Đề tài nghiên cứu Công nghệ VPN

Biên tập bởi:

Khoa CNTT ĐHSP KT Hưng Yên

Đề tài nghiên cứu Công nghệ VPN

Biên tập bởi:

Khoa CNTT ĐHSP KT Hưng Yên

Các tác giả:

Khoa CNTT ĐHSP KT Hưng Yên

Phiên bản trực tuyến:
http://voer.edu.vn/c/8f2b2b24

MỤC LỤC

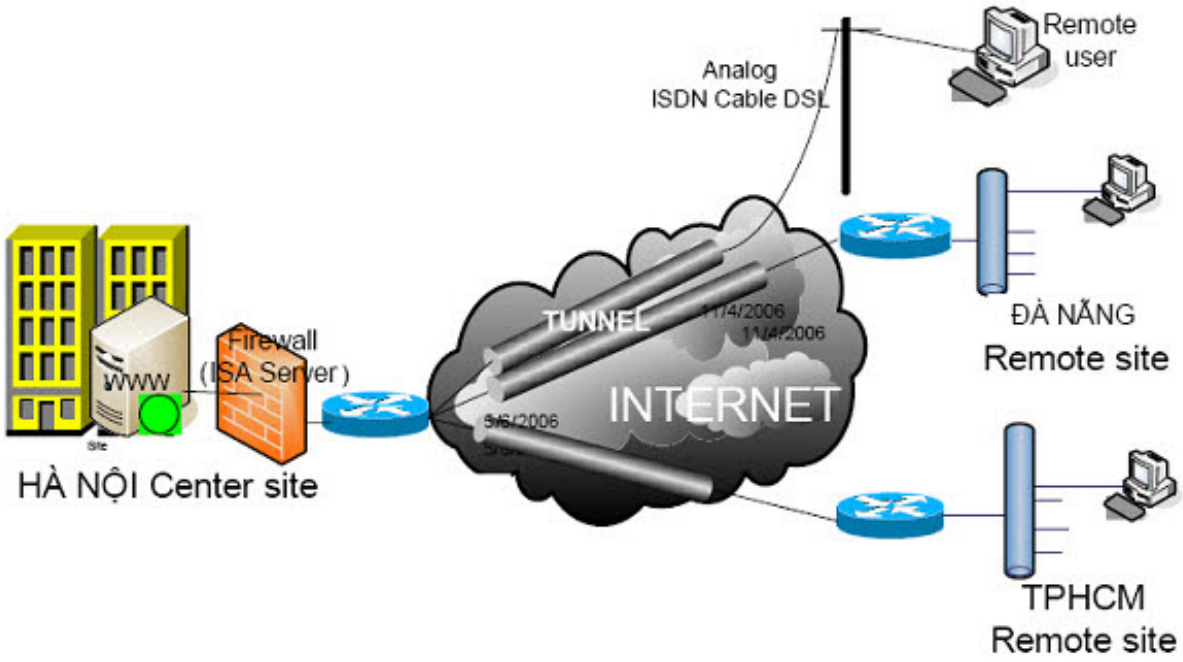
Bài 1: Giới thiệu về Công nghệ VPN

Giới thiệu về Công nghệ VPN

VPN là gì

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 đinh 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.

.



. .

VPN=Đường hầm + Mã hoá

Lợi ích của VPN đem lại

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.

Bài 2: Các loại VPN

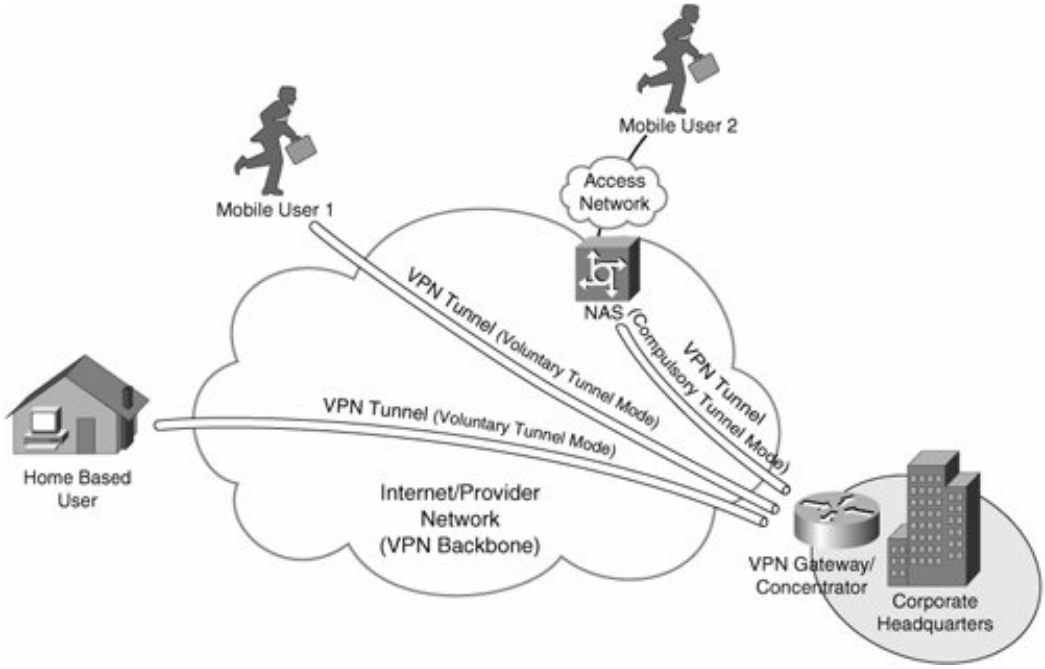
Các loại VPN

VPN được chia thành 02 loại:

- VPN Remote Accesss
- VPN Site to Site

VPN Intranet

VPN Extranet



VPN Remote Access

VPN Remote Access

VPN Remote Access—Cung cấp kết nối truy cập từ xa đến một mạng Intranet hoặc Extranet dựa trên hạ tầng được chia sẻ. VPN Remote Access sử dụng đường truyền Analog, Dial, ISDN, DSL, Mobile IP và Cable để thiết lập kết nối đến các Mobile user.

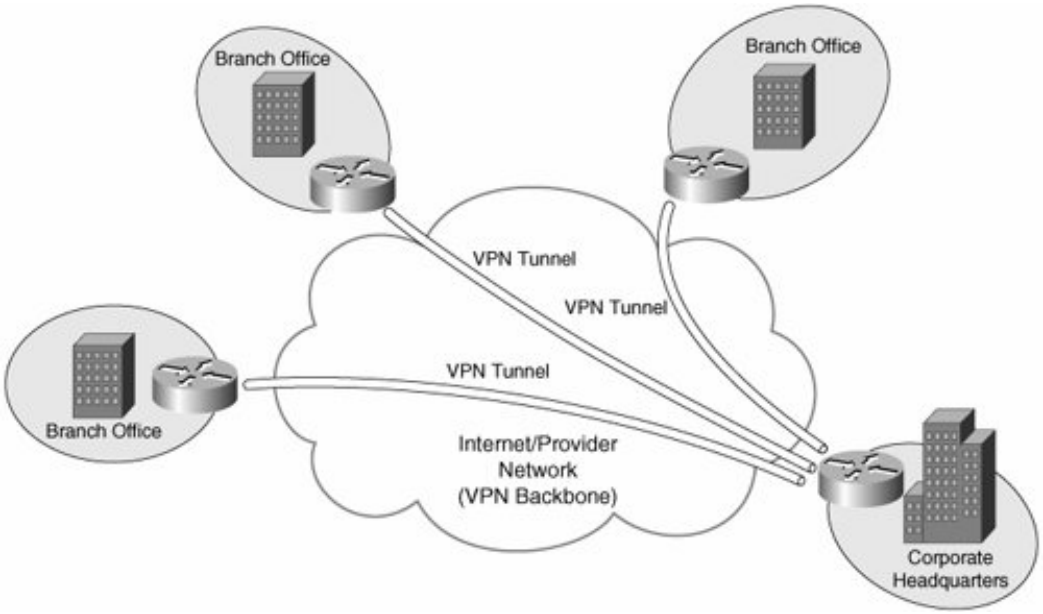
Một đặc điểm quan trọng của VPN Remote Access là: Cho phép người dùng di động truy cập từ xa vào hệ thống mạng nội bộ trong công ty để làm việc.

Để thực hiện được VPN Remote Access cần:

Có 01 VPN Getway(có 01 IP Public).

Đây là điểm tập trung xử lý khi VPN Client quay số truy cập vào hệ thống VPN nội bộ.

Các VPN Client kết nối vào mạng Internet



VPN Site to Site

VPN Site - to - Site

VPN Site - to - Site được chia làm hai loại nhỏ là VPN Intranet và VPN Extranet

Intranet VPN

—Kết nối văn phòng trung tâm, các chi nhánh và văn phòng ở xa vào mạng nội bộ của công ty dựa trên hạ tầng mạng được chia sẻ. Intranet VPN khác với Extranet VPN ở chỗ nó chỉ cho phép các nhân viên nội bộ trong công ty truy cập vào hệ thống mạng nội bộ của công ty.

Extranet VPN

—Kết nối bộ phận khách hàng của công ty, bộ phận tư vấn, hoặc các đối tác của công ty thành một hệ thống mạng dựa trên hạ tầng được chia sẻ. Extranet VPN khác với Intranet VPN ở chỗ cho phép các user ngoài công ty truy cập vào hệ thống.

Để thực hiện được VPN Site - to Site cần:

Có 02 VPN Getway(Mỗi VPN Getway có 01 IP Public). Đây là điểm tập trung xử lý khi VPN Getway phía bên kia quay số truy cập vào.

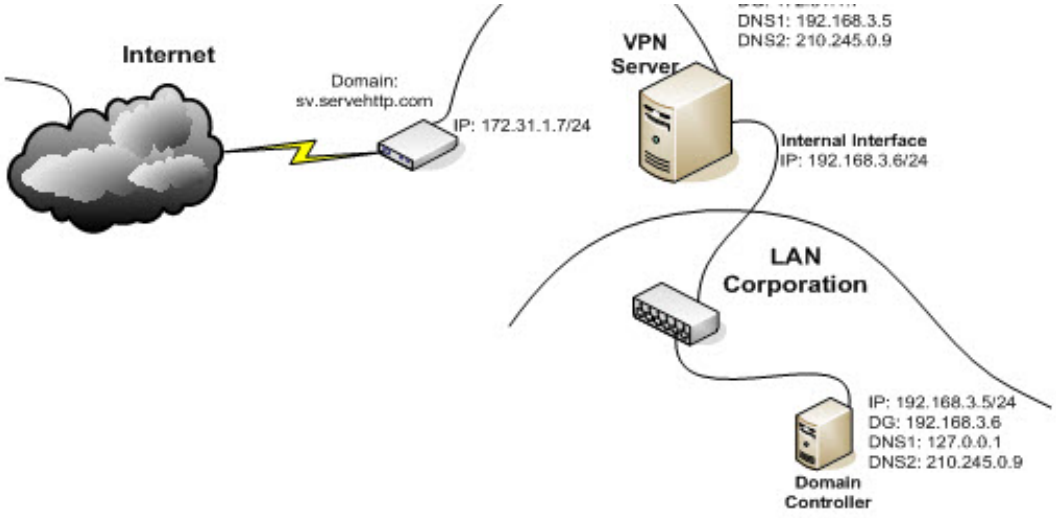
Các Client kết nối vào hệ thống mạng nội bộ

Mô hình áp dụng tại trường ĐH SPKT Hưng Yên.

Theo phân tích và qua khảo sát thực tế, hiện nay các thầy, cô đi công tác tại các cơ sở, chi nhánh liên kết ngoài trường đều có máy tính và mong muốn kết nối vào hệ thống mạng nội bộ trong trường để làm việc.

Tại thời điểm thực hiện đồ án này, trường ta chỉ có một cơ sở tại Huyện Khoái Châu, Tỉnh Hưng yên. Do vậy việc thiết lập mô hình hệ thống VPN Remote Access là phù hợp.

Khi trường ta có thêm các cơ sở tại Hải Dương và Phố Nối, chúng ta có thể chuyển sang mô hình Site - to - Site để kết nối 03 cơ sở này vào thành một hệ thống LAN nội bộ.



Mô hình VPN Remote Access áp dụng thử nghiệm tại Khoa CNTT Trường ĐH SPKT Hưng Yên

Điều kiện thiết bị cần có khi thực hiện VPN

Qua thử nghiệm cho thấy, một mạng VPN hoạt động tốt khi đáp ứng được các yêu cầu:

Hoạt động ổn định và liên tục

Tốc độ truy cập tốt

Đáp ứng được số kết nối đồng thời

Trong mô hình thử nghiệm của chúng ta ở trên, các thiết bị cần có là mức tối thiểu cho việc thử nghiệm một mạng VPN Remote Access gồm:

01 Đường ADSL

01 Modem ADSL

01 Máy chủ Server cài phần mềm ISA Server(Đóng vai trò là VPN Server)

Qua thử nghiệm cho thấy, với số lượng VPN Client ít, từ 5-10 kết nối đồng thời thì

mạng VPN hoạt động bình thường, nhưng khi số kết nối tăng nên nhiều hơn và dung lượng download, upload cao thì hay xảy ra hiện tượng Disconect. Vấn đề này hoàn toàn là do dung lượng đường truyền và khả năng xử lý của thiết bị

Để có thể thiết lập mạng VPN làm việc chuyên nghiệp tại trường ĐH SPKT Hưng Yên chúng ta cần các thiết bị chuyên dụng, có độ tin cậy cao như:

Cisco PIX 500 Series

Đây là dòng thiết bị an ninh chuyên dụng hàng đầu của Cisco cho phép nhiều kết nối VPN đồng thời tuỳ thuộc vào loại thiết bị như

PIX 515E cho phép 500 kết nối đồng thời dành cho các doanh nghiệp nhỏ và trung bình có giá tham khảo là $3700.

PIX 535E cho phép 10000 kết nối VPN đồng thời dành cho các tập đoàn lớn có giá tham khảo là $10,000

Đồng thời đường truyền cũng là một vấn đề rất quan trọng. Nếu đường truyền vào VPN Getway có dung lượng truyền cao và ổn định là một yếu tố đảm bảo hệ thống mạng hoạt động ổn định.

Bài 3: Các công nghệ và giao thức hỗ trợ VPN

Các công nghệ và giao thức hỗ trợ VPN

Đường hầm và mã hoá

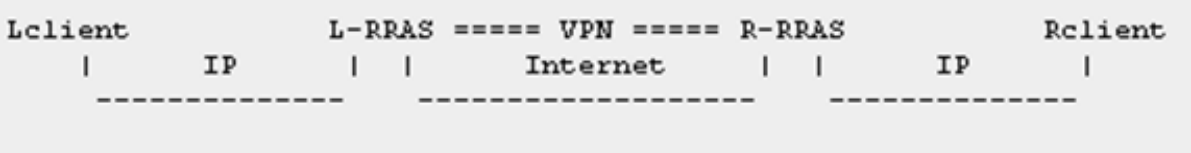
Chức năng chính của một mạng VPN là truyền thông tin đã được mã hoá trong một đường hầm dựa trên hạ tầng mạng được chia sẻ

Đường hầm

Đường hầm là một khái niệm quan trọng của mạng VPN, nó cho phép các công ty có thể tạo ra các mạng ảo dựa trên hệ thống mạng công cộng. Mạng ảo này không cho phép những người không có quyền truy cập vào. Đường hầm cung cấp một kết nối logic điểm đến điểm trên hệ thống mạng Internet hay trên các mạng công cộng khác. Để dữ liệu được truyền an toàn trên mạng, một giải pháp được đưa ra là mã hoá dữ liệu trước khi truyền. Dữ liệu truyền trong đường hầm chỉ có thể được đọc bởi người nhận và người gửi. Đường hầm tạo cho VPN có tính chất riêng tư trên mạng.

Để mô tả chi tiết nguyên lý khi gói tin truyền qua đường hầm ta nghiên cứu một loại đường hầm điển hình là GRE. Đây cũng là giao thức tạo đường hầm được sử dụng trong PPTP là giao thức tạo kết nối VPN Peer to Peer và Remote Access rất phổ biến của Microsoft.

Microsoft sử dụng dịch vụ RRA(Routing and Remote Access) để định tuyến giữa các LAN như hình sau:



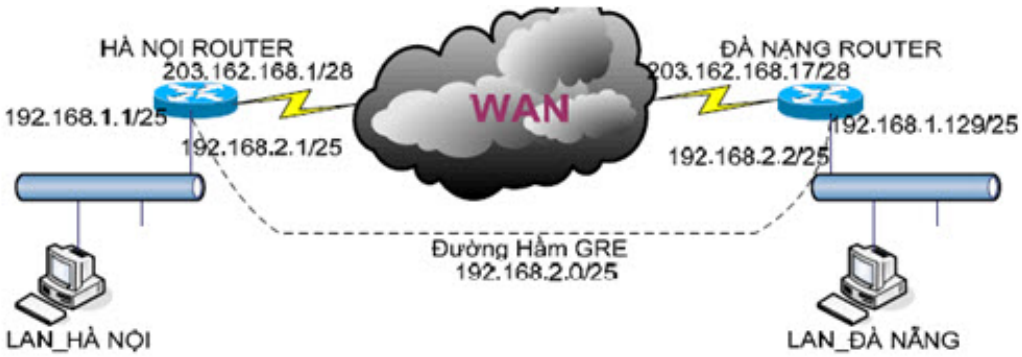
Định dạng gói tin GRE, đây cũng là giao thức Microsoft dùng để đóng gói dữ liệu như sau:

```
+-----------------------------------+
| Data Link (D/L) Header            |
+-----------------------------------+
| IP Header                         |
+-----------------------------------+
| GRE Header                        |
+-----------------------------------+
| PPP Header                        |
+-----------------------------------+
| Encrypted PPP Payload             |
+-----------------------------------+
| Data Link Trailer                 |
+-----------------------------------+
```

Dữ liệu từ Client đưa đến VPN Getway được đóng gói bởi giao thức PPP(Point - to - Point Protocol) với một PPP Header. Sau đó gói tin được đóng gói bởi GRE với một GRE Header và được truyền trong đường hầm. Tại đầu bên kia của đường hầm, gói tin được giải phóng khỏi GRE Header và PPP Header sau đó được vận chuyển đến đích. Các Header của mỗi gói tin được thể hiện trong hình sau:

```
Lclient            L-RRAS ===== VPN ===== R-RRAS            Rclient
    |      IP       |  |      Internet      |  |      IP       |
     ---------------    --------------------    ---------------
    D/L header             D/L header             D/L header
    IP header              IP header              IP header
    Payload                GRE header             Payload
                           PPP stub
                           Payload (encrypted)
```

Một ví dụ về đường hầm GRE sau khi được thiết lập trong mô hình Site - to



Mã hoá

Mã hoá là một đặc điểm cơ bản trong việc xây dựng và thiết kế mạng VPN. Mạng VPN sử dụng hạ tầng của hệ thống Internet và các mạng công cộng khác. Do vậy dữ liệu truyền trên mạng có thể bị bắt giữ và xem thông tin. Để đảm bảo thông tin chỉ được đọc bởi người nhận và người gửi thì dữ liệu phải được mã hoá với các thuật toán phức tạp.

Tuy nhiên chỉ nên mã hoá các thông tin quan trọng vì quá trình mã hoá và giản mã sẽ ảnh hưởng đến tốc độ truyền tải thông tin.

Các nhà cung cấp dịch vụ VPN chia VPN thành 3 tập hợp đó là VPN lớp 1, 2 và 3.

VPN lớp 1 được sử dụng để vận chuyển các dịch vụ lớp 1 trên hạ tầng mạng được chia sẻ, được điều khiển và quản lý bởi Generalized Multiprotocol Label Switching (GMPLS).

Hiện nay, việc phát triển VPN lớp 1 còn đang trong giai đoạn thử nghiệm nên VPN Layer 1 không được đề cập đến trong tài liệu này.

Hiểu đơn giản nhất, một kết nối VPN giữa hai điểm trên mạng công cộng là hình thức thiết lập một kết nối logic. Kết nối logic có thể được thiết lập trên lớp 2 hoặc lớp 3 của mô hình OSI và công nghệ VPN có thể được phân loại rộng rãi theo tiêu chuẩn này như là VPN lớp 2 và VPN lớp 3(Layer 2 VPNs or Layer 3 VPNs).

Công nghệ VPN lớp 2

Công nghệ VPN lớp 2 thực thi tại lớp 2 của mô hình tham chiếu OSI; Các kết nối point-to-point được thiết lập giữa các site dựa trên một mạch ảo(virtual circuit). Một mạch ảo là một kết nối logic giữa 2 điểm trên một mạng và có thể mở rộng thành nhiều điểm. Một mạch ảo kết nối giữa 2 điểm đầu cuối(end-to-end) thường được gọi là một mạch vĩnh cửu(Permanent Virtual Circuit-PVC). Một mạch ảo kết nối động 2 điểm trên mạng(point to point) còn được biết đến như mạng chuyển mạch(Switched Virtual Circuit - SVC). SVC ít được sử dụng hơn vì độ phức tạp trong quá trình triển khai cũng như khắc phục hệ thống lỗi. ATM và Frame Relay là 02 công nghê VPN lớp 2 phổ biến.

Các nhà cung cấp hệ thống mạng ATM và Frame Relay có thể cung cấp các kết nối site - to - site cho các tập đoàn, công ty bằng cách cấu hình các mạch ảo vĩnh cửu(PVC) thông qua hệ thống cáp Backbone được chia sẻ.

Một sự tiện lợi của VPN lớp 2 là độc lập với các luồng dữ liệu lớp 3. Các mạng ATM và Frame Relay kết nối giữa các site có thể sử dụng rất nhiều các loại giao thức được định tuyến khác nhau như IP, IPX, AppleTalk, IP Multicast...ATM và Frame Relay còn cung cấp đặc điểm QoS(Quality of Service). Đây là điều kiện tiên quyết khi vận chuyển các luồng dữ liệu cho Voice.

Công nghệ VPN Lớp 3

Một kết nối giữa các site có thể được định nghĩa như là VPN lớp 3. Các loại VPN lớp 3 như GRE, MPLS và IPSec. Công nghệ GRE và IPSec được sử dụng để thực hiện kết nối point - to - point, công nghệ MPLS thực hiện kết nối đa điểm(any - to - any)

Đường hầm GRE

Generic routing encapsulation (GRE) được khởi xướng và phát triển bởi Cisco và sau đó được IETF xác nhận thành chuẩn RFC 1702. GRE được dùng để khởi tạo các đường hầm và có thể vận chuyển nhiều loại giao thức như IP, IPX, Apple Talk và bất kỳ các gói dữ liệu giao thức khác vào bên trong đường hầm IP. GRE không có chức năng bảo mật cấp cao nhưng có thể được bảo vệ bằng cách sử dụng cơ chế IPSec. Một đường hầm GRE giữa 2 site, ở đó IP có thể vươn tới được có thể được mô tả như là một VPN bởi vì dữ liệu riêng giữa 2 site có thể được đóng gói thành các gói tin với phần Header tuân theo chuẩn GRE.

Bởi vì mạng Internet công cộng được kết nối trên toàn thế giới. Các chi nhánh của một tập đoàn nằm trên những vùng địa lý khác nhau. Để các chi nhánh này có thể truyền dữ liệu cho nhau và cho văn phòng chính tại trung tâm thì điều kiện cần là mỗi chi nhành chỉ cần thiết lập một kết nối vật lý đến nhà cung cấp dịch vụ Internet(ISP). Thông qua mạng VPN được thiết lập sử dụng GRE Tunnel. Tất cả các dữ liệu giữa các chi nhánh sẽ trao đổi với nhau trong một đường hầm GRE. Hơn thế dữ liệu còn được bảo mật và chống lại các nguy cơ tấn công

MPLS VPNs

Công nghệ MPLS VPN xây dựng các kết nối chuyển mạch nhãn(Label Switched Path) thông qua các Router chuyển mạnh nhãn(Label Switch Routers). Các gói tin được chuyển đi dựa vào Label của mỗi gói tin. MPLS VPN có thể sử dụng các giao thức TDP(Tag Distribution Protocol), LDP(Label Ditribution Protocol) hoặc RSVP(Reservation Protocol)

Khởi xướng cho công nghệ này là Cisco, MPLS có nguồn gốc là các Tag trong mạng chuyển mạch và sau đó được IETF chuẩn hoá thành MPLS. MPLS được tạo ra thông qua các Router sử dụng cơ chế chuyển mạch nhãn(Label Switch Routers). Trong một mạng MPLS, các gói tin được chuyển mạch dựa trên nhãn của mỗi gói tin. Các nhà cung cấp dịch vụ hiện nay đang tăng cường triển khai MPLS để cung cấp dịch vụ VPN MPLS đến khách hàng.

Nguồn gốc của tất cả các công nghệ VPN là dữ liệu riêng được đóng gói và phân phối đến đích với việc gắn cho các gói tin thêm phần Header; MPLS VPN sử dụng các nhãn(Label) để đóng gói dữ liệu gốc và thực hiện truyền gói tin đến đích.

RFC 2547 định nghĩa cho dịch vụ VPN sử dụng MPLS. Một tiện ích của VPN MPLS so với các công nghệ VPN khác là nó giảm độ phức tạp để cấu hình VPN giữa các site.

Ví dụ

Công ty chúng ta có 03 chi nhánh tại 3 địa điểm khác nhau, để các site này có thể truyền dữ liệu cho nhau chúng ta thực hiện cấu hình VPN any-to-any(Full Mesh) sử dụng các công nghệ như ATM hay Frame Relay, khi đó mỗi site đòi hỏi 02 Virtual Circuit hoặc tunnel đến mỗi site khác đồng thời chúng ta phải thiết lập cấu hình đến mỗi site do vậy hệ số phức tạp của mô hình này là O(n) với n là số site. Ngược lại, với mô hình VPN MPLS ta luôn có hệ số phức tạp là O(1) dù hệ thống có đến n site khác nhau đi chăng nữa.

Thực tế cho thấy các kết nối site-to-site không tạo đường hầm point-to-point của VPN MPLS có khả năng mở rộng dễ dàng. Các kết nối any-to-any giữa các site có thể được thực hiện dễ dàng bằng công nghệ MPLS.

Tuy nhiên công nghệ này gặp phải một trở ngại đó là phụ thuộc vào cơ sở hạ tầng nhà cung cấp dịch vụ VPN MPLS. Trong khi đó công nghệ VPN GRE lại có thể được sử dụng thông qua Internet để mở rộng tầm hoạt động một cách dễ dàng mà không phụ thuộc nhà cung cấp, thêm vào đó bản thân công nghệ VPN GRE tự chính nó đã đạt được một khả năng bảo mật cơ bản với công nghệ truyền dữ liệu trong đường hầm

IPSec VPNs

Một nội dung chính mà bất kỳ ai sử dụng VPN muốn bảo mật dữ liệu khi chúng được truyền trên hệ thống mạng công cộng. Một câu hỏi được đặt ra là làm thế nào để ngăn chặn mối nguy hiểm từ việc nghe trộm dữ liệu khi chúng được truyền đi trên mạng công cộng?

Mã hoá dữ liệu là một cách để bảo vệ nó. Mã hoá dữ liệu có thể được thực hiện bằng cách triển khai các thiết bị mã hoá/giải mã tại mỗi site.

IPSec là một tập giao thức được phát triển bởi IETF để thực thi dịch vụ bảo mật trên các mạng IP chuyển mạch gói. Internet là mạng chuyển mạch gói công cộng lớn nhất. Công nghệ IPSec VPN được triển khai có một ý nghĩa quan trọng là tiết kiệm chi phí rất lớn so với mạng VPN sử dụng Leased-Line VPN.

Dịch vụ IPSec cho phép chứng thực, kiểm tra tính toàn vẹn dữ liệu, điều khiển truy cập và đảm bảo bí mật dữ liệu. Với IPSec, thông tin được trao đổi giữa các site sẽ được mã hoá và kiểm tra. IPSec có thể được triển khai cả trên hai loại VPN là Remote Access Client và Site-to-Site VPN

Giao thức PPTP(Point-to-Point Tunneling Protocol)

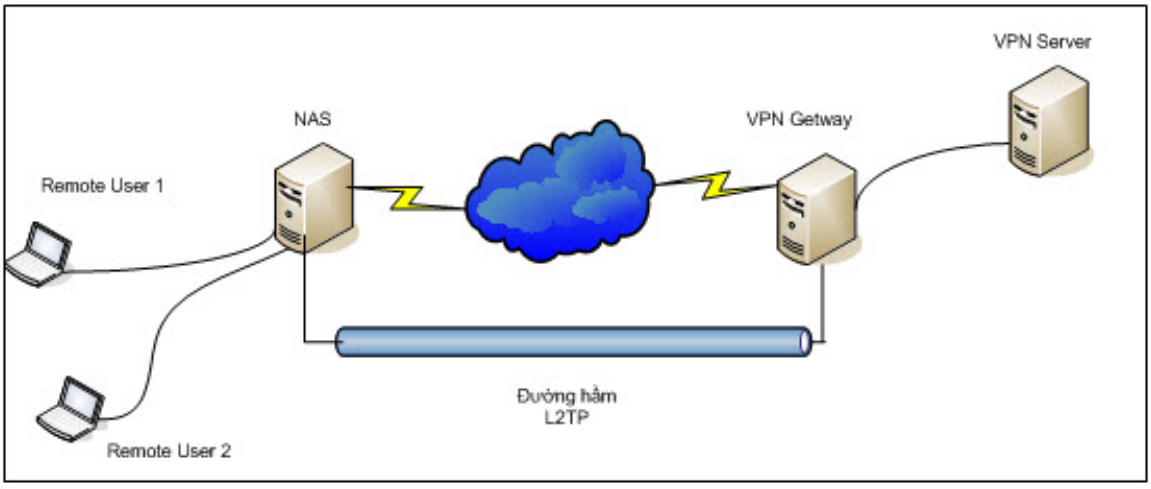
Đây là giao thức đường hầm phổ biến nhất hiện nay. Giao thức được phát triển bởi Microsoft.

PPTP cung cấp một phần của dịch vụ truy cập từ xa RAS(Remote Access Service). Như L2F, PPTP cho phép tạo đường hầm từ phía người dùng(Mobile User) truy cập vào VPN Getway/Concentrator

Giao thức L2F

Là giao thức lớp 2 được phát triển bởi Cisco System. L2F được thiết kế cho phép tạo đường hầm giữa NAS và một thiết bị VPN Getway để truyền các Frame, người sử dụng từ xa có thể kết nối đến NAS và truyền Frame PPP từ remote user đến VPN Getway trong đường hầm được tạo ra.

Giao thức L2TP



Là chuẩn giao thức do IETF đề xuất, L2TP tích hợp cả hai điểm mạnh là truy nhập từ xa của L2F(Layer 2 Forwarding của Cisco System) và tính kết nối nhanh Point - to Point của PPTP(Point to Point Tunnling Protocol của Microsoft). Trong môi trường Remote Access L2TP cho phép khởi tạo đường hầm cho các frame và sử dụng giao thức PPP truyền dữ liệu trong đường hầm.

Một số ưu điểm của L2TP

- L2TP hỗ trợ đa giao thức
- Không yêu cầu các phần mềm mở rộng hay sự hỗ trợ của HĐH. Vì vậy những người dùng từ xa cũng như trong mạng Intranet không cần cài thêm các phần mềm đặc biệt.

- L2TP cho phép nhiều Mobile user truy cập vào Remote Network thông qua hệ thống mạng công cộng
- L2TP không có tình bảo mật cao tuy nhiên L2TP có thể kết hợp với cơ chế bảo mật IPSec để bảo vệ dữ liệu.
- Với L2TP sự xác thực tài khoản dựa trên Host Getway Network do vậy phía nhà cung cấp dịch vụ không phải duy trì một Database để thẩm định quyền truy cập

IEEE 802.1Q tunneling (Q-in-Q)

Đường hầm 802.1Q cho phép nhà cung cấp dịch vụ tạo các đường hầm trên Ethernet sử dụng hạ tầng mạng được chia sẻ. Dữ liệu trong đường hầm 802.1Q được vận chuyển phụ thuộc vào tag 802.1Q

The Secure Sockets Layer (SSL)

SSL là giao thức bảo mật được phát triển bởi tập đoàn Netscape(SSL version 1,2 và 3). SSL cung cấp cơ chế bảo mật truy cập từ xa cho người dùng di động. Cơ chế SSL ít được triển khai hơn vì tính bảo mật của nó khi so sánh với các cơ chế khác(L2F, PPTP, L2TP, IPSec)

Giao thức Point to Point Protocol(PPP)

Đây là giao thức đóng gói để truyền dữ liệu qua kết nối Serial. Lợi thế lớn nhất của PPP là có thể hoạt động trên mọi Data Terminal Equipment (DTE) hoặc Data Connection Equipment(DCE). Một đặc điểm thuận lợi của PPP là nó không giới hạn tốc độ truy cập. PPP là sẵn sàng cho kết nối song công (Full Duplex) và là giải pháp tốt cho kết nối Dial-up.

Bài 4: Giao thức bảo mật IPSec

Giao thức bảo mật IPSec

Công nghệ VPN sử dụng cơ sở hạ tầng mạng công cộng và các môi trường truyền dẫn được chia sẻ khác để truyền dữ liệu, do vậy bảo mật dữ liệu trong mạng VPN là vấn đề vô cùng quan trọng. Để giải quyết vấn đề này, VPN xây dựng đường hầm(Tunnle) và sử dụng bộ giao thức IPSec để mã hoá dữ liệu trong đường hầm.

Một thuật toán mã hoá có hai chức năng mã hoá và giải mã

Mã hoá(Encryption):

Có chức năng chuyển dữ liệu ở dạng bản rõ(Plain text) thành dạng dữ liệu được mã hoá

Giải mã(Decryption):

Có chức năng chuyển thông tin đã được mã hoá thành dạng bản rõ(Plain Text) với key được cung cấp.

Các thuật toán mật mã được xếp vào hai loại sau:

- Đối xứng(Symmetric)
- Bất đối xứng(Asymmetric)

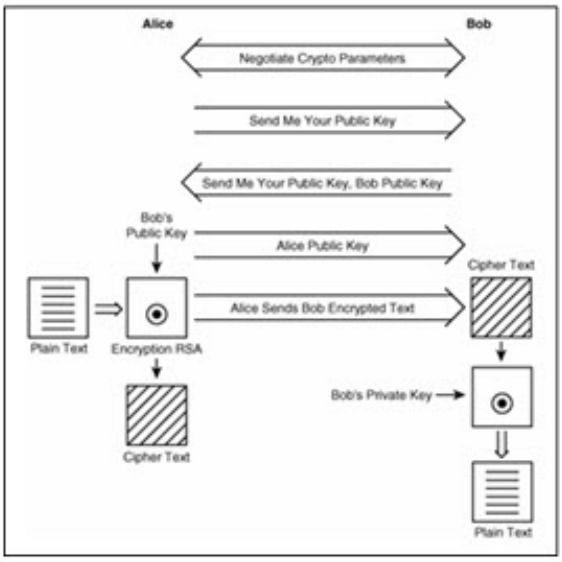
Thuật toán mật mã đối xứng(Symmetric)

Có đặc điểm là người nhận và người gửi cùng sử dụng chung một khoá bí mật(secret key). Bất kỳ ai có khoá bí mật đều có thể giải mã bản mã.

Thuật toán mật mã bất đối xứng(Asymmetric

Còn được biết đến như là thuật toán khoá công khai(Public Key). Khoá mã được gọi là khoá công khai và có thể được công bố, chỉ khoá ảo(Private Key) là cần được giữ bí mật. Như vậy Public Key và Private Key là liên quan đến nhau. Bất kỳ ai có Public Key đều có thể mã hoá bản Plain Text nhưng chỉ có ai có Private Key mới có thể giải mã từ bản mã về dạng rõ.

Để minh hoạ cho thuật toán này, chúng ta quay trở lại ví dụ về bài toán mật mã điển hình là: Bob và Alice cần truyêng thông tin bí mật cho nhau sử dụng thuật toán mã hoá công khai.

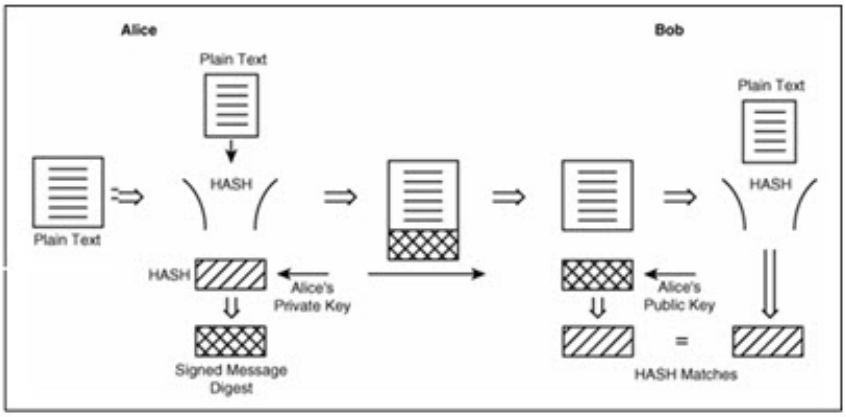


Cơ chế mã hoá và giải mã sử dụng Public Key

Trong thực tế thuật toán mã khoá công khai ít được sử dụng để mã hoá nội dung thông tin vì thuật toán này xử lý chậm hơn so với thuật toán đối xứng. tuy nhiên Public Key thường được dùng để giải quyết vấn đề phân phối Key của thuật toán đối xứng. Public Key không thay thế Symmetric mà chúng trợ giúp lẫn nhau.

Digital Signatures

Một ứng dụng khác của thuật toán mã hoá công khai là chữ ký điện tử(Digital Signature). Trở lại bài toán Alice và Bob. Lúc này Bob muốn chứng thực là thư Alice gửi cho mình do chính Alice gửi chứ không phải là một lá thư nặc danh từ một kẻ thức 3 nào đó. Do vậy một chữ ký điện tử được sinh ra và gắn kèm vào tệp tin của Alice, Bob sử dụng Public Key để giải mã và xác nhận đây đúng là chữ ký của Alice. Cơ chế xác thực như sau:



Cơ chế xác thực chữ ký số

- Máy tính Alice sử dụng hàm HASH băm văn bản cần muốn gửi cho Bob thành một tệp 512 byte gọi là tệp HASH.
- Alice mã hoá tệp HASH với Private Key thành chữ ký số. Chữ ký số được đính kèm vào văn bản gửi đi
- Bob giải mã chữ ký điện tử của Alice với Public key tạo ra tệp HASH1 và sau đó sử dụng hàm HASH băm tệp Plain Text nhận được từ Alice tạo ra tệp HASH2
- HASH1 và HASH2 được so sánh với nhau, nếu hợp nhất thì văn bản Bob nhận được đúng là của Alice gửi.

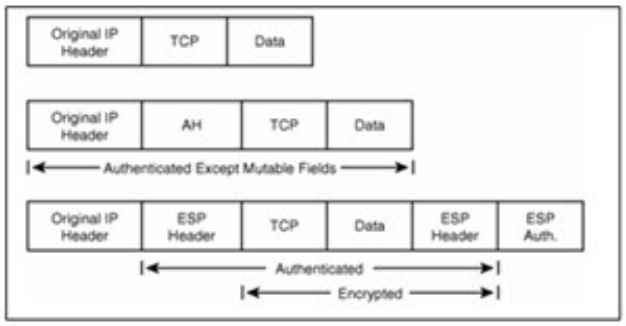
IPSec Security Protocol

Mục đích của IPSec là cung cấp dịch vụ bảo mật cho gói tin IP tại lớp Network. Những dịch vụ này bao gồm điều khiển truy cập, toàn vẹn dữ liệu, chứng thực và bảo mật dữ liệu.

Encapsulating security payload (ESP) và authentication header (AH) là hai giao thức chính được sử dụng để cung cấp tính năng bảo mật cho gói IP. IPSec hoạt động với hai cơ chế Transport Mode và Tunnel Mode

IPSec Transport Mode

Trong chế độ này một IPSec Transport Header(AH hoặc ESP) được chèn vào giữa IP Header và các Header lớp trên.



Hiển thị một IP Packet được bảo vệ bởi IPSec trong chế độ Transport Mode

Trong chế độ này, IP Header cũng giống như IP Header của gói dữ liệu gốc trừ trường IP Protocol là được thay đổi nếu sử dụng giao thức ESP(50) hoặc AH(51) và IP Header Checksum là được tính toán lại. Trong chế độ này, địa chỉ IP đích trong IP Header là không được thay đổi bởi IPSec nguồn vì vậy chế độ này chỉ được sử dụng để bảo vệ các gói có IP EndPoint và IPSec EndPoint giống nhau.

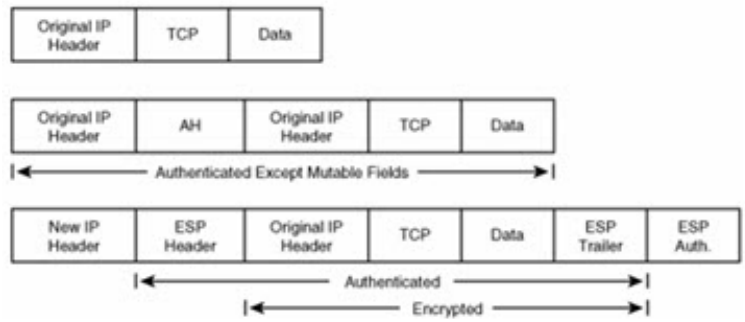
IPSec Transport Mode là rất tốt khi bảo vệ luồng dữ liệu giữa hai host hơn là mô hình site-to-site. Hơn thế hai địa chỉ IP của hai host này phải được định tuyến(Nhìn thấy nhau

trên mạng) điều đó tương đương với việc các Host không được phép NAT trên mang. Do vậy IPSec Transport Mode thường được dùng để bảo vệ các Tunnle do GRE khởi tạo giữa các VPN Getway trong mô hình Site-to-Site,

IPSec Tunnle Mode

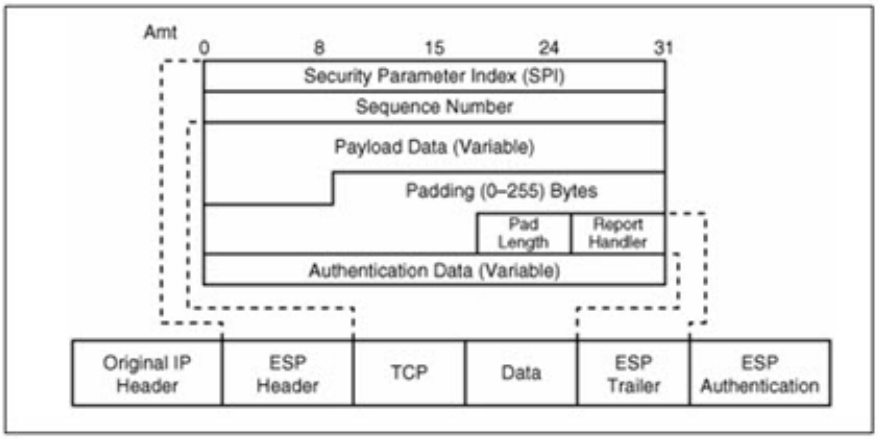
Dịch vụ IPSec VPN sử dụng chế độ Transport và phương thức đóng gói GRE giữa các VPN Getway trong mô hình Site-to-Site là hiệu quả. Nhưng khi các Client kết nối vào Getway VPN thì từ Client và Getway VPN là chưa được bảo vệ, hơn thế khi các Client muốn kết nối vào một Site thì việc bảo vệ IPSec cũng là một vấn đề. IPSec Tunnle Mode ra đời để hỗ trợ vấn đề này.

Ở chế độ Tunnle Mode, gói IP nguồn được đóng gói trong một IP Datagram và một IPSec header(AH hoặc ESP) được chèn vào giữa outer và inner header, bởi vì đóng gói với một "outer" IP Packet, chế độ Tunnle được có thể được sử dụng để cung cấp dịch vụ bảo mật giữa các IP Node đằng sau một VPN Getway



Gói IP trong chế độ IPSec Tunnle

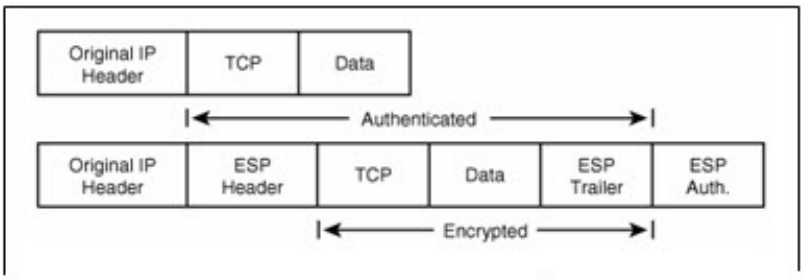
Encapsulating Security Header (ESP)



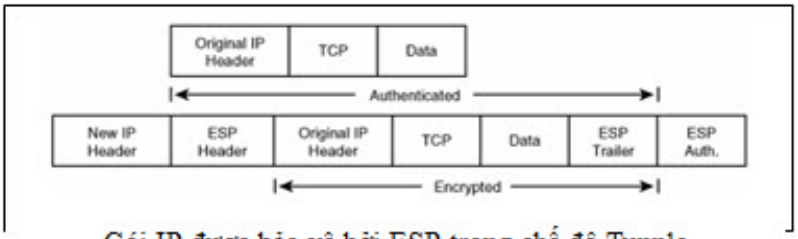
Gói dữ liệu IP được bảo vệ bởi ESP

ESP cung cấp sự bảo mật, toàn vẹn dữ liệu, và chứng thực nguồn gốc dữ liệu và dịch vụ chống tấn công Anti-reply

ESP điền giá trị 50 trong IP Header. ESP Header được chèn vào sau IP Header và trước Header của giao thức lớp trên. IP Header có thể là một IP Header mới trong chế độ Tunnle hoặc là IP Header nguồn nếu trong chế độ Transport.



Gói IP được bảo vệ bởi ESP trong chế độ Transport



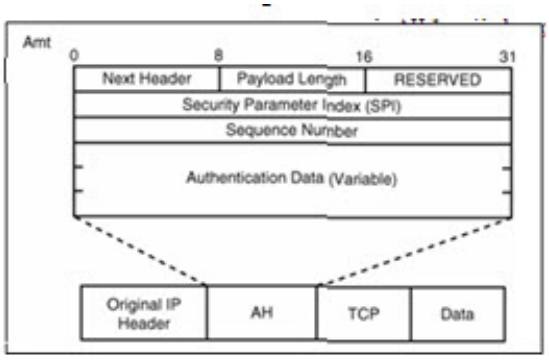
Gói IP được bảo vệ bởi ESP trong chế độ Tunnle

Tham số bảo mật *Security Parameter Index (SPI)* trong ESP Header là một giá trị 32 bit được tích hợp với địa chỉ đích và giao thức trong IP Header.

SPI là một số được lựa chọn bởi Host đích trong suốt quá trình diễn ra thương lượng Public Key giữa các Peer-to-Peer. Số này tăng một cách tuần tự và nằm trong Header của người gửi. SPI kết hợp với cơ chế Slide Window tạo thành cơ chế chống tấn công Anti-Replay.

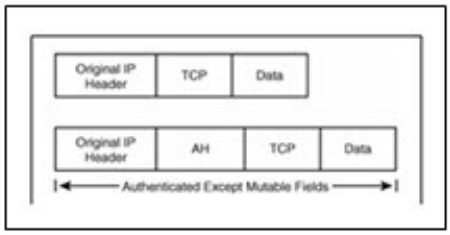
Authentication Header (AH)

AH cũng cung cấp cơ chế kiểm tra toàn vẹn dữ liệu, chứng thực dữ liệu và chống tấn công. Nhưng không giống EPS, nó không cung cấp cơ chế bảo mật dữ liệu. Phần Header của AH đơn giản hơn nhiều so với EPS

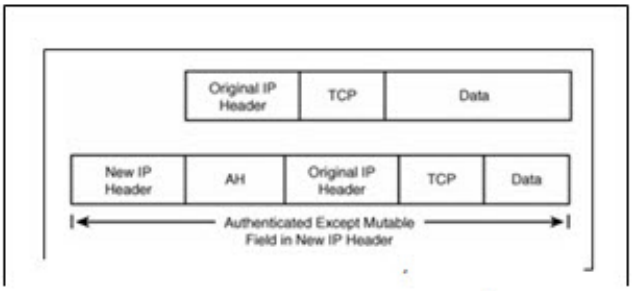


Gói IP được bảo vệ bởi AH

AH là một giao thức IP, được xác định bởi giá trị 51 trong IP Header. Trong chế độ Transport, gá trị giao thức lớp trên được bảo vệ như UPD, TCP..., trong chế độ Tunnle, giá trị này là 4. Vị trí của AH trong chế độ Transport và Tunnle như trong hình sau:



Gói IP được bảo vệ bởi AH trong chế độ Transport



Gói IP bảo vệ bởi AH trong chế độ Tunnle

Trong chế độ Transport, AH là rất tốt cho kết nối các endpoint sử dụng IPSec, trong chế độ Tunnle AH đóng gói gói IP và thêm IP Header vào phía trước Header. Qua đó AH trong chế độ Tunnle được sử dụng để cung cấp kết nối VPN end-to-end bảo mật. Tuy nhiên phần nội dung của gói tin là không được bảo mật

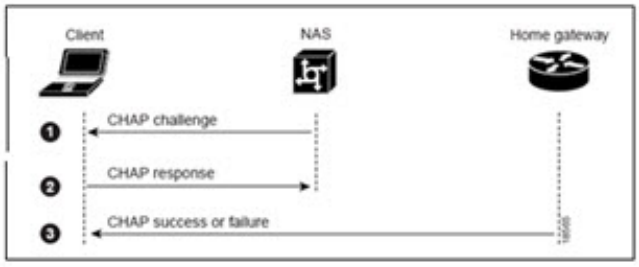
Tiến trình chứng thực bắt tay 3 bước -Three-Way CHAP Authentication Process

Khi thiết lập một kết nối VPN, Client, NAS hoặc Home Getway sử dụng cơ chế chứng thực qua 3 bước để cho phép hoặc không cho phép(Allow or Denied) tài khoản được phép thiết lập kết nối.

CHAP là giao thức chứng thực challenge/response(Hỏi đáp/phản hồi). Nó mã hoá Password thành một chữ ký có độ dài 64 bit thay cho việc gửi password đi trên mạng ở dạng Plain Text. Cơ chế này hỗ trợ bảo mật Password từ Client đến Home Getway.

Tiến trình này được mô tả như sau:

- Khi user khởi tạo một phiên kết nối PPP với NAS, NAS gửi một challenge đến Client
- Client gửi một CHAP Response đến NAS trong đó có user ở dạng clear text, NAS sử dụng số khi user quay số đến để xác nhận điểm cuối của đường hầm IP. Tại điểm này PPP đàm phán và tạm dừng ở đó, và NAS hỏi một AAA Server về thông tin đường hầm. AAA Server trợ giúp thông tin để chứng thực tunnle giữa NAS và Home Getway. NAS và Home Getway chứng thực và thiết lập đường hầm giữa NAS và Home Getway. Sau đó NAS chuyển các thông tin đàm phán PPP với Client đến Home Getway
- Home Getway chứng thực Client và sau đó trả về một Response, cái mà được chuyển tiếp qua NAS đến Client và gửi một CHAP success hoặc failure đến Client.



Tiến trình chứng thực CHAP 3 bước

Bài 5: Các chức năng của ISA

Các chức năng của ISA

ISA - Microsoft Internet Security and Acceleration là phần mềm tăng tốc và bảo mật hệ thống của Microsoft. ISA có nhiều phiên bản. Phiên bản mới nhất hiện nay là ISA2006. ISA 2006 có một số chức năng chính sau:

Tính năng Firewall

Kiểm soát các luồng dữ liệu di chuyển trên hệ thống luôn là công việc vất vả và khó khăn và yêu cầu người quản trị có một kiến thức sâu về hệ thống. ISA đưa ra một công cụ làm đơn giản hoá việc đó bằng tính năng Firewall. Tính năng Firewall trong ISA cho phép ta kiểm soát các luồng dữ liệu(traffic) của từng giao thức, ứng dụng và User trong mạng.

Tính năng Proxy

Khi các Client trong hệ thống truy cập ra Internet, việc để lộ IP nguồn ra Internet là cơ hội cho các Hacker tấn công vào hệ thống. ISA đưa ra một cơ chế che dấu các thông tin khi Client truy cập Internet.

Thiết lập mạng VPN

ISA cho phép xây dựng một hệ thống mạng riêng ảo cho phép người dùng từ xa Mobile User truy cập vào hệ thống mạng nội bộ để làm việc, ISA cũng có cơ chế Site-to-Site xây dựng hệ thống VPN giữa các chi nhánh với văn phòng chính thành một hệ thống mạng nội bộ

Tính năng Web Cache

Để tăng tốc truy cập Internet, ISA xây dựng cơ chế web Caching, cho phép Cache các trang web có lượng truy cập lớn về Server. Nếu các Client truy cập vào Site đã được Cache trong Server thì nội dung site đó được lấy về từ ISA Server mà không phải đi ra Internet. Từ đó tăng tốc độ truy cập Internet.

Tính năng Public Server

Để Public các Site lên Internet, chúng ta cần các IP Public. Do vậy chúng ta phải thanh toán chi phí thuê bao các địa chỉ IP này. Để tiết kiệm chi phí,

chúng ta chỉ sử dụng một IP Public và Public các Server nội bộ lên Internet nhờ ISA Server.

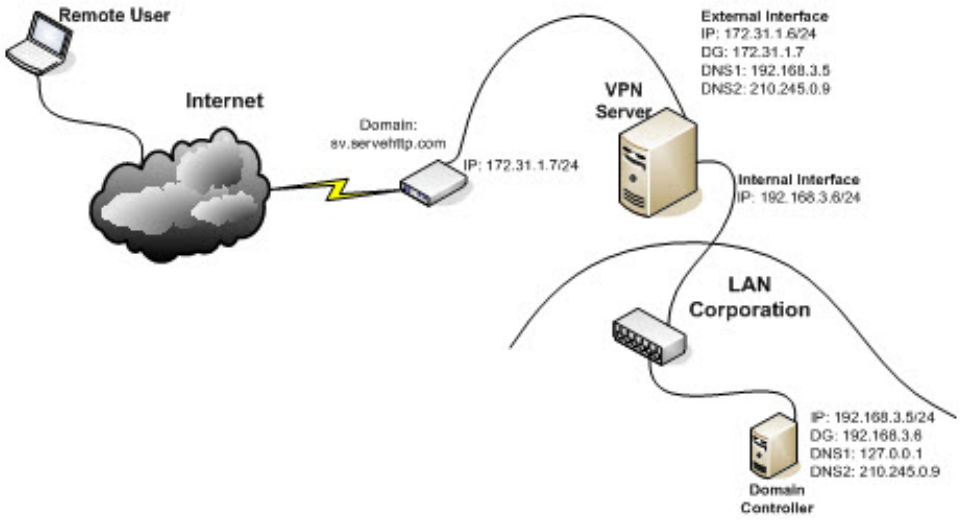
Bài 6: Bài toán thực tế

Bài toán thực tế

Bài toán

Xây dựng hệ thống VPN cho phép các thầy, cô và các bạn sinh viên truy cập vào hệ thống mạng nội bộ của khoa CNTT khi đang đi công tác xa hoặc làm việc tại nhà.

Sơ đồ hệ thống



Các bước cấu hình hệ thống

ISA Server 2004 firewall có thể được cấu hình trở thành môt VPN server. Khi bật chức năng VPN server nó có thể chấp nhận các kết nối vào từ VPN clients -incoming VPN client , nếu kết nối thành công, VPN client computer sẽ là thành viên cua Mạng được bảo vệ, không khác gì so với các Client bên trong LAN. VPN servers truyền thống cho phép VPN clients đầy đủ quyền truy cập vào Mạng khi đã được kết nối.

Ngược lại với ISA Server 2004 VPN server có khả năng cho phép chúng ta điều khiển những protocols nào và những servers nào mà VPN clients có thể kết nối đến dựa trên đặc quyền mà Client đã khai báo khi thiết lập kết nối-credentials đến VPN server.

Có thể dùng Microsoft Internet Security and Acceleration Server 2004 management console để quản lý tất cả cấu hình liên quan đến VPN server . Firewall sẽ quản lý danh sách các IP addresses được cấp phát cho VPN clients và bố trí các IP này trên một VPN clients network được chỉ định. Điều khiển truy cập sau đó có thể được bố trí dựa trên chiều giao tiếp, thông qua kiểm soát của các Access Rules : Đến hay từ VPN clients network.

Theo các bước sau tiến hành enable ISA Server 2004 VPN server:

- Enable VPN Server
- Tạo một Access Rule cho phép VPN clients truy cập vào Internal network
- Kiểm tra các kết nối VPN.

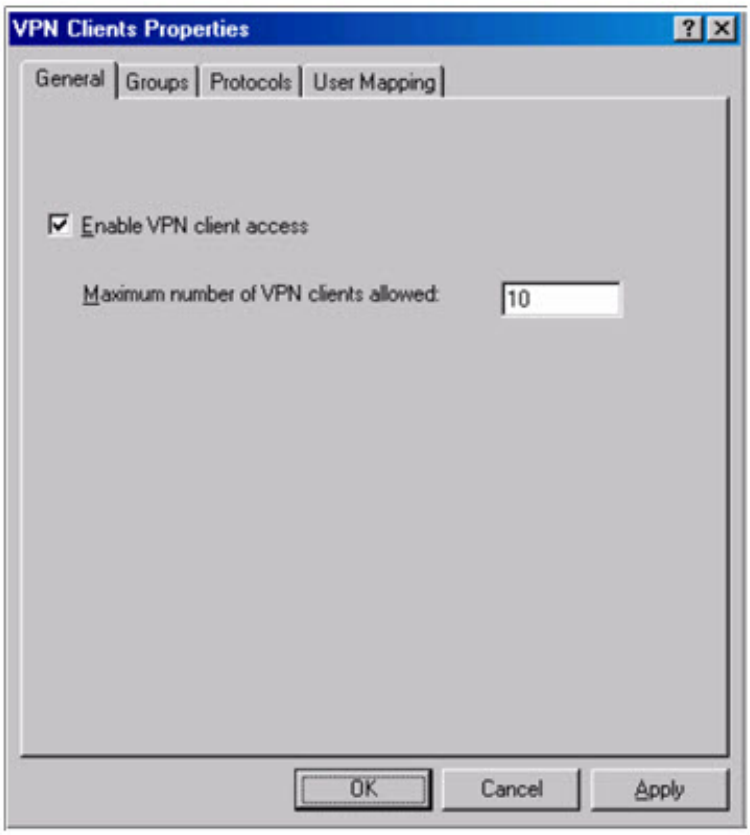
Enable VPN Server

Theo mặc định, thành phần VPN server trên ISA Server bị disabled. Bước đầu tiên là enable tính năng VPN server và cấu hình các thành phần VPN server.

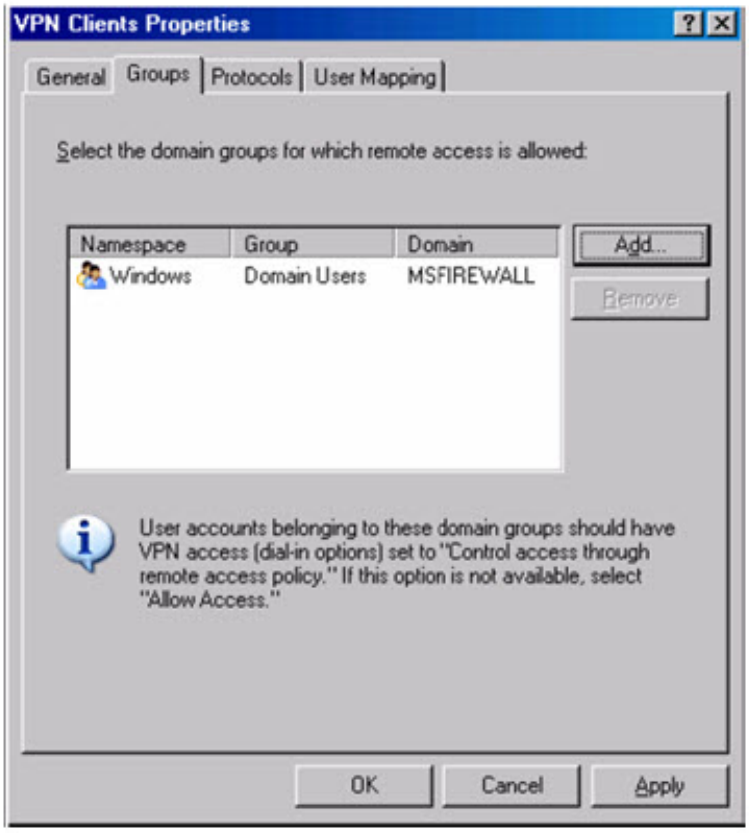
Tiến hành các bước sau để enable và cấu hình ISA Server 2004 VPN Server:

1. Mở Microsoft Internet Security and Acceleration Server 2004 management console , mở rộng server name. Click trên Virtual Private Networks (VPN) node.
2. Click trên Tasks tab trong Task Pane. Click Enable VPN Client Access.

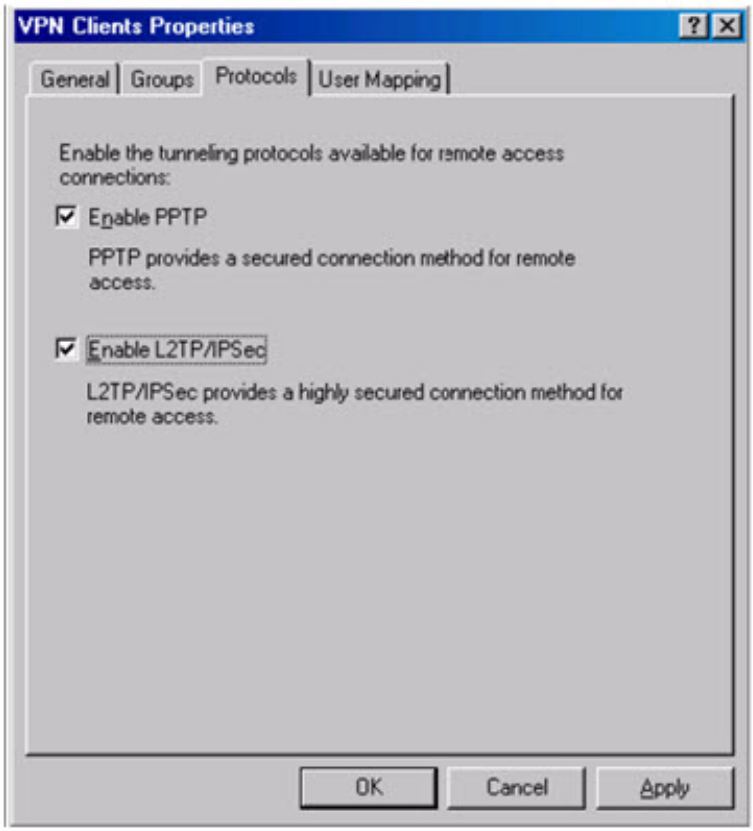
1. Click Apply để lưu những thay đổi và cập nhật firewall policy.
2. Click OK trong Apply New Configuration dialog box.
3. Click Configure VPN Client Access.
4. Trên General tab, thay đổi giá trị là Maximum number of VPN clients allowed
5. Từ 5 đến 10.



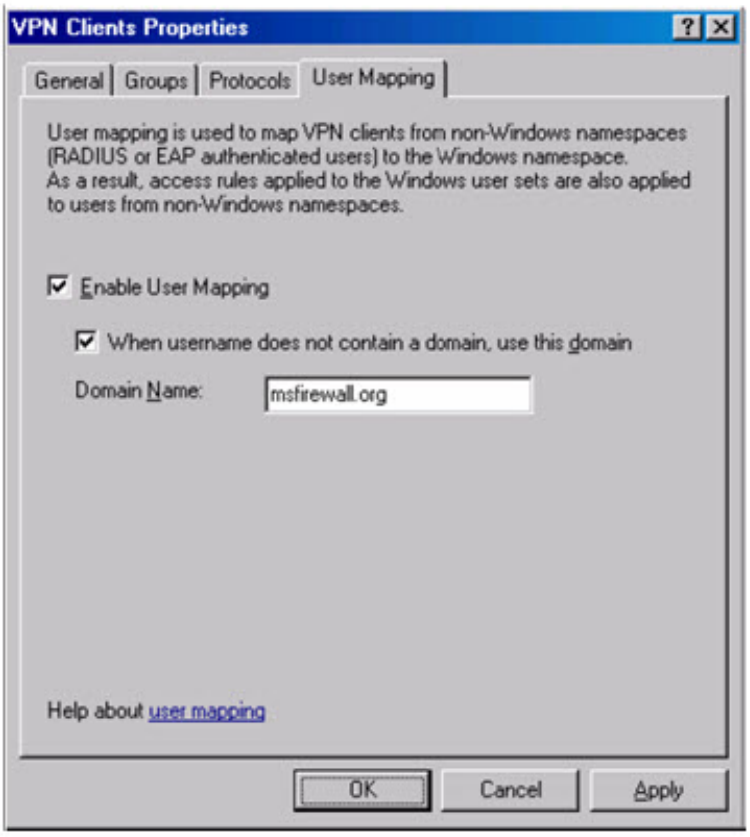
1. Click trên Groups tab. Trên Groups tab, click Add button.
2. Trong Select Groups dialog box, click Locations button. trong Locations dialog box, click msfirewall.org entry và click OK.
3. Trong Select Group dialog box, điền Domain Users trong Enter the object names to select text box. Click Check Names button. group name này sẽ có gạch dưới khi nó được tìm thấy trong Active Directory. Click OK.



1. Click Protocols tab. Trên Protocols tab, đánh dấu check vào Enable L2TP/ IPSec check box.



1. Click User Mapping tab. Đánh dấu check vào Enable User Mapping check box.
2. Đánh dấu check vào When username does not contain a domain, use this domain check box. Điền vào msfirewall.org trong Domain Name text box.



1. Click Apply trong VPN Clients Properties dialog box.
2. Click OK Microsoft ISA 2004

Dialog box nhận được thông báo rằng phải restart lại ISA Server firewall trước khi các xác lập có hiệu lực. Click OK.

1. Click Apply lưu lại những thay đổi và cập nhật cho firewall policy.
2. Click OK trong Apply New Configuration dialog box.
3. Restart ISA Server 2004 firewall.
4. Tạo một Access Rule cho phép VPN Clients truy cập vào Internal Network

Tại thời điểm này, VPN clients có thể kết nối đến VPN server. Tuy nhiên, VPN clients không thể truy cập đến bất cứ tài nguyên nào trên Internal network. Trước hết, bạn phải tạo một Access Rule cho phép các thành viên thuộc VPN clients network truy cập vào Internal network. Trong vd này, chúng ta sẽ tạo một Access Rule nhằm cho phép tất cả các lưu thông từ VPN clients network được vào Internal network. Trong môi trường thực tế, bạn có thể tạo ra access rules hạn chế hơn nhằm chặt chẽ việc Users trên VPN clients network chỉ có thể truy cập đến các tài nguyên mà họ có nhu

Tiến hành các bước sau để tạo VPN clients Access Rule:

1. Trong Microsoft Internet Security and Acceleration Server 2004 management console, mở rộng server name và click Firewall Policy node. Right click Firewall Policy node, chọn New và click Access Rule.
2. Trong Welcome to the New Access Rule Wizard page, đặt tên cho rule trong Access Rule name text box. Trong vd này, chúng ta sẽ đặt tên cho rule là VPN Client to Internal. Click Next.
3. Trên Rule Action page, chọn Allow và click Next.
4. Trên Protocols page, chọn All outbound protocols từ danh sách This rule applies to. Click Next.
5. Trên Access Rule Sources page, click Add. Trong Add Network Entities dialog box, click Networks folder và double click trên VPN Clients. Click Close.

1. Click Next trên Access Rule Sources page.
2. Trên Access Rule Destinations page, click Add. Trên Add Network Entities dialog box, click Networks folder và double click trên Internal. Click Close.
3. Trên User Sets page, chấp nhận xác lập mặc định là, All Users, và click Next.
4. Click Finish trên Completing the New Access Rule Wizard page.
5. Click Apply để lưu những thay đổi và cập nhật firewall policy.
6. Click OK trong Apply New Configuration dialog box.

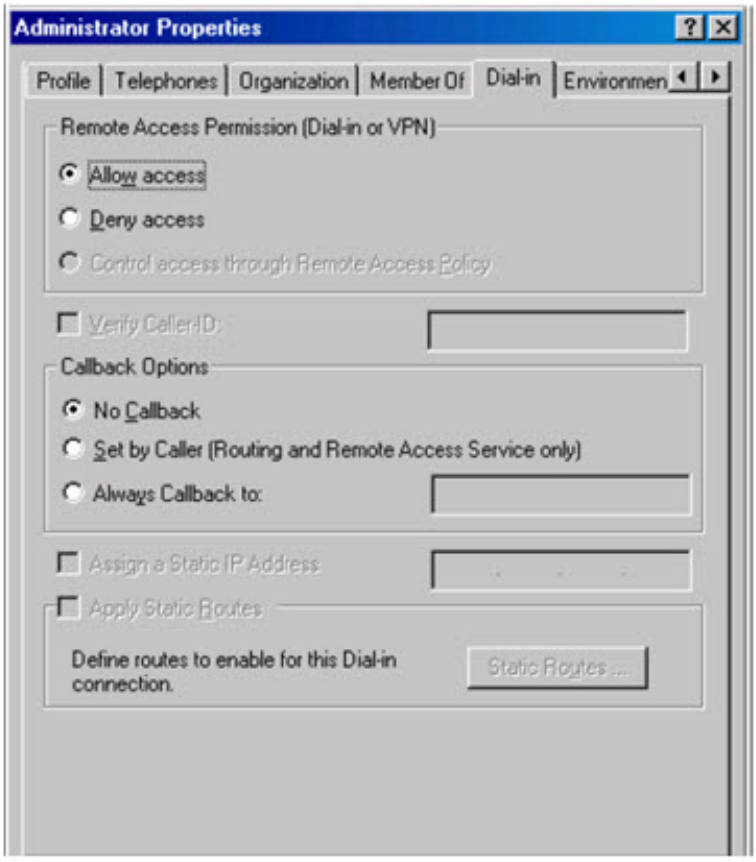
Enable truy cập quay số -Dial-in Access cho Administrator Account

Trong Active Directory domains không phải ở chế độ native mode (Native mode: Ở chế độ này tất cả các Domain Controllers trong domain ấy phải là Windows Server 2000/ 2003), Tất cả các tài khoản User đều bị disabled quyền quay số truy cập theo mặc định- dial-in access by default. Trong tình huống này, bạn phải enable dial-in access trên mỗi tài khoản

cơ bản. Ngược lại, thì Active Directory domains ở chế độ native mode có dial-in access được tập trung điều khiển bởi Remote Access Policy trong RRAS Server. Windows NT 4.0 dial-in access luôn được điều khiển căn cứ trên từng User account Trong ví dụ này, Active Directory ở dạng Windows Server 2003 mixed mode, và vì thế cần thay đổi thủ công các xác lập quyền quay số trên user account.

Tiến hành các bước sau trên domain controller để enable Dial-in access cho riêng Administrator account:

1. Click Start và chọn Administrative Tools. Click Active Directory Users and Computers.
2. Trong Active Directory Users and Computers console, click trên Users node trong khung trái. Double click trên Administrator account trong khung phải.
3. Click trên Dial-in tab. Trong khung Remote Access Permission (Dial-in or VPN), chọn Allow access. Click Apply và click OK.



1. Đóng Active Directory Users and Computers console.
2. Kiểm tra kết nối VPN ISA Server 2004 VPN server giờ đây đã chấp nhận các kết nối VPN client.

Tiến hành các bước sau để kiểm tra VPN Server:

1. Trên Windows 2000 external client, right click My Network Places icon trên desktop và click Properties.
2. Double click Make New Connection icon trong Network and Dial-up Connections window.
3. Click Next trên Welcome to the Network Connection Wizard page.
4. Trên Network Connection Type page, chọn Connect to a private network through the Internet option và click Next.
5. Trên Destination Address page, điền IP address 192.168.1.70 trong Host name or IP address text box. Click Next.
6. Trên Connection Availability page, chọn For all users option và click Next.

Không thay đổi trên Internet Connection Sharing page. và click Next.

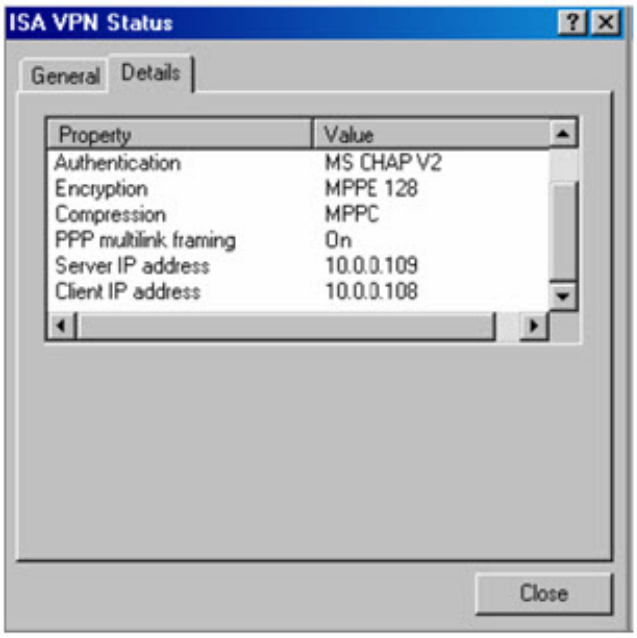
Trên Completing the Network Connection Wizard page, điền vào tên của VPN connection trong Type the name you want to use for this connection text box.

Trong vd này, chúng ta sẽ đặt tên kết nối là ISA VPN. Click Finish.

Trong Connect ISA VPN dialog box, điền vào user name

MSFIREWALL\administrator và password của administrator user account. Click Connect.

1. VPN client sẽ thiết lập một kết nối với ISA Server 2004 VPN server. Click OK
2. trong Connection Complete dialog box nhận được thông báo rằng kết nối đã được thiết lập.
3. Double click trên Connection icon trong system tray và click Details tab. Bạn có thể thấy chế độ mã hóa 128 bits dùng giao thức MPPE- MPPE 128 encryption được sử dụng để bảo vệ data và thấy IP address được cấp phát cho VPN client.



1. Click Start và Run command. Trong Run dialog box, điền vào \\EXCHANGE2003BE trong Open text box, và click OK. Các folder shares trên domain controller xuất hiện.
2. Right click Connection icon trong system tray và click Disconnect.

Tài liệu tham khảo

1. "An Ethernet Tutorial," www.Whatis.com
2. "VPN Technology," www.Google.com.vn
3. "Device"+ "VPN" www.Google.com.vn
4. Appian Communications."*Virual Ethernet Rings: LANs Across the WAN*," While pager, www.appiancom.com, January 2004.
5. Kawamoto, Wayne. "*New Generaion of 10 Gigabit Ethernet Products*," *ISP Planet* (May 24, 2005).
6. Titch, Steven. "GigE Evolution," *American's Network Magazine*,(January 15, 2006)
7. Regis J.(BUD) Bates. GPRS " *General Packet Radio Service*"(May 27, 2005).
8. Hoàng Minh Sơn. "*Mạng truyền thông công nghiệp*"(Nhà xuất bản Khoa Học và Kỹ Thuật 2006).
9. Dương Thế Tùng – "*Mạng truyền dẫn tốc độ cao – Công nghệ & Ứng dụng*"(Nhà xuất bản Thanh Niên 2005)

Tham gia đóng góp

Tài liệu: Đề tài nghiên cứu Công nghệ VPN

Biên tập bởi: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://voer.edu.vn/c/8f2b2b24

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Giới thiệu về Công nghệ VPN

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/d940c5d1

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Các loại VPN

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/b4116e99

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Các công nghệ và giao thức hỗ trợ VPN

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/fa830073

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Giao thức bảo mật IPSec

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/aa970ea7

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Các chức năng của ISA

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/53e5d576

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Module: Bài toán thực tế

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/14944d7a

Module: Tài liệu tham khảo

Các tác giả: Khoa CNTT ĐHSP KT Hưng Yên

URL: http://www.voer.edu.vn/m/cf85153e

Giấy phép: http://creativecommons.org/licenses/by/3.0/

Chương trình Thư viện Học liệu Mở Việt Nam

Chương trình Thư viện Học liệu Mở Việt Nam (Vietnam Open Educational Resources – VOER) được hỗ trợ bởi Quỹ Việt Nam. Mục tiêu của chương trình là xây dựng kho Tài nguyên giáo dục Mở miễn phí của người Việt và cho người Việt, có nội dung phong phú. Các nội dung đều tuân thủ Giấy phép Creative Commons Attribution (CC-by) 4.0 do đó các nội dung đều có thể được sử dụng, tái sử dụng và truy nhập miễn phí trước hết trong trong môi trường giảng dạy, học tập và nghiên cứu sau đó cho toàn xã hội.

Với sự hỗ trợ của Quỹ Việt Nam, Thư viện Học liệu Mở Việt Nam (VOER) đã trở thành một cổng thông tin chính cho các sinh viên và giảng viên trong và ngoài Việt Nam. Mỗi ngày có hàng chục nghìn lượt truy cập VOER (www.voer.edu.vn) để nghiên cứu, học tập và tải tài liệu giảng dạy về. Với hàng chục nghìn module kiến thức từ hàng nghìn tác giả khác nhau đóng góp, Thư Viện Học liệu Mở Việt Nam là một kho tàng tài liệu khổng lồ, nội dung phong phú phục vụ cho tất cả các nhu cầu học tập, nghiên cứu của độc giả.

Nguồn tài liệu mở phong phú có trên VOER có được là do sự chia sẻ tự nguyện của các tác giả trong và ngoài nước. Quá trình chia sẻ tài liệu trên VOER trở lên dễ dàng như đếm 1, 2, 3 nhờ vào sức mạnh của nền tảng Hanoi Spring.

Hanoi Spring là một nền tảng công nghệ tiên tiến được thiết kế cho phép công chúng dễ dàng chia sẻ tài liệu giảng dạy, học tập cũng như chủ động phát triển chương trình giảng dạy dựa trên khái niệm về học liệu mở (OCW) và tài nguyên giáo dục mở (OER) . Khái niệm chia sẻ tri thức có tính cách mạng đã được khởi xướng và phát triển tiên phong bởi Đại học MIT và Đại học Rice Hoa Kỳ trong vòng một thập kỷ qua. Kể từ đó, phong trào Tài nguyên Giáo dục Mở đã phát triển nhanh chóng, được UNESCO hỗ trợ và được chấp nhận như một chương trình chính thức ở nhiều nước trên thế giới.