

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**

-----o0o-----

TÌM HIỂU MẠNG RIÊNG ẢO VÀ ỨNG DỤNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

HẢI PHÒNG - 2019

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**

-----o0o-----

TÌM HIỂU MẠNG RIÊNG ẢO VÀ ỨNG DỤNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

Sinh viên thực hiện : **Hoàng Văn Hanh**

Mã sinh viên : **1512101003**

Giáo viên hướng dẫn : **TS. Ngô Trường Giang**

HẢI PHÒNG - 2019

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG**

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

-----o0o-----

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinh viên: **Hoàng Văn Hanh**

Mã sinh viên: **1512101003**

Lớp: **CT1901**

Ngành: **Công nghệ Thông tin**

Tên đề tài:

“TÌM HIỂU MẠNG RIÊNG ẢO VÀ ỨNG DỤNG”

MỞ ĐẦU

Ngày nay với sự phát triển của các phương tiện truyền thông, cùng với sự bùng nổ thông tin, lĩnh vực truyền thông mạng máy tính đã và đang phát triển không ngừng. Hiện nay trên thế giới có khoảng 3,9 tỷ người đang sử dụng Internet tương đương một nửa dân số trên thế giới và các ứng dụng trên Internet ngày càng 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.

Để đáp ứng yêu cầu đó, ngày nay đã có rất nhiều giải pháp bảo mật được đặt ra nhằm đảm bảo an toàn thông tin khi trao đổi thông tin thông qua mạng công cộng Internet. Một trong số các giải pháp đó là Mạng riêng ảo VPN. Vậy Mạng riêng ảo VPN là gì, cách thức hoạt động cũng như ứng dụng ra sao. Các câu hỏi sẽ được giải đáp trong đồ án này nhằm nắm bắt rõ về kỹ thuật VPN.

Đồ án gồm 3 hạng mục chính:

- Chương I: Tổng quan về an ninh mạng
- Chương II: Mạng riêng ảo VPN
- Chương III: Thực nghiệm cấu hình VPN trên thiết bị Cisco

MỤC LỤC

MỞ ĐẦU..... 1

MỤC LỤC 2

DANH MỤC TỪ VIẾT TẮT..... 5

DANH MỤC HÌNH VẼ..... 7

CHƯƠNG 1: TỔNG QUAN AN NINH MẠNG..... 8

1.1 An ninh mạng là gì 8

1.1.1 Khái niệm về an ninh mạng 8

1.1.2 Các đặc trưng kỹ thuật của an ninh mạng..... 9

1.1.2.1 Tính xác thực (Authentication)..... 9

1.1.2.2 Tính khả dụng (Availability) 9

1.1.2.3 Tính bảo mật (Confidential) 10

1.1.2.4 Tính toàn vẹn (Integrity) 10

1.1.2.5 Tính không chế (Accountability)..... 11

1.1.2.6 Tính không thể chối cãi (Nonreputation)..... 11

1.1.3 Các lỗ hổng và điểm yếu mạng 11

1.2 Một số phương thức tấn công mạng..... 12

1.2.1 Xem trộm thông tin (Release of Message Content) 12

1.2.2 Thay đổi thông điệp (Modification of Message) 13

1.2.3 Mạo danh (Masquerada) 13

1.2.4 Phát lại thông điệp (Replay)..... 14

1.3 Một số giải pháp bảo mật..... 14

1.3.1 Hệ thống tường lửa 14

1.3.2 Hệ thống phát hiện và chống xâm nhập IDS/IPS..... 15

1.3.3 Công nghệ mạng LAN ảo (VLAN) 16

1.3.4 Mạng riêng ảo (VPN) 17

CHƯƠNG 2: MẠNG RIÊNG ẢO VPN..... 19

2.1 Mạng riêng ảo VPN..... 19

2.1.1 Định nghĩa VPN 19

2.1.2	Các thành phần tạo nên VPN	20
2.1.2.1	VPN client	20
2.1.2.2	VPN server	20
2.1.2.3	IAS server	20
2.1.2.4	Firewall.....	21
2.1.2.5	Giao thức đường hầm (Tunneling Protocol)	21
2.1.3	Lợi ích của VPN	22
2.1.4	Các yêu cầu cơ bản đối với một giải pháp VPN	23
2.2	Ưu và nhược điểm của VPN	24
2.2.1	Ưu điểm.....	24
2.2.2	Nhược điểm	25
2.3	Các công nghệ VPN	25
2.3.1	Site – to – Site VPNs	26
2.3.1.1	Intranet VPNs (VPN nội bộ)	26
2.3.1.2	Extranet VPNs (VPN mở rộng).....	27
2.3.2	Remote Access VPNs (VPN truy cập)	29
2.4	Các giao thức trong VPN.....	30
2.4.1	Giao thức đường hầm điểm tới điểm (PPTP)	30
2.4.1.1	Giới thiệu PPTP	30
2.4.1.2	Nguyên tắc hoạt động.....	31
2.4.1.3	Ưu nhược điểm và khả năng ứng dụng	32
2.4.2	Giao thức đường hầm lớp 2 L2TP	33
2.4.2.1	Giới thiệu	33
2.4.2.2	Các thành phần của L2TP	34
2.4.2.3	Dữ liệu đường hầm L2TP.....	35
2.4.2.4	Những thuận lợi và bất lợi.....	37
2.4.3	Giao thức bảo mật IP (Internet Protocol Security).....	37
2.4.3.1	Giới thiệu	37
2.4.3.2	Giao thức đóng gói tải tin an toàn ESP	40
2.4.3.3	Giao thức xác thực tiêu đề AH	42

2.4.3.4	Giao thức trao đổi khóa IKE (Internet Key Exchange)	44
2.4.3.5	Quy trình hoạt động	44
2.4.3.6	Những hạn chế của IPSec.....	45
2.4.4	SSL/TSL.....	46
2.4.4.1	Giao thức SSL (Secure Socket Layer).....	46
2.4.4.2	Giao thức TLS	46
CHƯƠNG 3:	THỰC NGHIỆM CẤU HÌNH VPN TRÊN THIẾT BỊ	
CISCO	48
3.1	Phát biểu bài toán	48
3.2	Triển khai thực nghiệm.....	49
3.2.1	Mô hình triển khai thực nghiệm	49
3.2.2	Giải thích mô hình	49
3.2.3	Cấu hình thực nghiệm.....	51
3.2.3.1	Mô hình VPN Site – to – Site.....	51
3.2.3.2	Kết quả.....	54
3.2.3.3	Mô hình VPN Remote Access.....	65
3.2.3.4	Kết quả.....	68
KẾT LUẬN.....	71
TÀI LIỆU THAM KHẢO.....	72

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Từ đầy đủ	Ý nghĩa
ATM	Asynchronous Transfer Mode	Công nghệ truyền tải không đồng bộ
AH	Authentication Header	Giao thức tiêu đề xác thực
CLI	Command – line Interface	Giao diện dòng lệnh
ESP	Encapsulation Security Payload	Giao thức tải an ninh đóng gói
GRE	Generic Routing Encapsulation	Giao thức mã hóa định tuyến
IETF	Internet Engineering Task Force	Cơ quan chuẩn Internet
IKE	Internet Key Exchange	Giao thức trao đổi khoá Internet
IP	Internet Protocol	Giao thức Internet
IPSec	Internet Protocol Security	Giao thức bảo mật Internet
ISAKMP	Internet Security Association and Key Management Protocol	Hiệp hội bảo mật Internet và giao thức quản lý khóa
ISP	Internet Service Provides	Nhà cung cấp dịch vụ Internet
L2F	Layer 2 Forwarding	Giao thức chuyển tiếp lớp 2
L2TP	Layer 2 Tunneling Protocol	Giao thức đường hầm lớp 2
LAC	L2TP Access Concentrator	Bộ tập trung truy cập L2TP
LNS	L2TP Network Server	Máy chủ mạng L2TP
NAS	Network Access Server	Máy chủ truy cập mạng
NAT	Network Address Translation	Phân giải địa chỉ mạng
OSI	Open Systems Interconnection	Kết nối hệ thống mở
PAP	Password Authentication Protocol	Giao thức xác thực mật khẩu
POP	Post Office Protocol	Giao thức bưu điện
PPP	Point To Point Protocol	Giao thức điểm tới điểm

PPTP	Point To Point Tunneling Protocol	Giao thức đường ngầm điểm tới điểm
QoS	Quanlity of Service	Chất lượng dịch vụ
RAS	Remote Access Server	Dịch vụ truy nhập từ xa
SA	Security Association	Kết hợp an ninh
SPI	Security Parameter Index	Chỉ số thông số an ninh
TCP	Transmission Control Protocol	Giao thức điều khiển đường truyền
UDP	User DataGram Protocol	Giao thức UDP
VPN	Virtual Private Network	Mạng riêng ảo
WAN	Wide Are Network	Mạng diện rộng

DANH MỤC HÌNH VẼ

Hình 1-1 Xem trộm thông điệp.....	12
Hình 1-2 Thay đổi thông điệp.....	13
Hình 1-3 Mạo danh và gửi đi thông điệp	13
Hình 1-4 Sao chép và gửi đi thông điệp giả	14
Hình 1-5 Mô hình VLAN	17
Hình 2-1 Mô hình mạng VPN	19
Hình 2-2 Mô hình VPN nội bộ	26
Hình 2-3 Mô hình mạng VPN mở rộng	28
Hình 2-4 Mô hình VPN truy cập từ xa.....	29
Hình 2-5 Đường hầm L2TP.....	34
Hình 2-6 Quy trình đóng gói gói tin L2TP	35
Hình 2-7 Quá trình xử lý de – tunneling gói tin L2TP	36
Hình 2-8 Transport mode packet	39
Hình 2-9 Khuôn dạng gói ESP	41
Hình 2-10 AH Header	42
Hình 3-1 Mô hình VPN Site – to – Site	49
Hình 3-2 Mô hình VPN Remote Access	49
Hình 3-3 Cấu hình Router HQ.....	54
Hình 3-4 Cấu hình Router HQ.....	55
Hình 3-5 Cấu hình Router HQ.....	56
Hình 3-6 Cấu hình Router Branch	57
Hình 3-7 Cấu hình Router Branch	58
Hình 3-8 Cấu hình Router Branch	60
Hình 3-9 Cấu hình Router ISP	62
Hình 3-10 Ping thông giữa các máy Client	63
Hình 3-11 Truy xuất dữ liệu thành công.....	64
Hình 3-12 Thao tác với dữ liệu tại máy chủ.....	65
Hình 3-13 Khởi tạo kết nối VPN Remote Access	67
Hình 3-14 Cấu hình Router HQ.....	68
Hình 3-15 Cấu hình Router ISP	69
Hình 3-16 Khởi tạo kết nối VPN	70
Hình 3-17 Ping thành công từ máy Remote Access tới Server.....	70

CHƯƠNG 1: TỔNG QUAN AN NINH MẠNG

1.1 An ninh mạng là gì

1.1.1 Khái niệm về an ninh mạng

An ninh 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 ninh mạng bao gồm:

- Xác định 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. An toàn mạng là một vấn đề cực kì quan trọng trong các hoạt động, giao dịch điện tử và trong khai thác, sử dụng tài nguyên mạng.

Tầm quan trọng của lĩnh vực an ninh mạng ngày càng tăng do sự phụ thuộc ngày càng nhiều vào các hệ thống máy tính và Internet tại các quốc gia, cũng như sự phụ thuộc vào hệ thống mạng không dây như Bluetooth, Wi-Fi, và sự phát triển của các thiết bị thông minh, bao gồm điện thoại thông minh, TV và các thiết bị khác kết nối vào hệ thống Internet of Things.

Một thách thức đối với an ninh 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 nhập. 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 (như Firewall ...) và những biện pháp, chính sách cụ thể chặt chẽ.

1.1.2 Các đặc trưng kỹ thuật của an ninh mạng

1.1.2.1 Tính xác thực (Authentication)

Các hoạt động kiểm tra tính xác thực 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 ...

1.1.2.2 Tính khả dụng (Availability)

Tính khả dụng là đặc tính mà thông tin trên mạng được các thực thể 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.
- Không chế tiếp cận (bao gồm cả việc không chế tự tiếp cận và không chế tiếp cận cưỡng bức).
- Không chế lưu lượng (chống tắc nghẽn...).

- Không 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).

1.1.2.3 Tính bảo mật (Confidential)

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 không 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).

1.1.2.4 Tính toàn vẹn (Integrity)

Là đặc tính khi thông tin trên mạng chưa được uỷ quyền thì không thể tiến hành biến đổi được. 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 và 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.

1.1.2.5 Tính không chế (Accountability)

Là đặc tính về năng lực không chế truyền bá và nội dung vốn có của tin tức trên mạng.

1.1.2.6 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.

1.1.3 Các lỗ hổng và điểm yếu mạng

Các lỗ hổng bảo mật hệ thống là các điểm yếu có thể tạo ra sự ngưng trệ của dịch vụ, thêm quyền với người sử dụng hoặc cho phép các truy cập trái phép vào hệ thống. Các lỗ hổng tồn tại trong các dịch vụ như Web, Ftp ... và trong các hệ điều hành như Windows NT, Windows 95, UNIX hoặc trong các ứng dụng. Gồm có 3 loại lỗ hổng bảo mật:

Lỗ hổng loại C: cho phép thực hiện các phương thức tấn công theo kiểu từ chối dịch vụ DoS (Denial 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.

Lỗ 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.

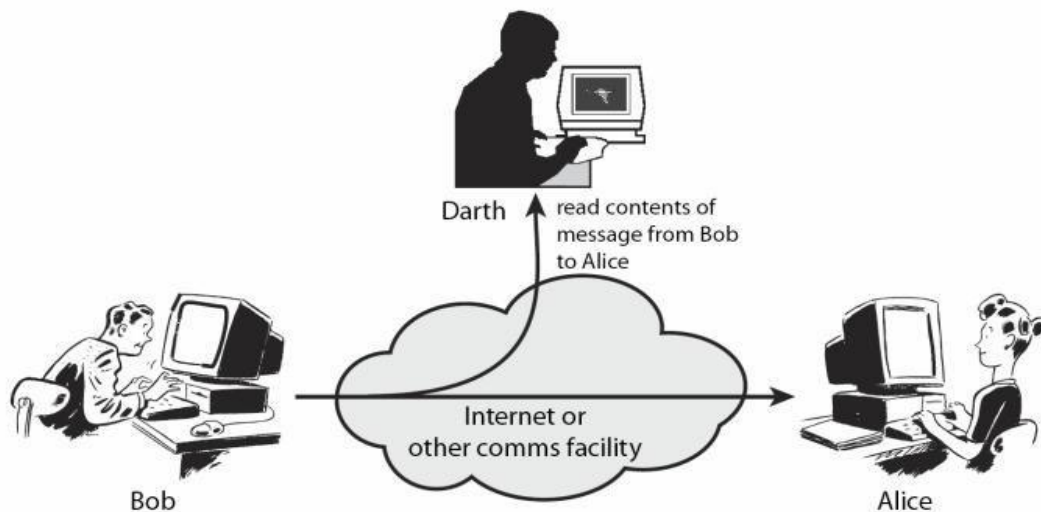
Lỗ hổng loại A: Các lỗ hổng này cho phép người sử dụng ở ngoài cho thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Hacker có thể lợi dụng những lỗ hổng trên để xâm nhập vào hệ thống, lợi dụng các lỗ hổng hệ thống, hoặc từ chính sách bảo mật, hoặc sử dụng các công cụ dò xét để cướp quyền truy nhập. Sau khi xâm nhập 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.

1.2 Một số phương thức tấn công mạng

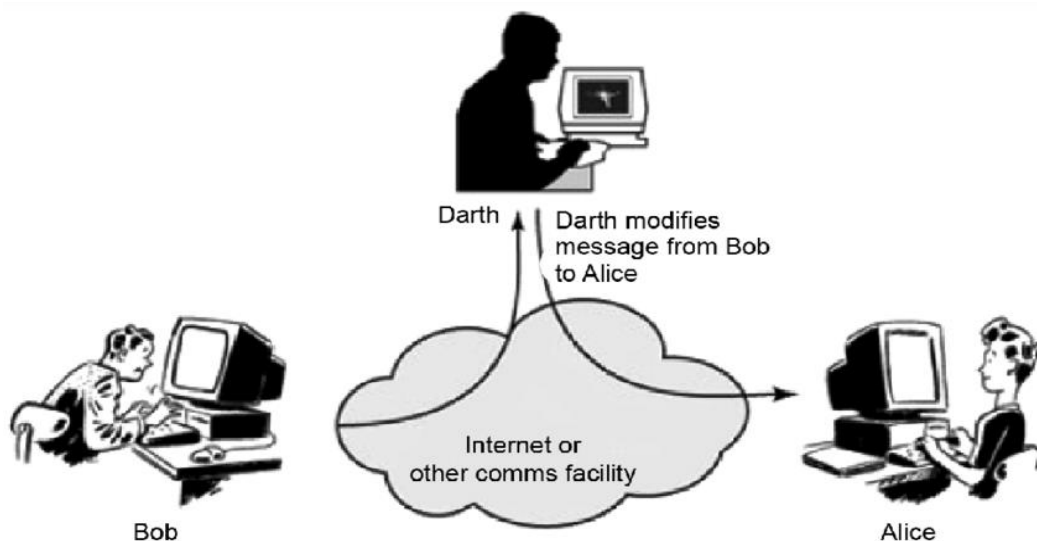
1.2.1 Xem trộm thông tin (Release of Message Content)

Trong trường hợp này Hacker ngăn chặn các thông điệp giữa người gửi và người nhận, và xem được nội dung của thông điệp đó.



Hình 1-1 Xem trộm thông điệp

1.2.2 Thay đổi thông điệp (Modification of Message)

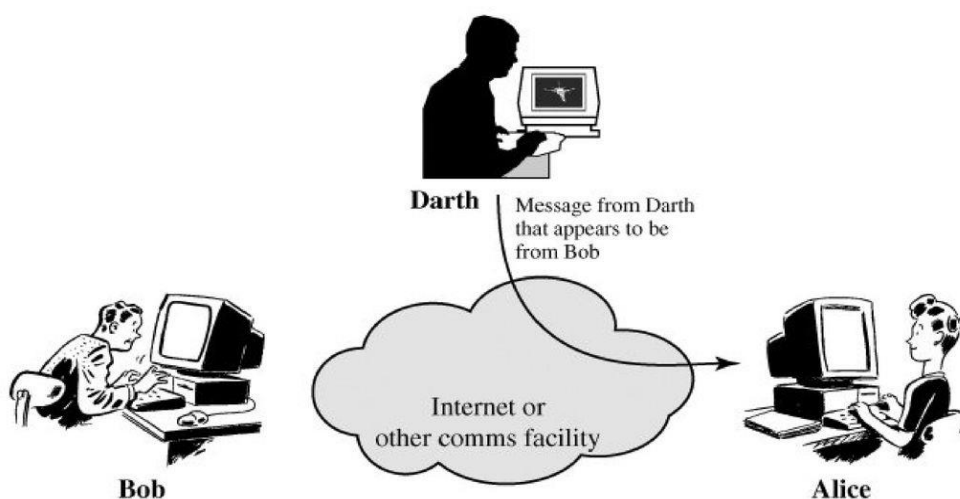


Hình 1-2 Thay đổi thông điệp

Trường hợp này Hacker chặn các thông điệp và ngăn không cho các thông điệp này tới đích. Sau đó thay đổi nội dung của thông điệp và gửi cho người nhận. Người nhận không hề biết nội dung thông điệp đã bị thay đổi.

1.2.3 Mạo danh (Masquerada)

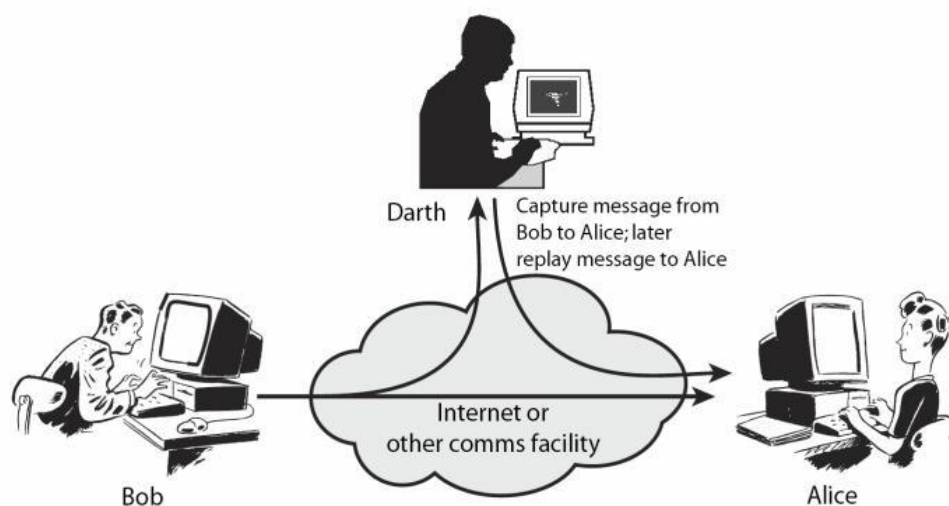
Trường hợp này Hacker sẽ giả là người gửi và gửi đi thông điệp cho người nhận. Người nhận không biết điều này và nghĩ rằng đó là thông điệp từ người gửi.



Hình 1-3 Mạo danh và gửi đi thông điệp

1.2.4 Phát lại thông điệp (Replay)

Trường hợp này Hacker sao chép lại thông điệp từ người gửi. Sau đó một thời gian Hacker gửi lại bản sao chép này cho người nhận. Người nhận tin rằng thông điệp này vẫn từ phía người gửi, nội dung của thông điệp là giống nhau.



Hình 1-4 Sao chép và gửi đi thông điệp giả

1.3 Một số giải pháp bảo mật

1.3.1 Hệ thống tường lửa

Tường lửa là hệ thống kiểm soát truy cập giữa mạng nội bộ và mạng Internet. 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.

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.

Firewalls có hai loại và mỗi loại có ưu điểm khác nhau. Firewall cứng có hiệu năng ổn định, không phụ thuộc vào hệ điều hành, virus, mã độc, ngăn

chặn tốt giao thức ở tầng mạng trong mô hình TCP/IP. Firewall mềm rất linh hoạt trong những cấu hình ở giao thức tầng ứng dụng trong mô hình TCP/IP.

1.3.2 Hệ thống phát hiện và chống xâm nhập IDS/IPS

Hệ thống phát hiện xâm nhập IDS (Intrusion Detect System) cung cấp thêm cho việc bảo vệ thông tin mạng ở mức độ cao hơn. IDS cung cấp thông tin về các cuộc tấn công vào hệ thống mạng. Tuy nhiên IDS không tự động cấm hoặc là ngăn chặn các cuộc tấn công.

Hệ thống ngăn chặn xâm nhập IPS (Intrusion Prevent System) nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ lưu lượng mạng bất hợp pháp, trong khi vẫn cho phép các hoạt động hợp pháp được tiếp tục.

IPS ngăn chặn các cuộc tấn công dưới những dạng sau:

- Ứng dụng không mong muốn và tấn công kiểu “Trojan horse” nhằm vào mạng và ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và danh sách kiểm soát truy nhập.
- Các tấn công từ chối dịch vụ như tràn các gói tin SYN và ICMP bởi việc dùng các thuật toán dựa trên cơ sở “ngưỡng”.
- Sự lạm dụng các ứng dụng và giao thức qua việc sử dụng những quy tắc giao thức ứng dụng và chữ kí.
- Những tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng giới hạn tài nguyên dựa trên cơ sở ngưỡng.

Ưu điểm: phát hiện các cuộc tấn công nhanh và chính xác, không đưa ra các cảnh báo sai làm giảm khả năng hoạt động của mạng, giúp người quản trị xác định các lỗ hổng bảo mật trong hệ thống của mình.

Nhược điểm: Không phát hiện được các tấn công không có trong mẫu, các tấn công mới. Do đó hệ thống phải luôn cập nhật các mẫu tấn công mới.

Hạn chế: So với Firewall, IDS/ IPS đã thể hiện được nhiều tính năng ưu việt. Nó không chỉ có khả năng phát hiện ra các cuộc tấn công, mà còn chống lại các cuộc tấn công này một cách hữu hiệu. Tuy vậy hệ thống này vẫn còn những hạn chế. Các sản phẩm IPS không thể nhận biết được trạng thái tầng ứng dụng (chỉ có thể nhận biết được các dòng thông tin trên tầng mạng). Do vậy các cuộc tấn công trên tầng ứng dụng sẽ không bị phát hiện và ngăn chặn.

1.3.3 Công nghệ mạng LAN ảo (VLAN)

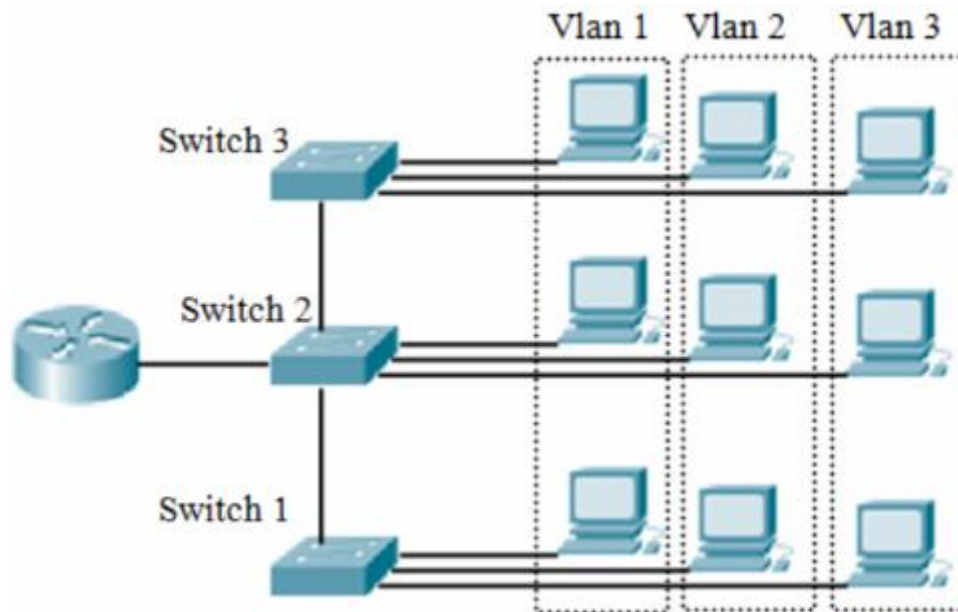
Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai tạo ra miền quảng bá. VLAN là một kỹ thuật kết hợp chuyển mạch lớp 2 và định tuyến lớp 3 để giới hạn miền đưng độ và miền quảng bá. VLAN còn được sử dụng để bảo mật giữa các nhóm VLAN theo chức năng nhóm.

VLAN là một đoạn mạng theo logic dựa trên chức năng, đội nhóm, hoặc ứng dụng của một tổ chức chứ không phụ thuộc vào vị trí vật lý hay kết nối vật lý trong mạng. Tất cả các trạm và server được sử dụng bởi cùng một nhóm làm việc sẽ được đặt trong cùng VLAN bất kể vị trí hay kết nối vật lý của chúng.

Ưu điểm: VLAN cho phép người quản trị mạng tổ chức mạng theo logic chứ không theo vật lý nữa. Nhờ đó những công việc sau thực hiện dễ dàng hơn:

- Có tính linh động cao: di chuyển máy trạm trong LAN dễ dàng.
- Thêm máy trạm vào LAN dễ dàng: Trên một switch nhiều cổng, có thể cấu hình VLAN khác nhau cho từng cổng, do đó dễ dàng kết nối thêm các máy tính với các VLAN.
- Tiết kiệm băng thông của mạng: do VLAN có thể chia nhỏ LAN thành các đoạn (là một vùng quảng bá). Khi một gói tin bùng nổ, nó sẽ được

truyền đi chỉ trong một VLAN duy nhất, không truyền đi ở các VLAN khác nên giảm lưu lượng quảng bá, tiết kiệm băng thông đường truyền.



Hình 1-5 Mô hình VLAN

1.3.4 Mạng riêng ảo (VPN)

VPN cung cấp kênh an toàn cho các kết nối, các cá nhân có thể dùng Internet truy cập tài nguyên trên mạng cục bộ một cách bảo mật và thoải mái khi họ ở nhà hoặc đi du lịch một cách nhanh chóng và hiệu quả trên cả máy tính hay thiết bị di động.

Mạng VPN đảm bảo an toàn và bảo vệ sự lưu thông trên mạng và cung cấp sự riêng tư, sự chứng thực và toàn vẹn dữ liệu thông qua các giải thuật mã hoá.

Để cung cấp kết nối giữa các máy tính, các gói thông tin được đóng gói bằng một header có chứa những thông tin định tuyến, cho phép dữ liệu có thể gửi từ máy truyền qua môi trường mạng chia sẻ và đến được máy nhận, như truyền trên các đường ống riêng được gọi là tunnel.

Khi truyền các gói tin cần phải áp dụng các cơ chế mã hóa và chứng thực để bảo mật như SSL (Secure Socket Layer), IPSec (IP Security Tunnel

Mode, PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol).

CHƯƠNG 2: MẠNG RIÊNG ẢO VPN

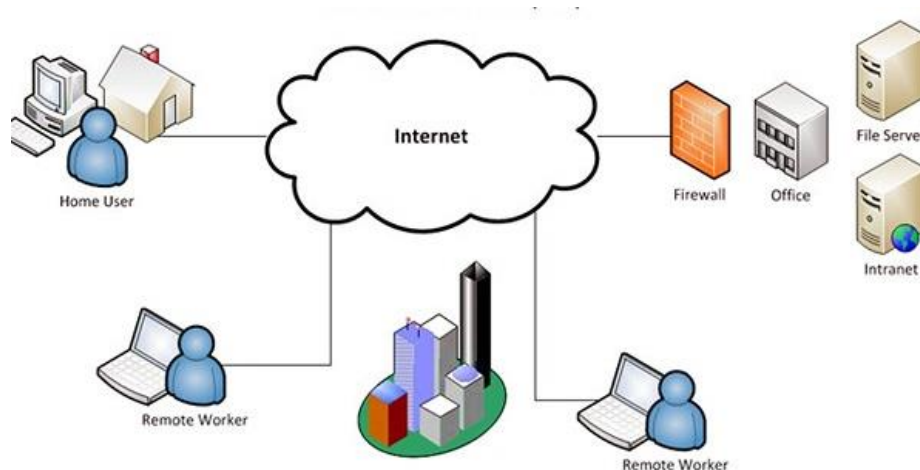
2.1 Mạng riêng ảo VPN

2.1.1 Định nghĩa VPN

VPN được hiểu như là một giải pháp mở rộng một mạng riêng thông qua một mạng chung (thường là Internet). Mỗi VPN sẽ kết nối với một VPN khác, các site khác hay nhiều người dùng từ xa. Thay thế cho kết nối thực như leased – line, VPN sử dụng các kết nối ảo được dẫn từ các mạng nội bộ tới các site của người dùng từ xa.

Các giải pháp VPN được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì phạm vi hoạt động rộng (toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn giúp tiết kiệm chi phí và thời gian.

VPN được gọi là mạng ảo bởi chúng chỉ sử dụng các kết nối tạm thời. Những kết nối bảo mật được thiết lập giữa các host, giữa host với mạng hay giữa hai mạng với nhau.



Hình 2-1 Mô hình mạng VPN

2.1.2 Các thành phần tạo nên VPN

2.1.2.1 VPN client

VPN client có thể là một máy tính hoặc một bộ định tuyến. Loại VPN khách hàng sử dụng cho mạng của công ty phụ thuộc vào nhu cầu cá nhân của công ty đó.

Mặt khác, nếu công ty có một vài nhân viên thường xuyên đi công tác xa và cần phải truy cập vào mạng của công ty trên đường đi, máy tính xách tay của nhân viên có thể thiết lập như VPN client.

Về mặt kỹ thuật, bất kỳ hệ điều hành đều có thể hoạt động như một VPN Client miễn là nó có hỗ trợ các giao thức như: giao thức đường hầm điểm-điểm PPTP (Point to Point Tunneling Protocol), giao thức đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol) và giao thức bảo mật Internet IPSec (Internet Protocol Security). Ngày nay, với các phiên bản Windows mới thì khả năng truy cập mạng VPN càng được phát triển tối ưu hơn, do đó vấn đề không tương thích với các phiên bản hệ điều hành hiện nay là không tồn tại.

2.1.2.2 VPN server

VPN server hoạt động như một điểm kết nối cho các VPN client. Về mặt kỹ thuật, một máy chủ VPN có thể được cài đặt trên một số hệ điều hành như Window Server, Linux ...

VPN Server khá đơn giản. Nó là một máy chủ được cài đặt dịch vụ máy chủ định tuyến và truy cập từ xa RRAS (Routing and Remote Access Server). Khi một kết nối VPN đã được chứng thực, các máy chủ VPN chỉ đơn giản là hoạt động như một bộ định tuyến cung cấp cho khách hàng VPN có thể truy cập đến một mạng riêng.

2.1.2.3 IAS server

Một trong những yêu cầu bổ sung cho một máy chủ VPN là cần có một máy chủ dịch vụ xác thực người dùng truy cập từ xa RADIUS (Remote

Authentication Dial in User Service). RADIUS là một server sử dụng quay số xác thực từ xa. RADIUS là cơ chế mà các nhà cung cấp dịch vụ Internet thường sử dụng để xác thực các thuê bao để thiết lập kết nối Internet.

Microsoft cũng có phiên bản riêng của RADIUS được gọi là dịch vụ xác thực Internet IAS (International Accounting Standards).

2.1.2.4 Firewall

Các thành phần khác theo yêu cầu của mạng riêng ảo VPN (Virtual Private Network) là một tường lửa tốt. Máy chủ VPN chấp nhận kết nối từ mạng ngoài, nhưng điều đó không có nghĩa là mạng ngoài cần phải có quyền truy cập đầy đủ đến máy chủ VPN. Chúng ta phải sử dụng một tường lửa để chặn bất kỳ cổng nào không sử dụng.

Yêu cầu cơ bản cho việc thiết lập kết nối VPN là địa chỉ IP của máy chủ VPN có thông qua tường lửa để tiếp cận với máy chủ VPN.

Chúng ta có thể đặt một máy chủ ISA giữa tường lửa và máy chủ VPN. Ý tưởng là có thể cấu hình tường lửa để điều chỉnh tất cả lưu lượng truy cập VPN có liên quan đến ISA Server chứ không phải là máy chủ VPN. ISA Server sau đó hoạt động như một proxy VPN. Cả hai VPN Client và VPN Server chỉ giao tiếp với máy chủ ISA mà không bao giờ giao tiếp trực tiếp với nhau. Điều này có nghĩa là ISA Server che chắn các VPN Server từ các VPN Client truy cập đến, vì thế cho VPN Server sẽ có thêm một lớp bảo vệ.

2.1.2.5 Giao thức đường hầm (Tunneling Protocol)

VPN client truy cập vào một máy chủ VPN qua một đường hầm ảo. Đường hầm ảo này là một lối đi an toàn qua môi trường công cộng (như Internet). Để có được đường hầm, cần phải sử dụng một trong các giao thức đường hầm. Một số giao thức để lựa chọn để tạo đường hầm như: IPSec, L2TP, PPTP và GRE. Nhưng để lựa chọn một giao thức đường hầm phù hợp

cho một mô hình mạng ở một công ty hay một doanh nghiệp bất kỳ là một quyết định quan trọng khi lập kế hoạch để triển khai hệ thống VPN cho doanh nghiệp, công ty đó.

Lợi thế lớn nhất mà L2TP hơn PPTP là nó dựa trên IPSec. IPSec mã hóa dữ liệu, cung cấp xác thực dữ liệu, dữ liệu của người gửi sẽ được mã hóa và đảm bảo không bị thay đổi nội dung trong khi truyền.

Mặc dù L2TP có vẻ là có lợi thế hơn so với PPTP, nhưng PPTP cũng có lợi thế riêng đó là khả năng tương thích. PPTP hoạt động tốt với các hệ điều hành Windows hơn L2TP.

2.1.3 Lợi ích của VPN

❖ *VPN giúp giảm đáng kể chi phí đường truyền*

VPN tiết kiệm chi phí cho việc thuê đường truyền và giảm chi phí phát sinh cho người dùng từ xa, họ có thể truy cập vào mạng nội bộ thông qua các điểm cung cấp dịch vụ ở địa phương POP (Point of Presence) hạn chế thuê đường truy cập của nhà cung cấp. Giá thành cho việc kết nối Lan – to – Lan giảm đáng kể so với việc thuê đường Leased – line, hay các giải pháp truyền tin truyền thống như Frame Relay, ATM hay IDSN.

❖ *Giảm chi phí quản lý và hỗ trợ*

Việc sử dụng dịch vụ nhà cung cấp chúng ta chỉ cần quản lý các kết nối đầu cuối tại các chi nhánh mạng mà không phải quản lý các thiết bị chuyển mạch trên mạng. Đồng thời có thể tận dụng cơ sở hạ tầng của mạng Internet và đội ngũ kỹ thuật của nhà cung cấp dịch vụ.

❖ *Đảm bảo an toàn thông tin*

Dữ liệu truyền trên mạng được mã hóa và phân quyền sử dụng cho từng người dùng (user) khác nhau, đồng thời được truyền trong các đường hầm (Tunnel) nên thông tin có độ an toàn cao.

❖ Dễ dàng kết nối

Hiện nay, một công ty thường sẽ có rất nhiều các chi nhánh tại nhiều quốc gia khác nhau. Việc quản lý, truy cập thông tin tại các chi nhánh là cần thiết. Sử dụng VPN có thể dễ dàng kết nối hệ thống giữa các chi nhánh thành một mạng LAN với chi phí thấp.

❖ Bảo mật địa chỉ IP

Thông tin gửi đi trên VPN đã được mã hóa các địa chỉ bên trong mạng riêng (private) và chỉ sử dụng các địa chỉ bên ngoài (public) internet.

❖ Hiệu suất băng thông

Sự lãng phí băng thông khi không có kết nối nào được kích hoạt. Trong kỹ thuật VPN thì các đường hầm chỉ được hình thành khi có yêu cầu truyền tải thông tin. Băng thông mạng chỉ được sử dụng khi có kích hoạt kết nối Internet. Do đó hạn chế rất nhiều sự lãng phí băng thông.

2.1.4 Các yêu cầu cơ bản đối với một giải pháp VPN

Khi xây dựng một mạng riêng ảo cần đáp ứng các yêu cầu:

❖ Tính tương thích (compatibility)

Các mạng nội bộ của các công ty, doanh nghiệp không thể kết nối trực tiếp với mạng Internet bởi không theo chuẩn TCP/IP. Muốn sử dụng được IP VPN thì các hệ thống mạng nội bộ cần phải được chuyển sang một hệ thống địa chỉ theo chuẩn được sử dụng trong Internet và bổ sung tính năng cần thiết cho việc tạo kênh kết nối ảo. Cũng như cài đặt cổng kết nối Internet có chức năng trong việc chuyển đổi các thủ tục khác nhau sang chuẩn IP. Vậy nên các nhà cung cấp dịch vụ phải tương thích với các thiết bị hiện có của người dùng.

❖ Tính bảo mật (security)

Bảo mật thông tin khách hàng là một yếu tố quan trọng đối với một giải pháp VPN. Các dữ liệu của người dùng cần được đảm bảo, đạt được mức độ an toàn giống như một hệ thống mạng dùng riêng.

Cung cấp tính năng bảo đảm an toàn cần đảm bảo giữa cung cấp tính năng an toàn thích hợp như cung cấp mật khẩu cho người dùng trong mạng, mã hóa dữ liệu đồng thời 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.

❖ *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 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.

2.2 Ưu và nhược điểm của VPN

2.2.1 Ưu điểm

VPN mang lại lợi ích thực sự và tức thời cho các công ty. Có thể dùng VPN để đơn giản hoá việc thông tin giữa các nhân viên làm việc ở xa, người dùng từ xa, mở rộng Intranet đến từng văn phòng, chi nhánh, không những chúng ta có thể triển khai Extranet đến tận khách hàng và các đối tác chủ chốt mà còn làm giảm chi phí cho các công việc trên thấp hơn nhiều so với việc mua thiết bị và đường dây cho mạng WAN riêng. Những lợi ích này dù trực tiếp hay gián tiếp đều bao gồm: tiết kiệm chi phí, tính mềm dẻo, khả năng mở rộng và một số ưu điểm khác.

2.2.2 Nhược điểm

Mặc dù phổ biến nhưng mạng riêng ảo VPN (Virtual Private Network) khi triển khai hệ thống cần lưu ý một số hạn chế.

VPN đòi hỏi sự hiểu biết chi tiết về vấn đề an ninh mạng, việc cấu hình và cài đặt phải cẩn thận, chính xác đảm bảo tính an toàn trên hệ thống mạng Internet công cộng.

Độ tin cậy và hiệu suất của một VPN dựa trên Internet không phải là dưới sự kiểm soát trực tiếp của công ty, vì vậy giải pháp thay thế là hãy sử dụng một nhà cung cấp dịch vụ Internet tốt và chất lượng.

Việc sử dụng các sản phẩm VPN và các giải pháp của các nhà cung cấp khác nhau không phải lúc nào cũng tương thích do các vấn đề về tiêu chuẩn công nghệ VPN. Khi sử dụng pha trộn và kết hợp các thiết bị sẽ có thể gây ra những vấn đề kỹ thuật hoặc nếu sử dụng không đúng cách sẽ lãng phí rất nhiều chi phí triển khai hệ thống.

Một hạn chế hay nhược điểm rất khó tránh khỏi của VPN đó là vấn đề bảo mật cá nhân, bởi vì việc truy cập từ xa hay việc nhân viên kết nối với hệ thống văn phòng bằng máy tính xách tay, máy tính riêng, khi đó nếu các máy tính của họ thực hiện hàng loạt các ứng dụng khác, ngoài việc kết nối tới văn phòng làm việc thì những tin tặc có thể lợi dụng yếu điểm từ máy tính cá nhân của họ tấn công vào hệ thống của công ty. Vì vậy việc bảo mật cá nhân luôn được các chuyên gia khuyến cáo phải đảm bảo an toàn.

2.3 Các công nghệ VPN

Các công nghệ VPN nhằm đáp ứng các yêu cầu cơ bản:

- Có thể truy cập hệ thống bất cứ lúc nào bằng các thiết bị thông minh như điện thoại, máy tính ..., và liên lạc giữa các nhân viên của một tổ chức tới các tài nguyên trên mạng.
- Kết nối thông tin giữa các văn phòng từ xa của một tổ chức.

- Điều khiển, quản lý truy nhập tài nguyên mạng khi cần thiết của khách hàng, nhà cung cấp và các đối tượng quan trọng của công ty.

Dựa theo những yêu cầu đó, ngày nay VPN đã phát triển và phân chia ra 2 loại công nghệ VPN chính:

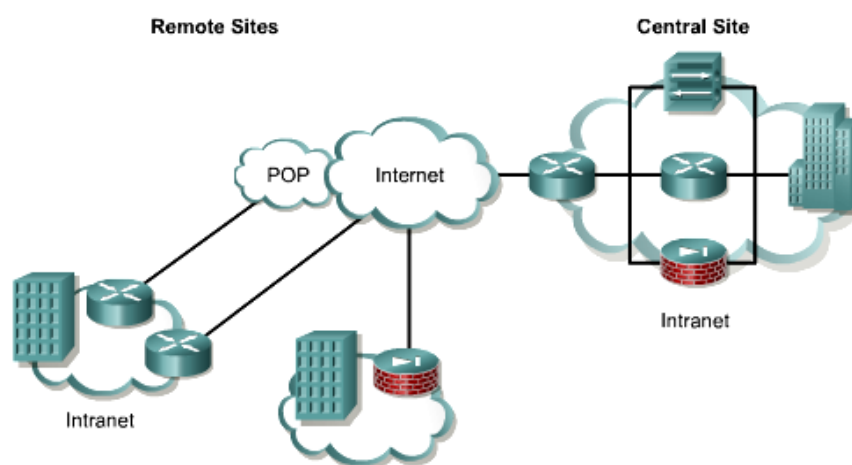
- Site – to – Site VPNs
- Remote Access VPNs

2.3.1 Site – to – Site VPNs

2.3.1.1 Intranet VPNs (VPN nội bộ)

VPN nội bộ được sử dụng để kết nối các chi nhánh văn phòng tới Corporate Intranet (Backbone router) sử dụng campus router. Cách thiết lập này rất tốn chi phí bởi phải sử dụng 2 router để thiết lập được mạng, cùng với đó là chi phí triển khai, quản lý và bảo trì mạng Intranet Backbone sẽ rất tốn kém.

VPN nội bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một tổ chức. Cho phép tất cả các điểm có thể truy cập các nguồn dữ liệu được cho phép trong toàn bộ mạng. Các VPN nội bộ liên kết các phòng, các chi nhánh trên một cơ sở hạ tầng chung và sử dụng các kết nối luôn luôn được mã hóa.



Hình 2-2 Mô hình VPN nội bộ

❖ Thuận lợi của Intranet dựa trên VPN

Giảm chi phí hơn do giảm số lượng router được sử dụng theo mô hình WAN Backbone.

Internet hoạt động như một kết nối trung gian nên nó dễ dàng cung cấp những kết nối mới ngang hàng.

Kết nối nhanh hơn do chỉ cần kết nối đến các nhà cung cấp dịch vụ, loại bỏ các vấn đề về khoảng cách địa lí.

❖ Một số bất lợi chính

Dữ liệu vẫn còn tunnel trong suốt quá trình chia sẻ trên mạng công cộng nên vẫn tồn tại các nguy cơ tấn công, điển hình là tấn công từ chối dịch vụ DoS.

Khả năng mất dữ liệu trên đường truyền khá cao.

Một số trường hợp trao đổi dữ liệu sẽ rất chậm khi dữ liệu là loại high-end hay multimedia do truyền thông qua Internet.

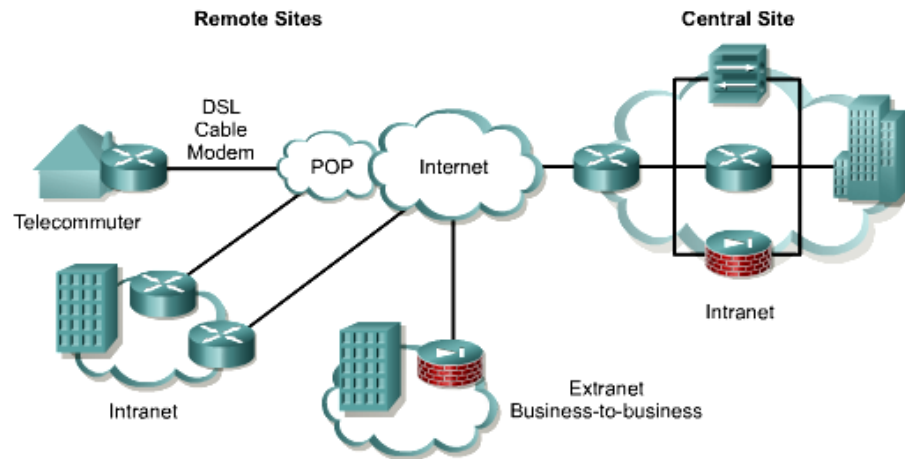
Kết nối dựa trên Internet nên tính hiệu quả không liên tục, QoS không được đảm bảo.

2.3.1.2 Extranet VPNs (VPN mở rộng)

Không giống như Intranet, Extranet không hoàn toàn cách li từ bên ngoài, Extranet cho phép truy cập những tài nguyên mạng cần thiết của khách hàng, nhà cung cấp hay những đối tác giữ vai trò quang trọng trong một tổ chức.

Mạng Extranet rất tốn kém do có nhiều đoạn mạng riêng biệt trên Intranet kết hợp lại với nhau để tạo nên một mạng Extranet. Điều này khiến cho việc triển khai và quản lý gặp khó khăn vì có nhiều các mạng con, đồng thời cũng gây khó khăn cho công tác bảo trì và quản trị. Mạng Extranet cũng rất khó để mở rộng bởi sẽ có những vấn đề gặp phải khi thêm mới một kết nối mạng Intranet.

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 2-3 Mô hình mạng VPN mở rộng

❖ *Một số thuận lợi*

Extranet hoạt động trên Internet nên có thể lựa chọn nhà phân phối và đưa ra các giải pháp giải quyết tùy theo nhu cầu của tổ chức.

Giảm bớt chi phí cho nhân viên bảo trì bởi nhà cung cấp sẽ bảo trì một phần Internet-connectivity.

Dễ dàng triển khai, quản lý và chỉnh sửa thông tin.

❖ *Một số bất lợi*

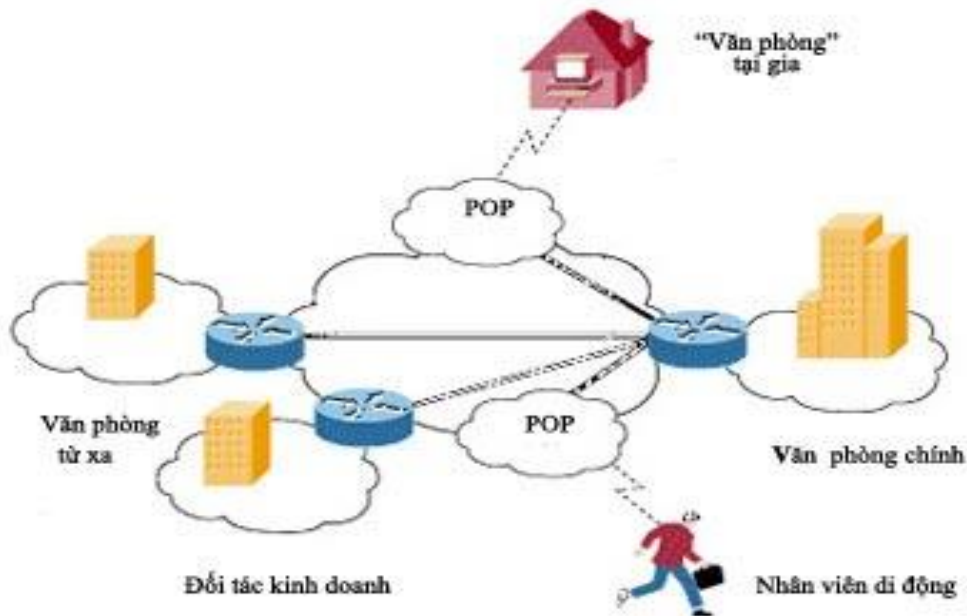
Do truyền thông qua Internet nên trao đổi dữ liệu sẽ rất chậm khi dữ liệu là loại high-end hay multimedia.

Kết nối dựa trên Internet nên tính hiệu quả không liên tục, QoS không được đảm bảo.

2.3.2 Remote Access VPNs (VPN truy cập)

Remote Access VPN cho phép truy cập bất cứ lúc nào bằng các thiết bị truyền thông của nhân viên 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.

Các VPN truy cập thường sẽ yêu cầu một phần mềm client chạy trên máy của người sử dụng. Được gọi là VPN truy cập từ xa.



Hình 2-4 Mô hình VPN truy cập từ xa

❖ *Một số thuận lợi*

Hỗ trợ cho người dùng cá nhân được loại trừ bởi kết nối từ xa đã được tạo điều kiện thuận lợi bởi ISP.

Việc quay số từ khoảng cách xa được thay thế bằng những kết nối cục bộ.

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

Tốc độ kết nối sẽ cao hơn so với kết nối trực tiếp đến những địa điểm xa do đây là kết nối mang tính cục bộ.

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.

❖ *Một số bất lợi*

Khả năng mất dữ liệu vẫn khá cao, các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất lạc.

Thuật toán mã hóa phức tạp, protocol overhead tăng đáng kể gây khó khăn cho quá trình xác nhận. Cùng với đó là việc nén dữ liệu IP và PPP-based diễn ra chậm.

Do truyền thông qua mạng Internet, nên khi trao đổi các gói dữ liệu lớn như các gói dữ liệu truyền thông, media, âm thanh sẽ rất chậm.

2.4 Các giao thức trong VPN

Giao thức đường hầm là nền tảng trong VPN. Giao thức đường hầm đóng vai trò quan trọng trong việc thực hiện đóng gói và vận chuyển các gói tin để truyền đi trên đường mạng Internet.

2.4.1 Giao thức đường hầm điểm tới điểm (PPTP)

2.4.1.1 Giới thiệu PPTP

Giao thức PPTP (Point – to – Point Tunneling Protocol) là một giao thức mạng cho phép chuyển giao an toàn dữ liệu từ một Client đến máy chủ bằng cách tạo ra đường hầm ảo trên TCP/IP dựa trên mạng lưới dữ liệu. PPTP hỗ trợ theo yêu cầu, đa giao thức, mạng riêng ảo trên các mạng công cộng như Internet.

Giao thức PPTP được phát triển bởi các công ty chuyên về thiết bị công nghệ viễn thông, xây dựng dựa trên nền tảng của PPP, PPTP có thể cung cấp khả năng truy nhập tạo đường hầm thông qua Internet đến các site đích. PPTP sử dụng phương thức đóng gói tin định tuyến chung GRE được mô tả để đóng và tách các gói PPP.

2.4.1.2 Nguyên tắc hoạt động

PPTP làm việc ở lớp liên kết dữ liệu trong mô hình OSI, bao gồm các phương thức đóng gói, tách gói tin IP và truyền gói tin từ máy này sang máy khác.

PPTP đóng các gói tin và khung dữ liệu của giao thức PPP vào trong một IP datagrams để truyền thông qua mạng Internet trên nền IP. Kết nối TCP (cổng 1723) được sử dụng để khởi tạo, duy trì đường hầm và GRE (Protocol 47) được dùng cho việc đóng gói những gói tin PPP cho dữ liệu trong kênh. Phần tải của khung PPP có thể được mã hóa và nén lại.

Cơ chế xác thực người dùng thường được cung cấp bởi ISP, việc xác thực trong quá trình thiết lập kết nối PPTP sử dụng các cơ chế xác thực của kết nối PPP. Một số cơ chế được sử dụng:

- 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 là một cơ chế xác thực hoạt động dựa trên nguyên tắc mật khẩu được gửi qua các kết nối và không bảo mật. CHAP là một giao thức xác thực mạnh hơn, sử dụng phương pháp bắt tay ba chiều để hoạt động và ngăn chặn các cuộc tấn công bằng cách sử dụng các giá trị bí mật duy nhất và không thể đoán được. Phương thức mã hóa điểm tới điểm MPPE được sử dụng để mã hóa phần tải tin PPP trên đường truyền. MPPE chỉ cung cấp mã

khóa trong lúc truyền dữ liệu trên đường truyền mà không cung cấp mã khóa tại các thiết bị đầu cuối.

Khi PPP được thiết lập kết nối, PPTP sử dụng quy luật đóng gói của PPP để đóng gói các gói truyền thông trong đường hầm. PPTP định nghĩa hai loại gói tin là điều khiển và dữ liệu, sau đó chúng được gán vào các kênh riêng biệt. 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.

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

Kênh điều khiển được sử dụng cho việc thiết lập một đường hầm giữa 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.

2.4.1.3 Ưu nhược điểm và khả năng ứng dụng

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 thích hợp cho việc quay số truy nhập với số lượng người dùng giới hạn. Một vấn đề của PPTP là việc xác thực người dùng thông qua hệ điều hành. Máy chủ PPTP cũng quá tải nếu như có một số lượng lớn người dùng truy nhập hay một lưu lượng lớn dữ liệu truyền

qua, đây là một trong số những yêu cầu của mạng LAN – LAN. Tính bảo mật của PPTP không mạnh như IPSec, nhưng quản lý bảo mật trong PPTP lại dễ dàng hơn nhiều.

Khó khăn lớn nhất mà PPTP gặp phải là cơ chế bảo mật yếu kém bởi PPTP sử dụng mã hóa đồng bộ trong khóa được xuất phát từ việc sử dụng mã hóa đối xứng của giao thức này là cách tạo ra khóa từ mật khẩu của người dùng. Hơn thế nữa, mật khẩu còn được gửi không bảo mật trong quá trình xác nhận.

2.4.2 Giao thức đường hầm lớp 2 L2TP

2.4.2.1 Giới thiệu

Giao thức L2TP là sự kết hợp của hai giao thức PPTP và L2F. Được phát triển bởi IETF, L2TP kết hợp những đặc điểm tốt nhất của PPTP và L2F. Vì vậy, L2TP có 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.

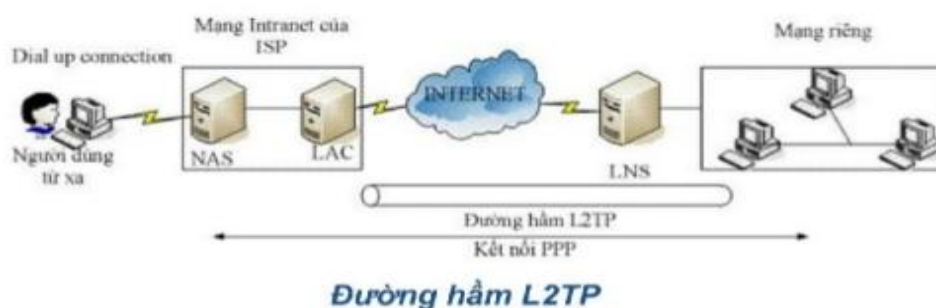
Các đặc tính của L2TP bao gồm:

- 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 công mạng máy chủ. Do đó, nhà cung cấp dịch vụ không cần dữ liệu xác nhận hoặc quyền truy cập của người dùng từ xa, mạng riêng Intranet cũng có thể tự định nghĩa những chính sách truy cập riêng. Khiến cho quy trình xử lý thiết lập đường hầm nhanh hơn so với giao thức tạo đường hầm trước đây.

L2TP thiết lập đường hầm PPP không giống như PPTP, không kết thúc ở gần vùng của ISP, những đường hầm được mở rộng đến cổng của mạng máy chủ (đích).

L2TP (Layer 2 Tunneling Protocol)



Hình 2-5 Đường hầm L2TP

Khi gói tin PPP được gửi thông qua đường hầm L2TP, chúng được đóng gói như thông điệp User Datagram Protocol (UDP). L2TP dùng những thông điệp UDP cho việc tạo đường hầm dữ liệu cũng như duy trì đường hầm.

2.4.2.2 Các thành phần của L2TP

L2TP bao gồm 3 thành phần cơ bản, một Network Access Server (NAS), một L2TP Access Concentrator (LAC) và một L2TP Network Server (LNS).

L2TP NAS là thiết bị truy cập điểm tới điểm được cung cấp dựa trên yêu cầu kết nối Internet đến người dùng từ xa. NAS 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. L2TP được đặt tại ISP site và có vai trò như client trong quá trình thiết lập L2TP Tunnel. NAS có thể hỗ trợ đồng thời nhiều yêu cầu kết nối và có thể hỗ trợ một phạm vi rộng các client (như các sản phẩm mạng của Microsoft, Unix, Linux, VAX – VMS).

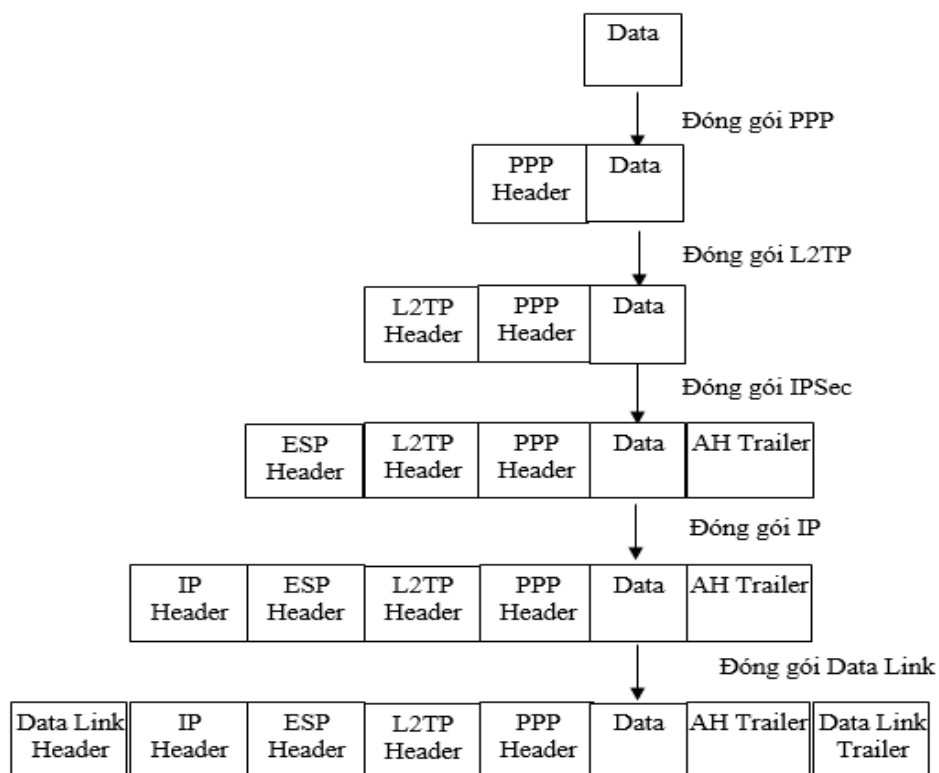
L2TP LACs là một bộ tập kết truy cập L2TP có vai trò thiết lập một đường hầm thông qua một mạng công cộng (như PSTN, Internet) đến LNS ở điểm cuối của mạng chủ. LACs như điểm kết thúc của môi trường vật lý giữa

client và LNS của mạng chủ. LACs thường được đặt tại ISP site, tuy nhiên người dùng từ xa cũng có thể hoạt động như LAC trong trường hợp đường hầm L2TP tự nguyện.

LNS được đặt tại cuối mạng chủ, chúng dùng để kết thúc kết nối L2TP ở cuối mạng chủ. Khi LNS nhận được yêu cầu cho kết nối ảo từ 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.

2.4.2.3 Dữ liệu đường hầm L2TP

Tương tự như PPTP, L2TP đóng gói dữ liệu thông qua nhiều tầng đóng gói.



Hình 2-6 Quy trình đóng gói gói tin L2TP

Đầu tiên, một PPP Header sẽ được thêm vào dữ liệu gốc, dữ liệu không mã hóa trước khi đóng gói.

L2TP đóng gói khung của PPP, một L2TP Header được thêm vào sau khi dữ liệu được đóng gói bên trong một PPP packet.

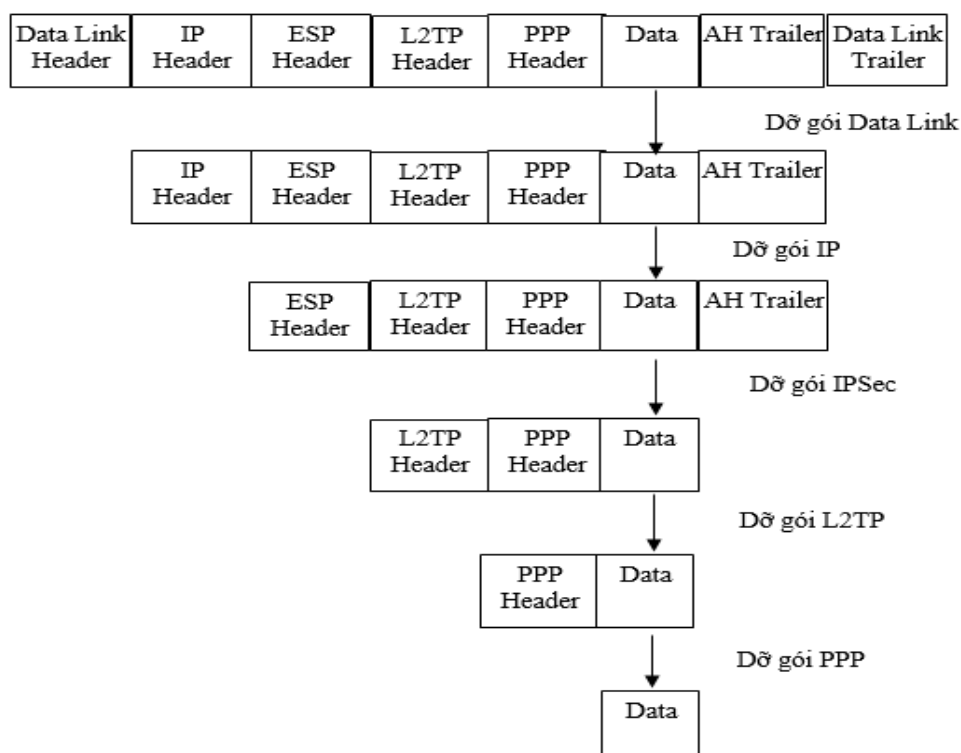
Kế tiếp, gói dữ liệu được đóng gói thêm bên trong một UDP frame, tức là một UDP header được thêm vào L2TP frame đã đóng gói.

UDP frame này được mã hóa, một phần đầu IPsec ESP được thêm vào. Một phần đuôi IPsec AH cũng được chèn vào gói dữ liệu đã được mã hóa.

Phần đầu IP cuối cùng được thêm vào gói dữ liệu IPsec đã được đóng gói. Phần đầu IP chứa địa chỉ IP của L2TP server (LNS) và người dùng từ xa.

Cuối cùng phần đầu và cuối của tầng Data Link được thêm vào gói dữ liệu IP. Hai phần này sẽ giúp gói tin đi đến nút đích.

Quy trình xử lý de – tunneling những gói dữ liệu L2TP đã tunnel thì ngược lại với quy trình đường hầm.



Hình 2-7 Quá trình xử lý de – tunneling gói tin L2TP

L2TP hỗ trợ 2 chế độ đường hầm là chế độ đường hầm bắt buộc (Compulsory Tunnel Mode) và chế độ đường hầm tự nguyện (Voluntary

Tunnel Mode). Những đường hầm này đóng vai trò quan trọng trong bảo mật dữ liệu.

2.4.2.4 Những thuận lợi và bất lợi

Những thuận lợi mà một giải pháp L2TP mang lại:

- L2TP là một nền tảng độc lập, nó hỗ trợ nhiều công nghệ mạng khác nhau. Ngoài ra L2TP còn hỗ trợ giao dịch qua kết nối WAN non – IP mà không cần một IP.
- L2TP không đòi hỏi bất kì cấu hình nào từ phía người dùng hay ISP.
- Với sự hỗ trợ của IPSec trong suốt quá trình tạo hầm, L2TP cung cấp một trong những kỹ thuật mã hóa an toàn nhất.
- 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 quá trình giao dịch bằng L2TP nhanh hơn so với quá trình giao dịch bằng L2F.
- Việc triển khai L2TP cũng gặp một số bất lợi như:
 - 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 giải pháp VPN dựng sẵn, một Routing and Remote Access Server (RRAS) cần có những cấu hình mở rộng.

2.4.3 Giao thức bảo mật IP (Internet Protocol Security)

2.4.3.1 Giới thiệu

IPSec – Internet Protocol Security có quan hệ tới một số bộ giao thức (AH, ESP, FIP – 140, ...) được phát triển bởi Internet Engineering Task Force (IETF). Mục đích của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network Layer) của mô hình OSI.

Mọi giao tiếp trong một mạng trên cơ sở IP đều dựa trên các giao thức IP. Do đó khi một cơ chế bảo mật cao được tích hợp với giao thức IP, toàn bộ

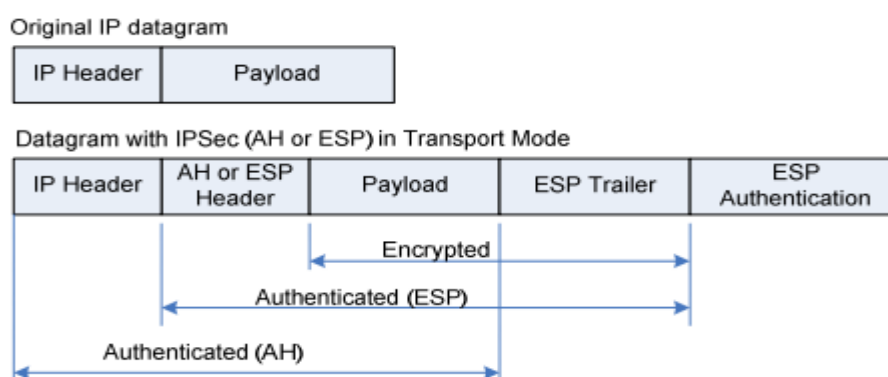
mạng được bảo mật bởi vì các giao tiếp đều đi qua tầng 3. Vì vậy IPSec được phát triển ở lớp 3 thay vì lớp 2. IPSec sử dụng các dịch vụ được định nghĩa trong IPSec để đảm bảo sự xác thực dữ liệu, tính toàn vẹn dữ liệu và sự tin cậy của dữ liệu khi trên hạ tầng mạng công cộng.

IPSec là một phương pháp để bảo vệ IP datagram. 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.

Encapsulating Security Payload (ESP) và Authentication Header (AH) là hai giao thức được sử dụng để cung cấp tính toàn vẹn cho các gói tin IP. Cơ chế hoạt động trong IPSec gồm có IPSec Transport Mode và IPSec Tunnel Mode và các dịch vụ của nó.

❖ IPSec Transport Mode

Transport mode bảo vệ giao thức tầng trên và các ứng dụng và 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. Trong Transport mode, chỉ mã hóa phần payload của mỗi gói tin.



Hình 2-8 Transport mode packet

Khó khăn lớn nhất khi triển khai Transport mode là 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. Do sự phức tạp trong việc triển khai trong thực tế, nên người ta sẽ sử dụng một VPN gateway để bảo vệ dữ liệu từ tất cả các site đến một site ngang hàng.

❖ IPSec Tunnel Mode

IPSec VPN sử dụng Transport mode và cơ chế đóng gói GRE là những cách sử dụng phổ biến tại các site trong một mạng site - to - site VPN. Nhưng vì một lý do nào đó một site lại không hỗ trợ GRE nhưng lại đòi hỏi thiết lập IPSec VPN với các site khác. Trong trường hợp này vấn đề sẽ được giải quyết nhanh chóng nếu sử dụng IPSec Tunnel Mode.

Trong chế độ Tunnel Mode cả phần header và payload đều được mã hóa để tăng cường tính bảo mật trong việc truyền tải dữ liệu. Gói tin IP sẽ được đóng gói thêm một IP Header mới và các IPSec Header (ESP hoặc AH) sẽ được chèn giữa IP Header cũ và mới.

Các giao thức bảo mật trong IPSec gồm hai giao thức chính là ESP và AH. ESP sử dụng IP Protocol number 50 và AH sử dụng IP Protocol number 51.

Khi hoạt động ở Transport mode thì IP Header vẫn được giữ nguyên và lúc này giao thức ESP sẽ được chèn vào giữa tải (Payload) và IP Header của gói tin. Còn ở Tunnel mode thì sau khi đóng gói dữ liệu thì giao thức ESP sẽ mã hoá payload và sẽ chèn một IP Header mới vào gói tin trước khi được truyền đi.

2.4.3.2 Giao thức đóng gói tải tin an toàn ESP

❖ Giới thiệu

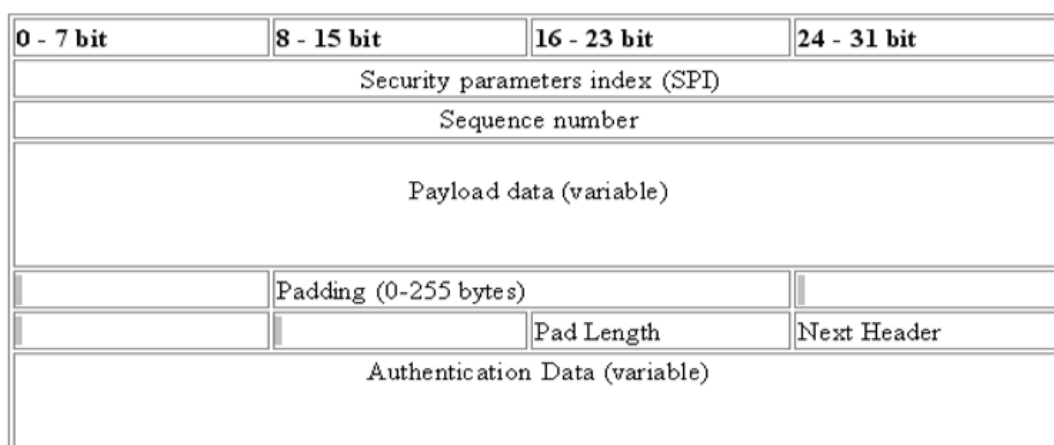
Giao thức ESP đảm nhận công việc mã hoá, xác thực và đảm bảo tính toàn vẹn dữ liệu. Sau khi đóng gói bằng giao thức ESP, mọi thông tin dùng mã hoá và giải mã gói tin sẽ nằm trong ESP Header. Các thuật toán mã hoá được dùng trong giao thức này là DES, 3DES, AES, MD5, SHA, ... ESP cũng có thể được sử dụng để mã hóa toàn bộ IP datagram hoặc phân đoạn tầng vận chuyển (TCP, UDP, ICMP, IGMP). Sự mã hoá của ESP có thể bị vô hiệu hoá thông qua thuật toán mã hoá Null ESP Algorithm. Vì vậy ESP chỉ có thể cung cấp mã hoá dữ liệu hoặc đảm bảo tính toàn vẹn dữ liệu hoặc mã hoá và đảm bảo tính toàn vẹn dữ liệu.

ESP hoạt động được ở hai chế độ Transport Mode và Tunnel Mode. Việc xử lý ESP phụ thuộc vào chế độ hoạt động của IPSec và phiên bản sử dụng của giao thức IP.

ESP thêm một header và trailer vào xung quanh nội dung của mỗi gói tin. ESP Header được cấu thành bởi hai trường là: SPI và Sequence Number.

❖ Cấu trúc gói tin ESP

Các trường trong cấu trúc một gói tin ESP được thể hiện trong hình sau:



Hình 2-9 Khuôn dạng gói ESP

SPI (chỉ số thông số an ninh): Là một số bất kì có độ dài 32 bit, mỗi đầu cuối của mỗi kết nối IPsec được tùy chọn giá trị SPI. Cùng với địa chỉ IP đích và giao thức an ninh ESP cho phép nhận dạng duy nhất chính sách SA (Security Associate) cho gói tin. SPI là trường bắt buộc và thường được lựa chọn bởi phía thu khi thiết lập SA.

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. Thường được dùng cung cấp dịch vụ anti - replay. Khi SPI được thiết lập, chỉ số này là 0. Trước khi mỗi gói tin được gửi, chỉ số này luôn tăng lên 1 và được đặt trong ESP header.

Payload Data (dữ liệu tải tin): Đây là trường bắt buộc, bao gồm một số lượng biến đổi các byte dữ liệu số 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. Thuật toán thường được dùng để mã hóa ESP là DES-CBC.

Padding (đệm): Có độ lớn trong khoảng 0 – 255 bit, là trường được thêm vào cho đủ kích thước mỗi gói tin.

Pad length (độ dài đệm): Chiều dài của padding, đây là trường bắt buộc có tác dụng xác định số byte đệm được thêm vào.

Next Header (tiêu đề tiếp theo): Là trường bắt buộc có độ dài 8 bit, nó xác định kiểu dữ liệu chứa trong phần tải tin. Trong Tunnel mode, Payload là gói tin IP, giá trị Next Header được cài đặt là 4. Trong Transport mode, Payload luôn là giao thức lớp 4. Nếu giao thức lớp 4 là TCP thì giá trị Next Header là 6, là UDP thì giá trị Next Header là 17. Mỗi ESP Trailer luôn chứa một giá trị Next Header.

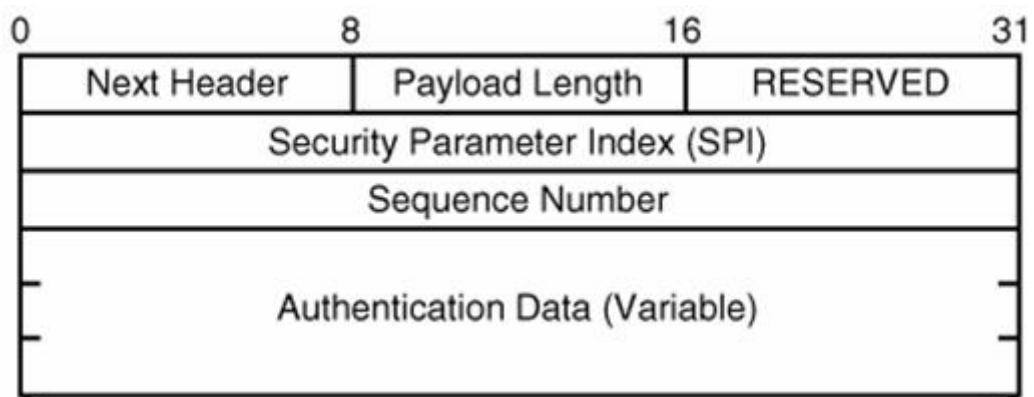
Authentication Data (dữ liệu xác thực): Trường này có độ dài biến đổi, chứa một giá trị kiểm tra tính toàn vẹn Integrity Check Value (ICV) tính trên dữ liệu của toàn bộ gói ESP trừ trường Authentication Data.

2.4.3.3 Giao thức xác thực tiêu đề AH

Authentication Header (AH) là một giao thức khóa trong kiến trúc IPsec. AH không mã hoá bất kì thành phần nào của gói tin và cung cấp tính xác thực và tính toàn vẹn cho IP datagram.

AH có thể chống phát lại bằng cách yêu cầu host đặt bit replay trong phần header để chỉ ra gói tin đã được nhìn thấy. 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.

Cấu trúc tiêu đề AH được mô tả bởi hình sau:



Hình 2-10 AH Header

Next Header (tiêu đề tiếp theo): Có độ dài 8 bit để nhận dạng loại dữ liệu của phần tải tin theo sau AH. Trong Tunnel mode, payload là gói tin IP, giá trị Next Header được đặt là 4. Trong Transport mode, payload luôn được xác định bởi giao thức của lớp Transport. Nếu giao thức lớp Transport là TCP thì giá trị Next Header là 6, còn UDP là 17.

Payload Length (độ dài tải tin): Có độ dài 8 bit chứa độ dài của tiêu đề AH.

Reserved (dự trữ): Trường 16 bit này được dùng để dự trữ cho các ứng dụng trong tương lai. Thường có giá trị bằng 0 và tham gia trong việc tính dữ liệu xác thực.

Security Parameters Index (SPI-chỉ số thông số an ninh): Có độ dài 32 bit, chứa giá trị ngẫu nhiên dùng để xác định chính sách Security Association (SA) dùng để bảo mật gói tin. Nếu giá trị này đặt là 0 thì gói tin không được bảo vệ. Giá trị ngẫu nhiên từ 1-255 đều được bảo vệ.

Sequence Number (số thứ tự): Là trường 32 bit không dấu chứa giá trị khi mỗi gói tin được gửi đi thì tăng lên 1 đơn vị. Giá trị ban đầu là 1, không bao giờ được đặt giá trị 0. Vì khi host gửi yêu cầu kiểm tra mà giá trị này không tăng lên và nó sẽ thoả thuận một SA mới nếu SA này được thiết lập. Host nhận sẽ dùng chuỗi số để phát hiện replayed datagrams. Bên nhận có thể không kiểm tra chuỗi số, nhưng bên gửi phải có để tăng giá trị này và gửi chuỗi số.

Authentication Data (dữ liệu xác thực): Chứa kết quả của giá trị Integrity Check Value (ICV). Trường này có độ dài thay đổi và luôn là bội số của 32 bit (đối với IPv4) hay 64 bit (đối với Ipv6). Có thể chứa thêm đệm nếu chiều dài của ICV trong các bytes chưa đầy.

2.4.3.4 Giao thức trao đổi khóa IKE (Internet Key Exchange)

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

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

IKE SA là quá trình hai chiều và cung cấp một kênh giao tiếp bảo mật giữa hai bên. Chức năng chủ yếu của IKE là thiết lập và duy trì các SA. IKE thực hiện quá trình dò tìm, quá trình xác thực, quản lý và trao đổi khóa. IKE sẽ dò tìm giữa hai đầu cuối IPSec và sau đó SA sẽ theo dõi tất cả các thành phần của một phiên làm việc IPSec. Sau khi đã dò tìm thành công, các thông số SA hợp lệ sẽ được lưu trữ trong cơ sở dữ liệu của SA.

Một phiên làm việc của IKE được tạo nên bởi 2 phase, phase I và II. IKE gồm có 4 chế độ chính:

- Chế độ chính (Main mode)
- Chế độ linh hoạt (Aggressive mode)
- Chế độ nhanh (Quick mode)
- Chế độ nhóm mới (New Group mode)

2.4.3.5 Quy trình hoạt động

IPSec đòi hỏi nhiều thành phần công nghệ và phương pháp mã hóa. 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
- IKE bước 1: Một tập dịch vụ được thỏa thuận và công nhận giữa các đối tượng ngang hàng.

- IKE bước 2: IKE thoả thuận các tham số SA IPSec và thiết lập “matching” các SA IPSec trong các đối tượng ngang hàng. Kết quả cuối cùng của hai bước IKE là một kênh thông tin bảo mật được tạo ra giữa các đối tượng ngang hàng.
- Truyền dữ liệu: Dữ liệu được truyền qua các đối tượng ngang hàng trên cơ sở các thông số bảo mật và các khóa đã được lưu trữ trong SA database.
- Kết thúc đường hầm: Kết thúc các SA IPSec bằng cách xóa hay timing out.

2.4.3.6 Những hạn chế của IPSec

IPSec vẫn còn ở trong giai đoạn phát triển để hướng tới hoàn thiện vì vậy vẫn tồn tại một số vấn đề cần phải giải quyết để hỗ trợ thực hiện VPN tốt hơn:

- Các gói tin được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề. Bằng cách nén dữ liệu khi mã hóa có thể khắc phục vấn đề đó nhưng các kỹ thuật này 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 cấu hình thấp.

2.4.4 SSL/TSL

2.4.4.1 Giao thức SSL (Secure Socket Layer)

Giao thức SSL nhằm mục đích bảo vệ thông tin trao đổi giữa Client và Server trong các mạng máy tính. Là giao thức tân phiên sử dụng các phương pháp mật mã cho việc bảo vệ thông tin. Dữ liệu khi truyền được giữ bí mật bằng việc mã hóa, trong khi việc tạo và kiểm tra chữ kí số đảm bảo tính xác thực và toàn vẹn thông tin.

Trong giao thức SSL có kết hợp mật mã đối xứng và bất đối xứng. Các thuật toán mật mã bất đối xứng như RSA và thuật toán Diffie – Hellman. Các hàm băm như MD5, SHA1. Các thuật toán mật mã đối xứng được hỗ trợ là RC2, RC4 và 3DES. SSL hỗ trợ các chứng chỉ số thỏa mãn chuẩn X.509.

Thủ tục thăm dò trước (bắt tay) được thực hiện trước khi bảo vệ trực tiếp sự trao đổi thông tin.

Các công việc được hoàn tất khi thực hiện thủ tục này bao gồm:

- Xác thực Client và Server
- Các điều kiện của thuật toán mật mã và nén được sử dụng
- Tạo một khóa chính bí mật
- Tạo một khóa phụ bí mật dựa trên khóa chính

2.4.4.2 Giao thức TLS

Được phát triển nhờ sử dụng SSL, TLS cho phép các Server và Client cuối liên lạc một cách an toàn qua các mạng công cộng không an toàn. Thêm vào các khả năng bảo mật được cung cấp bởi SSL, TLS cũng ngăn chặn nghe trộm, giả mạo, chặn bắt gói tin.

Trong khi triển khai VPN, SSL và TLS có thể được thực thi tạo Server VPN cũng như tại Client đầu cuối. Quá trình tạo mạng riêng ảo trên tầng phiên, tầng cao nhất thuộc mô hình OSI, nó có khả năng đạt hiệu suất cao và

các tham số về mặt chức năng cho việc trao đổi thông tin, kiểm soát truy cập là đáng tin cậy và dễ dàng quản lý.

Ngoài việc sử dụng bổ sung thêm sự bảo vệ bằng mật mã trong quá trình tạo mạng riêng ảo trên tầng phiên, nó cũng có khả năng thực thi các công nghệ Proxy. Hai giao thức SSL và TLS là hai giao thức thông dụng nhất hiện nay.

CHƯƠNG 3: THỰC NGHIỆM CẤU HÌNH VPN TRÊN THIẾT BỊ CISCO

3.1 Phát biểu bài toán

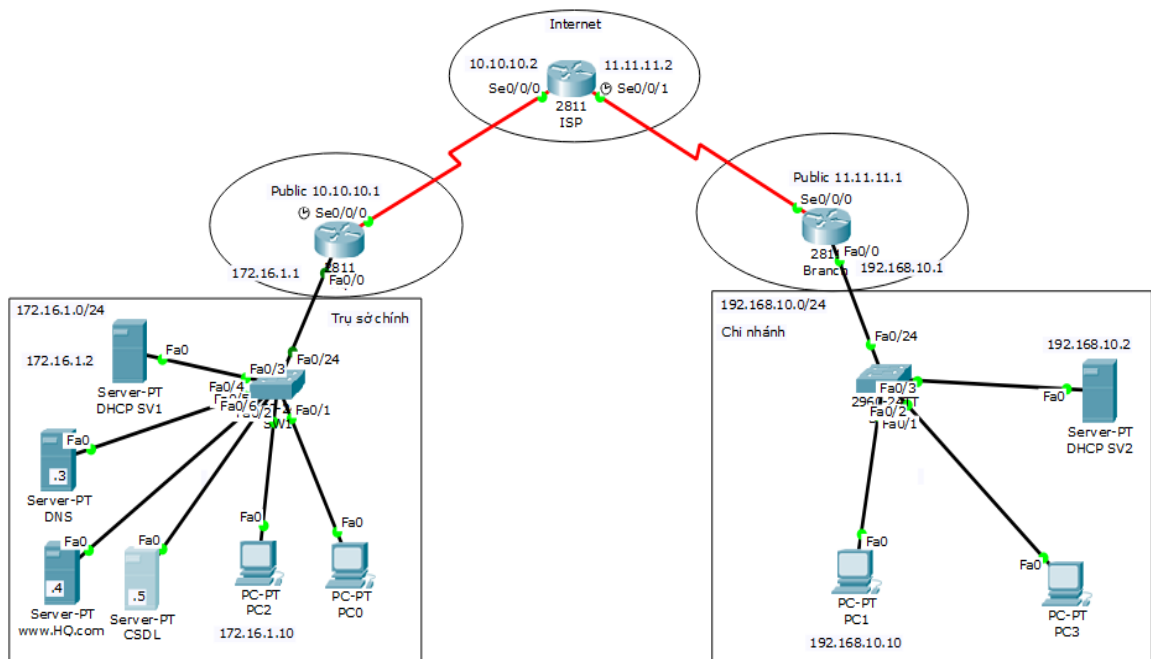
Công ty A hoạt động trong lĩnh vực thương mại. Với nhu cầu mở rộng thị trường, công ty muốn mở thêm chi nhánh tại một số thành phố trong nước. Tuy nhiên, các chi nhánh đều truy xuất chung cơ sở dữ liệu từ máy chủ được đặt tại trụ sở chính. Cùng với đó là yêu cầu đảm bảo an toàn thông tin khi chúng được trao đổi giữa các chi nhánh.

Bài toán đặt ra cho bộ phận IT đó là đưa ra một giải pháp để các chi nhánh mới có thể truy cập trực tiếp tới cơ sở dữ liệu được đặt tại trụ sở chính. Mặt khác, một số nhân viên của công ty thường xuyên phải đi công tác mong muốn truy cập đến cơ sở dữ liệu để làm việc.

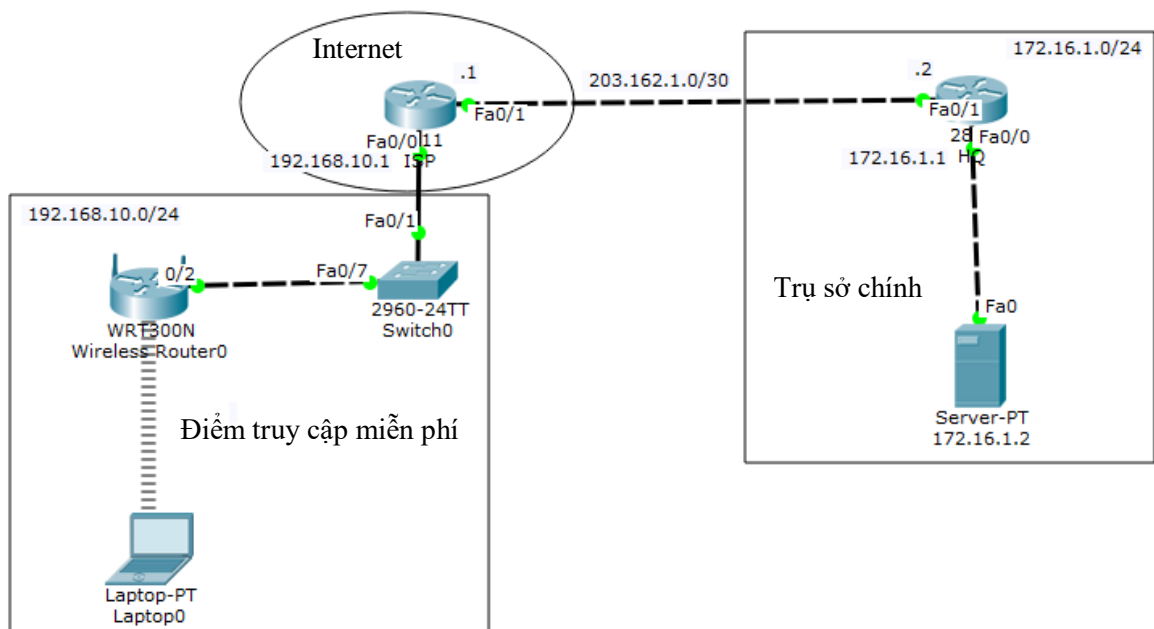
Xuất phát từ các nhu cầu nói trên, bộ phận IT đã đưa ra giải pháp triển khai hệ thống Mạng riêng ảo VPN. Trong đó, mô hình VPN Site – to – Site được đề xuất triển khai cho các chi nhánh mới và mô hình VPN Remote Access được triển khai cho nhân viên từ xa.

3.2 Triển khai thực nghiệm

3.2.1 Mô hình triển khai thực nghiệm



Hình 3-1 Mô hình VPN Site – to – Site



Hình 3-2 Mô hình VPN Remote Access

3.2.2 Giải thích mô hình

- ❖ Mô hình VPN Site – to – Site

Vùng “Trụ sở chính”: nơi đặt các máy chủ cơ sở dữ liệu của công ty như Web Server, DNS Server ... và các máy tính của các phòng ban trong công ty.

Vùng “Chi nhánh”: gồm có các máy tính của chi nhánh mới

Vùng “Internet”: là vùng ngoài công ty, cung cấp dịch vụ Internet cho công ty, quản lý bởi nhà cung cấp dịch vụ.

Để đáp ứng yêu cầu bài toán đặt ra là các máy tính tại Chi nhánh có thể truy cập trực tiếp đến Server của công ty đặt tại Trụ sở chính và các máy tính có thể truy xuất cho nhau, chúng ta tiến hành cấu hình VPN Site – to – Site cho router được đặt tại Trụ sở chính (Router HQ) và router đặt tại Chi nhánh (Router Branch). Một số yêu cầu kèm theo khi cấu hình là:

- Các máy tính tại Trụ sở chính có địa chỉ IP nằm trong dải 172.16.1.0/24 được cấp động qua DHCP Server (địa chỉ IP: 172.16.1.2).
- DNS server (địa chỉ IP: 172.16.1.3) dùng để phân giải tên miền cho Webserver (địa chỉ IP: 172.16.1.4).
- Các máy tính tại Chi nhánh có địa chỉ IP nằm trong dải địa chỉ 192.168.10.0/24 được cấp động qua DHCP Server (IP: 192.168.10.2).

❖ Mô hình VPN Remote Access

Vùng “Trụ sở chính”: nơi đặt máy chủ cơ sở dữ liệu của của công ty.

Vùng “Điểm truy cập miễn phí”: các điểm wifi công cộng nơi mà nhân viên công ty đến công tác.

Vùng “Internet”: cung cấp dịch vụ Internet, quản lý bởi nhà cung cấp dịch vụ.

Để đáp ứng yêu cầu bài toán là các nhân viên của công ty khi đi công tác xa vẫn có thể truy cập vào cơ sở dữ liệu tại trụ sở chính để làm việc, chúng ta cần cấu hình VPN Remote Access cho router đặt tại Trụ sở chính (router HQ). Một số yêu cầu kèm theo khi cấu hình:

- Máy tính cá nhân của nhân viên từ xa được cấp IP động thông qua Router Wireless nằm trong dải IP 192.168.10.0/24.
- Máy chủ cơ sở dữ liệu đặt tại Trụ sở chính có địa chỉ IP: 172.16.1.2.

3.2.3 Cấu hình thực nghiệm

Sử dụng phần mềm Cisco Packet Tracer để xây dựng mô hình giả lập cho hai bài toán VPN Site – to – Site và VPN Remote Access.

3.2.3.1 Mô hình VPN Site – to – Site

Tiến hành cấu hình cơ bản cho router HQ, router Branch và router ISP của mô hình.

Cấu hình VPN Site – to – Site cho router HQ:

- Assign Router cho router HQ
Router(config)#hostname HQ
HQ(config)#int f0/0
HQ(config-if)#ip address 172.16.1.1 255.255.255.0
HQ(config-if)#no shutdown
HQ(config-if)#int s0/0/0
HQ(config-if)#ip address 10.10.10.1 255.255.255.0
HQ(config-if)#no shutdown
- Configure Default Router
HQ(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
- Tạo Internet Key Exchange (IKE) key policy.
HQ(config)#crypto isakmp enable
HQ(config)#crypto isakmp policy 20
HQ(config-isakmp)#authentication pre-share
HQ(config-isakmp)#encryption 3des
HQ(config-isakmp)#hash md5

```
HQ(config-isakmp)#group 1
```

```
HQ(config-isakmp)#lifetime 3600
```

```
HQ(config-isakmp)#exit
```

```
HQ(config)#crypto isakmp key cisco123 address 11.11.11.1
```

- Configure VPN Site to Site

Configure ISAKMP policy:

```
HQ(config)#crypto isakmp enable
```

```
HQ(config)#crypto isakmp policy 20
```

```
HQ(config-isakmp)#authentication pre-share
```

```
HQ(config-isakmp)#encryption 3des
```

```
HQ(config-isakmp)#hash md5
```

```
HQ(config-isakmp)#group 1
```

```
HQ(config-isakmp)#lifetime 3600
```

```
HQ(config-isakmp)#exit
```

```
HQ(config)#crypto isakmp key cisco123 address 11.11.11.1
```

- Define IPSec Transform Set:

```
HQ(config)#crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

- Create Accesslist:

```
HQ(config)#access-list 100 permit ip 172.16.1.0 0.0.0.255 192.168.10.0  
0.0.0.255
```

- Create Crypto map for IPSec:

```
HQ(config)#crypto map mymap 20 ipsec-isakmp  
HQ(config-crypto-map)#set peer 11.11.11.1  
HQ(config-crypto-map)#set transform-set myset  
HQ(config-crypto-map)#match address 100  
HQ(config-crypto-map)#exit
```

- Apply the crypto map:

```
HQ(config)#int s0/0/0  
HQ(config)#crypto map mymap
```

- Testing and Verity VPN:

```
HQ#show crypto isakmp sa  
HQ#show crypto ipsec sa
```

Cấu hình tương tự cho router Branch.

3.2.3.2 Kết quả

- Hình ảnh của router HQ sau khi cấu hình đầy đủ:

```
HQ#show run
Building configuration...

Current configuration : 1130 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 20
  encr 3des
  hash md5
  authentication pre-share
  lifetime 3600
!
crypto isakmp key cisco123 address 11.11.11.1
!
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
```

Hình 3-3 Cấu hình Router HQ

```
crypto map mymap 20 ipsec-isakmp
  set peer 11.11.11.1
  set transform-set myset
  match address 100
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface FastEthernet0/0
  ip address 172.16.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  ip address 10.10.10.1 255.255.255.0
  clock rate 2000000
  crypto map mymap
!
```

Hình 3-4 Cấu hình Router HQ

```
interface Serial0/0/1
  no ip address
  clock rate 2000000
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
!
ip flow-export version 9
!
!
access-list 100 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end

HQ#
```

Hình 3-5 Cấu hình Router HQ

- Hình ảnh router Branch sau khi cấu hình đầy đủ:

```
Branch#show run
Building configuration...

Current configuration : 1116 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Branch
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 20
  encr 3des
  hash md5
  authentication pre-share
  lifetime 3600
!
crypto isakmp key cisco123 address 10.10.10.1
!
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
```

Hình 3-6 Cấu hình Router Branch

```
crypto map mymap 20 ipsec-isakmp
  set peer 10.10.10.1
  set transform-set myset
  match address 100
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  ip address 11.11.11.1 255.255.255.0
  crypto map mymap
!
```

Hình 3-7 Cấu hình Router Branch


```
interface Serial0/0/1
  no ip address
  clock rate 2000000
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.2
!
ip flow-export version 9
!
!
access-list 100 permit ip 192.168.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end

Branch#
```

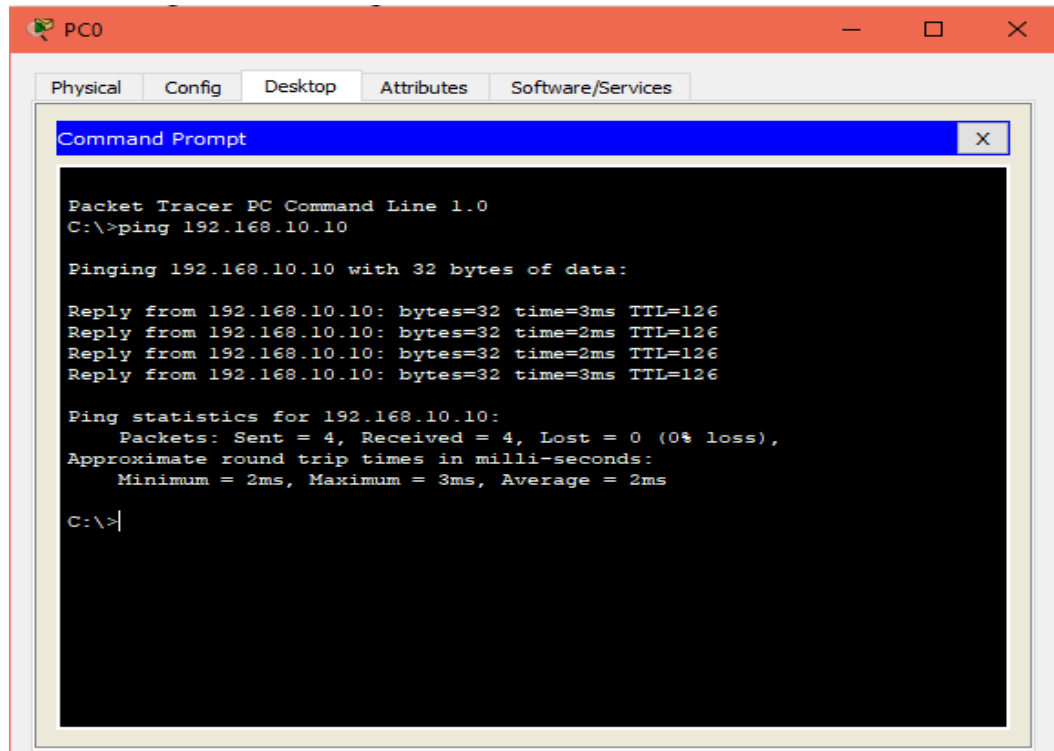
Hình 3-8 Cấu hình Router Branch

- Hình ảnh router ISP sau khi cấu hình đầy đủ:


```
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  ip address 10.10.10.2 255.255.255.0
!
interface Serial0/0/1
  ip address 11.11.11.2 255.255.255.0
  clock rate 2000000
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
ip route 172.16.1.0 255.255.255.0 10.10.10.1
ip route 192.168.10.0 255.255.255.0 11.11.11.1
!
ip flow-export version 9
!
!
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
```

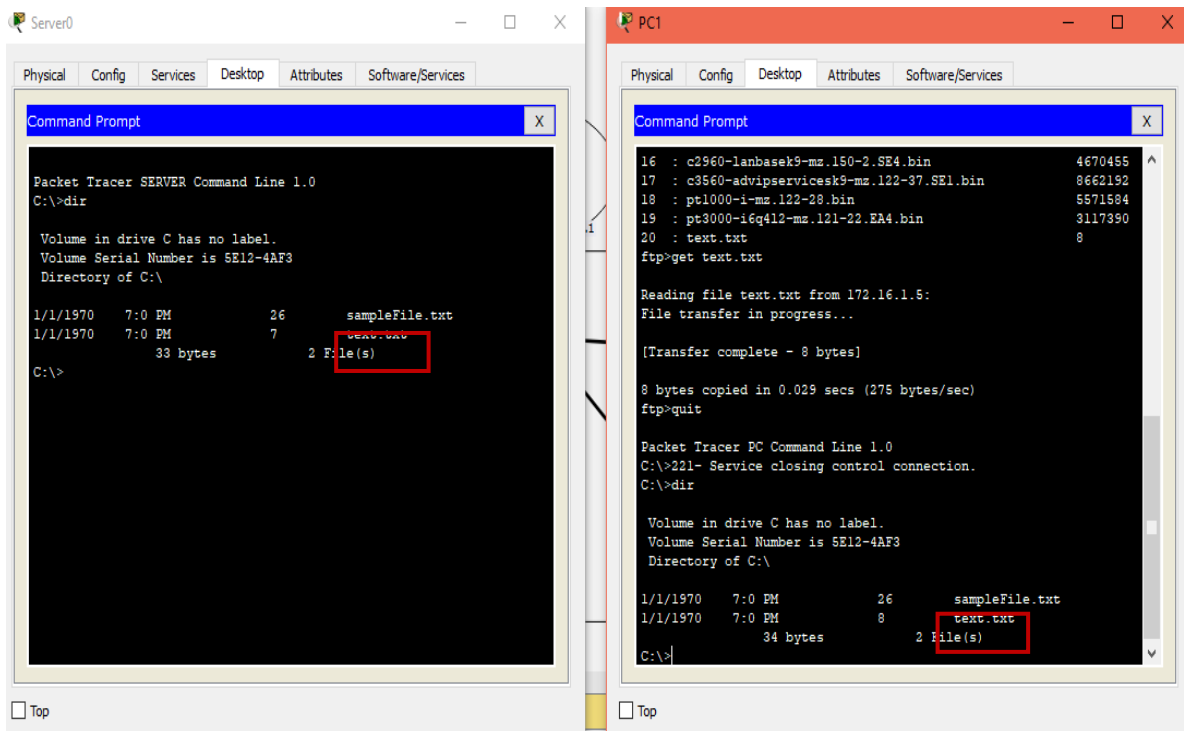
Hình 3-9 Cấu hình Router ISP

- Hình ảnh PC0 ở Trụ sở chính ping tới PC1 ở Chi nhánh thành công:

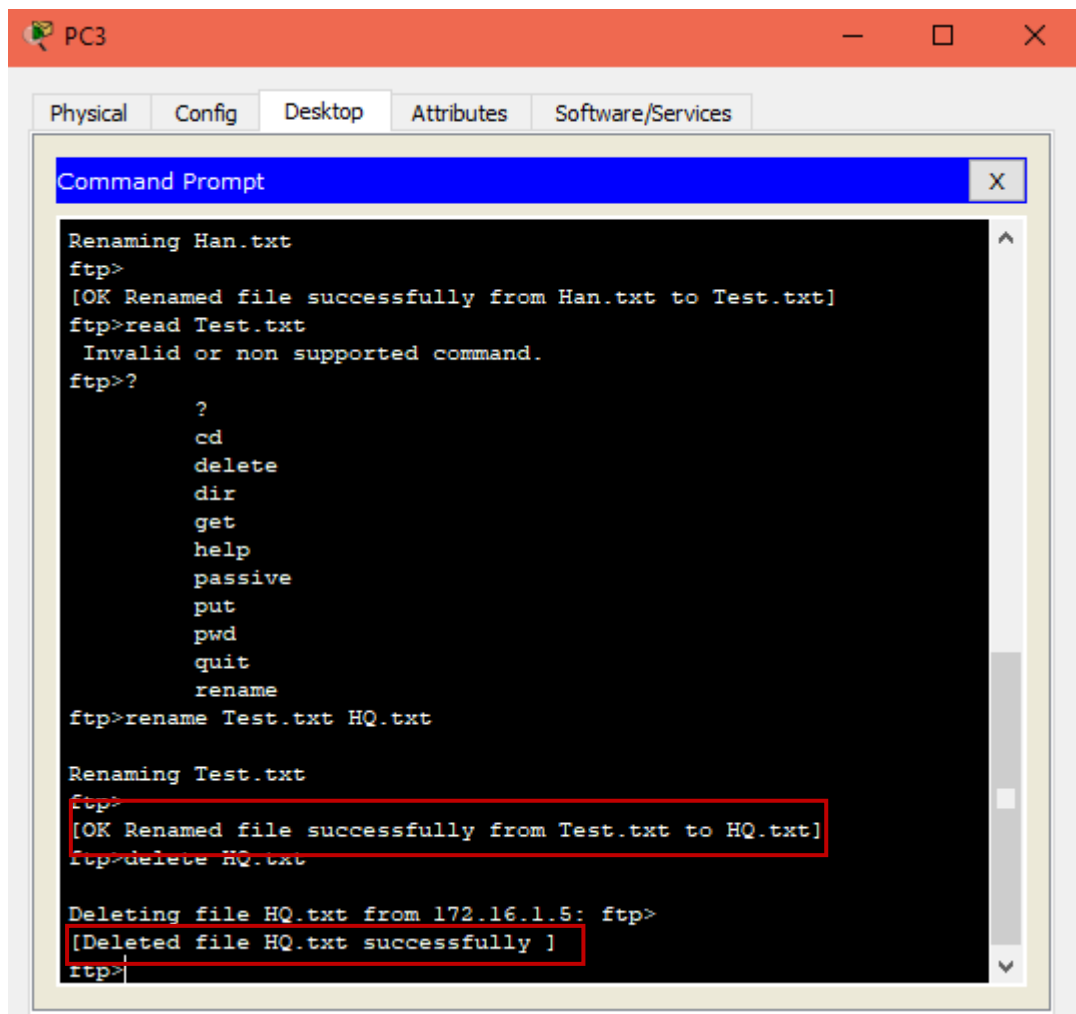


Hình 3-10 Ping thông giữa các máy Client

- Hình ảnh PC1 ở Chi nhánh kết nối thành công tới Server ở Trụ sở chính và lấy được dữ liệu từ Server nội bộ:



Hình 3-11 Truy xuất dữ liệu thành công



Hình 3-12 Thao tác với dữ liệu tại máy chủ

3.2.3.3 Mô hình VPN Remote Access

Cấu hình cơ bản cho router ISP và HQ.

Cấu hình Remote Access cho router HQ:

- Cấp chứng thực AAA trên router HQ theo phương thức local:
 HQ(config)# username cisco password cisco
 HQ(config)# aaa new-model
 HQ(config)# aaa authentication login default local none
- Tạo IP pool cho VPN client sử dụng để kết nối VPN:
 HQ(config)# ip local pool VPNCLIENTS 172.16.1.10 172.16.1.20
- Cấu hình Group Authorization (nhóm thẩm định với VPN Server):

```
HQ(config)# aaa authorization network VPNAUTH local
```

- Tạo IKE Policy và Group (sử dụng pre-share key và dùng AES để mã hóa với 256 bit):

```
HQ(config)# crypto isakmp policy 10
```

```
HQ(config-isakmp)# authentication pre-share
```

```
HQ(config-isakmp)# encryption aes 256
```

```
HQ(config-isakmp)# group 2
```

- Tạo ISAKMP group là ttggroup và password 123:

```
HQ(config)# crypto isakmp client configuration group ttggroup
```

```
HQ(config-isakmp-group)# key 123
```

```
HQ(config-isakmp-group)# pool VPNCLIENTS
```

```
HQ(config-isakmp-group)# netmask 255.255.255.0
```

- Cấu hình IPsec Transform sử dụng thuật toán 3DES và SHA-HMAC:

```
HQ(config)# crypto ipsec transform-set mytrans esp-3des esp-sha-hmac
```

- Tạo 1 Dynamic Crypto Map:

```
HQ(config)# crypto dynamic-map mymap 10
```

```
HQ(config-crypto-map)# set transform-set mytrans
```

```
HQ(config-crypto-map)# reverse-route
```

```
HQ(config)# crypto map mymap client configuration address respond
```

```
HQ(config)# crypto map mymap isakmp authorization list VPNAUTH
```

```
HQ(config)# crypto map mymap 10 ipsec-isakmp dynamic mymap
```

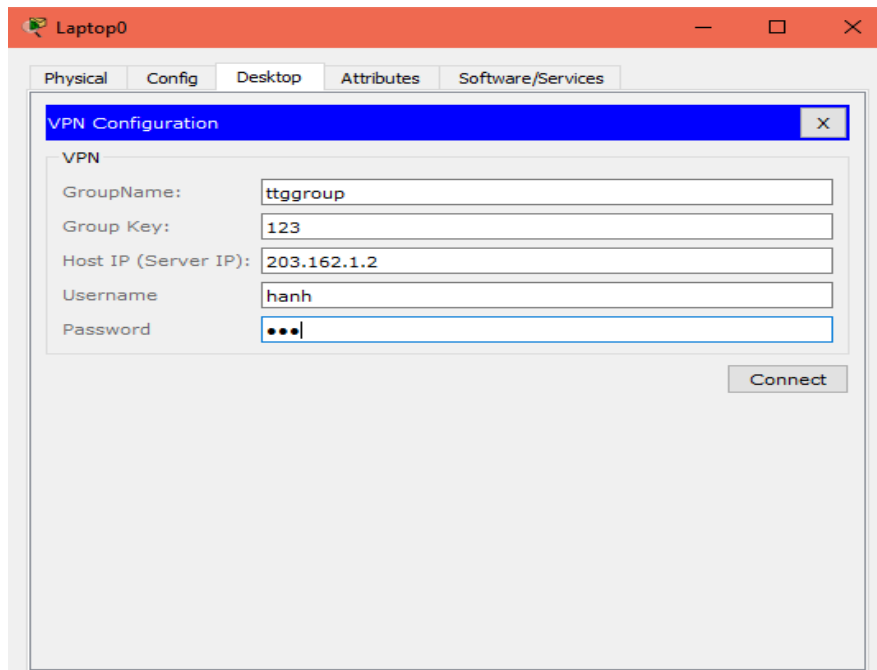
- Cấu hình user chứng thực:

```
HQ(config)# aaa authentication login VPNAUTH local
```

```
HQ(config)# username hanh password 123
```

```
HQ(config)# crypto map mymap client authentication list VPNAUTH
```

- Khởi tạo kết nối VPN tại máy Remote Access:



Hình 3-13 Khởi tạo kết nối VPN Remote Access

Thông tin khởi tạo kết nối VPN:

- Tên nhóm (GroupName): ttgroup
- Khóa nhóm (Group Key): 123
- Địa chỉ máy chủ (Host IP): 203.162.1.2
- Tên người dùng (Username): hanh
- Mật khẩu (Password): 123

3.2.3.4 Kết quả

- Router HQ sau khi cấu hình:

```
interface FastEthernet0/0
  ip address 172.16.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 203.162.1.2 255.255.255.252
  duplex auto
  speed auto
  crypto map mymap
!
interface Vlan1
  no ip address
  shutdown
!
ip local pool VPNCLIENTS 172.16.1.10 172.16.1.20
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ip flow-export version 9
!
!
access-list 100 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
!
!
!
end
```

Hình 3-14 Cấu hình Router HQ

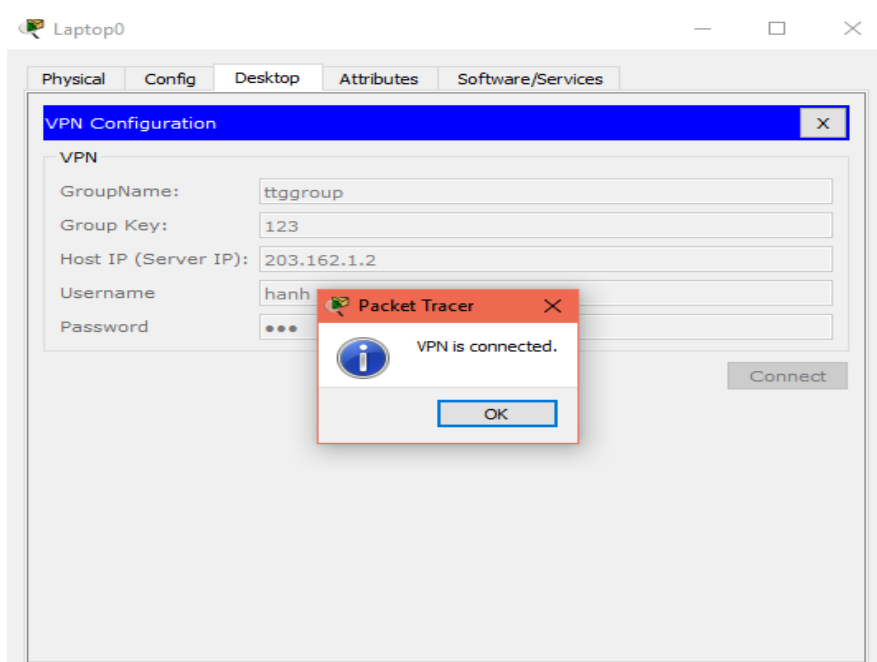
- Router ISP sau khi cấu hình:

```

interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 !
interface FastEthernet0/1
 ip address 203.162.1.1 255.255.255.252
 duplex auto
 speed auto
 !
interface Vlan1
 no ip address
 shutdown
 !
ip classless
 !
ip flow-export version 9
 !
 !
 !
 !
 !
 !
 !
line con 0
 !
line aux 0
 !
line vty 0 4
 login
 !
 !
 !
end
    
```

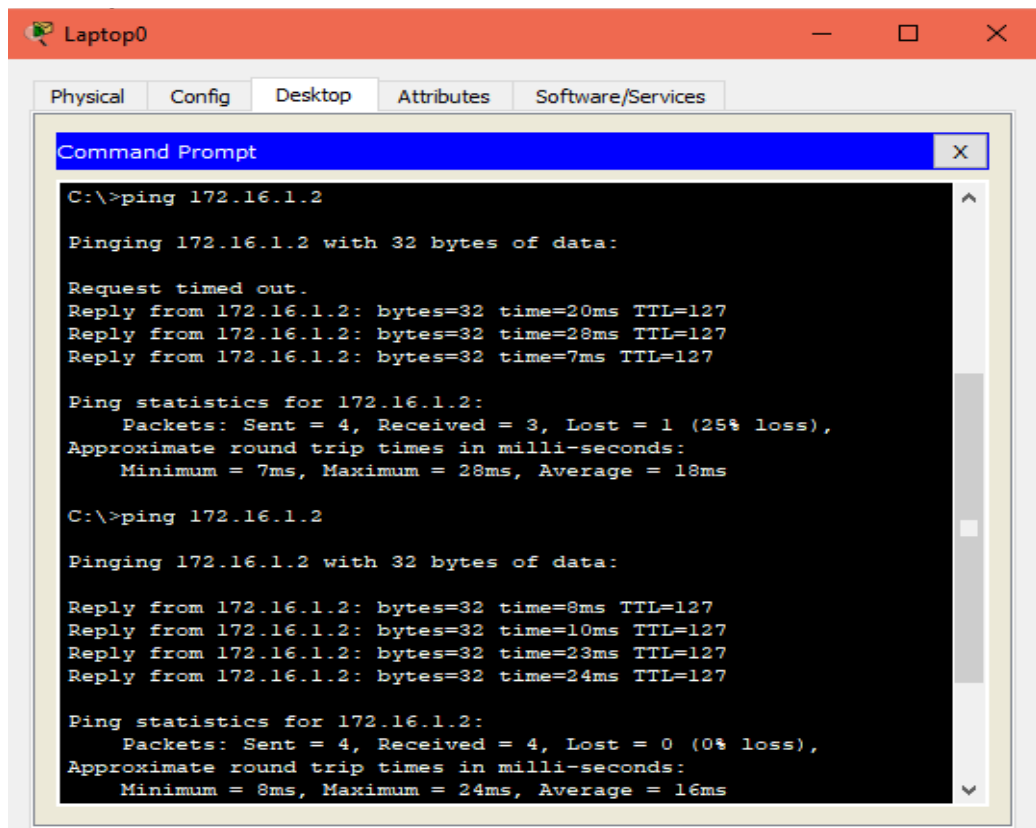
Hình 3-15 Cấu hình Router ISP

- Khởi tạo kết nối VPN thành công:



Hình 3-16 Khởi tạo kết nối VPN

- Ping thành công từ máy Remote Access tới Server tại HQ:



```
C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.2: bytes=32 time=20ms TTL=127
Reply from 172.16.1.2: bytes=32 time=28ms TTL=127
Reply from 172.16.1.2: bytes=32 time=7ms TTL=127

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 28ms, Average = 18ms

C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=8ms TTL=127
Reply from 172.16.1.2: bytes=32 time=10ms TTL=127
Reply from 172.16.1.2: bytes=32 time=23ms TTL=127
Reply from 172.16.1.2: bytes=32 time=24ms TTL=127

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 24ms, Average = 16ms
```

Hình 3-17 Ping thành công từ máy Remote Access tới Server

KẾT LUẬN

Đồ án “*Tìm hiểu về mạng riêng ảo và ứng dụng*” đã đạt được những kết quả như sau:

Về lý thuyết, đồ án đã trình bày và hiểu được:

- Tổng quan về an ninh mạng, các lỗ hổng bảo mật, một số phương thức tấn công mạng và một số giải pháp bảo mật.
- Tìm hiểu về Mạng riêng ảo VPN, các giao thức của VPN, ưu điểm và nhược điểm của VPN.

Về thực nghiệm, đồ án đã tiến hành:

- Cấu hình thực nghiệm VPN Site – to – Site và VPN Remote Access trên thiết bị Cisco thông qua phần mềm Cisco Packet Tracer.

Tuy nhiên, trong quá trình thực hiện đồ án, do năng lực còn hạn chế, thời gian cũng như khả năng đọc hiểu tiếng Anh trong quá trình nghiên cứu các tài liệu. Cũng như các chức năng của phần mềm Cisco Packet Tracer còn hạn chế nên trong đồ án vẫn còn tồn tại nhiều thiếu sót. Em rất mong nhận được sự đóng góp ý kiến của thầy cô để có thể khắc phục và hoàn thiện nội dung đồ án cũng như tiếp tục nghiên cứu sâu hơn phục vụ cho quá trình làm việc về sau.

TÀI LIỆU THAM KHẢO

- [1]. <http://vnpro.org/forum/>
- [2]. <http://www.nhatnghe.com/forum/>
- [3]. <http://www.ciscopress.com/>
- [4]. Greg Bastien & Christian Abera Degu, “CCSP Self-Study CCSP SECUR Exam Certification Guide”.
- [5]. Silviu Angelescu, “CCNA Certification All in One for Dummies”.
- [6]. Kỹ thuật mạng riêng ảo, tác giả ThS. Trần Công Hùng, NXB Bưu Điện năm 2002.