**Phần I:**

ĐẶT VẤN ĐỀ

Giới thiệu bài toán và giải pháp

Đài Tiếng Nói Nhân Dân TP.HCM là cơ quan truyền thông đại chúng, nhiệm vụ của Đài là tuyên truyền chủ trương chính sách của Đảng và nhà nước, nói lên tiếng nói của Đảng bộ và nhân dân TP.HCM. Trong giai đoạn mới hiện nay, việc áp dụng những thành tựu KHKT vào phục vụ công tác là việc tất yếu và là yếu tô" mang tính chất sống còn đối với hoạt động của Đài nói riêng và tất cả các nghành nghề nói chung. Đài TNND TP.HCM đã và đang ứng dụng CNTT vào trong hoạt động của mình. Tuy còn trong giai đoạn xây dựng và hoàn thiện từng bước, nhưng việc ứng dụng CNTT đã mang lại những hiệu quả nhất định, hỗ trợ hiệu quả cho việc thực hiện các chương trình phát thanh - một nhiệm vụ mang tính chất chính trị quan trọng của Đài.

1. **Giới thiêu hê thông :**

Trong giai đoạn đầu, Đài TNND TP.HCM đã tiến hành trang bị máy tính và thiết lập hệ thông mạng nội bộ để cải tiến, nâng cao hiệu quả công tác nghiệp vụ. Hiện trạng hệ thống đang hoạt động bao gồm:

Một mạng nội bộ kỹ thuật (LAN 1): tập hợp tất cả các máy tính được dùng để thực hiện các chương trình phát thanh, lưu trữ dữ liệu phục vụ cho việc xây dựng chương trình, truyền dữ liệu cho bộ phận phát sóng. Hiện nay để bảo đảm an toàn cho hoạt động phát thanh, không cho phép bất kỳ kết nối nào với mạng bên ngoài. ( sơ đồ mạng kỹ thuật- LAN 1 đài TNND TP.HCM).

* Một mạng nội bộ biên tập (LAN 2): tập hợp tất cả các máy tính dùng để phục vụ cho việc biên tập các chương trình phát thanh, cho phép truy cập Internet thông qua một đường thuê bao ADSL chung cho cả mạng. ( sơ đồ mạng biên tập LAN 2 đài TNND TP.HCM).

Cả hai mạng đều được quản lý tập trung, có những qui định rõ ràng về chính sách bảo mật. Việc trao đổi dữ liệu giữa hai mạng hiện đang được thực hiện một cách thủ công thông qua các thiết bị lưu trữ lưu động.

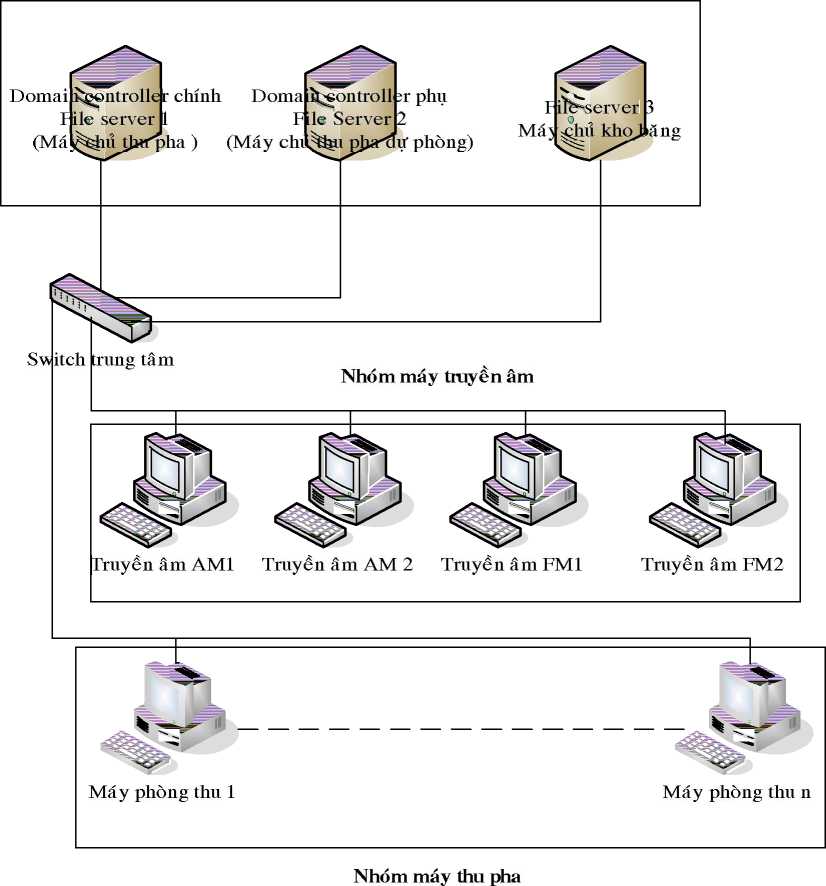
1. **Mạng nôi bọ kỹ thuật (LAN 1):**

Đây là phần quan trọng nhất của hệ thống, phải đảm bảo hoạt động liên tục, ổn định, an toàn. Đặc điểm của mạng:

* Hệ điều hành: Window 2000 server, window 98, Window XP.
* Sử dụng các phần mềm xử lý, convert, play các file âm thanh theo dạng chuẩn mp3 và một số phần mềm chuyên dụng cho phát thanh.
* Dữ liệu lưu trữ và trao đổi trong mạng là các file âm thanh ở dạng chuẩn mp3.
* Tất cả các máy tính và người dùng đều được quản lý. Mỗi cá nhân có những mức độ quyền hạn truy cập mạng khác nhau được quy định rõ ràng- chỉ được truy nhập mạng trên 1 máy cố định.
* Yêu cầu quản lý bảo mật cao. Không được kết nối trực tiếp ra ngoài, kể cả kết nối internet.

Sơ đồ mô tả mạng kỹ thuật:

Nhöm may Server



Cö 3 nhöm chinh:

* Nhöm server: läm nhiem cüa domain controller, file server. Server 1 vä server 2 dtfpc chia thänh nhieu tint muc, möi thif muc cö qui dinh truy xuat rieng. Server 3 düng de lifu trü tü lieu chi cho phep cäc may thupc nhöm thu pha truy xuät de täi du" lieu.
* Nhöm mäy truyen am: läm nhiem vu truyen du" lieu den bp phan phät söng. Chi cö quyen truy xuat den mpt so thuT muc tren cäc server 1 vä server 2- chi dpc, täi dff lieu ve khöng cho phep thay doi hoäc täi du" lieu len server, khöng cö quyen truy xuat väo server 3.
* Nhóm máy thu pha: thực hiện các chương trình phát thanh và tải chúng lên server. Nhóm này có quyền truy xuất vào server 3, được toàn quyền trên những thư mục riêng trên server 1 & 2.

1. **Mang nôi bô biên tâp (LAN 2):**

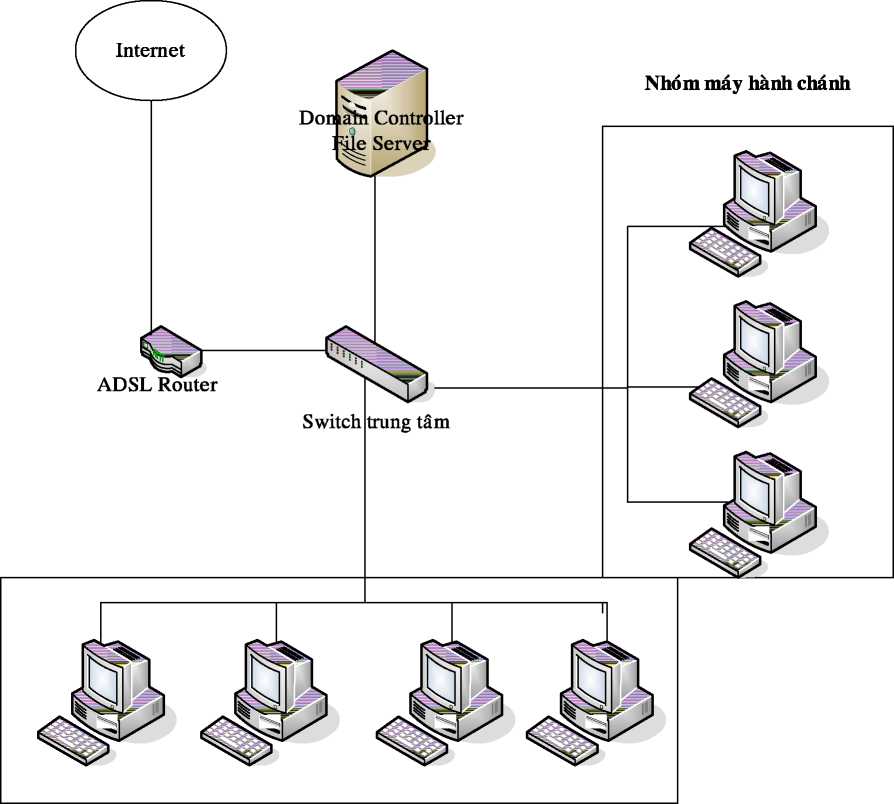
Đặc điểm chung:

* Hệ điều hành: Window 2000 server, window 98, Window XP.
* Sử dụng các phần mềm xử lý, convert, play các file âm thanh theo dạng chuẩn mp3 , các ứng dụng văn phòng và một số phần mềm khác.
* Dữ liệu lưu trữ và trao đổi trong mạng là các file âm thanh ở dạng chuẩn mp3 và file text.
* Tất cả các máy tính và người dùng đều được quản lý. Đa số user đều bị hạn chế quyền truy nhập các tài nguyên chung trong mạng, kể cả file server.
* Cung cấp khả năng kết nối internet có kiểm soát.
* Yêu cầu bảo mật cao.
* Địa chỉ mạng 192.168.24.0/24.
* Địa chỉ cổng ra internet 192.168.24.2.

Các máy tính trong mạng được chia làm 3 nhóm chính:

* Nhóm server: một server làm Domain controller, file server, kiểm soát kết nối internet. File server chỉ cho phép một số user đặc biệt truy nhập.
* Nhóm máy hành chánh: Tập hợp tất cả các máy của các phòng ban hành chánh (Tổ chức, tài vụ...). Không được phép truy cập vào file server. Dữ liệu trao đổi dưới dạng file text. Một số máy được phép truy cập internet.
* Nhóm máy biên tập: Tập hợp tất cả các máy của các ban biên tập. Được phép truy cập internet, một số user trên các máy này có quyền truy xuất vào file server. Dữ liệu trao đổi dưới dang file âm thanh và file text.

Sơ đồ mạng biên tập



Nhóm máy biên tập

1. **Các yêu cầu phát triển:**

Bước đầu hệ thống đã hoạt động tốt, đáp ứng được những yêu cầu nghiệp vụ cơ bản. Trong giai đoạn sắp tới hệ thống cần được hòan thiện thêm với những yêu cầu cụ thể như sau:

* Kết nối có kiểm soát giữa hai mạng nội bộ hiện có.
* Cho phép một số cá nhân truy cập từ xa ( Remote Access) vào mạng biên tập (LAN 2) của Đài.
* Thiết lập một kết nối giữa hệ thống mạng của Đài với một mạng nội bộ ở xa (site-to-site).

Yêu cầu chung:

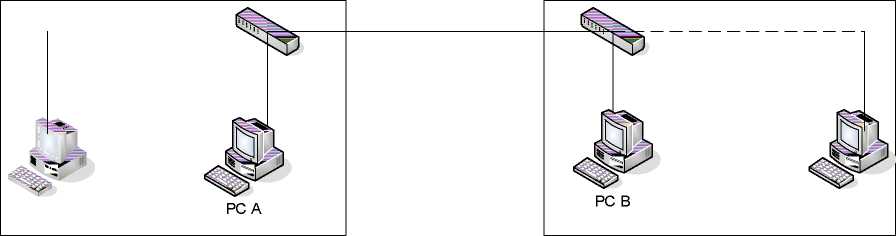
* Bảo đảm độ an toàn, độ tin cậy cao.
* Không gây xáo trộn hệ thống hiện có để tránh ảnh hưởng đến hoạt động của Đài.
* Chú ý xem xét đến yếu tố phức tạp về mặt kỹ thuật và tính kinh tế của giải pháp.

l.l.**Kết nốĩ cổ kiếm soát 2 mang nôi bỏ:**

Nhằm tạo thuận lợi hơn trong việc trao đổi dữ liệu giữa 2 mạng nội bộ hiện có, việc hợp nhất chúng thành một hệ thống chung là cần thiết, vấn đề đặt ra ở đây là phải kiểm soát được sự truy cập vào phần mạng kỹ thuật.

Sơ đổ mổ tả yêu cầu

Mạng KT (LAN 1) Mạng BT (LAN 2)



Yêu cầu cụ thể là chỉ có một vài tính ở phần mạng kỹ thuật được phép truy cập vào ServerBT để trao đổi dữ liệu, cấm tất cả những truy cập qua lại khác giữa 2 phần mạng của hệ thống.

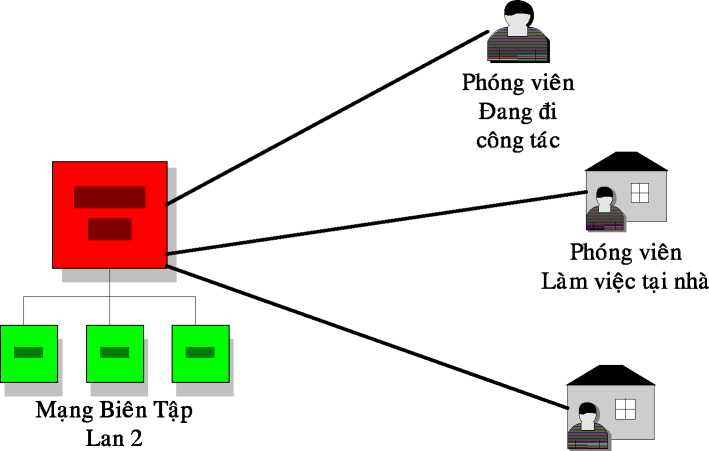
1. **Cho phép người dùng di đông truy xuất vào hê thông:**

Để nâng cao khả năng tác nghiệp của các phóng viên, cần xây dựng một cơ chế cho phép những người dùng riêng lẻ có thể truy cập vào hệ thống thông qua các phương tiện truyền thông công cộng phổ biến.

Yêu cầu cụ thể :

* Đảm bảo an toàn của hệ thống.
* Không quá phức tạp đối với người dùng, yêu cầu về thiết bị không cao.
* Cần chú ý đến chi phí thiết lập và duy trì hệ thống.

Sơ đồ mô tả yêu cầu



Phóng viên Làm việc tại nhà

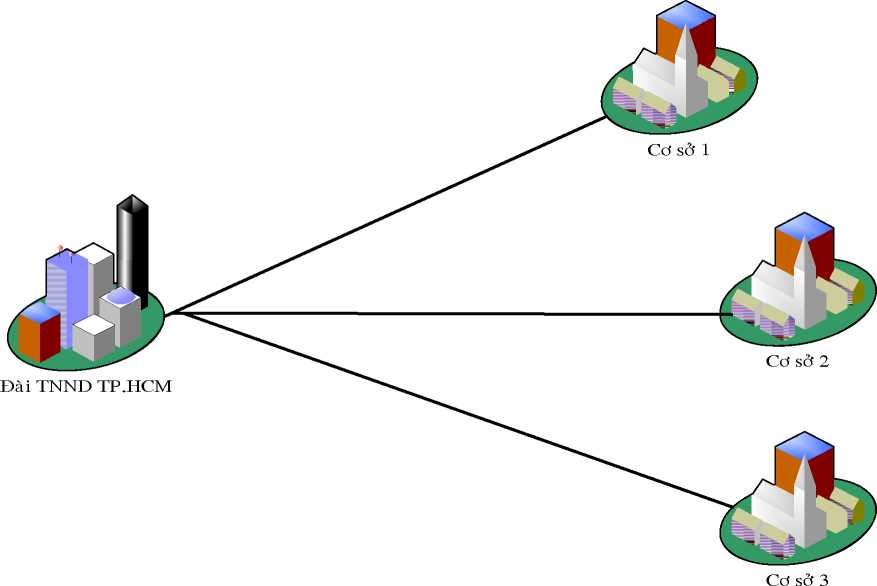
1. **Kết nốì 1 mang nôi bỏ ở xa YỞỈ hê thống:**

Do nhu cầu của công tác nghiệp vụ, Đài TNND TP.HCM dự định thiết lập thêm một số cơ sở như là các chi nhánh, mỗi chi nhánh có 1 mạng cục bộ riên). Cần thiết lập 1 kết nối mạng bảo mật giữa Đài và chi nhánh- kết nối site-to-site.

Yêu cầu cụ thể:

* Đảm bảo an toàn cho hệ thông.
* Đảm bảo an toàn cho kết nối.
* cần chú ý đến chi phí xây dựng cũng như duy trì hệ thống.

Sơ đồ mô tả yêu cầu



1. **Giải pháp thức hiên:**

Dựa trên cơ sở những cụ thể được nêu ở trên chúng ta có thể chia bài toán thành 2 phần riêng biệt có thể thực hiện độc lập với nhau:

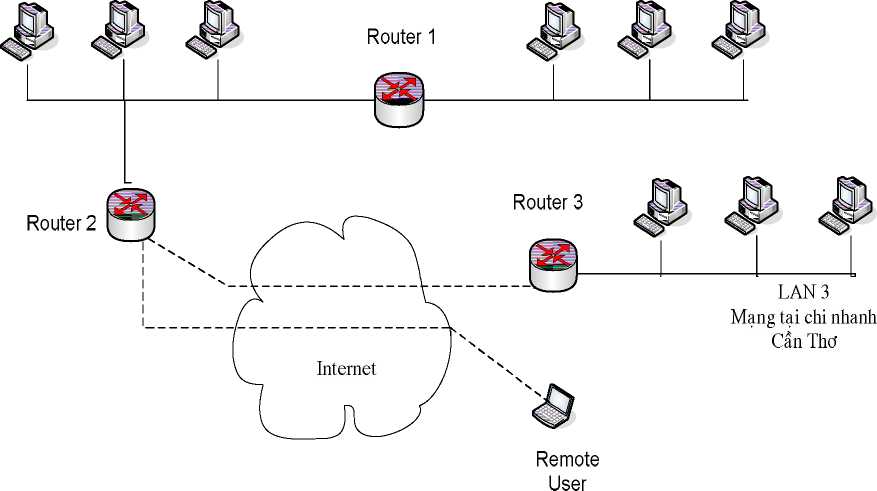
* Kết nối 2 mạng nội bộ và kiểm soát truy cập giữa chúng.
* Xây dựng một hệ thống cho phép kết nối 1 mạng ở xa (site-to-site) đồng thời cho phép một sô" người dùng có thể truy cập từ xa (Remote Access). Có rất nhiều giải pháp để giải quyết yêu cầu của bài toán, với much

đích khảo sát những phương án khả thi có thể thực hiện với hạ tầng cơ sở truyền thông của nước ta hiện nay, chúng ta sẽ giải quyết bài toán như sau:

* Dùng Access Control List để kết nôi và kiểm soát truy cập giữa 2 mạng nội bộ.
* Dùng IPSec VPN để xây dựng hệ thống kết nối site-to-site và cho phép truy cập từ xa.

Trong phạm vi đồ án này, chúng ta sẽ tập trung tìm hiểu cách thiết lập IPSec VPN - tiền đề cho việc giải quyết vấn đề chính của bài toán.

Sơ đồ mô tả hệ thông với giải pháp thực hiện



LAN 2

Mạng biên tập

LAN 1

Mạngkỹ thuật

**PHẨN II**

KIẾN THỨC CƠ SỞ

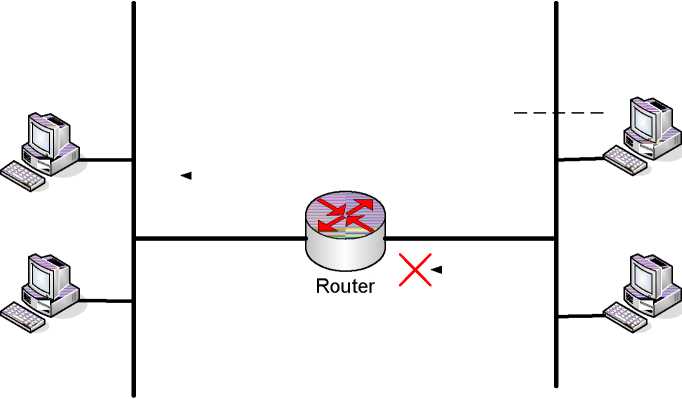
**Chương 1:**

Tổng quan Access List

Access list là kỹ thuật bảo mật (security technology) thường được sử dụng trong traffic filter và firewall, về bản chất Access list là 1 danh sách các điều kiện dùng để phân loại các packets, cho phép chúng đi qua hoặc bị chặn lại tại các router interface. Access list là cơ sở để router phân tích mỗi packet đi ngang qua interface theo 1 hướng đã được chỉ định và thực hiện, có thể được áp dụng cho cả các traffic ra và vào interface. Có thể dùng access list để:

* Cấm (restrict) các cập nhật định tuyến (routing updates).
* Cung cấp khả năng kiểm soát traffic.
* Cung cấp security cho mạng.

Sơ đồ mô tả khả năng của Access List



về cơ bản có 2 loại access list:

- Standard access list: cung cấp khả năng kiểm soát các truy cập tài nguyên của router, phân bố định tuyến (route distribution) và kiểm soát các packets đi qua router. Standard access list chỉ làm việc với các IP packets.

* Extended access list: cung cấp khả năng làm việc với nhiều protocol khác IP.

1. **Standard Access list:**

Standard Access List được dùng để xây dựng các bộ policy áp dụng cho địa chỉ IP và cho cả network number. Với các Policy được định nghĩa bằng Standard Access List, chúng ta có thể ngăn cấm việc truy xuất tới các tài nguyên của mạng, xác định các tuyến (route) được phân bố và cho phép, thay đổi metric định tuyến để điều chỉnh traffic mạng.

Những câu lệnh cấu hình Standard Access List:

* access-list access-list-number [denylpermit] source [source-wildcard] [log]

// khai báo các câu lệnh của access list

* access-list access-list-number remark text

// thêm dòng text gợi nhớ về chức năng của access list

* ip access-group {number I name[in I out]}

// áp dụng access list cho interface

* access-class number I Name [in lout]

Các câu lệnh kiểm tra cấu hình Standard Access List:

* show ip interface [type number]
* show access-list [access-list-number I access-list-name]
* show ip access-list [ access-list-number I access-list-name]

Standard access list dùng các con số từ 1 đến 99 hoặc từ 1300 đến 1999 để làm access list number ỊL Extended Access List:

Do Standrad Access List chỉ có tác dụng với IP traffic, còn đối với những protocol đặc biệt như TCP, UDP ( specific protocols port numbers) hoặc những giao thức có quan hệ với IP nên tác dụng của nó còn nhiều hạn chế. Extended Access List được sử dụng để khắc phục những hạn chế đó.

Extended Access List mở rộng thêm khả năng Standard Access List để có thể xử lý thêm các loại protocol khác ngoài IP, protocol port và đích đến theo định hướng cụ thể. Với những khả năng đó, Extended Access List thường được sử dụng cho firewall- đặc biệt là hữu dụng trong việc lọc các gói với những mức độ tin cậy khác nhau.

Các cấu hình Extended access list:

* access-list access-list-number [denylpermit] protocol source [source- wildcard] destination [destination-wildcard] [log I log-input]

// khai báo các câu lệnh của access list

* access-list access-list-number [denylpermit] tcp source [source- wildcard] [operatior [port]] destination [destination-wildcard] [operatior [port]] [established] [log I log-input]

// 1 dạng lệnh access list với các thông số của TCP.

* access-list access-list-number remark text

II thêm dòng text gợi nhớ về chức năng của access list

* ip access-group {number I name[in I out]}

// áp dụng access list cho interface

* access-class number I Name [in lout]

Các câu lệnh kiểm tra cấu hình Standard Access List:

* show ip interface [type number]
* show access-list [access-list-number I access-list-name]
* show ip access-list [ access-list-number I access-list-name]

Extended access list dùng các con số từ 100 đến 199 hoặc từ 2000 đến 2699 để làm access list number . Ta có thể kiểm tra tất cả các gói với TCP hoặc UDP header, có thể cấm hoặc cho phép các dịch vụ theo port number bằng thông số : eq [port number].

1. **Ap dung Access list:**

Mặc dù mỗi protocol có những qui luật và nhiệm vụ đặc trưng riêng cần phải lưu ý khi ta sử dụng traffic filter, nhưng nói chung việc cấu hình Access list bao gồm 2 bước cơ bản cần thực hiện:

* Tạo Access List: tạo ra bộ lọc (filter).
* Ap dụng Access list lên các interface của Router : sử dụng các bộ lọc vừa tạo ra để lọc (filtering).

1. **Tao Access List:**

Để tạo một Access List, Chúng ta phải thực hiện các bước sau:

* Xác định rõ protocol nào muốn lọc (filter).
* Ấn định một cái tên hoặc một con số để phân biệt cho Access List.
* Định nghĩa tiêu chuẩn của việc lọc gói- một Access List có thể có nhiều khai báo tiêu chuẩn lọc phức tạp.

Một số điểm cần lưu ý khi tạo Access List:

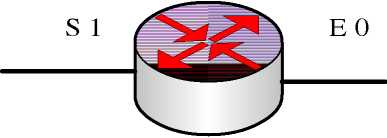
* Việc tạo 1 access list thực sự giống như việc lập trình với 1 chuỗi các câu phát biểu If- then, nghĩa là nếu gặp 1 điều kiện thì 1 hành động được thực thi, ngược lại điều kiện tiếp theo sẽ được xem xét.
* Các tiêu chuẩn Access list (Access list criteria) có thể là địa chỉ nguồn của traffic, địa chỉ đích của traffic, những giao thức của các lớp trên của mô hình OSI hoặc những thông tin khác.
* Với một Access list đơn, chúng ta có thể định nghĩa một tiêu chuẩn phức tạp bằng câu lệnh phức hợp hoặc bằng những câu lệnh riêng rẽ- các câu lệnh riêng rẽ của một Access List có cùng tên hoặc số nhận dạng của Access List, số lượng câu lệnh không bị hạn chế về số lượng, chỉ phụ thuộc vào dung lượng bộ nhớ của thiết bị. Tuy nhiên cần lưu ý rằng độ phức tạp sẽ tăng theo số lượng câu lệnh, sẽ khó nắm rõ và quản lý hiệu quả các Access list.
* Mặc định khi áp dụng Access List tất cả các packet không được cho phép sẽ bị cấm mà không cần khai báo, tuy vậy câu lệnh kết thúc của các Access List là câu lệnh cấm tất cả các traffic ( deny all traffic), cần chú ý là đối với hầu hết các protocol, nếu chúng ta định nghĩa một Access List cho 1 filter lọc traffic theo hướng đi vào mạng thì nhất thiết phải sử dụng câu lệnh cho phép cập nhật các thông tin định tuyến nếu không thì tất cả các packet đều bị khoá do đặc tính cấm mặc định của Access List.
* Một vấn đề nữa cần chú ý khi cấu hình một Access List là thứ tự của các câu lệnh. Trình tự các câu lệnh sẽ quyết định cách làm việc của Access List, các câu lệnh đặt không đúng thứ tự sẽ vô hiệu hóa tất cả những câu lệnh sau đó. Thông thường khi có các câu lệnh cho phép được thực hiện thì các câu lệnh s về au đó không có tác dụng nữa thay vào đó là tính năng cấm mặc định- Deny all traffic.
* Chúng ta không thể thêm các câu lệnh vào một Access List có sấn. Khi cần bổ sung Ta phải xoá Access List cũ và nhập lại.

1. **Ap dung các Access List lên các Router Interface:**

Sau khi được định nghĩa, tùy theo yêu cầu thực tế các Access List sẽ được khai báo áp dụng trên những interface cụ thể của thiết bị. Một Access list có thể được áp dụng cho nhiều interface và một interface có thể được áp dụng nhiều Access List cho những protocol khác nhau.

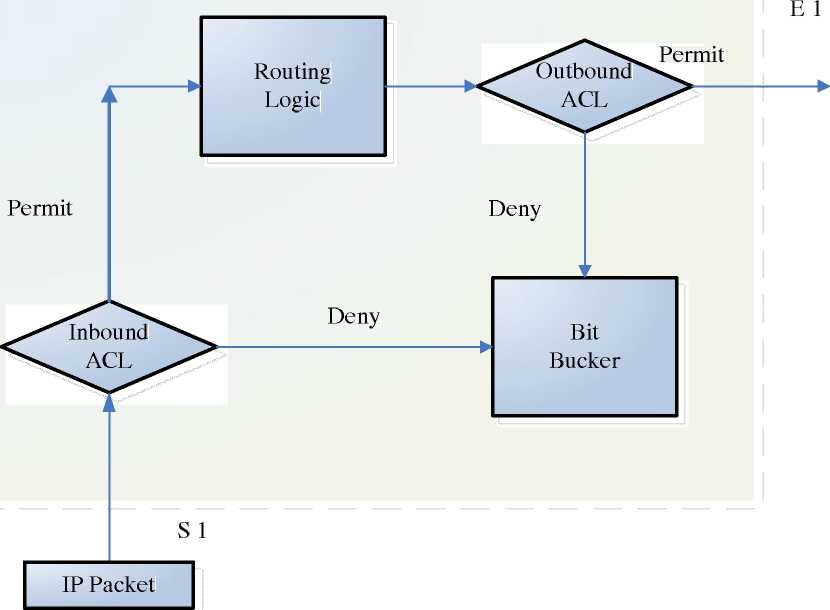
Khi áp dụng Access list ngoài việc chọn Interface, chúng ta còn cần phải chọn hướng của traffic cần kiểm soát. Sơ đồ dưới đây mô tả logic hoạt động của access list trong Router:

Minh họa về việc áp dụng access list



Router RI

Router RI



Theo lưu đồ trên, khi áp dụng 1 Access list, ta có thể dùng nó cho khi Packet vào (Inbound) hoặc khi Packet ra khỏi (Outbound) Router.

Đối với một số protocol, tại một interface Ta phải dùng 2 Access List, mỗi Access List kiển soát traffic theo một hướng riêng. Với một số protocol chỉ cần dùng 1 Access List cho cả 2 hướng.

1. Mốt số điểm cần chú V khi sử dung Access list:

Khi tạo và áp dụng access list trong hệ thống cần lưu ý:

* Có thể tạo Access list bằng các ứng dụng text editor ở ngòai Router, sau đó chép vào Router.
* Các Extended access list nên được đặt càng gần nơi xuất phát của các packet cần kiểm tra thì hiệu quả càng cao.
* Các Standard Access list nên được đặt gần đích đến của các Packet nhằm tránh việc đánh rớt các gói ngoài ý muốn.
* Nên để những câu lệnh quan trọng lên phía trước của access list.
* Nên vô hiệu Access list trên interface trước khi thực hiện bất cứ thay đổi nào về nội dung của Access list.
* Khi cần bổ sung thêm cho Accès list hiện có chúng ta phải khai báo lại tòan bộ Access list với những điều kiện mới thêm vào.

Nói chung Access list là một kỹ thuật tương đối đơn giản nhưng hiệu quả thường sử dụng để hỗ trợ cho công tác bảo mật của mạng như: kiểm soát traffic mạng, kiểm soát việc truy cập thiết bị mạng, ứng dụng trong firewall....

**Chương II;**

Tổng quan về mạng riêng ảo YPN

1. **Khái niêm về VPN:**

Mạng riêng ảo VPN- Virtual Private network là một công nghệ cho phép thực hiện các giao dịch riêng tư dựa trên các hệ thống công cộng, chẳng hạn như Internet, một cách an toàn và hiệu quả.

Virtual Private Network là một thuật ngữ để chỉ một mạng máy tính có các đặc tính:

* Ấo (virtual): vì truyền thông tin dựa trên kết nối logic, trong thực tế một đường hầm (tunnel) sẽ được tạo giữa hai đầu truyền tin bằng kỹ thuật đóng gói và mã hoá riêng.
* Riêng (Private): vì cho phép người dùng (user) truyền thông tin riêng tư một cách an toàn, bảo mật trong mội trường công cộng.

Có thể định nghĩa VPN 1 cách ngắn gọn qua công thức sau:

VPN= định đường hầm + bảo mật + các thoả thuận về QoS QoS chất lượng dịch vụ được cung cấp.

1. **Những lơi ích do VPN đem lai:**

Công nghệ mạng riêng ảo VPN có những ưu điểm đem lại những lợi ích thực sự sau:

* Giảm chi phí đầu tư.
* Giảm chi phí quản lý và duy trì hệthống.
* Giảm chi phí thường xuyên so với những hệ thống khác.
* Cho phép truy cập dễ dàng thông qua các hệ thống công cộng.
* Giải quyết được vấn đề bảo mật trong môi trường mạng công cộng.
* Tăng hiệu quả sử dụng của băng thông
* Khả năng phát triển cao

1. **Những han chế còn tổn tai của VPN:**

Những khuyết điểm của VPN còn tồn tại của VPN gồm:

* Phụ thuộc Internet.
* Thiếu sự hỗ trợ đối với các giao thức kế thừa, do được xây dựngchủ yếu dựa trên kỹ thuật IP.

1. **Những ván để cán quan tâm khỉ thiết lân VPN:**

Khi lực chọn giải pháp mạng dựa trên công nghệ VPN cần chú ý đến những vấn đề sau:

* Security: nên xem xét áp dụng những cơ chế bảo mật và giải thuật mã hóa mạnh nhằm đảm bảo tính an toàn của dữ liệu.
* Khả năng làm việc của các thiết bị của các nhà sản xuất khác nhau, cần phải kiểm tra trước tính tương thích của chúng để đảm bảo hệ thống hoạt động ổn định.
* Nên có sự quản lý tập trung.
* Giải pháp VPN phải dễ thực hiện và cấu hình.
* Các VPN software đặc biệt là VPN client software phải đơn giản, dễ hiểu, dễ sử dụng đối với người dùng.
* Phải có khả năng tương thích cao, có khả năng đáp ứng được những yêu cầu phát triển trong tương lai với những thay đổi tối thiểu về cấu trúc.
* Cần xem xét đến hiệu suất của hệ thống khi thực hiện các thuật toán và cơ chế mã hoá.
* Băng thông có ảnh hưởng quan trọng đến hiệu suất, khả năng hiệu dụng và đảm bảo về QoS.
* Việc lựa chọn ISP cũng là 1 việc quan trọng cần xem xét.
* Vì VPN sẽ kết nối trực tiếp với Internet nên việc bảo vệ hệ thống khỏi những traffic không mong muốn hoặc không được phép là cực kỳ quan trọng cần chú ý đặc biệt.

1. **Môt số** **thuât ngữ liên quan đến VPN:**

* Tính bảo mật: bảo mật là những gì làm cho VPN trở nên “ảo” và “riêng”. Nhờ đó mà hệ thống sử dụng các tài nguyên công cộng vẫn có những đặc tính như hệ thống được xây dựng riêng biệt, tiết kiệm đáng kể về chi phí. Việc đảm bảo tính bảo mật cho các kết nối VPN được thực hiện bằng cách kết hợp các sản phẩm và công nghệ với nhau.
* Đường hầm (Tunnel) : các đường hầm chính là đặc tính ảo của VPN, nó làm cho kết nối trở nên trong suốt (không thấy được) đối với các người dùng khác trên Internet, đồng thời tạo cho VPN khả năng duy trì những yêu cầu về bảo mật và quyền ưu tiên như đã được áp dụng trong mạng nội bộ. Những công nghệ đường hầm phổ biến cho truy cập VPN gồm: PPTPÌ L2TP va IPSec.
* Mã hóa : đây là tính năng tùy chọn làm nên tính “riêng tư” của VPN. Chỉ nên mã hóa những dữ liệu quan trọng để không ảnh hưởng đến tốc độ xử lý của CPU.
* Tường lửa : Firewall được dùng để bảo mật mạng nội bộ chống lại các cuộc tấn công từ bên ngoài. Firewall tốt có khả năng phân biệt các traffic dựa trên cơ sở người dùng, trình ứng dụng hay nguồn gốc.
* Định danh người dùng (User-Identification) : mọi người dùng đều phải chịu sự kiểm tra xác thực để hệ thống có thể biết thông tin về họ (quyền truy cập, mật khẩu..) và phải chịu sự ủy quyền để báo cho họ biết về những gì họ được phép làm. Một hệ thống tốt còn thực hiện việc tính toán để theo dõi những việc mà người dùng đã làm nhằm much đích tíng cước và bảo mật. Xác thực( Authentication), trao quyền (Authorization) và tính cước (Accouting) được gọi là các dịch vụ AAA.
* Tính ưu tiên: Cho phép gán thẻ ưu tiên cho 1 traffic của 1 ứng dụng nghiệp vụ quan trọng cần thực hiện trước. Khả năng gán ưu tiên sẽ phải độc lập với dữ liệu truyền để đảm bảo tính hoàn hảo thực sự của dịch vụ.

**ỊL Các loai mang VPN:**

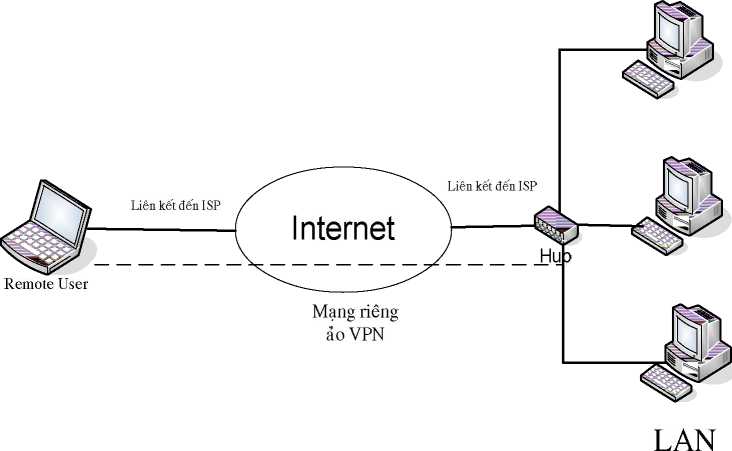
Có thể phân VPN ra làm 3 loại:

* Remote access VPN.
* Intranet VPN.
* Extranet VPN.

1. **Các VPN truy câp từ xa (Remote Access VPN):**

Các VPN này cung cấp truy cập tin cậy cho các người dùng ở xa như các nhân viên di động, các nhân viên ở xa và các văn phòng chi nhánh thuộc mạng lưới công ty. Người dùng có thể truy cập các tài nguyên VPN bất cứ khi nào nếu cần.

Đường truyền trong Access VPN có thể là tương tự, quay số, ISDN, các đường thuê bao số (SDL), IP di động và cáp để nối các người dùng di chuyển, máy tính từ xa hay các văn phòng lại với nhau.



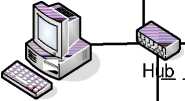
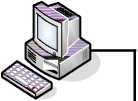
1. **Các VPN nối bô (Intranet VPNÌ:**

Cho phép các văn phòng chi nhánh được liên kết 1 cách bảo mật đến trụ sở chính của công ty.

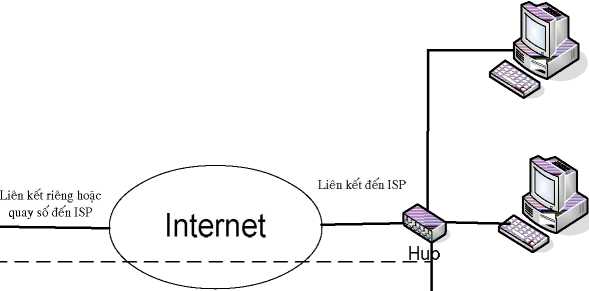
Có 2 phương pháp sử dụng mạng VPN để kết nối các mạng cục bộ LAN tại các điểm cuối ở xa:

* Dùng các đường kênh thuê riêng để kết nối.
* Dùng đường dây quay số để kết nối.

Dùng VPN để kết nốì 2 yị trí từ xa

LANA

LAN B

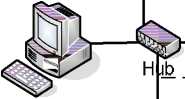
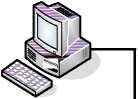


Mạng riêng ảo VPN

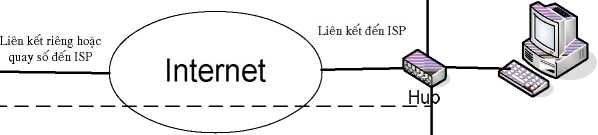
1. **Các VPN mđ rông (Extranet VPNÌ:**

Cho phép các khách hàng, các nhà cung cấp và các đối tác có thể truy cập 1 cách bảo mật đến mạng Intranet của công ty.

Dùng VPN để kết nốì 2 máy tính từ xa trong cùng 1 mạng LAN

LANA

LANA



Mạng riêng ảo VPN

**ĨĨL Kiến trúc và các khôi của VPN**

1. **Kiến trúc của 1 mang VPN:**

Hai thành phần cơ bản tạo nên mạng riêng ảo VPN là:

* Tiến trình định đường hầm (Tunneling), cho phép làm “ảo” một VPN.
* Những dịch vụ bảo mật đa dạng nhằm giữ cho dữ liệu của VPN được bảo mật.

a. **Đinh đường hầm:**

Việc tạo đường hầm là tạo ra một kết nối đặc biệt giữa 2 điểm cuối. Để tạo ra 1 đường hầm.

* Điểm nguồn phải đóng gói (encapsulate) các gói (Packet) của mình trong các gói IP (IP packet) để truyền qua mạng Internet- việc đóng gói bao gồm mã hoá gói gốc và thêm 1 tiêu đề IP (IP header) mới cho gói.
* Tại điểm cuối đích, cổng nối sẽ gỡ bỏ tiêu đề IP và giải mã cho gói và chuyển nó đến đích cần đến.

Gói kiểu đường hầm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | AH | ESP | header | Data |

Gói gốc

Việc tạo đường hầm cho phép các dòng dữ liệu và thông tin người dùng kết hợp được truyền trên mạng công cộng ữong một ống ảo (Virtual pipe), ống ảo sẽ làm cho việc định tuyến trên mạng trở nên trong suốt đối với người dùng.

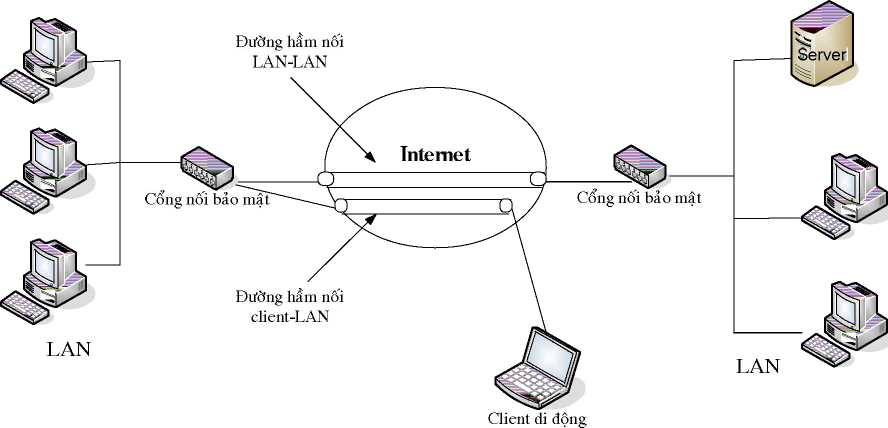
Thông thường đường hầm được địng nghĩa theo 2 loại: đường hầm tĩnh (Static tunnel) và đường hầm động (dynamic tunnel).

* Đường hầm tĩnh hay còn gọi là đường hầm thường trực (pernament) thường ít được dùng vì chiếm băng thông khi không sử dụng.
* Đường hầm động còn gọi là đường hầm tạm thời thường được sử dụng. Khi có yêu cầu đường hầm sẽ được thiết lập sau đó sẽ hủy bỏ khi không dùng đến.

Ngoài ra khi nói đến đường hầm, ta còn cần phải xem xét đến các điểm cuối của đường hầm (endpoint), có 2 loại điểm cuối:

* Máy tính đơn, khi kết nối phải chạy 1 phần mềm VPN Client.
* Mạng LAN với cổng nối bảo mật có thể làbộ địng tuyến hay tường lửa.

Các đường hầm VPN



b. **Các dich YU báo mât trong VPN:**

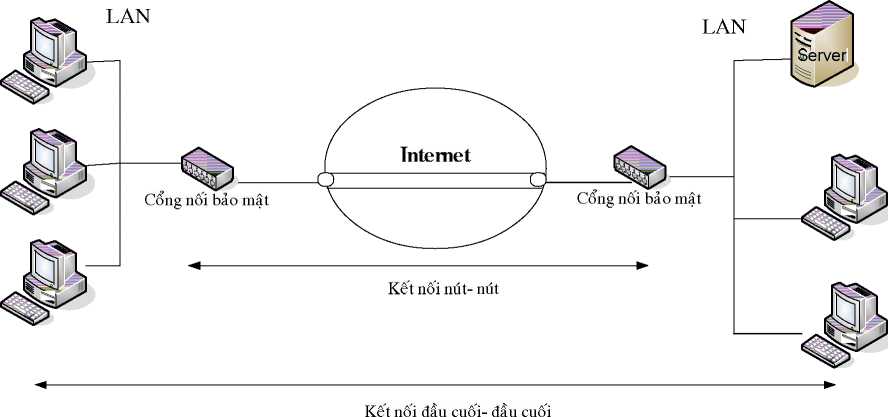
Mạng VPN cần được cung cấp 4 chức năng giới hạn để đảm bảođộ bảo mật cho dữ liệu. Bốn chức năng đó là:

* Xác thực (Authentication ): xác định nguồn gửi dữ liệu.
* Điều khiển truy cập (Access control): hạn chế những truy cập trái phép vào mạng.
* Tin cậy (Confidentality): đảm bảo ngăn những người không được phép đọc dữ liệu khi truyền trên mạng.
* Tính toàn vẹn của dữ liệu (Data integrity) : đảm bảo dữ liệu không bị thay đổi trong quá trình truyền trên mạng.

Việc xác thực người dùng và duy trì tính toàn yẹn của dữ liệu phụ thuộc vào các tiến trình mật mã (Cruptographic). Những tiến trình này sử dụng các bí mật được chia sẽ gọi là khoá (key) , việc quản lý và phân phối các khóa cũng tăng tính bảo mật của hệ thống.

Các dịch vụ Xác thực, mã hóa vàtoàn vẹn dữ liệu được cung cấp tại lớp Dta-link và lớp Network của mô hình OSI. Việc phát triển các dịch vụ bảo mật tại các lớp thấp của mô hình OSI làm cho các dịch vụ này trở nên trong suốt hơn với người dùng.

Có 2 hình thức áp dụng các dịch vụ bảo mật:

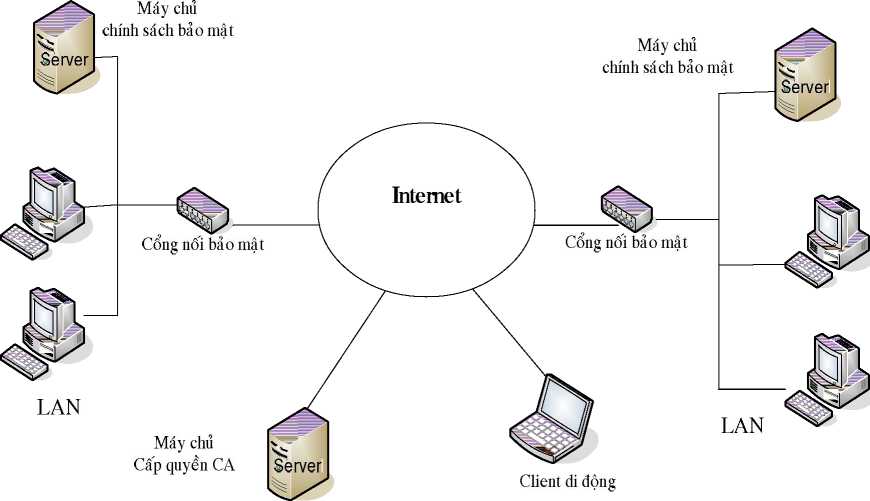


Mỗi hình thức kết nối có những ưu khuyết điểm khác nhau: kết nối đầu cuối- đầu cuối bảo mật hơn kết nối nút- nút nhưng nó làm tăng sự phức tạp cho ngưới dùng và có thể gây khó khăn hơn cho việc quản lý.

1. **Các khối trong mang VPN:**

Mạng Internet VPN cgồm các thành phấn chính sau:

* Internet.
* Cổng nối bảo mật.
* Máy chủ chính sách bảo mật (secutiry policy server).
* Máy chủ cấp quyền CA (certificate authority).



Các cổng nối bảo mật (security gateway) được đặt giữa các mạng công cộng và mạng riêng, ngăn chặn các xâm nhập trái phép vào mạng riêng. Chúng thể cung cấp khả năng tạo đường hầm và mã hóa dữ liệu trước khi chuyển đến mạng cộng cộng, cổng nối bảo mật cho mạng VPN gồm 1 trong các loại sau: bộ định tuyến (Router), tường lửa (firewall), phần mềm tích hợp VPN và phần mềm VPN.

Một thành phần quan trọng khác của mạng VPN là máy chủ chính sách bảo mật (security policy server). Máy chủ này bảo quản các danh sách điều khiển truy cập và các thông tin khác liên quan đến người dùng, những thông tin này được cổng nối dùng để xác các traffic nào được phép lưu thông.

Các máy chủ cấp quyền CA được để xác thực các khóa dùng chung để cấp quyền cho các người dùng thuộc hệ thống.

**III. Các giao thức trong VPN:**

1. **Các giao thức đường hẩm và báo mât:**

Việc truyền dữ liệu thông qua bất kỳ một phương tiện nào cũng phải tuân theo những giao thức nhất định. Đối với VPN, việc bảo vệ kênh giao tiếp riêng được thực hiện bằng kỹ thuật mã hoá ( ví dụ như DES hoặc 3DES) thông qua các giao thức bảo mật. Việc mã hoá có thể được thực hiện tại các tầng khác nhau trong kiến trúc OSI.

1. **Bô giao thức IP Security (IPSec):**

Much đích của bộ giao thức IPSec là đảm bảo tính bí mât, toàn vẹn và xác thực của thông tin trên nền giao thức Internet (IP). Bộ giao thức IPSec sử dụng kết hợp một số giao thức mã hoá mạnh có khả năng giải quyết các vấn đề bảo mật trong các mạng huyền thông dựa trên nền IP bao gồm:

* Internet Key Exchange (IKE): cung cấp một phương thức trao đổi khóa an toàn giữa các đối tác. Để làm việc đó giao thức IKE hỗ trợ các giải thuật mã hoá 3DES, giải thuật chia Tiger, giải thuật chữ ký điện tử RSA, giải thuật xác thực MD5....
* Encapsulating Security Payload (ESP): sử dụng các kỹ thuật mã hoá mạnh (RC5, 3DES, Blowfish...) để đóng gói thông tin để sau đó chỉ có người nhận thông tin có khóa bí mật mới đọc được. Ngoài ra ESP còn cung cấp khả năng che giấu thông tin về địa chỉ IP của người gửi và người nhận.
* Authentication Header (AH): giao thức này gắn các dữ liệu trong các gói (packet) với chữ ký điện tử cho phép người nhận kiểm tra danh tính người gửi cũng như tính toàn vẹn của thông tin.

IPSec hiện đang trở thành một phương tiện bảo mật giao tiếp chuẩn cho các nhà cung cấp.

1. **Giao thức PPTP và giao thức L2TP:**

Ngoài giao thức IPSec, người dùng cò có thể sử dụng 2 giao thức khác là PPTP (Point-to-Point Tunneling protocol) và L2TP (Layer 2 Tunneling Protocol). Cả hai giao thức này đã được tích hợp vào hệ điều hành Windows.

* Giao thức PPTP: có nguồn gốc từ giao thức ppp ( Point-to-Point Protocol) dùng trong kết nối mạng Internet qua đường quay số Dial-up, được xây dựng dựa trên Microsoft Point-to-Point Encryption (MPPE).
* Giao thức L2TP: là chuẩn mở được tích hợp giữa giao thứcPPTP của Microsoft và L2F của Cisco Systems.

1. **Các giao thức quán tri:**

Các giao thức quản trị được dùng để duy trì quyền truy cập cuả người dùng cùng với những thông tin bảo mật hên quan đến họ. Hai họ giao thức khác nhau hiện nay được sử dụng tùy theo loại mạng VPN cần quản lý:

* Đối với mạng quy số VPN hay kết nối client-LAN dùng đường hầm PPTP và L2TP dùng giao thức RADIUS để xác thực và tính cước.
* Đối với mạng LAN-LAN giao thứ ISAKMP/Oakley được sử dụng như 1 biến thể của IPSec.

Nhiều phương thức xác thực và mã hóa sử dụng trong mạng VPN yêu cầu xác định và phân phối các khóa dùng chung. Đối với những hệ thống nhỏ, việc phân phối các khóa được thực hiện bằng tay. Đối với những hệ thống lớn thì cần có 1 hệ thốngtạo ngẫu nhiên, quản lý và phân phối khóa tự động- key management system.

1. **Mã hỏa thống tin và tích hựp báo mật trong VPN:**
2. **Mã hoá thông tin:**

Hiện nay tồn tại 2 hệ thông mã hóa dựa ữên các giải thuật đối xứng (Symmetric) và không đối xứng (asymmeữic):

* Giải thuật Symmetric cho phép thông tin mã hoá và giải mã sử dụng một khóa bảo mật duy nhất.
* Giải thuật Asymmetric hay còn gọi là giải thuật khóa công khai (public- key) cho phép thông tin được mã hóa và giải mã sử dụng một cặp khóa liên đới, trong đó một khóa được giữ bí mật và một khóa công khai.

Kích thước khóa càng lớn thì độ an toàn của thông tin càng tăng lên nhưng hiệu suất xử lý thông tin càng giảm đi. Tùy thuộc vào từng ứng dụng cụ thể, kích thước khóa có thể thay đổi, ví dụ như kích thước khóatrong một số giải thuật sử dụng CBC-mode như CAST-128 (40-128 bits), RC5 (40-2040 bit), 3DES (192 bit), Blowfish (40-448bit)...

1. **Tích hơp bảo mât:**

VPN cho phép tích hợp nhiều đặc tính bảo mật nhằm nâng cao mức độ an tòan cho thông tin. Hiện có rất nhiều giải pháp cho vấn đề này, điển hình là 3 giải pháp sau:

* SSH ( Secure Shell): là chương trình bảo mật thay thế cho các công cụ truy cập từ xa khác như telnet,rlogin, ftp và các công cụ khác không được trang bị tính năng bảo mật. SSH cung cấp kênh giao tiếp thông tin mã hoá, ví dụ như từ một máy ở xa đến máy chủ POP3.
* SSL (Secure Sockets Layer): là giao thức dùng để cung cấp khả năng mã hóa mạnh khi truyền dữ liệu. Các giải pháp dựa trên SSL được chia thành hai loại là kết nối và đường hầm. Kết nối cung cấp sự bảo vệ cho một ứng dụng đơn lẻ sử dụng SSL, đường hầm SSL cho phép một hoặc nhiều ứng dụng truyền tin bảo mật qua mạng công cộng sử dụng SSL hoặc không.

- Giải pháp dùng các phần mềm truy cập từ xa cho phép người dùng từ bên ngoài có thể truy cập vào mạng cục bộ thông qua Internet, qua đó người dùng truy cập từ xa có thể truy xuất các ứng dụng, file và các tài nguyên khác trong mạng cục bộ.

Tuy nhiên, mặc dù SSH, SSL và IPSec có thể cung cấp các khả năng mã hóa thông tin tương tự nhau, nhưng thiết lập VPN sử dụng IPSec có nhiều thuận lợi hơn. Chẳng hạn như : đối với những ứng dụng khác nhau chúng ta cần mở các kết nối và đường hầm SSH và SSL khác nhau cho từng ứng dụng trong khi IPSec chỉ cần một kết nối chung cho tất cả các ứng dụng, thêm vào đó còn có khả năng che giấu địa chỉ IP- đây là một đặc tính cần thiết trong một số tình huống đặc biệt. Hiện nay trong giao thức Internet phiên bản IPv6, IPSec được xem là một thành phần bắt buộc và được cài đặt như một chức năng cơ sở.

1. **Đáng giá chung về VPN:**

Tóm lại VPN là 1 giải pháp nhanh chóng và hiệu quả hơn về chi phí so với các giải pháp mạng diện rộng WAN khác. Mạng riêng ảo đã thể hiện sự đột phá công nghệ, làm chuyển biến ngành công nghiệp và cách mạng hóa các dịch vụ do khách hàng yêu cầu. Hiện nay có nhiều vấn đề trong thực tế đang thúc đẩy việc khai thác VPN 1 cách rộng rãi, những thúc đẩy này có thể đưa đến sự phát triển vượt bậc của VPN.

**Chương III;**

Tổng quan về giao thức IPSec

1. **Khái niệm chung về IPSec:**

IPSec- Internet Protocol Security là một bộ giao thức có chuẩn mở đang được tổ chức Internet Engineering Task Force (IETF) phát triển nhằm hỗ trợ sự trao đổi an toàn các gói dữ liệu IP. Các bộ giao thức này cung cấp khả năng xác thực nguồn gốc, bảo vệ sự toàn vẹn và tin cậy của dữ liệu, khả năng bảo vệ chông replay. IPSec hoạt động trên giao thức IP và sử dụng Internet Key Exchange (IKE) để đàm phán các kết hợp bảo mật security association (SA) giữa các peer.

IPSec có thể được sử dụng độc lập như là 1 phương thức bảo mật trong trao đổi dữ liệu hoặc được dùng kèm trong các giải pháp mạng khác như VPN chẳng hạn.

IPSec hoạt động tại lớp thứ 3 (Network layer) của mô hình OSI:

Application Layer

Presentation Layer

Section Layer

Transport Layer

Network Layer

***IPSec***

DataLink Layer

Physical Layer

1. **Các giao thức của IPSec:**

Các giao thức thường gặp khi làm việc với IPSec gồm:

* IPSec (IP Security Protocol): các giao thức cung cấp traffic security.

o Authentication Header (AH), o Encapsulating Security Payload (ESP).

* Message Encrytion

o Data Encrytion Standard (DES). o Triple DES (3DES).

* Message Integrity (Hash) Function.

o Hash-based Message Authentication Code (HMAC). o Message Digest 5 (MD5). o Secure Hash Algorithm-1 (SHA-1)

* Peer Authentication

o Revset, Shamir, and Adelman (RSA) Digital Signatures, o RSA Encrypted Nonces.

* Key Management

o Deffie- Heilman (D-H). o Certificate Authority (CA).

* Security Association

o Internet Key Exchange (IKE).

o Internet Security Association and Key Management Protocol (ISAKMP).

1. **Mot** số' **chứ** V **khi ứng dung IPSec:**

* IPSec hỗ trợ High-Level Data-Link Control (HDLC), ATM, Point-to- Point Protocol (PPP), và Frame Relay seria encasulation.
* IPSec cũng làm việc với Generic Routing Encapsulation (GRE) và IP-in- IP Encapsulation Layer 3 tunneling Protocols.
* IPSec không hỗ trợ chuẩn data-link switching (DLSw), source-route bridging (SRB), hoặc những giao thức đường hầm Layer 3 khác.
* IPSec cũng không hỗ trợ đường hầm nhiều điểm (Multipoint tunnel).
* IPSec chỉ làm việc với unicast IP-datagram, không làm việc với multicast hoặc broadcast datagram.
* IPSec chậm hơn CiscoEncryption Technology (CET) vì IPSec cung cấp per-packet data authentication.
* IPSec cho phép thay đổi kích thước của các packet, từ đó chúng ta có thể chia nhỏ các gói lớn thành các gói nhỏ hơn trong quá trình truyền sau đó tái tạo lại tại nơi nhận. Việc này cũng là một trong nguyên nhân làm cho IPSec chậm hơn CET.
* Khi sử dụng NAT, phải thực hiện NAT trước khi IPSec đóng gói dữ liệu.

1. **Dang thức của IPSec:**

Hoạt động của IPSec ở mức cơ bản đòi hỏi phải có các phần chính sau:

* Kết hợp bảo mật SA (Security Association).
* Xác thực tiêu đề AH (Authentication Header).
* Bọc gói bảo mật tải ESP (encapsulating Security Payload).
* Chế độ làm việc

1. **Kết hỢp báo mật SA:**

Security Associations (SAs) là khái niệm cơ sở nền tảng của bộ giao thức IPSec. Để 2 đầu có thểtruyền dữ liệu đã được bảo mật (được xác thực và mã hóa), thì cả 2phải cùng thống nhất về giải thuật mã hóa, cách chuyển khóa và thời gian đổi khóa- tất cả những thông tin trên đều do SA đảm trách.

Việc truyền thông giữa bên gửi và bên nhận đòi hỏi ít nhất 1 SA, có thể nhiều hơn do các giao thức của IPSec cần có 1 SA riêng cho từng giao thức, mỗi gói xác thự cũng cần 1 SA riêng và mỗi gói mã hóa cũng vậy. Thậm chí nếu dùng chung giải thuật cho việc xác thực và mã hóa cũng cần phải có 2 SA khác nhau do dùng 2 bộ khóa khác nhau.

Một IPSec SA được định nghĩa bao gồm:

* Giải thuật xác thực sử dụng cho AH và khóa của nó.
* Giải thuật mã hóa ESP và khóa của nó.
* Dạng thức và kích thước của bộ mật mã sử dụng trong giải thuật mã hóa.
* Giao thức, giải thuật và khóa sử dụng cho việc truyền thông.
* Giao thức, giải thuật mã hóa, khóa sử dụng cho việc truyền thông riêng.
* Thời gian thay đổi khóa.
* Giải thuật xác thực, kiểu, chức năng sử dụng trong ESP và khóa được sử dụng trong giải thuật.
* Thời gian tồn tại của khóa.
* Thời gian tồn tại của SA.
* Địa chỉ nguồn của SA.

Có thể xem SA như 1 kênh bảo mật thông qua 1 mạng công cộng đến 1 người hay 1 nhóm làm việc cụ thể.

1. **Xác thức tiêu để AH:**

Xác thực tiêu đề AH- Authentication Header được sử dụng cho các dịch vụ xác thực. AH được chèn vào giữa tiêu đề IP và nội dung phía sau, nội dung của gói không bị thay đổi.

IP Header

AH Header

Payload

Tiêu đề xác thực gồm 5 trường:

- Trường tiêu đề kế tiếp (Next header Field): nhận diện giao thức bảo mật.

- Chiều dài tải (Payload length): xác định chiều dài của message theo sau AH Header.

* Chỉ tham số bảo mật SPI (Security Parameter Index): thông báo cho thiết bị nhận gói biết họ giao thức bảo mật phía gửi dùng trong truyền thông.
* Số tuần tự (sequence number)
* Dữ liệu xác thực (Authentication Data): mang thông tin về giải thuật mã hóa định nghĩa bởi SPI.

AH cung cấp các dịch vụ (Service): bảo đảm tính tòan vẹn của data, xác thực tính toàn vẹn của data, và antireplay. Những thuật toán xác thực được dùng trong AH là: HMAC-MD5 và HMAC-SHA1.

AH không cung cấp khả năng mã hoá

Định dạng của AH header

|  |  |  |
| --- | --- | --- |
| Original IP | Original Layer | Data |
| Header | 4 |  |

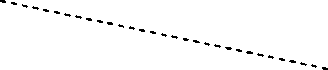
**Sequence Number Field**

Authentication Data (Variable Length- Integral Multi of

32 bits)

/ \

|  |  |  |  |
| --- | --- | --- | --- |
| Original IP | IPSec AH | Original Layer | Data |
| Header | 4 |  |



|  |  |  |
| --- | --- | --- |
| Next | Payload | Reserved |
| TTpadpr | lpmith |  |

Security Parameters Index (SPI)

1. **Boc gỏi báo mât tái ESP:**

Bọc gói bảo mật tải ESP- Encapsulating Security Payload được sử dụng cho việc mã hóa dữ liệu. Cũng như AH, tiêu đề ESP được chèn vào giữa tiêu đề IP và nội dung tiếp theo của goí. Tuy nhiên nội dung của gói sẽ bị thay đổi.

ESP cung cấp thêm khả năng tin tưởng trong việc xác thực người gửi và bảo đảm sự tòan vẹn dữ liệu. ESP mã hóa nội dung Datagram bằng các thuật toán mã hóa cao cap như: DES-CBG, NULL, CAST-128, IDEA va 3DES. Thêm vào đó ESP cũng sử dụng những thuật toán xác thực đã được dùng trong AH như: HMAC-MD5 và HMAC-SHA.

ESP không bảo vệ toàn bộ Datagram mà chỉ bảo vệ payload. Gói IP packet khi được thêm ESP header và trailer:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP Header | ESP Header | Payload | ESP Trailer | ESP Authentication |

Định dạng của ESP Header:

Security Parameter Index

ESP header TCP and Data

ESP trailer

Sequence Number

Authentication

Payload (variable)

Padding

Pad length Next

Authentication Data  
(variable size)

Encrypted

Như vậy là ESP cung cấp khả năng mã hóa và tùy chọn xác thực. Việc sử dụng ESP sẽ làm giảm kích thước các packet, làm tăng hiệu quả xử lý.

1. **Chế đô làm vỉêc:**

Có 2 chế độ làm việc trong IPSec:

* Chế độ giao vận (Transport mode): chỉ có đoạn lớp giao vận trong gói được xử lý.
* Chế độ đường hầm (Tunnel mode): toàn bộ gói sẽ được xử lý- mã hóa và xác thực.

Cả 2 chế độ đều có thể làm việc vơí AH và ESP.

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 chì bảo mật chống lại việc thay đổi nội dung dữ liệu nên cần phải cần phải có những phương tiện khác đểđảm bảo tính riêng tư của dữ liệu. ESP được dùng bảo mật chống nghe trộm rất có hiệu quả nhưng không bảo mật được toàn vẹn traffic.

Trong chế độ đường hầm, tiêu đề IP chứa địa chỉ nguồn và điạ chỉ đích, trong khi bộ xuất tiêu đề IP chứa các địa chỉ IP khác, chẳng hạn như địa chỉ cổng nối. AH bảo mật toàn bộ gói IP bao gồm cả bộ phận tiêu đề. ESP cung cấp các cơ chế bảo mật cho các gói bằng các mã hóa toàn bộ gói.

Để có thể áp dụng AH và ESP trong chế độ đường hầm hay chế độ giao vận, IPSec được yêu cầu phải hỗ trợ phương thức tổ hợp:

* Dùng chế độ đường hầm để mã hóa và xác thực các gói và tiêu đề rồi gắn vào AH hoặc ESP.
* Dùng cả AH và ESP trong chế độ giao vận.

1. **Quán Lý Khóa:**

Trong truyền thông sử dụng giao thức IPsec đòi hỏi phải có chuyển giao khóa, vì vậy cần phải có cơ chế quản lý khóa. Có 2 phương thức chuyển khóa:

* Chuyển khóa bằng tay.
* Chuyển khóa Internet IKE- Internet Key Exchange

Đối với những mạng chỉ có vài VPN peer, có thể thực hiện việc phân bố khóa bằng tay. Còn đối với các mạng lớn cần phải có một phương thức quản lý và kiểm soát khóa tự động. Giao thức quản lý chuyển giao khóa mặc định trong IPSec là IKE .

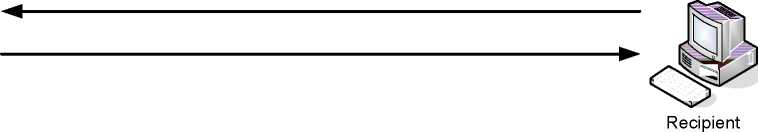
IKE là kết quả kết hợp giữa bảo mật ISA- Internet Security Association và giao thức chuyển giao khóa ISAKMP. IKE còn có 1 tên gọi khác là ISAKMP/Oakley. IKE có các khả năng sau:

* Cung cấp các phuơng tiện cho 2 bên thỏa thuận sử dụng các giao thức, giải thuật và khóa.
* Đảm bảo ngay từ lúc đầu là truyền thông đúng đối tượng.
* Quản lý các khóa sau khi chúng được chấp nhận trong tiến trình thỏa thuận.
* Đảm bảo các khóa được chuyển 1 cách bảo mật.

1. **Các chế đô và pharse của IKE:**

Hoạt động của IKE gồm 2 giai đoạn:

* Giai đoạn 1- Pharse 1: thiết lập 1 đường hầm bảo mật cho các hoạt động ISAKMP.
* Giai đoạn 2- Pharse 2: là tiến trình đàm phán các mụch đích SA.

Pharse II

Pharse I

Thiết lập kênh bảo mật  
cho IKE SA

Dàn xếp các mụch đích chung của  
SAs



**Sender**

IKE còn có 4 chế độ chuyển khóa và cài đặt các ISAKMP do giao thức Oakley qui định cho 2 giai đoạn:

* Chế độ chính (main mode): hoàn thành giai đoạn 1 của IKE sau khi đã thiết lập 1 kênh bảo mật.
* Chế độ năng động (Aggressivemode): tương tự như main mode, nhưng đơn giản và nhanh hơn vì nó truyền nhận dạng bảo mật cho tất cả các nút trước khi đàm phán được 1 kênh bảo mật.
* Chế độ nhanh (quick mode): hoàn thành giai đoạn 2 của IKE bằng cách đàm phán 1 SA cho các much đích của việc truyền thông.
* Chế độ nhóm mới (new group mode): chế độ này không thật sự thuộc giai đoạn 1 hay giai đoạn 2. Chế độ nhóm mới theo sau đàm phán của giai đoạn 1 và đưa ra 1 cơ chế định nghĩa nhóm riêng cho chuyển giao Diffie-Hellman.

Để thiết lập 1 bảo mật IKE cho 1 nút, 1 host hay 1 cổng nối cần ít nhất 4 yếu

tố:

* Một giải thuật mã hóa để bảo mật dữ liệu.
* Một giải thuật băm để giảm dữ liệu cho báo hiệu.
* Một phương thức xác thực cho báo hiệu dữ liệu.
* Thông tin về nhóm làm việc qua tổng đài.

1. **Đàm phán SA:**

Để thiết lập 1 SA, bên khởi tạo phải gửi 1 thông báo yêu cầu thông qua quick mode. Một đàm phán SA là kết quả của 2 SA: 1 hướng về (inbound) và 1 hướng đi khỏi (outbound) bên khởi tạo. Để tránh xung đột về SPI, nút nhận phải luôn chọn SPI, và thông báo cho bên kia biết. Mỗi SPI, kết hợp với địa chỉ IP đích, chỉ định 1 SA đơn duy nhất. Trong thực tế những SA này luôn có 2hướng , chúng có danh định về tham số, giải thuật, khóa, băm là 1 phần trong SPI.

1. **Những vân để còn tổn đong trong IPSec:**

Mặc dù IPSec có những đặc tính cần thiết cho việc bảo mật nhung nó vẫn còn trong giai đoạn phát triển nên còn một số hạn chế cần lưu ý:

* Các gói xử lý theo IPSec sẽ tăng kích thước làm thông lượng mạng giảm xuống.
* IKE vẫn là 1 công nghệ chưa được chứng minh trong khi phương thức chuyển khóa bằng tay lại không thích hợp cho mạng có 1 số lượng lớn các đối tượng di động.
* IPSec được thiết kế chỉ để điều khiển lưu lượng IP mà thôi.
* Việc tính tóan cho nhiều giải thuật trong IPSec là 1 vấn đề đối với các trạm làm việc và PC cũ.

**Chương IV:**

**Xây dựng IPSec YPN dựa trên Router Cisco**

1. **Giới thiêu chung về giải pháp VPN của Cisco:**

Cisco là 1 công ty chuyên cung cấp thiết bị và giải pháp lớn có uy tín trên thế giới. Đối với mạng riêng ảo VPN, Cisco cũng có những giải pháp và thiết bị hỗ trợ hiệu quả. Tùy theo từng loại VPN mà Cisco có những sản phẩm đáp ứng cụ thể.

* Site-to-Site VPN: đây là loại VPN có từ 2 endpoint ữở lên. Tại các endpoint có thể dùng các sản phẩm sau: Router, các VPN-enable firewall, các thiết bị phần cứng VPN...
* Access VPN: còn gọi là Remote AccessVPN. Thường dùng: Router, các VPN-enable firewall hoặc các VPN concentrator.

Ngoài ra Cisco còn có 1 giải pháp thiết lập VPN 1 cách đơn giản nhanh chóng gọi là Easy VPN. Với giải pháp Easy VPN, cần có 1 Cisco Easy VPN Server đặt tại trụ sở chính và các thiết bị khác có thể là: Cisco PIX 501 firewall, 3002 hardware VPN client, Cisco VPN client software.

Trong điều kiện khả năng hiện tại, với thiết bị của Cisco có thể tiếp cận là các Router có hỗ trợ VPN, nên trong phạm vi luận văn này chúng ta sẽ tập trung tìm hiểu về mô hình IPSec VPN được thiết lập bằng Router :.

Đối với những mạng chỉ có vài VPN peer, có thể thực hiện việc phân phối khóa bằng tay. Còn đối với các mạng lớn cần phải có Certificate Authority (CA) server, khi đó ta cần phải cài đặt ISAKMP để hỗ trợ phương thức khóa khóa mà ta đã chọn. Việc lựa chọn phương thức phân phối khóa cũng quyết định cấu hình xác thực của các peer.

Trong chương này chúng ta sẽ tìm hiểu cách thiết lập IPSec VPN trên Router Cisco:

* Preshared key cấu hình thủ công.
* Preshared key với RSA encrypted nonce
* Preshared key với RSA encrypted nonce có CA hỗ trợ việc xác thực.

1. **Mô tá quá trình thiết lâu IPSec VPN tunnel:**

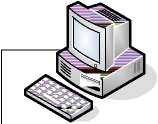
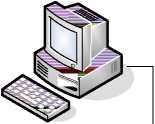
Có thể mô tả việc tạo và giới hạn IPSec VPN tunnel như 1 quá trình gồm 5 bước, các endpoint sẽ thực hiện những nhiệm vụ khác nhau nhằm thiết lập kết nối được mã hóa theo từng bước:

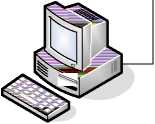
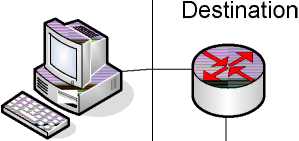
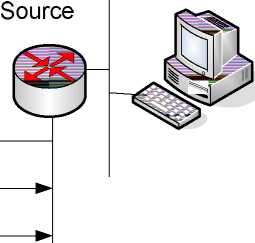
Step 1: user tại Source khởi tạo 1 kết nối tới hệ thống đích Destination . Router tại Source nhận được traffic như là 1 traffic cần quan tâm và thiết lập tiến trình IKE với router tại Destination.

Step 2: Các router endpoint dùng IKE để xác thực từng IKE peer và thoả thuận về IKE SA. Lúc này 1 kênh bảo mật được thiết lập để cho phép đàm phán IKE SA- thời điểm này xem như IKE pharse I.

Step 3: IKE lại được dùng để đàm phán IPSec SA giữa các peer. Khi việc đàm phán kết thúc, các IPSec peer có SA đã được thiết lập và chuẩn bị truyền dữ liệu- thời điểm này xem như IKE pharse II.

Step 4: Đường hầm đã được thiết lập và các thông tin IPSec SA đã được chứa trong SA database của cả 2 SA peer. Thêm vào đó, việc đàm phán khóa được tiến hành đối với mỗi thông số đã được đàm phán trong suốt pharse II.

Step 5: Các kết nối được giới hạn khi hết thời gian hoặc bị thoát từ bất cứ peer nào- nghĩa là không có traffic nào dùng IPSec nữa.

Step 1 Step 2 Step 3 Step 4

Step 5

Connection terminated

1. **Các bưđc thiết lâp VPN vđi IPSec:**

Trước khi tiến hành thiết lập IPSec VPN thực hiện 1 tiến trình gồm 5 bước với nhiều mục nhỏ cần thực hiện:

1. **Step 1-Thiết lâp IKE policy:**

Trước tiên chúng ta phải xác định các thông số cho IKE policy. IKE policy này phải được thiết lập giống hệt nhau tại các điểm cuối của VPN. Các thành phần của IKE policy cần được thiết lập bao gồm:

* Phương thức phân phối khóa: bằng tay hoặc dùng CA.
* Phương thức xác thực: phục thuộc vào phương thức phân phối khóa. Nều phân phối bằng tay thì dùng preshared keys. Phân phối dùng CA thì sử dụng RSA (RSA encrypted nonces hoặc RSA digital signatures).
* Địa chỉ IP và hostname của các peer.
* Các thông số IKE policy: các thông số này được ISAKMP dùng để thiết lập đường hầm bảo mật của IKE pharse 1. Các thông số này bao gồm: Các thuật toán mã hóa (DES/3DES), thuật toán Hash (MD5/SHA-1), phương thức xác thực (preshared, RSA encryptions, RSA signatures), trao đổi khóa (D-H group 1/D-H group 2) và IKE SA lifetime (mặc định là 86400 giãy).

1. **Step 2- Thiết lâp IPSec policy:**

Sau khi xác định các thông số IKE policy, chúng ta cần phải xác định các thông tin về IPSec policy gồm:

* Giao thức IPSec được dùng: AH hoặc ESP.
* Xác thực: MD5 hoặc SHA-1.
* Mã hóa: dùng DES hoặc 3DES.
* Transform và transform set: là kết hợp các thuật toán mã hóa và xác thực (AH-SHA-HMAC / ESP-3DES / ESP-MD5-HMAC).
* Chỉ định các traffic cần được bảo vệ: giao thức, nguồn, đích và port.
* Thiết lập SA: bằng tay hoặc dùng IKE.

1. **Step 3-Kiểm tra các cấu hình hiên cổ:**

Sau khi xác định các policy cho IKE và IPSec, chúng ta phải kiểm tra lai cấu hình hiện có tại các thiết bị để chắc chắn rằng không có tranh chấp giữa cấu hình hiện có với cấu hình sắp thực hiện.

1. **Step 4-Kiếm tra lai kết nốì mang trước khỉ áp dung IPSec:**

Chúng ta phải luôn đảm bảo có kết nối giữa các SA peer trước khi thử tạo

ra 1 kết nối VPN.

1. **Step 5- Cho phép các giao thức IPSec và các port của nổ:**

Nếu có áp dụng ACL tại các thiết bị hên đường đi của IPSec VPN, chúng ta phải đảm bảo các ACL này cho phép IPSec traffic:

* UDP port 500: ISAKMP.
* Protocol 50:ESP.
* Protocol 51: AH.

Sau khi thực hiện đầy đủ 5 bước nêu trên, chúng ta có thể bắt đầu cấu hình các thiết bị theo những policy đã được xác định ở bước 1 và bước 2.

1. **Các bưđc cấu hình Router Cisco cho IPSec VPN vđi Preshared Kev:**

IPSec VPN phân phối khóa bằng tay có thể sử dụng cho các hệ thống có sô" lượng peer ít. Lúc này ta có thể câu hình bằng tay (cấu hình tĩnh) cho tất cả các peer.

Preshared key là các khóa ký sô" (tương tự như password) được cấu hình trên từng Router và phải được sắp xếp 1 cách chính xác để các Router có thể thương lượng việc kết nối. Khi mạng càng lớn, số lượng peer tăng thì việc quản lý các kết nối VPN dùng Preshared key trở nên khó khăn.

Việc cấu hình IPSec VPN trên Router với Preshared key gồm 4 bước:

* Step 1: chuẩn bị như đã được mô tả ở trên.
* Step 2: Cấu hình IKE (enable IKE, tạo các policy và xác nhận việc cấu hình).
* Step 3: Cấu hình IPSec (Xác ding transform set, tạo các Crypto ACL, tạo các Crypto map, áp dụng các Crypto map).
* Step 4: kiểm tra lại các cấu hình vừa thực hiện, điều chỉnh lại nếu phát hiện sai sót.

1. Step 1- Chon lưa các thông số của IKE và IPSec:

Much đích là là xác định trước các thiết lập cần thiết tại mỗi peer nhằm đảm bảo khả năng thành công của việc đàm phán cho kết nối. Các việc phải thực hiện tại bước này gồm:

- Xác định IKE policy.

Các thông số có thể dùng khi cấu hình IKE:

|  |  |  |
| --- | --- | --- |
| Paramieter | Strong | Stronger |
| Encryption algorithm | DES | 3 DES |
| Hash algorithm | MD5 | SilA-l |
| Au l hen 11 cation met 11 od | Preshare | RSA signature RSA-encrypted nonce |
| Đilììe-Hellinnn key exchange | Group 1 | Group 2 |
| SA lifetime | 86,400 seconds | < 86,400 seconds |

- Xác định IPSec policy. Các thông số IPSec cần lưu ý:

|  |  |
| --- | --- |
| AH Transform | Description |
| A11-MÜ5-1IMAC | Ali. MD5 hash, IIMAC variant (authentication) |
| AH-SHA-HMAC | AEt, SliA-I hash, HMAC variant (authentication) |
| ESP Transform | Description |
| ESP-DES | ESI\*. DIES (encryption) |
| ESP-3 DES | ESP, 3DES (encryption) |
| ESP-MD5-IIVI At: | ESP, MD5? 1 [MAC variant |
|  | (This transform would be combined with ESP-DES. ESP-.!DES. or ESP- NULL.) |
| ESP-SHA-HMAC | ESP, SHA-lj HMAC variant |
|  | (This transform would be combined with ESP-DES, ESP-3DES, or ESP- NULL.) |

* Kiểm tra lại cấu hình hiện tại.
* Kiểm tra lại kết nấỉ
* Đảm bảo tính tương thích của cácACL. 2. Step 2- Cấu hình IKE:

Việc cấu hình IKE bao gồm:

* Enable IKE.
* Tạo IKE policy.
* cếu hình Preshared key.
* Kiểm tra lại việc cấu hình IKE vừ thực hiện. Ví dụ về các thông số cấu hìng IKE:
* Key Distribution: ISAKMP.
* Authentiction: Preshared Key.
* Encrytion Algorithm: 3DES.
* Hash Algorithm: MD5.
* Diffie-Hellman: 2(1024 bit).
* IKE SA Lifetime: 86,400 giây.

1. Step 3- Cấu hình ĨPSec:

Cấu hình IPSec gồm các bước sau:

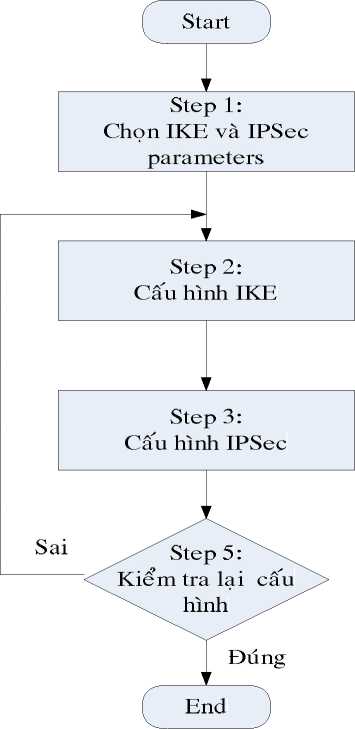
* Tạo transform set
* Cấu hình IPSec SA Lifetime.
* Tạo crypto ACL
* Tạp crypto map
* Ap dụng Crypto map Ví dụ về cấu hình IPSec:
* Authentication transform: ESP-MD5-HMAC.
* Encryption Transform: ESP-3DES.
* IPSec SA Lifetime: 3600 giây.

1. Step 4- Kiểm tra lai cấu hình vừa thực hiên:

Các câu lệnh có thể được dùng để kiểm tra cấu hình vừa thực hiện:

* Show crypto isakmp policy : hiển thị ISAKMP policy đang được cấu hình trên Router.
* Show crypto ipsec transform-set: hiển thi các transform set.
* Show crypto ipsec sa : hiển thị tình trạng của SA.
* Show crypto map : hiển thi crypto map hiện sử dụng.
* Show crypto dynamic-map : hiển thị dynamic crypto map set.
* Debug crypto isakmp : cho phép debug các IKE event
* Debug crypto IPSec : cho phép debug các IPSec event

Các bước câu hình IPSec trên Router



Lưu v:

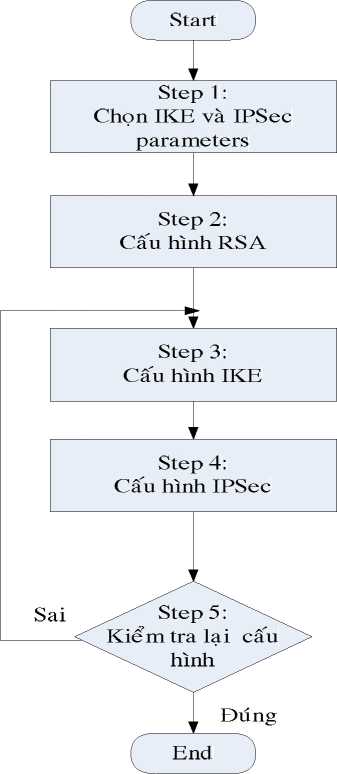
- Việc cấu hình phải được thực hiện giống nhau tại cả 2 peer cần thiết lập IPSec VPN.

1. **Các bưđc cấu hình Router dùng RSA nonces:**

Trong việc cấu hình IPSec bằng tay chúng ta phải đưa các khóa cần thiết để thiết lập kết nối vào trước 1 cách thủ công, việc này không được khuyến khích do khổ quản lý và không bảo mật. Có 1 phương thức được sử dụng để thay thế là dùng RSA encrypted nonce. Phương thức này cho phép tạo khóa 1 cách ngẫu nhiên, các khóa này được trao đổi giữa các peer dựa ữên cơ chế ữao đổi khóa Diffie-hellman.

Các bước cấu hình IPSec dùng RSA encrypted nonce cũng tương tự như cấu hình IPSec bằng tay, có thêm 1 bước cấu hình RSA key:

Các bước câu hình IPSec VPN có dùng RSA nonces



* Step 1: chọn các thông sô" IKE và IPSec.
* Step 2: Cấu hình RSA key.
* Step 3: Câu hình IKE (enable IKE, tạo các policy và xác nhận việc cấu hình).
* Step 4: Cấu hình IPSec (Xác ding transform set, tạo các Crypto ACL, tạo các Crypto map, áp dụng các Crypto map).
* Step 5: kiểm tra lại các cấu hình vừa thực hiện, điều chỉnh lại nếu phát hiện sai sót

Việc cấu hình và qủan lý RSA key gồm các bước sau:

* Lên kế hoạch thiết lập việc dùng RSA key.
* Cấu hình hostname và domain name cho Router.
* Tạo các RSA key.
* Nhập các khóa RSA công cộng của peer.
* Kiểm tra lại việc cấu hình khóa.
* Cuối cùng là việc quản lý các khóa

1. **Lên kế hoach viêc dùng RSA kev:**

Cũng tương tự như việc lên kế hoạch cho việc cấu hình IPSec, tuy nhiên cần phải chú ý đến việc tạo và trao đổi khóa.

1. **Cấu hình hostname và domain name cho Router:**

Phần quan trọng của của việc xác thực la'hệ thống phải nhận dạng đưọc chính bản thân nó. Để làm được việc này, chúng ta phải cấu hình hostname và domain name cho các Router.

1. **Tao các RSA kev:**

Mặc định các đôi khóa RSA không tồn tại trên Router, chúng ta phải thêm tùy chọn usage-key vào câu lệnh tạo khóa mã hóa và khóa xác thực:

Crypto key generate rsa usage-key

Câu lệnh trên sẽ tạo ra 1 pair khóa (public hoặc private) của cặp khóa.

1. **Nhân các khóa RSA công cống;**

Sau khi nhận được public key ta phải nhập khóa đó vào Router. Để thực hiện việc này cần dùng các lệnh sau:

crypto key pubkey-chain crypto key pubkey-chain rsa addressed-key key-address named-key key-name key-string

1. **Kiểm tra lai viêc câu hình khóa:**

Sau khi thực hiện việc cấu hình khóa, ta phải kiểm ữa lại các thông số- có thể dùng các lệnh sau:

* Show crypto key mypubkey rsa: hiển thị các public key đượa cài trên Router.
* Show crypto key pubkey-chain rsa: hiển thị tất cả các peer được cài khóa.

1. **Viêc quán lý khóa;**

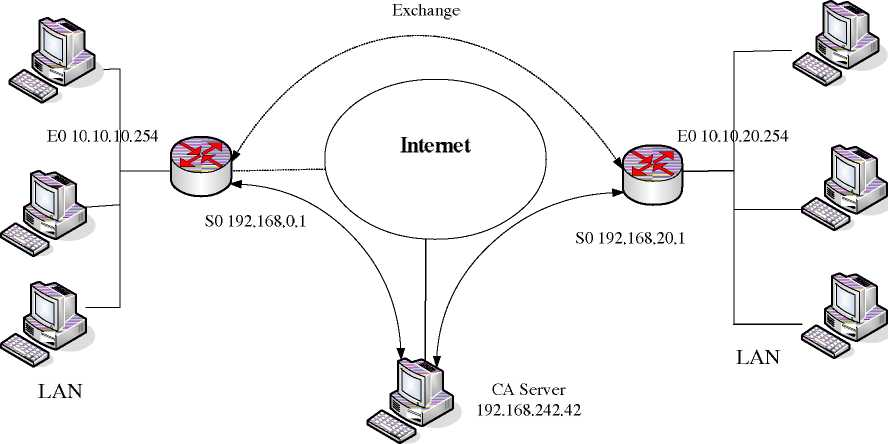
Sau được tạo và cài đặt, chỉ có thể xóa các RSA key bằng câu lệnh:

Show crypto key zeroize rsa **VL Các bưđc cấủ hình IPSec VPN vđỉ CA:**

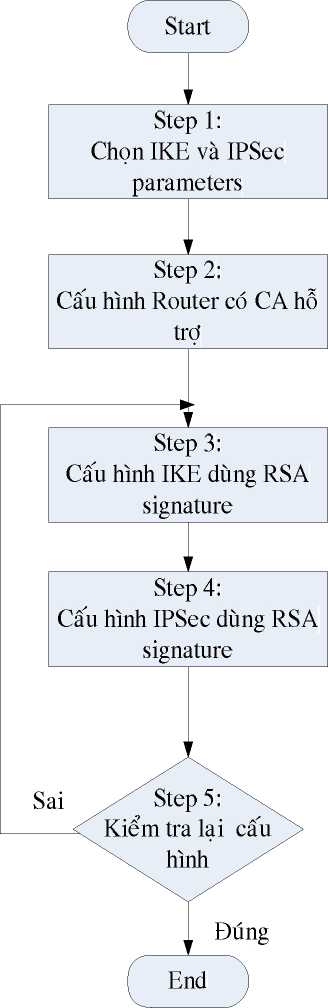
ưu điểm của việc dùng IPSec VPN với CA là các peer không cần phải trao đổi preshared key hoặc nonce bằng cách thủ công, vì lúc này khi 2 peer bắt đầu đàm phán IKE chúng chỉ trao đổi các khóa công cộng (public key), các khóa này sau đó sẽ được CA xác thực. Việc quản trị sẽ trở nên đơn giản hơn do không cần phải theo dõi các khóa.

Xác thực Peer dùng CA

Digital certificate

Để cấu hình Router cho IPSecVNP có hỗ trợ CA, chúng ta phải hoàn tất 5 bước, mỗi bước có nhiều tác vụ cần thực hiện.

* Chọn các thông số IKE và IPSec.
* Cấu hình Router hỗ trợ CA.
* Cấu hình IKE dùng RSA signature.
* Cấu hình IPSec dùng RSA signature.
* Kiểm tra lại các cấu hình đã thực hiện.



Công việc cụ thể của từng bước như sau:

1. **Lựa chon các thông số\* IKE và IPSec:**

Mụch đích là xác định trước các thiết lập cần thiết tại mỗi peer nhằm đảm bảo khả năng thành công của việc đàm phán cho kết nối. Các việc phải thực hiện tại bước này gồm:

- Lên kế hoạch hỗ trợ CA.

* Xác định IKE policy (pharse 1).
* Xác định IPSec policy
* Kiểm tra lại cấu hình hiện có của Router
* Kiểm tra lại các kết nối.
* Đảm bảo sự tương thích của các ACL.

1. **Câu hình Router hỗ trỢ CA:**

Để cấu hình Router hỗ trợ CA cần phải thực hiện 11 bước khác nhau, bao gồm cả việc cấu hình Router, tạo khóa, và liên lạc với CA Server.

* Cấu hình hostname và domain name cho router.
* Thiết lập Date, Time và Time zone cho Router.
* Add CA Server vào Host table của Router.
* Tạo ra RSA key pair.
* Khai báo CA.
* Xác thực CA.
* Yêu cầu được chứng nhận.
* Lưu lại các cấu hình vừa thực hiện.
* Quản lý các khóa chứa trong NVRAM.
* Quản lý các khóa trên Router.
* Kiểm tra laị các cấu hình CA.

1. **Cấu hình IKE dùng RSA signature:**

Cách cấu hình cũng tương tự như preshared key xác thực thủ công. Ví dụ có thể cấu hình với những thông số sau:

* Key Distribution: ISAKMP.
* Authentiction: Preshared Key.
* Encrytion Algorithm: 3DES.
* Hash Algorithm: MD5.
* Diffie-Hellman: 2(1024 bit).
* IKE SA Lifetime: 86,400 giây.

1. **Câu hình IPSec dùng RSA signature:**

Các bước cấu hình IPSec gồm:

* Tạo IPSectransform set.
* Cấu hình IPSec SA Lifetime.
* Tạo Crypto access list.
* Tạo Crypto map.
* Ấp dụng Crypto map.

Ví dụ về các thông số cấu hình:

* Authentication transform: ESP-MD5-HMAC.
* Encryption Transform: ESP-3DES.
* IPSec SA Lifetime: 3600 giây.

1. **Kiểm tra lai câu hình:**

Có thể dùng các lệnh sau để kiểm tra lại cấu hình đã thực hiện:

* crypto ca identity : Hiển thị cấu hình CA mà Router được cấu hình.
* Debug crypto pki {callback, message, transaction}: cho phép hiển thị callback, transtion hoặc message giữa Router và CA.
* Show crypto ca certificates : Hiển thị thông tin về certificate của SA và RAS.

**Phần ĩĩĩ;**

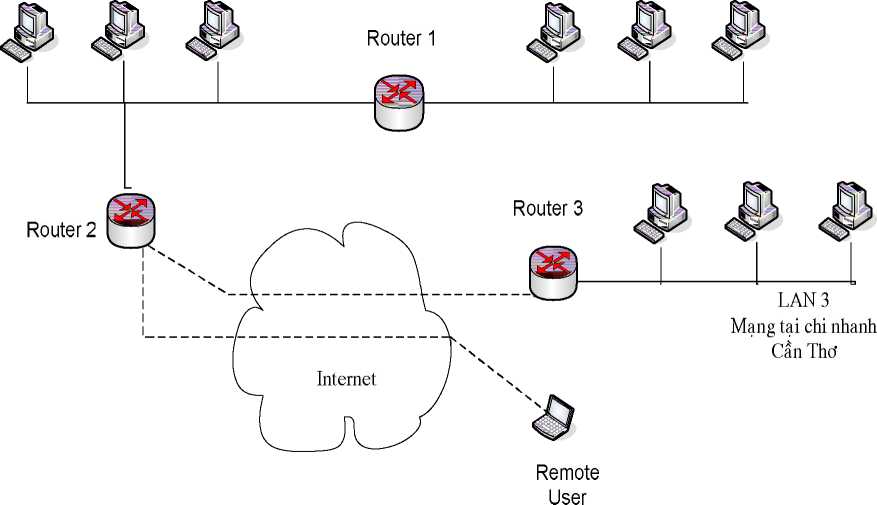
MÔ hình giải quyết bài toán

**Chương V:**

**Xây dựng mô hình giải quyết bài toán**

Dựa trên giải pháp và mô hình đã lựa chọn:

LANS? LAN1 M?nễblêntập Mạngkỳ thuật



Chúng ta chia việc thực hiện thành 2 phần, có thể thiết lập độc lập với nhau:

* Phần thứ nhất: thiết lập kết nối giữa 2 mạng nội bộ LAN 1 và LAN 2.
* Phần thứ hai: Thiết lập hệ thống IPSec VPN.

I. Thiết lâp kết nốì cổ kiểm soát giữa 2 mang nôi bô LAN 1 và LAN2: Với yêu cầu kết nối 2 mạng nội bộ riêng lẻ hiện nay lại thành một hệ thống hợp nhất, có kiểm soát việc trao đổi dữ liệu giữa chúng với nhau, chúng ta có thể áp dụng mô hình đơn giản là dùng một Router có thiết lập Access list như sơ đồ phía dưới:

Tuy nhiên do loại Router có nhiều module Ethernet interface có giá thành cao hơn nhiều so với loại Router thường chỉ có 1 Ethernet Interface nên ta có thể dùng 2 Router thường, 2 Router này kết nối với nhau qua Serial Interface:

LAN 1

Mạng kỹ thuật



LAN 2

Mạng Biên tập





PC-B



Router



Sever BT

LAN 1

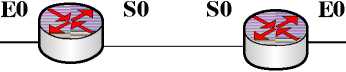
Mạng kỹ thuật



LAN 2

Mạng Biên tập





Router A Router B

Việc kiểm soát traffic giữa 2 mạng được thực hiện bằng ACL- Access Control List. Có thể chia việc thực hiện thành 2 bước:



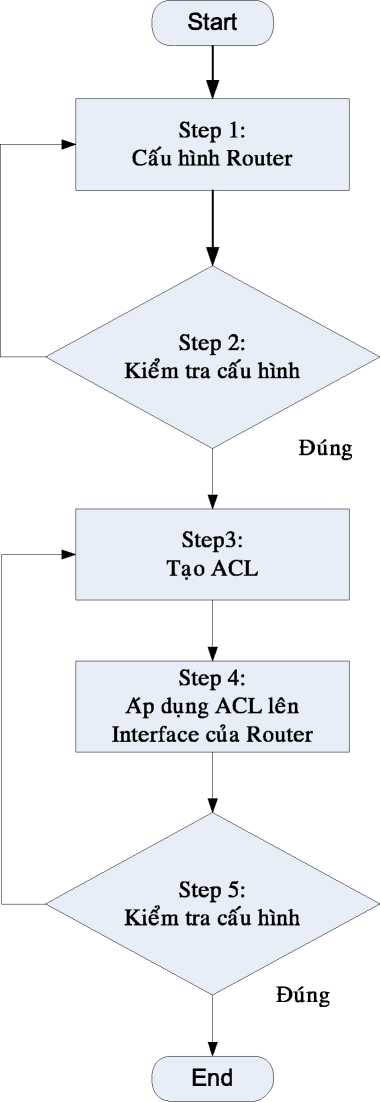
PC-B



Sever BT

- Bước 1: Xây dựng Access list theo yêu cầu kiểm soát traffic.

- Bước 2: áp dụng các Access list đã được xây dựng ở bước 1 lên các interface của Router.

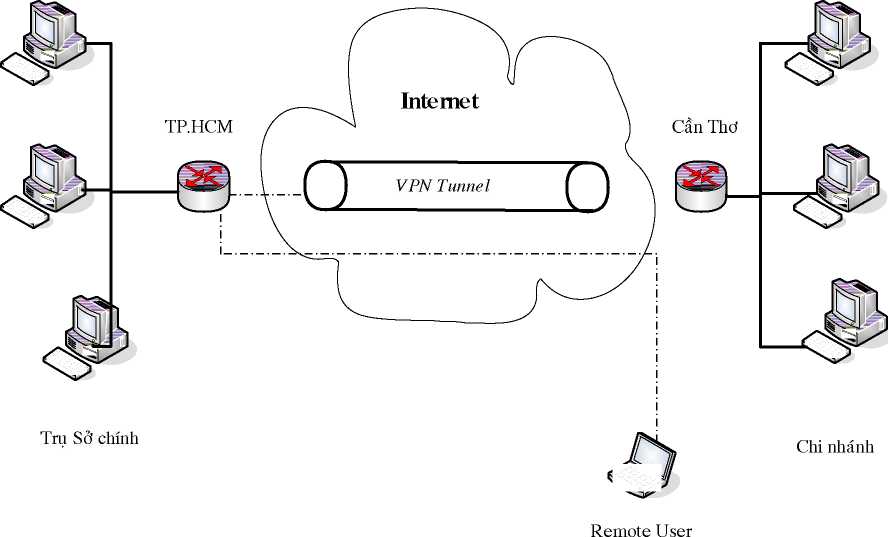
Các bước thực hiện cụ thể

Sai

Sai

**II Các bước thiết lâp hê thông IPSec VPN:**

Mô hình thiết lập IPSec VPN cho Đài TNND TP.HCM



Dưạ trên tính năng của các sản phẩm Cisco VPN và điều kiện hạ tầng cơ cở Internet tại Việt Nam hiện nay, chúng ta có thể thiết lập 1 mô hình VPN bao gồm:

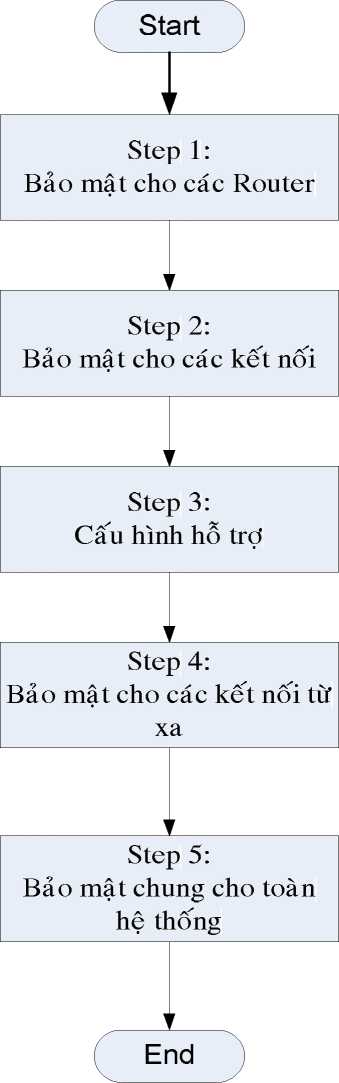
* Sử dụng Router Cisco để thiết lập các Endpoint tại trụ sở chính TP.HCM và cơ sở chi nhánh ( ví dụ như Chi nhánh tại cần Thơ).
* Các Router sẽ được cấu hình IPSec VPN cho phép kết nối Site-to-Site đồng thời cho 1 sô" người dùng di động kết nối vào mạng tại trụ so83 chính TP.HCM .
* Các người dùng từ xa sẽ được cài đặt VPN client Software để có thể truy cập vào mạng tại trụ sở chính TP.HCM.

Để thiết lập mạng VPN theo mô hình trên, chúng ta thực hiện các công việc sau:

* Bảo mật cho các Router đặt tại các endpoint : TP.HCM và cần Thơ.
* Bảo mật cho kết nối site-to-site giữa TP.HCM và cần Thơ.
* Cấu hình hỗ trợ CA.
* Bảo mật cho các kết nối từ xa.
* Bảo mật chung cho toàn hệ thống.

Các công việc trên đòi hỏi phải có sự chuẩn bị kỹ lưỡng từ khâu chuẩn bị đến thực hiện.

Các bước thiết lập mạng VPN cho Đài TNND TP.HCM



1. **Báo mât cho các router:**

Việc bảo mật cho các router gồm:

* Thiết lập quyền truy nhập quản lý cho mỗi router.
* Thiết lập SSH để vô hiệu truy cập telnet, có thể kiểm soát truy cập router bằng Access list.
* Vô hiệu hóa các dịch vụ không cần thiết trên từng router.

1. **Báo mật cho kết nốĩ site-to-sỉte:**

Để bảo mật cho cho kết nối site-to-site cần thực hiện 5 việc sau:

* Định nghĩa các thông số cấu hình VPN.
* Cấu hình các thông số IKE.
* Cấu hình các thông số IPSec.
* Cấu hình các ACL (Access Control list).
* Tạo và áp dụng các Crypto map.

1. **Câu hình hỗ trơ CA**

Chúng ta cần thực hiện một sô" bước cấu hình router để hỗ ữợ CA:

* Câu hình Host Name và Domain Name
* Cấu hình NTP
* Enroll with the CA

1. **Báo mât Remote Access:**

Đối với các truy cập từ xa của các user đơn lẻ thì tại Router TP.HCM chúng ta cần thực hiện các công việc sau:

* Thiết lập AAA.
* Cấu hình ACLs.
* Thiết lập VPN sử dụng CA.

Ngoài ra tại máy của người dùng từ xa còn cần phải cài đặt phần mềm client VPN.

1. **Báo mât cho toàn hê thông:**

* Thiết lập Cisco IOS firewall IDS.
* Thiết lập Authentication Proxy.
* Thiết lập CBAC.

**Phần ĨV**

MÔ hình minh hoa

**Chương VI:**

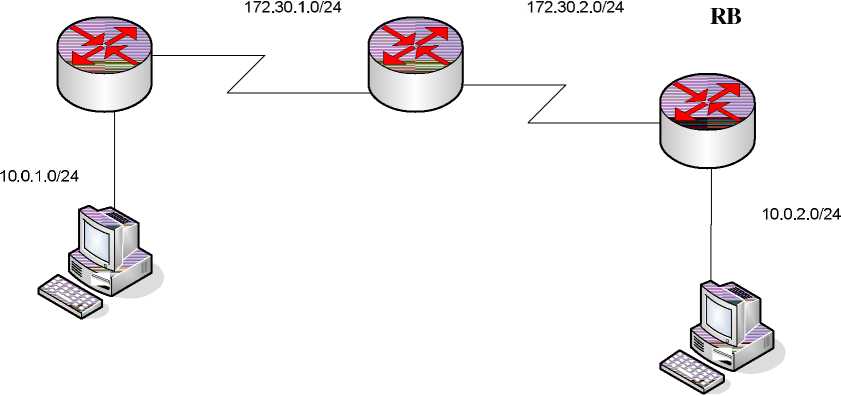
**Mô hình minh họa:**

■

**Thiết lập IPSec VPN dùng preshared key trên Router Cisco**

**I. Mô tá mỏ hình:**

RA RI



Mô hình giả sử 1 công ty có 2 điạ điểm: 1 trụ sở chính và 1 chi nhánh. Muốn tạo 1 kết nối private qua 1 môi trường truyền public ta sử dụng VPN để thực hiện nhiệm vụ này. Ta tạo 1 kênh riêng giữa 2 Router: RA và RB, qua môi trường Internet- do Router RI giả lập làm ISP. Bất cứ traffic TCPnào từ 10.0.1.0/24 đến 10.0.2.0/24 đều sẽ được mã hóa và gửi ngang qua mội trường public.

**ỊL Thực hiện:**

Sau khi đã cấu hình cho các Router như topo, ta bước qua phần cấu hình VPN. Việc cấu hình VPN gồm những bước sau:

- Bước 1: Cấu hình IKE

o Bật IKE: mặc định IKE đã được bật, nếu bị tắt ta có thể mở lại bằng câu lệnh.

Routerịconfig)#crypto isakmp enable

o Tạo IKE policy:

Router(confỉg)#crypto ỉsakmp policy priority o Tạo các IKE policy ở mode config- isakmp: authentication, encryption, hash...

- Bước 2: Cấu hình IPSec:

o Cấu hình transform set:tạo transform set giúp ta áp dụng các chính sách bảo mật cho traffic. Có thể tạo 3 ữansíorm ữong 1 set, mỗi set được giới hạn: 1 AH và 2ESP. Mode mặc định cho transform là tunnel.

Router(config)#crypto ipsec transform-set *name* [transl [trans2 [trans3]]]

Routerị cfg-crypto-trans )#

o Tạo crypto ACL: thực hiện các chức năng sau: xác định các dòng dữ liệu được bảo vệ bởi IPSec, chọn outbound traffic được bảo vệ

* Tạo ACL để xác định traffic cần bảo vệ.
* Tạo crypto map

Router(config)#crypto map *name seq* ỉpsec-manual I ipsec- ỉsakmp

4 sử dụng các sequence no khác nhau cho mỗi peer, nhiều peer có thể xác định trong cùng 1 crypto map.

* Ap crypto map vào interface

**Cu thế là:**

**Router RA**

RA(config)#crypto isakmp enable <-Bật crypto isakmp RA(config)#crypto isakmp policy 100 RA(config-isakmp)#hash md5

RA(config-isakmp)#authentication pre-share <-xác định các phương pháp xác minh

RA(config-isakmp)#exit

RA(config)#crypto isakmp identity address 4-xác định cách xác định peer qua địc chỉ chứ không phải qua hostname

RA(config)#crypto isakmp key cisco address 172.30.2.2 ^-xác định key cho preshare key của peer

RA(config)#crypto ipsec transform-set mine esp-des <-xác định giải thuật mã hoá là esp-des cho transform-set tên mine

RA(cfg-crypto-trans)#exit

RA(config)#crypto map lee 10 ipsec-isakmp <-tạo crypto map tên lee

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

RA(config-crypto-map)#set peer 172.30.2.2 4-xác định peer là interface bên kia

RRA(config-crypto-map)#set transform-set mine áp transform set mine vào crypto map lee

RA(config-crypto-map)#match address 110 4-xác đinh ACL RA(config-crypto-map)#exit

RA(config)#access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255 <-tạo ACL để xác định traffic được mã hoá

RA(config)#int s0/0

RA(config-if)#crypto map lee <-áp cryto map lee vào interface so/o Router RB: cấu hình tương tự như RA:

RB(config)#crypto isakmp enable

RB(config)#crypto isakmp policy 100 RB(config-isakmp)#hash md5 RB(config-isakmp)#authenticationpre-share

RB(config-isakmp)#exit RB(config)#crypto isakmp identity address RB(config)#crypto isakmp key cisco address 172.30.1.2 RB(config)#crypto ipsec transform-set mine esp-des RB(cfg-crypto-trans)#exit RB(config)#crypto map lee 10 ipsec-isakmp % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

RB(config-crypto-map)#set peer 172.30.1.2 RB(config-crypto-map)#set transform-set mine RB(config-crypto-map)#match address 100 RB(config-crypto-map)#exit

RB(config)#access-list 100 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255 RB(config)#int s0/0 RB(config-if)#crypto map lee

Chú ý các giải thuật mã hóa và phương pháp xác minh phải được đồng bộ giữa 2 bên.

**Kiểm tra:**

Ta sử dụng lệnh Show và Debug để kiểm tra:

* Dùng telnet service trên 2 PC ở 2 LAN để telnet qua lại.
* Dùng debug để ghi nhận trên 2 Router.

**Phẩn V:**

**Kết Luận**

Trong một khỏang thời gian ngắn, với vốn kiến thức còn nhiều hạn chế chúng em đã cố gắng tập hợp, nghiên cứu tài liệu, thử nghiệm để phát thảo nên một mô hình ứng dụng, có thể đáp ứng được những yêu cầu đặt ra. Mô hình được xây dựng ữong luận văn đã đưa ra phương thức giải quyết 2 vấn đề cụ thể:

* Kiểm soát truy cập giữa 2 mạng LAN bằng Access list.
* Xây dựng IPSec VPN cho phép kết nối Site-to-Site và Remote Access.

Trong mô hình được xây dựng, thì việc ứng dụng Access list để kiểm soát truy cập giữa 2 mạng LAN là có thể đưa vào sử dụng ngay. Với điều kiện khả năng hiện tại việc thực hiện IPSec VPN chỉ dừng lại ở mức xây dựng mô hình, và tìm hiểu cách thức thiết lập IPSec VPN preshared key cấu hình trên Router Cisco- 1 phương thức có nhều khả năng áp dụng nhất.

Nói chung, từ mô hình đến thực tế ứng dụng còn nhiều vấn đề cần giải quyết, cần phải có thêm thời gian nghiên cứu tài liệu, thử nghiệm trên những thiết bị để có thể áp dụng 1 cách thực tế hiệu quả.

Tài liêu tham khảo

1. CCSP Self-Study CCSP SECUR Exam Certification Guide
2. Cisco I OS Access Lists - O'Reilly
3. Sybex CCNA 4.0 study Guide
4. CCIE Security Exam CertificationGuide Henry Benjamin
5. CCSP Cisco Secure VPN Exam Certification Guide

John F. Roland MarkJ. Newcomb

1. Building a Virtual Private Network **Meeta Gupta**