**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**------------------**



**Báo cáo môn học**

**Nhập môn an toàn thông tin**

**Đề tài: Bảo mật cho mạng IP, Ipsec,**

**Mạng riêng ảo VNP, Ứng dụng**

**Giáo viên hướng dẫn: PGS.TS Nguyễn Linh Giang**

**Nhóm sinh viên: Nhóm 9**

Bùi Phó Bền 20172968

Đồng Văn Hiệp 20173104

Lê Tùng Lâm 20173218

Phùng Ngọc Minh 20173257

**Hà Nội - tháng 6, 2020**

**Hà Nội – Tháng 6 Năm 2020**

**Thành phố Hồ Chí Minh - Năm 2014**

Mục lục

[**GIỚI THIỆU** 3](#_Toc43069246)

[**NỘI DUNG** 4](#_Toc43069247)

[1. Giao thức IP 4](#_Toc43069248)

[1.1. Tổng quát 4](#_Toc43069249)

[1.2. Các giao thức trong mạng IP 5](#_Toc43069250)

[1.3. Các bước hoạt động của mạng IP 6](#_Toc43069251)

[2. Các nguy cơ tấn công mạng IP 7](#_Toc43069252)

[2.1. Tấn công TCP Syn Flood 7](#_Toc43069253)

[2.2. Giả mạo địa chỉ IP (IP Spoofing) 7](#_Toc43069254)

[2.3. Hack kết nối (Connection Hacking) 9](#_Toc43069255)

[2.4. Tấn công giao thức định tuyến RIP 9](#_Toc43069256)

[2.5. Tấn công tràn ngập gói tin ICMP 10](#_Toc43069257)

[2.6. Tấn công giả mạo DNS( DNS Spoofing Attack) 11](#_Toc43069258)

[3. IPsec(Internet Protocol Security) 11](#_Toc43069259)

[3.1. Tổng quan về IPsec 11](#_Toc43069260)

[3.2. Kiến trúc IPSec: 13](#_Toc43069261)

[3.2.1. Kiến trúc: 13](#_Toc43069262)

[3.2.2. Chế độ hoạt động (mode): 14](#_Toc43069263)

[3.2.3. Khung giao thức của IPSec: 15](#_Toc43069264)

[3.2.4. Các tính năng của IPSec: 16](#_Toc43069265)

[3.2.5. Giao thức Authentication Header (AH): 16](#_Toc43069266)

[3.2.6. Giao thức Encapsulating Security Payload (ESP): 18](#_Toc43069267)

[3.2.7. Quản lý khóa với IKE: 20](#_Toc43069268)

[3.3. Hoạt động của IPSec: 21](#_Toc43069269)

[3.4. Ưu, nhược điểm của IPSec và ứng dụng: 21](#_Toc43069270)

[3.4.1. Ưu điểm: 21](#_Toc43069271)

[3.4.2. Nhược điểm: 22](#_Toc43069272)

[3.4.3. Ứng dụng: 22](#_Toc43069273)

[4. Virtual Private Network(VPN): 23](#_Toc43069274)

[4.1. Tổng quan về VPN: 23](#_Toc43069275)

[4.1.1. Giới thiệu 23](#_Toc43069276)

[4.1.2. Chức năng của VPN 24](#_Toc43069277)

[4.1.3. Ưu điểm 24](#_Toc43069278)

[4.1.4. Các yêu cầu cơ bản đối với một giải pháp VPN 26](#_Toc43069279)

[4.1.5. Đường hầm và mã hóa 27](#_Toc43069280)

[4.2. Phân loại VPN: 28](#_Toc43069281)

[4.3 Các giao thức trong VPN: 29](#_Toc43069282)

[4.3.1. Giới thiệu về giao thức đường hầm: 29](#_Toc43069283)

[4.3.2. Giao thức đường hầm điểm tới điểm PPTP 30](#_Toc43069284)

[4.3.3. Giao thức chuyển tiếp lớp 2 (L2F) 32](#_Toc43069285)

[4.3.4 Giao thức đường hầm lớp 2 L2TP(Layer 2 Tunneling Protocol) 34](#_Toc43069286)

[4.3.5. Giao thức GRE (Generic Routing Encapsulation) 36](#_Toc43069287)

[4.3.6. Giao thức IPSec: 37](#_Toc43069288)

[4.4. Quy trình tạo và sử dụng VPN 37](#_Toc43069289)

[5. Ứng dụng của VNP 37](#_Toc43069290)

[**KẾT LUẬN** 39](#_Toc43069291)

**GIỚI THIỆU**

Internet là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau. Hệ thống này truyền thông tin theo kiểu nối chuyển gói dữ liệu (packet switching) dựa trên một giao thức liên mạng đã được chuẩn hóa (giao thức IP). Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của các doanh nghiệp, của các viện nghiên cứu và các trường đại học, của người dùng cá nhân và các chính phủ trên toàn cầu... Mạng Internet mang lại rất nhiều tiện ích hữu dụng cho người sử dụng, một trong các tiện ích phổ thông của Internet là hệ thống thư điện tử (email), trò chuyện trực tuyến (chat),công cụ tìm kiếm (search engine), các dịch vụ thương mại và chuyển ngân và các dịch vụ về y tế giáo dục như là chữa bệnh từ xa hoặc tổ chức các lớp học ảo. Chúng cung cấp một khối lượng thông tin và dịch vụ khổng lồ trên Internet. Trong thập kỷ qua, Internet đã phát triển bùng nổ với tốc độ chóng mặt trên toàn thế giới cả về số lượng và về kĩ thuật. Và sự phát triển đó không có dấu hiệu sẽ dừng lại. Sự phát triển không chỉ đơn giản là số lượng lớn thành viên mới kết nối vào hệ thống Internet mỗi giờ mà còn là sự xâm nhập của nó vào các khía cạnh cuộc sống hiện đại, vào các hoạt động thương mại với quy mô lớn nhỏ khác nhau...

Ban đầu, các tổ chức cơ quan sử dụng Internet để giới thiệu các sản phẩm và dịch vụ bằng các website của mình. Cùng với thời gian, nó sẽ phát triển thành thương mại điện tử, mọi hoạt động kinh doanh, các giao dịch được thực hiện qua mạng internet. Bài toán đặt ra là làm thế nào để bảo mật an toàn cho các dữ liệu trong quá trình truyền qua mạng? Làm thế nào có thể bảo vệ chống lại các cuộc tấn công trong quá trình truyền tải các dữ liệu đó? Sau đây chúng ta sẽ đi tìm hiểu về bảo mật các dữ liệu qua mạng IP, IPSec và mạng VPN.

# 

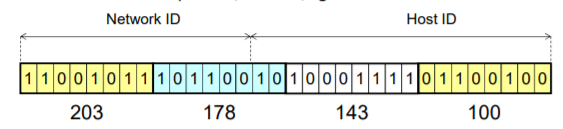
**NỘI DUNG**

# 1. Giao thức IP

## 1.1. Tổng quát

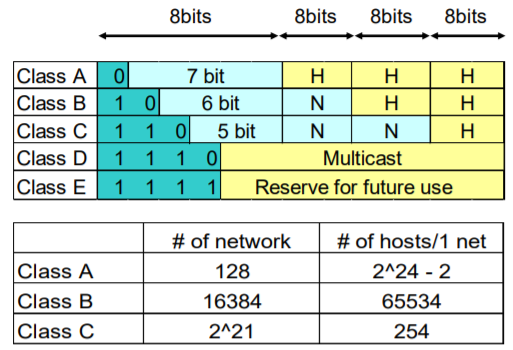
Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết(connectionless) có ý nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Sơ đồ địa chỉ hóa để định danh các trạm(host) trong liên mạng được gọi là địa chỉ IP 32 bits(32 bit IP address). Mỗi giao diện trong một máy có hỗ trợ giao thức IP đều phải được gán 1 địa chỉ IP (một máy tính có thể gắn mới nhiều mạng , do vậy có thể có nhiều địa chỉ IP). Địa chỉ IP gồm 2 phần: địa chỉ mạng(network id) và địa chỉ máy(host id) . Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng (mỗi vùng 1 byte) có thể biểu thị dưới dạng thập phân, bát phân, thập lục phân hay nhị phân. Cách phổ biến nhất là dùng thập phân có dấu chấm để tách các vùng. Mục đích của địa chỉ IP là định danh duy nhất cho một máy tính bất kỳ trên liên mạng.



Do tổ chức và độ lớn của các mạng con (subnet) của liên mạng có thể khác nhau, người ta chia các địa chỉ IP thành 5 lớp, ký hiệu là A, B, C, D và E. Trong lớp A, B, C chứa địa chỉ có thể gán được. Lớp D dành riêng cho lớp kỹ thuật multicasting. Lớp E được dành những ứng dụng trong tương lai.

Netid trong địa chỉ mạng dùng để nhận dạng từng mạng riêng biệt. Các mạng liên kết phải có địa chỉ mạng (netid) riêng cho mỗi mạng. Ở đây các bit đầu tiên của byte đầu tiên được dùng để định danh lớp địa chỉ (0 - lớp A, 10 - lớp B, 110 - lớp C, 1110 - lớp D và 11110 - lớp E).



Ở đây ta xét cấu trúc của các lớp địa chỉ có thể gán được là lớp A, lớp B, lớp C

Cấu trúc của các địa chỉ IP như sau:

* Mạng lớp A: địa chỉ mạng (netid) là 1 Byte và địa chỉ host (hostid) là 3 byte.
* Mạng lớp B: địa chỉ mạng (netid) là 2 Byte và địa chỉ host (hostid) là 2 byte
* Mạng lớp C: địa chỉ mạng (netid) là 3 Byte và địa chỉ host (hostid) là 1 byte.

Lớp A cho phép định danh tới 126 mạng, với tối đa 16 triệu host trên mỗi mạng. Lớp này được dùng cho các mạng có số trạm cực lớn.

Lớp B cho phép định danh tới 16384 mạng, với tối đa 65534 host trên mỗi mạng.

Lớp C cho phép định danh tới 2 triệu mạng, với tối đa 254 host trên mỗi mạng. Lớp này được dùng cho các mạng có ít trạm.

*Một số địa chỉ có tính chất đặc biệt*: Một địa chỉ có hostid = 0 được dùng để hướng tới mạng định danh bởi vùng netid. Ngược lại, một địa chỉ có vùng hostid gồm toàn số 1 được dùng để hướng tới tất cả các host nối vào mạng netid, và nếu vùng netid cũng gồm toàn số 1 thì nó hướng tới tất cả các host trong liên mạng

## 1.2. Các giao thức trong mạng IP

Để mạng với giao thức IP hoạt động được tốt người ta cần một số giao thức bổ sung, các giao thức này đều không phải là bộ phận của giao thức IP và giao thức IP sẽ dùng đến chúng khi cần.

* *Giao thức ARP (Address Resolution Protocol):* Ở đây cần lưu ý rằng các địa chỉ IP được dùng để định danh các host và mạng ở tầng mạng của mô hình OSI, và chúng không phải là các địa chỉ vật lý (hay địa chỉ MAC) của các trạm trên đó một mạng cục bộ (Ethernet, Token Ring.). Trên một mạng cục bộ hai trạm chỉ có thể liên lạc với nhau nếu chúng biết địa chỉ vật lý của nhau. Như vậy vấn đề đặt ra là phải tìm được ánh xạ giữa địa chỉ IP (32 bits) và địa chỉ vật lý của một trạm. *Giao thức ARP* đã được xây dựng để tìm địa chỉ vật lý từ địa chỉ IP khi cần thiết.
* *Giao thức RARP (Reverse Address Resolution Protocol)*: Là giao thức ngược với *giao thức ARP.* Giao thức RARP được dùng để tìm địa chỉ IP từ địa chỉ vật lý.
* *Giao thức ICMP (Internet Control Message Protocol):* Giao thức này thực hiện truyền các thông báo điều khiển (báo cáo về các tình trạng các lỗi trên mạng.) giữa các gateway hoặc một nút của liên mạng. Tình trạng lỗi có thể là: một gói tin IP không thể tới đích của nó, hoặc một router không đủ bộ nhớ đệm để lưu và chuyển một gói tin IP, Một thông báo ICMP được tạo và chuyển cho IP. IP sẽ "bọc" (encapsulate) thông báo đó với một IP header và truyền đến cho router hoặc trạm đích.

## 1.3. Các bước hoạt động của mạng IP

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.

Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

* Tạo một IP datagram dựa trên tham số nhận được.
* Tính checksum và ghép vào header của gói tin.
* Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
* Chuyển gói tin xuống tầng dưới để truyền qua mạng.

Đối với router, khi nhận được một gói tin đi qua, nó thực hiện các động tác sau:

1) Tính checksum , nếu sai thì loại bỏ gói tin.

2) Giảm giá trị tham số Time - to Live. nếu thời gian đã hết thì loại bỏ gói tin.

3) Ra quyết định chọn đường.

4) Phân đoạn gói tin, nếu cần.

5) Kiến tạo lại IP header, bao gồm giá trị mới của các vùng Time - to -Live, Fragmentation và Checksum.

6) Chuyển datagram xuống tầng dưới để chuyển qua mạng.

Cuối cùng khi một datagram nhận bởi một thực thể IP ở trạm đích, nó sẽ thực hiện bởi các công việc sau:

1) Tính checksum. Nếu sai thì loại bỏ gói tin.

2) Tập hợp các đoạn của gói tin (nếu có phân đoạn)

3) Chuyển dữ liệu và các tham số điều khiển lên tầng trên.

# 2. Các nguy cơ tấn công mạng IP

## 2.1. Tấn công TCP Syn Flood

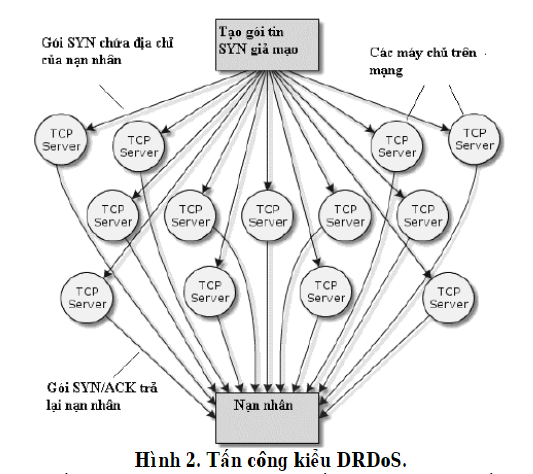
Kiểu tấn công TCP SYN Flood là một kiểu tấn công trực tiếp vào máy chủ bằng cách tạo ra một số lượng lớn các kết nối TCP nhưng không hoàn thành các kết nối này. Hacker sử dụng cơ chế bắt tay ba bước trong quá trình thiết lập kết nối giữa hai thực thể TCP. Máy hacker sử dụng một địa chỉ giả mạo và gửi hàng loạt bản tin yêu cầu kết nối tới máy tính nạn nhân với bit SYN được bật (bước 1), khi đó nạn nhân nhận được gói tin này ngay lập tức nó sẽ dành một phần bộ nhớ cho kết nối này, máy tính nạn nhân nhận được yêu cầu trên thì trả lời lại với bản tin bit ACK, SEQ được bật (bước 2) và chờ để hacker trả lời, nhưng hacker không trả lời điều này sẽ làm cho máy tính nạn nhân luôn ở trong tình trạng chờ và dần dần sẽ cạn kiệt tài nguyên không thể phục vụ được nữa.

## 2.2. Giả mạo địa chỉ IP (IP Spoofing)

Địa chỉ IP giả mạo liên quan đến việc tạo ra các gói TCP/IP sử dụng địa chỉ IP giả với mục đích để che giấu danh tính hoặc giả mạo danh tính chủ sở hữu của địa chỉ IP được sử dụng. Hành vi này có thể thực hiện các cuộc tấn công khác nhau như sau:

• Tấn công từ chối dịch vụ (Denial of Service Attack-DoS): Hacker có thể gửi một số lượng lớn các gói tin yêu cầu kết nối (SYN) tới máy nạn nhân mà không cần quan tâm phản hồi (ACK) vì Hacker sẽ không nhận được bất kỳ gói tin phản hồi từ các nạn nhân. Tất cả gói phản hồi sẽ được hướng tới các địa chỉ IP giả mạo. Ngoài ra, danh tính của kẻ tấn công cũng sẽ không được tiết lộ. Cuộc tấn công này làm cho nạn nhân bị loại khỏi dịch vụ.

• Tấn công từ chối dịch vụ phản xạ nhiều vùng (Distributed Reflection DOS- DRDoS): Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy nạn nhân, làm tắc nghẽn hoàn toàn đường kết nối từ máy nạn nhân vào xương sống của Internet và làm tiêu hao tài nguyên. Trong suốt quá trình máy nạn nhân bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy nạn nhân đó, tất cả các dịch vụ chạy trên nền TCP/IP như: DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa. Hacker sử dụng các server phản xạ, hacker sẽ gửi yêu cầu kết nối (SYN) tới các server có bandwidth rất cao trên mạng – server phản xạ, các gói tin yêu cầu kết nối này mang địa chỉ IP giả - chính là địa chỉ IP của máy nạn nhân. Các server phản xạ này gửi lại máy nạn nhân các gói SYN/ACK dẫn tới hiện tượng nhân băng thông – bandwidth multiplication (Hình 2)



• Tấn công môi trường xác thực bằng địa chỉ IP: Là tấn công môi trường xác thực dựa trên địa chỉ IP. Trong trường hợp mạng nội bộ, xác thực bằng địa chỉ IP, không cần một tên đăng nhập hoặc mật khẩu để truy cập. Hacker có thể giả địa chỉ IP để có được quyền truy cập trái phép vào máy tính nạn nhân mà không xác thực..

• Kiểu tấn công người đứng giữa (Man in The Middle Attack): Nó liên quan đến việc hack một phiên liên lạc được xác thực giữa hai máy tính A và B. Hacker sau khi hoàn thành các bước xác thực sẽ giả mạo địa chỉ IP của một nạn nhân A hoặc B đã được xác thực và nhận được các gói tin qua lại giữa hai máy A và B..

**Các biện pháp bảo vệ chống lại tấn công IP Spoofing được đưa ra sau đây:**

• Dùng mật mã xác thực: Nếu cả hai đầu của cuộc nói chuyện đã được xác thực, khả năng tấn công theo kiểu Man-in-the-Middle Attack có thể được ngăn chặn. Mã hoá traffic giữa các thiết bị (giữa 2 router, hoặc giữa 2 hệ thống đầu cuối và router) bằng một IPSec tunnel.

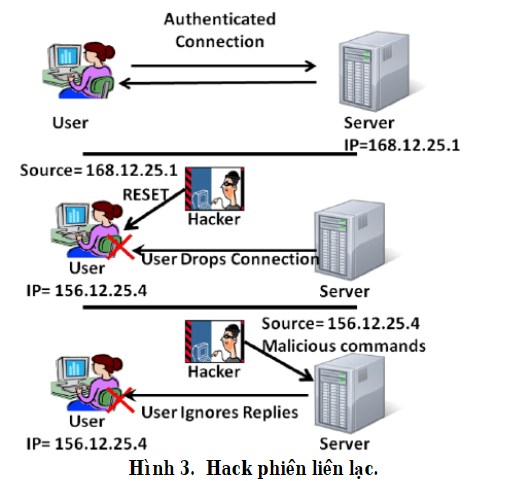
• Dùng danh sách kiểm tra truy cập Access Control List (ACL) trên các interface của router. Một ACL có thể được dùng để loại bỏ những traffic từ bên ngoài mà lại được đóng

gói bởi một địa chỉ trong mạng cục bộ khi bị lôi cuốn vào một cuộc tấn công DDoS.

• Bộ lọc các gói dữ liệu: Điều này ngăn chặn các gói tin gửi đến, chúng không đáp ứng các tiêu chí chính sách bảo mật, như các yêu cầu ping từ bên ngoài mạng được lọc. Tương tự như vậy, gói tin đi ra cũng có thể được lọc dựa trên tiêu chí địa chỉ cổng, IP của nguồn hoặc đích.

• Sử dụng lớp trên: Kết hợp cơ chế phòng vệ ở tầng trên có thể ngăn chặn IP giả mạo như sử dụng số thứ tự trong trường số thứ tự của gói tin TCP ở tầng giao vận như vậy kẻ tấn công phải đoán được số thứ tự trước khi giả mạo gói tin.

## 2.3. Hack kết nối (Connection Hacking)



Xác thực giữa User và Server diễn ra trong giai đoạn đầu thiết lập kết nối. Từ đó không có yêu cầu xác nhận. Như Hình 3, hacker có thể lợi dụng điều này bằng cách giả mạo địa chỉ IP của Server (168.12.25.1) gửi một thiết lập lại cho User và sau đó hacker tiếp tục giả mạo địa chỉ IP của User (156.12.25.4) tiếp tục phiên làm việc với Server bằng sử dụng địa chỉ IP giả mạo. Một cách khác của việc hack phiên liên lạc là Hacker có thể ăn cắp tập tin cookie được lưu trữ trên máy nạn nhân hoặc có được cookie của máy nạn nhân bằng cách nghe lén (Sniffer) các gói tin trên mạng không được mã hóa. Sau đó, những cookie có thể được sử dụng với các Web server để thiết lập một phiên xác thực. Các biện pháp phòng chống hack kết nối được chỉ ra trong như sau:

• Mã hóa: Mã hóa bảo đảm cho việc trao đổi gói tin giữa User và Server không bị Hacker đọc được nội dung và cũng không thể sử dụng chúng cho việc cướp quyền.

• Sử dụng tái xác thực: Yêu cầu xác thực định kỳ sau một thời gian nhất định.

## 2.4. Tấn công giao thức định tuyến RIP

Routing Information Protocol (RIP) là một giao thức định tuyến được sử dụng trong bộ giao thức TCP/IP để định tuyến các gói dựa trên số chặng (hop). Trước khi đưa ra quyết định định tuyến RIP đếm số bước nhảy trên mọi hướng có thể và chọn đường đi tới đích có số bước nhảy ngắn nhất. Giá trị đếm hop tối đa có thể là 15 hop và bất cứ trường hợp nào lớn hơn 15 được coi là vô hạn. Cơ chế này được sử dụng để tránh gói tin rơi vào vòng lặp. Phiên bản chuẩn của RIP không có phần xác thực. Thông tin cung cấp trong bản tin RIP thường được sử dụng mà không có sự kiểm tra xác thực lại chính nó. Hacker có thể giả mạo 1 bản tin RIP, ví dụ xác định máy X có tuyến ngắn nhất ra ngoài mạng. Như vậy, mọi gói tin gửi ra từ mạng này sẽ được định tuyến qua X và máy X có thể kiểm soát, sửa đổi gói tin. Để phòng chống lại tấn công giao thức RIP, sử dụng một số biện pháp:

• Sử dụng thuật toán xác thực mật khẩu đơn giản, làm cho việc tấn công qua RIP khó khăn hơn.

• Giải pháp IPsec VPN cũng cung cấp khả năng mã hóa thông tin định tuyến qua các router sử dụng IPsec VPN.

• Các gói dữ liệu được lọc dựa trên mã nguồn và đích.

• Phân tích nhật ký (log) thường xuyên nhằm phát hiện bất thường.

• Kiểm tra các đường truyền trước khi chấp nhận

## 2.5. Tấn công tràn ngập gói tin ICMP

Giao thức Internet Control Message Protocol (ICMP) thực hiện truyền các thông báo điều khiển (báo cáo về tình trạng lỗi trên mạng ...) giữa các gateway hay các trạm của liên mạng. Tình trạng lỗi có thể là: một datagram không thể tới được đích của nó, hoặc một router không đủ bộ đệm để lưu và chuyển một datagram. Ping là một chương trình dùng để báo cho người sử dụng biết hai host trên mạng có thông với nhau không. Ping dựa trên giao thức ICMP. Nó cho phép người sử dụng gửi các gói tin tới một hệ thống ở xa và hiển thị khoảng thời gian từ khi gửi gói tin đến khi nhận được phản hồi từ phía nhận (Round Trip Time: RTT). Gói tin được gửi đi là ICMP echo request, gói tin phản hồi là ICMP echo receive. Hacker sẽ sử dụng giao thức ICMP này để tấn công nạn nhân theo cách sau:

• Bước 1: Kẻ tấn công giả mạo là nạn nhân, gửi đi một lệnh Ping với địa chỉ IP là của nạn nhân và địa chỉ đích là dạng broadcast của một mạng nào đó. Sau bước này tất cả các host trong mạng 10.0.0.x sẽ nhận được gói tin ICMP từ host của nạn nhân.

• Bước 2: Do sự nhầm lẫn như trên mà tất cả các host trong mạng 10.0.0.x đều gửi về cho nạn nhân một gói tin ICMP echo receive. Hàng loạt các gói tin dạng này là nguyên nhân gây nên hiện tượng làm băng thông tới host của nạn nhân bị chiếm dụng. Nạn nhân sẽ không thể giao dịch với các host khác trên mạng.

**Phòng chống lại các cuộc tấn công ICMP có bằng các biện pháp sau đây:**

• Đối với các firewall cứng, kích hoạt cơ chế ICMP Flooding Protection.

• Đối với các firewall mềm trên linux như iptables, có thể sử dụng lệnh sau:

*# iptables –A INPUT –p icmp –m limit–limit 2/second –limit-burst 2 –j ACCEPT*

• Đối với hệ điều hành window, chặn toàn bộ các gói tin ping bằng cách sử dụng lệnh sau trên cmd:

*# netsh firewall set icmpsetting type all mode disable*

## 2.6. Tấn công giả mạo DNS( DNS Spoofing Attack)

Domain Name System (DNS) là một dịch vụ được sử dụng trong lớp ứng dụng để ánh xạ một địa chỉ IP sang một tên miền và ngược lại. Tấn công giả mạo DNS liên quan tới nhiễm độc bộ nhớ đệm DNS (DNS cache poisoning), hay còn được gọi là giả mạo DNS, là một kiểu tấn công khai thác lỗ hổng trong hệ thống tên miền (DNS – domain name system) để chuyển hướng lưu lượng truy cập Internet từ máy chủ hợp pháp tới các máy chủ giả mạo. Cách phòng chống giả mạo DNS được đề cập:

• Sử dụng xác thực dựa trên địa chỉ IP thay vì dựa trên tên miền.

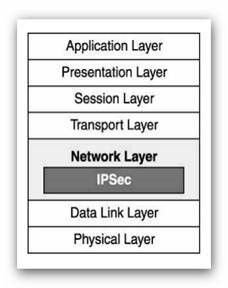
• Sử dụng mã hóa để ngăn chặn giả mạo DNS.

# 3. IPsec(Internet Protocol Security)

## 3.1. Tổng quan về IPsec

IP Security (IPSec) là một giao thức được chuẩn hoá bởi IETF từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Nó là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.

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 (Network layer) trong mô hình OSI. (Đó là lý do tại sao IPSec được phát triển ở giao thức tầng 3 thay vì tầng 2).



IPSec trong mô hình OSI

IPSec được thiết kế như phần mở rộng của giao thức IP, được thực hiện thống nhất trong cả hai phiên bản IPv4 và IPv6. Đối với IPv4, việc áp dụng IPSec là một tùy chọn, nhưng đối với IPv6, giao thức bảo mật này được triển khai bắt buộc.

IPSec có hai cơ chế cơ bản để đảm bảo an toàn dữ liệu đó là AH (Authentication Header) và ESP (Encapsulating Security Payload), trong đó IPSec phải hỗ trợ ESP và có thể hỗ trợ AH:

+ AH cho phép xác thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn dữ liệu và dịch vụ tùy chọn chống phát lại của các gói IP truyền giữa hai hệ thống. AH không cung cấp tính bảo mật, điều này có nghĩa là nó gửi đi thông tin dưới dạng bản rõ.

+ ESP là một giao thức cung cấp tính an toàn của các gói tin được truyền bao gồm: Mật mã dữ liệu, xác thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn phi kết nối của dữ liệu. ESP đảm bảo tính bí mật của thông tin thông qua việc mật mã gói tin IP. Tất cả lưu lượng ESP đều được mật mã giữa hai hệ thống. Với đặc điểm này thì xu hướng sẽ sử dụng ESP nhiều hơn AH để tăng tính an toàn cho dữ liệu.

+ Cả AH và ESP là các phương tiện cho điều khiển truy nhập, dựa vào sự phân phối của các khóa mật mã và quản lý các luồng giao thông có liên quan đến những giao thức an toàn này.

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

SPI

Destination IP Address

Security Protocol

+ SPI(Security Parameter Index):là một trường 32 bits dùng nhận dạng các giao thức bảo mật, được định nghĩa bởi các trường Security protocol trong bộ IPSec đang dùng. SPI như là phần đầu của giao thức bảo mật và thường chọn bởi hệ thống đích trong suốt quá trình thỏa thuận của SA.

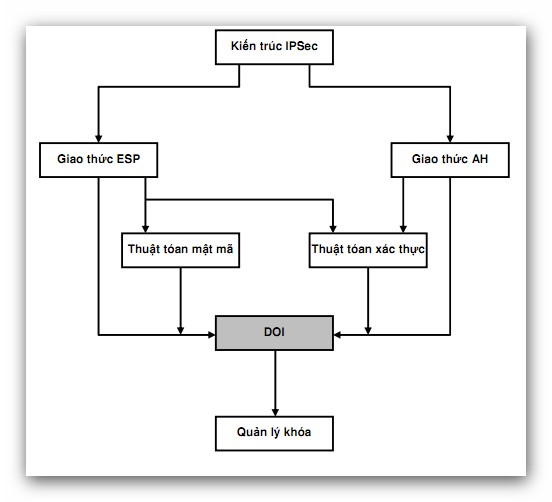
+Destination IP address:địa chỉ IP của nút đích. Cơ chế quản lý của SA chỉ được định nghĩa cho hệ thống unicast mặc dù nó có thể là hệ thống broadcast, unicast hay multicast.

+Security protocol: mô tả giao thức bảo mật IPSec, là AH hoặc ESP. SA trong IPSec được triển khai theo 2 chế độ :transport mode và tunnel mode.

## 3.2. Kiến trúc IPSec:

### 3.2.1. Kiến trúc:

IPSec là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá… Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản sau đây, mỗi thành phần được định nghĩa trong một tài liệu riêng tương ứng:



- **Kiến trúc IPSec (RFC 2401)**: Quy định các cấu trúc, các khái niệm và yêu cầu của IPSec.

- **Giao thức ESP (RFC 2406):** Mô tả giao thức ESP, là một giao thức mật mã và xác thực thông tin trong IPSec.

- **Giao thức AH (RFC 2402)**: Định nghĩa một giao thức khác với chức năng gần giống ESP. Như vậy khi triển khai IPSec, người sử dụng có thể chọn dùng ESP hoặc AH, mỗi giao thức có ưu và nhược điểm riêng.

- **Thuật toán mật mã:** Định nghĩa các thuật toán mã hoá và giải mã sử dụng trong IPSec. IPSec chủ yếu dựa vào các thuật toán mã hoá đối xứng.

- **Thuật toán xác thực:** Định nghĩa các thuật toán xác thực thông tin sử dụng trong AH và ESP.

- **Quản lý khóa (RFC 2408)**: Mô tả các cơ chế quản lý và trao đổi khóa trong IPSec.

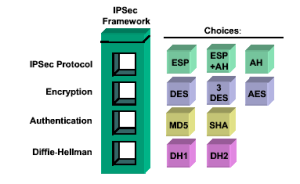
- **Miền thực thi (Domain of Interpretation – DOI):** Định nghĩa môi trường thực thi IPSec. IPSec không phải là một công nghệ riêng biệt mà là sự tổ hợp của nhiều cơ chế, giao thức và kỹ thuật khác nhau, trong đó mỗi giao thức, cơ chế đều có nhiều chế độ hoạt động khác nhau. Việc xác định một tập các chế độ cần thiết để triển khai IPSec trong một tình huống cụ thể là chức năng của miền thực thi.

### 3.2.2. Chế độ hoạt động (mode):

IPsec có thể được hoạt động theo chế độ vận chuyển (transport mode) từ máy chủ này đến máy chủ khác cũng như chế độ đường hầm (tunnel mode) trong mạng:

* Chế độ vận chuyển: Transport mode cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn (TCP, UDP hoặc ICMP). Chỉ có trọng tải (dữ liệu được truyền) của gói tin IP mới được mã hóa và/hoặc chứng thực. Trong quá trình Routing cả IP header đều không bị chỉnh sửa hay mã hóa. Transport mode sử dụng trong tình huống giao tiếp host to host.
* Chế độ Tunnel: Trong chế độ tunnel, toàn bộ gói tin IP sẽ được mã hóa và/hoặc chứng thực. Sau đó nó được đóng gói vào một gói tin IP mới với tiêu đề IP mới. Khi đó các gói IP gốc được xem như di chuyển trong một đường hầm (tunnel) từ đầu này đến đầu kia của mạng mà các nút trung gian không xen vào được. Chế độ tunnel được sử dụng để tạo Virtual Private Network (mạng riêng ảo) phục vụ cho việc liên lạc giữa các mạng, liên lạc giữa máy chủ và mạng (ví dụ như truy cập người sử dụng từ xa), và giữa các máy chủ.

### 3.2.3. Khung giao thức của IPSec:



*Khung giao thức được sử dụng trong IPSec*

*Một số tính năng được khuyến khích sử dụng khi làm việc với IPSec:*

**– Các giao thức bảo mật IPSec**

+ AH (Authentication Header)

+ ESP (Encapsulating Security Payload)

**– Các thuật toán mã hóa**

+ DES (Data Encryption Standard)

+ 3 DES (Triple DES)

**– Các chức năng toàn vẹn dữ liệu**

+ HMAC (Hash – based Message Authentication Code)

+ MD5 (Message Digest 5)

+ SHA-1 (Secure Hash Algorithm -1)

**– Các phương pháp xác thực (peer Authentication)**

+ Rivest, Shamir, and Adleman (RSA) Digital Signatures

+ RSA Encrypted Nonces

**– Các giao thức quản lý khoá**

+ DH (Diffie- Hellman)

+ CA (Certificate Authority)

**– Các chính sách an ninh**

+ IKE (Internet Key Exchange)

+ ISAKMP (Internet Security Association and Key Management Protocol)

### 3.2.4. Các tính năng của IPSec:

Để thực hiện được chức năng chính của mình là bảo mật dữ liệu trong VPN, IPSec cung cấp những tính năng sau:

***Sự bảo mật dữ liệu (Data Confidentiality):*** Đảm bảo dữ liệu được an toàn, tránh những kẻ tấn công phá hoại bằng cách thay đổi nội dung hoặc đánh cắp dữ liệu quan trọng. Việc bảo vệ dữ liệu được thực hiện bằng các thuật toán mã hóa như DES, 3DES và AES. Tuy nhiên, đây là một tính năng tùy chọn trong IPSec.

***Sự toàn vẹn dữ liệu (Data Integrity)****:* Đảm bảo rằng dữ liệu không bị thay đổi trong suốt quá trình trao đổi. Data Integrity bản thân nó không cung cấp sự an toàn dữ liệu. Nó sử dụng thuật toán băm (hash) để kiểm tra dữ liệu bên trong gói tin có bị thay đổi hay không. Những gói tin nào bị phát hiện là đã bị thay đổi thì sẽ bị loại bỏ. Những thuật toán băm: MD5 hoặc SHA-1.

***Chứng thực nguồn dữ liệu (Data Origin Authentication):*** Mỗi điểm cuối của VPN dùng tính năng này để xác định đầu phía bên kia có thực sự là người muốn kết nối đến mình hay không. Lưu ý là tính năng này không tồn tại một mình mà phụ thuộc vào tính năng toàn vẹn dữ liệu. Việc chứng thực dựa vào những kĩ thuật: Pre-shared key, RSA-encryption, RSA-signature.

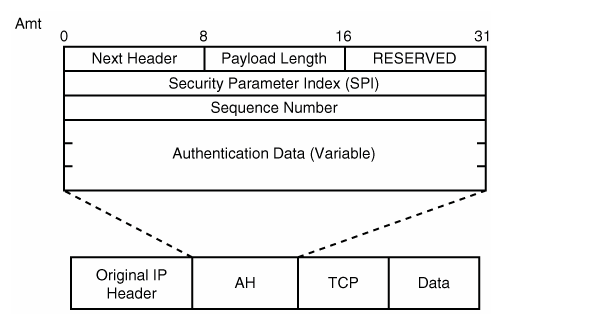
***Tránh trùng lặp (Anti-replay):*** Đảm bảo gói tin không bị trùng lặp bằng việc đánh số thứ tự. Gói tin nào trùng sẽ bị loại bỏ, đây cũng là tính năng tùy chọn.

### 3.2.5. Giao thức Authentication Header (AH):

AH (Authentication Header) là một giao thức xác thực dùng trong IPSec, có chức năng đảm bảo tính toàn vẹn của dữ liệu chuyển đi trên mạng IP. AH cho phép xác thực người dùng, xác thực ứng dụng và thực hiện các cơ chế lọc gói tương ứng. Ngoài ra, AH còn có khả năng chống tấn công giả danh (spoofing) và tấn công phát lại (replay).

Cơ chế hoạt động của AH dựa trên mã xác thực MAC (Message Authentication Code), do đó, để thực thi AH thì hai đầu cuối của SA phải dùng chung một khóa bí mật.

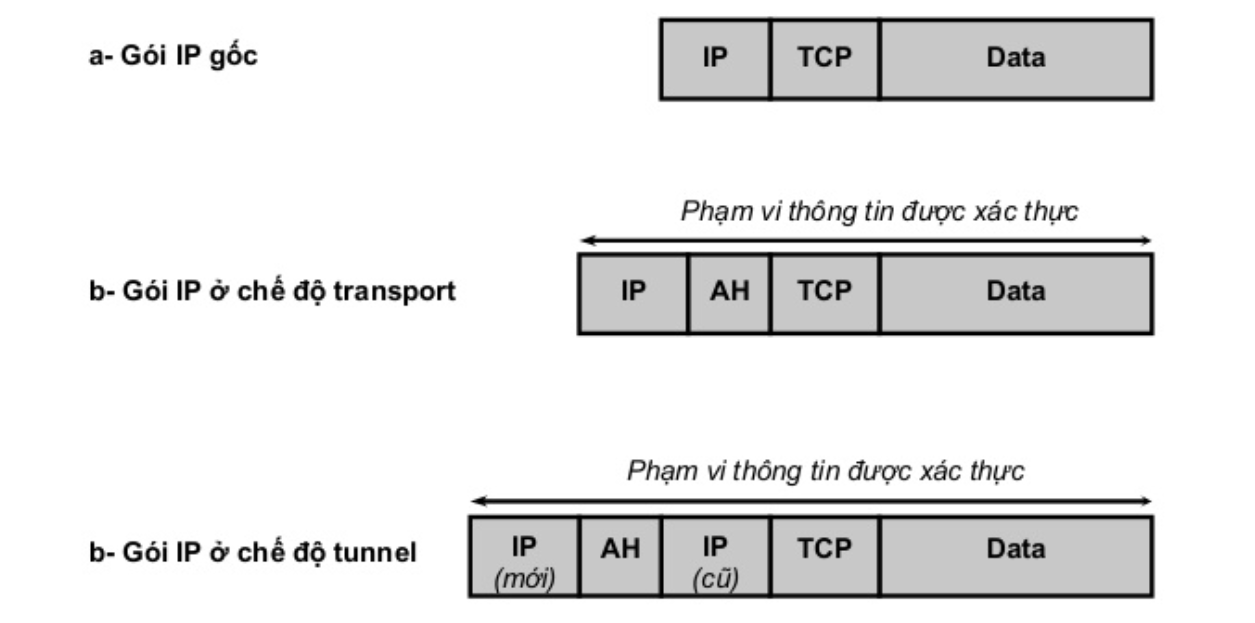
* ***Cấu trúc tiêu đề của gói AH :***



* *Next Header (tiêu đề kế tiếp - 8 bit):* nhận dạng kiểu tiêu đề đi liền sau tiêu đề của AH.
* *Payload Length (kích thước dữ liệu - 8 bit):* Chiều dài của gói AH, tính bằng đơn vị 32 bit trừ đi 2. Ví dụ, chiều dài phần dữ liệu xác thực là 96 bit (=3\*32 bit), cộng với chiều dài phần tiêu đề AH (cố định) là 3\*32 bit nữa thành 6\*32 bit, khi đó giá trị của trường kích thước dữ liệu là 4.
* *Reserved (Dành riêng - 16 bit):* Phần riêng, chưa dùng.
* *Security Parameters Index (SPI - 32 bits) :* nhận dạng SA.
* *Sequence Number (số thứ tự gói - 32 bits):* số thứ tự.
* *Authentication Data (Mã xác thực):* dữ liệu xác thực, có chiều dài thay đổi nhưng phải là bội số của 32. Trường này chứa giá trị kiểm tra ICV (Integrity Check Value) hoặc MAC (Message Authentication Code) cho toàn bộ gói.
* ***Quá trình xử lý AH:***

Hoạt động của AH được thực hiện qua các bước như sau:

* *Bước 1:* Toàn bộ gói IP (bao gồm IP header và tải tin) được thực hiện qua một hàm băm một chiều.
* *Bước 2:* Mã hash thu được dùng để xây dựng một AH header, đưa header này vào gói dữ liệu ban đầu.
* *Bước 3*: Gói dữ liệu sau khi thêm AH header được truyền tới đối tác IPSec.
* *Bước 4*: Bên thu thực hiện hàm băm với IP header và tải tin, kết quả thu được một mã hash.
* *Bước 5*: Bên thu tách mã hash trong AH header.
* *Bước 6:* Bên thu so sánh mã hash mà nó tính được mà mã hash tách ra từ AH header. Hai mã hash này phải hoàn toàn giống nhau. Nếu khác nhau chỉ một bit trong quá trình truyền thì 2 mã hash sẽ không giống nhau, bên thu lập tức phát hiện tính không toàn vẹn của dữ liệu.
* ***Áp dụng giao thức AH trong 2 chế độ transport mode và tunnel mode:***



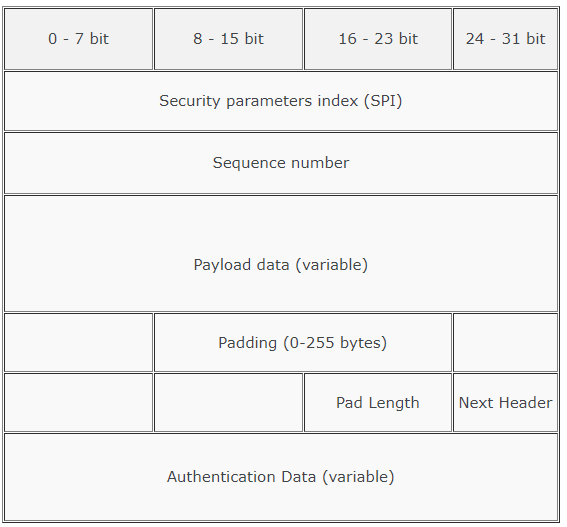
* ***Các thuật toán xác thực:***

Thuật toán xác thực sử dụng để tính ICV được xác định bởi kết hợp an ninh SA (Security Association). Đối với truyền thông điểm tới điểm, các thuật toán xác thực thích hợp bao gồm các hàm băm một chiều (MD5, SHA-1). Đây chính là những thuật toán bắt buộc mà một ứng dụng AH phải hỗ trợ.

### 3.2.6. Giao thức Encapsulating Security Payload (ESP):

Cũng như AH, giao thức này được phát triển hoàn toàn cho IPSec. Chức năng chính của giao thức này là cung cấp tình bảo mật cho dữ liệu truyền trên mạng IP bằng các kỹ thuật mật mã. Thêm vào đó, ESP cũng cung cấp nhận thực nguồn gốc dữ liệu, kiểm tra tính toàn vẹn dữ liệu, dịch vụ chống phát lại và một số giới hạn về luồng lưu lượng cần bảo mật. Dịch vụ bảo mật được cung cấp độc lập với các dịch vụ khác. Do đó khi dùng ESP, người dùng có thể lựa chọn hoặc không lựa chọn chức năng xác thực, còn chức năng mã hóa là chức năng mặc định của ESP.

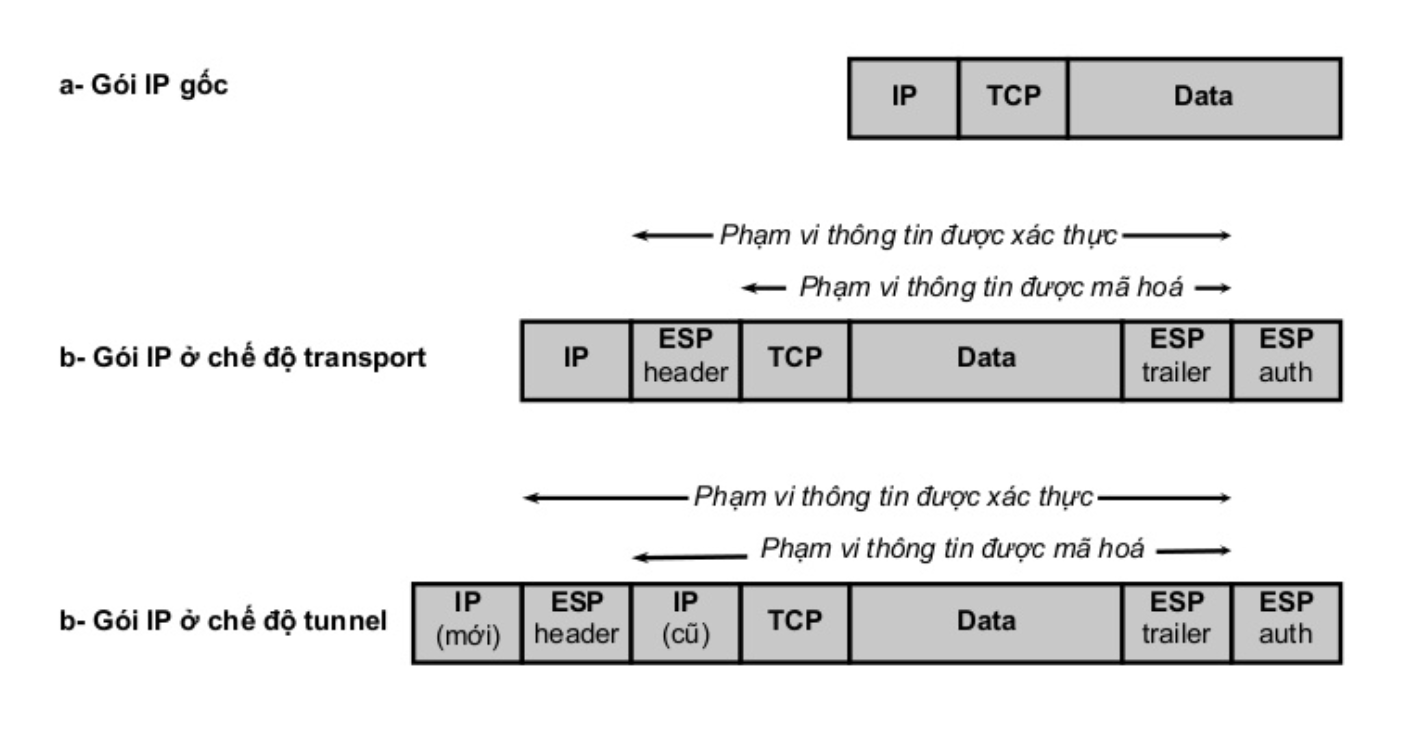
* ***Cấu trúc gói ESP:***



* *Security Parameters Index (SPI - 32 bits*): nhận dạng SA như trong giao thức AH.
* *Sequence Number (số thứ tự - 32 bits)*: số thứ tự, tương tự như trong AH.
* *Payload Data (Dữ liệu)*: đây là phần dữ liệu được bảo vệ bằng mật mã. Trường này có độ dài thay đổi. Trong chế độ vận chuyển, đây là toàn bộ gói dữ liệu của lớp 4 (TCP hoặc UDP). Còn trong chế độ đường hầm, đây là toàn bộ gói IP. ESP chuẩn sử dụng thuật toán mã hóa đối xứng DES, tuy nhiên, có thể dùng các thuật toán mã hóa khác như 3DES (3 khóa), RC5, IDEA, triple IDEA (3 khóa), CAST, Blowfish..
* *Padding (dữ liệu chèn):* một số thuật toán mật mã yêu cầu kích thước dữ liệu gốc phải cố định. Các byte dữ liệu giả được thêm vào để đảm bảo độ dài vùng dữ liệu. Tuy nhiên, theo quy định của ESP, chiều dài trường Pad-length và Next Header phải cố định là 32 bit tính từ bên phải, do vậy, phần padding phải có kích thước sao cho toàn bộ phần thông tin cần mã hóa là bội số của 32 bit.
* *Pad Length (kích thước chèn - 8 bits):* cho biết số byte của vùng dữ liệu chèn.
* *Next Header (tiêu đề kế tiếp - 8 bits):* nhận dạng kiểu dữ liệu chứa trong phần payload data.
* *Authentication Data (mã xác thực - 8 bits):* Chứa thông tin xác thực, có chiều dài thay đổi nhưng phải là bội số của 32 bits. Thông tin xác thực được tính trên toàn gói ESP ngoại trừ phần Authentication Data.
* ***Áp dụng trong transport mode và tunnel mode:***

*Transport mode:* chức năng mã hóa và xác thực thông tin được thực hiện trên phần dữ liệu (payload data) của gói IP (tức toàn bộ đơn vị dữ liệu của lớp trên IP).

*Tunnel mode:* toàn bộ gói IP được mã hóa và xác thực.



* ***Các thuật toán:***

Có các thuật toán sau được sử dụng với ESP:

– DES, 3DES in CBC.

– HMAC with MD5.

– HMAC with SHA-1.

– NULL Authentication algorithm.

– NULL Encryption algorithm.

### 3.2.7. Quản lý khóa với IKE:

IPSec dùng một giao thức thứ ba Internet Exchange Key (IKE) thực hiện tính năng thứ ba là quản lý khóa để thỏa thuận các giao thức bảo mật và các thuật toán mã hóa trước và trong suốt quá trình giao dịch. IKE là giao thức thực hiện quá trình trao đổi khóa và thỏa thuận các thông số bảo mật như: thuật toán mã hóa được áp dụng, khoảng thời gian khóa cần được thay đổi . Sau khi thỏa thuận xong thì sẽ thiết lập “hợp đồng” giữa 2 bên, khi đó IPSec SA (Security Association) được tạo ra. SA là những thông số bảo mật đã được thỏa thuận thành công, các thông số SA này sẽ được lưu trong cơ sở dữ liệu của SA. Ngoài ra IKE còn dùng 2 giao thức khác để chứng thực đầu cuối và tạo khóa: ISAKMP (Internet Security Association and Key Management Protocol) và Oakley.

* ISAKMP: là giao thức thực hiện việc thiết lập, thỏa thuận và quản lý chính sách bảo mật SA.
* Oakley: là giao thức làm nhiệm vụ chứng thực khóa, bản chất là dùng thuật toán Diffie-Hellman để trao đổi khóa bí mật thông qua môi trường chưa bảo mật

## 3.3. Hoạt động của IPSec:

Mục đích chính của IPSec là bảo vệ luồng dữ liệu mong muốn dựa trên các dịch vụ bảo mật có sẵn, hoạt động của IPSec có thể chia thành 5 bước chính như sau:



* A gửi các traffic cần bảo vệ tới B
* Router A và B thỏa thuận các tham số IKE Phase 1:
  + IKE SA ← IKE Phase 1 → IKE SA
* Router A và B thỏa thuận các chính sách IKE Phase 2:
  + IPSec SA ← IKE Phase 2 → IPSec SA
* Thông tin được truyền dẫn qua tunnel IPSec
* Kết thúc tunnel IPSec

***Bước 1:*** Traffic cần được bảo vệ khởi tạo quá trình IPSec. Ở đây, các thiết đầu cuối IPSec sẽ nhận ra đâu là lưu lượng cần được bảo vệ thông qua trường địa chỉ.

***Bước 2:*** IKE Phase 1 – IKE xác thực các bên và một tập các dịch vụ bảo mật được thỏa thuận và công nhận để thiết lập IKE SA. Trong phase này, sẽ thiết lập một kênh truyền thông an toàn để tiến hành thỏa thuận IPSec SA trong Phase 2.

***Bước 3:*** IKE Phase 2 – IKE thỏa thuận các tham số IPSec SA và thiết lập các IPSec SA tương đương ở hai phía. Các tham số bảo mật này được sử dụng để bảo vệ dữ liệu và các gói tin trao đổi giữa các điểm đầu cuối. Kết quả cuối cùng của hai bước trên sẽ tạo ra một kênh thông tin bảo mật giữa hai bên.

***Bước 4:*** Truyền dữ liệu – Dữ liệu được truyền giữa các bên IPSec dựa trên cơ sở các thông số bảo mật và các khoá được lưu trữ trong cơ sở dữ liệu SA.

***Bước 5:*** Kết thúc đường hầm IPSec – Do các IPSec SA hết hạn hoặc bị xóa.

## 3.4. Ưu, nhược điểm của IPSec và ứng dụng:

### 3.4.1. Ưu điểm:

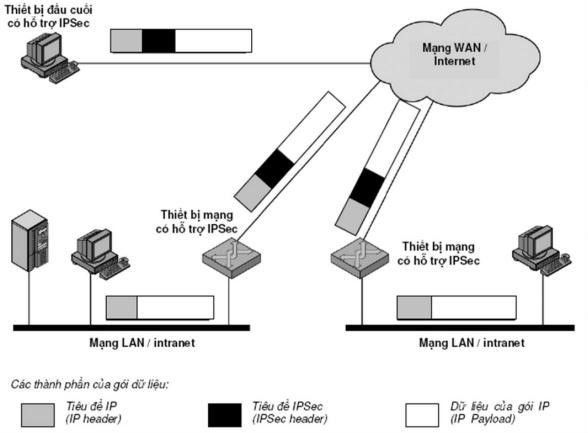
* Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan tới bảo mật
* IPSec được thực hiện bên dưới lớp TCP và UDP ,đồng thời nó hoạt động trong suốt đối với các lớp này.Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
* IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối,điều này giúp che dấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua internet.

### 3.4.2. Nhược điểm:

* Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
* IPSec được thiết kế chỉ để hỗ trợ bảo mật 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 phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

### 3.4.3. Ứng dụng:

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



# 4. Virtual Private Network(VPN):

## 4.1. Tổng quan về VPN:

### 4.1.1. Giới thiệu

Mạng riêng ảo VPN (Virtual Private Network) là công nghệ cung cấp một phương thức giao tiếp an toàn giữa các mạng riêng dựa vào kỹ thuật gọi là tunneling để tạo ra một mạng riêng trên nền Internet. Về bản chất, đây là quá trình đặt toàn bộ gói tin vào trong một lớp header chứa thông tin định tuyến có thể truyền qua mạng trung gian. VPN được hiểu đơn giản như là sự mở rộng của một mạng riêng (private network) thông qua các mạng công cộng. Về căn bản, mỗi VPN là một mạng riêng rẽ sử dụng một mạng chung (thường là internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường leased line, mỗi VPN sử dụng các kết nối ảo được dẫn đường qua Internet từ mạng riêng của các công ty tới các site hay các nhân viên từ xa.

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.

### 4.1.2. Chức năng của VPN

Bản chất của giao thức VPN là một tập hợp các giao thức. Có một số chức năng mà mọi VPN phải giải quyết được:

- **Confidentiality(tính bảo mật):** Đây là dịch vụ quan trọng nhất mà mọi VPN cung cấp. Vì dữ liệu riêng của người dùng được gửi qua mạng công cộng nên tính bảo mật là tất yếu và có thể thực hiện bằng việc mã hoá dữ liệu. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.

- **Authentication(tính xác thực):** xác nhận nguồn gốc của dữ liệu được gửi tới. Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng “giao tiếp” với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định

- **Tunnelling (kỹ thuật truyền dữ liệu qua nhiều mạng có giao thức khác nhau):**Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chứng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunnelling và bên nhận trích xuất để có được thông tin.

- **Integrity( tính toàn vẹn):** xác nhận rằng gói tin VPN không bị thay đổi trong quá trình truyền.

- **Anti-replay(chống gửi lại):** Khả năng phát hiện và từ chối gửi lại gói tin.

**- Quản lý phiên:** Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục “giao tiếp” với nó trong một khoảng thời gian.

### 4.1.3. Ưu điểm

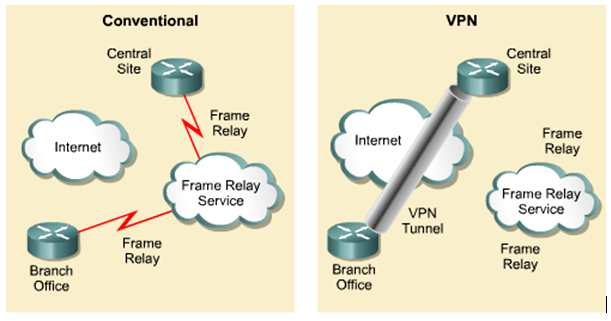
VPN có nhiều ưu điểm hơn so với các mạng leased-line truyền thống. Nó bao gồm:

- 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%.

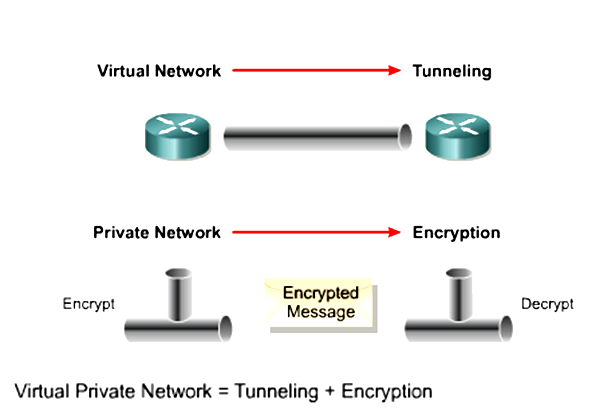
- VPN tạo ra tính mềm dẻo cho khả năng quản lý Internet. Các VPN đã kết thừa phát huy hơn nữa tính mềm dẻo và khả năng mở rộng kiến trúc mạng hơn là các mạng WAN truyền thống. Điều này giúp các doanh nghiệp có thể nhanh chóng và hiệu quả kinh tế cho việc mở rộng hay huỷ bỏ kết nối của các trụ sở ở xa, 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.



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.



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.

### 4.1.4. 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 vậy không 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):

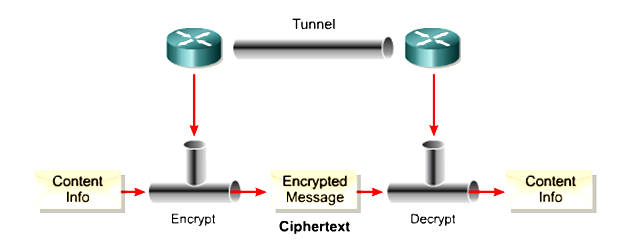
Một giải pháp VPN cần thiết phải cung cấp được tính bảo đảm về chất lượng, hiệu suất sử dụng dịch vụ cũng như dung lượng truyền.

* 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

### 4.1.5. Đường hầm và mã hóa

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



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 hóa 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.

## 4.2. Phân loại VPN:

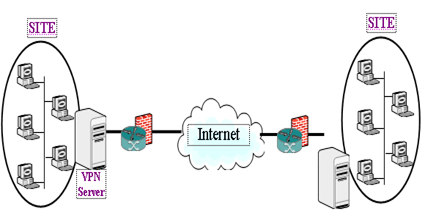
Có 2 loại VPN phổ biến:

**a. Site-to-site VPN:** Bao gồm thiết bị mạng ở mỗi địa chỉ, kết nối bằng một đường hầm VPN. Cuối mỗi đường hầm VPN sẽ thực hiện việc mã hoá gói tin IP gốc, thêm header VPN, header IP mới, và sau đó chuyển gói tin đã mã hoá tới đầu kia của đường hầm.

Đây là cách kết nối nhiều văn phòng trụ sở xa nhau thông qua các thiết bị chuyên dụng và một đường truyền được mã hoá ở quy mô lớn hoạt động trên nền Internet. Site to Site VPN gồm 2 loại:

• *Các VPN nội bộ (Intranet VPN )* Đây là kiểu kết nối site to site VPN. Các chi nhánh có riêng một Server VPN và kết nối lại với nhau thông qua Internet. Và các chi nhánh này sẽ kết nối lại với nhau thành một mạng riêng duy nhất (Intranet VPN) và kết nối LAN to LAN.

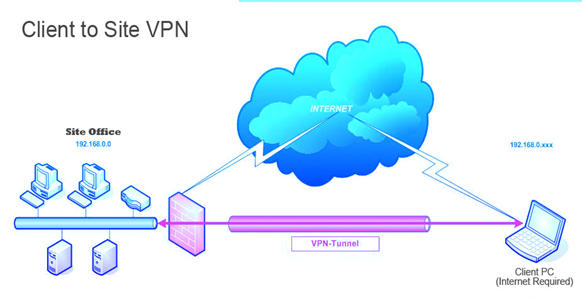
• *Các VPN mở rộng ( Extranet VPN* ) Khi một công ty có quan hệ mật thiết với công ty khác (ví dụ như một đối tác, nhà cung cấp hay khách hàng) họ có thể xây dựng một extranet VPN nhằm kết nối Lan to Lan và cho phép các công ty này cùng làm việc trao đổi trong một môi trường chia sẻ riêng biệt (tất nhiên vẫn trên nền Internet)



Site-to-site VPN

**b. . Client-to-site VPN( remote-access user):**

Có tên gọi khác là VPN người dùng từ xa. Người dùng cài đặt một VPN client trên thiết bị của người đó. Đường hầm VPN được thiết lập giữa thiết bị của người dùng và thiết bị mạng từ xa. Nó còn được gọi là mạng Dial-up riêng ảo (VPDN), là một kết nối người dùng-đến-LAN. Ví dụ như công ty muốn thiết lập một VPN lớn phải cần đến một nhà cung cấp dịch vụ Internet(ISP). ISP này tạo ra một máy chủ truy cập mạng và cung cấp cho những người sử dụng từ xa một phần mềm máy khách cho máy tính của họ. Sau đó, người sử dụng có thể gọi một số miễn phí để liên hệ với máy chủ truy cập mạng và dùng phần mềm VPN máy khách để truy cập vào mạng riêng của công ty. Loại VPN này cho phép các kết nối an toàn, có mật mã.



## 4.3 Các giao thức trong VPN:

### 4.3.1. Giới thiệu về giao thức đường hầm:

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 rất nhiều giao thức đường hầm khác nhau trong công nghệ VPN, và việc sử dụng các giao thức nào liên 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 kỹ 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 những 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.

### 4.3.2. Giao thức đường hầm điểm tới điểm PPTP

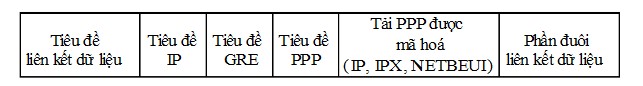
* ***Định nghĩa:***

Giao thức cũ nhất vẫn đang được sử dụng là PPTP(Point-To-Point Tunneling Protocol). PPTP lần đầu tiên được sử dụng vào năm 1995, được đưa ra bởi một nhóm các công ty được gọi là PPTP Forum. Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng. Người dùng ở xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo đường hầm bảo mật tới mạng riêng của họ.

Giao thức PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy cập tạo ra một đường hầm bảo mật thông qua Internet đến site đích. PPTP sử dụng giao thức bọc gói định tuyến chung GRE (Generic Routing Encapsulation) được mô tả lại để đóng gói và tách gói PPP, giao thức này cho phép PPTP mềm dẻo xử lý các giao thức khác không phải IP như: IPX, NETBEUI. Do PPTP dựa trên PPP nên nó cũng sử dụng PAP, CHAP để xác thực.

PPTP có thể sử dụng PPP để mã hoá dữ liệu nhưng Microsoft đã đưa ra phương thức mã hoá khác mạnh hơn đó là mã hoá điểm - điểm MPPE (Microsoft Point- to- Point Encryption) để sử dụng cho PPTP.Một ưu điểm của PPTP là được thiết kế để hoạt động ở lớp 2 (lớp liên kết dữ liệu) trong khi IPSec chạy ở lớp 3 của mô hình OSI. Bằng cách hỗ trợ việc truyền dữ liệu ở lớp thứ 2, PPTP có thể truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói IP trong đường hầm.

* ***Cấu trúc gói PPTP:***



+ Đóng gói khung PPP. Phần tải PPP ban đầu được mật mã và đóng gói với phần tiêu đề PPP để tạo ra khung PPP. Sau đó, khung PPP được đóng gói với phần tiêu đề của phiên bản sửa đổi giao thức GRE. Đối với PPTP, phần tiêu đề của GRE được sửa đổi một số điểm sau:

- Một bit xác nhận được sử dụng để khẳng định sự có mặt của trường xác nhận 32 bit.

- Trường Key được thay thế bằng trường độ dài Payload 16bit và trường nhận dạng cuộc gọi 16 bit. Trường nhận dạng cuộc goi Call ID được thiết lập bởi PPTP client trong quá trình khởi tạo đường hầm PPTP.

- Một trường xác nhận dài 32 bit được thêm vào. GRE là giao thức cung cấp cơ chế chung cho phép đóng gói dữ liệu để gửi qua mạng IP.

+ Đóng gói các gói GRE Tiếp đó, phần tải PPP đã được mã hoá và phần tiêu đề GRE được đóng gói với một tiêu đề IP chứa thông tin địa chỉ nguồn và đích cho PPTP client và PPTP server.

+ Đóng gói lớp liên kết dữ liệu Do đường hầm của PPTP hoạt động ở lớp 2 - Lớp liên kết dữ liệu trong mô hình OSI nên lược đồ dữ liệu IP sẽ được đóng gói với phần tiêu đề (Header) và phần kết thúc (Trailer) của lớp liên kết dữ liệu.

Ví dụ, Nếu IP datagram được gửi qua giao diện Ethernet thì sẽ được đóng gói với phần Header và Trailer Ethernet. Nếu IP datagram được gửi thông qua đường truyền WAN điểm tới điểm thì sẽ được đóng gói với phần Header và Trailer của giao thức PPP.

* ***Ưu nhược điểm:***

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.

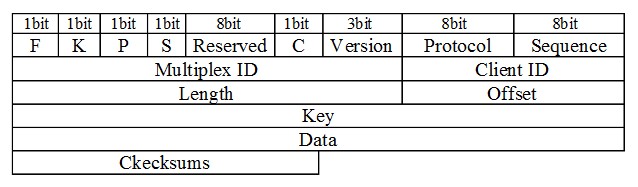
Khó khăn lớn nhất gắn kèm với PPTP là cơ chế yếu kém về bảo mật do nó dùng mã hóa đồng bộ trong khóa được xuất phát từ việc nó sử dụng mã hóa đối xứng là cách tạo ra khóa từ mật khẩu của người dùng. Điều này càng nguy hiểm hơn vì mật khẩu thường gửi dưới dạng phơi bày hoàn toàn trong quá trình xác nhận.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

### 4.3.3. Giao thức chuyển tiếp lớp 2 (L2F)

* ***Định nghĩa:***

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 mạng 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.

* ***Cấu trúc gói***:



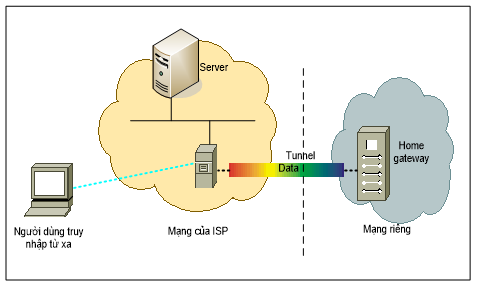
Trong đó:

* F: Trường “Offset” có mặt nếu bit này được thiết lập.
* K: Trường “Key” có mặt nếu bit này được thiết lập.
* P (Priority): Gói này là một gói ưu tiên nếu bit này được thiết lập
* S: Trường “Sequence” có mặt nếu bit này được thiết lập
* Reserved: luôn được đặt là 00000000
* Version: Phiên bản chính của L2F dùng để tạo gói. 3 bit luôn là 111
* Protocol: Xác định giao thức đóng gói L2F
* Sequence: Số chuỗi được đưa ra nếu trong L2F Header bit S=1
* Multiplex ID: nhận dạng một kết nối riêng trong một đường hầm (tunnel)
* Client ID: Giúp tách đường hầm tại những điểm cuối
* Length: chiều dài của gói (tính bằng byte) không bao gồm phần checksum
* Offset: Xác định số byte trước L2F header, tại đó dữ liệu tải tin được bắt đầu. Trường này có khi bit F=1 Key: Trường này được trình bày nếu bit K được thiết lập. Đây là một phần của quá trình nhận xác thực
* Checksum: Kiểm tra tổng của gói. Trường checksum có nếu bit C=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.



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 thỏa thuận bởi đầu cuối người sử dụng và NAS. Home Gateway chấp nhận kết nối hay thỏa 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.

##### ***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.

### 4.3.4 Giao thức đường hầm lớp 2 L2TP(Layer 2 Tunneling Protocol)

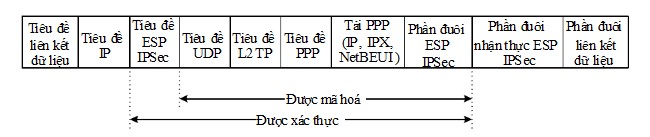
* ***Định nghĩa:***

Giao thức đường hầm lớp 2 L2TP là sự kết hợp giữa hai giao thức PPTP và L2F- chuyển tiếp lớp 2. PPTP do Microsoft đưa ra còn L2F do Cisco khởi xướng. Hai công ty này đã hợp tác cùng kết hợp 2 giao thức lại và đăng ký chuẩn hoá tại IETF. Giống như PPTP, L2TP là giao thức đường hầm, nó sử dụng tiêu đề đóng gói riêng cho việc truyền các gói ở lớp 2. Một điểm khác biệt chính giữa L2F và PPTP là L2F không phụ thuộc vào IP và GRE, cho phép nó có thể làm việc ở môi trường vật lý khác. Bởi vì GRE không sử dụng như giao thức đóng gói, nên L2F định nghĩa riêng cách thức các gói được điều khiển trong môi trường khác. Nhưng nó cũng hỗ trợ TACACS+ và RADIUS cho việc xác thực.

Có hai mức xác thực người dùng: Đầu tiên ở ISP trước khi thiết lập đường hầm, Sau đó là ở cổng nối của mạng riêng sau khi kết nối được thiết lập. L2TP mang đặc tính của PPTP và L2F. Tuy nhiên, L2TP định nghĩa riêng một giao thức đường hầm dựa trên hoạt động của L2F. Nó cho phép L2TP truyền thông qua nhiều môi trường gói khác nhau như X.25, Frame Relay, ATM.

Mặc dù nhiều công cụ chủ yếu của L2TP tập trung cho UDP của mạng IP, nhưng có thể thiết lập một hệ thống L2TP mà không cần phải sử dụng IP làm giao thức đường hầm. Một mạng ATM hay frame Relay có thể áp dụng cho đường hầm L2TP. Do L2TP là giao thức ở lớp 2 nên nó cho phép người dùng sử dụng các giao thức điều khiển một cách mềm dẻo không chỉ là IP mà có thể là IPX hoặc NETBEUI. Cũng giống như PPTP, L2TP cũng có cơ chế xác thực PAP, CHAP hay RADIUS.

* ***Cấu trúc gói tin:***



Cấu trúc gói L2TP

+ Đóng gói L2TP: Phần tải PPP ban đầu được đóng gói với một PPP header và một L2TP header.

+ Đóng gói UDP: Gói L2TP sau đó được đóng gói với một UDP header, các địa chỉ nguồn và đích được đặt bằng 1701.

+ Đóng gói IPSec: Tuỳ thuộc vào chính sách IPSec, gói UDP được mật mã và đóng gói với ESP IPSec header và ESP IPSec Trailer, IPSec Authentication Trailer.

+ Đóng gói IP: Gói IPSec được đóng gói với IP header chứa địa chỉ IP ngưồn và đích của VPN client và VPN server.

+ Đóng gói lớp liên kết dữ liệu: Do đường hầm L2TP hoạt động ở lớp 2 của mô hình OSI- lớp liên kết dữ liệu nên các IP datagram cuối cùng sẽ được đóng gói với phần header và trailer tương ứng với kỹ thuật ở lớp đường truyền dữ liệu của giao diện vật lý đầu ra.

Ví dụ, khi các IP datagram được gửi vào một giao diện Ethernet thì IP datagram này sẽ được đóng gói với Ethernet header và Ethernet Trailer. Khi các IP datagram được gửi trên đường truyền WAN điểm-tới-điểm (chẳng hạn đường dây điện thoại hay ISDN, ) thì IP datagram được đóng gói với PPP header và PPP trailer.

* ***Ưu nhược điểm 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 quá 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 quá 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 giải pháp VPN dựng sẵn, một Routing and Remote Access Server (RRAS) cần có những cấu hình mở rộng.

### 4.3.5. Giao thức GRE (Generic Routing Encapsulation)

* Giao thức mạng 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.

### 4.3.6. Giao thức IPSec:

Như đã trình bày ở trên.

## 4.4. Quy trình tạo và sử dụng VPN

* Chuẩn bị các thành phần chính của VPN

Chúng ta cần một VPN client, một VPN server và một VPN router. Client có thể sử dụng trên các thiết bị như smartphones hoặc laptop, kể cả khi người dùng đang sử dụng mạng wifi công cộng. Để bảo mật và mã hoá toàn bộ network, cần dùng đến VPN router.

* Chuẩn bị các thiết bị

Trong nhiều trường hợp, VPN clients có thể xung đột với các clients khác, hoặc không hoạt động đúng cách.Do đó cần chuẩn bị hệ thống network trước khi cài đặt VPN. Trước tiên, gỡ cài đặt những phần mềm VPN client không cần đến.Trên lý thuyết, VPN clients sẽ làm việc hiệu quả cùng nhau, nhưng các client cạnh tranh khác có thể dẫn tới các hệ luỵ.

Sau đó cần cân nhắc cấu hình mạng. Nếu như muốn cài đặt VPN cho một lượng lớn người dùng truy cập tài nguyên online bằng nhiều cách khác nhau như Wi-Fi, 4G modems và kết nối bằng dây, thì việc cấu hình mạng là hết sức quan trọng.

* Tải và cài đặt VPN clients

Cách đơn giản nhất để chạy VPN là cài đặt từ một nhà cung cấp VPN. Tuy nhiên, sản phẩm của họ có thể không hỗ trợ mọi hệ điều hành. Nếu cài đặt ban đầu thành công, có thể liên hệ với nhà cung cấp VPN về clients cho những platform khác.

* Đăng nhập vào VPN
* Chọn VPN protocols

VPN protocols quyết định dữ liệu được điều hướng như thế nào giữa máy tính của người dùng và VPN server. Một số protocols giúp cải thiện tốc độ, một số khác giúp nâng cao tính bảo mật.

# 5. Ứng dụng của VNP

Mặc dù là công cụ khá đơn giản, nhưng VPN lại có khá nhiều lợi ích:

- **Truy cập Business Network trong khi đi du lịch**: VPN thường được các du khách đi du lịch với mục đích kinh doanh (business traveler) sử dụng để truy cập mạng lưới kinh doanh của họ, bao gồm tất cả các nguồn tài nguyên mạng cục bộ. Các nguồn tài nguyên mạng cục bộ không được tiếp xúc trực tiếp với Internet để tăng cường tính bảo mật.

- **Truy cập Home Network trong khi đi du lịch** : Ngoài ra bạn có thể thiết lập một VPN của riêng mình để truy cập khi đi du lịch. Điều này sẽ cho phép bạn truy cập Windows Remote Desktop thông qua Internet, tức là bạn sẽ được phép truy cập vào máy tính cá nhân của mình thông qua Internet, chia sẻ các tập tin, làm việc trên dữ liệu máy tính ở nhà và thậm chí là chơi game trên máy tính đó.

- **Ẩn hoạt động duyệt web từ mạng cục bộ và ISP** : Nếu đang sử dụng kết nối Wifi công cộng, và bạn duyệt web trên các trang web không phải HTTPS, khi đó các hoạt động của bạn sẽ được hiển thị với mọi người (nếu họ biết cách để xem hoạt động của bạn).

Nếu muốn ẩn hoạt động duyệt web của mình để đảm bảo tính bảo mật, quyền riêng tư, bạn có thể kết nối với VPN. Mạng cục bộ sẽ chỉ nhìn thấy một kết nối VPN an toàn và duy nhất. Tất cả các traffic khác sẽ thông qua kết nối VPN. Và có thể sử dụng để bỏ qua việc giám sát của nhà cung cấp dịch vụ Internet (ISP) của bạn.

- **Truy cập các trang web bị chặn về mặt địa lý** : Dù cho bạn là công dân sinh sống tại Hoa Kỳ, nhưng bạn đang đi du lịch tại một các quốc gia khác, không phải Hoa Kỳ và bạn muốn truy cập Netflix, Pandora hay Hulu thì điều này là không thể. Tuy nhiên nếu kết nối với một VPN đặt tại Hoa Kỳ thì việc truy cập Netflix, Pandora hay Hulu lại là hoàn toàn có thể.

- **Sử dụng VPN để** **bỏ qua kiểm duyệt Internet** .

- **Tải các file** : Nhiều người dùng sử dụng kết nối VPN để tải các file thông qua BitTorrent. Điều này thực sự hữu ích nếu bạn muốn tải toàn bộ Torrent hợp lệ - nếu ISP của bạn đang điều khiển BitTorrent và nó khá chậm, bạn có thể sử dụng BitTorrent trên VPN để được trải nghiệm tốc độ nhanh hơn.

**KẾT LUẬN**

TCP/IP là sự lựa chọn gần như bắt buộc trong các hệ thống hiện nay do giao thức này được sử dụng làm giao thức nền tảng của mạng Internet. Vào thời điểm thiết kế giao thức này, vấn đề bảo mật thông tin chưa thật sự được quan tâm, do đó, các giao thức trong bộ TCP/IP hầu như không được trang bị bất cứ giao thức nào. Cấu trúc gói dữ liệu (IP, TCP,UDP và cả các giao thức ứng dụng) được mô tả công khai, bắt được gói IP trên mạng, ai cũng có thể phân tích gói để đọc phần dữ liệu chứa bên trong, đó là chưa kể hiện nay, các công cụ bắt và phân tích gói được xây dựng với tính năng mạnh và phát hành rộng rãi. Việc bổ sung các cơ chế bảo mật vào mô hình TCP/IP, bắt đầu từ giao thức IP là một nhu cầu cấp bách. IPSec và VPN là các cơ chế ra đời để bù đắp cho những thiếu sót này, và ngày nay nó đã trở nên không thể thiếu trong hệ thống mạng Internet toàn cầu.

Khi không có gì để mất thì chúng ta hay coi thường về bảo mật thông tin trên internet. Nhưng đến lúc bị hacker ghé thăm và đánh cắp dữ liệu, chúng ta mới nhận ra sức mạnh của bảo mật.Với IPSec và công nghệ mạng riêng ảo VPN (Virtual Private Network), chúng ta có thể chống lại các nguy cơ đó. Tuy nhiên đây là các công nghệ tương đối mới, và sẽ phải thay đổi cải thiện từng ngày nên việc nghiên cứu và triển khai các vấn đề này còn gặp nhiều thách thức và đòi hỏi nhiều thời gian và công sức.