BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TPHCM

*****

ĐỒ ÁN CHUYÊN NGÀNH

ĐỀ TÀI

Tìm hiểu và so sánh các kỹ thuật mã hóa trong kết nối VPN

Ngành : **CÔNG NGHỆ THÔNG TIN**

Chuyên ngành : **MẠNG MÁY TÍNH**

Giảng viên hướng dẫn: THẦY NGUYỄN QUANG ANH

Sinh viên thực hiện :

Họ và tên	MSSV	Lớp
Nguyễn Đăng Quang	1311061016	13DTHM02
Lý Tiến Tân	1311061094	13DTHM02

TP.HCM - Tháng 11, năm 2016

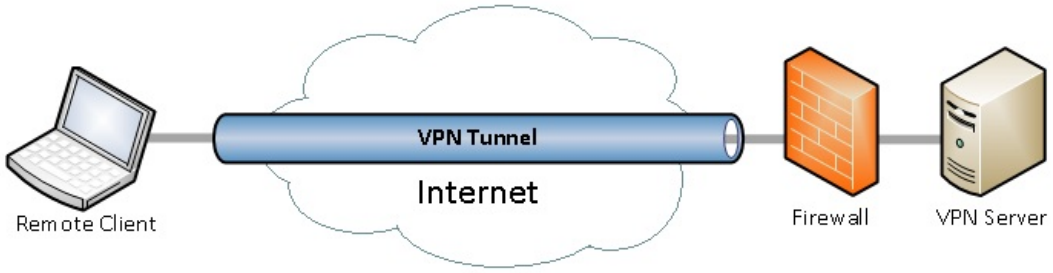
MỤC LỤC

CHƯƠNG I : TỔNG QUAN VỀ VPN

1.1 Tìm hiểu về Mạng riêng ảo (VPN)

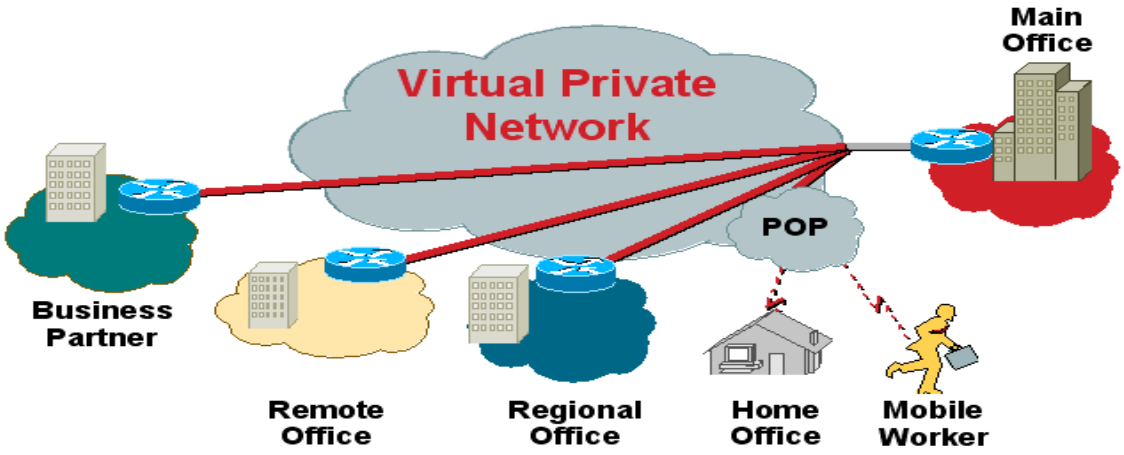
1.1.1 Định nghĩa

Mạng riêng ảo hay còn được biết đến với từ viết tắt VPN, đây không phải là một khái niệm mới trong công nghệ mạng. VPN có thể được định nghĩa như là ***một dịch vụ mạng ảo được triển khai trên cơ sở hạ tầng của hệ thống mạng công cộng với mục đích tiết kiệm chi phí cho các kết nối điểm-điểm***. Một cuộc điện thoại giữa hai cá nhân là ví dụ đơn giản nhất mô tả một kết nối riêng ảo trên mạng điện thoại công cộng. Hai đặc điểm quan trọng của công nghệ VPN là "riêng" và "ảo"tương ứng với hai thuật ngữ tiếng anh (Virtual and Private). VPN có thể xuất hiện tại bất cứ lớp nào trong mô hình OSI, VPN là sự cải tiến cơ sở hạ tầng mạng WAN, làm thay đổi và làm tăng thêm tích chất của mạng cục bộ cho mạng WAN.



Hình 1.1.1.1 : Sơ đồ kết nối từ cơ sở U với cơ sở A của trườn HUTECH thông qua công nghệ VPN

Về căn bản, mỗi VPN(virtual private network) là một mạng riêng rẽ sử dụng một mạng chung (thường là Internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường Leased Line, mỗi VPN sử dụng các kết nối ảo được dẫn qua đường Internet từ mạng riêng của công ty tới các site của các nhân viên từ xa.



Hình 1.1.1.2 Mô hình mạng VPN

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

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

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

1.1.2 Chức năng của VPN

VPN cung cấp ba chức năng chính:

- *Sự tin cậy (Confidentiality):* Người gửi có thể mã hoá các gói dữ liệu trước khi truyền chúng ngang qua mạng. Bằng cách làm như vậy, không một ai có thể truy cập thông tin mà không được cho phép. Và nếu có lấy được thì cũng không đọc được.

- *Tính toàn vẹn dữ liệu (Data Integrity):* người nhận có thể kiểm tra rằng dữ liệu đã được truyền qua mạng Internet mà không có sự thay đổi nào.
- *Xác thực nguồn gốc (Origin Authentication):* Người nhận có thể xác thực nguồn gốc của gói dữ liệu, đảm bảo và công nhận nguồn thông tin.

1.1.3 Lợi ích của VPN

✓ *VPN làm giảm chi phí thường xuyên*

VPN cho phép tiết kiệm chi phí thuê đường truyền và giảm chi phí phát sinh cho nhân viên ở xa nhờ vào việc họ truy cập vào hệ thống 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 dẫn đến giá thành cho việc kết nối Lan - to - Lan giảm đi đáng kể so với việc thuê đường Leased-Line.

✓ *Giảm chi phí quản lý và hỗ trợ*

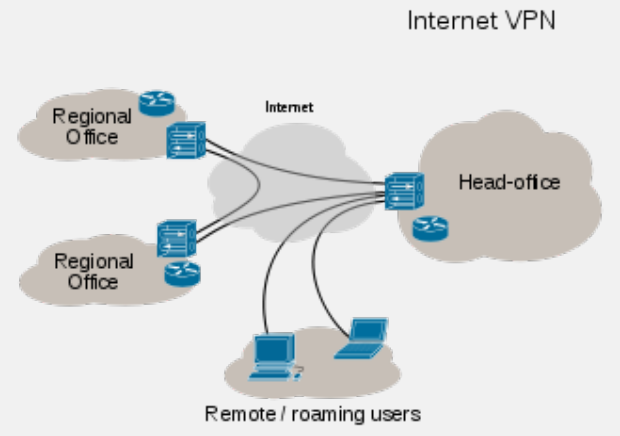
Với việc sử dụng dịch vụ của nhà cung cấp, chúng ta chỉ phải quản lý các kết nối đầu cuối tại các chi nhánh mạng không phải quản lý các thiết bị chuyển mạch trên mạng. Đồng thời tận dụng cơ sở hạ tầng của mạng Internet và đội ngũ kỹ thuật của nhà cung cấp dịch vụ từ đó công ty có thể tập trung vào các đối tượng kinh doanh.

✓ *VPN đảm bảo an toàn thông tin, tính toàn vẹn và xác thực*

Dữ liệu truyền trên mạng được mã hoá bằng các thuật toán, đồng thời được truyền trong các đường hầm (Tunnle) nên thông tin có độ an toàn cao.

✓ *VPN dễ dàng kết nối các chi nhánh thành một mạng cục bộ*

Với xu thế toàn cầu hoá, một công ty có thể có nhiều chi nhành tại nhiều quốc gia khác nhau. Việc tập trung quản lý thông tin tại tất cả các chi nhánh là cần thiết. VPN có thể dễ dàng kết nối hệ thống mạng giữa các chi nhành và văn phòng trung tâm thành một mạng LAN với chi phí thấp.



Hình 1.1.3.1 : VPN giúp kết nối các chi nhánh thành 1 mạng riêng biệt

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

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

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

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

- ***Tính bảo mật (security)***

Tính bảo mật cho khách hàng là một yếu tố quan trọng nhất đối với một giải pháp VPN. Người sử dụng cần được đảm bảo các dữ liệu thông qua mạng VPN đạt được mức độ an toàn giống như trong một hệ thống mạng dùng riêng do họ tự xây dựng và quản lý.

Việc cung cấp tính năng bảo đảm an toàn cần đảm bảo hai mục tiêu sau:

- Cung cấp tính năng an toàn thích hợp bao gồm: cung cấp mật khẩu cho người sử dụng trong mạng và mã hoá dữ liệu khi truyền.

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

- ***Tính khả dụng (Availability):***

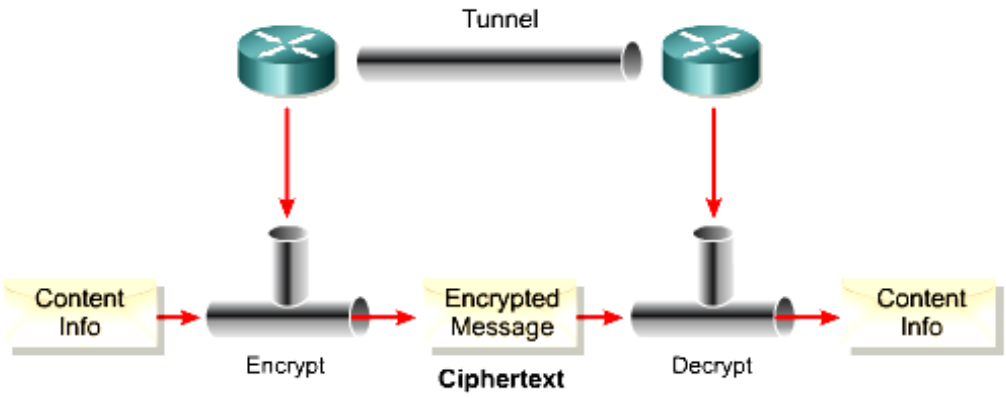
Một giải pháp VPN cần thiết phải cung cấp được tính bảo đảm về chất lượng, hiệu suất sử dụng dịch vụ cũng như dung lượng truyền.

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

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

1.1.5 Đường hầm và mã hóa

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



Hình 1.1.5.1 Đường hầm VPN

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

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

1.2 Mô hình VPN thông dụng

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

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

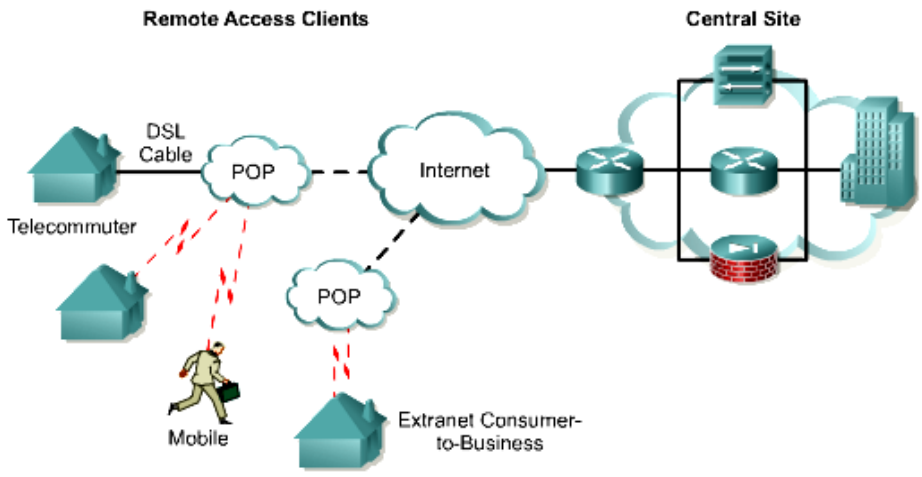
Dựa trên những nhu cầu cơ bản trên, ngày nay VPNs đã phát triển và phân chia ra làm 3 phân loại chính sau :

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

1.2.1 Các VPN truy cập (Remote Access VPNs)

Giống như gợi ý của tên gọi, Remote Access VPNs cho phép truy cập bất cứ lúc nào bằng Remote, mobile, và các thiết bị truyền thông của nhân viên các chi nhánh kết nối đến tài nguyên mạng của tổ chức. Đặc biệt là những người dùng thường xuyên di chuyển hoặc các chi nhánh văn phòng nhỏ mà không có kết nối thường xuyên đến mạng Intranet hợp tác.

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



Hình 1.2.1.1 Mô hình mạng VPN truy cập

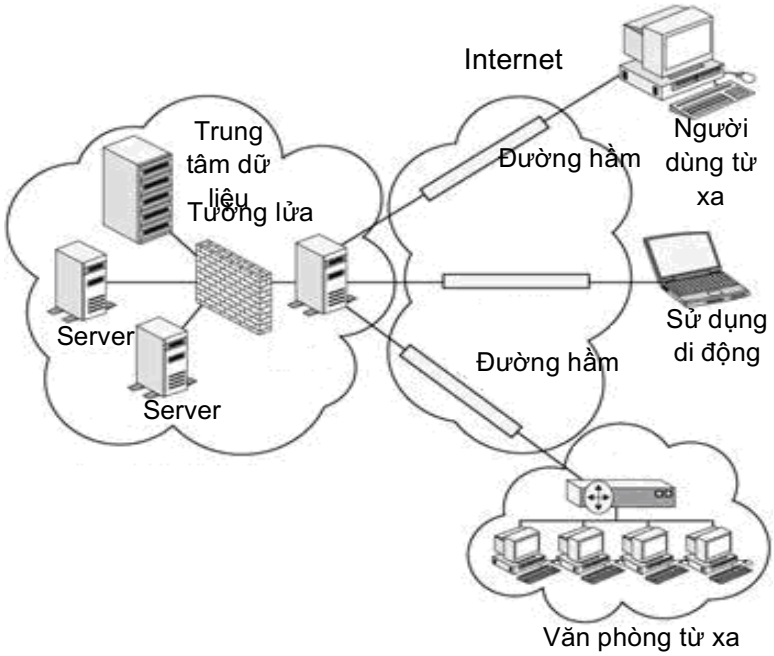
Một số thành phần chính :

Remote Access Server (RAS) : được đặt tại trung tâm có nhiệm vụ xác nhận và chứng nhận các yêu cầu gửi tới.

Quay số kết nối đến trung tâm, điều này sẽ làm giảm chi phí cho một số yêu cầu ở khá xa so với trung tâm.

Hỗ trợ cho những người có nhiệm vụ cấu hình, bảo trì và quản lý RAS và hỗ trợ truy cập từ xa bởi người dùng.

Bằng việc triển khai Remote Access VPNs, những người dùng từ xa hoặc các chi nhánh văn phòng chỉ cần cài đặt một kết nối cục bộ đến nhà cung cấp dịch vụ ISP hoặc ISP's POP và kết nối đến tài nguyên thông qua Internet.



Hình 1.2.1.2: Cài đặt Remote Access VPN

Thuận lợi chính của Remote Access VPNs :

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

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

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

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

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

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

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

✓ Remote Access VPNs cũng không bảo đảm được chất lượng phục vụ.

✓ Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát.

✓ Do độ phức tạp của thuật toán mã hoá, protocol overhead tăng đáng kể, điều này gây khó khăn cho quá trình xác nhận. Thêm vào đó, việc nén dữ liệu IP và PPP-based diễn ra vô cùng chậm chạp và tồi tệ.

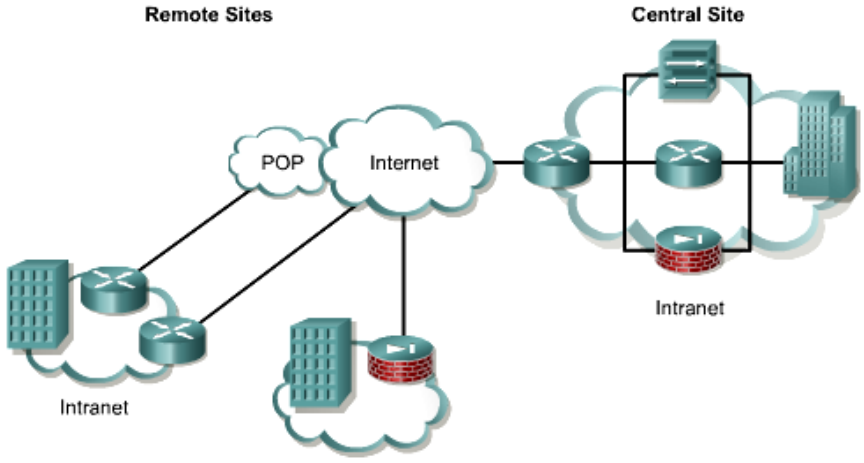
✓ Do phải truyền dữ liệu thông qua Internet, nên khi trao đổi các dữ liệu lớn như các gói dữ liệu truyền thông, phim ảnh, âm thanh sẽ rất chậm.

1.2.2 Các VPN nội bộ (Intranet VPNs):

Intranet VPNs được sử dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Corporate Intranet (backbone router) sử dụng campus router. Theo mô hình này sẽ rất tốn chi phí do phải sử dụng 2 router để thiết lập được mạng, thêm vào đó, việc triển khai, bảo trì và quản lý mạng Intranet Backbone sẽ rất tốn kém còn tùy thuộc vào lượng lưu thông trên mạng đi trên nó và phạm vi địa lý của toàn bộ mạng Intranet.

Để giải quyết vấn đề trên, sự tốn kém của WAN backbone được thay thế bởi các kết nối Internet với chi phí thấp, điều này có thể giảm một lượng chi phí đáng kể của việc triển khai mạng Intranet.

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



Hình 1.2.2.1 Mô hình mạng VPN nội bộ

Những thuận lợi chính của Intranet setup dựa trên VPN:

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

✓ Giảm thiểu đáng kể số lượng hỗ trợ yêu cầu người dùng cá nhân qua toàn cầu, các trạm ở một số remote site khác nhau.

✓ Bởi vì Internet hoạt động như một kết nối trung gian, nó dễ dàng cung cấp những kết nối mới ngang hàng.

✓ Kết nối nhanh hơn và tốt hơn do về bản chất kết nối đến nhà cung cấp dịch vụ, loại bỏ vấn đề về khoảng cách xa và thêm nữa giúp tổ chức giảm thiểu chi phí cho việc thực hiện Intranet.

Những bất lợi chính kết hợp với cách giải quyết :

✓ Bởi vì dữ liệu vẫn còn tunnel trong suốt quá trình chia sẽ trên mạng công cộng-Internet-và những nguy cơ tấn công, như tấn công bằng từ chối dịch vụ (denial-of-service), vẫn còn là một mối đe doạ an toàn thông tin.

✓ Khả năng mất dữ liệu trong lúc di chuyễn thông tin cũng vẫn rất cao.

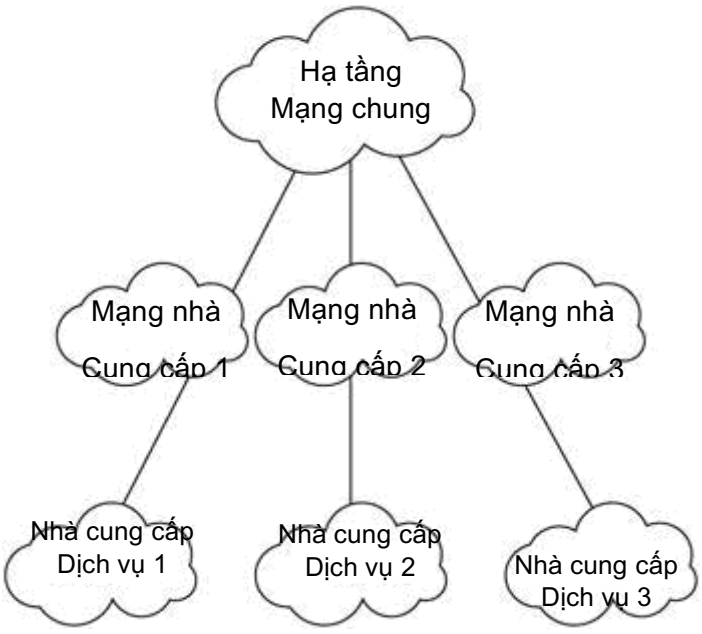
✓ Trong một số trường hợp, nhất là khi dữ liệu là loại high-end, như các tập tin mulltimedia, việc trao đổi dữ liệu sẽ rất chậm chạp do được truyền thông qua Internet.

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

1.2.3 Các VPN mở rộng (Extranet VPNs):

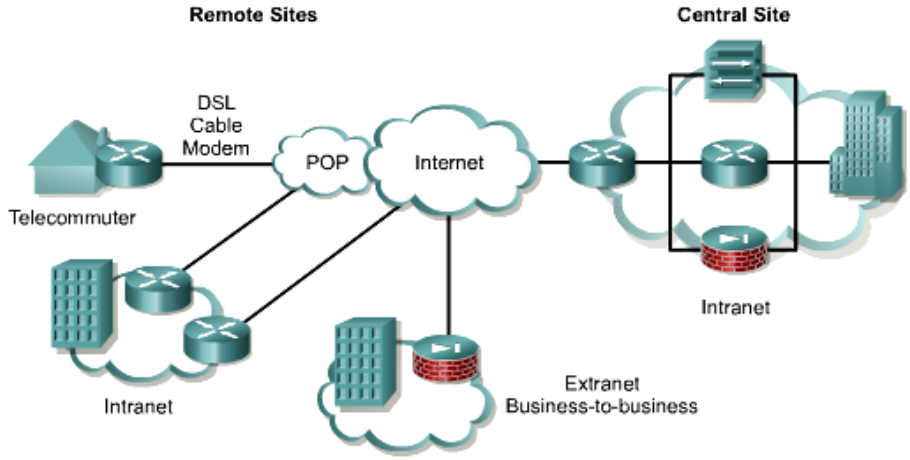
Không giống như Intranet và Remote Access-based, Extranet không hoàn toàn cách li từ bên ngoài (outer-world), Extranet cho phép truy cập những tài nguyên mạng cần thiết của các đối tác kinh doanh, chẳng hạn như khách hàng, nhà cung cấp, đối tác những người giữ vai trò quan trọng trong tổ chức.

Mạng Extranet rất tốn kém do có nhiều đoạn mạng riêng biệt trên Intranet kết hợp lại với nhau để tạo ra một Extranet. Điều này làm cho khó triển khai và quản lý do có nhiều mạng, đồng thời cũng khó khăn cho cá nhân làm công việc bảo trì và quản trị. Thêm nữa là mạng Extranet sẽ khó mở rộng do điều này sẽ làm rối tung toàn bộ mạng Intranet và có thể ảnh hưởng đến các kết nối bên ngoài mạng. Sẽ có những vấn đề bạn gặp phải bất thình lình khi kết nối một Intranet vào một mạng Extranet. Triển khai và thiết kế một mạng Extranet có thể là một cơn ác mộng của các nhà thiết kế và quản trị mạng.



Hình 1.2.3.1: Thiết lập Extranet truyền thống

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



Hình 1.2.3.2 Mô hình mạng VPN mở rộng

Một số thuận lợi của Extranet :

✓ Do hoạt động trên môi trường Internet, chúng ta có thể lựa chọn nhà phân phối khi lựa chọn và đưa ra phương pháp giải quyết tuỳ theo nhu cầu của tổ chức.

✓ Bởi vì một phần Internet-connectivity được bảo trì bởi nhà cung cấp (ISP) nên cũng giảm chi phí bảo trì khi thuê nhân viên bảo trì.

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

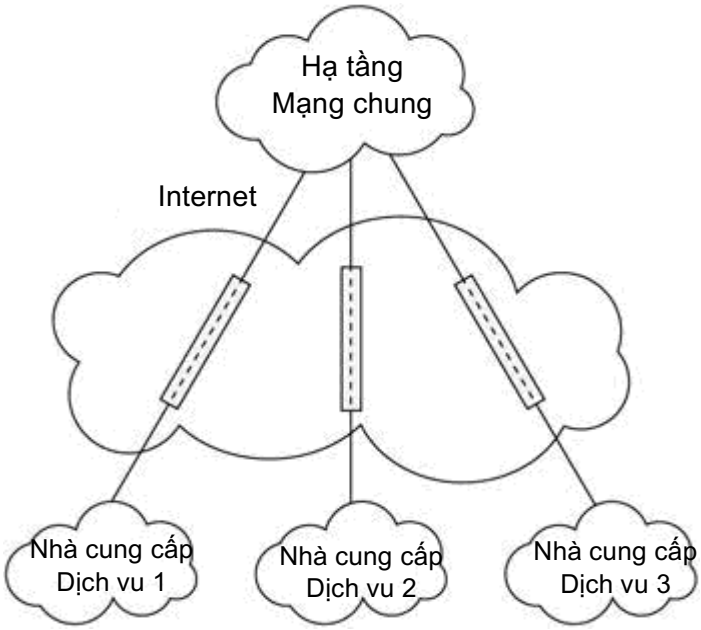
Một số bất lợi của Extranet :

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

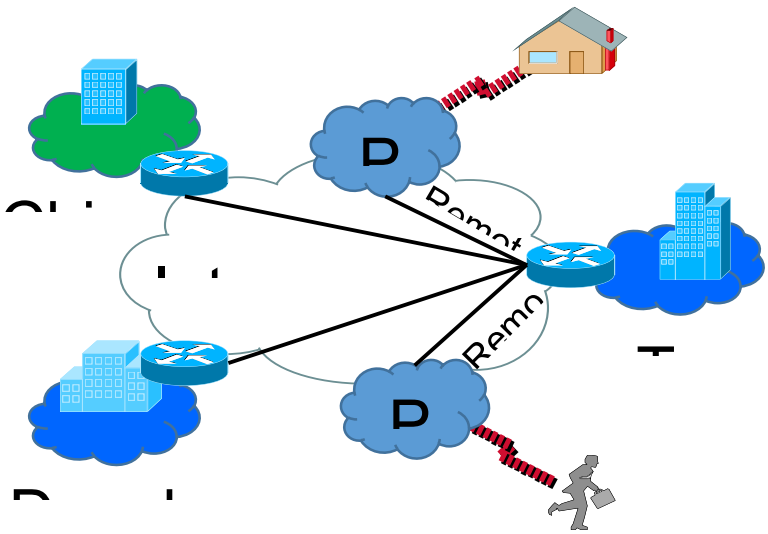
✓ Tăng thêm nguy hiểm sự xâm nhập đối với tổ chức trên Extranet.

✓ Do dựa trên Internet nên khi dữ liệu là các loại high-end data thì việc trao đổi diễn ra chậm chạp.

✓ Do dựa trên Internet, QoS cũng không được bảo đảm thường xuyên.



Hình 1.2.3.3: Thiết lập Extranet VPN



Hình 1.2.3.4 Ba loại mạng riêng ảo

CHƯƠNG II. BẢO MẬT THÔNG TIN

2.1 Tìm hiểu về bảo mật

Trước đây khi công nghệ máy tính chưa phát triển, khi nói đến vấn đề bảo mật thông tin (Information Security), chúng ta thường hay nghĩ đến các biện pháp nhằm đảm bảo cho thông tin được trao đổi hay cất giữ một cách an toàn và bí mật. Chẳng hạn là các biện pháp như :

- Đóng dấu và ký niêm phong một bức thư để biết rằng lá thư có được chuyển nguyên vẹn đến người nhận hay không.
- Dùng mật mã mã hóa thông điệp để chỉ có người gửi và người nhận hiểu được thông điệp. Phương pháp này thường được sử dụng trong chính trị và quân sự.
- Lưu giữ tài liệu mật trong các két sắt có khóa, tại các nơi được bảo vệ nghiêm ngặt, chỉ có những người được cấp quyền mới có thể xem tài liệu.

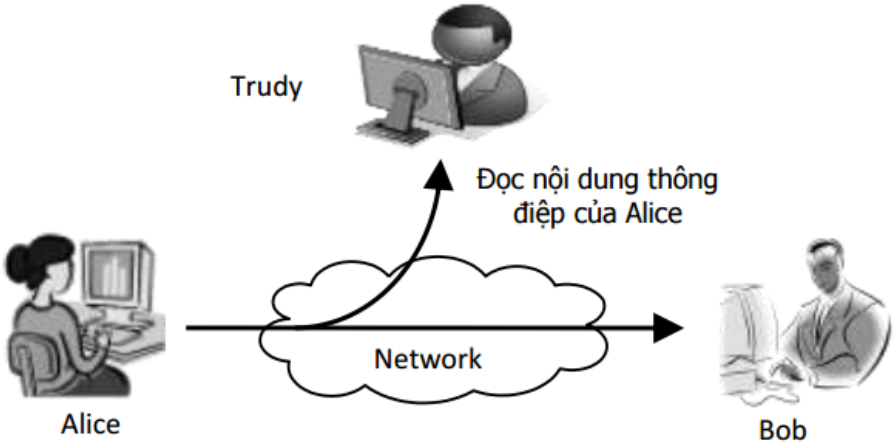
Với sự phát triển mạnh mẽ của công nghệ thông tin, đặt biệt là sự phát triển của mạng Internet, ngày càng có nhiều thông tin được lưu giữ trên máy vi tính và gửi đi trên mạng Internet. Và do đó xuất hiện nhu cầu về an toàn và bảo mật thông tin trên máy tính. Có thể phân loại mô hình an toàn bảo mật thông tin trên máy tính theo hai hướng chính như sau:

- Bảo vệ thông tin trong quá trình truyền thông tin trên mạng (Network Security)
- Bảo vệ hệ thống máy tính, và mạng máy tính, khỏi sự xâm nhập phá hoại từ bên ngoài (System Security)

2.2 Các hình thức tấn công

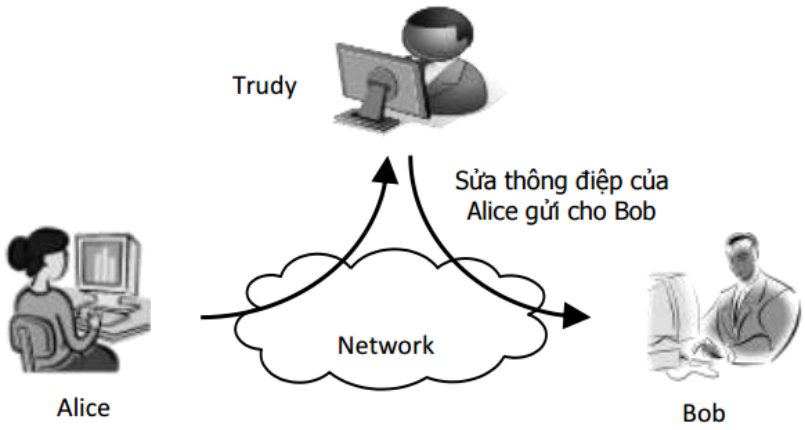
Để xem xét những vấn đề bảo mật liên quan đến truyền thông trên mạng, chúng ta hãy lấy một bối cảnh sau: có ba nhân vật tên là Alice, Bob và Trudy, trong đó Alice và Bob thực hiện trao đổi thông tin với nhau, còn Trudy là kẻ xấu, đặt thiết bị can thiệp vào kênh truyền tin giữa Alice và Bob. Sau đây là các loại hành động tấn công của Trudy mà ảnh hưởng đến quá trình truyền tin giữa Alice và Bob:

1. Xem trộm thông tin (Release of Message Content) Trong trường hợp này Trudy chặn các thông điệp Alice gửi cho Bob, và xem được nội dung của thông điệp.



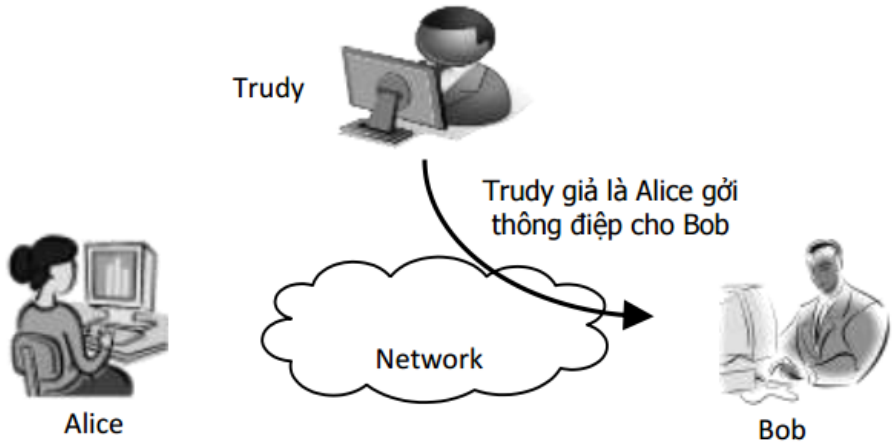
Hình 2.2.1 Xem trộm thông điệp

2. Thay đổi thông điệp (Modification of Message) Trudy chặn các thông điệp Alice gửi cho Bob và ngăn không cho các thông điệp này đến đích. Sau đó Trudy thay đổi nội dung của thông điệp và gửi tiếp cho Bob. Bob nghĩ rằng nhận được thông điệp nguyên bản ban đầu của Alice mà không biết rằng chúng đã bị sửa đổi.



Hình 2.1.2 Sửa sai thông điệp

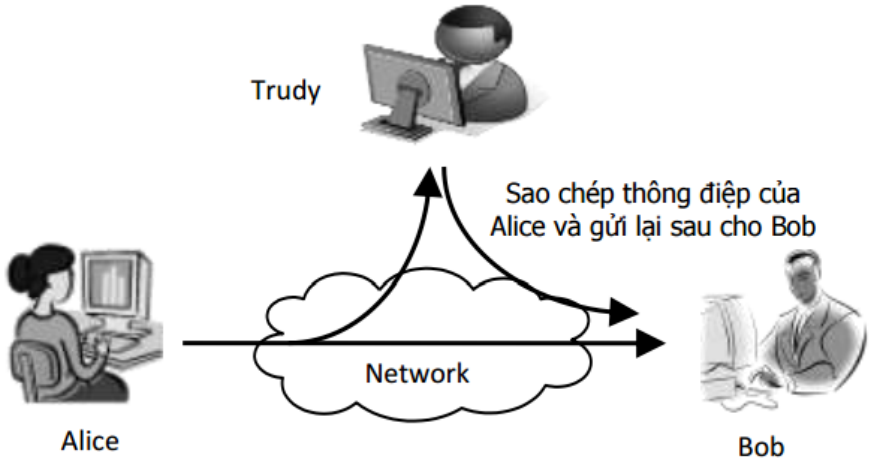
3. Mạo danh (Masquerade) Trong trường hợp này Trudy giả là Alice gửi thông điệp cho Bob. Bob không biết điều này và nghĩ rằng thông điệp là của Alice.



Hình 2.1.3 Mạo danh để gửi đi thông điệp

4. Phát lại thông điệp (Replay) Trudy sao chép lại thông điệp Alice gửi cho Bob. Sau đó một thời gian Trudy gửi bản sao chép này cho Bob. Bob tin rằng thông điệp thứ hai vẫn là từ Alice, nội dung hai thông điệp là giống nhau. Thoạt đầu có thể nghĩ rằng việc phát lại này là vô hại, tuy nhiên trong nhiều trường hợp cũng gây ra tác hại không kém so với việc giả mạo thông điệp. Xét tình huống sau: giả sử Bob là ngân hàng còn Alice là một khách hàng. Alice gửi thông điệp đề nghị Bob chuyển cho Trudy 1000$. Alice có áp dụng các biện pháp như chữ ký điện tử với mục đích không cho Trudy mạo danh cũng như sửa thông điệp. Tuy nhiên nếu Trudy sao chép và phát lại thông điệp thì các

biện pháp bảo vệ này không có ý nghĩa. Bob tin rằng Alice gửi tiếp một thông điệp mới để chuyển thêm cho Trudy 1000$ nữa.



Hình 2.1.4 Phát đi thông điệp giả

2.3 Các hình thức tấn công trong mạng riêng ảo (VPN)

- Tấn công các giao thức VPN chính như PPTP, IPSec…
- Tấn công mật mã
- Tấn công từ chối dịch vụ

❖ Tấn công trên PPTP

PPTP là dễ bị tổn thương trên hai khía cạnh. Chúng bao gồm:

- ✓ Generic Routing Encapsulation (GRE)
- ✓ Mật khẩu trao đổi trong quá trình xác thực

❖ Tấn công trên IPSec

Như chúng ta biết IPSec không phải là thuật toán mã hóa thuần túy cũng không phải một cơ chế xác thực. Trong thực tế, IPSec là một sự kết hợp của cả hai và giúp các thuật toán khác bảo vệ dữ liệu. Tuy nhiên, IPSec là dễ bị các cuộc tấn công:

- ✓ Các cuộc tấn công chống lại thực hiện IPSec
- ✓ Tấn công chống lại quản lý khóa
- ✓ Các cuộc tấn công quản trị và ký tự đại diện

❖ Tấn công mật mã

Mật mã như là một trong các thành phần bảo mật của một VPN. Tùy thuộc vào các kỹ thuật mật mã và các thuật toán khác nhau, các cuộc tấn công giải mã được biết là tồn tại. Những phần sau tìm hiểu về một số cách thức tấn công giải mã nổi tiếng:

- ✓ Chỉ có bản mã (ciphertext-Only)
- ✓ Tấn công biết bản rõ (know plaintext attacks)
- ✓ Tấn công lựa chọn bản rõ
- ✓ Man-in-the-Middle (tấn công trung gian)
- ✓ Tấn công Brute Force (duyệt toàn bộ)
- ✓ Tấn công thời gian (Timing attacks)

❖ Tấn công từ chối dịch vụ

Các cuộc tấn công DDoS đang trở nên khá phổ biến ngày này vì nó không yêu cầu bất kỳ phần mềm đặc biệt hoặc truy cập vào mạng mục tiêu. Chúng được dựa trên khái niệm của sự tắc nghẽn mạng. Bất kỳ kẻ xâm nhập có thể gây ra tắc nghẽn mạng bằng cách gửi các tải các dữ liệu rác vào mạng. Điều này làm cho các máy tính mục tiêu không thể được truy cập trong một khoảng thời gian bởi đường truyền bị quá tải hoặc máy tính mục tiêu không thể phục vụ do quá tải. Tình trạng quá tải thông tin thậm chí có thể dẫn đến việc sụp đổ của máy tính mục tiêu

Một số phương pháp thường được sử dụng để bắt đầu cuộc tấn công DoS như sau:

- ✓ SYN Floods (lụt gói SYN)
- ✓ Broadcast Storm (bão gói tin quảng bá)
- ✓ Smurf DoS
- ✓ Ping of Death

2.3 Một số giải pháp bảo mật

Giải pháp bảo mật thường được chia làm hai phần : hệ thống thiết kế (bên ngoài) và hệ thống phát hiện tấn công (bên trong).

2.3.1 Về hệ thống thiết kế

Thiết kế, quy hoạch một hệ thống mạng lớn không đơn thuần là phát triển thêm các thiết bị hỗ trợ người dùng mà phải dựa trên mô hình chuẩn đã và đang áp dụng cho các hệ thống mạng tiên tiến tại các cơ quan, doanh nghiệp phát triển trên thế giới, đó chính là mô hình mạng Định hướng Kiến trúc Dịch vụ (Service-Oriented Architecture – SOA).

2.3.2 Về hệ thống phát hiện tấn công

- ***Hệ thống tường lửa***

Hệ thống tường lửa là hệ thống kiểm soát truy nhập giữa mạng Internet và mạng nội bộ. Tường lửa có 2 loại: phần cứng và phần mềm. Mỗi loại có các ưu điểm khác nhau. Phần 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 tham chiếu TCP/IP. Phần mềm rất linh hoạt trong những cấu hình ở giao thức tầng ứng dụng trong mô hình TCP/IP.

- ***Hệ thống phát hiện và chống xâm nhập IDS/IPS***

Hiện nay các hình thức tấn công của người có ý đồ xấu ngày càng nhiều và tinh vi. Ví dụ: Trong đơn vị có thể tự cài đặt các công cụ (Ethereal, Cain & abel…) trên máy tính làm việc hoặc máy tính xách tay để tiến hành nghe lén hay quét trực tiếp lên các máy chủ, từ đó có thể lấy các tài khoản email, Web, FTP, SQL server nhằm thay đổi điểm thi, tiền học phí đã nộp, thay đổi lịch công tác…các hình thức tấn công kiểu này, hệ thống tường lửa không thể phát hiện.

Giải pháp hữu hiệu cho thực trạng này là xây dựng hệ thống IDS/IPS (Intrusion Detection System/Intrusion prevention system). IDS/IPS là hệ thống bảo mật vô cùng quan trọng, nó có khả năng phát

hiện ra các cuộc tấn công dựa vào các dấu hiệu thiết lập sẵn hoặc các đoạn mã độc hại, bất thường trên giao thông mạng; đồng thời có thể loại bỏ chúng trước khi có thể gây hại cho hệ thống.

2.4 Công nghệ bảo mật trong VPN

Nền tảng VPN có thể bị tấn công bằng rất nhiều cách. Dưới đây là một số loại tấn công phổ biến vào và hệ thống VPN

- Các mối đe dọa an ninh cho các thành phần VPN
- Các cuộc tấn công các giao thức VPN
- Các cuộc tấn công mật mã
- Các cuộc tấn công từ chối dịch vụ/IPS

Ngày nay, công nghệ phần mềm ngày càng phát triển mạnh mẽ. Đặc biệt là công nghệ mã nguồn mở. Nếu tận dụng được những xu thế này, tức là phần mềm mã nguồn mở vào ứng dụng VPN thì sẽ giảm được khá nhiều chi phí cho việc triển khai. Điều này sẽ đem lại lợi thế rất lớn so với các sản phẩm thương mại.

- ***Giải pháp kernel space***

Các giải pháp không gian nhân là những giải pháp sửa đổi nhân qua các bản vá lỗi. Chúng phức tạp hơn và ít linh hoạt hơn so với các giải pháp không gian người dùng. Hầu hết các giải pháp triển khai trên giao thức bảo mật IPsec. Hoặc là có nguồn gốc được hỗ trợ bởi nhân hoặc thông qua các bản vá nhân. Một số dự án: Một số dự án kernel space: FreeS/WAN, Kame….

- ***Giải pháp user space***

Giải pháp user space hoạt động trong không gian người sử dụng và do đó không có phụ thuộc hoàn toàn vào mô đun nhân hoặc các bản vá. Giải pháp này dễ cài đặt, khá linh hoạt và mềm dẻo trên một số hệ điều hành. User space VPNs sử dụng “giao diện đường hầm ảo", tạo nên các chức năng kết nối mạng ở mức độ thấp, để đạt đươợc đường hầm IP. Ví dụ như Tinc, CIPE, vTun và OpenVPN. Giải pháp user space có thể được nhóm lại dựa trên giao thức bảo mật được sử dụng. - Các giao thức sử dụng chức năng mã hóa tiêu chuẩn được cung cấp bởi OpenSSL (OpenVPN, vTun, Tinc) - Các giao thức, phương thức mã hóa riêng (CIPE, PPTP, L2tpd).

CHƯƠNG III : CÁC THUẬT TOÁN MÃ HÓA TRONG VPN

3.1 Các thuật toán & công nghệ mã hóa

3.1.1 RSA

Bắt tay RSA (cũng có thể là khóa mã hóa hoặc chứng chỉ mã hóa). Để đảm bảo một cách an toàn cho kết nối VPN, SSL thường sử dụng hệ thống mã hóa khóa công khai RSA.

Thuật toán RSA có hai khóa: *khóa công khai* (hay khóa công cộng) và *khóa bí mật* (hay khóa cá nhân). Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa cá nhân (bí mật) mới có thể giải mã được.

Ta có thể mô phỏng trực quan một hệ mật mã khoá công khai như sau: Bob muốn gửi cho Alice một thông tin mật mà Bob muốn duy nhất Alice có thể đọc được. Để làm được điều này, Alice gửi cho Bob một chiếc hộp có khóa đã mở sẵn và giữ lại chìa khóa. Bob nhận chiếc hộp, cho vào đó một tờ giấy viết thư bình thường và khóa lại (như loại khoá thông thường chỉ cần sập chốt lại, sau khi sập chốt khóa ngay cả Bob cũng không thể mở lại được-không đọc lại hay sửa thông tin trong thư được nữa). Sau đó Bob gửi chiếc hộp lại cho Alice. Alice mở hộp với chìa khóa của mình và đọc thông tin trong thư. Trong ví dụ này, chiếc hộp với khóa mở đóng vai trò khóa công khai, chiếc chìa khóa chính là khóa bí mật.

RSA đóng vai trò như một loại mật mã và thuật toán ký số được sử dụng để xác thực các chứng chỉ TLS/SSL, và là cơ sở bảo mật trên internet trong suốt 20 năm qua.

Tuy nhiên nó đã được chứng minh vào năm 2010, 1024-bit RSA (RSA-1024) mã hóa khóa riêng có thể bị bẻ khóa, dẫn đầu là Google trong năm 2013 để nâng cấp tất cả các chứng chỉ SSL đến mức an toàn hơn, tăng chiều dài khóa lên tới ***2048-bit RSA***, đây là cách sao chép trong hầu hết các công nghệ an ninh mạng.

RSA-2048 là loại mã hóa được xem chuẩn an toàn, mặc dù có thể thực hiện mã hóa lên tới 3072-bit hoặc 4096-bit mã hóa để chắc chắn

hơn nữa. Hiện nay, mã hóa RSA-2048 là tiêu chuẩn tối thiểu cho các nhà cung cấp VPN thương mại.

3.1.2 AES

Trong mật mã học, AES (viết tắt của từ tiếng Anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa tiên tiến) là một thuật toán mã hóa khối được chính phủ Hoa kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp thuận làm tiêu chuẩn liên bang bởi Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm.

Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen. Thuật toán được đặt tên là "Rijndael" khi tham gia cuộc thi thiết kế AES.

Mặc dù 2 tên AES và Rijndael vẫn thường được gọi thay thế cho nhau nhưng trên thực tế thì 2 thuật toán không hoàn toàn giống nhau. AES chỉ làm việc với các khối dữ liệu (đầu vào và đầu ra) 128 bít và khóa có độ dài 128, 192 hoặc 256 bít trong khi Rijndael có thể làm việc với dữ liệu và khóa có độ dài bất kỳ là bội số của 32 bít nằm trong khoảng từ 128 tới 256 bít. Các khóa con sử dụng trong các chu trình được tạo ra bởi quá trình tạo khóa con Rijndael. Mỗi khóa con cũng là một cột gồm 4 byte. Hầu hết các phép toán trong thuật toán AES đều thực hiện trong một trường hữu hạn của các byte. Mỗi khối dữ liệu 128 bit đầu vào được chia thành 16 byte (mỗi byte 8 bit),có thể xếp thành 4 cột, mỗi cột 4 phần tử hay là một ma trận 4x4 của các byte,nó được gọi là ma trận trạng thái, hay vắn tắt là trạng thái (tiếng Anh: state, trang thái trong Rijndael có thể có thêm cột). Trong quá trình thực hiện thuật toán các toán tử tác động để biến đổi ma trận trạng thái này.

Quá trình mã hóa

Bao gồm các bước:

1. **Khởi động vòng lặp**
   - AddRoundKey — Mỗi cột của trạng thái đầu tiên lần lượt được kết hợp với một khóa con theo thứ tự từ đầu dãy khóa.
2. **Vòng lặp**

1. SubBytes — đây là phép thế (phi tuyến) trong đó mỗi byte trong trạng thái sẽ được thế bằng một byte khác theo bảng tra (Rijndael S-box).
2. ShiftRows — dịch chuyển, các hàng trong trạng thái được dịch vòng theo số bước khác nhau.
3. MixColumns — quá trình trộn làm việc theo các cột trong khối theo một phép biến đổi tuyến tính.
4. AddRoundKey

3. Vòng lặp cuối

4. SubBytes
5. ShiftRows
6. AddRoundKey

Tại chu trình cuối thì bước MixColumns không thực hiện.

3.1.3 SHA

SHA (Secure Hash Algorithm hay thuật giải băm an toàn) là năm thuật giải được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao.

Năm thuật giải *SHA là SHA-1 (trả lại kết quả dài 160 bit), SHA-224 (trả lại kết quả dài 224 bit), SHA-256 (trả lại kết quả dài 256 bit), SHA-384 (trả lại kết quả dài 384 bit), và SHA-512 (trả lại kết quả dài 512 bit).* Thuật giải SHA là thuật giải băm mật được phát triển bởi cục an ninh quốc gia Mĩ (National Security Agency hay NSA) và được xuất bản thành chuẩn của chính phủ Mĩ bởi viện công nghệ và chuẩn quốc gia Mĩ (National Institute of Standards and Technology hay NIST). Bốn thuật giải sau thường được gọi chung là SHA-2.

Các phiên bản phổ biến nhất của SHA sử dụng trên internet là SHA-1 (160-bit), chiếm hơn 28% cho chứng nhận số hiện có (bao gồm cả những người sử dụng bởi nhiều nhà cung cấp VPN). Và điều không may là SHA1 đã bị hỏng .

Lỗi này đã bị trong một khoảng thời gian gần đây, Microsoft, Google và Mozilla đều đã thông báo rằng trình duyệt tương ứng của họ ***sẽ ngừng nhận SHA-1 chứng chỉ SSL vào năm 2017***. Vào tháng tám năm 2015, NIST công bố rằng SHA-3 là tiêu chuẩn băm thay thế cho SHA-2 làm chuẩn thay thế mới.

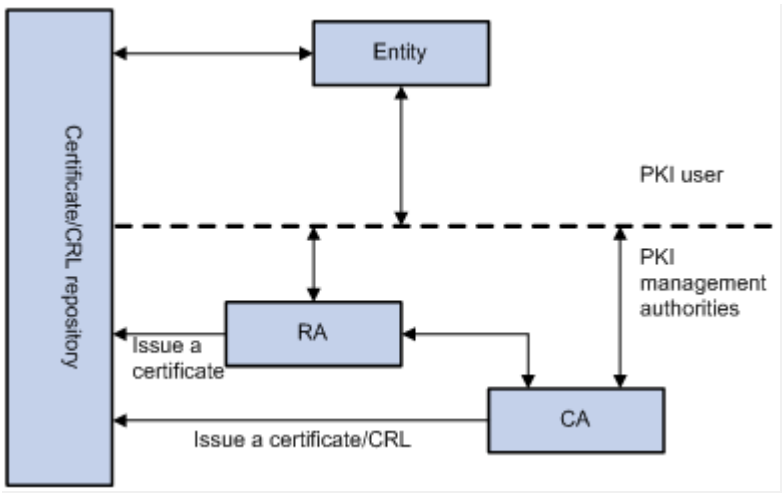
3.1.4 Hạ tầng PKI

Public Key Infrastructure (PKI) là một cơ chế để cho một bên thứ ba (thường là nhà cung cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp public/private. Các quá trình này thường *được thực hiện bởi một phần mềm đặt tại trung tâm* và các phần mềm khác tại các địa điểm của người dùng. Khoá công khai thường được phân phối trong chứng thực khóa công khai – hay PublicKey Infrastructure.

Các thành phần PKI

Một hệ thống PKI gồm 4 thành phần sau :

- ✓ Certification Authorities (CA) : Cấp và thu hồi chứng chỉ
- ✓ Registration Authorities (RA) : Gắn kết giữa kháo công khai và định danh của người giữ chứngchỉ
- ✓ Clients : Người sử dụng chứng chỉ PKI hay theo cách khác được xác định như những thực thểcuối.
- ✓ Repository : Hệ thống (có thể phân tán) lưu trữ chứng chỉ và danh sách các chứng chỉ bị thuhồi.



Hình 3.1.4.1 Các thành phần PKI

Chức năng cơ bản của PKI

Những hệ thống cho phép PKI có những chức năng khác nhau. Nhưng nhìn chung có hai chức năng chình là: chứng thực và kiểm tra.

Chứng thực (Certification) : là chức năng quan trong nhất của hệ thống PKI. Đây là quá trình ràng buộc khóa công khai với định danh của thực thể. CA là thực thể PKI thực hiện chứng năng, chứng thực.

Thẩm tra (validation) : quá trình các định liệu chứng chỉ đã đưa ra có thể được sử dụng đúng mục đích thích hợp hay không được xem như là quá trình kiểm tra tính hiệu lực của chứng chỉ.

3.1.5 Tường lửa

VPN thực chất chỉ là 1 mạng ảo, môi trường thực hiện vẫn là Internet mà Internet thì vô cùng phức tạp và nguy hiểm vì vậy cần phải có sự can thiệp của tường lửa để bảo vệ cho hệ thống đảm bảo tính bảo mật 1 cách an toàn nhất.

Tường lửa (Firewall) *dùng để bảo mật mạng nội bộ chống lại những cuộc tấn công vào lưu lượng trên mạng và những kẻ phá hoại.* Tường lửa có thể phân biệt các lưu lượng dựa trên cơ cở người dùng, trình ứng dụng hoặc nguồn gốc. Tường lửa (firewall) là rào chắn vững chắc giữa mạng riêng và Internet. Có thể thiết lập các tường lửa để hạn chế số lượng cổng mở, loại gói tin và giao thức được chuyển qua.

3.1.6 Giấy chứng nhận điện tử (digital certificate):

Giấy chứng nhận điện tử dùng để chứng nhận khoá công khai (public key) của một cá nhân nào đó. Một giấy chứng nhận điện tử thường bao gồm:

- Tên cơ quan cấp giấy chứng nhận (issuer's name)
- Tên thực thể (entity) được cấp giấy chứng nhận(còn được gọi là đối tượng - subject)
- Khoá công khai (public key) của subject
- Tem thời gian (time-stamps) cho biết thời gian có hiệu lực của giấy chứng nhận

Chỉ có các cơ quan có thẩm quyền Certificate Authority (thường được gọi tắt là CA) mới đươc phép cấp giấy chứng nhận. Giấy chứng nhận được kí bằng khóa riêng (private key) của người cấp. CA cũng được tổ chức theo dạng cây "hierarchy" tương tự như domain-name. Cũng có thể tạo ra một CA mới cho riêng cho mình.

Chúng ta hãy xem giao thức này:

A->B Xin chào!
B->A Chào, Mình là Bob. Đây là giấy chứng nhận của mình!
A->B Hãy đưa bằng chứng đi!
B->A Alice, Mình là Bob đây!
private_Bob{*digest*[“Alice, Mình là Bob đây!”]}

Bằng cách gửi Giấy chứng nhận điện tử (digital certificate) của mình cho Alice (có nghĩa là Alice sẽ biết khoá công khai của Bob) thì bắt buộc thông điệp phải được mã hoá bằng chính private key của Bob thì Alice mới xác nhận được.

Ai đó dùng giấy chứng nhận của Bob để giả mạo Bob sẽ bị Alice phát hiện ngay!

A->M Xin chào
M->A Chào, Mình là Bob. Đây là giấy chứng nhận của mình!
A->M Hãy đưa bằng chứng đi!
M->A ???

Mallet không biết khóa riêng (private key) của Bob nên không thể xây dựng được message để Alice có thể tin mình là Bob.

CHƯƠNG IV : CÁC GIAO THỨC MÃ HÓA TRONG VPN

4.1.PPTP

4.1.1 Giới thiệu về PPTP

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

4.1.2 Nguyên tắc hoạt động của PPTP

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

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

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

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

trong quá trình thiết lập kết nối dựa trên PPTP sử dụng các cơ chế xác thực của kết nối PPP. Một số cơ chế xác thực được sử dụng là:

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

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

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

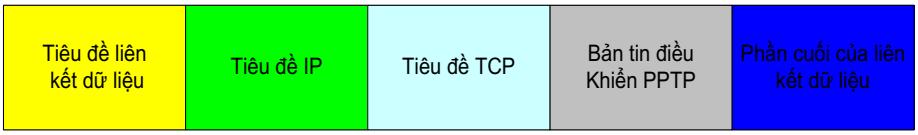
Các gói dữ liệu là dữ liệu thông thường của người dùng. Các gói điều khiển được đua vào theo một chu kì để lấy thông tin và trạng thái kết nối và quản lý báo hiệu giữa ứng máy khách PPTP và máy chủ PPTP. Các gói điều khiển cũng được dùng để gửi các thông tin quản lý thiết bị, thông tin cấu hình giữa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

Kênh điều khiển được yêu cầu cho việc thiết lập một đường hầm giữa các máy khách và máy chủ PPTP. Máy chủ PPTP là một Server có sử dụng giao thức PPTP với một giao diện được nối với Internet và một

giao diện khác nối với Intranet, còn phần mềm client có thể nằm ở máy người dùng từ xa hoặc tại các máy chủ ISP.

4.1.3 Nguyên tắc kết nối của PPTP

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

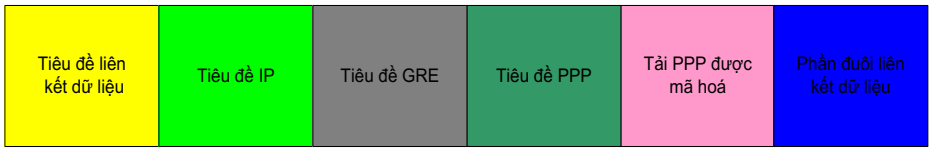


Hình 4.1.3.1 : Gói dữ liệu kết nối điều khiển PPTP

4.1.4 Nguyên lý đóng gói dữ liệu đường hầm PPTP

Đóng gói khung PPP và gói định tuyến chung GRE

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



Hình 4.1.4.1 : Mô hình đóng gói dữ liệu đường hầm PPTP

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

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

Đóng gói IP

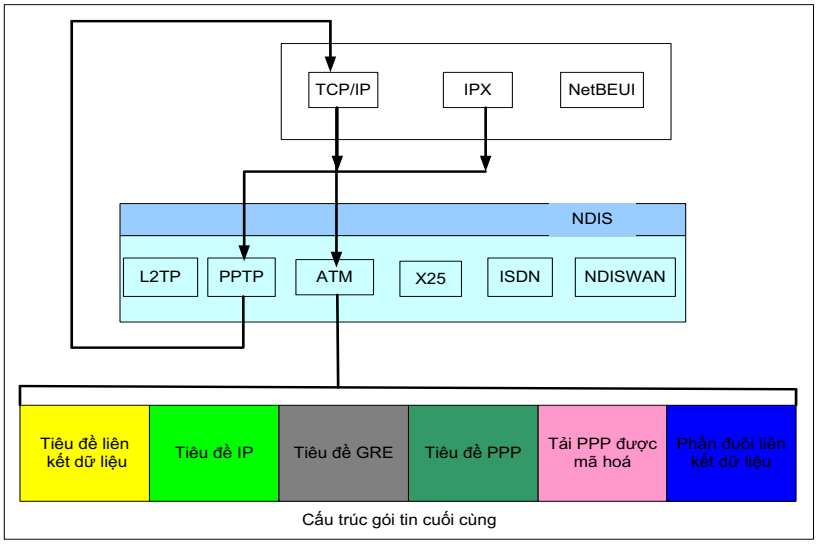
Trong khi truyền tải phần tải PPP và các tiêu đề GRE sau đó được đóng gói với một tiêu đề IP chứa các thông tin địa chỉ nguồn và đích thích hợp cho máy trạm và máy chủ PPTP.

Đóng gói lớp liên kết dữ liệu

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

Sơ đồ đóng gói trong giao thức PPTP

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



Hình 4.1.4.2 : Sơ đồ đóng gói PPTP

- Các gói tin IP, IPX, hoặc khung NetBEUI được đưa tới giao diện ảo đại diện cho kết nối VPN bằng các giao thức tương ứng sử dụng đặc tả giao diện thiết bị mạng NDIS.

- NDIS đưa gói tin dữ liệu tới NDISWAN, nơi thực hiện việc mã hoá và nén dữ liệu, cũng như cung cấp tiêu đề PPP phần tiêu đề PPP này chỉ gồm trường mã số giao thức PPP không có trường Flags và trường chuỗi kiểm tra khung (FCS). Giả định trường địa chỉ và điều khiển được

thoả thuận ở giao thức điều khiển đường truyền (LCP) trong quá trình kết nối PPP.

- NDISWAN gửi dữ liệu tới giao thức PPTP, nơi đóng gói khung PPP với phần tiêu đề GRE. Trong tiêu đề GRE, trường chỉ số cuộc gọi được đặt giá trị thích hợp xác định đường hầm.
- Giao thức PPTP sau đó sẽ gửi gói tin vừa tạo ra tới TCP/IP.
- TCP/IP đóng gói dữ liệu đường hầm PPTP với phần tiêu đề IP sau đó gửi kết quả tới giao diện đại diện cho kết nối quay số tới ISP cục bộ NDIS.
- NDIS gửi gói tin tới NDISWAN, cung cấp các tiêu đề và đuôi PPP.
- NDISWAN gửi khung PPP kết quả tới cổng WAN tương ứng đại diện cho phần cứng quay số.

4.1.5 Nguyên tắc thực hiện

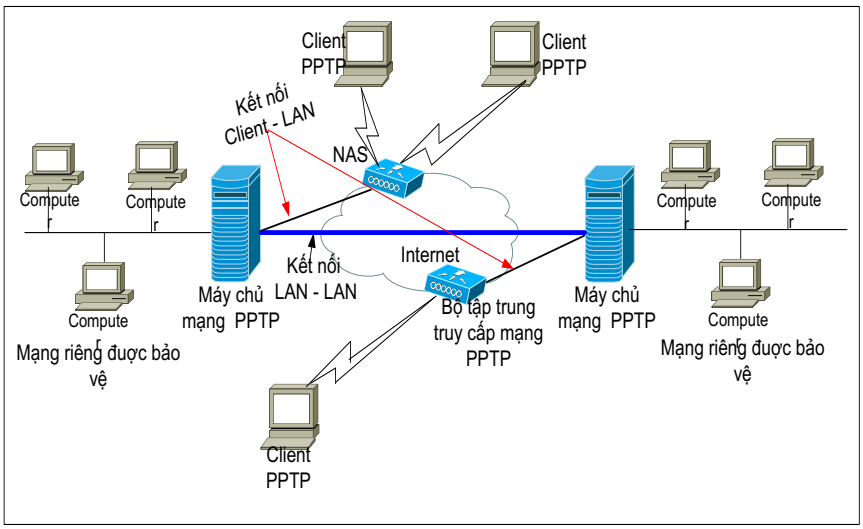
Khi nhận được được dữ liệu đường hầm PPTP, máy trạm và máy chủ PPTP, sẽ thực hiện các bước sau.

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

4.1.6 Triển khai VPN dự trên PPTP

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

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



Hình 4.1.6.1 : Các thành phần hệ thống cung cấp VPN dựa trên PPTP

Máy chủ PPTP

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

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

Một thiết bị khác được đua ra năm 1998 do hãng 3Com có chức năng tương tự như máy chủ PPTP gọi là chuyển mạch đường hầm. Mục đích của chuyển mạch đường hầm là mở rộng đường hầm từ một mạng đến một mạng khác, trải rộng đường hầm từ mạng của ISP đến mạng riêng. Chuyển mạch đường hầm có thể được sử dụng tại bức tường lửa làm tăng khả năng quản lý truy nhập từ xa vào tài nguyên của mạng nội bộ. Nó có thể kiểm tra các gói tin đến và đi, giao thức của các khung PPP hoặc tên của người dùng từ xa.

Phần mềm Client PPTP

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

Máy chủ truy nhập mạng

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

4.1.7 Ưu điểm của PPTP

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

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

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

4.2. L2TP

4.2.1. Giới thiệu về L2TP

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

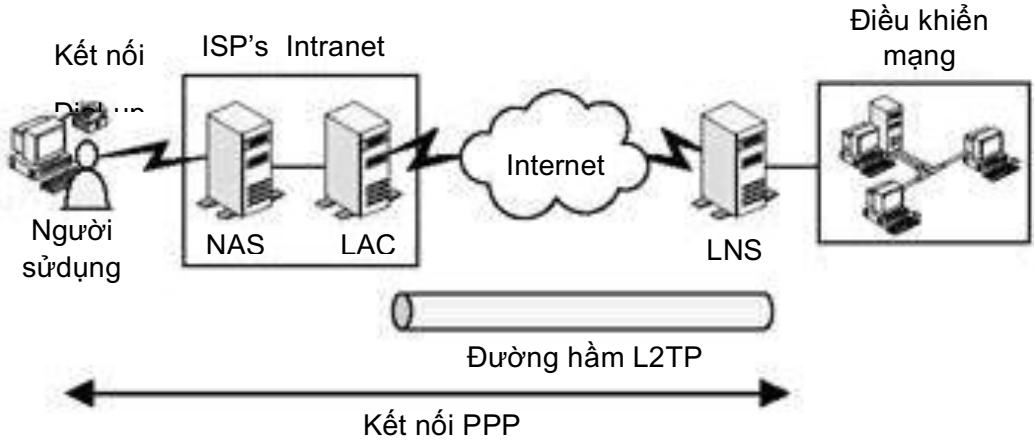
Do đó L2TP là sự trộn lẫn cả hai đặc tính của PPTP và L2F, bao gồm:

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

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

Điểm chính của L2TP tunnels là L2TP thiếp lập đường hầm PPP không giống như PPTP, không kết thúc ở gần vùng của ISP. Thay vào đó, những đường hầm mở rộng đến cổng của mạng máy chủ (hoặc

đích), như hình 3.23, những yêu cầu của đường hầm L2TP có thể khởi tạo bởi người dùng từ xa hoặc bởi cổng của ISP.



Hình 4.2.1.1 : Đường hầm L2TP

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

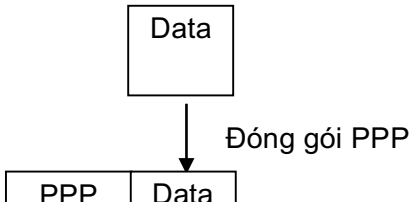
4.2.2 Dữ liệu đường hầm L2TP

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

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

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

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

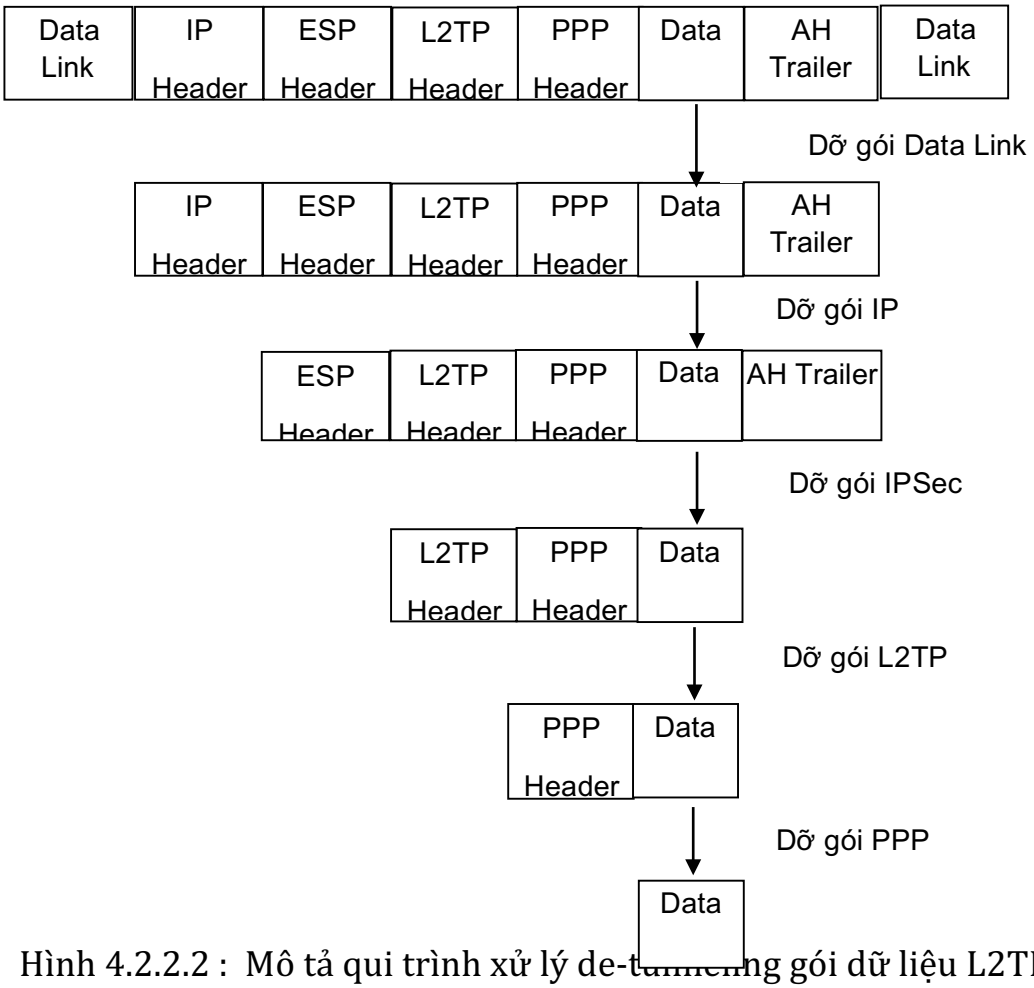


Hình 4.2.2.1 : Quá trình hoàn tất của dữ liệu qua đường hầm

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

Qui trình xử lý de-tunneling những gói dữ liệu L2TP đã tunnel thì ngược lại với qui trình đường hầm. Khi một thành phần L2TP (LNS hoặc người dùng cuối) nhận được L2TP tunneled packet. Kế tiếp, gói dữ liệu được xử lý sâu hơn và phần IP header được gỡ bỏ. Gói dữ liệu sau đó được xác nhận bằng việc sử dụng thông tin mang theo bên trong phần IPSec ESP header và AH trailer. Phần IPSec ESP header cũng được dùng để giải mã và mã hóa thông tin. Kế tiếp, phần UDP header được xử lý rồi loại ra. Cuối cùng, phần PPP header được xử lý và được gỡ bỏ

và phần PPP payload được chuyển hướng đến protocol driver thích hợp cho qui trình xử lý.

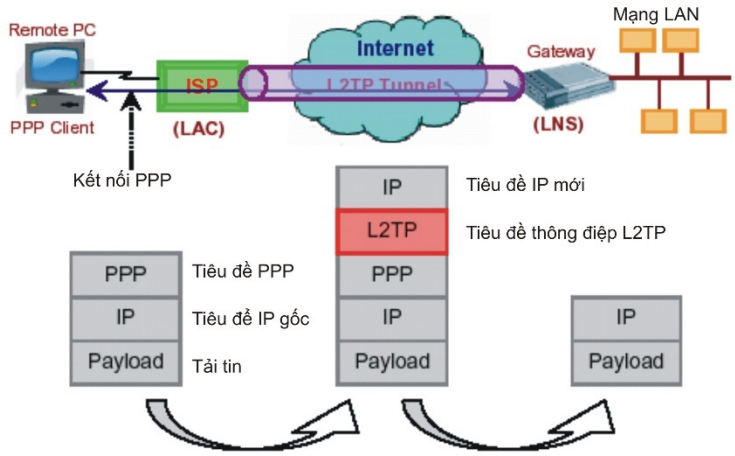


Hình 4.2.2.2 : Mô tả qui trình xử lý de-tunneling gói dữ liệu L2TP

4.2.3 Chế độ đường hầm L2TP

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

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



Hình 4.2.3.1 : Chế độ đường hầm bắt buộc L2TP.

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

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

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

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

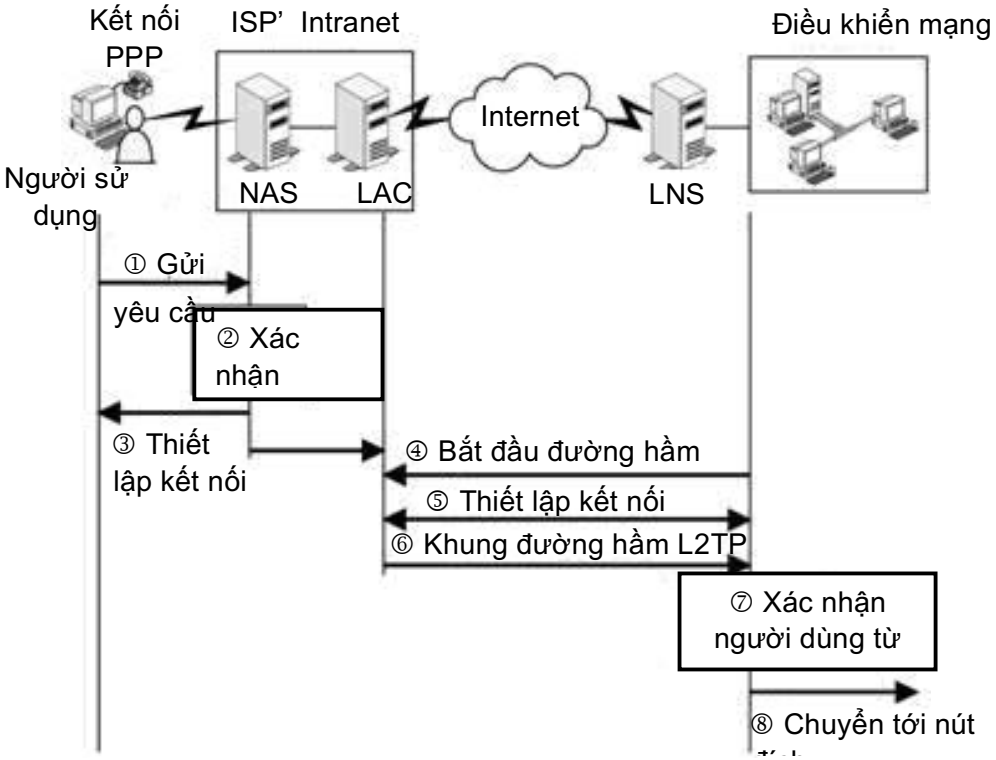
(4) LAC khởi tạo một L2TP tunnel đến một LNS ở mạng chủ cuối.

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

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

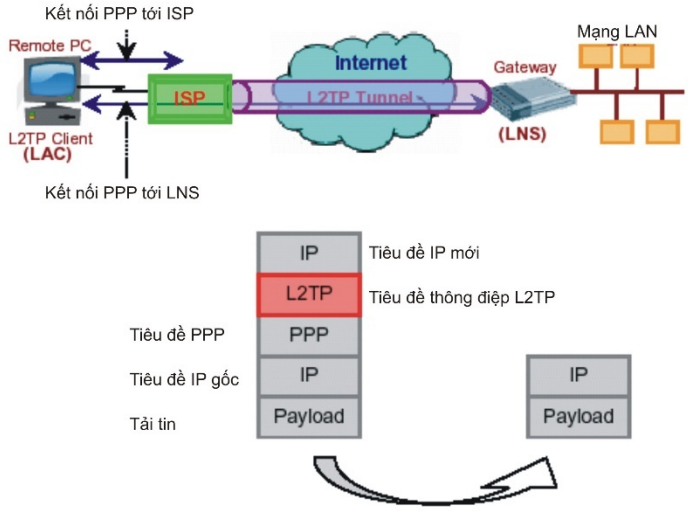
(7) Cuối cùng, LNS xác nhận người dùng và nhận các gói dữ liệu. Nếu người dùng được xác nhận hợp lệ, một địa chỉ IP thích hợp được ánh xạ đến frame

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



Hình 4.2.3.2 Thiết lập một đường hầm bắt buộc

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



Hình 4.2.3.3 Chế độ đường hầm tự nguyện L2TP.

Thuận lợi lớn nhất của đường hầm tự nguyện L2TP là cho phép người dùng từ xa kết nối vào internet và thiết lập nhiều phiên làm việc

VPN đồng thời. Tuy nhiên, để ứng dụng hiệu quả này, người dùng từ xa phải được gán nhiều địa chỉ IP. Một trong những địa chỉ IP được dùng cho kết nối PPP đến ISP và một được dùng để hỗ trợ cho mỗi L2TP tunnel riêng biệt. Nhưng lợi ích này cũng là một bất lợi cho người dùng từ xa và do đó, mạng chủ có thể bị tổn hại bởi các cuộc tấn công.

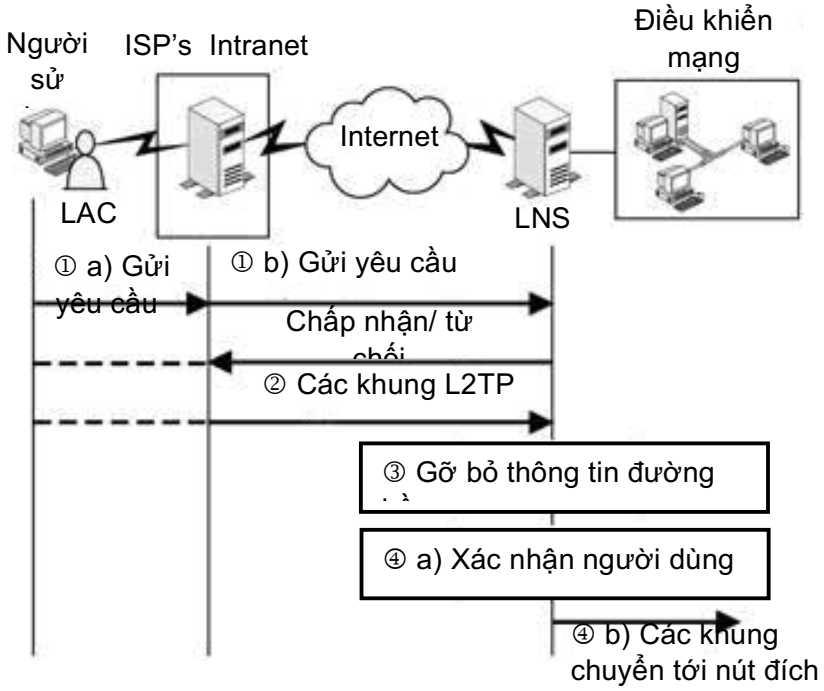
Việc thiết lập một voluntary L2TP tunnel thì đơn giản hơn việc thiết lập một đường hầm bắt buộc bởi vì người dùng từ xa đảm nhiệm việc thiết lập lại kết nối PPP đến điểm ISP cuối. Các bước thiết lập đường hầm tự nguyện L2TP gồm :

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

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

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

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



Hình 4.2.3.4 : Thiết lập L2TP đường hầm tự nguyện.

4.2.4 Những thuận lợi và bất lợi của L2TP

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

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

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

- L2TP cho phép một tổ chức điều khiển việc xác nhận người dùng thay vì ISP phải làm điều này.

- L2TP cung cấp chức năng điều khiển cấp thấp có thể giảm các gói dữ liệu xuống tùy ý nếu đường hầm quá tải. Điều này làm cho qua trình giao dịch bằng L2TP nhanh hơn so với quá trình giao dịch bằng L2F.

- L2TP cho phép người dùng từ xa chưa đăng ký (hoặc riêng tư) địa chỉ IP truy cập vào mạng từ xa thông qua một mạng công cộng.

- L2TP nâng cao tính bảo mật do sử dụng IPSec-based payload encryption trong suốt qua trình tạo hầm, và khả năng triển khai xác nhận IPSec trên từng gói dữ liệu.

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

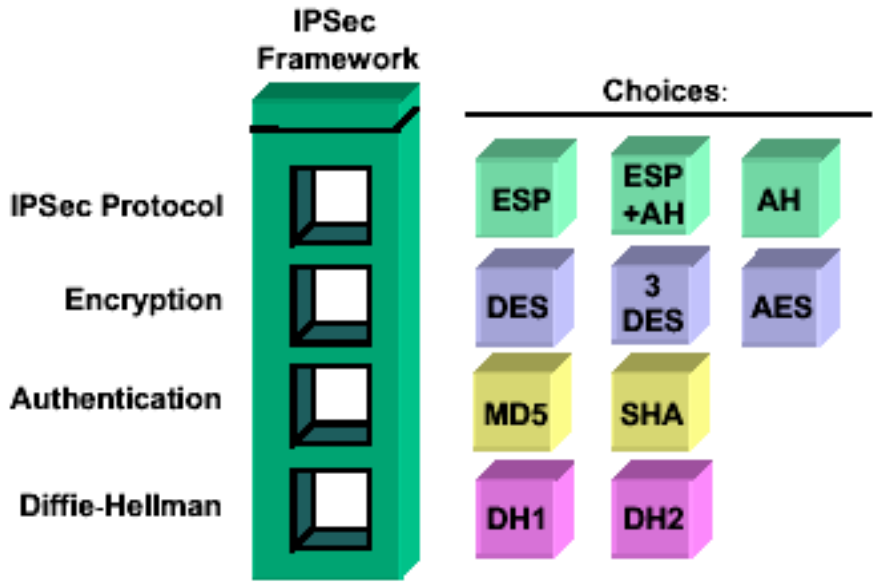
- L2TP chậm hơn so với PPTP hay L2F bởi vì nó dùng IPSec để xác nhận mỗi gói dữ liệu nhận được.

- Mặc dù PPTP được lưu chuyển như một giai pháp VPN dựng sẵn, một Routing and Remote Access Server (RRAS) cần có những cấu hình mở rộng.

4.3 IPSec

4.3.1 Giới thiệu về IPSec

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



Hình 4.3.1.1 Sơ đồ khung IPSec

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

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

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

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

- Từ người gửi yêu cầu.

- Dữ liệu gốc từ người gửi.

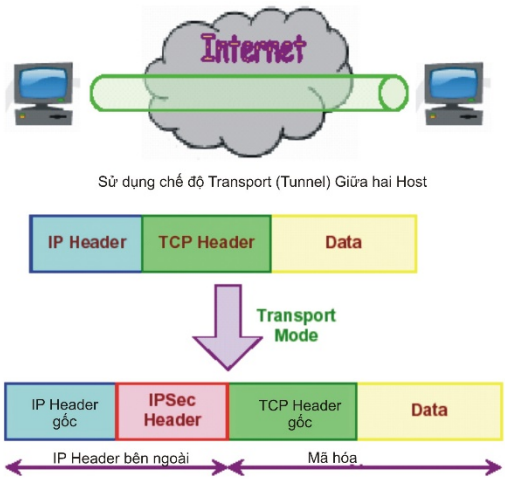
- Không bị kiểm tra bởi bên thứ 3 trong khi gói tin đang được gửi từ nguồn tới đích.

IPSec là một phương pháp để bảo vệ IP datagram. IPSec bảo vệ IP datagram bằng cách định nghĩa một phương pháp định rõ lưu lượng

để bảo vệ, cách lưu lượng đó được bảo vệ và lưu lượng đó được gửi tới ai. IPSec có thể bảo vệ gói tin giữa các host, giữa cổng an ninh mạng, hoặc giữa các host và cổng an ninh. IPSec cũng thực hiện đóng gói dữ liệu và xử lý các thông tin để thiết lập, duy trì, và hủy bỏ đường hầm khi không dùng đến nữa. Các gói tin truyền trong đường hầm có khuôn dạng giống như các gói tin bình thường khác và không làm thay đổi các thiết bị, kiến trúc cũng như các ứng dụng hiện có trên mạng trung gian, qua đó cho phép giảm đáng kể chi phí để triển khai và quản lý.

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

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



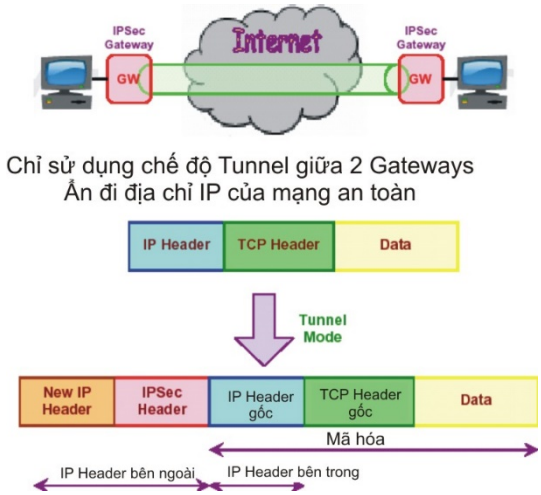
Hình 4.3.1.2 Chế độ Transport

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

Nhược điểm của chế độ này là nó cho phép các thiết bị trong mạng nhìn thấy địa chỉ nguồn và đích của gói tin và có thể thực hiện một số xử lý (như phân tích lưu lượng) dựa trên các thông tin của tiêu

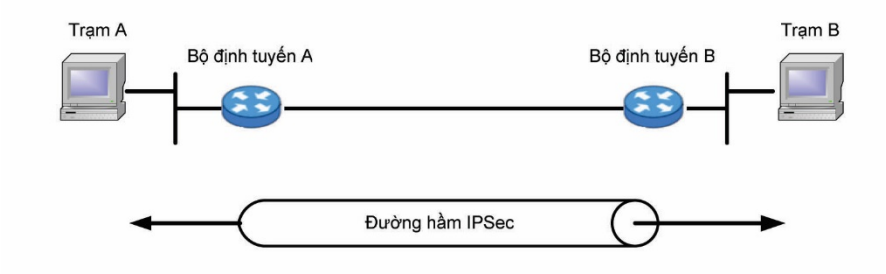
đề IP. Tuy nhiên, nếu dữ liệu được mã hóa bởi ESP thì sẽ không biết được thông tin cụ thể bên trong gói tin IP là gì. Theo IETF thì chế độ truyền tải chỉ có thể được sử dụng khi hai hệ thống đầu cuối IP-VPN có thực hiện IPSec.

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

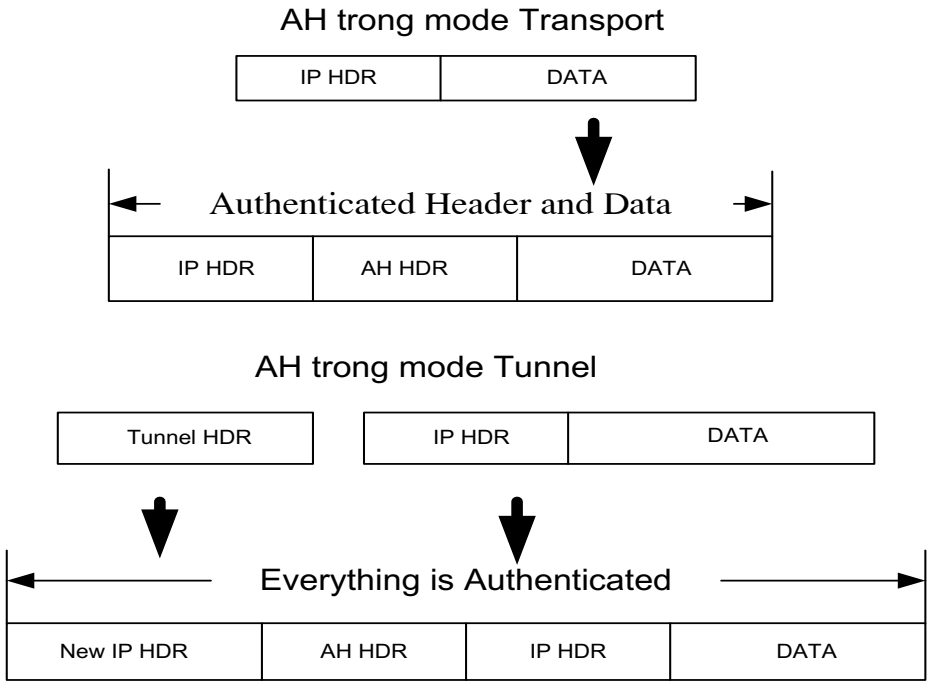


Hình 4.3.1.3 Chế độ tunnel

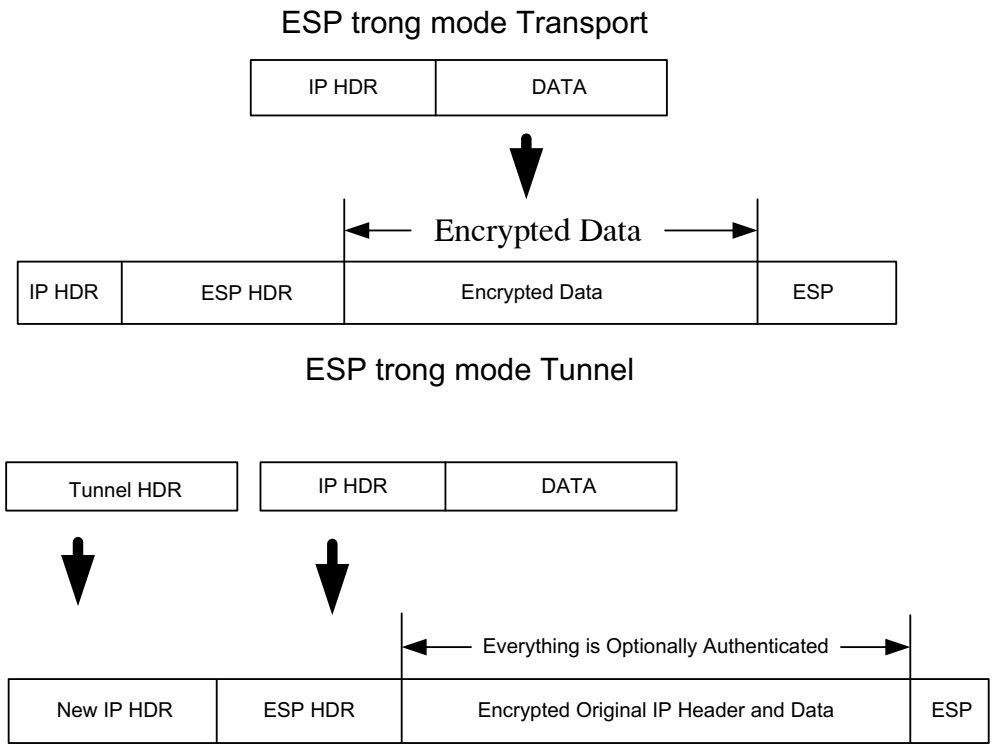
Chế độ này cho phép các thiết bị mạng như bộ định tuyến thực hiện xử lý IPSec thay cho các trạm cuối (host). Trong ví dụ trên hình 3.9, bộ định tuyến A xử lý các gói từ trạm A, gửi chúng vào đường hầm. Bộ định tuyến B xử lý các gói nhận được trong đường hầm, đưa về dạng ban đầu và chuyển chúng tới trạm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



Hình 4.3.1.4: Thiết bị mạng thực hiện trong IPSec trong chế độ đường hầm



Hình 4.3.1.5 AH trong mode Tunnel và transport



Hình 4.3.1.6 ESP trong mode Tunnel và transport

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

- *Tính xác thực*: Mọi người đều biết là dữ liệu nhận được giống với dữ liệu được gửi và người gửi yêu cầu là người gửi hiện tại.
- *Tính toàn vẹn*: Đảm bảo rằng dữ liệu được truyền từ nguồn tới đích mà không bị thay đổi hay có bất kỳ sự xáo trộn nào.
- *Tính bảo mật:* Người gửi có thể mã hóa các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu lấy được cũng không đọc được.
- *Mã hóa*: Một cơ cấu cơ bản được sử dụng để cung cấp tính bảo mật.
- *Phân tích lưu lượng*: Phân tích luồng lưu lượng mạng cho mục đích khấu trừ thông tin hữu ích cho kẻ thù. Ví dụ như thông tin thường xuyên được truyền, định danh của các bên đối thoại, kích cỡ gói tin, định danh luồng sử dụng, vv..

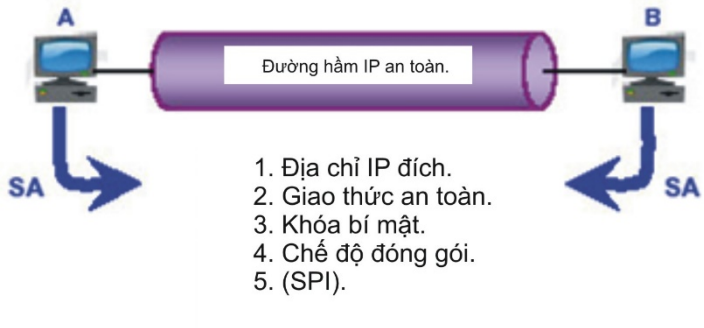
- *SPI*: Viết tắt của chỉ số tham số an toàn (security parameter index), nó là chỉ số không có kết cấu rõ ràng, được sử dụng trong liên kết với địa chỉ đích để định danh liên kết an toàn tham gia.

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

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

4.3.2 Liên kết an toàn

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



Hình 4.3.2.1 Liên kết an toàn

Chính sách

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

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

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

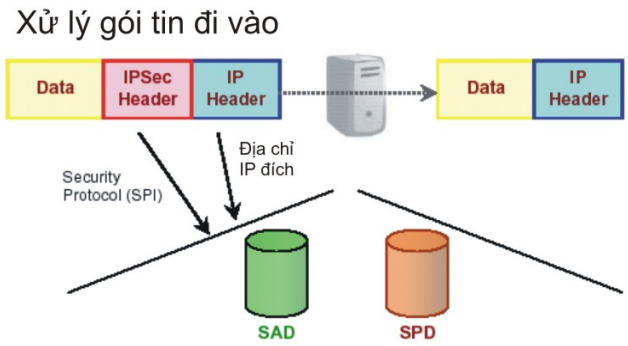
Lưu lượng IP được tạo ra thành chính sách IPSec bởi người chọn lựa. Người lựa chọn IPSec là: địa chỉ IP đích, địa chỉ IP nguồn, tên hệ thống, giao thức tầng trên, cổng nguồn và cổng đích và độ nhạy của dữ liệu.

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

Kiến trúc IPSec định nghĩa sự tương tác của SAD và SPD với chức năng xử lý IPSec như đóng gói và dỡ gói, mã hóa và giải mã, bảo vệ tính

toàn vẹn và xác minh tính toàn vẹn. Nó cũng định nghĩa cách thực thi IPSec khác nhau có thể tồn tại.

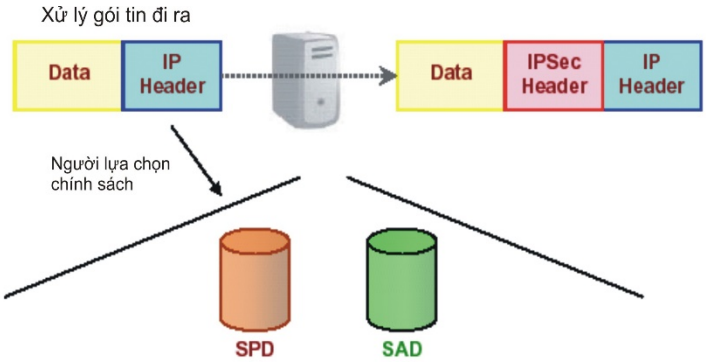
Khi nhận được gói tin vào máy tính thì đầu tiên máy tính đó tham khảo cơ sở dữ liệu về chính sách. Trong trường hợp cần xử lý thì xử lý header, tham khảo cơ sở dữ liệu, tìm đến SA tương ứng.



Hình 4.3.2.2 Chính sách IPSec: xử lý gói tin đầu vào

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

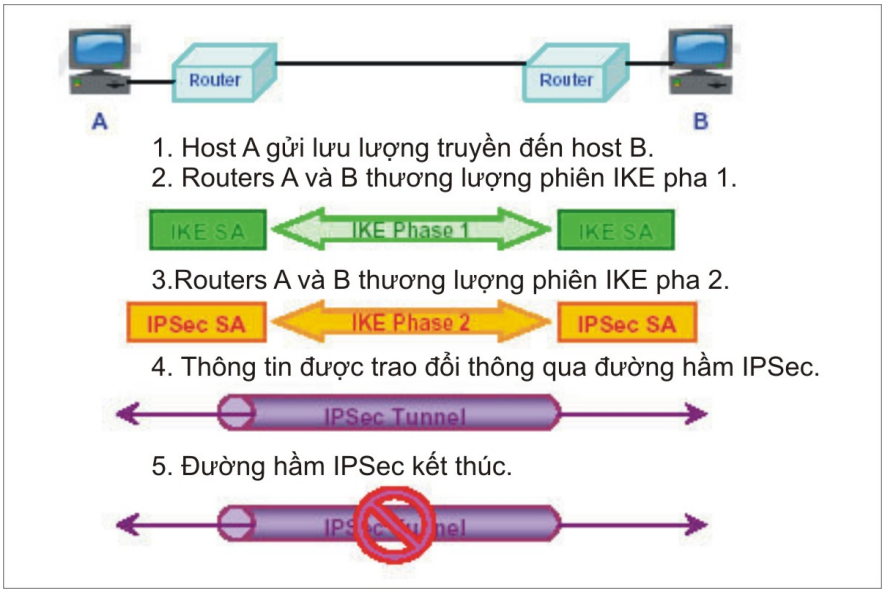
- Cấm hoàn toàn, gói tin không được phép truyền qua.
- Được truyền qua nhưng không có mã hóa và xác thực.
- Có SA tương ứng



Hình 4.3.2.3 Chính sách IPSec: xử lý gói tin đầu ra.

4.3.3. Quá trình hoạt động của IPSec

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



Hình 4.3.3.1 Các bước hoạt động của IPSec

Hình 4.3.3.2 Sơ đồ kết nối hai Router chạy IPSec

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

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

➢ Kết thúc đường hầm "Tunnel": Kết thúc các SA IPSec qua việc xoá hay timing out.

Năm bước được tổng kết của IPSec

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

4.3.4. Những hạn chế của IPSec

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

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu

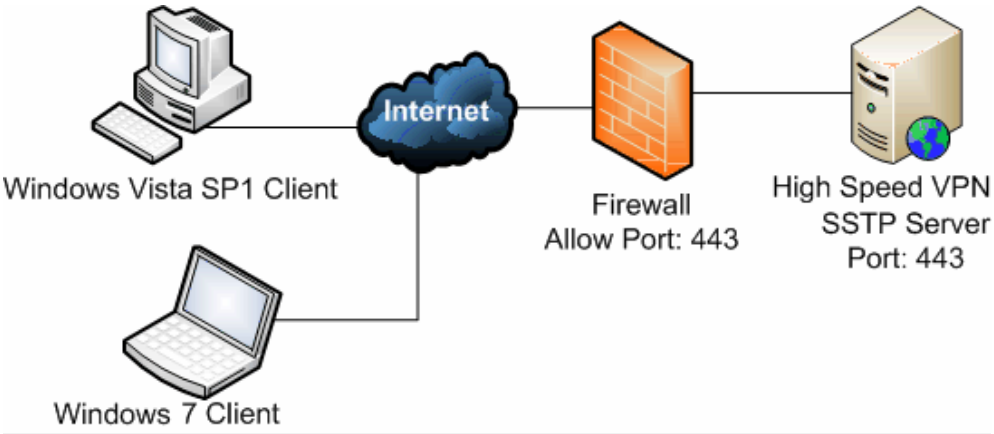
dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.

- IKE vẫn là công nghệ chưa thực sự khẳng định được khả năng của mình. Phương thức chuyển khóa thủ công lại không thích hợp cho mạng có số lượng lớn các đối tượng di động.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phầm mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

4.4 SSTP

4.4.1. Giới thiệu về SSTP

SSTP (Secure Socket Tunneling Protocol) là một dạng của kết nối VPN trong Windows Vista và Windows Server 2008. SSTP sử dụng các kết nối HTTP đã được mã hóa SSL để thiết lập một kết nối VPN đến VPN gateway. SSTP là một giao thức rất an toàn vì các thông tin quan trọng của người dùng không được gửi cho tới khi có một "đường hầm" SSL an toàn được thiết lập với VPN gateway. SSTP cũng được biết đến với tư cách là PPP trên SSL, chính vì thế nó cũng có nghĩa là bạn có thể sử dụng các cơ chế chứng thực PPP và EAP để bảo đảm cho các kết nối SSTP được an toàn hơn.



Hình 4.4.1.1 SSTP-VPN

4.4.2 Lý do sử dụng SSTP trong VPN

Mạng riêng ảo VPN cung cấp một cách kết nối từ xa đến hệ thống mạng thông qua Internet. Windows Server 2003 hỗ trợ các đường hầm VPN dựa vào PPTP và L2TP/IPSec. Nếu người dùng truy cập từ xa ở đằng sau một Firewall, những đường hầm này đòi hỏi các port riêng biệt được mở bên trong các firewall như các port TCP 1723 và giao thức IP GRE để cho phép kết nối PPTP.

Có những tình huống như nhân viên ghé thăm khách hàng, địa điểm đối tác hoặc khách sạn mà hệ thống chỉ cho truy cập web (HTTP, HTTPs), còn tất cả các port khác bị ngăn chặn. Kết quả, những user từ xa này gặp phải vấn đề khi thực hiện kết nối VPN do đó làm tăng cuộc gọi nhờ trợ giúp và giảm năng suất của nhân viên. Secure Socket Tunneling Protocol (SSTP) là một đường hầm VPN mới được giới thiệu trong Windows Server 2008 nhằm giải quyết vấn đề kết nối VPN này.

SSTP thực hiện điều này bằng cách sử dụng HTTPs làm lớp vận chuyển sao cho các kết nối VPN có thể đi qua các firewall, NAT và server web proxy thường được cấu hình. Bởi vì kết nối HTTPs (TCP 443) thường được sử dụng để truy cập các site Internet được bảo vệ như các web site thương mại, do đó HTTPs thường được mở trong các firewall và có thể đi qua các Proxy web, router NAT.

VPN Server chạy trên nền Windows Server 2008 dựa vào SSTP để lắng nghe các kết nối SSTP từ VPN client. SSTP server phải có một Computer Certificate được cài đặt thuộc tính Server Authentication. Computer Certificate này được sử dụng để xác thực server SSTP với client SSTP trong quá trình thiết lập session SSL. Client hiệu lực hóa certificate của server SSTP. Để thực hiện điều này thì Root CA cấp phát certificate cho SSTP server phải được cài đặt trên client SSTP.

Đường hầm VPN dựa vào SSTP có chức năng như một đường hầm peer-L2TP và dựa vào PPTP. Điều này có nghĩa PPTP được bao bọc trên SSTP mà sao đó gửi các lưu lượng cho cho kết nối HTTPs. Như vậy,tất cả các tính năng khác của VPN như kiểm tra sức khỏe dựa vào NAT, tải lưu lượng IPV6 trên VPN,các thuật toán xác thực như username và smartcard... và client VPN dựa vào trình quản lý kết nối vẫn không thay đổi đối với SSTP, PPTP và L2TP. Nó giup cho Admin một đường dẫn di trú tốt để di chuyển từ L2TP/PPTP đến SSTP.

4.4.3 Cách hoạt động của SSTP

SSTP hoạt động trên HTTPs tức là chỉ HTTP sử dụng SSL cho sự bảo mật thông tin và dữ liệu. SSL cũng cung cấp cơ chế xác thực các điểm cuối khi được yêu cầu sử dụng PKI. SSTP sử dụng SSL để xác thực server với client và nó dựa vào PPP chạy trên để xác thực client với server. Nghĩa là Client xác thực server bằng certificate và Server xác thực Client thông qua giao thức hiện có được hỗ trợ bởi PPP.

Khi Client kết nối với Remote Access Server bằng cách sử dụng SSTP làm giao tác tạo lập đường hầm, SSTP thiết lập session HTTPs với server từ xa tại port 443 ở một địa chỉ URL riêng biệt. Các xác lập proxy HTTP được cấu hình thông qua IE sẽ được sử dụng để thiết lập kết nối này.

Với session HTTPs, client đòi hỏi server cung cấp certificate để xác thực. Khi thiết lập quan hệ SSL hoàn tất, các session HTTP được thiết lập trên đó. Sau đó, SSTP được sử dụng để thương lượng các tham số giữa Client và Server. Khi lớp SSTP được thiết lập, việc thương lượng SSTP được bắt đầu nhằm cung cấp cơ chế xác thực client với server và tạo đường hầm cho dữ liệu.

4.5 IKEv2

Internet Key Exchange (phiên bản 2) là một IPSec dựa trên giao thức đường hầm đã được phát triển bởi Microsoft và Cisco, và được đưa vào từ Windows 7 trở lên. Các tiêu chuẩn được hỗ trợ bởi các thiết bị Blackberry, và phát triển một cách độc lập (phần lớn là tương thích) phiên bản của IKE đã được phát triển cho Linux (thông qua thực thi mã nguồn mở khác nhau) và hệ điều hành khác.

Được mệnh danh là VPN Connect của Microsoft, giao thức IKEv2 đặc biệt tốt trong tự động tái thiết lập một kết nối VPN khi người dùng tạm thời mất kết nối internet của họ (chẳng hạn như khi vào hoặc ra khỏi một đường hầm xe lửa).

Người dùng di động nói riêng (mobile user) được hưởng lợi nhiều nhất từ việc sử dụng giao thức IKEv2, trong đó có hỗ trợ cho ***Kết nối nhiều mạng – Multihoming*** (MOBIKE), cũng làm cho nó rất bền để có thể thay đổi mạng lưới. Đây là một tin tuyệt vời cho người sử dụng điện thoại di động, ví dụ, người kết nối điện thoại thông minh của họ với một mạng WiFi trong khi ở nhà, nhưng chuyển sang dữ liệu di động sử dụng khi ra ngoài, hoặc những người thường xuyên chuyển đổi giữa các điểm nóng.

Giao thức IKEv2 thậm chí hữu ích hơn cho người dùng Blackberry, vì nó là một trong số ít các giao thức VPN được hỗ trợ bởi các thiết bị Blackberry.

Giao thức này không phổ biến như IPSec (được hỗ trợ trên nền tảng ít nhiều), nhưng giao thức IKEv2 được coi tốt nhất so với L2TP / IPsec về an ninh, hiệu suất (tốc độ), tính ổn định và khả năng thành lập (và tái lập) một kết nối.

Thức IKEv2 cũng là rất tốt (an toàn và nhanh chóng) giao thức, đặc biệt là cho người dùng di động thậm chí có thể thích nó để OpenVPN nhờ vào khả năng cải tiến của nó để kết nối lại khi kết nối Internet bị gián đoạn. Đối với người dùng Blackberry, thì đây là sự lựa chọn tốt nhất.

4.6 SSL/TLS

4.6.1 Giao thức SSL

Giao thức Secure Socket Layer (SSL), ban đầu định hướng là nhằm mục đích bảo vệ thông tin trao đổi giữa Client và Server trong các mạng máy tính, là giao thức tầng phiên, nó sử dụng các phương pháp mật mã cho việc bảo vệ thông tin. Dữ liệu được truyền được giữ bí mật bằng việc mã hoá, trong khi việc tạo và kiểm tra chữ ký số đảm bảo tính xác thực và toàn vẹn thông tin.

Trong giao thức SSL có sự kết hợp của 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 thoã 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.

Khi thực hiện thủ tục này, các công việc sau được hoàn tất:

- Xác thực Client và Server
- Các điều kiện của thuật toán mật mã và nén sẽ được sử dụng
- Tạo một khoá chủ bí mật
- Tạo một khoá phiên bí mật trên cơ sở khoá chủ

4.6.2 Giao thức TLS

TLS được phát triển nhờ sử dụng SSL, giống như 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 kẻ nghe trộm, giả mạo, chặn bắt gói tin.

Trong các kịch bản mạng riêng ảo, SSL và TLS có thể được thực thi tạo Server VPN cũng như tại Client đầu cuối. Tầng phiên là tầng cao nhất của mô hình OSI có khả năng tạo các kết nối mạng riêng ảo. Lúc tạo các mạng riêng ảo trên tầng phiên, 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 trị.

Như vậy, lúc tạo các mạng riêng ảo trên tầng phiên, ngoài việc bổ sung thêm sự bảo vệ bằng mậtmã (bao gồm cả xác thực), nó cũng có khả năng thực thi các công nghệ Proxy. SSL/TSL là hai giao thức thông dụng nhất hiện nay.

4.7. So sánh các giao thức mã hóa trong VPN

Giao thức	Ưu điểm	Khuyết điểm
PPTP	- Sử dụng trên nền tảng cho client - Rất dễ cài đặt - Nhanh	- Không an toàn (Chứng thực MS CHAPv2 dễ bị tấn công mặc dù được sử dụng nhiều) - Phải được sự thông qua của NSA
L2TP và IPSec	- Khá an toàn - Dễ dàng cài đặt - Có sẵn hầu hết trên các nền tảng - Nhanh hơn OpenVPN	- Hạn chế khi gặp tường lửa
SSTP	- Rất an toàn (phụ thuộc trên số mã hóa) - Hoàn toàn tích hợp vào Windows (Windows Vista SP1,	- Chỉ làm việc đúng trên môi trường Windows - Thuộc quyền sở hữu của Microsoft vì thế không thể kiểm tra được backdoor

	Windows 7, Windows 8) - Hỗ trợ Microsoft - Hầu hết bỏ qua các tường lửa	
IKEv2	- Nhanh hơn PPTP, SSTP và L2TP, vì nó không liên quan đến các chi phí liên quan đến giao thức Point-to-Point (PPP) - Rất ổn định - đặc biệt là khi chuyển đổi mạng hoặc kết nối lại sau khi kết nối Internet bị mất - Rất an toàn - hỗ trợ AES 128, AES 192, AES 256 và thuật toán mã hóa 3DES - Dễ dàng cài đặt ở người dùng cuối) - Giao thức được hỗ trợ trên các thiết bị Blackberry - Sử dụng Perfect Forward Secrecy (PFS)	- Không hỗ trợ trên nhiều nền tảng - Thi hành các giao thức IKEv2 tại máy chủ cuối là phương pháp, điều đó có thể dẫn đến những vấn đề phát sinh

CHƯƠNG V : TÌM HIỂU GIAO THỨC OPENVPN

5.1 Lịch sử của OpenVPN

Năm 2003, James Yonan đi du lịch ở châu Á và phải kết nối với văn phòng qua các ISP của châu Á hoặc Nga.Ông nhận thấy thực tế rằng những kết nối này đi qua những nước không đảm bảo được sự an toàn.Theo những nghiên cứu của James thì có hai mục tiêu chính của một hệ thống VPN đó là tính an toàn và khả dụng.Ipsec có thể chấp nhận được về mặt an toàn nhưng hệ thống xử lý của nó khó thiết lập

và cấu trúc phức tạp của nó làm nó dễ bị tổn thương bởi các cuộc tấn công.Chính vì vậy James đã tiếp cận giải pháp dùng thiết bị card mạng ảo có trong hệ điều hành Linux.Việc chọn thiết bị TUN/TAP cho mạng Lan đã ngay lập tức đưa ra được tính linh hoạt mà các giải pháp VPN khác không thể có được.Trong khi các giải pháp VPN nền tảng SSL/TLS khác cần một trình duyệt để thiết lập kết nối thì openvpn chuẩn bị gần như những thiết bị mạng thật trên gán gần như tất cả các hoạt động của mạng.Rồi Yohan chọn tên OpenVPN với sự tôn trọng dành cho những thư viện và những chương trình của dự án Open SSI, và muốn đưa ra thông điệp: Đây là mã nguồn mở và phần mềm miễn phí.Open VPN sử dụng thiết bị Tun/Tap(hầu như có sẵn trên các bản Linux) và OpenSSL để xác thực,mã hoá và giải mã khi nhận đường truyền giữa hai bên thành chung một mạng.

Hình 5.1.1 James Yonan cha đẻ của OpenVPN

5.2 OpenVPN là gì?

5.2.1 Logo hiện nay của OpenVPN

OpenVPN là một phần mềm mạng riêng ảo mã nguồn mở dành cho việc tạo các đường ống (tunnel) điểm-tới-điểm được mã hóa giữa các máy chủ. Phần mềm này do James Yonan viết và được phổ biến dưới giấy phép GNU GPL.

OpenVPN cho phép các máy đồng đẳng xác thực lẫn nhau bằng một khóa bí mật được chia sẻ từ trước, chứng chỉ mã công khai (public key certificate), hoặc tên người dùng/mật khẩu. Phần mềm này được cung cấp kèm theo các hệ điều hành Solaris, Linux, OpenBSD, FreeBSD, NetBSD, Mac OS X, vàWindows 2000/XP. Nó có nhiều tính năng bảo mật và kiểm soát. Nó không phải một mạng riêng ảo web, và không tương thích với IPsec hay các gói VPN khác. Toàn bộ phần mềm gồm có một file nhị phân cho cả các kết nối client và server, một file cấu hình không bắt buộc, và một hoặc nhiều file khóa tùy theo phương thức xác thực được sử dụng.

Hình 5.2.2 Trang web hiện nay của OpenVPN

5.3 Ưu điểm của OpenVPN

- Bảo vệ người làm việc bên ngoài bằng bức tường lửa nội bộ
- Các kết nối OpenVPN có thể đi qua được hầu hết mọi tường lửa và proxy: Khi truy cập các trang web HTTPS, thì đường hầm

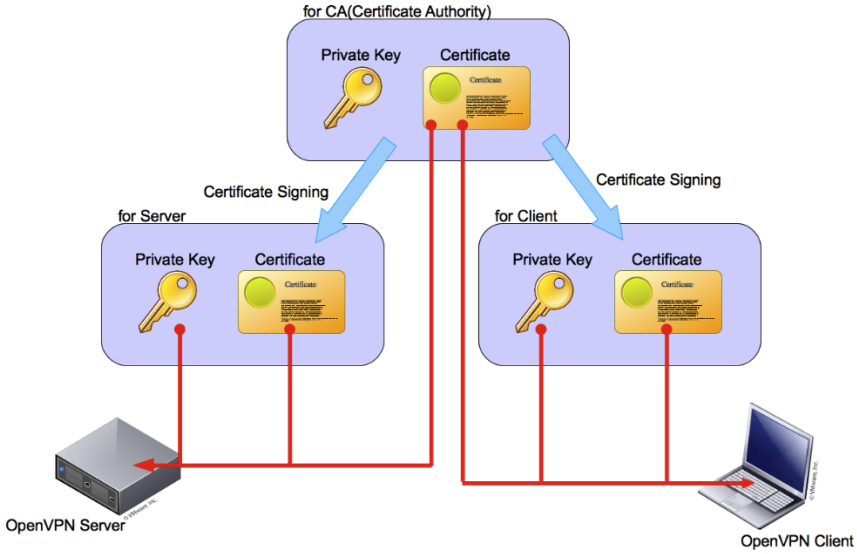
OpenVPN làm việc.Việc thiết lập đường hầm OpenVPN bị cấm là rất hiếm.OpenVPN có hỗ trợ uỷ quyền đầy đủ bao gồm xác thực.

- Hộ trợ UDP và TCP: OpenVPN có thể được cấu hình để chạy dịch vụ TCP hoặc UDP trên máy chủ hoặc client.Là một máy chủ, OpenVPN chỉ đơn giản là chờ đợi cho đến khi một khách hàng yêu cầu một kết nối, kết nối này được thiết lập theo cấu hình của khách hàng.
- Chỉ cần một cổng trong tường lửa được mở là cho phép nhiều kết nối vào: Kể từ phần mềm OpenVPN 2.0, máy chủ đặc biệt này cho phép nhiều kết nối vào trên cùng một cổng TCP hoặc UDP, đồng thời vẫn sử dụng các cấu hình khác nhau cho mỗi một kết nối.
- Không có vấn đề gì với NAT: Cả máy chủ và máy khách OpenVPN có thể nằm trong cùng một mạng và sử dụng các địa chỉ IP riêng. Mỗi tường lửa có thể được dùng để gửi lưu lượng tới điểm cuối đường hầm.
- Giao diện ảo chấp nhận các quy tắc về tường lửa: Tất cả các quy tắc, các cơ chế chuyển tiếp, và NAT có thể dùng chung đường hầm OpenVPN. Nhưng giao thức cũng có thể, có thể tạo đường hầm VPN khác như IPsec bên trong đường hầm OpenVPN.
- Độ linh hoạt cao với khả năng mở rộng kịch bản: OpenVPN cung cấp nhiều điểm trong quá trình thiết lập kết nối để bắt đầu các kịch bản riêng. Những kịch bản có thể được sử dụng cho một loạt các mục đích từ xác thực,chuyển đổi dự phòng và nhiều hơn nữa.

- Hỗ trợ khả năng hoạt động cao, trong suốt cho IP động: Hai đầu đường hầm có thể sử dụng IP động và ít bị thay đổi. Nếu bị đổi IP, cá phiên làm việc của Windows Terminal Server và Secure Shell (SSH) có thể chỉ bị ngưng trong vài giây và sẽ tiếp tục hoạt động bình đường.
- Cài đặt đơn giản trên bất kỳ hệ thống nào: Đơn giản hơn nhiều so với IPsec.
- Thiết kế kiểu Modun

5.4 Các mô hình bảo mật OpenVPN

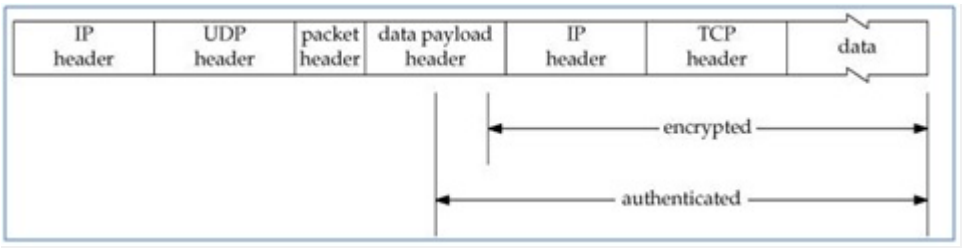
OpenVPN sử dụng giao thức SSL để xác thực mỗi điểm cuối VPN đến các máy chủ, trao đổi khóa và thông tin điều khiển khác. Trong phương pháp này, OpenVPN Thiết lập một phiên SSL/TLS với máy của nó để kiểm soát các kênh. Trong giai đoạn xác thực, các máy trao đổi giấy chứng nhận được ký bởi một CA tin cậy lẫn nhau. Điều này đảm bảo cả hai bên rằng họ đang nói chuyện với chính xác bạn bè của họ, ngăn chặn các cuộc tấn công man-in-the-middle.



Hình 5.4.1 Mô hình lưu khóa sử dụng Openvpn

5.5 Các kênh dữ liệu OpenVPN

OpenVPN có thể tùy chọn sử dụng kết nối TCP thay vì UDP datagrams. Mặc dù đây là thuận tiện trong một số trường hợp, nó có vấn đề về xung đột và nên tránh các lớp độ tin cậy khi có thể.



Hình 5.5.1 Các OpenVPN kênh dữ liệu Đóng gói

OpenVPN chia tách các tải tiêu đề thành hai phần: phần tiêu đề gói (packet header), nhận dạng

loại gói và dạng khóa và tiêu đề tải dữ liệu (data payload header), bao gồm chứng thực, IV, và các

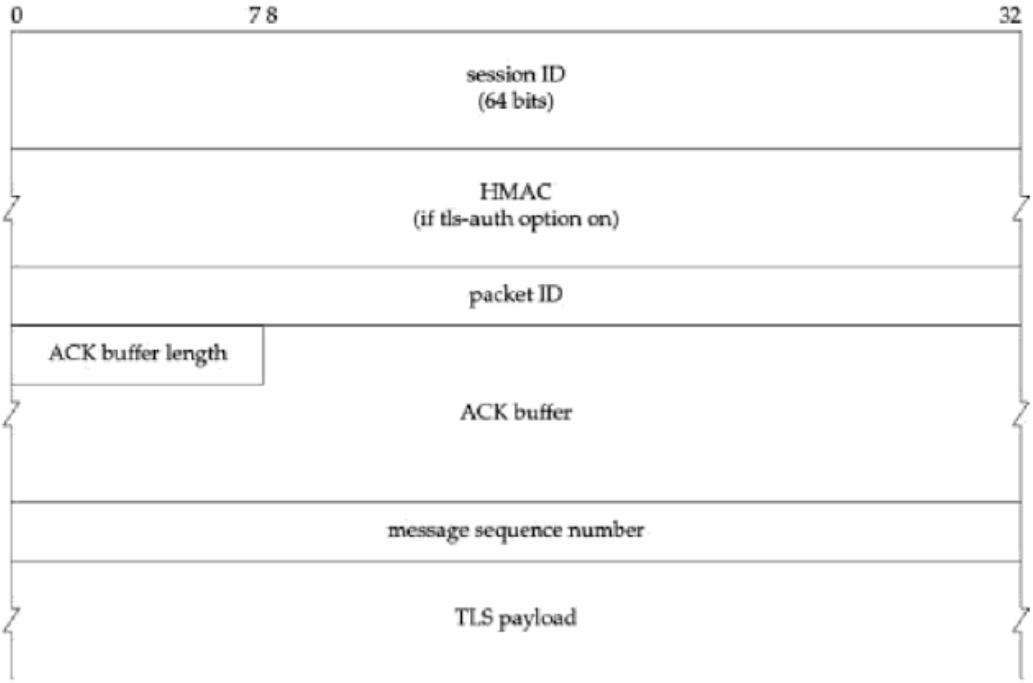
trường số thứ tự (sequence number fields) cho các gói dữ liệu.

5.6 Ping và giao thức OCC

Ngoài băng thông sử dụng, các kênh dữ liệu mang một số lượng hạn chế thông tin điều khiển. OpenVPN có thể được cấu hình để có các nút gửi, giữ các thông điệp còn sống (keep-alive) và xóa bỏ hoặc khởi động lại VPN nếu không nhận được lưu lượng truy cập trong một thời gian quy định. Mặc dù OpenVPN đề cập đến các thông điệp còn sống như các gói tin ping (ping packets), không phải theo nghĩa ping ICMP, đúng hơn là nếu một nút không có thông lượng được gửi trong một thời gian quy định, nó sẽ gửi tới chính các máy của nó một lệnh ping. Khi nhận được ping, máy muốn thiết lập lại bộ đếm thời gian nhận được gói tin của nó và loại bỏ các gói.

5.7 Kênh điều khiển

Như chúng ta đã thấy với SSL, SSH và các mạng riêng ảo khác, hai trong những phần khó nhất của việc cung cấp một kênh dữ liệu an toàn là quản lý khóa và xác thực. Lỗi trong một trong hai dịch vụ có thể làm cho các kênh dữ liệu không an toàn. Trong mục này, chúng ta tìm hiểu làm thế nào OpenVPN xử lý các khía cạnh quan trọng của VPN.



Hình 5.7.1 Gói điều khiển kênh OpenVPN

Các trường session ID là số ngẫu nhiên 64-bit được sử dụng để xác định các phiên VPN.

Trường tùy chọn HMAC được sử dụng để giúp ngăn ngừa tấn công từ chối dịch vụ. Trường này xác thực toàn bộ gói tin và cho phép một nút xóa một gói tin giả không được chứng nhận.

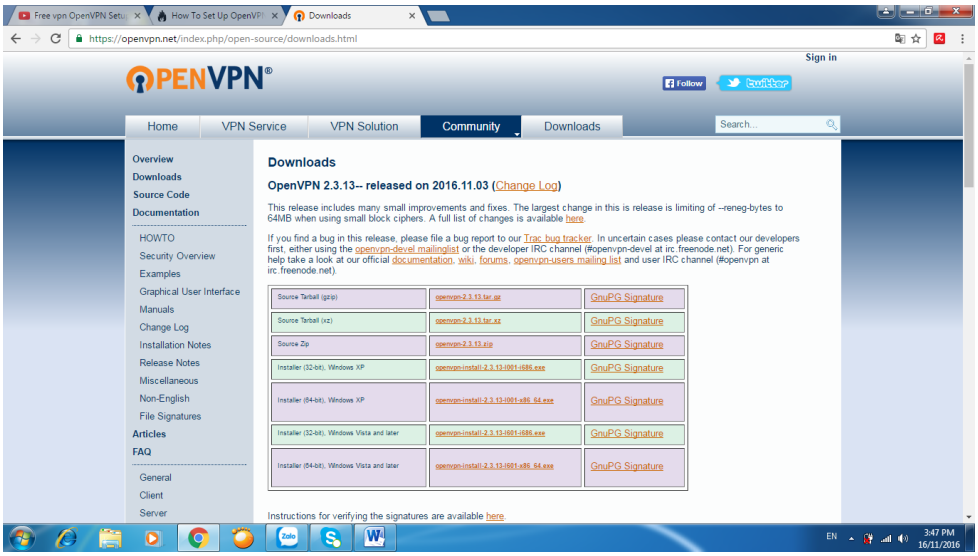
Trường Pecket ID được sử dụng để ngăn chặn các cuộc tấn công phát lại (replay attack). Nó đóng vai trò tương tự trong các gói tin kênh dữ liệu. Khi phương thức TLS được sử dụng, trường này là 32bit, nếu không nó là 64 bit.

Các bộ đệm ACK được sử dụng bởi các lớp tin cậy để xác nhận các gói tin của một máy.

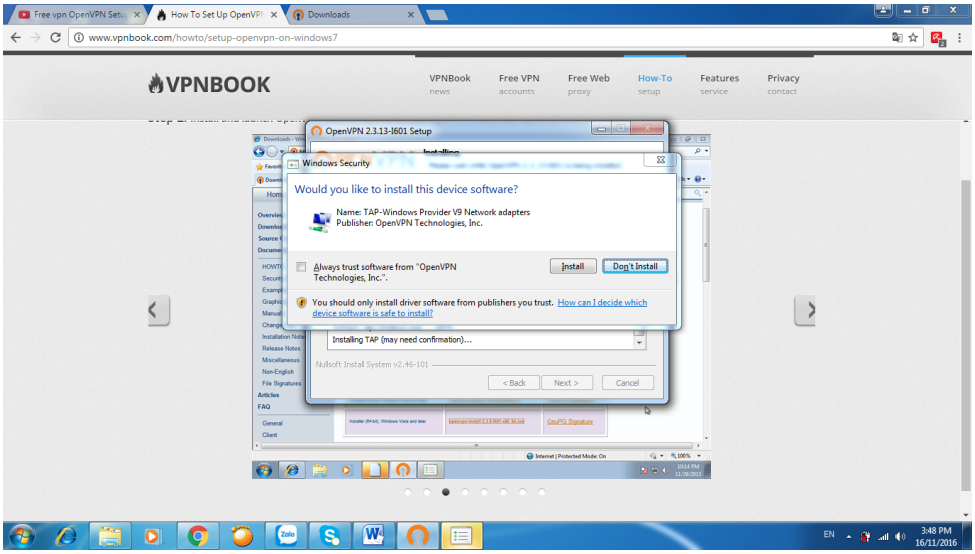
CHƯƠNG VI : TRIỂN KHAI DỊCH VỤ OPENVPN

6.1. Trên Windows

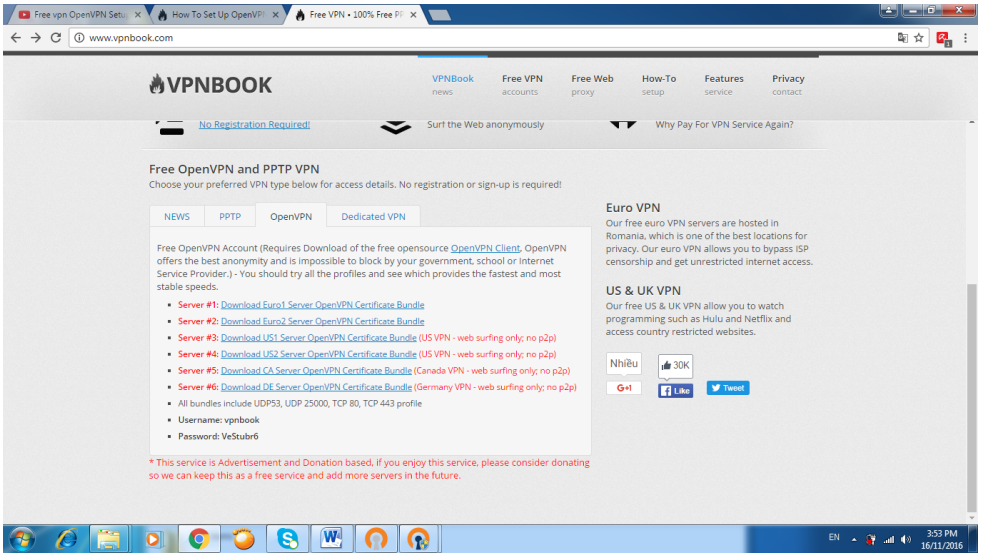
Trang chủ OpenVPN Free.



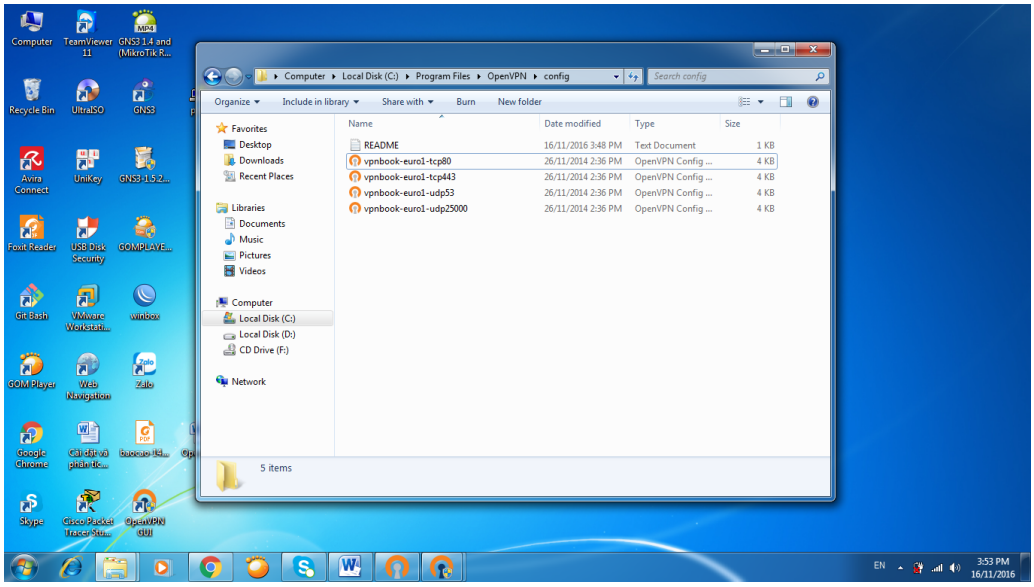
Bước 1 : Download OpenVPN Windows Client (Download 32bit cài đặt trên 32bit Windows).



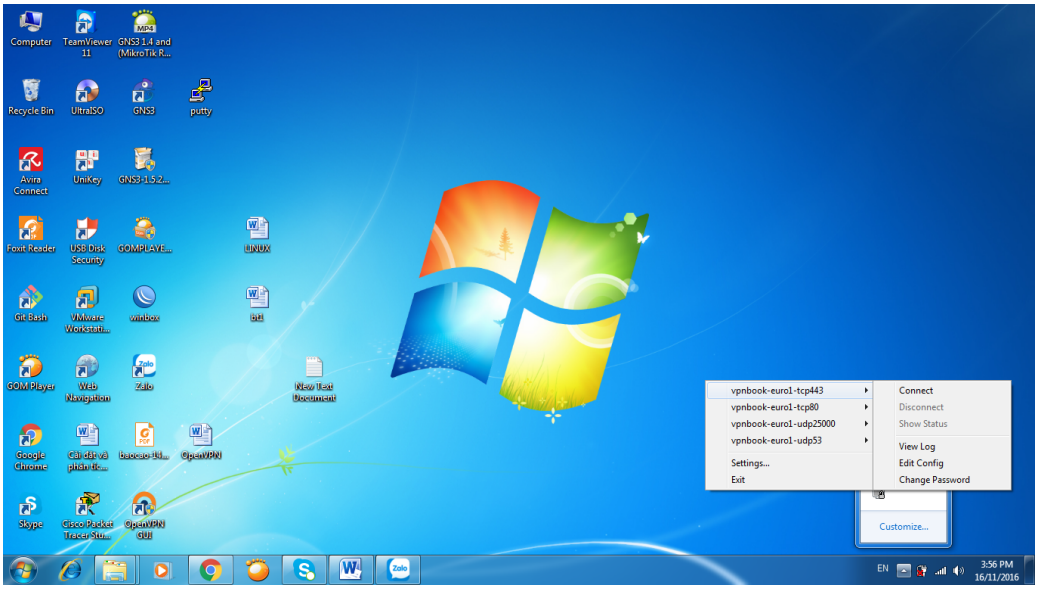
Bước 2: Install and launch OpenVPN client (Important: Run OpenVPN client as Administrator).



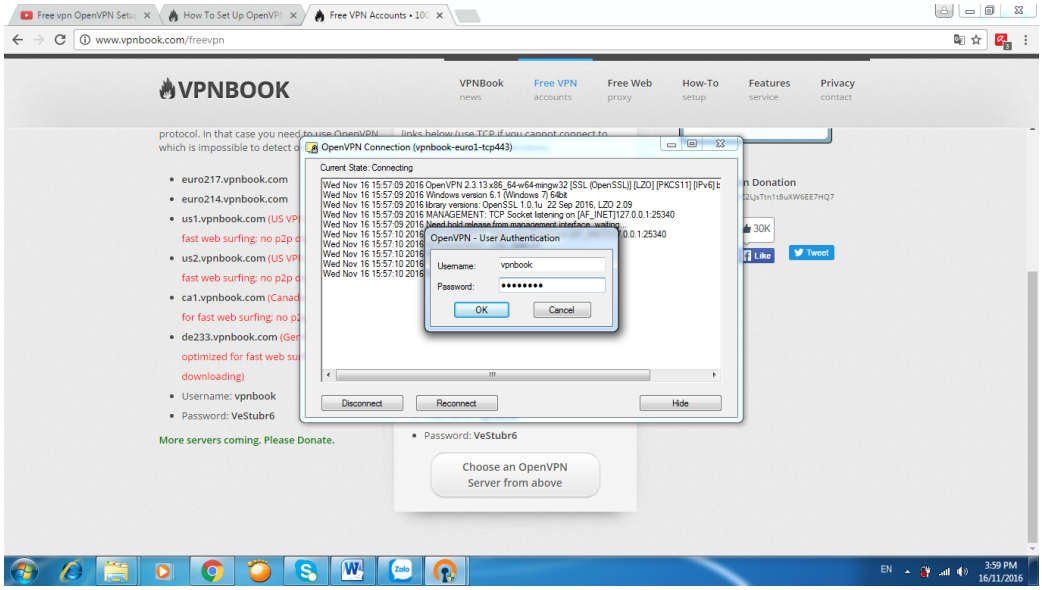
Bước 3: Download một trong những chứng chỉ của VPNBook OpenVPN.



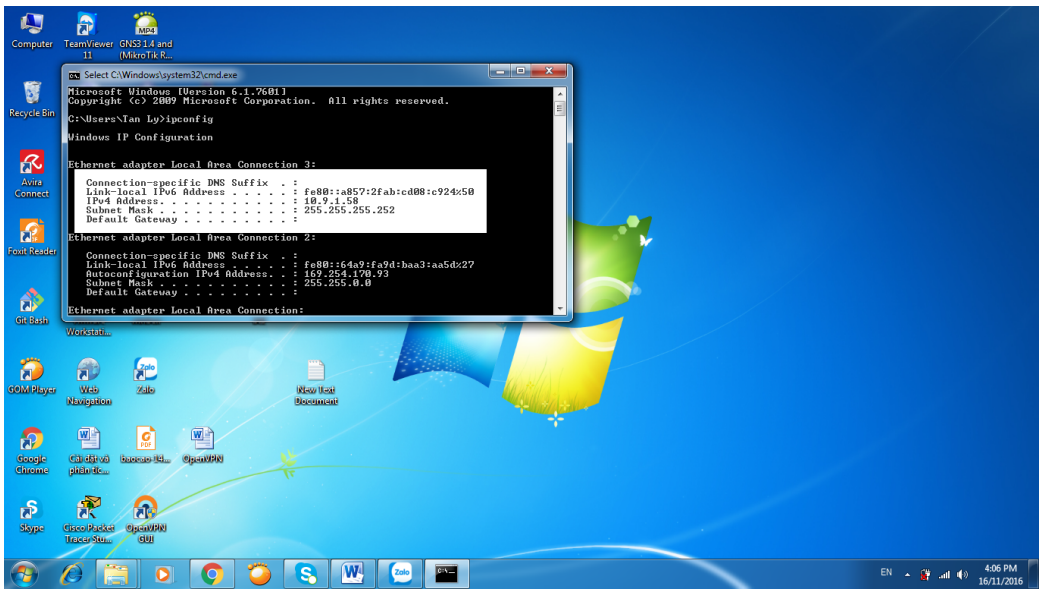
Bước 4: Giải nén và copy OpenVPN profiles đến đường dẫn C:\Program Files\OpenVPN\config.



Bước 5: Chuột phải vào biểu tượng OpenVPN Client, chọn một trong những profiles và nhấn Connect.

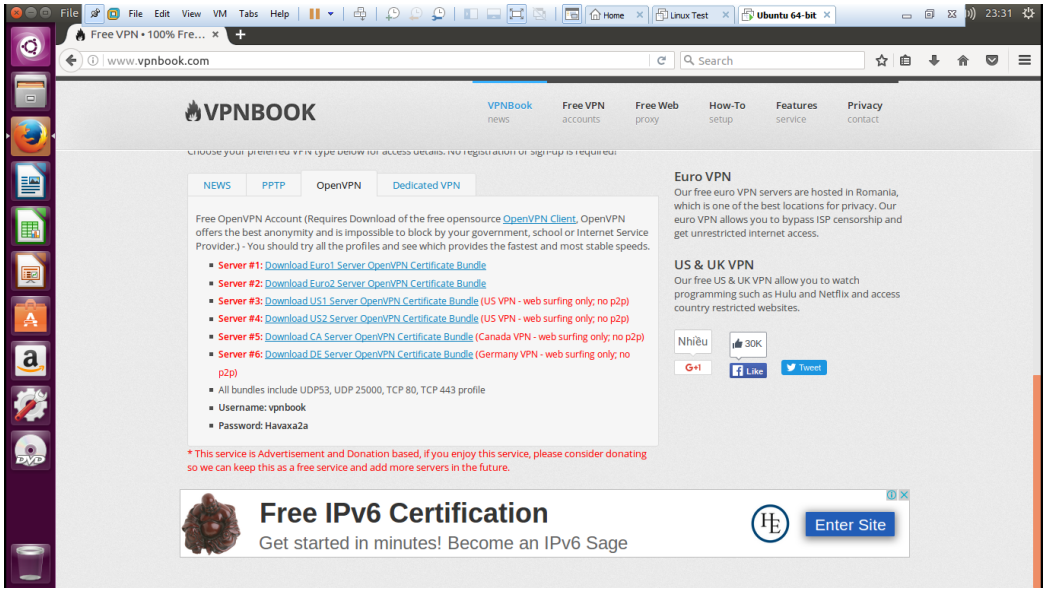


Bước 6: Nhập username/password từ đường dẫn http://vpnbook.com/freevpn.

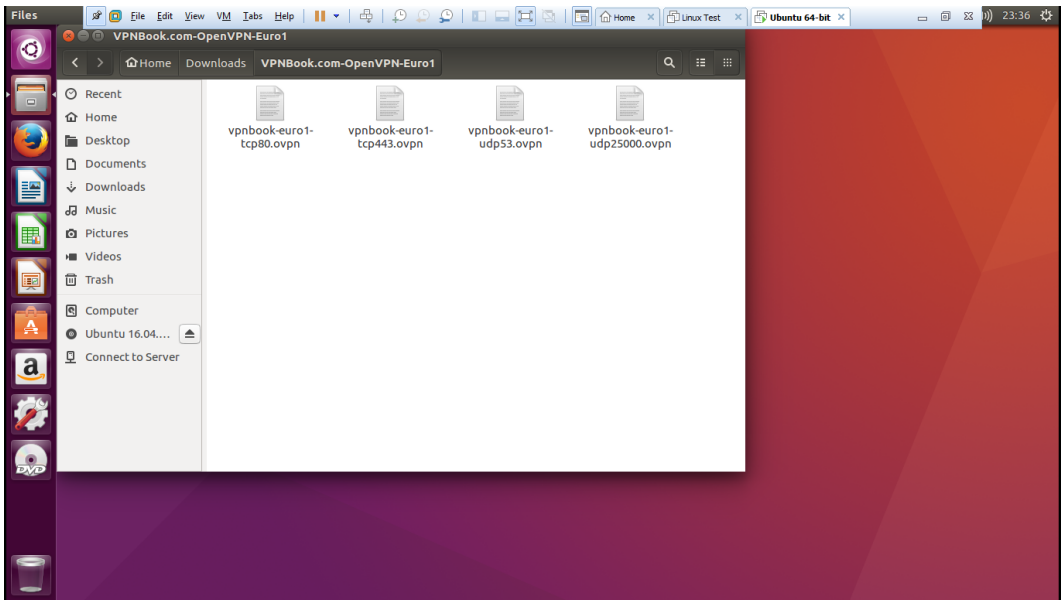


Bước 7: OpenVPN Client kết nối thành công đến VPNBook Server. Địa chỉ IP Public của bạn hiện tại đã được thay đổi đến địa chỉ IP VPNBook Server.

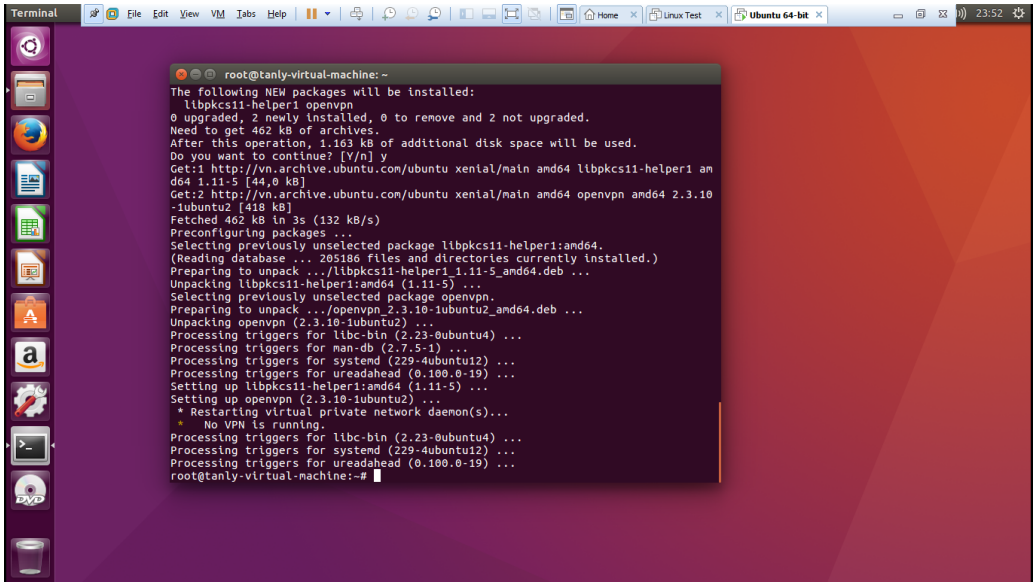
6.2. Trên Linux



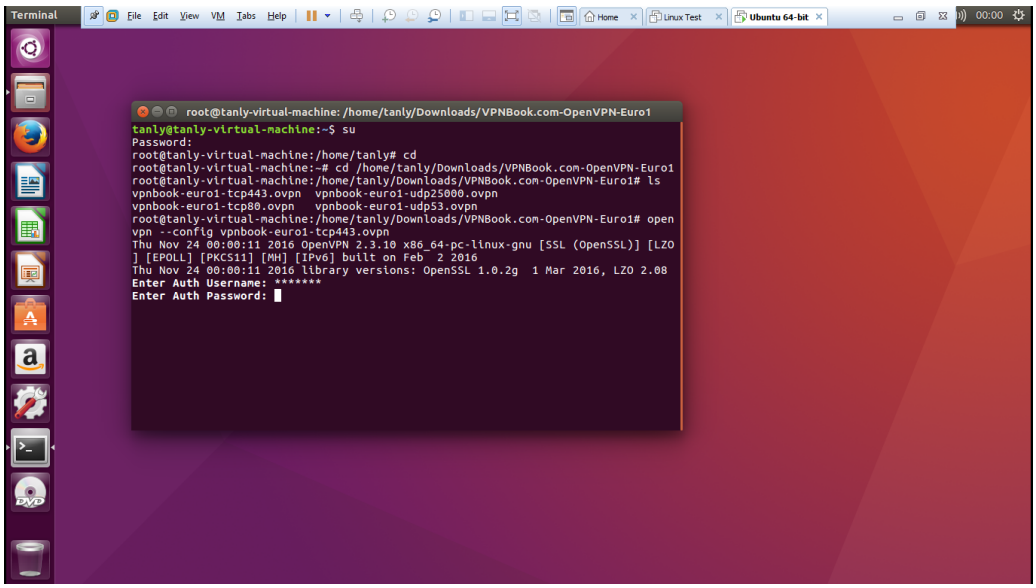
Bước 1: Download một trong những chứng chỉ của VPNBook OpenVPN.



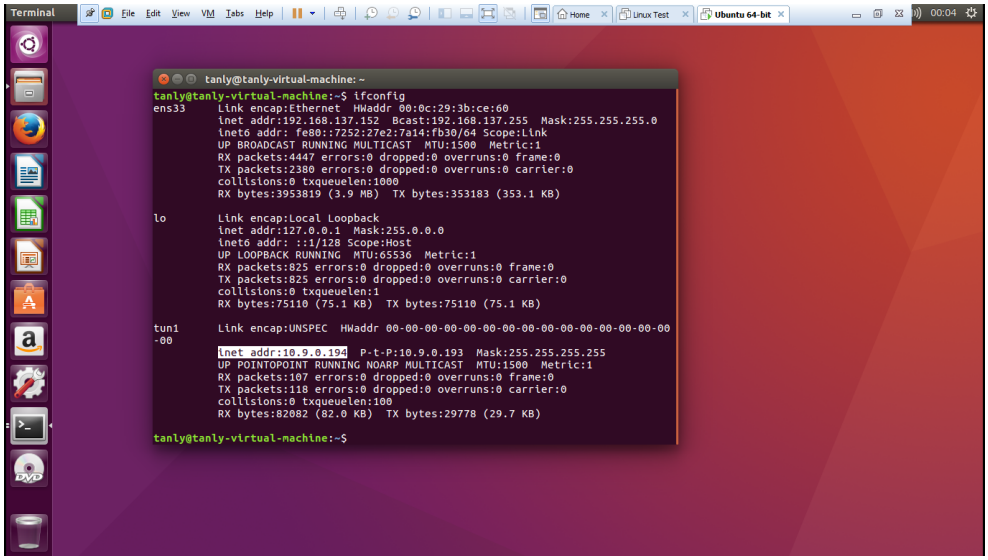
Bước 2: Giải nén chứng chỉ OpenVPN vừa mới download.



Bước 3: Vào dòng lệnh OpenVPN Client gõ “apt-get install openvpn”.



Bước 4: Cấu hình OpenVPN Client với một trong những VPNBook OpenVPN profiles. Với lệnh là: “openvpn –config vpnbook-euro1-tcp443.ovpn”. Sau đó nhập username/password từ đường dẫn http://vpnbook.com/freevpn.



Bước 5: Địa chỉ IP Public của bạn hiện tại đã được thay đổi đến địa chỉ IP VPNBook Server.

TÀI LIỆU THAM KHẢO

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

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

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

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

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

[6]. Website BestVPN.com, 2016

[7 Nghiên cứu xây dựng giải pháp Bảo mật mạng riêng ảo VPN dựa trên công nghệ mở - ThS. Nguyễn Anh Đoàn, năm 2012

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