****

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**Khoa An Toàn Thông Tin**

**---\*\*\*---**

**BÀI BÁO CÁO**

**MÔN PHÒNG CHỐNG VÀ**

**ĐIỀU TRA TỘI PHẠM MÁY TÍNH**

**Đề tài : Đường hầm trong mạng riêng ảo VPN**

*Giảng viên hướng dẫn: Lại Minh Tuấn*

*Sinh viên thực hiện: Nguyễn Thị Hồng Nhung – AT12I*

*Lâm Thị Trà Nam – AT12I*

*Nguyễn Thị Huyền Trang – AT12G*

**Hà Nội – 2019**

**MỤC LỤC**

LỜI MỞ ĐẦU ……………………………………………………………………..3

DANH MỤC HÌNH ẢNH ...……………………………………………………....4

[Chương 8: ĐƯỜNG HẦM TRONG MẠNG RIÊNG ẢO VPN 5](#_Toc25764296)

[1.1 Tổng quan về VPN 5](#_Toc25764298)

[1.2 Các mô hình VPN 6](#_Toc25764300)

[*1.2.1 VPNs truy cập từ xa (Remote access VPNs)* 6](#_Toc25764301)

[*1.2.2 VPNs điểm tới điểm (Point – to – Point VPNs)* 8](#_Toc25764303)

[1.3 AAA trong VPNs 9](#_Toc25764305)

[1.4 Đường hầm hoạt động như thế nào? 10](#_Toc25764307)

[2.1 Đường hầm SSH 12](#_Toc25764309)

[2.2 Các loại giao thức đường hầm 13](#_Toc25764310)

[*2.2.1 Giao thức đường hầm Point-to-Point* 13](#_Toc25764311)

[*2.2.2 Giao thức đường hầm Layer 2* 14](#_Toc25764313)

[*2.2.3 Giao thức đường hầm Secure Socket* 16](#_Toc25764316)

[3. Lỗ hổng VNP khác nhau và ghi nhật kí 17](#_Toc25764317)

[KẾT LUẬN 21](#_Toc25764318)

**LỜI MỞ ĐẦU**

Từ ngày xưa cho đến bây giờ, những kẻ buôn lậu đã vận chuyển hàng lậu ra nước ngoài (sản phẩm trái phép) qua biên giới mà không bị lực lượng an ninh biên giới hoặc hải quan phát hiện. Để làm điều này, đường hầm đã được sử dụng phổbiến.

Thế giới mạng có những điểm tương đồng đáng ngạc nhiên khi nó không được hỗ trợ vận chuyển và những giao thức không được phép truy cập biên giới mạng. Điều này được thực hiện bằng phương tiện của đường hầm. Tóm lại, những gì liên quan đến một đường hầm là gói gọn giao thức không được hỗ trợ (hoặc không được cấp phép) trong vị trí dữ liệu của datagram IP và sử dụng giao thức IP để gửi nó. Những giao thức đường hầm làm việc chủ yếu là tại tầng thứ 4 của mô hình OSI. Đây có nghĩa rằng họ thay thế những giao thức như TCP hoặc UDP.

Các mạng riêng ảo hoặc VPN ngắn gọn phụ thuộc hoàn toàn trong đường hầm cho hoạt động của chúng. Chương này sẽ bao gồm những hoạt động và đường hầm VPN, đường hầm chức năng và che giấu đường hầm. Chúng ta sẽ xem xét các giao thức đường hầm khác nhau cũng như nghiên cứu về lỗ hổng của hệ thống.

Chương này sẽ bao gồm những chủ đề sau:

* Tổng quan về VPN
* Đường hầm làm việc như thế nào?
* Các loại giao thức đường hầm
* Lỗ hổng VPN khác nhau và ghi nhật ký

*Nhóm sinh viên thực hiện*

**DANH MỤC HÌNH ẢNH**

[Hình 1.1: Mô hình VPN 6](#_Toc25764299)

[Hình 1.2: Remote access VPN 7](#_Toc25764302)

[Hình 1.3: Site-to-site VPNS 8](#_Toc25764304)

[Hình 1.4: Mô hình AAA 10](#_Toc25764306)

[Hình 1.5: Vận chuyển gói tin trong VPN 11](#_Toc25764308)

[Hình 2.1: VPN sử dụng giao thức Point-to-Point 14](#_Toc25764312)

[Hình 2.2: VPN sử dụng giao thức đường hầm Layer 2 15](#_Toc25764314)

[Hình 2.3: VPN sử dụng giao thức IPsec 16](#_Toc25764315)

# **Chương 8:**

# **ĐƯỜNG HẦM TRONG MẠNG RIÊNG ẢO VPN**

* 1. **Tổng quan về VPN**

Hầu hết các tổ chức có mạng riêng chỉ dành riêng tới sử dụng tổ chức. Mạng có thể là LAN, WAN hoặc MAN, phụ thuộc liên quan đến địa lý và những yêu cầu của tổ chức. Mạng riêng ảo (Virtual private networks- VPNs) như tên được đề cập, là những mạng ảo được cung cấp kinh nghiệm mạng riêng cho những người sử dụng trên một mạng công khai (không được bảo mật) – Internet. Chính xác là một VPN cung cấp một đường hầm bảo mật tới kết nối những người sử dụng bên ngoài mạng riêng với mạng tổ chức của họ. VNPS sử dụng mã hóa và xác thực cho dữ liệu gửi giữa tổ chức và người sử dụng bên ngoài ranh giới mạng:

* VPN là gì?
* Một mạng riêng ảo (VPN) mở rộng một mạng riêng truy cập tới một

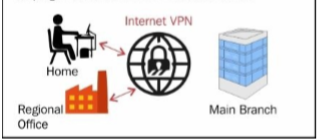
mạng công khai như là Internet, nó cho phép người sử dụng tới gửi và nhận dữ liệu truy cập được chia sẻ hoặc những mạng công khai.

* Điều khiển truy cập những kết nối VPN cho phép những người sử dụng

làm việc tại nhà hoặc trên đường tới truy cập một dịch vụ trên một mạng riêng sử dụng cơ sở hạ tầng được cung cấp bởi một mạng công khai như là Internet.

* Những kết nối VPN site-to-site cho phép tổ chức điều khiển những kết

nối giữa những văn phòng riêng hoặc với những tổ chức khác trên một mạng công khai trong khi giúp đỡ duy trì liên lạc an toàn.

Hình 1.1: Mô hình VPN

VPN có thể cũng sử dụng tới sáng tạo kết nối bảo mật giữa hai văn phòng khác nhau, như văn phòng chi nhánh và trụ sở chính. VPN có thể đóng một vai trò hoàn toàn khác nhau. Mỗi khi một người sử dụng muốn truy cập tới tài nguyên nhất định và không muốn lưu lượng bị chặn hoặc địa chỉ IP được xác định, người sử dụng có thể sử dụng một VPN để truy cập tài nguyên đó.

# **1.2 Các mô hình VPN**

VPN đáp ứng một nhu cầu rất quan trọng và khá phổ biến. Có 2 mô hình thông dụng của VPN gồm:

* VPN truy cập từ xa (Remote access VPNs)
* VPN điểm tới điểm (Point-to-point VPNs)

## *1.2.1 VPN truy cập từ xa (Remote access VPNs)*

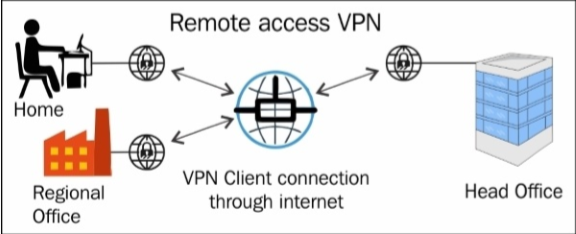
VPN truy cập từ xa được sử dụng để cung cấp an toàn mạng tổ chức truy cập tới điều khiển người sử dụng hạ tầng viễn thông công cộng như là Internet. Điều này liên quan đến việc cài đặt một máy khách chuyên dụng trên máy tính người dùng từ xa hoặc thiết bị cầm tay. Máy khách kết nối với một cổng VPN trên mạng tổ chức. Đầu tiên, cổng yêu cầu thiết bị người dùng từ xa phải trải qua xác thực danh tính sau đó nó tạo ra một liên kết mạng được mã hóa trở lại thiết bị từ xa. Liên kết hoặc đường hầm này cho phép người dùng từ xa hoạt động như thể nó có mặt cục bộ trong mạng này, tiếp cận và sử dụng các tài nguyên mạng nội bộ của tổ chức như máy chủ, máy in,...

Một số VPN truy cập từ xa cung cấp quyền truy cập an toàn vào một ứng dụng và được thiết kế dành riêng cho ứng dụng đặc biệt (ví dụ: mạng riêng ảo SSL) trong khi các mạng khác cung cấp quyền truy cập Lớp 2 (IPSec) cho toàn bộ mạng nội bộ. Chúng thường yêu cầu một giao thức đường hầm, chẳng hạn như PPTP hoặc L2TP chạy trên kết nối IPSec.

VPN truy cập từ xa thường bao gồm hai thành phần chính:

Đầu tiên là Máy chủ truy cập từ xa (RAS) còn được gọi là Máy chủ truy

cập mạng (NAS) (khác với lưu trữ đính kèm mạng, thường được liên kết với từ viết tắt NAS). NAS này xác nhận thông tin đăng nhập của người dùng và cho phép người dùng đăng nhập vào VPN. NAS có thể có quy trình xác thực riêng hoặc sử dụng máy chủ xác thực có trên mạng để xác thực người dùng từ xa:



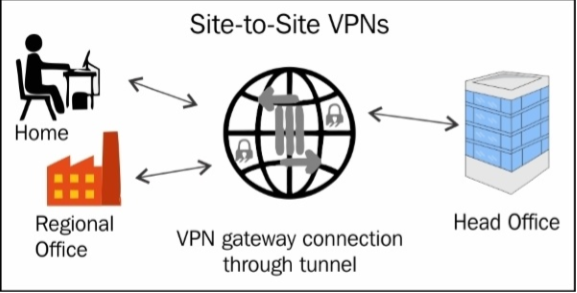
# Hình 1.2: VPN truy cập từ xa

Thành phần thứ hai là phần mềm máy khách VPN. Vai trò của phần mềm VPN là xây dựng một đường hầm đến máy chủ VPN cũng như đảm bảo mã hóa dữ liệu trong đường hầm. Rất nhiều HĐH có khả năng VPN tích hợp. Các công cụ VPN bên ngoài cũng có sẵn và khá phổ biến.

* + 1. *VPNs điểm tới điểm (Point-to-point VPNs)*

Point-to-point VPNs có thể nằm giữa các vị trí hoặc trang web cụ thể (trong trường hợp đó, chúng ta sẽ gọi nó là site-to-site VPN) hoặc giữa các máy chủ / máy tính cụ thể như máy chủ ở hai trung tâm dữ liệu khác nhau .

Trong site-to-site VPN, toàn bộ mạng ở một vị trí cụ thể được kết nối với mạng khác tại một số vị trí khác (chẳng hạn như văn phòng chi nhánh) thông qua các thiết bị cổng. Không có máy khách VPN nào được yêu cầu cài đặt trên các máy tính người dùng cuối tại các vị trí này. Các máy tính này truy cập mạng bình thường và tất cả các yêu cầu kết nối với mạng khác được xử lý liền mạch bởi cổng.



# Hình 1.3. Site-to-site VPNS

Hầu hết các VPN kết nối một trang web với một trang web khác qua Internet đều sử dụng IPSec. Thay vì sử dụng Internet công cộng, các đám mây MPLS của nhà mạng cũng có thể được sử dụng làm phương tiện giao thông. Kết nối có thể là Lớp 2 (Dịch vụ LAN riêng ảo) hoặc Lớp 3 (MPLS).

Các máy tính cụ thể cũng có thể được thiết lập để liên lạc trực tiếp với nhau thông qua VPN. Thông thường, đây có thể là các máy chủ bảo mật cao trong các trung tâm dữ liệu khác nhau về mặt địa lý, trong đó nhu cầu bảo mật cao hơn nhiều so với thiết lập cho môi trường mạng hiện tại.

# **1.3 AAA trong VPNs**

AAA là viết tắt của xác thực (Authentication), ủy quyền (Authorization) và kiểm soát (Accounting). Ba cái này là nền tảng của truy cập an toàn trong môi trường VPN:

* *Xác thực*: Điều này liên quan đến việc xác thực người dùng bằng tên

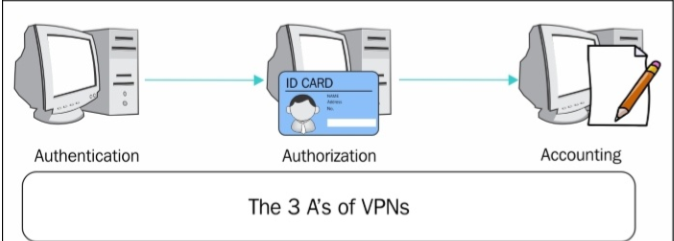
người dùng và mật khẩu hợp lệ. Trong trường hợp không có cơ chế xác thực, bất kỳ ai có máy khách VPN được cấu hình sẵn đều có quyền truy cập trực tiếp vào mạng từ xa an toàn. Dữ liệu xác thực người dùng (tên người dùng và mật khẩu) có thể được lưu trữ trên thiết bị VPN hoặc trên máy chủ AAA riêng.

* *Ủy quyền*: Đây là giai đoạn thứ hai, tại thời điểm này máy chủ đã xác

thực người dùng và bây giờ chuyển sang xác định mức ủy quyền của người dùng. Điều này xác định những gì người dùng được phép làm.

* *Kiểm soát*: Giai đoạn kiểm soát là duy trì một bản ghi của tất cả các

hoạt động được thực hiện bởi người dùng. Đây là giai đoạn đăng nhập được sử dụng rộng rãi cho kiểm toán an ninh, pháp y và mục đích báo cáo.



Hình 1.4. Mô hình AAA

Chìa khóa để kết nối và bảo mật VPN là đường hầm an toàn được thực hiện thông qua các mạng công cộng như Internet.

**1.4 Đường hầm hoạt động như thế nào?**

Quá trình đóng gói một gói trong một gói khác và sau đó gửi nó qua mạng được gọi là đường hầm.

Như chúng ta biết, mọi gói đều có một tiêu đề chứa các chi tiết liên quan đến phiên bản IP, độ dài của tiêu đề IP, kích thước của datagram IP, địa chỉ nguồn, địa chỉ đích, cờ và một loạt dữ liệu khác. Độ dài tiêu đề thường là 20 byte. Phần còn lại của gói là dữ liệu. Đường hầm liên quan đến việc ẩn các gói không được hỗ trợ hoặc không được ủy quyền trong phần dữ liệu của datagram IP. Trong những trường hợp như vậy, không gian có sẵn ít hơn so với thông thường và đôi khi điều này có thể gây ra sự cố trong dữ liệu được truyền.

Đường hầm dữ liệu thường được sử dụng để ẩn nguồn gốc của lưu lượng truy cập trên mạng. Gói và tiêu đề ban đầu được gói gọn và mã hóa và một tiêu đề lớp 3 bổ sung được thêm vào đầu. Theo cách này, quá trình tạo đường hầm giấu gọn gàng nguồn gốc của gói. Tại đích, máy tính đáng tin cậy sẽ loại bỏ tiêu đề ban đầu và xác định nguồn thực và giải mã tiêu đề ban đầu. Một điều quan trọng cần xem xét là việc tự đào hầm không đảm bảo an ninh. Trong trường hợp thiết bị bắt gói được bật, dữ liệu được gói trong gói khác có thể hiển thị nếu gói không được mã hóa.

Có ba loại giao thức đường hầm khác nhau bao gồm:

* *Giao thức hành khách*: Đây là giao thức được thực hiện trong datagram

chính IP, IPX và NetBUEI là những ví dụ về giao thức hành khách.

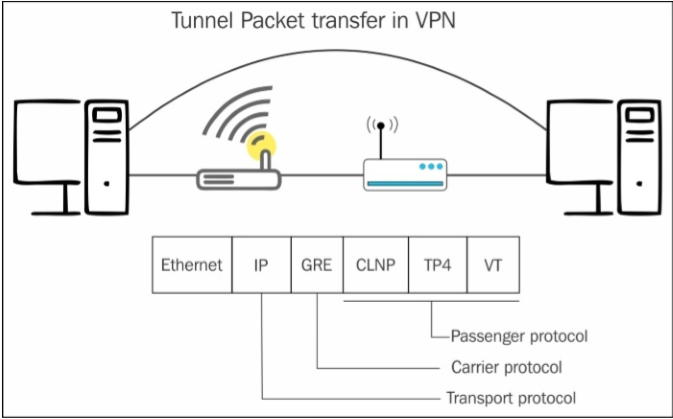
* *Giao thức đóng gói*: Đây là giao thức bao bọc, có nghĩa là giao thức bao

bọc dữ liệu hành khách. Ví dụ: IPSec, GRE, L2F, L2TP và PPTP.

* *Giao thức vận chuyển:* Đây là giao thức được sử dụng bởi mạng để

truyền dữ liệu. Thông tin đi qua giao thức này. IP là giao thức vận chuyển chính.

Gói giao thức hành khách được đóng gói và đôi khi được mã hóa trong giao thức đóng gói datagram. Điều này sau đó được đưa vào giao thức mạng di động (thường là IP) để truyền qua Internet. Điều này cho phép truyền an toàn và bảo mật các giao thức mà thông thường sẽ không được truyền qua Internet (chẳng hạn như NetBEUI).



Hình 1.5: Vận chuyển gói tin trong VPN

Tại thời điểm này, nó sẽ hữu ích cho các nhà điều tra để lưu ý rằng IPSec đã trở nên khá phổ biến ngày nay. IPSec cung cấp dịch vụ bảo mật cho các gói IP bằng cách mã hóa dữ liệu lưu lượng. Cách IPSec hoạt động trong chế độ đường hầm là mã hóa gói IP sau đó đóng gói, thêm tiêu đề IP mới và cuối cùng gửi nó đến đầu kia của đường hầm. Cách thức các giao thức đường hầm khác nhau hoạt động với IPSec được liệt kê trong các phần sau.

# **2.1 Đường hầm SSH**

Đường hầm SSH hoặc Secure Shell liên quan đến việc tạo đường hầm được mã hóa thông qua kết nối giao thức SSH. Các đường hầm SSH có thể được thiết lập như một kênh được mã hóa để vận chuyển lưu lượng không được mã hóa (chẳng hạn như giao thức khối tin nhắn SMB của máy chủ SMB trên máy Microsoft Windows) qua mạng. Đường hầm về cơ bản liên quan đến chuyển tiếp cổng. Khi thiết lập đường hầm SSH, chúng ta có thể định cấu hình máy khách SSH cục bộ để chuyển tiếp số cổng cục bộ sang số cổng được chỉ định trên máy từ xa. Sau khi thiết lập đường hầm SSH, người dùng cục bộ chỉ cần kết nối với cổng cục bộ đã chỉ định để được bảo mật truy cập vào máy từ xa thông qua cổng này. Nó không cần thiết cho các số cổng giống nhau để chuyển tiếp cổng hoạt động một cách liền mạch.

Trong ví dụ SMB trước đó, nếu chúng ta đặt một máy Windows và truy cập từ xa thì bất kỳ ai chặn lưu lượng truy cập đều có thể có quyền truy cập đầy đủ vào các tệp được chuyển. Điều này là do giao thức SMB không được mã hóa. Tuy nhiên, nếu chúng ta sử dụng một đường hầm SSH để định tuyến tất cả lưu lượng SMB đến từ máy từ xa dữ liệu sẽ được bảo mật bởi đường hầm SSH được mã hóa và dữ liệu chỉ có thể được truy cập đối với người dùng được ủy quyền.

Đường hầm SSH cũng có thể được sử dụng để vượt qua tường lửa và proxy được cấu hình để giám sát hoạt động của người dùng trong tổ chức. Trong một tổ chức hạn chế duyệt web trực tiếp bằng cách định tuyến tất cả lưu lượng truy cập cho cổng 80 thông qua proxy (từ góc độ giám sát hoạt động Internet), người dùng cục bộ có thể truy cập máy chủ SSH từ xa để cho phép đường hầm SSH cho phép chuyển tiếp cổng của một cổng cục bộ (ví dụ: 3001) sang cổng 80 của máy chủ web từ xa. Tuy nhiên, điều quan trọng cần lưu ý là điều này chỉ có thể nếu các chính sách của tổ chức cho phép kết nối đi.

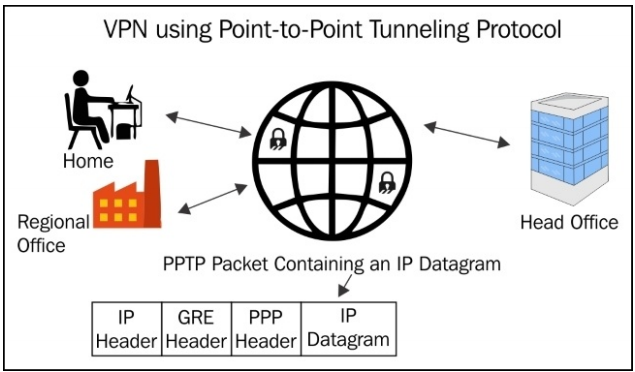
Một điểm đáng chú ý khác là khía cạnh chuyển tiếp cổng động. Một số máy khách SSH cho phép chuyển tiếp cổng động. Điều này cho phép người dùng tạo proxy SOCKS 4/5. Khi điều này được thực hiện, người dùng có thể định cấu hình ứng dụng của họ để sử dụng máy chủ proxy SOCKS linh hoạt hơn. Trong trường hợp này không cần tạo đường hầm SSH tới một cổng duy nhất trên máy chủ từ xa.

# **2.2 Các loại giao thức đường hầm**

Như chúng ta đã biết trong các phần trước, một đường hầm là một cách vận chuyển một giao thức nước ngoài qua một mạng không hỗ trợ trực tiếp. Hãy cùng xem các giao thức đường hầm khác nhau và các đặc điểm của chúng để xem cách thực hiện.

## *2.2.1 Giao thức đường hầm Point-to-Point*

Giao thức đường hầm điểm tới điểm (Point-to-Point) còn được gọi là PPTP. Điều này được tạo ra bởi một tập đoàn bao gồm Microsoft và các công ty khác. PPTP là một giao thức nhanh, ngoài Windows cũng có sẵn cho người dùng Linux và Mac. Trong khi PPTP không có khả năng cung cấp mã hóa lưu lượng, nó dựa vào giao thức Point-to-Point (PPP) để cung cấp các biện pháp bảo mật trong suốt quá trình truyền tải.

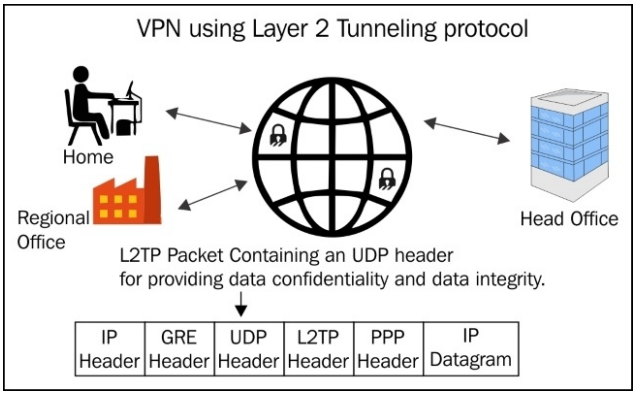


Hình 2.1: VPN sử dụng giao thức Point-to-Point

PPTP cho phép lưu lượng truy cập với các giao thức khác nhau được mã hóa và sau đó được gói gọn trong một datagram IP được gửi qua mạng IP như Internet. PPTP đóng gói các khung PPP trong các datagram IP bằng cách sử dụng một phiên bản sửa đổi của Generic Routing Encapsulation (GRE) đã sửa đổi. Một kết nối TCP được sử dụng để quản lý đường hầm. Tải trọng đóng gói có thể được nén, mã hóa hoặc cả hai trước khi truyền. Khung PPP được đóng gói này được mã hóa đầu tiên bằng cách sử dụng mã hóa Point-to-Point (MPPE) của Microsoft. MPPE hỗ trợ khóa 128 bit (đây là mã mạnh nhất), khóa 56 bit và mã 40 bit (tiêu chuẩn). Một điểm cần lưu ý là MPPE bị giới hạn trong mã hóa và không có bất kỳ vai trò nào trong việc nén hoặc mở rộng dữ liệu trong các khung PPP được xử lý bởi nén Point-to-Point của Microsoft.

## *2.2.2 Giao thức đường hầm Layer 2*

Giao thức đường hầm lớp 2 (Layer 2) thường được gọi là L2TP. Giao thức này được Microsoft và Cisco cùng phát triển với mục tiêu cung cấp tính toàn vẹn dữ liệu và bảo mật dữ liệu được cung cấp bởi giao thức PPTP. Tương tự như giao thức PPTP, L2TP không cung cấp mã hóa và sử dụng PPP để thực hiện việc này.



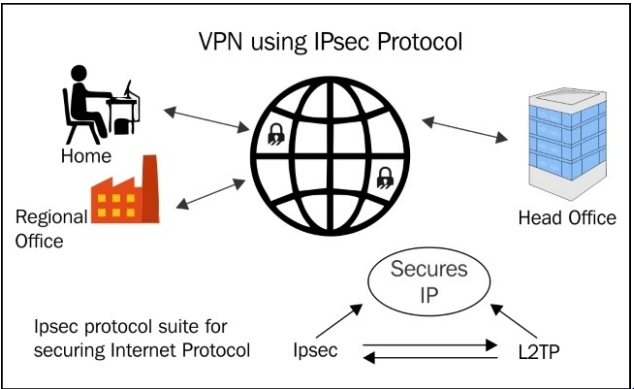
# Hình 2.2 : VPN sử dụng giao thức đường hầm lớp 2

Trong triển khai L2TP của Microsoft, việc mã hóa các datagram PPP không được thực hiện bằng MPPE mà với bảo mật Giao thức Internet hoặc IPSec. Do đó, giao thức này thường được gọi là L2TP / IPSec. Để L2TP / IPSec hoạt động, cả máy chủ VPN và máy khách cần phải có hỗ trợ cho việc này.

L2TP / IPSec được xây dựng trong hầu hết các hệ điều hành như Windows, Linux và Apple. Nó rất dễ thực hiện.

IPSec được coi là khá an toàn từ góc độ bảo mật và không có bất kỳ lỗ hổng lớn nào được biết đến (cho đến nay). Tuy nhiên, Snowden, như một phần trong nhiều tiết lộ của ông đã đề cập rằng IPSec đã bị NSA xâm phạm. Với mục đích xác thực, L2TP hỗ trợ các khóa chia sẻ trước hoặc chứng chỉ máy tính. Xác thực chứng chỉ máy tính yêu cầu PKI cấp chứng chỉ cho máy chủ VPN và tất cả các máy khách VPN. Việc sử dụng L2TP / IPSec cung cấp xác thực máy tính / máy chủ ở lớp IPSec và xác thực lớp người dùng ở lớp PPP. L2TP được mã hóa bằng thuật toán mã hóa dữ liệu DES hoặc 3DES.

Việc sử dụng IPSec đảm bảo tính bảo mật, toàn vẹn và xác thực dữ liệu cho kết nối VPN.



# Hình 2.3: VPN sử dụng giao thức Ipsec

## *2.2.3 Giao thức đường hầm Secure Socket*

Secure Socket Tunneling Protocol còn được gọi là SSTP. Đây là một giao thức đường hầm mới sử dụng HTTPS qua cổng TCP 443. Điều này cho phép nó truyền lưu lượng qua tường lửa và proxy có thể được cấu hình theo cách khác để chặn lưu lượng PPTP hoặc L2TP / IPSec. SSTP hoạt động bằng cách thiết lập lớp HTTPS hai chiều với máy chủ SSTP. Các gói dữ liệu SSTP chảy qua lớp HTTPS này.

Lớp HTTPS hoặc lớp cổng bảo mật này thực hiện kiểm tra tính toàn vẹn lưu lượng truy cập, cũng như mã hóa và bảo mật cấp vận chuyển. SSTP phù hợp với VPN truy cập máy khách từ xa và thường không hỗ trợ các đường hầm VPN tại chỗ.

Vì SSTP hoạt động trên truyền tải TCP, hiệu suất của nó phụ thuộc vào tính khả dụng của băng thông trên kênh TCP. Trong trường hợp thiếu băng thông, hiện tượng TCP phổ biến là meltdown.

Trong tất cả ba giao thức đường hầm trước đó, các khung PPP được thực hiện trên đỉnh của giao thức mạng. Do đó, các tính năng PPP như đàm phán IPv4 và IPv6, bảo vệ truy cập mạng cũng như xác thực là phổ biến trên cả ba giao thức.

# **3. Lỗ hổng VNP khác nhau và ghi nhật kí**

Với việc sử dụng rộng rãi VPN, chức năng mở rộng mà chúng cung cấp, tính kinh tế của việc sử dụng và tính minh bạch của chúng đối với người dùng, đó chỉ là vấn đề thời gian trước khi kẻ xấu bắt đầu nhắm mục tiêu VPN. Một số lý do khiến VPN là mục tiêu tấn công:

* Người dùng có xu hướng sử dụng VPN để truyền thông tin nhạy cảm.

Điều này cũng dễ hiểu bởi niềm tin chung là VPN được bảo mật.

* VPN thường có quyền truy cập đầy đủ và không hạn chế vào các mạng

nội bộ. Đạt được truy cập thông qua VPN cung cấp quyền truy cập đầy đủ và không bị cản trở vào các mạng công ty.

* VPN cung cấp ẩn danh từ IDS nếu chúng được cấu hình để hoạt động

bên ngoài VPN. Bất kỳ kẻ xấu nào có quyền truy cập vào VPN đều có thể ẩn trong đường hầm được mã hóa và không được phát hiện bởi IDS.

* VPN là mục tiêu tương đối mềm. Điều này là do mọi người có xu hướng

xem xét IPSec tương đối an toàn và có xu hướng dành tài nguyên làm cứng các thành phần mạng khác.

Vậy những cách mà VPN có thể bị xâm phạm là gì? Hiểu điều này sẽ giúp chúng ta hiểu những gì chúng ta nên tìm kiếm từ góc độ điều tra. Để bắt đầu, hãy có một cái nhìn nhanh hơn về cấu trúc của VPN. Ở một đầu là máy chủ VPN và đầu khác là máy khách VPN. Cả hai đều được kết nối với nhau sử dụng đường hầm an toàn. Từ góc độ bảo mật, các điểm dễ thỏa hiệp nhất là hai điểm cuối. Thông thường, máy khách VPN được bảo vệ ít nhất và được sử dụng trong tất cả các khu vực an ninh thấp, chẳng hạn như sân bay và khu vực Wi-Fi miễn phí.

Máy khách VPN được triển khai trong thiết bị cầm tay. Một khía cạnh của máy khách VPN đang chạy trên các thiết bị như đây là sự sẵn có. Từ góc nhìn của một kẻ xấu, họ càng tiếp cận lâu với thiết bị thì cơ hội để có thể thỏa hiệp nó càng cao. Đây có thể không phải là trường hợp khi chúng ta xem xét người dùng từ xa bằng cách sử dụng máy khách VPN. Ngược lại, máy chủ VPN (như một phần mô tả công việc của nó) liên tục có sẵn và tìm kiếm các kết nối. Do đó, cả hai điểm cuối có thể phải chịu các loại tấn công khác nhau khi mục tiêu là tận dụng các lỗ hổng của họ.

Hiện tại, IPSec là giao thức quan trọng nhất khi nói đến VPN. Nó phần lớn được coi là an toàn nhất trong tất cả các triển khai VPN. Thật không may, nó cũng rất phức tạp để thực hiện chính xác. Quản trị viên có chuyên môn và kinh nghiệm là cần thiết để triển khai IPSec hiệu quả. Việc thiếu các quản trị viên như vậy dẫn đến mặc định cấu hình hoặc cấu hình sai, góp phần tạo một bảo mật yếu trong số lượng lớn các trường hợp.

Một trong những phương pháp dễ dàng nhất và thực sự rất phổ biến để có được quyền truy cập vào mạng công ty là đánh cắp máy tính xách tay của công ty. Rất nhiều người dùng có xu hướng lưu thông tin đăng nhập truy cập VPN của họ trên các thiết bị / máy tính từ xa. Do đó, mất máy tính xách tay như vậy có thể có nghĩa là mất dữ liệu từ mạng của công ty. Thông tin lưu trữ bộ nhớ cache VPN bao gồm dữ liệu được lưu trữ trong sổ đăng ký có thể được lấy và sử dụng cho mục đích xấu.

Một phương pháp khác để có quyền truy cập vào VPN là thỏa hiệp máy khách hoặc máy chủ máy bằng cách lây nhiễm hệ thống hoặc tấn công người trung gian (MITM). Trong trường hợp máy bị nhiễm, thông tin người dùng có thể bị xâm phạm và sử dụng sai.

Một số phương pháp bảo đảm các thỏa hiệp như vậy là bằng cách mã hóa toàn bộ máy khách (WDE) trong trường hợp trộm cắp, tường lửa mạnh và bảo vệ chống vi-rút để ngăn chặn máy khách và máy chủ thỏa hiệp, xác thực bằng cách sử dụng mã thông báo và hệ thống kiểm soát truy cập với người dùng cung cấp và hệ thống nhận dạng với quản trị VPN.

Một ví dụ khác là quên vô hiệu hóa tài khoản VPN của nhân viên bị khi nhân viên nghỉ việc. Năm 2005, đây là nguyên nhân của một cuộc tấn công lớn vào mạng Walmart, đã bị vi phạm và dữ liệu nội bộ có thể truy cập được cho nhân viên cũ. Điều này bao gồm thông tin thẻ thanh toán. Cuộc tấn công này kéo dài trong khoảng 18 tháng và chỉ được phát hiện một cách tình cờ.

Một trường hợp thú vị liên quan đến một nhân viên cũ bán hết cổng VPN đã sử dụng, được tìm thấy bởi người mua vẫn được cấu hình để truy cập mạng công ty rất lâu sau khi nhân viên đã rời khỏi tổ chức.

Vào năm 2010, một lỗ hổng cấu hình cao liên quan đến IPv6 và PPTP đã được công khai. Điều này làm lộ địa chỉ IP, địa chỉ MAC và tên máy tính. Gần đây hơn, năm 2015 các nhà nghiên cứu từ Đại học Sapienza của Rome và Đại học Queen Mary ở Luân Đôn đã phát hiện ra các lỗ hổng bảo mật trong 14 nhà cung cấp VPN phổ biến. Nó đã được tìm thấy rằng một số trong số này đã tiết lộ một lịch sử duyệt hoàn chỉnh của người dùng. Những lỗ hổng này được phân loại là rò rỉ lưu lượng IPv6 và chiếm quyền điều khiển DNS.

Các sản phẩm VPN không có khách hàng cũng gây ra rủi ro bảo mật. Các dữ liệu này tổng hợp dữ liệu được truy xuất từ ​​các trang web khác nhau và cung cấp dữ liệu đó để nó xuất hiện như là từ SSL VPN. Điều này cho phép một trang web độc hại cũng được phục vụ cho người xem trong khi dường như đến từ một nguồn thông qua SSL VPN. Kẻ xấu có thể chiếm quyền điều khiển phiên người dùng hoặc nắm bắt tổ hợp phím của người dùng và giành quyền truy cập vào VPN.

Chế độ xâm phạm trao đổi khóa Internet (IKE) (AM) cũng có thể gây nghiêm trọng vi phạm an ninh thông tin trên các khách hàng lớn tuổi. IPSec, khi đàm phán một đường hầm kết nối, thực hiện trao đổi thông tin giữa hai khách hàng. Trao đổi khóa này có thể xảy ra ở chế độ Chính hoặc chế độ Tích cực. Trong khi chế độ Chính sử dụng một bắt tay sáu chiều, chế độ tấn công sử dụng bắt tay ba chiều. Trong quá trình bắt tay, thiết bị VPN gửi PSK băm ở dạng không được mã hóa. Điều này cho phép một kẻ tấn công để thực hiện một cuộc tấn công bằng các công cụ như L0phtcrack, psk-crack, Cain, John the Ripper.

Mặc dù các phương thức thỏa hiệp VPN được đề cập trước đây nhưng không có nghĩa là đầy đủ, chìa khóa cho các nhà điều tra là nhật ký tài liệu tất cả các mạng tương tác và các chỉ số của sự thỏa hiệp. Điều này giúp chúng ta xác định ai đã làm gì, ở đâu, khi nào và như thế nào.

Thông tin cần phải nắm bắt bao gồm những điều sau đây:

* Người sử dụng
* Ngày và giờ sự kiện
* Quyền điều khiển
* Trạng thái xác thực (Thành công / Thất bại)
* Tình trạng ủy quyền (Thành công / Thất bại)
* Thay đổi cấu hình (để phát hiện giả mạo bằng Anti-virus / IDS / IPS /

Tường lửa và v.v.) - ví dụ, Trojan ngân hàng được biết là vô hiệu hóa tường lửa địa chỉ mạng.

* Các giao thức mạng
* Quyền truy cập đặc quyền

Tất cả các cuộc điều tra sẽ yêu cầu chúng ta phải xem xét các con đường kiểm toán này để di chuyển thành công mạng lưới điều tra pháp y của chúng ta về phía trước.

**KẾT LUẬN**

Trong chương này, nhóm em đã hiểu khái niệm về mạng riêng ảo và vai trò của chúng trong mạng. Nhóm em đã xem xét các loại VPN khác nhau và các giao thức đường hầm của chúng. Nhóm cũng đã nghiên cứu cách thức, giống như những kẻ buôn lậu, VPN được sử dụng để vận chuyển các giao thức nước ngoài thông qua các đường hầm vào mạng công ty. Cuối chương, nhóm em đã xem xét các cách thức mà VPN có thể bị xâm phạm và do đó, dẫn đến sự thỏa hiệp của các mạng của chúng ta.