Nội dung trình bày

Nội dung:

I. Giới thiệu tổng quan về VPN

II. VPN và bảo mật INTERRNET VPN

III. Thiết kế các khối của một VPN

IV. Quản lý VPN

V. Tổng kết

2

Những kiến thức liên quan

- Lý thuyết mạng 
- TCP/IP 
- Mã hoá thông tin 
- Firewall 

3

I. GIỚI THIỆU TỔNG QUAN VỀ VPN
1.MẠNG RIÊNG ẢO LÀ GÕ?

- **V**irtual
- **P**rivate
- **N**etwork

4

Virtual Private Network gọi là mạng riêng ảo -VPN được khởi sự năm 1997

• Khái niệm mạng riêng ảo

Là phương pháp làm cho một mạng công cộng hoạt động như một mạng cục bộ kết hợp với các giải pháp bảo mật trên đường truyền. VPN cho phép thành lập các kết nối riêng với người dùng ở xa, các văn phòng chi nhánh của công ty và các đối tác của công ty đang sử dụng chung một mạng công cộng.

• Khái niệm định đường hầm (Tunneling)

Là cơ chế dùng cho việc đóng gói một giao thức trong một giao thức khác. Định đường hầm cho phép che dấu giao thức lớp mạng nguyên thuỷ bằng cách mã hoá gói dữ liệu và chứa gói đã mã hoá vào trong một vỏ bọc IP.

5

Khái niệm về chất lượng dịch vụ

VPN còn cung cấp các thoả thuận về chất lượng dịch vụ (QoS), định ra một giới hạn trên cho phép về độ trễ trung bình của gói trong mạng.

VPN= Định đường hầm + Bảo mật + Các thoả thuận QoS

Tại sao phải xây dựng VPN ?

✓ **Giảm chi phí đường truyền: cho phép tiết kiệm đến 60% chi phí so với thuê bao đường truyền và giảm đáng kể tiền cước.**

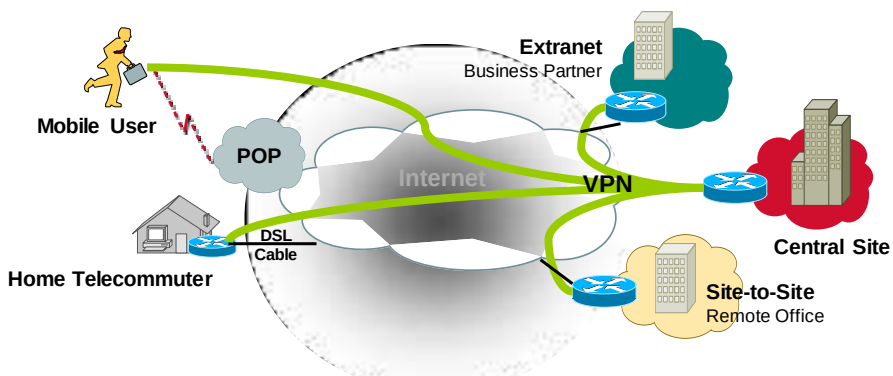
✓ **Giảm chi phí đầu tư. VPN không tốn chi phí đầu tư cho máy chủ, bộ định tuyến, các bộ chuyển mạch như khi đầu tư cho một mạng WAN của công ty (có thể thuê của các nhà cung cấp dịch vụ).**

6

- ✓ Giảm chi phí quản lý và hỗ trợ. Với quy mô kinh tế của mình các nhà cung cấp dịch vụ có thể mang lại cho công ty những tiết kiệm có giá trị so với với việc tự quản lý mạng
- ✓ Truy cập mọi lúc mọi nơi. VPN không làm ảnh hưởng đến bất kỳ một dịch vụ truền thống nào của Internet.

7

2.Phân loại mạng riêng ảo

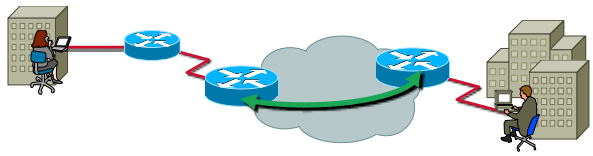


- Truy cập từ xa (Remote Access)
- Kết nối chi nhánh của công ty (Site to Site)
- Mạng mở rộng (ExtranetVPN)

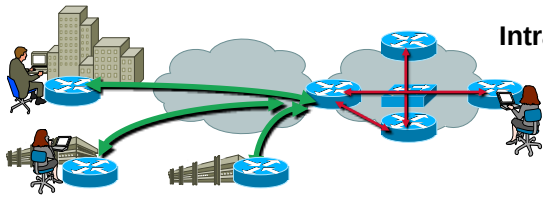
8

Ba loại liên kết trong mạng VPN

Remote User Access



Intranet



Extranet

9

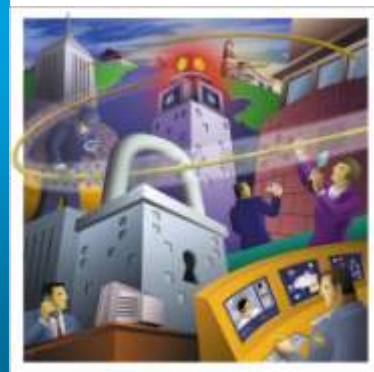
3.Cấu trúc của VPN

- **Tính tương thích (Compatibility)**
  - *Hỗ trợ nhiều chuẩn giao thức*
- **Tính bảo mật (Sercurity)**
  - *Password cho User trong mạng*
  - *Mã hoá dữ liệu khi truyền*
  - *Đơn giản trong quản lý, sử dụng*
- **Tính khả dụng (Availability)**
  - *Tốc độ kết nối*
  - *Chất lượng dịch vụ (QoS)*
- **Khả năng hoạt động tương tác**
  - *Đồng bộ với thiết bị sử dụng*

10

II. VPN và bảo mật internet vpn

- Kiến trúc VPN
- Bảo mật với VPN
- Giao thức trên VPN



11

1.Kiến trúc mạng VPN

Kiến trúc của một mạng VPN

Đường hầm: phần ảo trong VPN:

✓Không duy trì kết nối thường trực giữa các điểm cuối, thay vào đó một nối chỉ được tạo ra giữa hai **site** khi cần thiết, khi không còn cần thiết nữa thì nó sẽ bị huỷ bỏ, tài nguyên mạng sẵn sàng cho những kết nối khác.

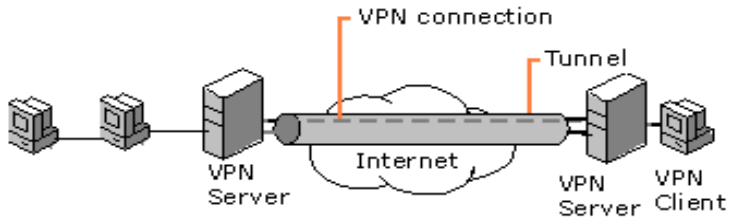
✓Đối với người sử dụng VPN những thành phần vật lý của mạng được các ISP giấu đi. Việc che giấu cơ sở hạ tầng của ISP và Internet được thực hiện bởi khái niệm gọi là định đường hầm (Tunneling)

12

- ✓ Việc tạo đường hầm tạo ra một kết nối đặc biệt giữa hai điểm cuối. Để tạo ra một đường hầm điểm cuối nguồn phải đóng các gói của mình trong những gói IP (IP Packet) cho việc truyền qua Internet. Trong VPN việc đóng gói bao gồm cả việc mã hoá gói gốc. Điểm cuối nhận, cổng nối (Gateway) gỡ bỏ tiêu đề IP và giải mã gói nếu cần và và chuyển gói đến đích của nó.
- ✓ Việc tạo đường hầm cho phép những dòng dữ liệu và thông tin người dùng kết hợp được truyền trên một mạng chia sẻ trong một ống ảo (virtual pipe). ống này làm cho việc định tuyến trên mạng hoàn toàn trở nên trong suốt đối với người dùng.

13

Gói tin kiểu đường hầm



14

Các dịch vụ bảo mật: phần riêng trong VPN

Authemtication: Bảo đảm dữ liệu đến có nguồn gốc rõ ràng.
Access control: ngawnhững người dùng bất hợp pháp.
Confidentiality: Hạn chế việc dữ liệu bị phá hoại trên đường truyền.
Data intergity: Bảo không ai có thể thay đổi nội dung dữ liệu trên đường truyền.

Mặc dù những đường hầm có thể làm cho việc truyền dữ liệu trên Internet được bảo mật, nhưng việc xác thực người dùng và duy trì tính toàn vẹn dữ liệu phụ thuộc vào các tiến trình mã hoá như: chữ ký điện tử, xác nhận văn bản. Những tiến trình này được sử dụng thông qua các khoá, phải được phân phối và quản lý chặt chẽ, đây là một công việc của mạng VPN. Mặt khác các dịch vụ bảo mật dữ liệu được thực hiện ở tầng 2 và tầng 3.

15

2. Một số giao thức cho VPN

a. Point to Point Tunneling Protocol (PPTP)

PPTP là mở rộng của giao thức PPP (RFC 1661).

Dịch vụ đường hầm mà PPTP cung cấp chạy phía trên của lớp IP, ngược lại thì giao thức PPP truyền thống lại nằm ở phía dưới. PPP thích hợp cho việc biến đổi bởi vì hoạt động của nó cũng gần giống như hoạt động mà VPN cần, nhưng PPP không an toàn.

Kết nối điều khiển PPTP: Khi sử dụng kết nối tới Internet được thiết lập bởi PPP, PPTP thiết lập kết nối điều khiển, sử dụng cổng TCP 1723, kết nối này dùng TCP để thiết lập.

Xác thực: Các máy khách PPTP được nhận thực khi sử dụng giao thức PPP. Các mật khẩu rõ ràng được sử dụng các cách xác thực là PAP – Password Authentication Protocol, CHAP – Chalenge Handshake Authentication Protocol. RFC 1334, RFC1994, RFC2284.

16

b. Layer 2 Tunneling Protocol (L2TP)

Giao thức đường hầm lớp 2 lai ghép (Hybrid Layer 2 tunneling)

- Giao thức để xây dựng đường hầm cho VPN đối với nhu cầu truy cập từ xa. Là mở rộng của giao thức PPP, kết hợp được ưu điểm của L2F của Cisco và PPTP của Microsoft.

- Hỗ trợ cho môi trường đa giao thức: Truyền được bất kỳ giao thức nào được định tuyến gồm: IP, IPX, AppleTalk.

- Phương tiện độc lập: L2PT hoạt động trên bất kỳ mạng nào có khả năng truyền khung IP, hỗ trợ bất kỳ đường trục WAN nào: Frame Relay, ATM, X25, SONET, hỗ trợ các phương tiện LAN: Ethernet, TokenRing, FDDI.

- Có thể thiết lập từ máy chủ truy cập mạng (Network Access Server) hoặc từ phần mềm client tới một router hoạt động như điểm đầu cuối của đường hầm.

17

3. Minh hoạ kiến trúc VPN của Cisco

Khối truy cập VPN

Khối truy cập làm nền cho các ứng dụng thương mại, được thiết kế tuân theo các yêu cầu và quy định giống như mạng riêng của công ty.

Khối bảo mật

@ Kiến trúc xác thực

Trong môi trường truy cập VPN, khía cạnh bảo mật quan trọng nhất liên quan đến việc nhận dạng ra một người dùng của công ty và thiết lập một đường hầm đến cổng nối của công ty. Cổng nối này phải có khả năng xác thực người dùng, các quyền truy cập và tính cước (AAA).

@ Xác thực đơn phương

Để xác thực người dùng, đầu tiên Client sẽ thiết lập kết nối đến mạng cung cấp dịch vụ thông qua một POP, sau đó thiết một kết nối thứ hai với mạng khách hàng.

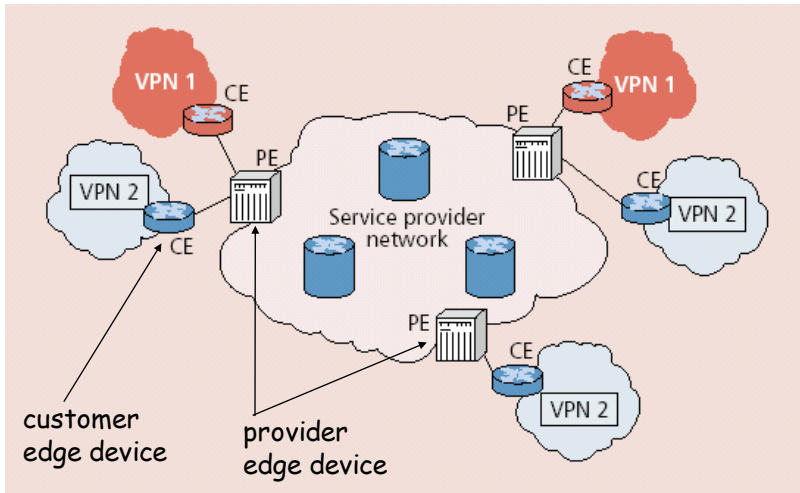
18

Các điểm cuối của đường hầm trong truy cập VPN xác thực với nhau. Kế tiếp người dùng kết nối đến các thiết bị đầu cuối khách hàng (CPE) Các

Cổng nối người dùng sử dụng giao thức phân tích chất lượng thành viên hay giao thức Internet tuyến nối tiếp SLIP (Serial Line Internet Protocol) và được xác thực thông qua một giao thức xác định tên/mật khẩu như : PAP (Password Authentication Protocol), giao thức xác thực yêu cầu bắt tay CHAP (Chanllenge Handshake Protocol) hay một hệ thống điều khiển truy cập cứng.

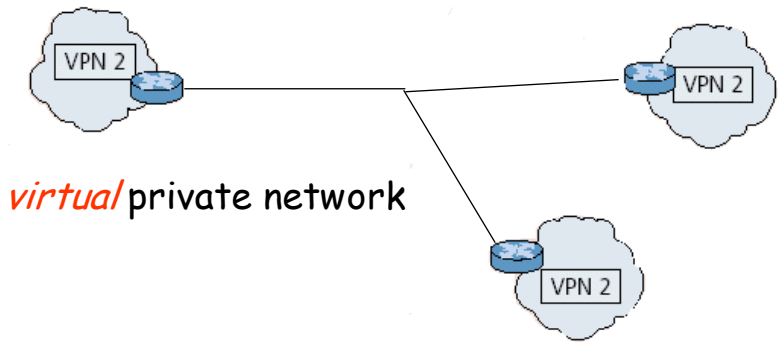
19

VPN reference architecture



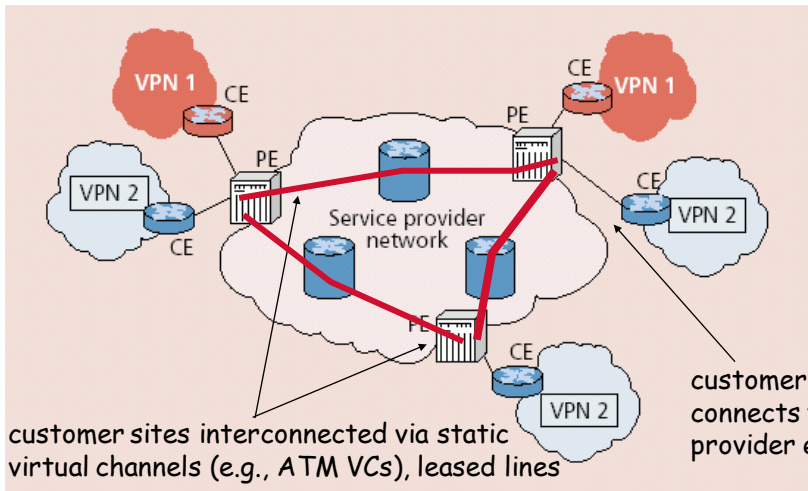
20

VPN: logical view



21

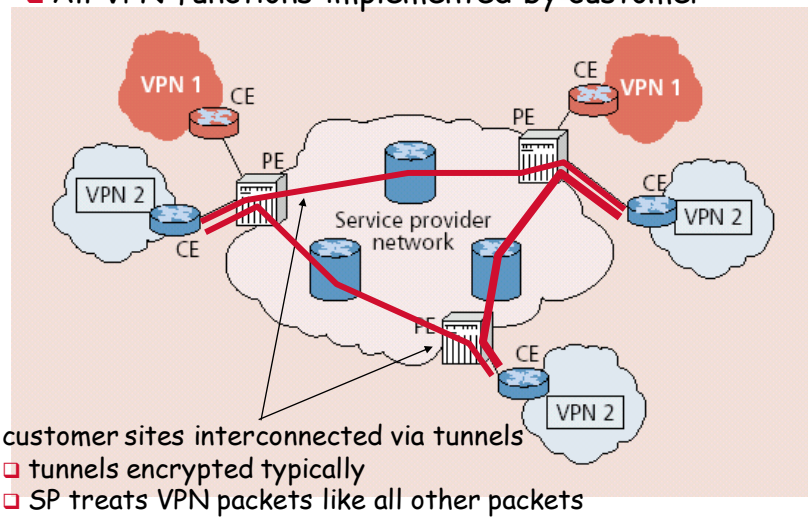
Leased-line VPN



22

Customer premise VPN

- All VPN functions implemented by customer

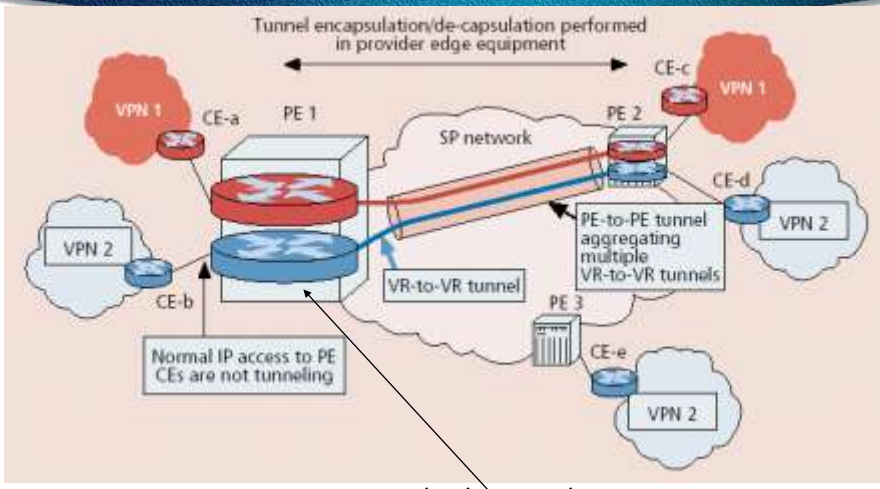


customer sites interconnected via tunnels

- tunnels encrypted typically
- SP treats VPN packets like all other packets

23

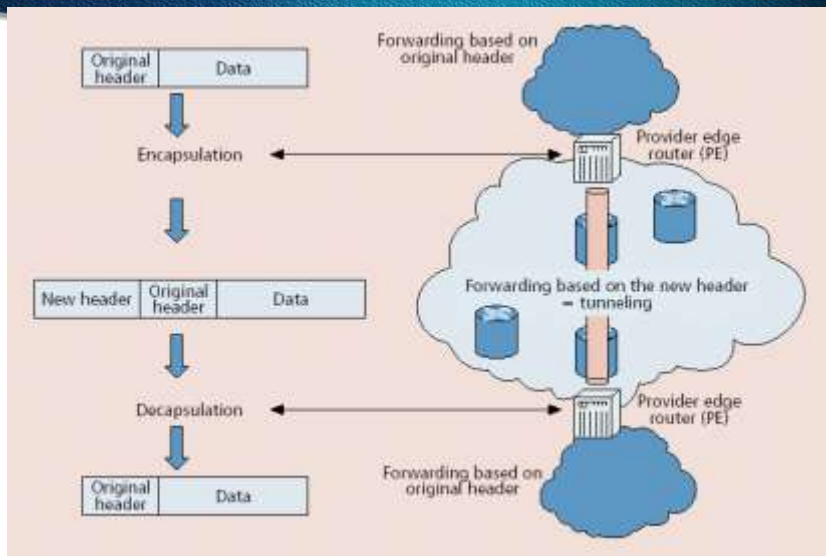
Network-based Layer 3 VPNs



multiple virtual routers
in single provider edge device

24

Tunneling



25

b- Xác thực song phương

Đầu tiên, người dùng sẽ quay số đến điểm truy cập POP của ISP, sau đó ISP sẽ nhận diện người gọi thông qua một số nhận diện chung. Máy chủ truy cập mạng NAS (Network Access Server) sẽ biết được số nhận diện này thuộc mạng khách hàng nào. Kế tiếp, NAS sẽ thiết lập một đường hầm với cổng nối phía khách hàng. Cuối cùng, người dùng được xác thực lần thứ hai bởi cổng nối phía mạng công ty.

27

5. Fire wall - Bức tường lửa

Cisco IPX Fire wall cho phép 64,000 kết nối hoạt động cùng một một lúc, hoạt động dựa trên thuật toán bảo mật tương thích ASA (Adaptive Security Algoritm), thuật toán này bảo mật một cách hiệu quả truy cập đến các máy mạng nội bộ.

Các đặc điểm chính:

- Điều khiển truy cập dựa trên ngữ cảnh CBAC (Context - based access control): cung cấp bảo mật, lọc các ứng dụng cho lưu lượng IP, cung cấp các giao thức mới nhất.

- Java bloking - bảo mật chống lại các Java applet nguy hiểm, chỉ cho phép các applet từ các nguồn đáng tin cậy.

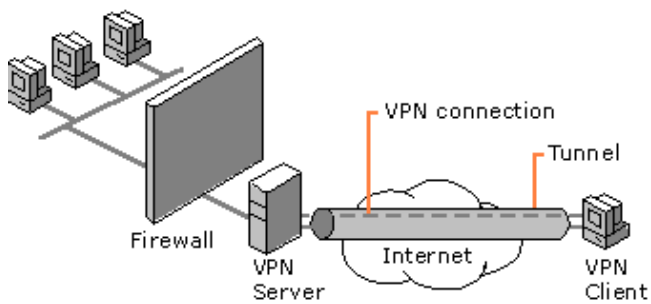
- Phát hiện và ngăn ngừa từ chối dịch vụ (Denial - of - service detection and prevention) để bảo mật các tài nguyên bộ định tuyến chống lại các tấn công thông thường.

- Cảnh báo thời gian thực (real-time alert) cảnh báo trong trường hợp của các tấn công từ chối dịch vụ và các tình trạng đacự biệt khác.

- Theo dõi, kiểm tra (Audit trail): dò tìm người truy cập bằng thời gian, địa chỉ nguồn và đích, cổng, tổng số byte được chuyển đi.

29

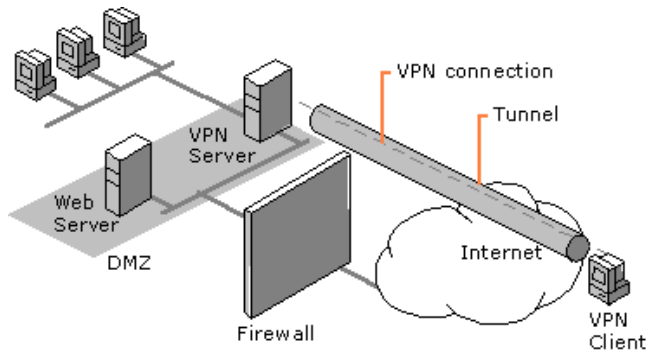
a- Mô hình bức tường lửa (1)



VPN Server nằm phía trước Firewall

30

b- Mô hình bức tường lửa (2)



VPN Server nằm phía sau Firewall

31

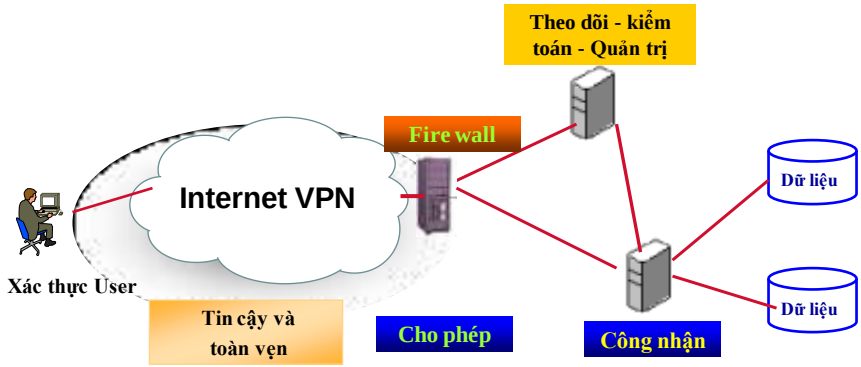
6. Kỹ thuật mã hoá và xác thực

- **Một khung bảo mật cho một tổ chức, cơ quan bao gồm 7 thành phần khác nhau:**
  - **Xác thực (Authentication)**
  - **Toàn vẹn (Integrity)**
  - **Công nhận (Nonrepudiation)**
  - **Theo dõi kiểm toán (Audit trail)**
  - **Tin cậy (Confidentiality)**
  - **Cho phép (Authorization)**
  - **Quản trị (Administration)**

- **Cụng dụng của hệ thống mó hoỏ và xác thực trong VPN**
  - ***Bảo mật dữ liệu khi truyền***
  - ***Hai bờn cựng giữ bớ mật về việc liờn lạc (nhận thực)***
  - ***Toàn vẹn thụng tin***
- **Cụng nghệ mật mó phổ biến được dựng trong VPN bao gồm DES, Triple DES, RC2, RC4, RSA.**

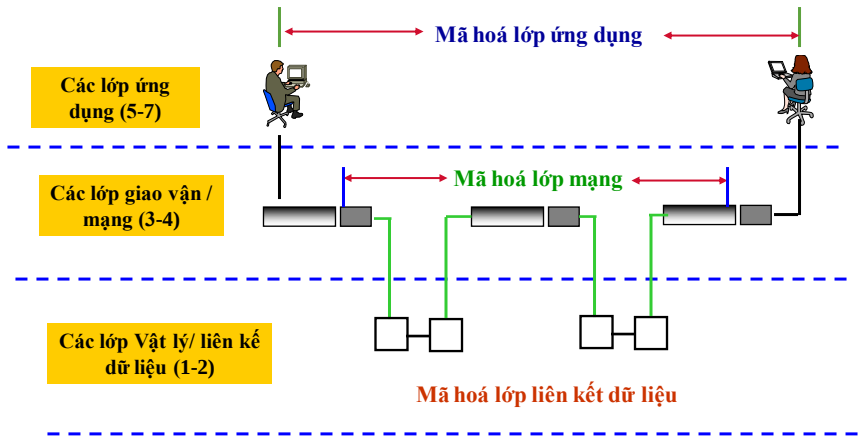
32

a- Mô hình xác thực



33

b- Mô hình mã hoá



34

7. Các nguy cơ an ninh mạng

Việc truyền dữ liệu trên các mạng IP có thể chịu nhiều mối nguy hiểm , trong đó có một loại thông dụng: đánh lừa (spoofing), ăn cắp phiên (session hijacking), nghe trộm (sniffing) và tấn công chính diện (the man-in the-middle-attack)

✠ **Đánh lừa**

Tấn công kiểu đánh lừa là một kẻ tấn công có thể sử dụng địa chỉ IP của một ai đó trong mạng và giả vờ trả lời người khác. Sau khi kẻ tấn công xác định hai trạm A và B đang truyền thông với nhau keo kiểu client / server, sẽ cố gắng giả làm một trong hai trạm đó (A chẳng hạn) bằng cách nào đó để trạm còn lại (trạm B) vẫn tin rằng mình đang kết nối với B.

Kẻ tấn công thực hiện điều này bằng cách tạo ra một bản tin giả với địa chỉ nguồn là địa chỉ của A, yêu cầu kết nối đến B. Khi B nhận được bản tin này, nó sẽ xác thực (Acknowlegment) kèm theo số tuần tự cho việc truyền dữ liệu với A. Những số tuần tự từ máy chủ A là duy nhất đối với kết nối giữa hai máy.

35

Để hoàn tất một phiên làm việc giữa A và B, B sẽ mong chờ A xác thực con số tuần tự của B trước khi tiến hành bất cứ một sự trao đổi thông tin nào, để người tấn công đóng vai bên A, anh ta phải đoán số

số tuần tự mà B sẽ sử dụng và phải ngăn chặn bên A trả lời. Tuy nhiên, không quá khó để xác định số tuần tự.

Để giữa cho máy A không đáp ứng được bất kỳ việc truyền dữ liệu nào của B, người tấn công thường xuyên truyền một số lượng lớn các gói đến A, làm cho A bị quá tải.

Kiểu tấn công đánh lừa tương đối dễ bảo mật, bằng cách cấu hình các bộ định tuyến để loại bỏ các gói tin quay về nào mà bắt phải hình thành từ một máy tính trong mạng nội bộ.

✠ **Ăn cắp phiên**

Kẻ tấn công cố gắng tiếp quản một kết nối sẵn có giữa hai máy tính trong mạng.

Đầu tiên, kẻ tấn công điều khiển thiết bị mạng trên mạng LAN, có thể là bức tường lửa hay một máy tính khác, do đó có thể giám sát kết nối giữa hai máy tính, kẻ tấn công có thể xác định được số tuần tự được sử dụng bởi hai bên.

36

Sau khi giám sát được kết nối, kẻ tấn công có thể tạo ra một lưu lượng, lưu lượng này xuất hiện để đến từ một trong các bên truyền thông, chiếm láy phiên làm việc từ một trong các cá nhân tham gia.

Kẻ tấn công sẽ làm cho một trong các máy tính truyền thông quá tải bởi việc xử lý các gói tin.

Để tránh việc ăn cắp phiên chỉ cần có một xác nhận thành viên trong một phiên làm việc mà biện pháp an toàn nhất là mã hoá.

✠ Nghe trộm

Bản chất của việc nghe lén trên mạng tạo ra một số Card giao tiếp giả theo chuẩn Ethernet để có thể nhận được một số gói tin kiểu Broadcast. Kẻ tấn công có thể dùng một loại phần mềm gọi là đánh hơi (sniffer) có thể ghi lại các lưu lượng mạng chuyển qua chúng, đó là một phần cần thiết để chẩn đoán mạng nào làm việc với mạng Ethernet, cho phép xác định một cách nhanh chóng điều gì đang diễn ra trên một đoạn mạng bất kỳ. Các sản phẩm Sniffer cũng là một công cụ ghi lại những gói đăng nhập vào mạng và sau đó sử dụng những thông tin này để xâm nhập vào một mạng mà anh ta không có quyền truy cập.

Giám sát vật lý là cách tốt nhất để giảm nguy cơ nghe trộm.

37

Tấn công trực diện

Rõ ràng là việc sử dụng những kỹ thuật mã hoá để bảo mật và xác thực dữ liệu là giải pháp hữu hiệu cho các nguy cơ bảo mật

trên, nhưng mã hoá cũng có những nguy cơ tiềm ẩn như là việc quản lý một các cẩn thẩn hệ thống khoá. Kẻ tấn công có thể dùng nhiều biện pháp để thu được các thông tin về việc trao đổi khoá giữa các thành viên trong mạng. Kiểu tấn công đó gọi là tấn công trực diện.

38

8. Kỹ thuật xác thực

Xác thực là một phần không thể thiếu của kiến trúc bảo mật trên VPN.

Xác thực dựa trên ba thuộc tính: cái gì ta có (một khoá hay một card token), cái gì chúng ta biết (mật khẩu) và cái gì để nhận diện (giọng nói, quét võng mặc, dấu vân tay,…. ….)

✠ Mật khẩu truyền thống

Các loại xác thực đơn như ID, mật khẩu được duy trì trong một khoảng thời gian nhất định không đủ mạnh để bảo mật truy cập trên mạng ngay cả khi người dùng luôn cảnh giác.

Vì vậy giải pháp mật khẩu một lần hữu hiệu hơn.

✠ Mật khẩu một lần OTP (One Time Password)

Hệ thống mật khẩu một lần trong đó loại S/Key là loại xác thực điển hình. Hệ thống S/Key tạo ra một cách tự động danh sách mật khẩu cho mỗi phiên làm việc của người dùng.

Nhược điểm của phương pháp này là khó quản trị danh sách mật khẩu cho một số lượng lớn người dùng.

39

✠ Các giao thức xác thực

Giao thức xác thực mật khẩu PAP (Password Authentication Protocol)

Giao thức PAP được thiết kế một cách đơn giản cho một máy tính tự xác thực đến một máy tính khác khi giao thức điểm - điểm được sử dụng làm giao thức truyền thông.PAP là giao thức bắt tay hai chiều máy tính chủ tạo kết nối gửi một nhận dạng người dùng và mật khẩu kép đến hệ thống đích mà nó cố gắng thiết lập kết nối và sau đó hệ thống đích xác thực rằng máy tính đó được xác thực đúng và chấp nhận cho việc truyền thông.

PAP không bảo mật bởi vì thông tin xác thực được truyền đi rõ ràng và không có gì bảo mật chống lại tấn công trở lại hay lặp lại quá nhiều bởi những người tấn công nhằm đoán ra mật khẩu đúng.

Giao thức xác thực yêu cầu bắt tay CHAP (Challenge Handshake Authentication Protocol).

Giao thức CHAP là một giao thức bắt tay ba chiều, xác thực này gồm 3 bước:

1- Bộ xác thực gửi một bản tin thách đố đến máy tính ngang cấp

2- Máy tính ngang cấp tính toán một giá trị sử dụng hàm băm 1 chiều gửi trả lại cho bộ xác thực.

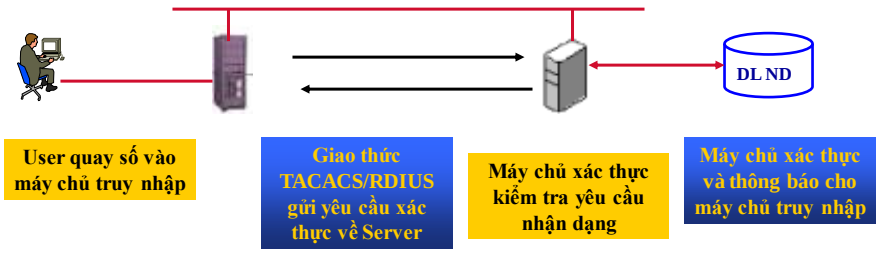
3- Máy tính xác thực có thể đáp ứng chấp nhận nếu tương ứng với giá trị mong muốn.

40

✠ Hệ thống điều khiển truy cập bộ điều khiển truy cập đầu cuối – TACACS

TACACS (Terminal Access Controller Access System) là một trong những

Hệ thống được phát triển để không chỉ cung cấp cơ chế xác thực, mà còn để thêm hai chức năng 2A trong việc bảo mật truy cập từ xa, đó là : cho phép (Authorization) và tính cước (Accouting). Không như những mối quan hệ ngang cấp được thiết kế trong PAP và CHAP,TACACS được thiết kế có chức năng như một hệ thông Client/Server, trong đó mang tính mềm dẻo hơn, đặc biệt trong việc quản lý bảo mật mạng. Trung tâm hoạt động của TACACS và RADIUS là một máy chủ xác thực (authentication server)



41

✠ Các hệ thống phần cứng cơ bản

A- Smart card và PC card

Card thông minh (Smart card) là thiết bị có kích thước giống như thẻ tín dụng bao gồm: 01 bộ vi xử lý và 01 bộ nhớ. Để đọc các thông tin từ Smart card cần 01 đầu đọc. Smart card có thể lưu trữ một khoá riêng của từng người dùng cùng với bất kỳ ứng dụng nào được gài đặt nhằm đơn giản hoá quá trình xác thực, đặc biệt đối với người dùng di động. Hiện nay xuất hiện một số SC gồm một bộ đồng xử lý mã hoá và giải mã, khi đó việc mã và giải mã dễ dàng và nhanh chóng.

Các hệ thống chứng nhận điện tử đơn giản nhất yêu cầu người nhập vào số nhận diện cá nhân PIN để hoàn tất tiến trình xác thực. Trong rất nhiều hệ thống người ta kết hợp giữa PIN của SC và các thông tin về sinh trắc học của người dùng như vân tay. Để dùng hệ thống này người ta trang bị 1 máy quét vân tay, sau đó so sánh với dữ liệu được lưu trên SC.

PC card là một bo mạch nhỏ được cắm vào slot mở rộng trên bo mạch chủ của máy tính. Các PC card kém linh hoạt hơn nhưng có bộ nhớ lớn hơn SC nên có thể lưu trữ lượng tông tin xác thực lớn hơn.

42

B- Các thiết bị thẻ bài (token Devices)

Thẻ bài được xây dựng dựa trên phần cứng riêng biệt dùng để hiển thị các mã nhận dạng (pascode) thay đổi mà người dùng phải nhập vào máy. Bộ xử lý bên trong thẻ bài lưu giữ một tập các khoá mã bí mật được dùng để phát các mã nhận dạng một lần. Các mã này được chuyển đến một máy chủ bảo mật trên mạng, máy chủ này kiểm tra tính hợp lệ và chuyển quyền truy cập cho người dùng.

Trước khi người dùng được xác thực, các thiết bị thẻ yêu cầu một PIN, sau đó sử dụng một trong ba cơ chế sau:

1- Cơ chế đáp ứng thách đố, máy chủ bảo mật phát ra một con số ngẫu nhiên khi người dùng đăng nhập vào mạng. Một con số thách đố xuất hiện trên màn hình, người dùng nhập vào số các số trong thẻ bài. Thẻ bài mã hoá các con số thách đố này với mã khoá bí mật của nó và hiển thị lên màn hình LCD, sau đó người dùng nhập kết quả này vào máy tính. Trong khi đó, máy chủ mã hoá con số thách đố với cùng một khoá và nếu như hai kết quả này phù hợp thì người dùng sẽ được phép vào mạng.

2- Cơ chế đồng bộ thời gian

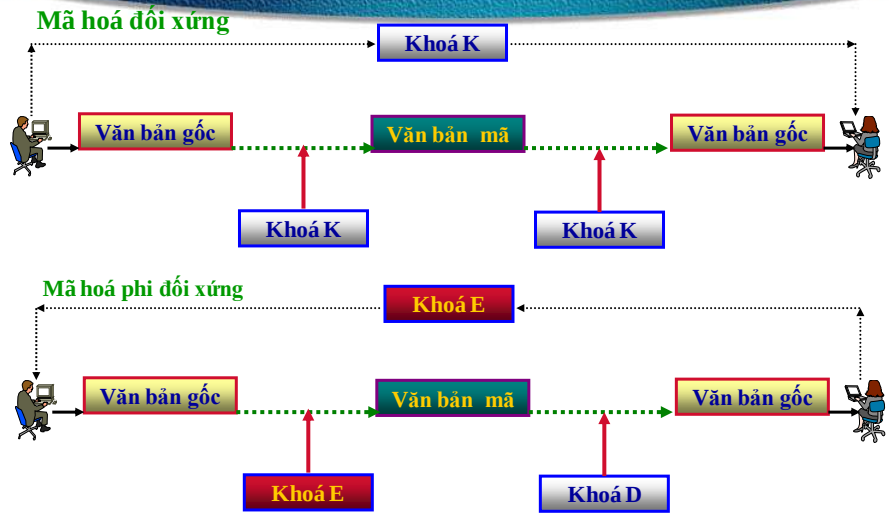
ở đây thẻ bài hiển thị một số được mã hoá với khoá bí mật mà khoá này thay đổi cứ 60 giây. Người dùng được nhắc cho con số khi cố gắng đăng nhập vào máy chủ. Bởi đồng hồ trên máy chủ và thẻ được đồng bộ, cho nên máy chủ có thể xác nhận người dùng bằng cách giải mã con số thẻ và so sánh kết quả.

3- Cơ chế đồng bộ sự kiện. ở đây, một bộ đếm ghi lại số lần vào mạng của người dùng. Sau mỗi lần vào mạng, bộ đếm được cập nhật và một mã nhận dạng khác được tạo ra cho lần đăng nhập kế tiếp.

C- Hệ thống sinh trắc học

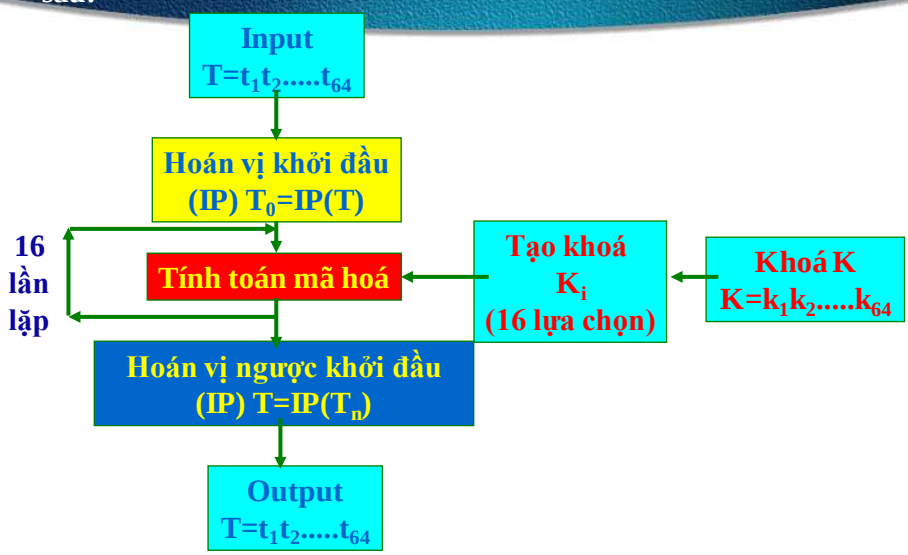
Hệ thống sinh trắc học phụ thuộc vào việc sử dụng một dấu vết cá nhân duy nhất để xác định người dùng. Các dấu vết thường được sử dụng là : vân tay, giọng nói, võng mạc.

9. Kỹ thuật mật mã



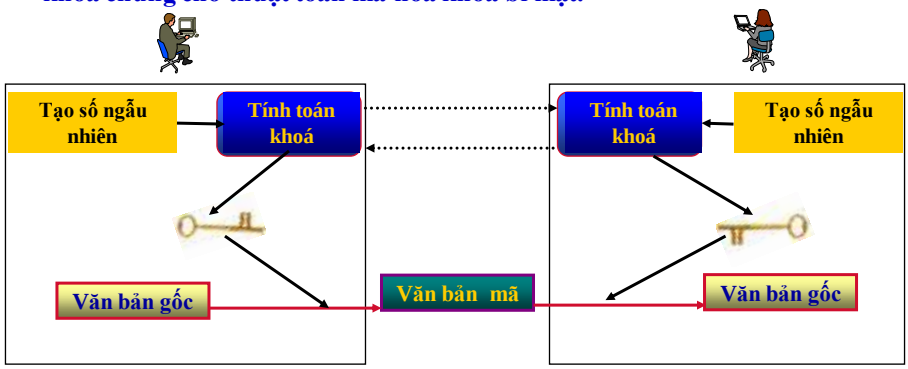
45

Mã hoá đối xứng. Kỹ thuật mã hoá DES trong đó 56 bits dùng làm khoá và 8 bits dùng để kiểm soát lỗi. Sơ đồ thuật toán như sau:



46

Mã hoá phi đối xứng. Kỹ thuật mã hoá Diffie – Hellman (DH), cơ chế làm việc: hai bên trao đổi có thể sử dụng kỹ thuật DH để tạo ra một giá trị bí mật dùng chung mà sau đó có thể được dùng như một khoá chung cho thuật toán mã hoá khoá bí mật.



47

Phương pháp mã hoá công khai RSA (Rivest, Shamir, Adleman).

Năm 1978 Rivest, Shamir và Adleman đã đề xuất phương pháp mã hoá RSA – mã Công khai. Thuật toán RSA dựa trên nhận xét sau: có thể dễ dàng sinh ra 2 số nguyên tố lớn và nhân chúng với nhau, nhưng cực kỳ khó phân tích một hợp số thành 2 số nguyên tố. Thuật giải được mô tả như sau:

1- Chọn 2 số nguyên tố lớn p và q

2- Tính n= pxq và $\Phi(n)=(p-1)(q-1)$

3- Chọn ngẫu nhiên D ($3 < D < \Phi(n)$) sao cho USCLN(D, Φ (n))=1

4- Chọn E sao cho $ED \bmod \Phi(n) = 1$

5- n và E là khoá công khai D là khoá bí mật.

Giả sử văn bản gốc là V ta biểu diễn V dưới dạng các số nguyên dương T gồm các số nằm trong [1,n-1], khi đó văn bản mã được tính như sau: $W = T^E \bmod n$.

Giải mã: $T = W^D \bmod n$.

48

10. Giao thức trong VPN

a- Giao thức IPSEC

Giao thức IPSec được chuẩn hoá vào năm 1995, IPSec định nghĩa 2 loại tiêu đề cho các gói tin IP để điều khiển quá trình xác thực và mã hoá: một là xác thực tiêu đề IP-AH (IP Authentication Header) điều khiển việc xác thực và hai là bọc gói bảo mật tải ESP (Encapsulation Security Payload) cho mục đích mã hoá. Việc hỗ trợ cho IPSec chủ yếu là cho IPv4 còn IPv6 thì có sẵn IPSec.

Đặc điểm cơ bản của IPSec

@ Kết hợp bảo mật SA (Security Association)

@ Xác thực tiêu đề AH (Authentication Header)

@ Bọc gói bảo mật tải ESP (Encapsulation Security Payload)

@ Chế độ làm việc

49

1- Kết hợp bảo mật SA

Để hai bên có thể truyền và nhận dữ liệu đã được bảo mật, cả bên truyền và nhận phải cùng thống nhất sử dụng giải thuật mã hoá và phương pháp quản lý và chuyển khoá. Việc truyền tin có thể đòi hỏi một hoặc nhiều SA vì mỗi gói tin theo giao thức IPSEC được mã hoá cũng yêu cầu phải có SA.

Một IPSec SA mô tả các vấn đề sau:

- **Thuật giải xác thực sử dụng cho AH và khoá của nó**
- **Thuật giải mã hoá ESP và khoá của nó**
- **Dạng thức và kích thước của bộ mã sử dụng trong thuật giải mã hoá**
- **Giao thức, thuật giải mã hoá, khoá sử dụng cho việc truyền thông**
- **Thời gian sống của khoá của SA**
- **Địa chỉ nguồn của SA**

50

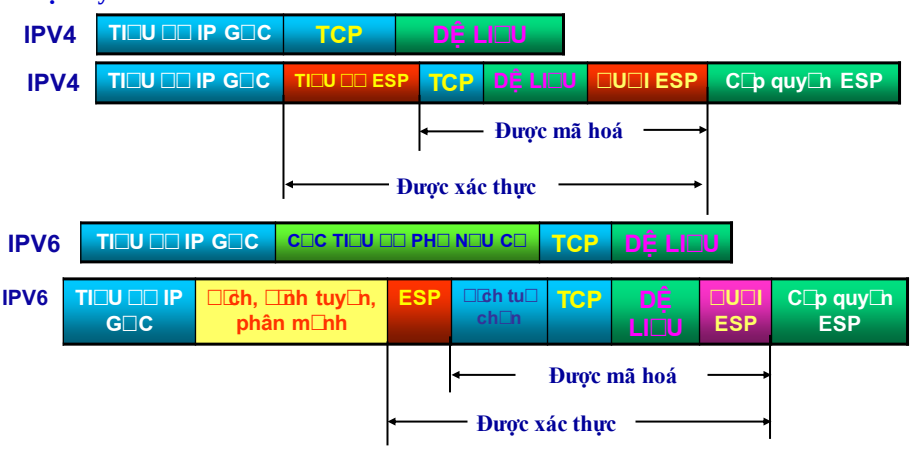
2- Xác thực tiêu đề AH

Xác thực tiêu đề AH trong hệ thống IPSec được chèn vào giữa tiêu đề IP và nội dung, không làm thay đổi nội dung của gói dữ liệu. Xác thực tiêu đều AH gồm 5 trường: trường tiêu đề kế tiếp (Next Header Field), chiều dài tải (Payload Length), chỉ số tham số bảo mật SPI (Security Parameter Index), số tuần tự (Sequence Number), dữ liệu xác thực (Authentication Data).

Cần chú ý AH không giữ được bí mật gói tin mà chỉ làm nhiệm vụ xác thực. Để bảo mật dữ liệu cần sử dụng thành phần thứ 2 là ESP

3- Bọc gói bảo mật tải ESP

Bọc gói bảo mật tải ESP có nhiệm vụ mã hoá dữ liệu, nên nội dung của gói sẽ bị thay đổi.



Gống như tiêu đề AH, ESP gồm các SPI để chỉ cho bên nhận biết cơ chế bảo mật thích hợp cho việc xử lý gói tin. Số tuần tự trong ESP là bộ đếm tăng mỗi khi gói được gửi đến cùng một địa chỉ

4- Chế độ làm việc

Có hai chế độ làm việc trong IPSec:

- **Chế độ giao vận (Transport Mode) Chỉ có đoạn trong lớp giao vận trong gói là được xử lý.**

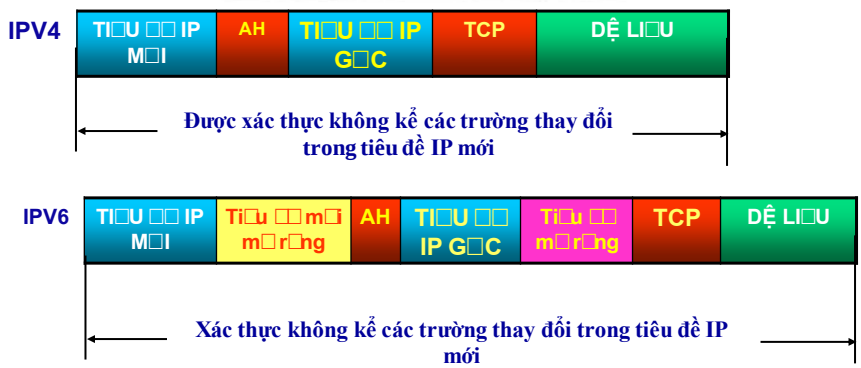
Chế độ giao vận sử dụng cho cả cổng nối và Host, cung cấp cơ chế bảo mật cho các giao thức lớp trên. Trong chế độ giao vận, AH được chèn vào sau tiêu đề IP và trước các giao thức lớp trên (TCP, UDP hay ICMP) hoặc trước bất kỳ tiêu đề IPSec đã được chèn vào trước đó.

- **Chế độ đường hầm (Tunnel Mode); Toàn bộ gói sẽ được xử lý cho mã khoá xác thực**

Trong chế độ đương hầm tiêu đề IP chứa địa chỉ nguồn, địa chỉ đích. AH bảo mật toàn bộ gói IP.

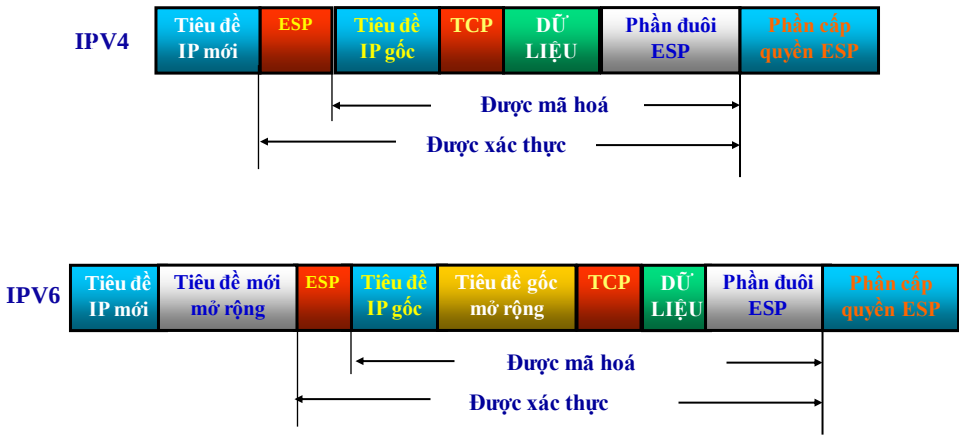
53

Chế độ đường hầm AH chỉ chống lại việc thay đổi nội dung dữ liệu nên cần phải có phương tiện khác để bảo đảm tính riêng tư của dữ liệu.



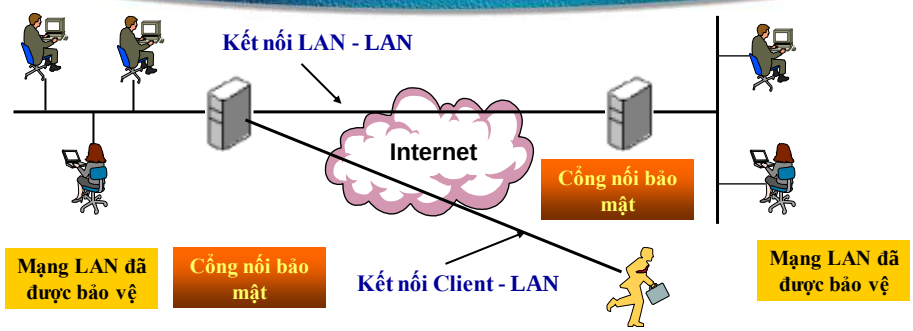
54

Chế độ đường hầm ESP bảo chống lại nghe trộm một cách có hiệu quả, nhưng không bảo mật được toàn bộ lưu lượng.



55

5- Sử dụng IPSec



Muốn tạo một VPN mà tất cả các máy tính có thể liên lạc với nhau thông qua giao thức IPSec thì phải gài đặt phần mềm IPSecs trên tất cả các máy tính và các cổng bảo mật.

56

b- Giao thức PPTP

Giao thức định hướng đường hầm PPTP (Point to Point Tunneling

Protocol) được đưa ra bởi một nhóm các công ty gọi là PPTP forum. ý tưởng cơ bản của giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng lợi ích của các cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa client và mạng riêng. Người dùng từ xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo một đường hầm bảo mật tới mạng riêng của họ.

Đặc điểm cơ bản của PPTP

@ PPTP có thể truyền trong đường hầm bằng nhiều giao thức khác nhau, trong khi IPSec chỉ làm việc với IP;

@ PPTP được thiết kế để hoạt động ở tầng liên kết dữ liệu DataLink. Trong khi IPSec chạy ở tầng Network;

@ Thiết lập và kết thúc kết nối vật lý;

57

1- Dạng thức của PPTP

PPTP dựa trên PP để tạo ra kết nối quay số giữa khách hàng và máy chủ

truy cập mạng. Sau khi PPP thiết lập kết nối, PPTP sử dụng các quy luật đóng gói của PPP để đóng gói các gói dữ liệu truyền trong đường hầm.

Để tận dụng ưu điểm của kết nối tạo ra bởi PPP, PPTP định nghĩa 2 loại gói: gói điều khiển và gói dữ liệu, gán chúng vào 2 kênh riêng. Sau đó PPTP phân tách các kênh điều khiển và kênh dữ liệu thành luồng điều khiển với giao thức TCP và luồng dữ liệu với giao thức IP. Kết nối TCP được tạo giữa client PPTP và máy chủ PPTP được sử dụng để chuyển thông báo điều khiển. Các gói điều khiển được gửi đi theo chu kỳ để lấy thông tin về trạng thái kết nối và quản lý báo hiệu giữa client PTP và máy chủ mạng, Các gói điều khiển cũng được dùng để gửi thông tin quản lý thiết bị, thông tin cấu hình giữa hai đầu của đường hầm.

Kênh điều khiển được yêu cầu cho việc thiết lập một đường hầm giữa client PTP và máy chủ PPTP. Phần mềm client có thể nằm người dùng thừ xa hay nằm ở tại máy chủ ISP.

58

Sau khi đường hầm được thiết lập dữ liệu của người dùng được truyền từ client đến máy chủ PPTP. Các gọi PPTP chứa các gói dữ liệu IP. Gói dữ liệu IP được đóng gói bởi tiêu đề GRE, sử dụng số ID của host điều khiển truy nhập. ACK giám sát tốc độ truyền DL trong đường hầm.

Bởi vì PPTP hoạt động ở tầng liên kết dữ liệu, nên cần phải có tiêu đề môi trường truyền trong gói để cho biết dữ liệu được truyền trong đường hầm theo phương thức nào. Tuỳ theo kiến trúc hạ tầng của các nhà ISP mà các phương thức này có thể là: Ethernet, Frame Relay hay kết nối PPP.

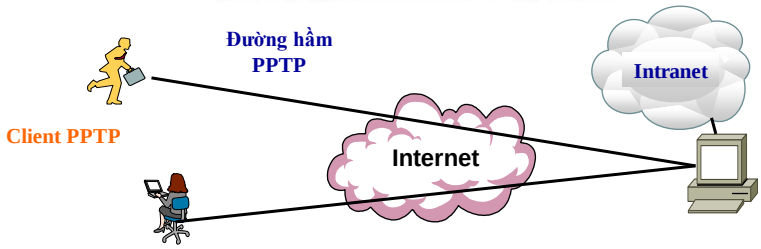
2- Đường hầm

PPTP cho phép người dùng và các ISP có thể tạo ra nhiều loại đường hầm khác nhau. Người dùng có thể chỉ định điểm kết thúc của đường hầm ngay tại máy của mình nếu như có cài các client PTP, hay tại máy chủ ISP nếu như máy tính của họ chỉ có PPP mà không có PPTP. Các đường hầm có thể chia làm hai loại tự nguyện và bắt buộc.

Đường hầm tự nguyện được tạo ra theo yêu cầu của người dùng cho mục đích xác định. Khi sử dụng đường hầm tự nguyện, người dùng có thể đồng thời mở một đường hầm bảo mật thông qua Internet bằng giao thức TCP/IP bình thường.

59

Đường hầm tự nguyện thường được sử dụng để cung cấp tính riêng tư và toàn vẹn dữ liệu cho lưu lượng Intranet thông qua Internet.



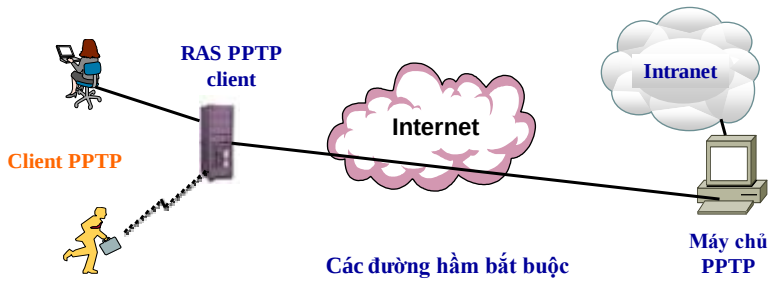
Các đường hầm tự nguyện

đường hầm bắt buộc tạo ra không thông qua người dùng nên nó trong suốt đối người dùng đầu cuối. Điểm kết thúc của đường hầm bắt buộc nằm ở máy chủ truy cập từ xa. Tất cả dữ liệu truyền đi từ người dùng qua đường hầm PPTP thông qua RAS. Bởi vì đường hầm bắt buộc định trước điểm kết thúc và người dùng không thể truy cập phần còn lại của Internet nên nó điều khiển truy cập tốt hơn hơn đường hầm tự nguyện. Điều đó có nghĩa là không

60

Người dùng truy cập Internet trong khi truy cập VPN, mặt khác vẫn cho truy cập từ Internet vào VPN. Đường hầm bắt buộc có thể cùng một lúc thiết lập được nhiều kết nối.

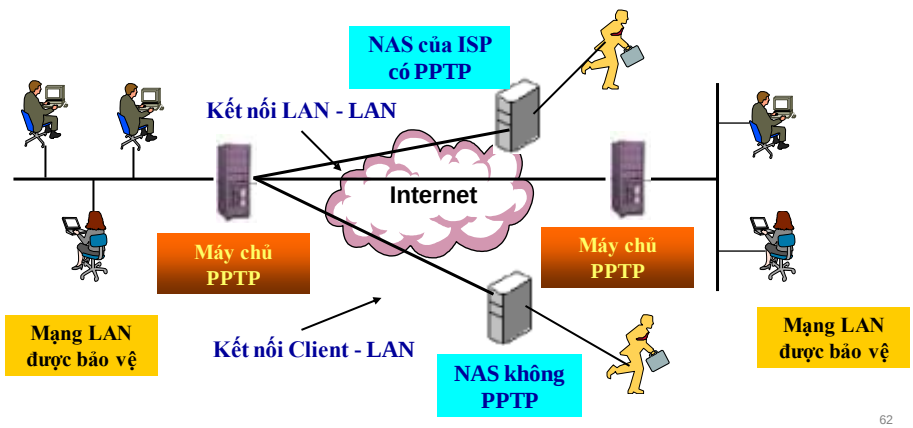
Một đường hầm bắt buộc tĩnh được cấu hình bởi thiết bị hay bằng tay. Cấu hình bằng thiết bị yêu cầu người dùng gọi một số điện thoại đặc biệt để tạo kết nối. Cấu hình bằng tay, RAS sẽ kiểm tra một phần tên người dùng gọi là Realm để quyết định nơi nào sẽ liên lạc với người dùng đó. Đường hầm Realm cơ bản cho phép người dùng liên kết với một Realm cho trước và được đối xử như nhau.



61

3- Sử dụng PPTP

Đặc điểm chủ yếu nhất của giao thức PPTP là cung cấp phương thức quay số truy cập bảo mật vào VPN và định nghĩa điểm kết thúc của đường hầm, một trong các điểm kết thúc này có thể nằm ở thiết bị của nhà cung cấp dịch vụ Internet nên để cấu hình được phải có sự hợp tác giữa ISP và người quản lý mạng trong việc xác thực người dùng.



62

c- Giao thức L2TP

Giao thức định hướng đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol) là sự kết hợp giữa 2 giao PPTP và L2F (Layer 2 Forwarding) do vậy L2TP kế thừa các đặc tính của cả PPTP và L2F.

Đặc điểm cơ bản của L2TP

@ L2TP được thiết kế để hoạt động ở tầng liên kết dữ liệu DataLink.

@ L2TP có thể truyền trong đường hầm bằng nhiều giao thức khác nhau.

@ Microsoft có kế hoạch hỗ trợ L2TP trong Window NT và Window 98.

1- Dạng thức của L2TP

L2TP dựa trên PPP để tạo kết nối quay số giữa và máy chủ truy cập NAS.

L2TP sử dụng PPP để tạo kết nối vật lý, tiến hành giai đoạn xác thực đầu, tạo gói dữ liệu PPP và đóng kết nối khi hết phiên làm việc.

63

Sau khi PPP tạo kết nối xong, L2TP sẽ xác định NAS tại site chính có chấp nhận người dùng và sẵn sàng đóng vai trò là điểm kết thúc đường hầm cho người dùng đó. Sau khi đường hầm được tạo, L2TP sẽ đóng các gói PPP rồi truyền lên môi trường mà ISP đã gán cho đường hầm đó. L2TP tạo đường hầm giữa NAS của ISP và máy chủ mạng của Client, nó có thể gán nhiều phiên làm việc cho đường hầm. L2TP tạo ra các số nhận dạng cuộc gọi Call ID cho mỗi phiên làm việc và chèn Call ID vào tiêu đề L2TP của mỗi gói để chỉ ra nó thuộc phiên làm việc nào.

L2TP cũng có thể tạo ra nhiều đường hầm giữa NAS của ISP và máy chủ mạng client. Bằng việc chọn gán một phiên làm việc của người dùng cho một đường hầm thay vì ghép nhiều phiên làm việc vào một đường hầm, cho phép gán các người dùng khác nhau vào các môi trường đường hầm tuỳ theo chất lượng dịch vụ của họ.

L2TP cũng định nghĩa 2 loại thông báo: thông báo điều khiển và thông báo dữ liệu. Thông báo điều khiển dùng để cho việc thiết lập, quản lý và giải phóng phiên làm việc trên đường hầm.

Thông báo dữ liệu bao gồm tiêu đề môi trường để chỉ ra đường hầm làm việc ở môi trường nào.

64