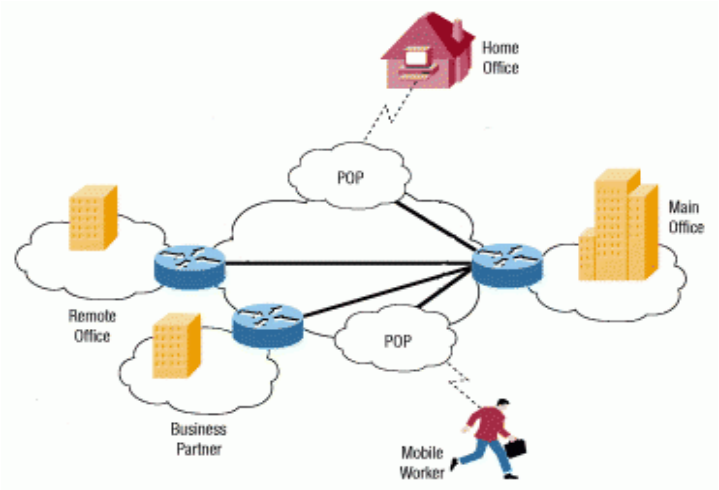
Cấu Hình IPSEC/VPN Trên Thiết Bị Cisco



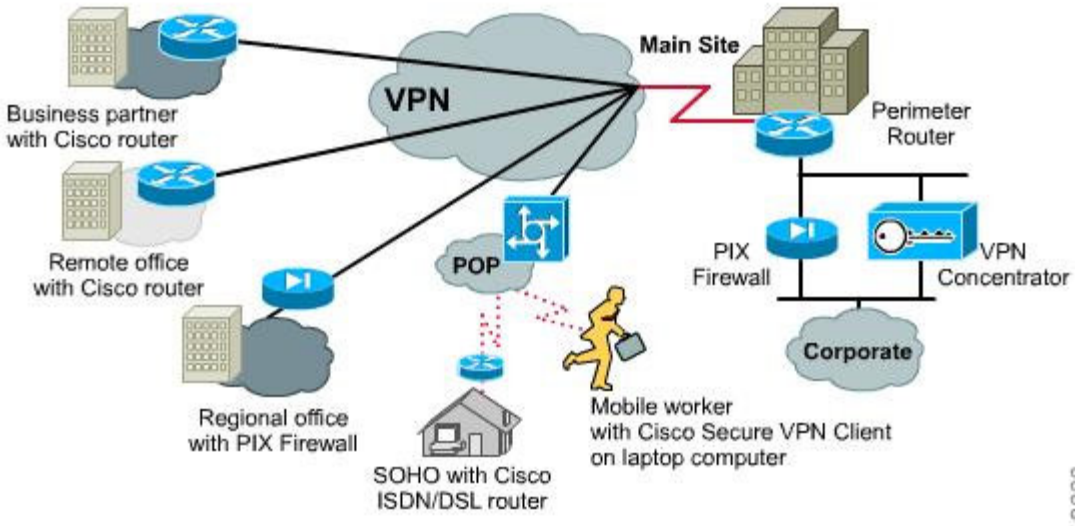
I. Tổng Quan Về VPN:

Trong thời đại ngày nay, Internet đã phát triển mạnh về mặt mô hình cho đến công nghệ, đáp ứng các nhu cầu của người sử dụng. Internet đã được thiết kế để kết nối nhiều mạng khác nhau và cho phép thông tin chuyển đến người sử dụng một cách tự do và nhanh chóng mà không xem xét đến máy và mạng mà người sử dụng đó đang dùng. Để làm được điều này người ta sử dụng một máy tính đặc biệt gọi là router để kết nối các LAN và WAN với nhau. Các máy tính kết nối vào Internet thông qua nhà cung cấp dịch vụ (ISP-Internet Service Provider), cần một giao thức chung là TCP/IP. Điều mà kỹ thuật còn tiếp tục phải giải quyết là năng lực truyền thông của các mạng viễn thông công cộng. Với Internet, những dịch vụ như giáo dục từ xa, mua hàng trực tuyến, tư vấn y tế, và rất nhiều điều khác đã trở thành hiện thực.Tuy nhiên, do Internet có phạm vi toàn cầu và không một tổ chức, chính phủ cụ thể nào quản lý nên rất khó khăn trong

việc bảo mật và an toàn dữ liệu cũng như trong việc quản lý các dịch vụ. Từ đó người ta đã đưa ra một mô hình mạng mới nhằm thoả mãn những yêu cầu trên mà vẫn có thể tận dụng lại những cơ sở hạ tầng hiện có của Internet, đó chính là mô hình mạng riêng ảo (Virtual Private Network - VPN). Với mô hình mới này, người ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật, độ tin cậy vẫn đảm bảo, đồng thời có thể quản lý riêng được sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà, trên đường đi hay các văn phòng chi nhánh có thể kết nối an toàn đến máy chủ của tổ chức mình bằng cơ sở hạ tầng được cung cấp bởi mạng công cộng.[5] Nó có thể đảm bảo an toàn thông tin giữa các đại lý, người cung cấp, và các đối tác kinh doanh với nhau trong môi trường truyền thông rộng lớn. Trong nhiều trường hợp VPN cũng giống như WAN (Wide Area Network), tuy nhiên đặc tính quyết định của VPN là chúng có thể dùng mạng công cộng như Internet mà đảm bảo tính riêng tư và tiết kiệm hơn nhiều.

1. Định Nghĩa VPN:

VPN được hiểu đơn giản như là sự mở rộng của một mạng riêng (private network) thông qua các mạng công cộng. Về căn bản, mỗi VPN là một mạng riêng rẽ sử dụng một mạng chung (thường là internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường leased line, mỗi VPN sử dụng các kết nối ảo được dẫn đường qua Internet từ mạng riêng của các công ty tới các site hay các nhân viên từ xa. Để có thể gửi và nhận dữ liệu thông qua mạng công cộng mà vẫn bảo đảm tính an tòan và bảo mật VPN cung cấp các cơ chế mã hóa dữ liệu trên đường truyền tạo ra một đường ống bảo mật giữa nơi nhận và nơi gửi (Tunnel) giống như một kết nối point-to-point trên mạng riêng. Để có thể tạo ra một đường ống bảo mật đó, dữ liệu phải được mã hóa hay che giấu đi chỉ cung cấp phần đầu gói dữ liệu (header) là thông tin về đường đi cho phép nó có thể đi đến đích thông qua mạng công cộng một cách nhanh chóng. Dữ liệu được mã hóa một cách cẩn thận do đó nếu các packet bị bắt lại trên đường truyền công cộng cũng không thể đọc được nội dung vì không có khóa để giải mã. Liên kết với dữ liệu được mã hóa và đóng gói được gọi là kết nối VPN. Các đường kết nối VPN thường được gọi là đường ống VPN (VPN Tunnel).



2. Lợi ích của VPN:

VPN cung cấp nhiều đặc tính hơn so với những mạng truyền thống và những mạng mạng leased-line.Những lợi ích đầu tiên bao gồm:

- Chi phí thấp hơn những mạng riêng: VPN có thể giảm chi phí khi truyền tới 20-40% so với những mạng thuộc mạng leased-line và giảm việc chi phí truy cập từ xa từ 60-80%.

- Tính linh hoạt cho khả năng kinh tế trên Internet: VPN vốn đã có tính linh hoạt và có thể leo thang những kiến trúc mạng hơn là những mạng cổ điển, bằng cách đó nó có thể hoạt động kinh doanh nhanh chóng và chi phí một cách hiệu quả cho việc kết nối mở rộng. Theo cách này VPN có thể dễ dàng kết nối hoặc ngắt kết nối từ xa của những văn phòng, những vị trí ngoài quốc tế,những người truyền thông, những người dùng điện thoại di động, những người hoạt động kinh doanh bên ngoài như những yêu cầu kinh doanh đã đòi hỏi.

- Đơn giản hóa những gánh nặng.

- Những cấu trúc mạng ống, vì thế giảm việc quản lý những gánh nặng: Sử dụng một giao thức Internet backbone loại trừ những PVC tĩnh hợp với kết nối hướng những giao thức như là Frame Rely và ATM.
- Tăng tình bảo mật: các dữ liệu quan trọng sẽ được che giấu đối với những người không có quyền truy cập và cho phép truy cập đối với những người dùng có quyền truy cập.

- Hỗ trợ các giao thức mạn thông dụng nhất hiện nay như TCP/IP

- Bảo mật địa chỉ IP: bởi vì thông tin được gửi đi trên VPN đã được mã hóa do đó các địa chỉ bên trong mạng riêng được che giấu và chỉ sử dụng các địa chỉ bên ngoài Internet.

3. Các thành phần cần thiết để tạo kết nối VPN:

- *User Authentication:* cung cấp cơ chế chứng thực người dùng, chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.

- *Address Management:* cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên trên mạng nội bộ.

- *Data Encryption:* cung cấp giải pháp mã hoá dữ liệu trong quá trình truyền nhằm bảo đảm tính riêng tư và toàn vẹn dữ liệu.

- *Key Management:* cung cấp giải pháp quản lý các khoá dùng cho quá trình mã hoá và giải mã dữ liệu.

4. Các thành phần chính tạo nên VPN Cisco:

a. Cisco VPN Router: sử dụng phần mềm Cisco IOS, IPSec hỗ trợ cho việc bảo mật trong VPN. VPN tối ưu hóa các router như là đòn bẩy đang tồn tại sự đầu tư của Cisco. Hiệu quả nhất trong các mạng WAN hỗn hợp.

b. Cisco Secure PIX FIREWALL: đưa ra sự lựa chọn khác của cổng kết nối VPN khi bảo mật nhóm "riêng tư" trong VPN.

c. Cisco VPN Concentrator series: Đưa ra những tính năng mạnh trong việc điều khiển truy cập từ xa và tương thích với dạng site-to-site VPN. Có giao diện quản lý dễ sử dụng và một VPN client.

d. Cisco Secure VPN Client : VPN client cho phép bảo mật việc truy cập từ xa tới router Cisco và Pix Firewalls và nó là một chương trình chạy trên hệ điều hành Window.

e. Cisco Secure Intrusion Detection System(CSIDS) và Cisco Secure Scanner thường được sử dụng để giám sát và kiểm tra các vấn đề bảo mật trong VPN.

f. Cisco Secure Policy Manager and Cisco Works 2000 cung cấp việc quản lý hệ thống VPN rộng lớn.

5. Các giao thức VPN:

Các giao thức để tạo nên cơ chế đường ống bảo mật cho VPN là L2TP, Cisco GRE và IPSec.

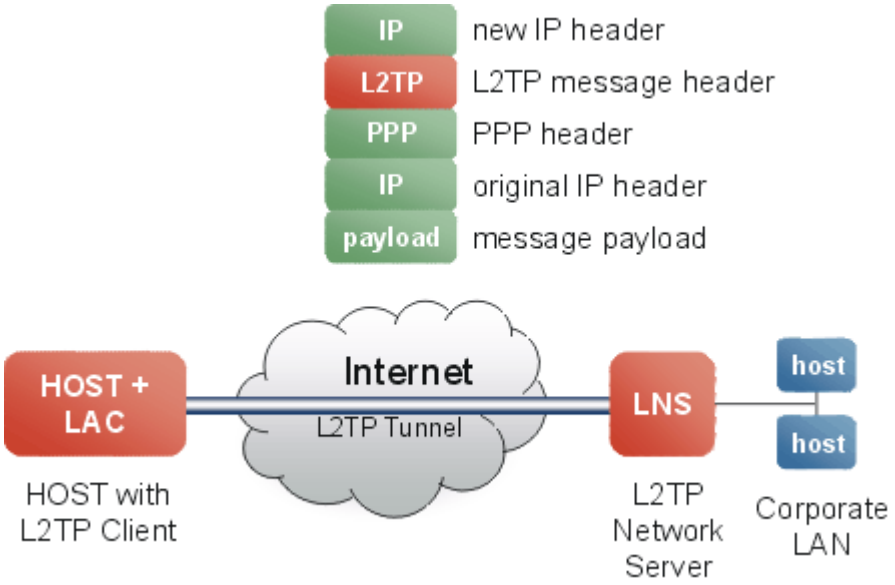
a. L2TP:

- Trước khi xuất hiện chuẩn L2TP (tháng 8 năm 1999), Cisco sử dụng Layer 2 Forwarding (L2F) như là giao thức chuẩn để tạo kết nối VPN. L2TP ra đời sau với những tính năng được tích hợp từ L2F.

- L2TP là dạng kết hợp của Cisco L2F và Mircosoft Point-to-Point Tunneling Protocol (PPTP). Microsoft hỗ trợ chuẩn PPTP và L2TP trong các phiên bản WindowNT và 2000

- L2TP được sử dụng để tạo kết nối độc lập, đa giao thức cho mạng riêng ảo quay số (Virtual Private Dail-up Network). L2TP cho phép người dùng có thể kết nối thông qua các chính sách bảo mật của công ty (security policies) để tạo VPN hay VPDN như là sự mở rộng của mạng nội bộ công ty.

- L2TP không cung cấp mã hóa.



- L2TP là sự kết hợp của PPP(giao thức Point-to-Point) với giao thức L2F(Layer 2 Forwarding) của Cisco do đó rất hiệu quả trong kết nối mạng dial, ADSL, và các mạng truy cập từ xa khác. Giao thức mở rộng này sử dụng PPP để cho phép truy cập VPN bởi những ngườI sử dụng từ xa.

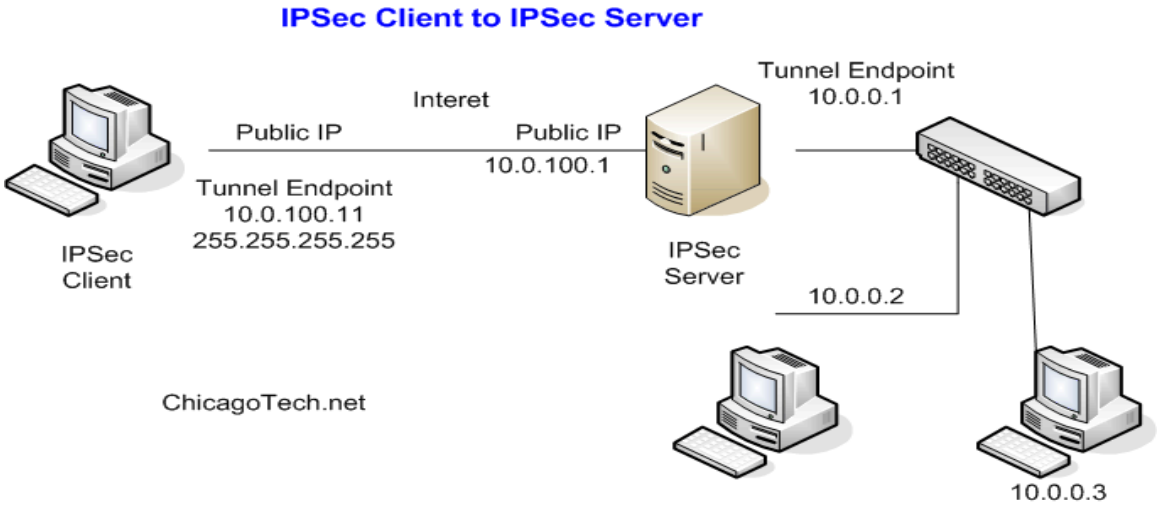
b. GRE:

- Đây là đa giao thức truyền thông đóng gói IP, CLNP và tất cả cá gói dữ liệu bên trong đường ống IP (IP tunnel)

- Với GRE Tunnel, Cisco router sẽ đóng gói cho mỗi vị trí một giao thức đặc trưng chỉ định trong gói IP header, tạo một đường kết nối ảo (virtual point-to-point) tới Cisco router cần đến. Và khi gói dữ liệu đến đích IP header sẽ được mở ra

- Bằng việc kết nối nhiều mạng con với các giao thức khác nhau trong môi trường có một giao thức chính. GRE tunneling cho phép các giao thức khác có thể thuận lợi trong việc định tuyến cho gói IP.

c. IPSec:



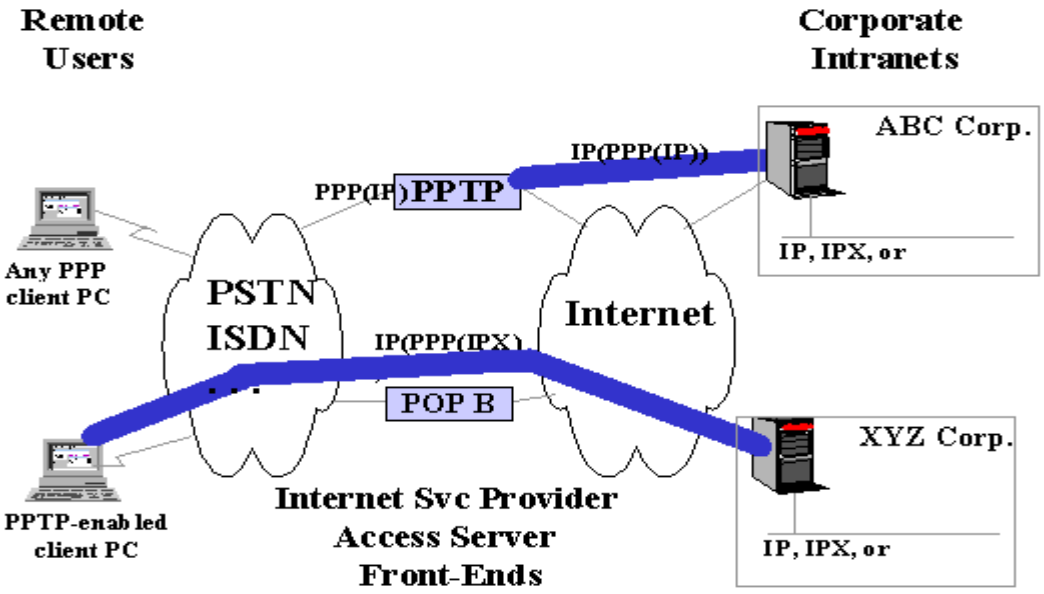
- IPSec là sự lựa chọn cho việc bảo mật trên VPN. IPSec là một khung bao gồm bảo mật dữ liệu (data confidentiality), tính tòan vẹn của dữ liệu (integrity) và việc chứng thực dữ liệu.

- IPSec cung cấp dịch vụ bảo mật sử dụng KDE cho phép thỏa thuận các giao thức và thuật tóan trên nền chính sách cục bộ (group policy) và sinh ra các khóa bảo mã hóa và chứng thực được sử dụng trong IPSec.

d. Point to Point Tunneling Protocol (PPTP):

- Được sử dụng trện các máy client chạy HĐH Microsoft for NT4.0 và Windows 95+ . Giao thức này đươc sử dụng để mã hóa dữ liệu lưu thông trên Mạng LAN. Giống

như giao thức NETBEUI và IPX trong một packet gửI lên Internet. PPTP dựa trên chuẩn RSA RC4 và hỗ trợ bởI sự mã hóa 40-bit hoặc 128-bit.

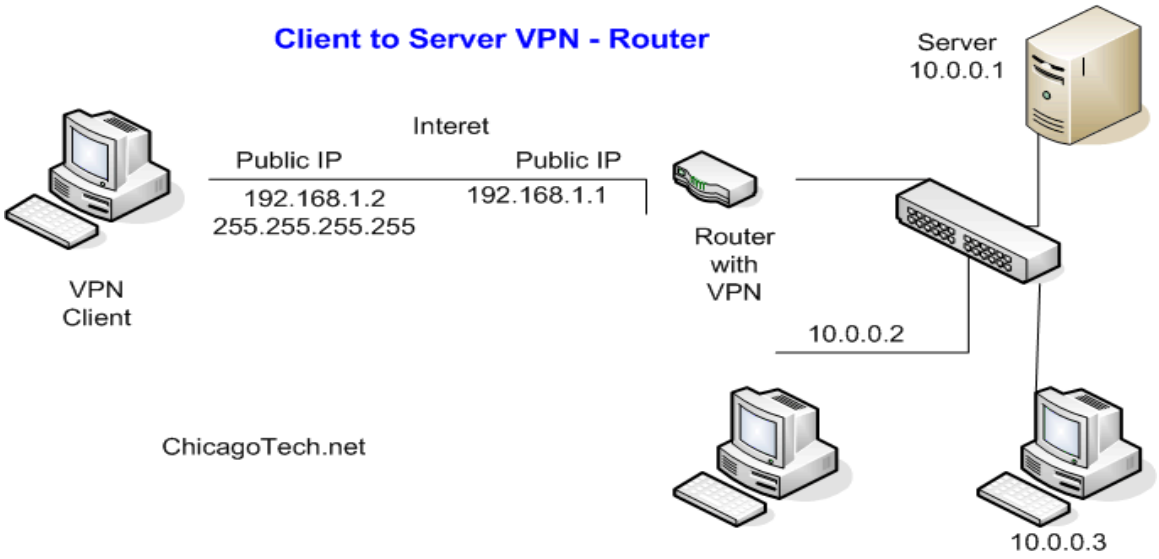


- Nó không được phát triển trên dạng kết nốI LAN-to-LAN và giới hạn 255 kết nối tớI 1 server chỉ có một đường hầm VPN trên một kết nối. Nó không cung cấp sự mã hóa cho các công việc lớn nhưng nó dễ cài đặt và triển khai và là một giảI pháp truy cập từ xa chỉ có thể làm được trên mạng MS. Giao thức này thì được dùng tốt trong Window 2000. Layer 2 Tunneling Protocol thuộc về IPSec.

6. Thiết lập một kết nối VPN:

a. Máy VPN cần kết nối (VPN client) tạo kết nốt VPN (VPN Connection) tới máy chủ cung cấp dịch vụ VPN (VPN Server) thông qua kết nối Internet.

b. Máy chủ cung cấp dịch vụ VPN trả lời kết nối tới



c. Máy chủ cung cấp dịch vụ VPN chứng thực cho kết nối và cấp phép cho kết nối

d. Bắt đầu trao đổi dữ liệu giữa máy cần kết nối VPN và mạng công ty

7. Các dạng kết nối VPN:

a. Remote Access VPNs :

Remote Access VPNs cho phép truy cập bất cứ lúc nào bằng Remote, mobile, và các thiết bị truyền thông của nhân viên các chi nhánh kết nối đến tài nguyên mạng của tổ chức.

Remote Access VPN mô tả việc các người dùng ở xa sử dụng các phần mềm VPN để truy cập vào mạng Intranet của công ty thông qua gateway hoặc VPN concentrator (bản chất là một server). Vì lý do này, giải pháp này thường được gọi là client/server. Trong giải pháp này, các người dùng thường thường sử dụng các công nghệ WAN truyền thống để tạo lại các tunnel về mạng HO của họ.

Một hướng phát triển khá mới trong remote access VPN là dùng wireless VPN, trong đó một nhân viên có thể truy cập về mạng của họ thông qua kết nối không dây. Trong thiết kế này, các kết nối không dây cần phải kết nối về một trạm wireless (wireless terminal) và sau đó về mạng của công ty. Trong cả hai trường hợp, phần mềm client trên máy PC đều cho phép khởi tạo các kết nối bảo mật, còn được gọi là tunnel.

Một phần quan trọng của thiết kế này là việc thiết kế quá trình xác thực ban đầu nhằm để đảm bảo là yêu cầu được xuất phát từ một nguồn tin cậy. Thường thì giai đoạn ban đầu này dựa trên cùng một chính sách về bảo mật của công ty. Chính sách này bao

gồm: qui trình (procedure), kỹ thuật, server (such as Remote Authentication Dial-In User Service [RADIUS], Terminal Access Controller Access Control System Plus [TACACS+]…).

Một số thành phần chính :

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

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

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

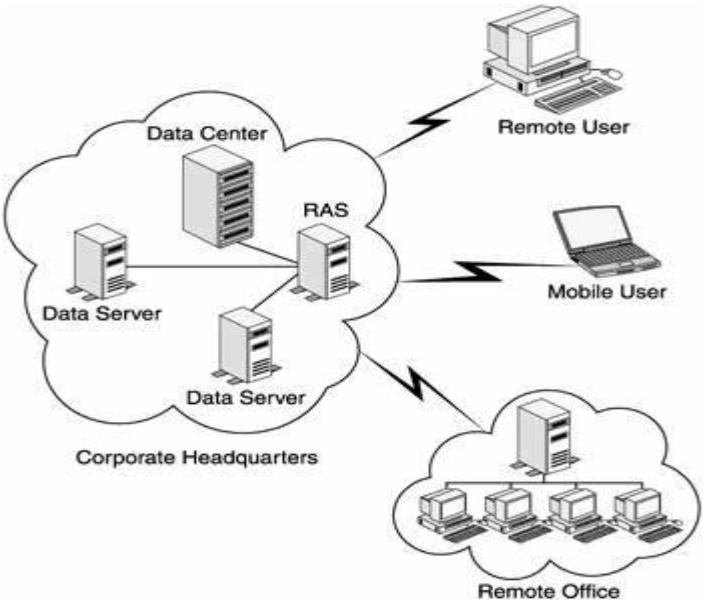


Figure 1-2: The non-VPN remote access setup.

- Bằng việc triển khai Remote Access VPNs, những người dùng từ xa hoặc các chi nhánh văn phòng chỉ cần cài đặt một kết nối cục bộ đến nhà cung cấp dịch vụ ISP hoặc ISP’s POP và kết nối đến tài nguyên thông qua Internet. Thông tin Remote Access Setup được mô tả bởi hình vẽ sau :

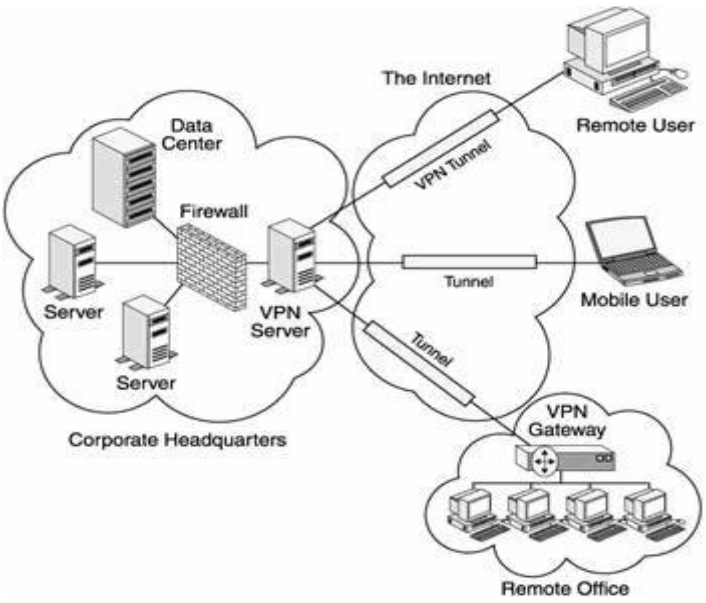


Figure 1-3: The Remote Access VPN setup

Như bạn có thể suy ra từ hình 1-3, thuận lợi chính của Remote Access VPNs :

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

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

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

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

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

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

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

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

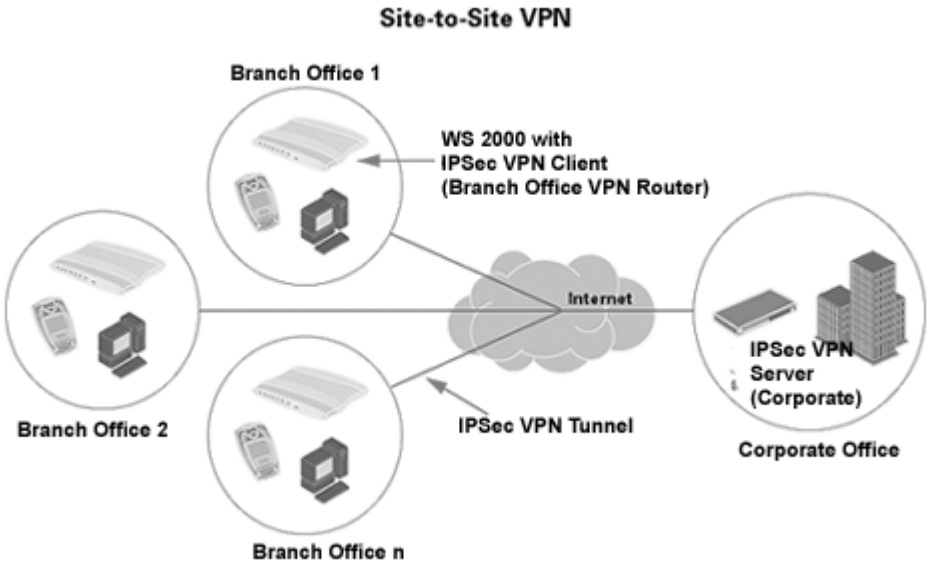
- Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát.

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

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

b. Site - To – Site (Lan – To - Lan):

- Site-to-site VPN(Lan-to-Lan VPN):được áp dụng để cài đặt mạng từ một vị trí này kết nốI tớI mạng của một vị trí khác thông qua VPN. Trong hoàn cảnh này thì việc chứng thực ban đầu giữa các thiết bị mạng được giao cho người sử dụng. Nơi mà có một kết nốI VPN được thiết lập giữa chúng. Khi đó các thiết bị này đóng vai trò như là một gateway, và đảm bảo rằng việc lưu thông đã được dự tính trước cho các site khác. Các router và Firewall tương thích vớI VPN, và các bộ tập trung VPN chuyên dụng đều cung cấp chức năng này.



- Lan-to-Lan VPN có thể được xem như là intranet VPN hoặc extranet VPN(xem xét về mặt chính sách quản lý). Nếu chúng ta xem xét dướI góc độ chứng thực nó có thể được xem như là một intranet VPN, ngược lạI chúng được xem như là một extranet VPN. Tính chặt chẽ trong việc truy cập giữa các site có thể được điều khiển bởi cả hai(intranet và extranet VPN) theo các site tương ứng của chúng. Giải pháp Site to site

VPN không là một remote access VPN nhưng nó được thêm vào đây vì tính chất hoàn thiện của nó.

- Sự phân biệt giữa remote access VPN và Lan to Lan VPN chỉ đơn thuần mang tính chất tượng trưng và xa hơn là nó được cung cấp cho mục đích thảo luận. Ví dụ như là các thiết bị VPN dựa trên phần cứng mớI(Router cisco 3002 chẳng hạn) ở đây để phân loạI được, chúng ta phảI áp dụng cả hai cách, bởI vì harware-based client có thể xuất hiện nếu một thiết bị đang truy cập vào mạng. Mặc dù một mạng có thể có nhiều thiết bị VPN đang vận hành. Một ví dụ khác như là chế độ mở rộng của giảI pháp Ez VPN bằng cách dùng router 806 và 17xx.

- Lan-to-Lan VPN là sự kết nốI hai mạng riêng lẻ thông qua một đường hầm bảo mật. đường hầm bảo mật này có thể sử dụng các giao thức PPTP, L2TP, hoặc IPSec, mục đích của Lan-to-Lan VPN là kết nốI hai mạng không có đường nốI lạI vớI nhau, không có việc thỏa hiệp tích hợp, chứng thực, sự cẩn mật của dữ liệu. bạn có thể thiết lập một Lan-to-Lan VPN thông qua sự kết hợp của các thiết bị VPN Concentrators, Routers, and Firewalls.

- Kết nốI Lan-to-Lan được thiết kế để tạo một kết nốI mạng trực tiếp, hiệu quả bất chấp khoảng cách vật lý giữa chúng. Có thể kết nốI này luân chuyển thông qua internet hoặc một mạng không được tin cậy.Bạn phảI đảm bảo vấn đề bảo mật bằng cách sử dụng sự mã hóa dữ liệu trên tất cả các gói dữ liệu đang luân chuyển giữa các mạng đó.

1. **Intranet VPNs:**

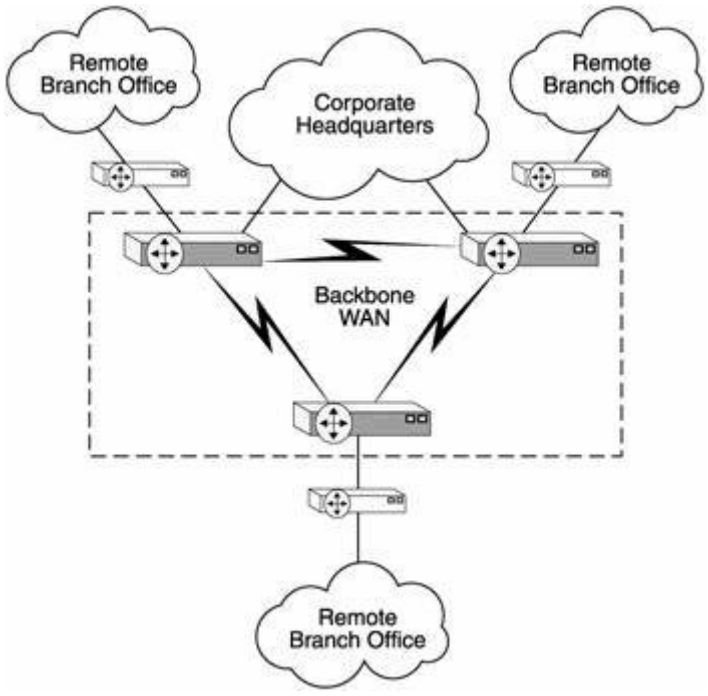


Figure 1-4: The intranet setup using WAN backbone

- Intranet VPNs được sữ dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Corperate Intranet (backbone router) sữ dụng campus router, xem hình bên dưới :

- Theo mô hình bên trên sẽ rất tốn chi phí do phải sữ dụng 2 router để thiết lập được mạng, thêm vào đó, việc triển khai, bảo trì và quản lý mạng Intranet Backbone sẽ rất tốn kém còn tùy thuộc vào lượng lưu thông trên mạng đi trên nó và phạm vi địa lý của toàn bộ mạng Intranet.

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

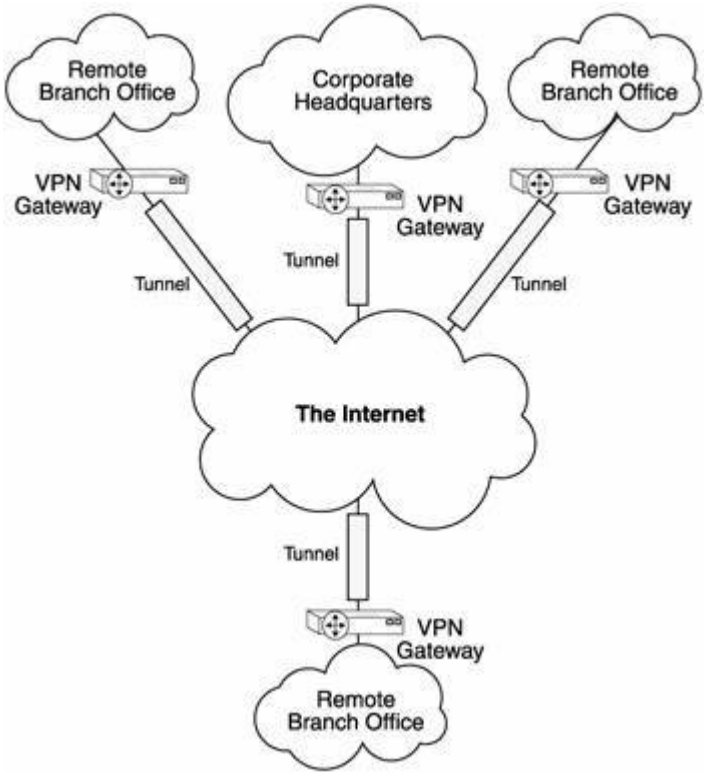


Figure 1-5: The intranet setup based on VPN.

Những thuận lợi chính của Intranet setup dựa trên VPN theo hình 1-5 :

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

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

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

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

Những bất lợi chính kết hợp với cách giải quyết :

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

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

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

2. Extranet VPNs:

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

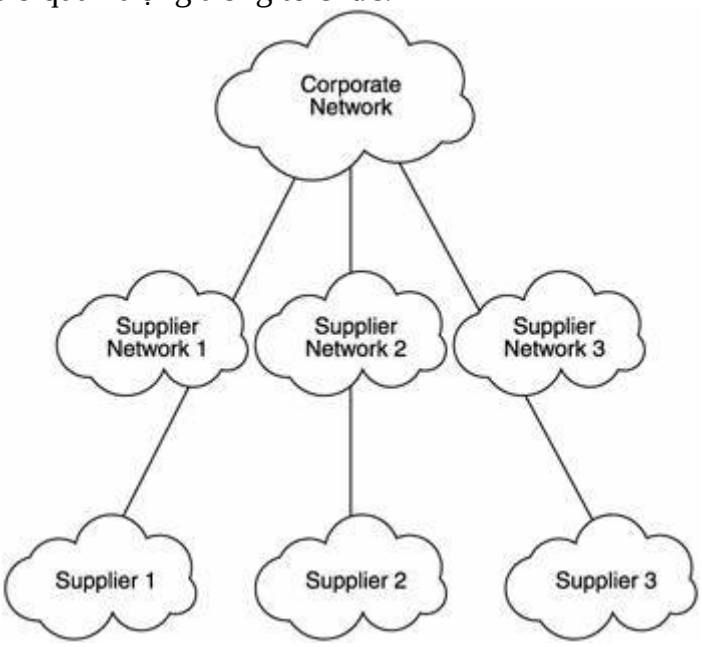


Figure 1-6: The traditional extranet setup.

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

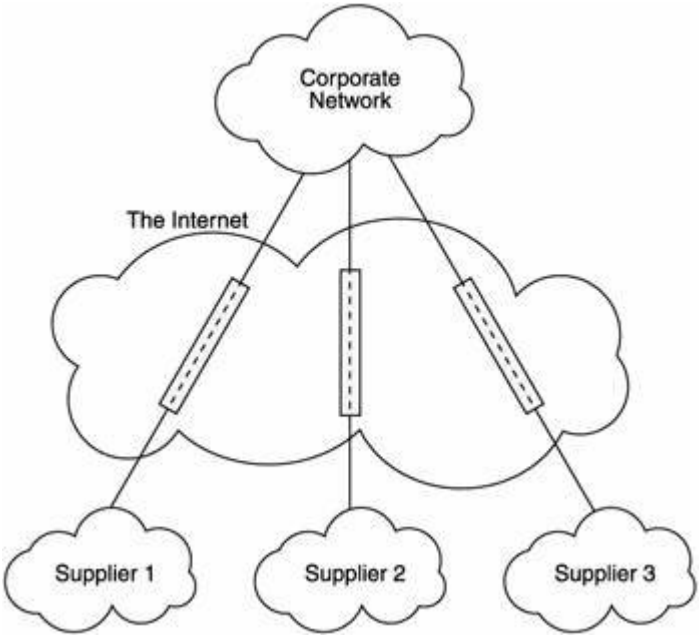


Figure 1-7: The Extranet VPN setup

Một số thuận lợi của Extranet :

- Do hoạt động trên môi trường Internet, bạn có thể lựa chọn nhà phân phối khi lựa chọn và đưa ra phương pháp giải quyết tuỳ theo nhu cầu của tổ chức.- Bởi vì một phần Internet-connectivity được bảo trì bởi nhà cung cấp (ISP) nên cũng giảm chi phí bảo trì khi thuê nhân viên bảo trì.- Dễ dàng triển khai, quản lý và chỉnh sữa thông tin.

Một số bất lợi của Extranet :

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

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

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

- Do dựa trên Internet, QoS(Quality of Service) cũng không được bảo đảm thường xuyên.

II. Tìm Hiểu Về Giao Thức IPSec:

- Thuật ngữ IPSec là một từ viết tắt của thuật Internet Protocol Security. Nó có quan hệ tới một số bộ giao thức (AH, ESP, FIP-140-1, và một số chuẩn khác) được phát triển bởi Internet Engineering Task Force (IETF). Mục đích chính của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI, như hình 6-1.

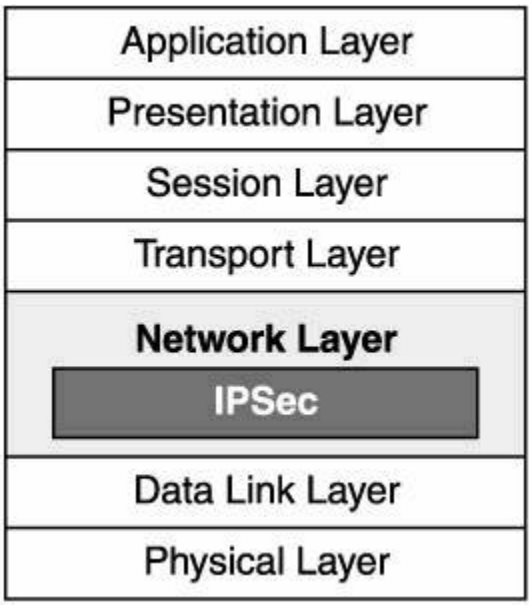


Figure 6-1: The position of IPSec in the OSI model.

- Mọi giao tiếp trong một mạng trên cơ sở IP đều dựa trên các giao thức IP. Do đó, khi một cơ chế bảo mật cao được tích hợp với giao thức IP, toàn bộ mạng được bảo mật bởi vì các giao tiếp đều đi qua tầng 3. (Đó là lý do tai sao IPSec được phát triển ở giao thức tầng 3 thay vì tầng 2).

- IPSec VPN dùng các dịch vụ được định nghĩa trong IPSec để đảm bảo tính toàn vẹn dữ liệu, tính nhất quán, tính bí mật và xác thực của truyền dữ liệu trên một hạ tầng mạng công cộng.

- Ngoài ra,với IPSec tất cả các ứng dụng đang chạy ở tầng ứng dụng của mô hình OSI đều độc lập trên tầng 3 khi định tuyến dữ liệu từ nguồn đến đích. Bởi vì IPSec được tích hợp chặt chẽ với IP, nên những ứng dụng có thể dùng các dịch vụ kế thừa tính năng bảo mật mà không cần phải có sự thay đổi lớn lao nào. Cũng giống IP, IPSec trong suốt với người dùng cuối, là người mà không cần quan tâm đến cơ chế bảo mật mở rộng liên tục đằng sau một chuỗi các hoạt động.

- IPSec hoạt động dựa trên mô hình ngang hàng (peer-to-peer) hơn là mô hình client/server. Security Association (SA) là một qui ước giữa hai bên trong đó thúc đẩy các trao đổi giữa hai bên giao tiếp. Mỗi bên giao tiếp (có thể là thiết bị, phần mềm) phải thống nhất với nhau về các chính sách hoặc các qui tắc bằng cách sẽ dò tìm các chính sách này với đối tác tìm năng của nó. Có hai kiểu SA: ISAKMP SA (còn được biết đến với tên gọi là IKE SAs) và IPSec SA.

- Security Associations (SAs) là một khái niệm cơ bản của bộ giao thức IPSec. SA là một kết nối luận lý theo một phương hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec.

- Các giao thức xác nhận, các khóa, và các thuật toán

- Phương thức và các khóa cho các thuật toán xác nhận được dùng bởi các giao thức Authentication Header (AH) hay Encapsulation Security Payload (ESP) của bộ IPSec

- Thuật toán mã hóa và giải mã và các khóa.

- Thông tin liên quan khóa, như khoảng thời gian thay đổi hay khoảng thời gian làm tươi của các khóa.

- Thông tin liên quan đến chính bản thân SA bao gồm địa chỉ nguồn SA và khoảng thời gian làm tươi.

- Cách dùng và kích thước của bất kỳ sự đồng bộ mã hóa dùng, nếu có.

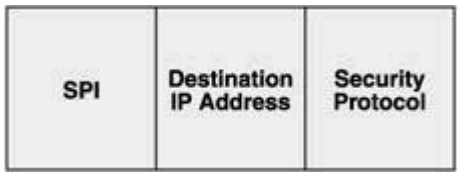


Figure 6-2: A generic representation of the three fields of an IPSec SA.

Như hình 6-2, IPSec SA gồm có 3 trường :

- SPI (Security Parameter Index). Đây là một trường 32 bit dùng nhận dạng giao thức bảo mật, được định nghĩa bởi trường Security protocol, trong bộ IPSec đang dùng. SPI được mang theo như là một phần đầu của giao thức bảo mật và thường được chọn bởi hệ thống đích trong suốt quá trình thỏa thuận của SA.

- Destination IP address. Đây là địa chỉ IP của nút đích. Mặc dù nó có thể là địa chỉ broadcast, unicast, hay multicast, nhưng cơ chế quản lý hiện tại của SA chỉ được định nghĩa cho hệ thống unicast.

- Security protocol. Phần này mô tả giao thức bảo mật IPSec, có thể là AH hoặc ESP.

- Chú thích :

- Broadcasts có nghĩa cho tất cả hệ thống thuộc cùng một mạng hoặc mạng con. Còn multicasts gửi đến nhiều (nhưng không phải tất cả) nút của một mạng hoặc mạng con cho sẵn. Unicast có nghĩa cho 1 nút đích đơn duy nhất. Bởi vì bản chất theo một chiều duy nhất của SA, cho nên 2 SA phải được định nghĩa cho hai bên thông tin đầu cuối, một cho mỗi hướng. Ngoài ra, SA có thể cung cấp các dịch vụ bảo mật cho một phiên VPN được bảo vệ bởi AH hoặc ESP. Do vậy, nếu một phiên cần bảo vệ kép bởi cả hai AH và ESP, 2 SA phải được định nghĩa cho mỗi hướng. Việc thiết lập này của SA được gọi là SA bundle.

- Một IPSec SA dùng 2 cơ sở dữ liệu. Security Association Database (SAD) nắm giữ thông tin liên quan đến mỗi SA. Thông tin này bao gồm thuật toán khóa, thời gian sống của SA, và chuỗi số tuần tự. Cơ sở dữ liệu thức hai của IPSec SA, Security Policy Database (SPD), nắm giữ thông tin về các dịch vụ bảo mật kèm theo với một danh sách thứ tự chính sách các điểm vào và ra. Giống như firewall rules và packet filters, những điểm truy cập này định nghĩa lưu lượng nào được xữ lý và lưu lượng nào bị từ chối theo từng chuẩn của IPSec.

Bộ IPSec đưa ra 3 khả năng chính bao gồm :

- Tính xác nhận và Tính nguyên vẹn dữ liệu (Authentication and data integrity). IPSec cung cấp một cơ chế mạnh mẽ để xác nhận tính chất xác thực của người gửi và kiểm chứng bất kỳ sự sữa đổi không được bảo vệ trước đó của nội dung gói dữ liệu bởi người nhận. Các giao thức IPSec đưa ra khả năng bảo vệ mạnh để chống lại các dạng tấn công giả mạo, đánh hơi và từ chối dịch vụ.

- Sự cẩn mật (Confidentiality). Các giao thức IPSec mã hóa dữ liệu bằng cách sử dụng kỹ thuật mã hóa cao cấp, giúp ngăn cản người chưa chứng thực truy cập dữ liệu

trên đường đi của nó. IPSec cũng dùng cơ chế tạo hầm để ẩn địa chỉ IP của nút nguồn (người gửi) và nút đích (người nhận) từ những kẻ nghe lén.

- Quản lý khóa (Key management). IPSec dùng một giao thức thứ ba, Internet Key Exchange (IKE), để thỏa thuận các giao thức bao mật và các thuật toán mã hóa trước và trong suốt phiên giao dịch. Một phần quan trọng nữa, IPSec phân phối và kiểm tra các khóa mã và cập nhật những khóa đó khi được yêu cầu.

- Hai tính năng đầu tiên của bộ IPSec, authentication and data integrity, và confidentiality, được cung cấp bởi hai giao thức chính của trong bộ giao thức IPSec. Những giao thức này bao gồm Authentication Header (AH) và Encapsulating Security Payload (ESP).

- Tính năng thứ ba, key management, nằm trong bộ giao thức khác, được bộ IPSec chấp nhận bởi nó là một dịch vụ quản lý khóa mạnh. Giao thức này là IKE.

- SAs trong IPSec hiện tại được triển khai bằng 2 chế độ đó là chế độ Transport và chế độ Tunnel được mô tả ở hình 6-7. Cả AH và ESP có thể làm việc với một trong hai chế độ này.

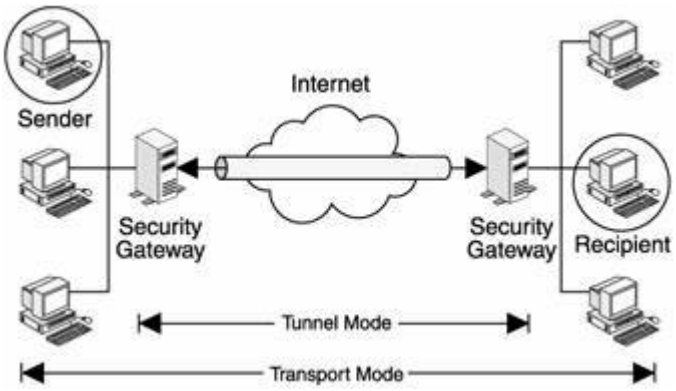


Figure 6-7: The two IPSec modes.

Transport Mode :

- Transport mode bảo vệ giao thức tầng trên và các ứng dụng. Trong Transport mode, phần IPSec header được chèn vào giữa phần IP header và phần header của giao thức tầng trên, như hình mô tả bên dưới, AH và ESP sẽ được đặt sau IP header nguyên thủy. Vì vậy chỉ có tải (IP payload) là được mã hóa và IP header ban đầu là được giữ nguyên vẹn. Transport mode có thể được dùng khi cả hai host hỗ trợ IPSec. Chế độ transport này có thuận lợi là chỉ thêm vào vài bytes cho mỗi packets và nó cũng cho phép các thiết bị trên mạng thấy được địa chỉ đích cuối cùng của gói. Khả năng này cho

phép các tác vụ xử lý đặc biệt trên các mạng trung gian dựa trên các thông tin trong IP header. Tuy nhiên các thông tin Layer 4 sẽ bị mã hóa, làm giới hạn khả năng kiểm tra của gói.

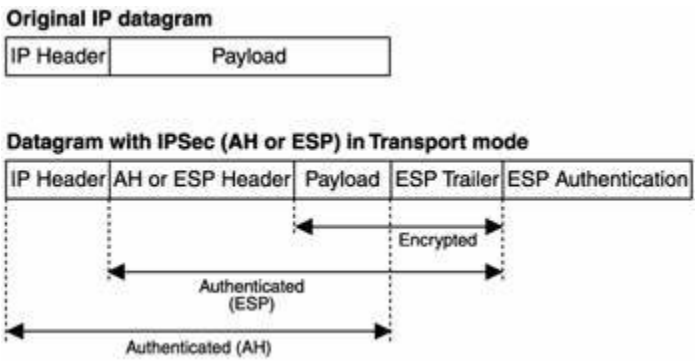


Figure 6-8: IPSec Transport mode—a generic representation.

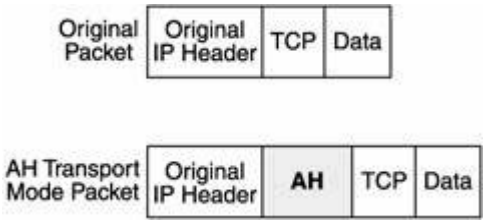


Figure 6-9: AH Transport mode.

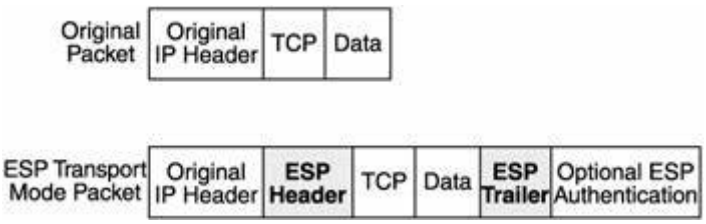


Figure 6-10: ESP Transport mode.

- Transport mode thiếu mất quá trình xữ lý phần đầu, do đó nó nhanh hơn. Tuy nhiên, nó không hiệu quả trong trường hợp ESP có khả năng không xác nhận mà cũng không mã hóa phần đầu IP.

Tunnel Mode :

- Không giống Transport mode, Tunnel mode bảo vệ toàn bộ gói dữ liệu. Toàn bộ gói dữ liệu IP được đóng gói trong một gói dữ liệu IP khác và một IPSec header được chèn vào giữa phần đầu nguyên bản và phần đầu mới của IP.Toàn bộ gói IP ban đầu sẽ bị đóng gói bởi AH hoặc ESP và một IP header mới sẽ được bao bọc xung quanh gói dữ liệu. Toàn bộ các gói IP sẽ được mã hóa và trở thành dữ liệu mới của gói IP mới. Chế độ này cho phép những thiết bị mạng, chẳng hạn như router, hoạt động như một IPSec proxy thực hiện chức năng mã hóa thay cho host. Router nguồn sẽ mã hóa các packets và chuyển chúng dọc theo tunnel. Router đích sẽ giải mã gói IP ban đầu và chuyển nó về hệ thống cuối. Vì vậy header mới sẽ có địa chỉ nguồn chính là gateway.

- Với tunnel hoạt động giữa hai security gateway, địa chỉ nguồn và đích có thể được mã hóa. Tunnel mode được dùng khi một trong hai đầu của kết nối IPSec là security gateway và địa chỉ đích thật sự phía sau các gateway không có hỗ trợ IPSec

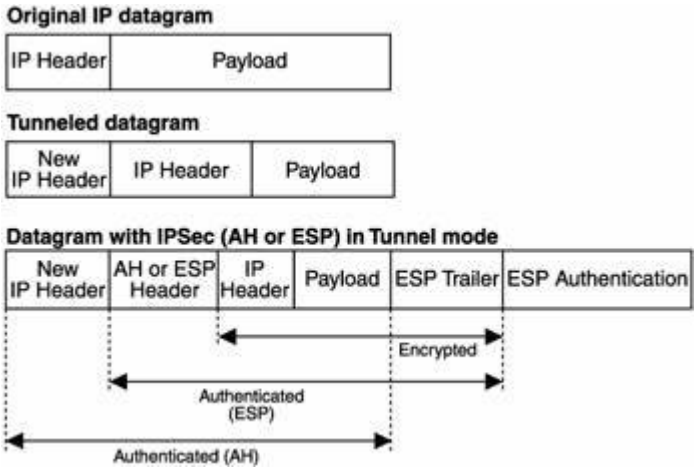


Figure 6-11: IPSec Tunnel mode—a generic representation.

- Trong AH Tunnel mode, phần đầu mới (AH) được chèn vào giữa phần header mới và phần header nguyên bản, như hình bên dưới.

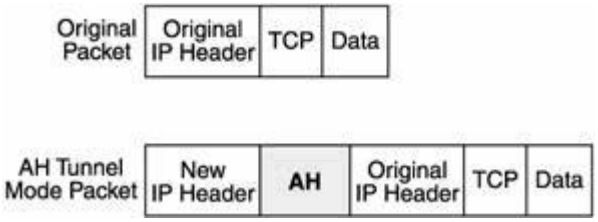


Figure 6-12: AH Tunnel mode.

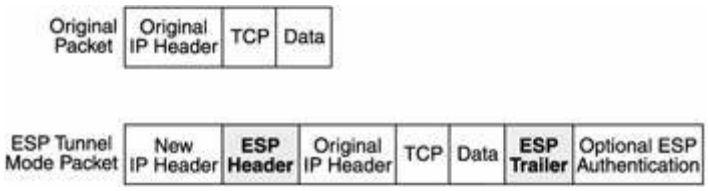


Figure 6-13: ESP Tunnel mode.

- IKE SA là quá trình hai chiều và cung cấp một kênh giao tiếp bảo mật giữa hai bên. Thuật ngữ 'hai chiều' có ý nghĩa là khi đã được thiết lập, mỗi bên có thể khởi tạo chế độ QuickMode, Informational và NewGroupMode. IKE SA được nhận ra bởi các cookies của bên khởi tạo, được theo sau bởi các cookies của trả lời của phía đối tác. Thứ tự các cookies được thiết lập bởi phase 1 sẽ tiếp tục chỉ ra IKE SA, bất chấp chiều của nó. Chức năng chủ yếu của IKE là thiết lập và duy trì các SA. Các thuộc tính sau đây là mức tối thiểu phải được thống nhất giữa hai bên như là một phần của ISAKMP (Internet Security Association and Key Management Protocol) SA:

• Thuật giải mã hóa

• Thuật giải băm được dùng

• Phương thức xác thực sẽ dùng

• Thông tin về nhóm và giải thuật DH

- IKE thực hiện quá trình dò tìm, quá trình xác thực, quản lý và trao đổi khóa. IKE sẽ dò tìm ra được một hợp đồng giữa hai đầu cuối IPSec và sau đó SA sẽ theo dõi tất cả các thành phần của một phiên làm việc IPSec. Sau khi đã dò tìm thành công, các thông số SA hợp lệ sẽ được lưu trữ trong cơ sở dữ liệu của SA.

- Thuận lợi chính của IKE bao gồm:

- IKE không phải là một công nghệ độc lập, do đó nó có thể dùng với bất kỳ cơ chế bảo mật nào.
- Cơ chế IKE, mặc dù không nhanh, nhưng hiệu quả cao bở vì một lượng lớn những hiệp hội bảo mật thỏa thuận với nhau với một vài thông điệp khá ít.

IKE Phases

- Giai đoạn I và II là hai giai đoạn tạo nên phiên làm việc dựa trên IKE, hình 6-14 trình bày một số đặc điểm chung của hai giai đoạn. Trong một phiên làm việc IKE, nó

giả sử đã có một kênh bảo mật được thiết lập sẵn. Kênh bảo mật này phải được thiết lập trước khi có bất kỳ thỏa thuận nào xảy ra.

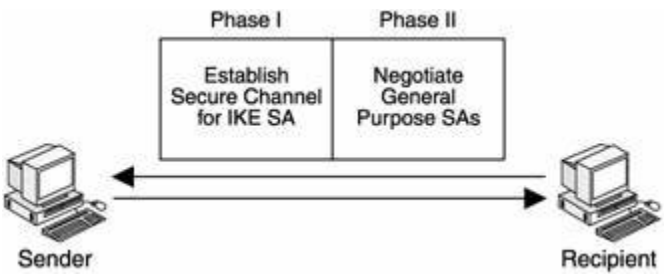


Figure 6-14: The two IKE phases—Phase I and Phase II.

Giai đoạn I của IKE

- Giai đoạn I của IKE đầu tiên xác nhận các điểm thông tin, và sau đó thiết lập một kênh bảo mật cho sự thiết lạp SA. Tiếp đó, các bên thông tin thỏa thuận một ISAKMP SA đồng ý lẫn nhau, bao gồm các thuật toán mã hóa, hàm băm, và các phương pháp xác nhận bảo vệ mã khóa.

- Sau khi cơ chế mã hóa và hàm băm đã được đồng ý ở trên, một khóa chi sẽ bí mật được phát sinh. Theo sau là những thông tin được dùng để phát sinh khóa bí mật :

- Giá trị Diffie-Hellman
- SPI của ISAKMP SA ở dạng cookies
- Số ngẫu nhiên known as nonces (used for signing purposes)

- Nếu hai bên đồng ý sử dụng phương pháp xác nhận dựa trên public key, chúng cũng cần trao đổi IDs. Sau khi trao đổi các thông tin cần thiết, cả hai bên phát sinh những key riêng của chính mình sử dụng chúng để chia sẽ bí mật. Theo cách này, những khóa mã hóa được phát sinh mà không cần thực sự trao đổi bất kỳ khóa nào thông qua mạng.

Giai đoạn II của IKE

- Trong khi giai đoạn I thỏa thuận thiết lập SA cho ISAKMP, giai đoạn II giải quyết bằng việc thiết lập SAs cho IPSec. Trong giai đoạn này, SAs dùng nhiều dịch vụ khác nhau thỏa thuận. Cơ chế xác nhận, hàm băm, và thuật toán mã hóa bảo vệ gói dữ liệu IPSec tiếp theo (sử dụng AH và ESP) dưới hình thức một phần của giai đoạn SA.

- Sự thỏa thuận của giai đoạn xảy ra thường xuyên hơn giai đoạn I. Điển hình, sự thỏa thuận có thể lặp lại sau 4-5 phút. Sự thay đổi thường xuyên các mã khóa ngăn cản các hacker bẻ gãy những khóa này và sau đó là nội dung của gói dữ liệu.

- Tổng quát, một phiên làm việc ở giai đoạn II tương đương với một phiên làmviệc đơn của giai đoạn I. Tuy nhiên, nhiều sự thay đổi ở giai đoạn II cũng có thể được hổ trợ bởi một trường hợp đơn ở giai đoạn I. Điều này làm qua trình giao dịch chậm chạp của IKE tỏ ra tương đối nhanh hơn.

- Oakley là một trong số các giao thức của IKE. Oakley is one of the protocols on which IKE is based. Oakley lần lượt định nghĩa 4 chế độ phổ biến IKE.

IKE Modes

4 chế độ IKE phổ biến thường được triển khai :

- Chế độ chính (Main mode)
- Chế độ linh hoạt (Aggressive mode)
- Chế độ nhanh (Quick mode)
- Chế độ nhóm mới (New Group mode)

Main Mode

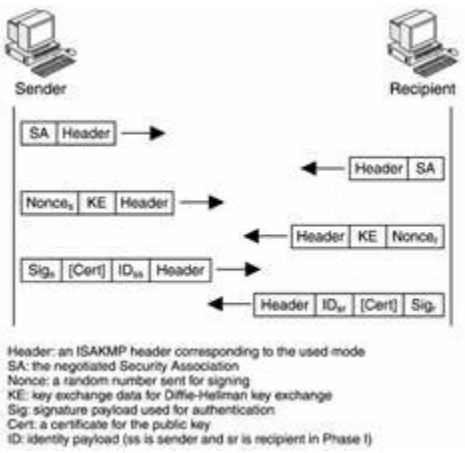
- Main mode xác nhận và bảo vệ tính đồng nhất của các bên có liên quan trong qua trình giao dịch. Trong chế độ này, 6 thông điệp được trao đổi giữa các điểm:

- 2 thông điệp đầu tiên dùng để thỏa thuận chính sách bảo mật cho sự thay đổi.

- 2 thông điệp kế tiếp phục vụ để thay đổi các khóa Diffie-Hellman và nonces. Những khóa sau này thực hiện một vai tro quan trọng trong cơ chế mã hóa.

- Hai thông điệp cuối cùng của chế độ này dùng để xác nhận các bên giao dịch với sự giúp đỡ của chữ ký, các hàm băm, và tuỳ chọn với chứng nhận.

Hình 6-15 mô tả quá trình giao dịch trong chế độ IKE.



Aggressive Mode

- Aggressive mode về bản chất giống Main mode. Chỉ khác nhau thay vì main mode có 6 thông điệp thì chết độ này chỉ có 3 thông điệp được trao đổi. Do đó, Aggressive mode nhanh hơn mai mode. Các thông điệp đó bao gồm :

- Thông điệp đầu tiên dùng để đưa ra chính sách bảo mật, pass data cho khóa chính, và trao đổi nonces cho việc ký và xác minh tiếp theo.

- Thông điệp kế tiếp hồi đáp lại cho thông tin đầu tiên. Nó xác thực người nhận và hoàn thành chính sách bảo mật bằng các khóa.

- Thông điệp cuối cùng dùng để xác nhận người gửi (hoặc bộ khởi tạo của phiên làm việc).

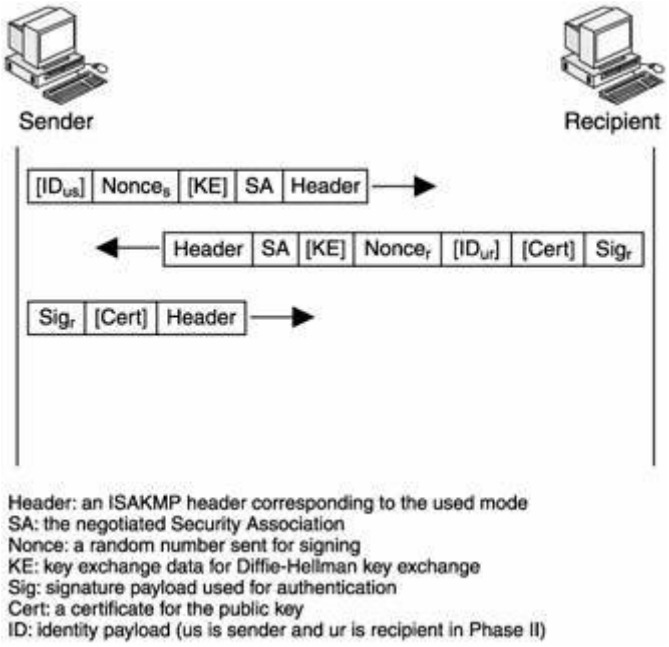


Figure 6-16: Message exchange in IKE Aggressive mode.

Cả Main mode và Aggressive mode đều thuộc giai đoạn I.

Quick Mode

- Chế độ thứ ba của IKE, Quick mode, là chế độ trong giai đoạn II. Nó dùng để thỏa thuận SA cho các dịch vụ bảo mật IPSec. Ngoài ra, Quick mode cũng có thể phát sinh khóa chính mới. Nếu chính sách của Perfect Forward Secrecy (PFS) được thỏa thuận trong giai đoạn I, một sự thay đổi hoàn toàn Diffie-Hellman key được khởi tạo. Mặt khác, khóa mới được phát sinh bằng các giá trị băm.

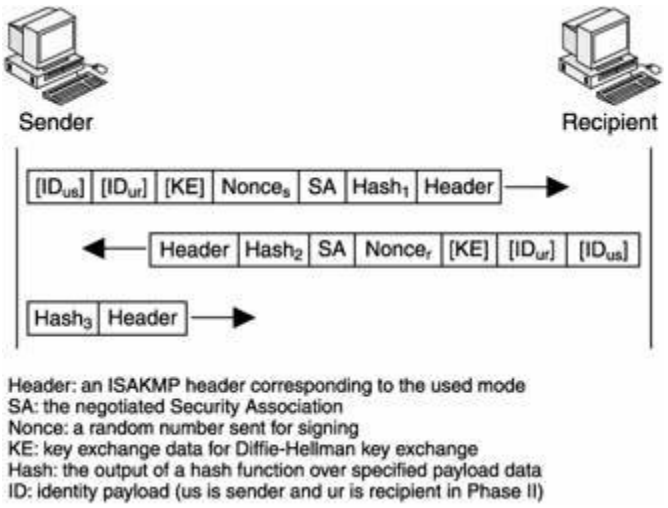


Figure 6-17: Message exchange in IKE Quick mode, which belongs to Phase II.

New Group Mode

- New Group mode được dùng để thỏa thuận một private group mới nhằm tạo điều kiện trao đổi Diffie-Hellman key được dễ dàng. Hình 6-18 mô tả New Group mode. Mặc dù chế độ này được thực hiện sau giai đoạn I, nhưng nó không thuộc giai đoạn II.

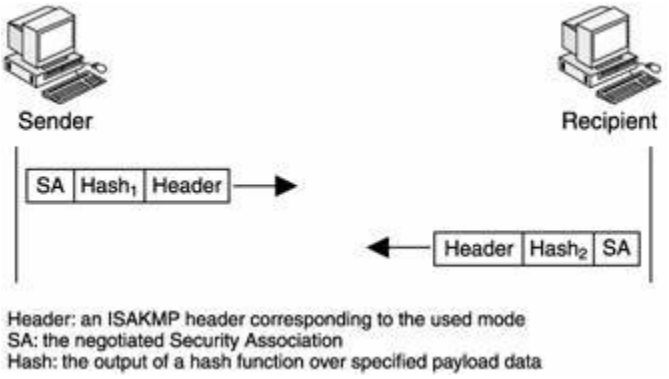


Figure 6-18: Message exchange in IKE New Group mode.

- Ngoài 4 chế độ IKE phổ biến trên, còn có thêm Informational mode. Chế độ này kết hợp với quá trình thay đổ của giai đoạn II và SAs. Chế độ này cung cấp cho các bên có liên quan một số thông tin thêm, xuất phát từ những thất bại trong quá trình thỏa thuận. Ví dụ, nếu việc giải mã thất bại tại người nhận hoặc chữ ký không được xác minh thành công, Informational mode được dùng để thông báo cho các bên khác biết.

III. Tổng Quan Hệ Điều Hành Cisco IOS:

1. Kiến trúc hệ thống:

- Giống như là 1 máy tính, router có 1 CPU có khả năng xử lý các câu lệnh dựa trên nền tảng của router. Hai ví dụ về bộ xử lý mà Cisco dùng là Motorola 68030 và Orion/R4600. Phần mềm Cisco IOS chạy trên Router đòi hỏi CPU hay bộ vi xử lý để giải quyết việc định tuyến và bắc cầu, quản lý bảng định tuyến và một vài chức năng khác của hệ thống. CPU phải truy cập vào dữ liệu trong bộ nhớ để giải quyết các vấn đề hay lấy các câu lệnh.

- Có 4 loại bộ nhớ thường dùng trên một Router của Cisco là

- **ROM :** là bộ nhớ tổng quát trên một con chip hoặc nhiều con. Nó còn có thể nằm trên bảng mạch bộ vi xử lý của router. Nó chỉ đọc nghỉa là dữ liệu không thể ghi lên trên nó. Phần mềm đầu tiên chạy trên một router Cisco được gọi là *bootstrap software* và thường được lưu trong ROM. *Bootstrap software* được gọi khi router khởi động.

- **Flash :** bộ nhớ Flash nằm trên bảng mạch SIMM nhưng nó có thể được mở rộng bằng cách sử dụng thẻ PCMCIA (có thể tháo rời). Bộ nhớ flash hầu hết được sử dụng để lưu trữ một hay nhiều bản sao của phần mềm Cisco IOS. Các file cấu hình hay thông tin hệ thống cũng có thể được sao chép lên flash. Ở vài hệ thống gần đây, bộ nhớ flash còn được sử dụng để giữ bootstrap software.

- Flash memory chứa Cisco IOS software image. Đối với một số loại, Flash memory có thể chứa các file cấu hình hay boot image. Tùy theo loại mà Flash memory có thể là EPROMs, single in-line memory (SIMM) module hay Flash memory card:

- Internal Flash memory:

o Internal Flash memory thường chứa system image.

o Một số loại router có từ 2 Flash memory trở lên dưới dạng single in-line memory modules (SIMM). Nếu như SIMM có 2 bank thì được gọi là dual-bank Flash memory. Các bank này có thể được phân thành nhiều phần logic nhỏ

- Bootflash:

  o Bootflash thường chứa boot image.

  o Bootflash đôi khi chứa ROM Monitor.

- Flash memory PC card hay PCMCIA card:

- Flash memory card dùng để gắn vào Personal Computer Memory Card

- International Association (PCMCIA) slot. Card này dùng để chứa system image, boot image và file cấu hình.

- Các loại router sau có PCMCIA slot:

  o Cisco 1600 series router: 01 PCMCIA slot.

  o Cisco 3600 series router: 02 PCMCIA slots.

  o Cisco 7200 series Network Processing Engine (NPE): 02 PCMCIA slots

  o Cisco 7000 RSP700 card và 7500 series Route Switch Processor (RSP) card chứa 02 PCMCIA slots.

- **RAM :** là bộ nhớ rất nhanh nhưng nó làm mất thông tin khi hệ thống khởi động lại. Nó được sử dụng trong máy PC để lưu các ứng dụng đang chạy và dữ liệu. Trên router, RAM được sử để giữ các bảng của hệ điều hành IOS và làm bộ đệm. RAM là bộ nhớ cơ bản được sử dụng cho nhu cầu lưu trữ các hệ điều hành

- ROM monitor, cung cấp giao diện cho người sử dung khi router không tìm thấy các file image không phù hợp.

- Boot image, giúp router boot khi không tìm thấy IOS image hợp lệ trên flash memory.

- **NVRAM :** Trên router, NVRAM được sử dụng để lưu trữ cấu hình khởi động. Đây là file cấu hình mà IOS đọc khi router khởi động. Nó là bộ nhớ cực kỳ nhanh và liên tục khi khởi động lại.

- Mặc dù CPU và bộ nhớ đòi hỏi một số thành phần để chạy hệ điều hành IOS, router cần phải có các interface khác nhau cho phép chuyển tiếp các packet. Các interface nhận vào và xuất ra các kết nối đến router mang theo dữ liệu cần thiết đến router hay switch. Các loại interface thường dùng là Ethernet và Serial. Tương tự như là các phần mềm driver trên máy tính với cổng parallel và cổng USB, IOS cũng có các driver của thiết bị để hỗ trợ cho các loại interface khác nhau.

- Tất cả các router của Cisco có một cổng console cung cấp một kết nối serial không đồng bộ EIA/TIA-232. Cổng console có thể được kết nối tới máy tính thông qua kết nối serial để làm tăng truy cập đầu cuối tới router. Hầu hết các router đều có cổng auxiliary, nó tương tự như cổng console nhưng đặc trưng hơn, được dùng cho kết nối modem để quản lý router từ xa.

- VD: xem màn hình console của một router 3640 đã khởi động. Chú ý bộ xử lý, interface và thông tin bộ nhớ được liệt kê

Cisco 3640 Router Console Output at Startup

System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

Copyright (c) 1999 by Cisco Systems, Inc.

C3600 processor with 98304 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled program load complete, entry point: 0x80008000, size: 0xa8d168

Self decompressing the image :
[OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software – Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) 3600 Software (C3640-IS-M), Version 12.2(10), RELEASE SOFTWARE (fc2)

Copyright (c) 1986-2002 by Cisco Systems, Inc.

Compiled Mon 06-May-02 23:23 by pwade

Image text-base: 0x60008930, data-base: 0x610D2000

cisco 3640 (R4700) processor (revision 0x00) with 94208K/4096K bytes of memory.

Processor board ID 17746964

R4700 CPU at 100Mhz, Implementation 33, Rev 1.0

Bridging software.

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

5 Ethernet/IEEE 802.3 interface(s)

1 Serial network interface(s)

DRAM configuration is 64 bits wide with parity disabled.

125K bytes of non-volatile configuration memory.

8192K bytes of processor board System flash (Read/Write)

16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

- Khi một router mới khởi động lần đầu, IOS sẽ chạy tiến trình tự động cài đặt và người sử dụng được nhắc trả lời 1 vài câu hỏi. Sau đó IOS sẽ cấu hình hệ thống dựa trên những thông tin nhận được. Sau khi hoàn tất việc cài đặt, cấu hình thường sử dụng nhất được chỉnh sửa bằng cách dùng giao diện câu lệnh (CLI). Còn có một số cách khác để cấu hình router bao gồm HTTP và các ứng dụng quản trị mạng.

2. Cisco IOS CLI:

- Cisco có 3 mode lệnh, với từng mode sẽ có quyền truy cập tới những bộ lệnh khác nhau

- **User mode:** Đây là mode đầu tiên mà người sử dụng truy cập vào sau khi đăng nhập vào router. User mode có thể được nhận ra bởi ký hiệu > ngay sau tên router. Mode này cho phép người dùng chỉ thực thi được một số câu lệnh cơ bản chẳng hạn như xem trạng thái của hệ thống. Hệ thống không thể được cấu hình hay khởi động lại ở mode này.

- **Privileged mode:** mode này cho phép người dùng xem cấu hình của hệ thống, khởi động lại hệ thống và đi vào mode cấu hình. Nó cũng cho phép thực thi tất cả các câu lệnh ở user mode. Privileged mode có thể được nhận ra bởi ký hiệu # ngay sau tên router. Người sử dụng sẽ gõ câu lệnh **enable** để cho IOS biết là họ muốn đi vào Privileged mode từ User mode. Nếu enable password hay enabel secret password được cài đặt, người sử dụng cần phải gõ vào đúng mật khẩu thì mới có quyền truy cập vào privileged mode. Enable secret password sử dụng phương thức mã hoá mạnh hơn khi nó được lưu trữ trong cấu hình, do vậy nó an toàn hơn. Privileged mode cho phép người sử dụng làm bất cứ gì trên router, vì vậy nên sử dụng cẩn thận. Để thoát khỏi privileged mode, người sử dụng thực thi câu lệnh **disable.**

- **Configuration mode:** mode này cho phép người sử dụng chỉnh sửa cấu hình đang chạy. Để đi vào configuration mode, gõ câu lệnh **configure terminal** từ privileged mode. Configuration mode có nhiều mode nhỏ khác nhau, bắt đầu với global configuration mode, nó có thể được nhận ra bởi ký hiệu (config)# ngay sau tên router. Các mode nhỏ trong configuration mode thay đổi tuỳ thuộc vào bạn muốn cấu hình cái gì, từ bên trong ngoặc sẽ thay đổi. Chẳng hạn khi bạn muốn vào mode interface, ký hiệu sẽ thay đổi thành (config-if)# ngay sau tên router. Để thoát khỏi configuration mode, người sủ dụng có thể gõ **end** hay nhấn tổ hợp phím Ctrl-Z

- Chú ý ở các mode, tuỳ vào tình huống cụ thể mà câu lệnh **?** tại các vị trí sẽ hiển thị lên các câu lệnh có thể có ở cùng mức. Ký hiệu **?** cũng có thể sử dụng ở giữa câu lệnh để xem các tuỳ chọn phức tạp của câu lệnh. Example 4-2 hiển thị cách sử dụng câu lệnh **?** với từng mode

- VD: Using Context-Sensitive Help

Router>**?**

Exec commands:

access-enable Create a temporary Access-List entry

access-profile Apply user-profile to interface

clear Reset functions

…

- Bước tiếp theo sẽ hướng dẫn bạn sử dụng câu lệnh thay đổi mode, xem cấu hình hệ thống và cấu hình password. Màn hình CLI của một router 3640 đang chạy hệ điều hành Cisco IOS được hiển thị.

- Bước 1: Vào enable mode bằng cách gõ **enable** và nhấn phím **Enter**

  Router> **enable**

  Router#

- Bước 2: Để xem phiên bản của hệ điều hành IOS đang chạy, gõ lệnh **show version**

  Router# **show version**

  Cisco Internetwork Operating System Software

  IOS (tm) 3600 Software (C3640-IS-M), Version 12.2(10), RELEASE SOFTWARE (fc2)

  Copyright (c) 1986-2002 by Cisco Systems, Inc.

  Compiled Mon 06-May-02 23:23 by pwade

  Image text-base: 0x60008930, data-base: 0x610D2000

  ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE

  (fc1)

  Router uptime is 47 minutes

  System returned to ROM by reload

  System image file is "slot0:c3640-is-mz.122-10.bin"

  cisco 3640 (R4700) processor (revision 0x00) with 94208K/4096K bytes of memory.

  Processor board ID 17746964

R4700 CPU at 100Mhz, Implementation 33, Rev 1.0

Bridging software.

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

5 Ethernet/IEEE 802.3 interface(s)

1 Serial network interface(s)

DRAM configuration is 64 bits wide with parity disabled.

125K bytes of non-volatile configuration memory.

8192K bytes of processor board System flash (Read/Write)

16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Configuration register is 0x2002

- Từ màn hình hiển thị trên cho ta thấy, router này đang chạy hệ điều hành Cisco IOS phiên bản 12.2(10) và bản sao của nó được lưu trong thẻ nhớ Flash PCMCIA trong slot 0

- Bước 3: Tiếp theo, cấu hình tên router thành IOS. Vào configuration mode bằng cách gõ lệnh **configure terminal**

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **hostname IOS**

IOS(config)#

- Chú ý rằng ký hiệu sẽ chuyển ngay thành IOS sau khi bạn gõ câu lệnh **hostname.** Tất cả các thay cấu hình trong Cisco IOS sẽ thực thi ngay lập tức

- Bước 4: Tiếp theo, bạn cần đặt enable password và enable secret password. Enable secret password được lưu trữ bằng cách dùng thuật toán mã hoá rất mạnh và được ghi đè lên enable password nếu nó đã được cấu hình

IOS(config)# **enable password cisco**

IOS(config)# **enable secret san-fran**

IOS(config)# **exit**

IOS#

- Để vào enable mode bạn cần gõ mật khẩu là **san-fran.** Câu lệnh **exit** sẽ đưa bạn quay lại 1 mức trong cấu hình hay thoát khỏi mode con hiện tại

- Bước 5: Sau khi cấu hình tên router và cài đặt password, bạn có thể xem cấu hình đang chạy

IOS# **show running-config**

Building configuration...

Current configuration : 743 bytes

!

version 12.2

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname IOS

!

enable secret 5 1IP7a$HClNetI.hpRdox84d.FYU.

enable password cisco

!

ip subnet-zero

!

```
call rsvp-sync
!
interface Ethernet0/0
no ip address
shutdown
half-duplex
!
interface Serial0/0
no ip address
shutdown
no fair-queue
!
interface Ethernet2/0
no ip address
shutdown
half-duplex
!
interface Ethernet2/1
no ip address
shutdown
half-duplex
!
interface Ethernet2/2
no ip address
```

```
shutdown
half-duplex
!
interface Ethernet2/3
no ip address
shutdown
half-duplex
!
ip classless
ip http server
ip pim bidir-enable
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
!
end
```

- Bước 6: Màn hình sau khi gõ **show running-config** sẽ hiển thị cấu hình hiện thời đang hoạt động trong hệ thống, tuy nhiên cấu hình này sẽ mất nếu như hệ thống khởi động lại. Để lưu cấu hình vào NVRAM, bạn chắc chắn phải gõ lệnh

```
IOS# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

[OK]

- Bước 7: Để xem cấu hình được lưu trong NVRAM, bạn dùng lệnh **show startup-config**

- Trong chuỗi các bước trên, chú ý interface Ethernet và serial được hiển thị trong file cấu hình. Mỗi interface cần có những thông số chắc chắn như sự đóng gói và địa chỉ được cài đặt trước khi interface có thể sử dụng một cách đúng đắn. Thêm vào đó, định tuyến IP và bắc cầu cần phải được cấu hình. Tham khảo việc cài đặt Cisco IOS và hướng dẫn cấu hình tại www.cisco.com cho phiên bản phần mềm của bạn để tham khảo thêm về tất cả các tuỳ chọn cấu hình có thể có và hướng dẫn chi tiết.

- Một vài câu lệnh thường dùng để quản lý hệ thống

Cisco IOS Command	Miêu tả
show interface	Hiển thị trạng thái hiện tại và chi tiết cấu hình cho tất cả các interface trong hệ thống
show processes cpu	Hiển thị việc sử dụng CPU và các tiến trình đang chạy trong hệ thống
show buffers	Xem có bao nhiêu buffers đang được cấp phát hiện thời và sự hoạt động cho việc chuyển tiếp các packet
show memory	Xem có bao nhiêu bộ nhớ được cấp phát cho các chưc năng khác của hệ thống và việc sử dụng bộ nhớ
show diag	Hiển thị chi tiết các thẻ nhớ trong hệ thống
show ip route	Hiển thị bảng IP route đang sử dụng
show arp	Hiển thị địa chỉ MAC ánh xạ từ địa chỉ IP đang dùng trong bảng ARP

3.

IV. Qui Trình Cấu Hình 4 Bước IPSec/VPN Trên Cisco IOS:

- Ta có thể cấu hình IPSec trên VPN qua 4 bước sau đây:

1. Chuẩn bị cho IKE và IPSec
2. Cấu hình cho IKE
3. Cấu hình cho IPSec
   - ✓ Cấu hình dạng mã hóa cho gói dữ liệu

     Crypto ipsec transform-set
   - ✓ Cấu hình thời gian tồn tại của gói dữ liệu và các tùy chọn bảo mật khác

     Crypto ipsec sercurity-association lifetime
   - ✓ Tạo crytoACLs bằng danh sách truy cập mở rộng (Extended Access List)

     Crypto map
   - ✓ Cấu hình IPSec crypto maps
   - ✓ Áp dụng các crypto maps vào các cổng giao tiếp (interfaces)

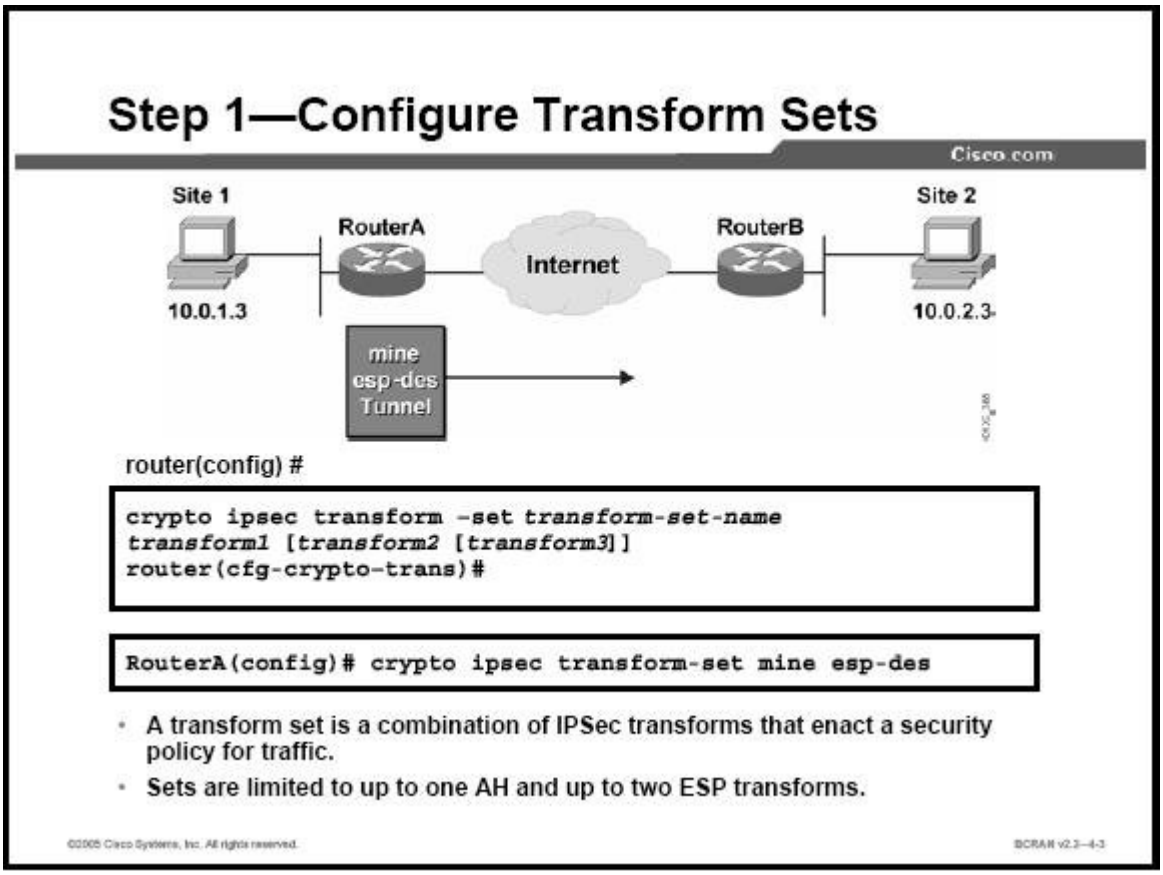
     Crypto map map-name
4. Kiểm tra lại việc thực hiện IPSec

A. Cấu hình cho mã hóa dữ liệu:

- Sau đây bạn sẽ cấu hình Cisco IOS IPSec bằng cách sử dụng chính sách bảo mật IPSec (IPSec Security Policy) để định nghĩa các các chính sách bảo mật IPSec (transform set).

- Chính sách bảo mật IPSec (transform set) là sự kết hợp các cấu hình IPSec transform riêng rẽ được định nghĩa và thiết kế cho các chính sách bảo mật lưu thông trên mạng. Trong suốt quá trình trao đổi ISAKMP IPSec SA nếu xảy ra lỗi trong quá trình IKE Phase 2 quick mode, thì hai bên sẽ sử dụng transform set riêng cho việc bảo vệ dữ liệu riêng của mình trên đường truyền. Transform set là sự kết hợp của các nhân tố sau:

- Cơ chế cho việc chứng thực: chính sách AH
- Cơ chế cho việc mã hóa: chính sách ESP
- Chế độ IPSec (phương tiện truyền thông cùng với đường hầm bảo mật)



- Transform set bằng với việc kết hợp các AH transform, ESP transform và chế độ IPSec (hoặc cơ chế đường hầm bảo mật hoặc chế độ phương tiện truyền thông). Transform set giới hạn từ một cho tới hai ESP transform và một AH transform. Định

nghĩa Transform set bằng câu lệnh cryto ipsec transform-set ở chế độ gobal mode. Và để xoá các cài đặt transform set dùng lệnh dạng no.

- Cú pháp của lệnh và các tham số truyền vào như sau:

crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]

- Các tham số của lệnh crypto ipsec transform-set

Tham số	**Ý nghĩa**
transform-set-name	Chỉ định tên của Transform được tạo hay được thay đổi
transform1, transform2, transform3	Chỉ từ 3 transform trở lên. Những transform được định nghĩa cho giao thức bảo mật IPSec (IPSec Security Protocol) và thuật tóan

- Bạn có thể cấu hình nhiều transform set và chỉ rõ một hay nhiều transform set trong mục crypto map. Định nghĩa các transform set trong mục crypto map được sử dụng trong trao đổi IPSec SA để bảo vệ dữ liệu được đinh nghĩa bởi ACL của mục crypto map. Trong suốt quá trình trao đổi, cả hai bên sẽ tìm kiếm các transform set giống nhau ở cả hai phiá. Khi mà các transform set được tìm thấy, nó sẽ được sử dụng để bảo vệ dữ liệu trên đường truyền như là một phần của các IPSec Sa ở cả 2 phía.

- Khi mà ISAKMP không được sử dụng để thiết lập các Sa, một transform set riêng rẽ sẽ được sử dụng. Transform set đó sẽ không được trao đổi.

- Thay đổi cấu hình Transform set:

B1: Xóa các tranform set từ crypto map

B2: Xóa các transform set trong chế độ cấu hình gobal mode

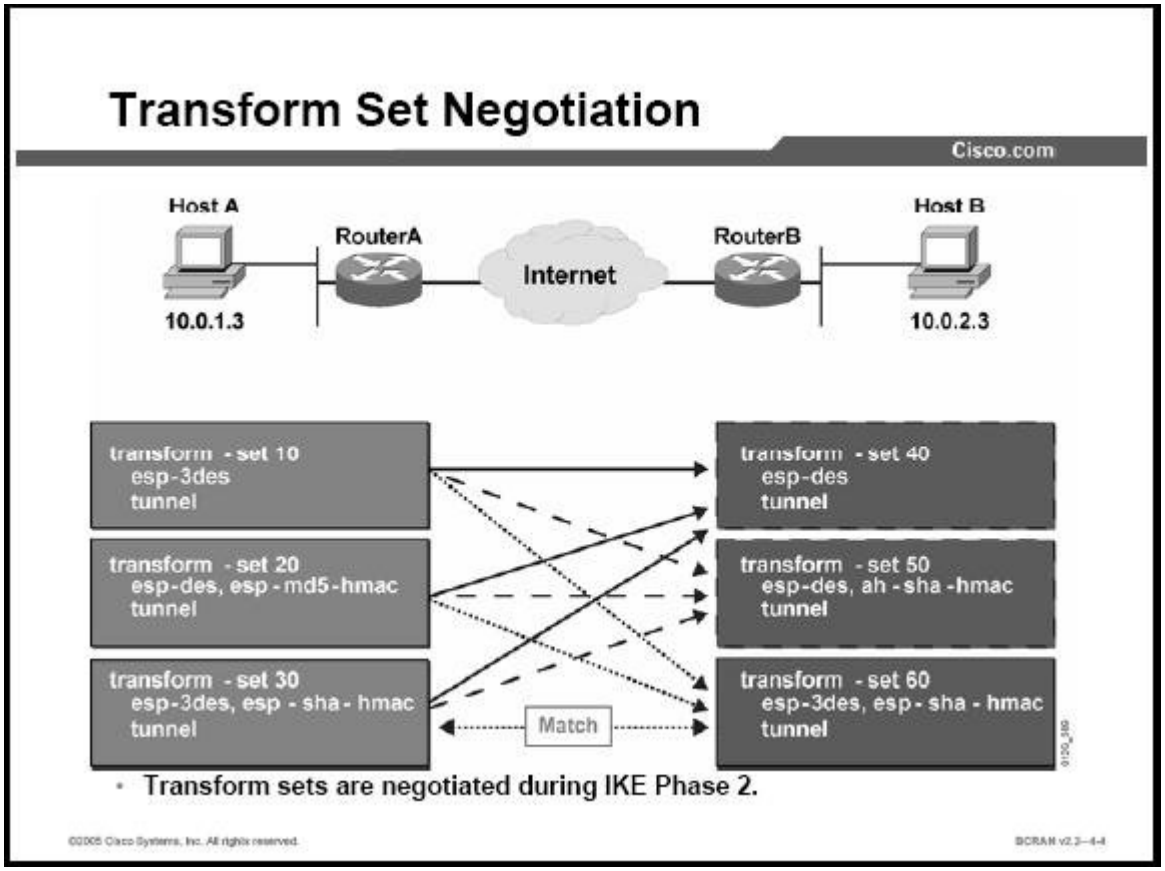
B3: Cấu hình lại transform set với những thay đổi

B4: Gán transform set với crypto map

B5: Xóa cơ sở dữ liệu SA (SA database)

B6: Theo dõi các trao đổi SA và chắc chắn nó hoạt động tốt

- **Cấu hình cho việc trao đổi transform:**



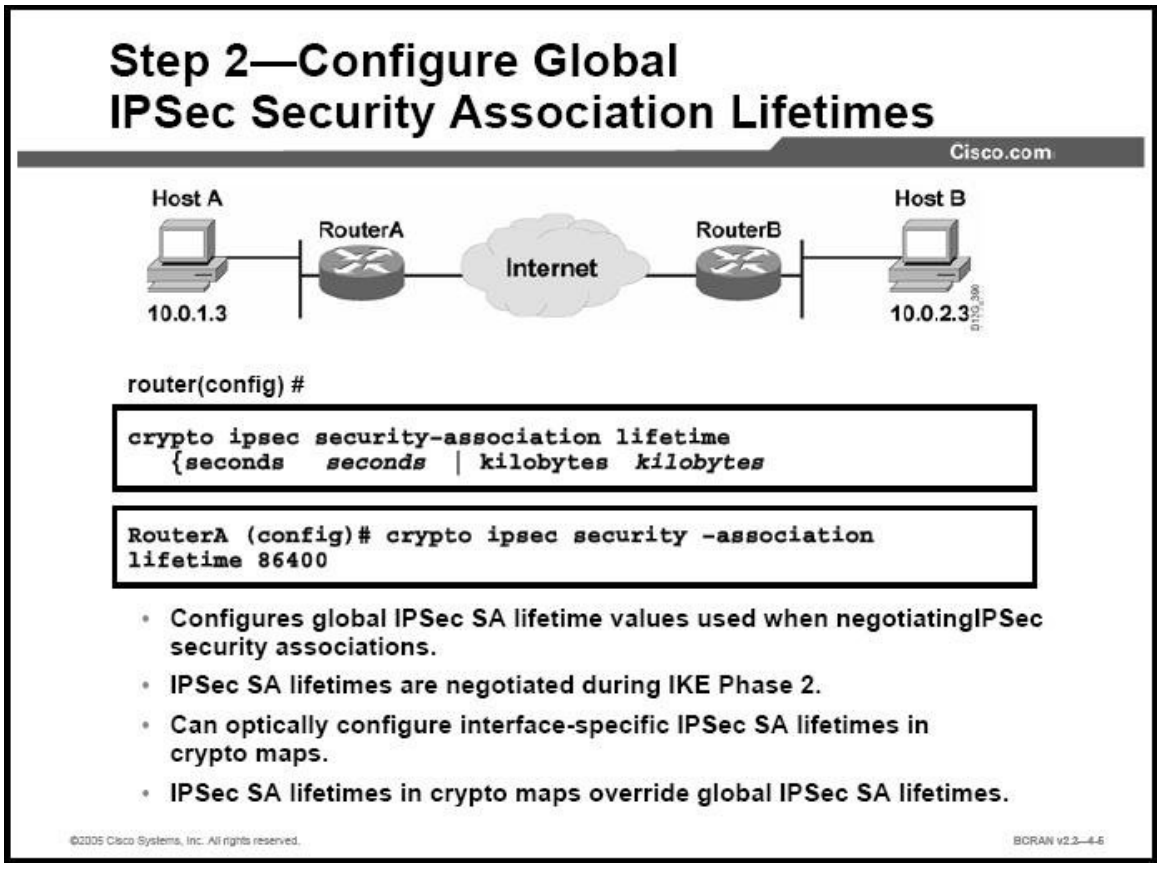
- Tranform set được trao đổi trong suốt chế độ quick mode trong IKE Phase 2 là những các transform set mà bạn cấu hình ưu tiên sử dụng. Bạn có thể cấu hình nhiều transform set và có thể chỉ ra một hay nhiều transform set trong mục crypto map. Cấu hình transform set từ những bảo mật thông thường nhỏ nhất giống như trong chính sách bảo mật của bạn. Những transform set được định nghĩa trong mục crypto map được sử dụng trong trao đổi IPSec SA để bảo vệ dữ liệu được định nghĩa bởi ACL của mục crypto map.

- Trong suốt quá trình trao đổi mỗi bên sẽ tìm kiếm các transform set giống nhau ở cả hai bên như minh họa ở hình trên. Các transform set của Router A được so sánh với một transform set của Router B và cứ tiếp tục như thế. Router A transform set 10, 20, 30 được so sánh với transform set 40 của Router B. Nếu mà không trả về kết quả đúng thì tất cả các transform set của Router A sau đó sẽ được so sánh với transform set tiếp theo của Router B. Cuối cùng transform set 30 của Router A giống với transform set 60 của Router B. Khi mà transform set được tìm thấy, nó sẽ được chọn và áp dụng cho

việc bảo vệ đường truyền như là một phần của IPSec SA của cả hai phía. IPSec ở mỗi bên sẽ chấp nhận một transform duy nhất được chọn cho mỗi SA.

B. Cấu hình thời gian tồn tại của IPSec trong quá trình trao đổi:

- IPSec SA được định nghĩa là thời gian tồn tại của IPSec SA trước khi thực hiện lại quá trình trao đổi tiếp theo. Cisco IOS hỗ trợ giá trị thời gian tồn tại có thể áp dụng lên tất cả các crypto map. Giá trị của global lifetime có thể được ghi đè với những mục trong crypto map.



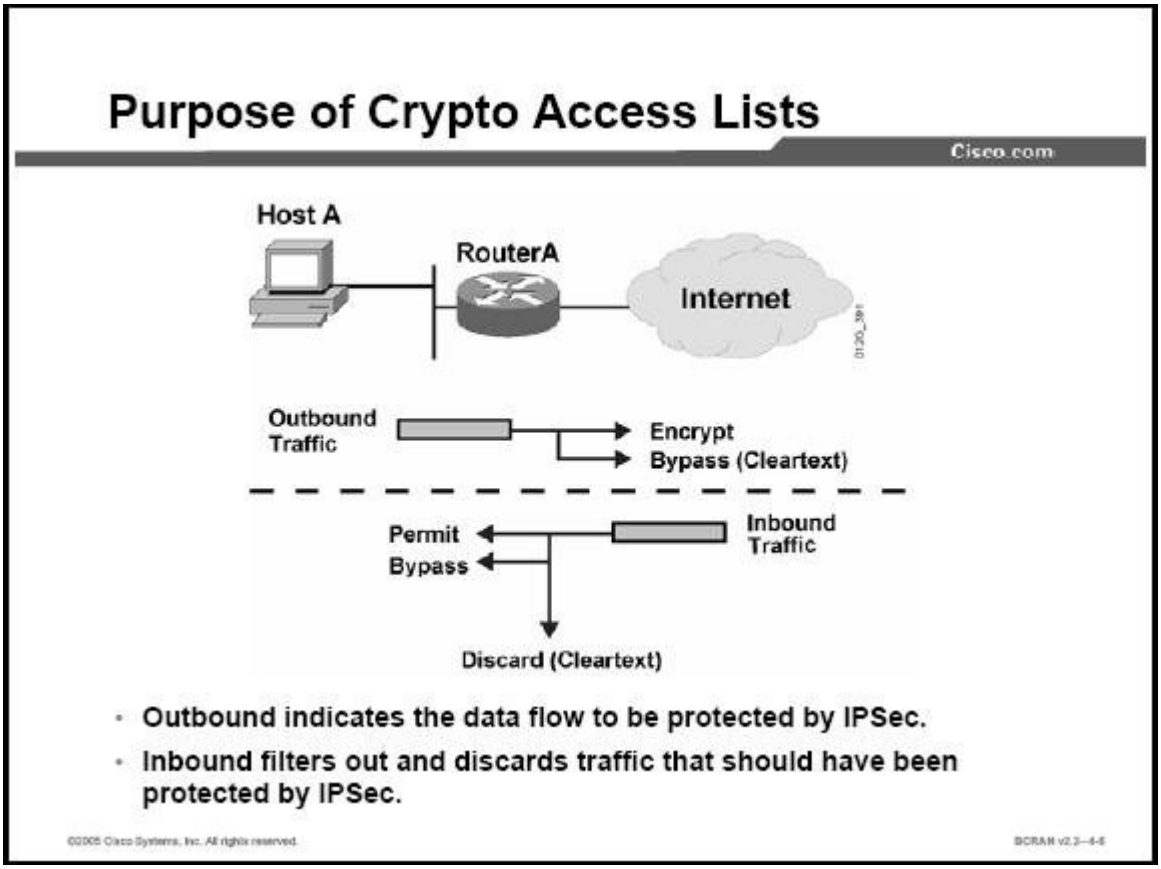
- Bạn có thể thay đổi giá trị thời gian tồn tại của IPSec SA bằng câu lệnh **crypto ipsec security-association lifetime** ở chế độ global configuration mode. Để trả về giá trị mặc định ban đầu sử dụng dạng câu lệnh **no**. Cấu trúc và các tham số của câu lệnh được định nghĩa như sau:

cryto ipsec security-association lifetime {seconds seconds | kilobytes kilobytes}

Câu lệnh	Tham số
seconds seconds	Chỉ định khoảng thời gian tồn tại của IPSec SA. Mặc định là 3600 giây (một giờ)
kilobytes kilobytes	Chỉ định dung lượng trong lưu thông IPSec giữa 2 bên sử dụng để đưa SA trước khi SA hết hạn. Giá trị mặc định 4,608,000 KB

- Cisco khuyến cáo bạn nên sử dụng các giá trị mặc định. Bản thân thời gian tồn tại của mỗi IPSec SA có thể được cấu hình bằng cách sử dụng crypto map.

- Định nghĩa Crypto Access Lists:



-Crypto access list (Crypto ACLs) được sử dụng để định nghĩa những lưu thông (traffic) nào được sử dụng hay kho sử dụng IPSec.

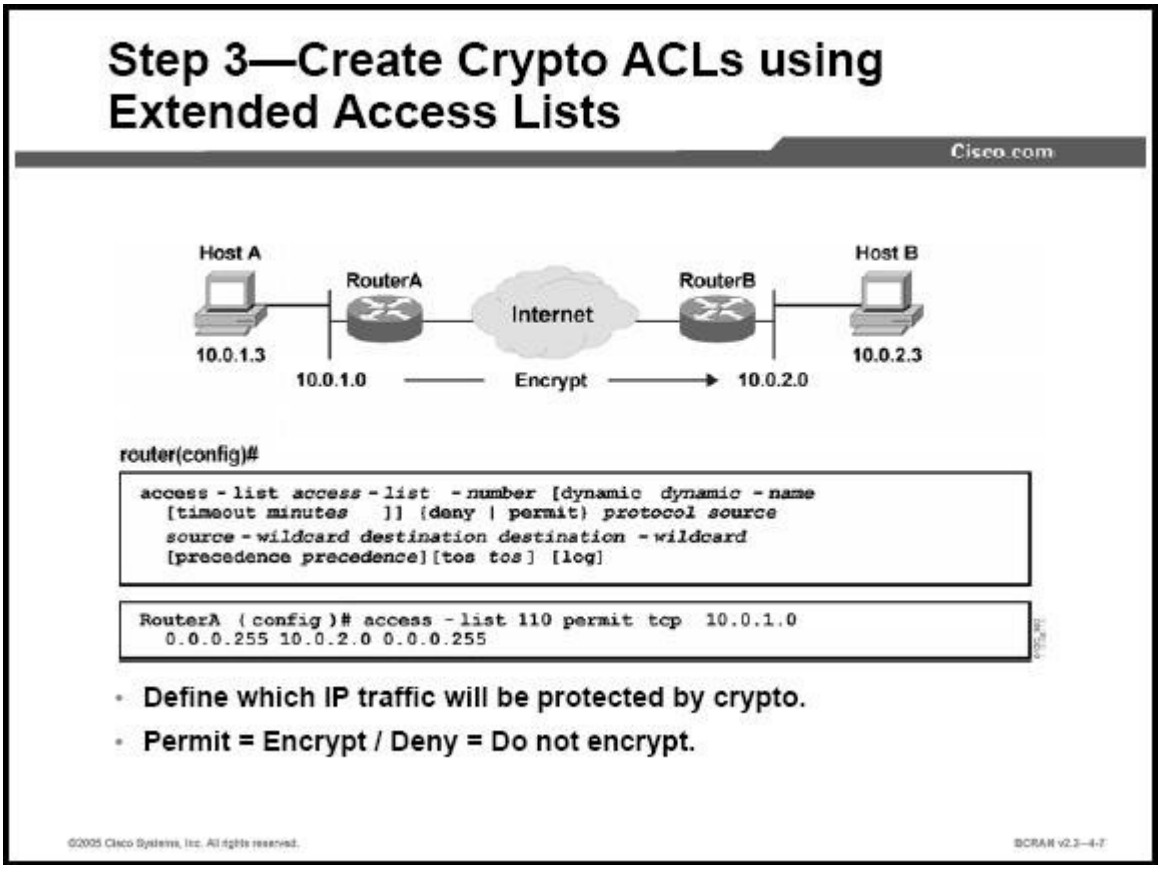
- Crypto ACLs thực hiện các chức năng sau:

- Outbound: Chọn những traffic được bảo vệ bởi IPSec. Những traffic còn lại sẽ được gửi ở dạng không mã hóa.

- Inbound: Nếu có yêu cầu thì inbound access list có thể tạo để lọc ra và loại bỏ những traffic kho được bảo vệ bởi IPSec.

C. Tạo cryto ACLs bằng danh sách truy cập mở rộng (Extends access list):

- Cryto ACLs được định nghĩa để bảo vệ những dữ liệu được truyền tải trên mạng. Danh sach truy cập mở rộng (Extended IP ACLs) sẽ chọn những luồng dữ liệu (IP traffic) để mã hóa bằng cách sử dụng các giao thức truyền tải (protocol), địa chỉ IP (IP address), mạng (network), mạng con (subnet) và cổng dịch vụ (port). Mặc dù cú pháp ACL và extended IP ACLs là giống nhau, nghĩa là chỉ có sự khác biệt chút ít trong crypto ACLs. Đó là cho phép (permit) chỉ những gói dữ liệu đánh dấu mới được mã hóa và từ chối (deny) với những gói dữ liệu được đánh dấu mới không được mã hóa. Crypto ACLs hoạt động tương tự như extendeds IP ACL đó là chỉ áp dụng trên những luồng dữ liệu đi ra (outbound traffic) trên một interface.



- Cú pháp câu lệnh và các tham số được định nghĩa cho dạng cơ bản của danh sách extended IP ACL như sau:

access-list access-list-number { permit | deny } protocol source

Source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log]

Access-list access-list-number command	Tham Số
Permit	Tất cả các luồng dữ liệu (traffic IP)sẽ được đánh dấu để được bảo vệ bằng cryto phải sử dụng chính sách bảo mật (policy) liệt kê cho phù hợp với các mục trong crypto map (crypto map entry)
Deny	Cho biết những luồng dữ liệu (traffic) từ router nào tới router nào là an tòan
Source and destination	Đó là những mạng (network), mạng con (subnet) hoặc là máy trạm (host)

- **Ghi chú:** Mặc dù cấu trúc ACL là không đổi nhưng về ý nghĩa có khác so với cryto ACLs. Đó là chỉ cho phép (permit) những gói dữ liệu được đánh dấu mới được mã hóa và từ chối (deny) những gói dữ liệu được đánh dấu không được mã hóa.

- Bất cứ luồng dữ liệu nào đến (traffic inbound) không được bảo vệ sẽ được đánh dấu *permit* trong crypto ACL của mục crypto map giống như IPSec sẽ hủy bỏ gói tin đó. Gói tin bọ hủy bỏ bởi vì luồng dữ liệu đã được bảo vệ bằng IPSec.

- Nếu bạn thực sự muốn dữ liệu tới nơi nhận là sự kết hợp của chỉ một dạng bảo mật IPSec (chỉ chứng thực-authentication) và những dữ liệu khác tới nơi nhận là sự kết hợp của nhiều dạng bảo mật khác (cả chứng thực và mã hóa) thì bạn phải tạo hai crypto ACLs khác nhau để định nghĩa hai dạng của dữ liệu gửi đi. Hai ACLs khác nhau sẽ được sử dụng trong những mục crypto map khác nhau của những IPSec policy khác nhau.

- **Chú ý:** Cisco khuyến cáo bạn nên tránh việc sử dụng từ khóa **any** để những địa chỉ nơi gửi và đích tới. Câu lệnh **permit any any** rất dễ xảy ra lỗi bởi vì tất cả các

luồng dữ liệu gửi đi (outbound traffic) sẽ được bảo vệ và tất cả sẽ được gử tới nơi nhận phù hợp trong crypto map entry. Sau đó tất cả dữ liệu gửi tới (inbound packet) mà thiếu sự bảo vệ của IPSec sẽ bị bỏ đi, bao gồm cả các gói dữ liệu cho giao thức định tuyến (routing protocol), NTP, echo, echo response và nhiều cái khác.

- Phải giới hạn những cái cần thiết khi mà định nghĩa những gói dữ liệu được bảo mật trong cryptoACLs. Nếu cần phải sử dụng từ khóa **any** trong câu lệnh permit, cần phải mở đầu câu lệnh với một chuỗi các câu lệnh **deny** để lọc các luồng dữ liệu đi ra mà bạn không muốn bảo vệ.

D. Cấu hình IPSec crypto maps:

E. Áp dụng các crypto maps vào các cổng giao tiếp (interfaces):

V. Cách Thức Truy Cập Vào Thiết Bị Mạng (Telnet/SNMP):

VI.

.