thông dụng là CHAP, RSA

Authentication thường được thực hiện khi bắt đầu phiên truy cập, và sau đó lại được thực hiện ngẫu nhiên tại thời điểm nào đó trong suốt thời gian của phiên đó để đảm bảo chắc chắn rằng không có kẻ mạo danh nào thâm nhập trái phép. Ngoài ra authentication cũng có thể được sử dụng để đảm bảo sự nguyên vẹn của dữ liệu. Bản thân dữ liệu cũng được đưa vào hàm băm để thu được giá trị băm và nó được gửi đi cùng dữ liệu, tương tự như checksum của một bản tin. Bất kỳ sự sai khác nào giữa giá trị được gửi đi với giá trị nhận được tại các trạm kế tiếp thì điều đó có nghĩa là dữ liệu đã bị phá huỷ ,bị chặn trong quá trình truyền tin hoặc dữ liệu đã bị thay đổi trên đường truyền.

5.4.3. Encryption (mã hoá)

Encryption được sử dụng để chắc chắn rằng bản tin không bị đọc bởi bất kỳ ai nhưng có thể đọc được bởi người nhận. Khi mà càng có nhiều thông tin lưu thông trên mạng thì sự cần thiết đối với việc mã hoá thông tin càng trở nên quan trọng. Mã hoá sẽ biến đổi nội dung thông tin thành trong một văn bản mật mã mà là vô nghĩa trong dạng mật mã của nó. Chức năng giải mã để khôi phục văn bản mật mã thành nội dung thông tin có thể dùng được cho người nhận

Quá trình này mật mã dữ liệu khi truyền đi khỏi máy tính theo một quy tắc nhất định và một máy được phép từ xa có thể giải mã được. Hầu hết các hệ thống mã hoá máy tính thuộc về một trong hai loại sau:

- Mã hoá sử dụng khoá riêng (Symmetric-key encryption)
- Mã hoá sử dụng khoá công khai (Public-key encryption)

Trong hệ symmetric-key encryption, mỗi máy tính có một mã bí mật sử dụng để mã hoá các gói tin trước khi truyền đi. Khoá riêng này cần được cài trên mỗi máy tính có trao đổi thông tin sử dụng mã hoá riêng và máy tính phải biết được trình tự giả mã đã được quy ước trước. Ví dụ: Bạn tạo ra một bức thư mã hoá mà trong nội dung thư mỗi ký tự được thay thế bằng ký tự ở sau nó 2 vị trí trong bảng ký tự . Như vậy A sẽ được thay bằng C, và B sẽ được thay bằng D. Bạn đã nói với người bạn khoá riêng là Dịch đi 2 vị trí (Shift by 2). Bạn của bạn nhận được thư sẽ giải mã sử dụng chìa khoá riêng đó. Còn những người khác sẽ không đọc được nội dung thư. *(symetric key), sau đó sử dụng khoá bí mật này để giải mã dữ liệu*

Hệ Public-key encryption sử dụng một tổ hợp khoá riêng và khoá công cộng để thực hiện mã hoá, giải mã. Khoá riêng chỉ sử dụng tại máy tính đó, còn khoá công cộng được truyền đi đến các máy tính khác mà nó muốn trao đổi thông tin bảo mật. Để giải mã dữ liệu mã hoá, máy tính kia phải sử dụng khoá công cộng nhận được, và khoá riêng của chính nó.

5.4.4 Đường hầm (Tunnel)

Cung cấp các kết nối logic, điểm tới điểm qua mạng IP không hướng kết nối. Điều này giúp cho việc sử dụng các ưu điểm các tính năng bảo mật. Các giải pháp đường hầm cho VPN là sử dụng sự mã hoá để bảo vệ dữ liệu không bị xem trộm bởi bất cứ những ai không được phép và để thực hiện đóng gói đa giao thức nếu cần thiết. Mã hoá được sử dụng để tạo kết nối đường hầm để dữ liệu chỉ có thể được đọc bởi người nhận và người gửi.

CHƯƠNG VI: KẾT LUẬN

Công nghệ mạng riêng ảo VPN (Virtual Private Network) là một công nghệ tương đối mới, việc nghiên cứu và triển khai các loại mạng VPN đòi hỏi nhiều thời gian và công sức.

Trong bản đồ án này, chúng tôi đã trình bày những khái niệm cơ bản nhất về VPN, vấn đề bảo mật hệ thống, nghiên cứu một cách kỹ lưỡng cơ sở lý thuyết

Trong phần thực nghiệm của đồ án, chúng tôi đã xây dựng và cấu hình thành công mạng VPN **Client to site**.

Trong một khoảng thời gian ngắn, chúng tôi không thể tránh khỏi những sai sót, chúng tôi xin chân thành cảm ơn thầy cô đặc biệt là thầy Nguyễn Trung Phú, bạn bè, đồng nghiệp đã giúp đỡ, góp ý chúng tôi hoàn thành đồ án này.

TÀI LIỆU THAM KHẢO

[1]. Quản trị mạng và ứng dụng của Active Directory, tác giả K/S Ngọc Tuấn NXB Thống kê năm 2004

[2]. Mạng truyền thông công nghiệp, tác giả Hoàng Minh Sơn, NXB Khoa học kỹ thuật năm 2004

[3]. 100 thủ thuật bảo mật mạng, tác giả K/S Nguyễn Ngọc Tuấn, Hồng Phúc NXB Giao thông vận tải, năm 2005

[4]. TS Nguyễn Tiến Ban và Thạc sĩ Hoàng Trọng Minh, "Mạng riêng ảo VPN", 2007.

[5]. PGS-TS.Nguyễn Văn Tam - Giáo trình An toàn mạng ĐH Thăng Long.

[6]. D_link Australia & NZ, "Vitual Private Network self study"

[7]. Stephen Thomas, "SSL and TLS Essential"

[8]. David Bruce, Yakov Rekhter - (2000) Morgan Kaufmann Publisher - MPLS Technology and Application MPLS_Cisco.pdf

BẢNG ĐỐI CHIẾU THUẬT NGỮ VIỆT - ANH

Danh sách điều khiển truy nhập	Access Control List
Chế độ truyền không đồng bộ	Asynchronous Transfer Mode
Đầu nhận thực	Authentication Header
Số lượng bảo mật gói gọn	Encapsulation Security Payload
Giao thức đường đi chung	Generic Routing Protocol
Nhà cung cấp dịch vụ Internet	Internet Service Provides
Giao thức Internet	Internet Protocol
Bảo mật địa chỉ IP	IP Security
Độ mạnh chủ đề kỹ sư Internet	Internet Engineering Task Force
Trao đổi gói làm việc trên Internet	Internetwork Packet Exchange
Giao thức thông điệp điều khiển Internet	Internet Control Message protocol
Giao thức quản lý nhóm Internet	Internet Group Management Protocol
Giao thức quản lý khóa và tích hợp an ninh	Security Association and Key Management Protocol
Trao đổi khóa Internet	Internet Key Exchange
Giao thức điều khiển chuyển đổi	Transfer Control Protocol/Internet Protocol
Máy chủ truy cập mạng	Network Access Server
Truy cập tập trung giao thức tầng hầm lớp 2	L2TP Access Concentrator
Máy chủ mạng L2TP	L2TP Network Server
Mạng cục bộ	Local area network
Giao thức tầng hầm lớp 2	Layer 2 Tunneling Protocol
Chuyển tiếp lớp 2	Layer 2 Forwarding
Đường truyền cáp quang	Optical carrier-3
Mô hình liên kết các hệ thống mở	Open Systems Interconnection
Giao thức điểm nối điểm	Point To Point Protocol
Giao thức xác thực mật mã	Password Authentication Protocol

Giao thức bưu điện	Post Office Protocol
Dịch vụ quay số ảo	Point To Point Tunneling Protocol
Mạch ảo cố định	Permanent Virtual Circuit
Chất lượng phục vụ	Quanlity of Service
Bảo mật tổng quan	Security Association
Chính sách bảo mật CSDL	Security Policy Database
Chỉ số giới hạn an ninh	Security Parameter Index
CSDL tích hợp bảo mật	Security Association Database
Máy chủ truy cập từ xa	Remote Access Server
Giao thức sơ đồ người dùng	User DataGram Protocol
Mạng riêng ảo	Virtual Private Network
Mạng Wan	Wide Are Network