BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC HOA SEN
KHOA KHOA HỌC VÀ CÔNG NGHỆ

KHÓA LUẬN TỐT NGHIỆP

Tên đề tài:

XÂY DỰNG FIREWALL ASA VÀ IPS BẢO VỆ MẠNG

Giảng viên hướng dẫn : Thầy Đinh Ngọc Luyện
Nhóm sinh viên thực hiện: Trần Kim Phượng
Lê Trung Tín
Lớp : VT071

Tháng 12 /năm 2010

TRÍCH YẾU LUẬN ÁN

Trong thời gian thực hiện khóa luận tốt nghiệp, chúng tôi đã nghiên cứu về những công nghệ bảo mật sau:

- Tìm hiểu các công nghệ chung của tường lửa tại lớp Network, Transport và Application.
- Phân tích các dạng, phương thức hoạt động và giao thức cũng như thuật toán trong VPN.
- Phân tích nguyên lý hoạt động, cách phát hiện tấn công trên IDS/IPS.
- Xây dựng tường lửa hệ thống mạng trường Đại học Hoa Sen, triển khai VPN và IDS/IPS.

Nhờ việc sử dụng thành công phần mềm mô phỏng các thiết bị mạng, nhóm chúng tôi có thể tự tay xây dựng hệ thống mạng trường Đại Học Hoa Sen từ giai đoạn phân tích yêu cầu, xác định các tài khoản người dùng, thiết kế, phác thảo mô hình mạng đến khi đi vào cấu hình trên các phần mềm mô phỏng. Qua đó, chúng tôi đã đạt được những kết quả đáng khích lệ sau:

- Hiểu thêm về tường lửa, kiến trúc cũng như chức năng tường lửa. Ngoài ra, chúng tôi còn đi sâu phân tích các công nghệ chung của tường lửa tại lớp Network, Transport và Application trong mô hình OSI.
- Nghiên cứu về VPN, giao thức sử dụng trong VPN đồng thời tìm hiểu cách thức hoạt động VPN. Tìm hiểu nguyên lý hoạt động IDS/IPS, phân tích các phương thức phát hiện tấn công, lợi ích cũng như hạn chế từng phương thức.
- Hiểu được các bước xây dựng hệ thống mạng doanh nghiệp, từ giai đoạn phân tích yêu cầu, thiết kế sơ đồ mạng đến bước triển khai cấu hình đồng thời ứng dụng giải pháp VPN và hệ thống IDS/IPS.
- Đi sâu tìm hiểu một số công nghệ triển khai thêm nhằm tăng tính bảo mật an toàn dữ liệu nhằm bảo đảm hệ thống mạng luôn sẵn sàng hoạt động liên tục ngay cả khi gặp sự cố, tận dụng tối đa tài nguyên hệ thống cũng như phân chia tải mạng cho dãy tường lửa kiểm tra như Load Balancing, Failover, HSRP…; xác thực người dùng với kỹ thuật IEEE 802.1x và công nghệ VOIP nhằm cung cấp dịch vụ thoại cho người dùng.

MỤC LỤC

Trang

Phần 3: Xây dựng VPN giữa hai cơ sở của đại học Hoa Sen

Phần 4: Xây dựng IPS & IDS

DANH SÁCH HÌNH

DANH SÁCH BẢNG

LỜI CẢM ƠN

Trước tiên, chúng tôi xin chân thành cảm ơn toàn thể Ban Giám Hiệu Đại học Hoa Sen Thành phố Hồ Chí Minh đã tạo điều kiện cho chúng tôi hoàn thành tốt bài cáo cáo khóa luận tốt nghiệp này.

Đồng thời, chúng tôi cũng gửi đến quý thầy cô trong khoa Khoa Học và Công Nghệ trường Đại Học Hoa Sen lời cảm ơn sâu sắc và chân thành. Các thầy cô đã tận tình chỉ bảo giúp đỡ trong suốt quá trình thực hiện khóa luận. Đặc biệt là thầy Đinh Ngọc Luyện – Giảng viên khoa Khoa Học và Công Nghệ, người trực tiếp hướng dẫn em hoàn thành đề tài này.

Tuy nhiên, do thời gian có hạn cũng như kiến thức và kinh nghiệm còn hạn chế nên báo cáo này không tránh khỏi những thiếu sót. Sự góp ý chân thành của thầy cô sẽ giúp chúng tôi hoàn thiện hơn bài báo cáo này cũng như tích lũy thêm kiến thức và kinh nghiệm cho bản thân. Đây sẽ là hành trang giúp chúng tôi tự tin đương đầu với các thử thách mới ngoài xã hội

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Giáo viên hướng dẫn ký tên

LỜI MỞ ĐẦU

Trong thời kì hội nhập, khi nhu cầu trao đổi dữ liệu qua hệ thống mạng máy tính ngày càng tăng cao, Internet càng trở nên vô cùng quan trọng, ảnh hưởng đến tất cả các lĩnh vực kinh tế xã hội, an ninh quốc phòng của quốc gia. Thực tế ở Việt Nam, Internet đã được ứng dụng và phát triển rộng rãi (phổ cập tới xấp xỉ 25% dân số), dẫn đến số tội phạm công nghệ cao ngày càng nhiều, có không ít cuộc tấn công trên mạng gây ra hậu quả hết sức nghiêm trọng, làm tê liệt hệ thống giám sát an ninh hay phá hoại cơ sở dữ liệu quốc gia, đánh cắp thông tin mật Nhà nước… Đối với doanh nghiệp, vấn đề bảo đảm an ninh, an toàn thông tin trên mạng là mối quan tâm hàng đầu của hầu hết công ty, tổ chức và các nhà cung cấp dịch vụ. Cùng với sự bùng nổ khoa học kỹ thuật, các phương thức tấn công ngày càng tinh vi hơn khiến hệ thống an ninh mạng trở nên mất hiệu qủa.

Bill Archer, Chủ tịch hãng AT&T tại châu Âu, phát biểu "Chúng tôi nhận thấy mật độ tấn công trong vòng 6 tháng qua đã dày hơn rất nhiều so với hai năm trước". Đặc biệt ở Việt Nam, vấn đề trên càng phải đầu tư, xem xét hơn bao giờ hết. Theo khảo sát của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) dựa vào các tiêu chuẩn an toàn thông tin thì 40% doanh nghiệp Việt Nam không có hệ thống tường lửa, 70% không có quy trình xử lý sự cố an toàn thông tin và 85% không có chính sách về an ninh mạng. Hơn nữa, theo phân tích của Kaspersky, năm 2010, Việt Nam đứng thứ 5 thế giới trong số những quốc gia chịu nhiều thiệt hại nhất do tấn công trên mạng (sau Ấn Độ và Mỹ, xếp đầu bảng là Trung Quốc và Nga). Việc xây dựng hệ thống an ninh mạng sao cho vừa đảm bảo an toàn, bảo mật thông tin vừa tận dụng hiệu năng mạng đang trở thành câu hỏi đau đầu đối với các tổ chức doanh nghiệp không những ở Việt Nam mà còn trên toàn thế giới.

Nhận thấy những nguy cơ đó, xuất phát từ niềm say mê nghiên cứu các kỹ thuật bảo mật mạng, nhóm chúng tôi quyết định chọn đề tài "Xây dựng Firewall ASA và IPS bảo vệ mạng", với mong muốn đem lại cho doanh nghiệp mô hình đáp ứng được các yêu cầu về bảo mật mà vẫn đảm bảo hiệu năng hoạt động mạng. Qua đó, chúng tôi cũng trang bị cho mình thêm nhiều kiến thức để chuẩn bị thử sức với thách thức mới ngoài xã hội.

PHẦN 1: TỔNG QUAN BÁO CÁO

1.1 Mục tiêu nghiên cứu

Như đã đề cập, nhóm chúng tôi tập trung nghiên cứu các công nghệ chung của tường lửa tại lớp Network, Transport và Application đồng thời phân tích kỹ thuật liên quan VPN, thiết kế xây dựng hệ thống VPN. Bên cạnh đó, để tăng cường bảo mật mạng, chúng tôi tìm hiểu IDS/IPS, nguyên lý hoạt động và các loại IDS/IPS sử dụng phổ biến ngày nay. Cuối cùng, nhóm chúng tôi xây dựng thành công các kỹ thuật này trên hệ thống mạng Đại Học Hoa Sen.

1.2 Giới hạn đề tài

Do thời gian và chi phí đầu tư còn hạn chế, nhóm chúng tôi xây dựng, triển khai hệ thống mạng dựa trên phần mềm mô phỏng thiết bị thực tế như tường lửa, Switch, Router…mà ở đây chủ yếu là tường lửa Cisco ASA - một trong những tường lửa phổ biến hiện nay, hỗ trợ:

- Sự kết hợp hài hòa, bổ sung cho nhau giữa Stateful Packet Filtering và Proxy. ASA cung cấp cái nhìn toàn vẹn lưu lượng mạng nhờ kiểm tra, phân tích gói tin từ lớp 3 đến lớp 7.
- Xác thực (Authentication) và ủy quyền (Authorization).
- Triển khai hệ thống VPN, IPS/IDS.
- Khả năng dự phòng, cân bằng tải khi gặp sự cố.

1.3 Phương pháp nghiên cứu

Nhờ việc kết hợp sử dụng các phương pháp bàn giấy, phương pháp thực nghiệm – xây dựng các bài thực hành nghiên cứu tính năng của tường lửa và phương pháp tổng hợp phân tích dựa trên cơ sở lý thuyết bảo mật và các kết quả rút ra từ thực tế, chúng tôi đã hiểu thêm được nhiều các công nghệ tường lửa và các kỹ thuật bảo mật khác nhau trong hệ thống mạng.

1.4 Cấu trúc trình bày

Phần 1: Tổng quan bài báo cáo khóa luận tốt nghiệp, giới thiệu lý do chọn đề tài, giới hạn đề tài cùng các phương pháp nghiên cứu.

Phần 2: Công nghệ kỹ thuật chung của tường lửa ở lớp Network, Transport và Application.

Phần 3: Xây dựng VPN giữa hai cơ sở của Đại Học Hoa Sen.

Phần 4: Xây dựng IDS/IPS.

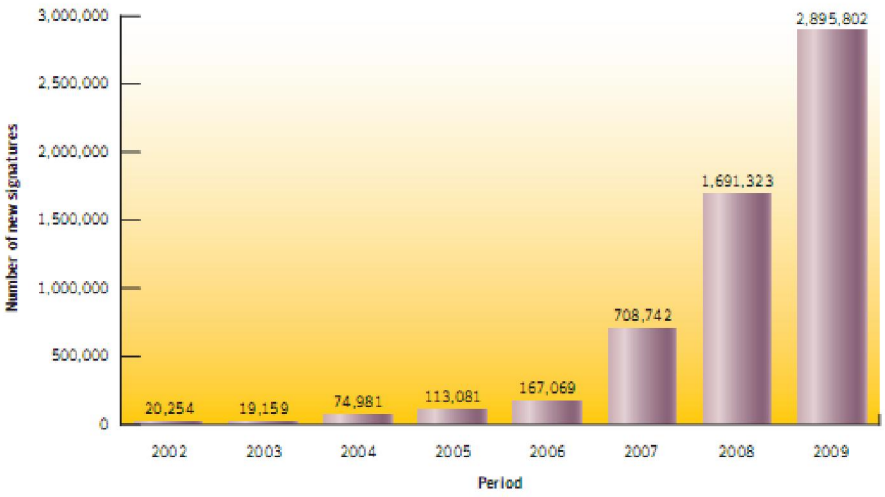
Phần 5: Xây dựng tường lửa cho hệ thống mạng trường Đại Học Hoa Sen.

PHẦN 2: CÔNG NGHỆ KỸ THUẬT CHUNG CỦA TƯỜNG LỬA TẠI LỚP NETWORK, TRANSPORT VÀ APPLICATION

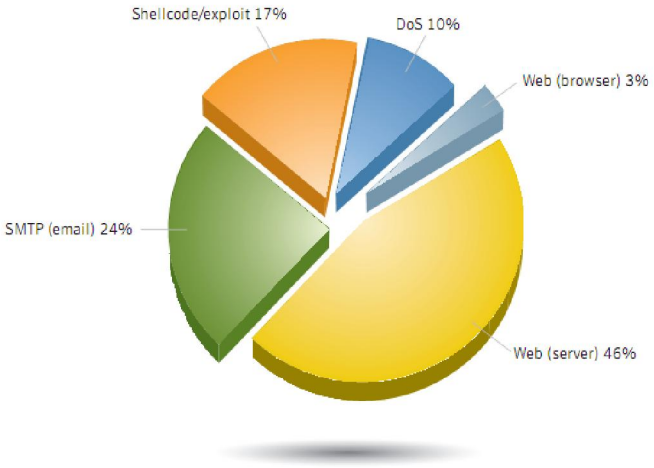
2.1 Tầm quan trọng của việc bảo mật và an toàn thông tin

Thông tin đóng vai trò vô cùng quan trọng đối với hầu hết tổ chức doanh nghiệp, nhất là trong môi trường kinh doanh cạnh tranh hiện nay. Sự tiến bộ vượt bậc của khoa học kỹ thuật dẫn đến các thủ đoạn tấn công ngày càng tinh vi.

Tập đoàn Symantec ngày 10/03/2010 đã chính thức công bố kết quả "Nghiên cứu toàn cầu về Hiện trạng bảo mật doanh nghiệp năm 2010", thông qua khảo sát 2.100 giám đốc thông tin, giám đốc bảo mật thông tin và các nhà quản trị CNTT từ 27 nước khác nhau trên thế giới vào tháng 1/2010. Nghiên cứu cho biết các doanh nghiệp ngày càng phải chịu những cuộc tấn công thường xuyên hơn. Trong vòng 12 tháng trở lại đây, 75% tổ chức được khảo sát đã bị tấn công mạng ít nhất một lần và mức độ tổn thất trung bình là 2 triệu USD mỗi năm.



Hình 1 – Biểu đồ thể hiện sự gia tăng mã độc hại



Hình 2 – Biểu đồ thể hiện các loại tấn công nhiều nhất hiện nay

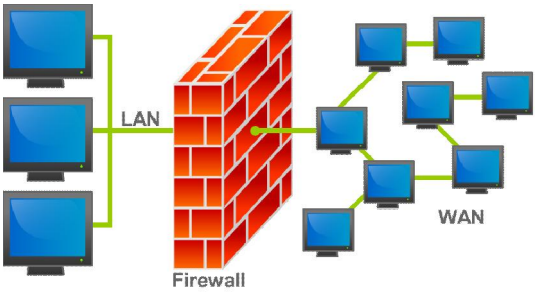
Do đó, việc bảo mật thông tin ngày càng trở nên khó khăn, bởi lẽ thông tin luôn chịu sự đe dọa từ rất nhiều nguồn khác nhau - bên trong tổ chức, bên ngoài, các thảm họa hay các mã độc hại trên mạng. Cùng với việc gia tăng sử dụng các công nghệ mới cho lưu trữ, truyền dẫn và thu thập thông tin, là sự gia tăng tương ứng về số lượng và chủng loại các mối đe dọa.

An toàn bảo mật thông tin không chỉ là công nghệ mà còn tác động trực tiếp danh tiếng, quá trình hoạt động cũng như sự tồn tại của tổ chức. Chúng tôi dễ dàng thống nhất rằng việc xây dựng hệ thống bảo mật thông tin là quá trình, đòi hỏi đầu tư nhiều thời gian và tiền bạc.

2.2 Tổng quan về tường lửa

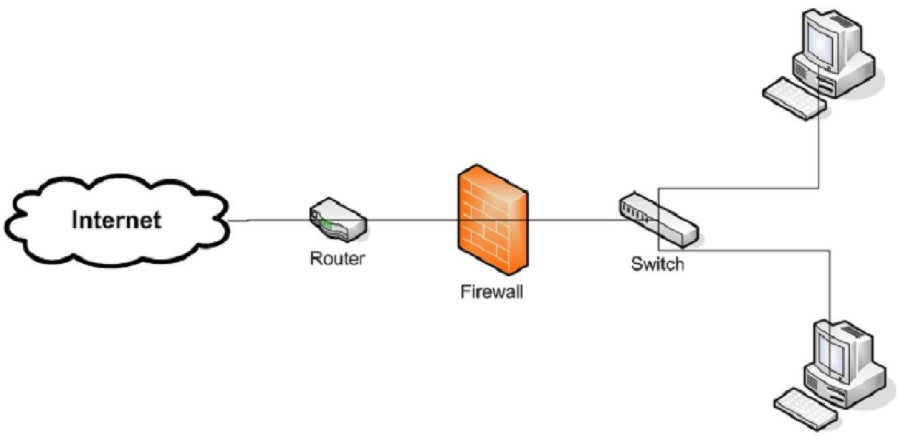
2.2.1 Giới thiệu

Tường lửa là thiết bị được sử dụng nhằm hạn chế sự tấn công, bảo vệ các nguồn thông tin quan trọng bởi các chính sách an ninh do cá nhân, doanh nghiệp hay các tổ chức chính phủ đặt ra.

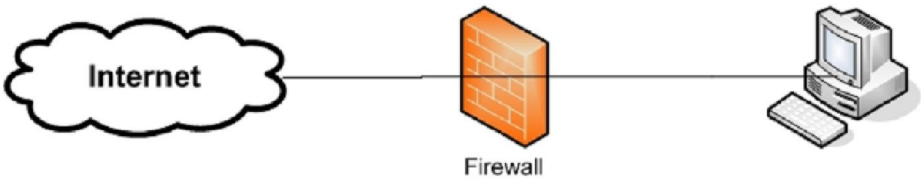


Hình 3 – Hệ thống tường lửa

Đặt sau Router biên, giữa hai vùng mạng bảo đảm việc lọc lưu lượng ra vào hệ thống mạng nhằm khóa luồng dữ liệu độc hại đi vào trong khi vẫn cho phép dữ liệu cần thiết đi qua. Tường lửa đóng vai trò vô cùng quan trọng và cần thiết đối với hầu hết tổ chức doanh nghiệp ngày nay, nhất là khi các cuộc xâm nhập phá hoại hệ thống mạng ngày càng tăng. Dù sử dụng bất kì kiến trúc nào từ tường lửa cá nhân (Personal Firewall) chuyên bảo vệ máy tính cá nhân đến dãy tường lửa trong hệ thống mạng các công ty lớn hay tổ chức chính phủ (Network Firewall) thì mục tiêu cuối cùng là xây dựng hệ thống mạng bền vững, chống lại sự xâm nhập trái phép đồng thời bảo đảm an toàn dữ liệu.



Hình 4 – Tường lửa trong hệ thống mạng (Network Firewall)



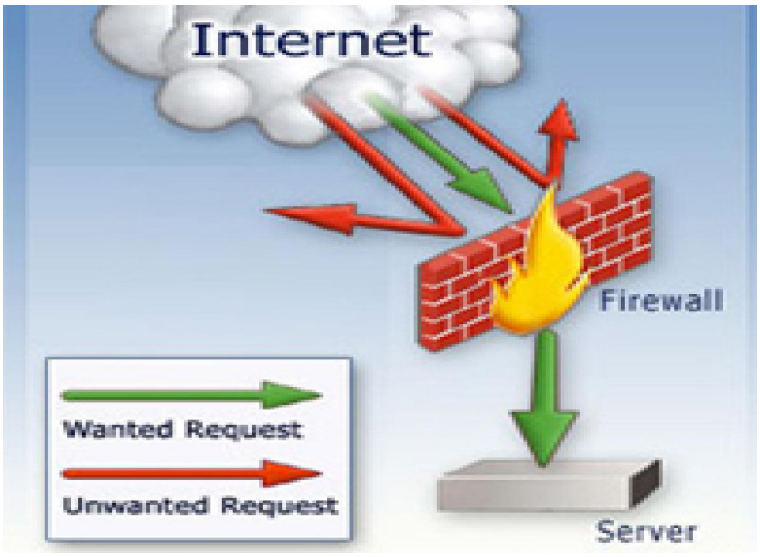
Hình 5 – Tường lửa cá nhân (Personal Firewall hay Desktop Firewall)

2.2.2 Chức năng

Kiểm soát và thiết lập cơ chế điều khiển luồng dữ liệu giữa mạng cục bộ và Internet, cụ thể:

- Cho phép hoặc cấm những dịch vụ truy cập ra ngoài hay từ ngoài truy cập vào.
- Theo dõi các luồng dữ liệu di chuyển qua tường lửa.
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- Xác nhận người dùng hợp lệ và các quyền được cấp cho người đó.
- Kiểm soát nội dung thông tin lưu chuyển trên mạng.

Tường lửa khảo sát tất cả các luồng lưu lượng ra vào hệ thống mạng xem có phù hợp với chính sách đặt ra hay không.



Hình 6 – Chức năng của tường lửa

Nếu phù hợp, luồng dữ liệu đó được định tuyến giữa các mạng, ngược lại bị hủy. Ngoài ra, tường lửa còn quản lý việc truy cập từ bên ngoài vào nguồn tài nguyên mạng bên trong, ghi lại tất cả cố gắng xâm nhập mạng riêng và đưa ra cảnh báo nhanh chóng khi phát hiện tấn

công. Tường lửa còn lọc các gói dữ liệu dựa vào địa chỉ nguồn, địa chỉ đích và số cổng. Hơn nữa, ở mức độ cao hơn, tường lửa còn lọc cả nội dung thông tin luân chuyển trên hệ thống.

2.3 Công nghệ kỹ thuật chung của tường lửa tại các lớp

Để chống lại các phương thức tấn công ngày càng tinh vi, con người không ngừng nghiên cứu sáng tạo các công nghệ mới nhằm tăng độ bảo mật tường lửa. Hiện nay, dù tường lửa cứng hay mềm, đều được sản xuất dựa trên các công nghệ sau:

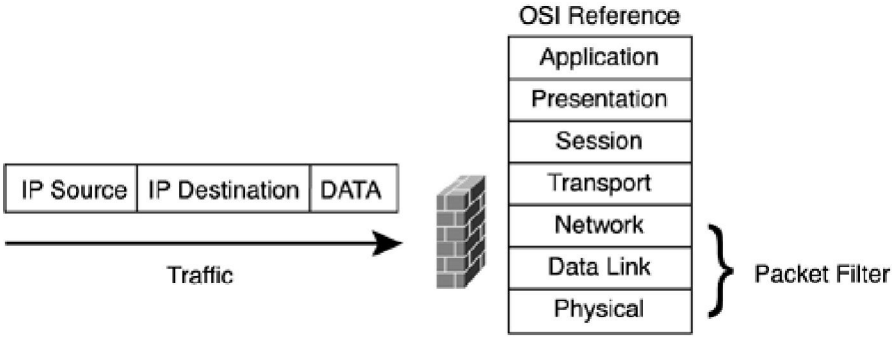
- Packet filtering
- NAT Firewall
- Stateful packet filtering
- Proxy firewalls (hay Application Layer Gateways)
- Stateful Inspection Firewall (SIF)

Nhìn chung, các công nghệ này xây dựng trên mô hình OSI (Open Systems Interconnection Reference Model), bởi hầu hết giao thức mạng đều hoạt động dựa trên mô hình này. Do đó, để kiểm soát chặt chẽ các lưu lượng ra vào, tường lửa cũng ứng dụng công nghệ khác nhau ở các lớp khác nhau, chủ yếu tại ba lớp chính sau:

2.3.1 Lớp Network và Transport

2.3.1.1 Kỹ Thuật Lọc Gói Tin (Packet Filtering)

Lúc bắt đầu, tường lửa chỉ xác định nguồn gốc và đích gói tin ở lớp Network, số cổng hay kiểu giao thức TCP/UDP ở lớp Transport mà không xác định trạng thái hay nội dung gói tin. Việc kiểm soát truy cập mạng thực hiện bằng danh sách điều khiển truy cập (Access Control List – ACL) để lọc một cách cơ bản chống xâm nhập trái phép. Từ đó, giới hạn lưu lượng độc hại đi vào, gọi là "Kỹ thuật lọc gói tin" (Packet Filtering) - một trong các kỹ thuật đơn giản nhất sử dụng phổ biến trên tường lửa mềm và cứng, cung cấp chức năng không thể thiếu cho hầu hết tường lửa. Vì trước khi kiểm tra nội dung hay trạng thái gói tin, cần bảo đảm gói tin này truyền tải trên kết nối tin cậy.

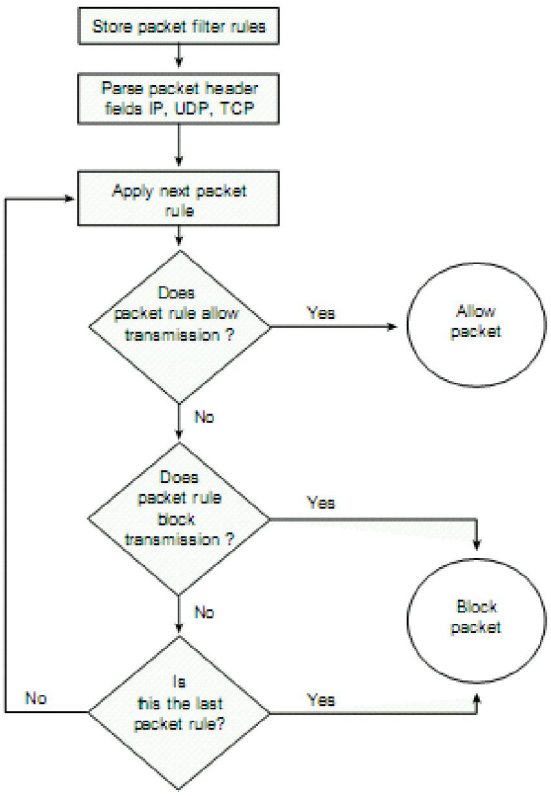


Hình 7 – Cơ chế hoạt động của Packet Filtering

Với kỹ thuật này, tường lửa cho phép (Permit) hay từ chối (Deny) truy cập dựa trên kiểu của gói tin và các trường khác định nghĩa bởi danh sách truy cập (ACL – Access Control List) để quyết định xem đoạn dữ liệu đó có thoả mãn các điều kiện lọc hay không, dựa trên các thông tin ở đầu mỗi gói tin (Packet Header) và các trường:

- Địa chỉ IP nguồn (IP Source Address)
- Địa chỉ IP đích (IP Destination Address)
- Những thủ tục truyền tin (TCP, UDP, ICMP, IP Tunnel)
- Cổng TCP/UDP nguồn (TCP/UDP Source Port)
- Cổng TCP/UDP đích (TCP/UDP Destination Port)
- Dạng thông báo ICMP (ICMP Message Type)
- Cổng giao tiếp gói tin đến (Incoming Interface of Packet)
- Cổng giao tiếp gói tin đi (Outgoing Interface of Packet)

Khi nhận được gói tin, tường lửa lần lượt so sánh với chính sách đề ra nhằm kiểm tra tính hợp lệ của gói tin. Nếu hợp lệ, gói tin chuyển qua tường lửa, ngược lại, bị bỏ đi. Nhờ vậy, tường lửa ngăn cản kết nối vào máy chủ hay vùng tin cậy, khoá truy cập hệ thống mạng nội bộ từ các địa chỉ không cho phép. Ngoài ra, tường lửa so sánh header hiên tại và header gói tin trước đó, giúp phân tích nhiều thông tin hơn cũng như xem xét cổng giao tiếp gói tin ra vào.



Hình 8 - Cách kiểm tra gói tin của Packet Filtering

Ưu điểm

- Tốc độ xử lý nhanh nên sử dụng phổ biến bởi hầu hết tường lửa hiện nay.
- Dễ triển khai, cài đặt và bảo trì, chi phí triển khai thấp vì cơ chế lọc gói tin được tích hợp sẵn trên các Router.
- Ứng dụng độc lập, ít tác động đến hiệu năng mạng.
- Trong suốt đối với người sử dụng và các ứng dụng.
- Không yêu cầu người quản trị phải có kiến thức cao.

Nhược điểm: Một số vấn đề với Packet Filtering:

- Tất cả gói tin đều có thể vượt qua tường lửa nếu phù hợp các chính sách đề ra. Kẻ tấn công có thể lợi dụng điểm này bằng cách chia nhỏ dữ liệu lồng vào gói tin hợp lệ.
- Mỗi chính sách thể hiện bằng ACL (Access Control List), do đó để xây dựng hệ thống hoàn chỉnh đòi hỏi việc cấu hình nhiều chính sách. Tuy nhiên, vấn đề tổng hợp, thống nhất và tối ưu các chính sách mới là mối quan tâm hàng đầu hầu hết doanh nghiệp.
- Việc triển khai kỹ thuật này cho các dịch vụ có số cổng không xác định là không khả thi, đòi hỏi ứng dụng các kỹ thuật kiểm tra các lớp cao hơn (từ lớp Transport trở lên).
- Không hỗ trợ tính năng xác thực người dùng.
- Không ngăn chặn tấn công giả mạo địa chỉ.
- Mức an ninh thấp. Do các tiêu chuẩn lọc dựa trên các trường ở đầu mỗi gói tin (Packet Header) nên không kiểm soát được nội dung thông tin và trạng thái gói tin.

2.3.1.2 Tường lửa NAT (NAT Firewall)

Hoạt động ở lớp Network và Transport. NAT (Network Address Translation) thay đổi địa chỉ IP gói tin nếu cần thiết vì thế NAT cho phép người dùng bên trong sử dụng địa chỉ công cộng truy cập Internet mà ẩn đi địa chỉ thật sự bên trong. Ngoài ra, NAT quản lý việc truy cập Internet bằng cách quyết định người dùng nào được phép sử dụng. Cụ thể hơn, khi người dùng khởi tạo kết nối ra ngoài, NAT thay đổi IP nguồn gói tin và gửi đi, đồng thời ghi lại trạng thái trong bảng chuyển đổi (Translation Table). Khi gói tin từ ngoài về, NAT tra bảng và thay đổi IP đến của gói tin thành IP ban đầu để gói tin trở về đúng nơi xuất phát. Ngoài ra, kỹ thuật thay đổi cổng nguồn và đích gói tin gọi là PAT (Port and Address Translation).

Như đề cập, NAT sử dụng bảng chuyển đổi (Translation Table) lưu giữ trạng thái kết nối chuyển đổi, vì thế người dùng bên ngoài không thể chủ động khởi tạo kết nối vào bên trong.

Ưu điểm

- Bảo vệ mạng bên trong khỏi sự "dòm ngó" từ bên ngoài.
- Xác định cụ thể dịch vụ nào dùng NAT, như đối với các máy trong hệ thống.
- Chỉ với một địa chỉ IP công cộng các máy tính nội bộ đều truy cập được Internet.

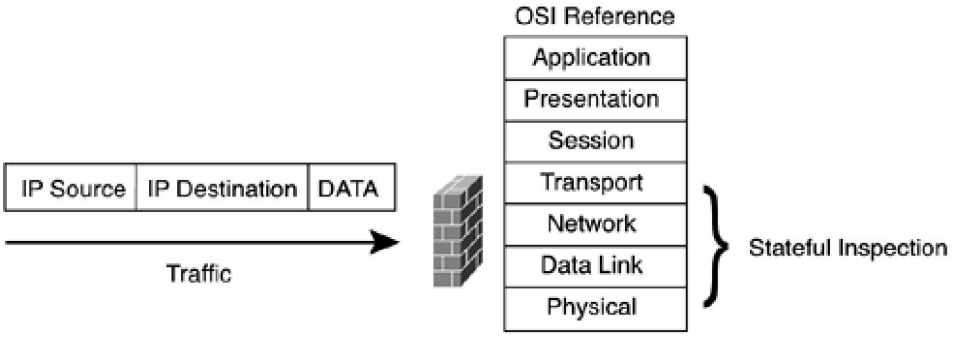
Nhược điểm

- Với TCP, việc xác định khi nào ngừng chuyển đổi địa chỉ IP hết sức dễ dàng vì TCP là giao thức bắt tay ba bước. Tuy nhiên với UDP, lại là vấn đề vì UDP không thiết lập kết nối. Do đó NAT phải đoán khi nào kết nối kết thúc, nếu sai dẫn đến mất kết nối.

2.3.1.3 Kỹ Thuật Lọc Gói Tin Ghi Nhớ Trạng Thái (Stateful Packet Filtering)

Hoạt động ở lớp Network, Trasport và Session, theo dõi và ghi nhận trạng thái kết nối (lưu lượng TCP/UDP) ra vào hệ thống nhằm phân biệt gói tin hợp lệ cho những kết nối khác nhau. Cách thức kiểm tra như Packet Filtering, tuy nhiên kỹ thuật này cho phép duy trì trạng thái kết nối. Mỗi khi kết nối TCP/UDP khởi tạo từ mạng bên trong hay bên ngoài, thông tin trạng thái kết nối được lưu lại trong bảng trạng thái (Stateful Session Flow Table). Với mỗi phiên làm việc được khởi tạo, các thông số phiên này phải chính xác so với các thông tin trong bảng trạng thái thì phiên này mới được thiết lập. Với cách hoạt động như thế, kỹ thuật này chủ yếu hoạt động trên kết nối chứ không chỉ làm việc trên từng gói tin riêng lẻ.

Bảng trạng thái chứa địa chỉ IP nguồn, IP đích, số cổng, các cờ trạng thái ứng với mỗi kết nối và số thứ tự (sequence number) ngẫu nhiên trước khi gói tin chuyển đi và hoàn tất kết nối. Do đó, tất cả gói tin từ trong ra (Outbound) hay từ ngoài vào (Inbound) được so sánh đối chiếu cẩn thận trước khi chuyển tiếp, đảm bảo kết nối thực hiện từ một hướng từ trong ra ngoài (Inside to Outside), chứ không theo hướng ngược lại nhằm ngăn chặn gói tin độc hại đi vào hệ thống cũng như ngăn cản máy tính bên ngoài gửi dữ liệu vào các máy bên trong.



Hình 9 – Cơ chế hoạt động của Stateful Packet Filtering

Đây là phương thức tân tiến hơn so với thế hệ trước với ba lý do sau:

- Kiểm soát cả kết nối và gói tin, hiệu suất hoạt động cao hơn.
- Lưu giữ trạng thái kết nối TCP/UDP trong bảng trạng thái, dùng tham khảo, xác định xem gói tin này thuộc về kết nối đã được thiết lập từ trước hay do truy cập trái phép.
- Khả năng phân tích cổng hoạt động giao thức FTP, từ đó cập nhật bảng trạng thái giúp lưu lượng FTP có thể đi qua tường lửa. Hơn nữa, nó còn tạo ra số thứ tự (sequence number) động cho gói tin TCP và truy vấn DNS. Những tính năng này giảm nguy hiểm tấn công TCP RST flood và DNS cache poisoning.

Ưu điểm

- Phương thức bảo vệ chính trong môi trường hẹp, lọc lưu lượng vào ra hệ thống mạng.
- Bảo vệ vòng ngoài, nơi Router giao tiếp vùng mạng không tin tưởng.
- Phương tiện tăng cường khả năng lọc gói tin.
- Phương thức tối ưu chống tấn công giả mạo (Spoofing) và từ chối dịch vụ (Denial of Service – DoS) vì trạng thái tất cả kết nối đều được ghi nhận lại vào bảng trạng thái, chỉ những gói tin phù hợp mới được phép đi qua, ngược lại thì bị bỏ đi.

Nhược điểm: Stateful Packet Filtering **không thể:**

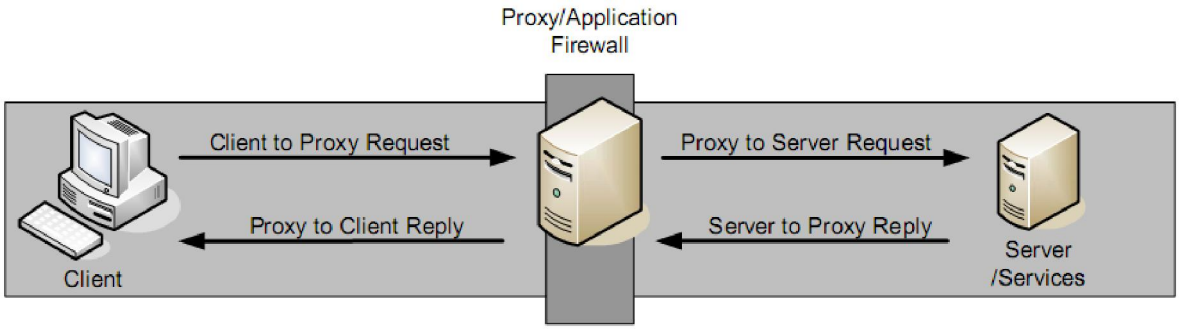
- Chặn các cuộc tấn công ở lớp Application do không thể phân tích nội dung dữ liệu.
- Hỗ trợ xác thực người dùng.

2.3.2 Lớp Application

2.3.2.1 Proxy Firewall

Khi công nghệ càng phát triển, nhu cầu quản lý truy cập mạng càng được chú trọng. Tấn công vào các hạn chế của kỹ thuật lọc gói tin, người dùng dễ dàng tránh các biện pháp canh phòng bảo mật của tường lửa mà xâm nhập hệ thống trái phép. Do đó, để gia tăng mức độ bảo mật của tường lửa, kỹ thuật Proxy Firewall – thế hệ tường lửa thứ hai - hoạt động ở lớp Network, Transport, Session và Application, thay mặt mạng bên trong (Inside Network) giao tiếp bên ngoài (Outside Network), nhờ đó, che dấu mọi dữ liệu quan trọng.

Khi tường lửa nhận được yêu cầu từ phía người dùng, nó tiến hành xác thực thông qua các quy định được cấu hình. Nếu tài khoản người dùng hợp lệ, tường lửa thay mặt người dùng bên trong giao tiếp với các máy ngoài Internet. Proxy Firewall chỉ chuyển tiếp gói tin có lớp Network và Transport phù hợp và trả về gói tin có lớp Session và Application thích hợp.

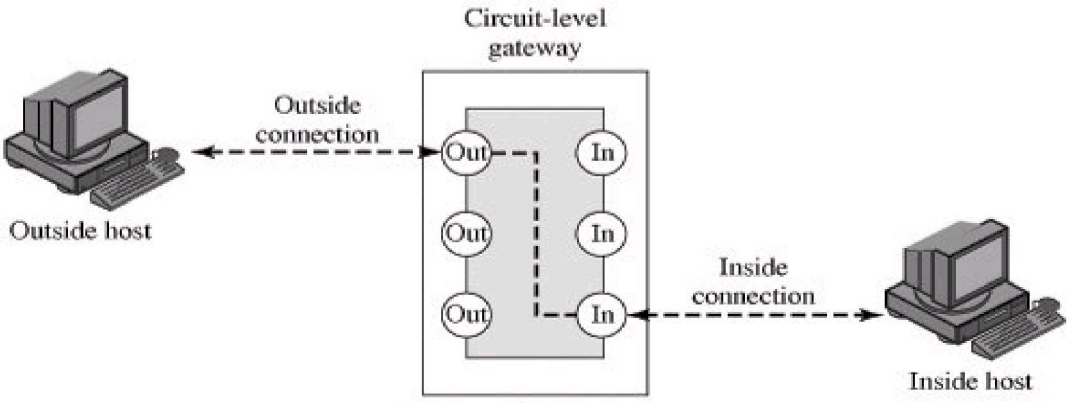


Hình 10 – Cơ chế hoạt động của Proxy Firewall

Proxy Firewall ngăn cản trao đổi gói tin trực tiếp giữa hai thiết bị. Mọi giao tiếp giữa các thiết bị đều phải thông qua Proxy, giúp kiểm tra gói tin nhanh và sâu hơn so với kỹ thuật truyền thống, gồm hai dạng:

- ***Circuit Level Gateway***

Hoạt động tương đối phức tạp hơn Packet Filtering, ngoài khả năng lọc các lưu lượng mạng bởi địa chỉ IP và số cổng, nó còn kiểm tra quá trình bắt tay của giao thức TCP ở lớp Session.



Hình 11 – Circuit Level Gateway

Quá trình hoạt động

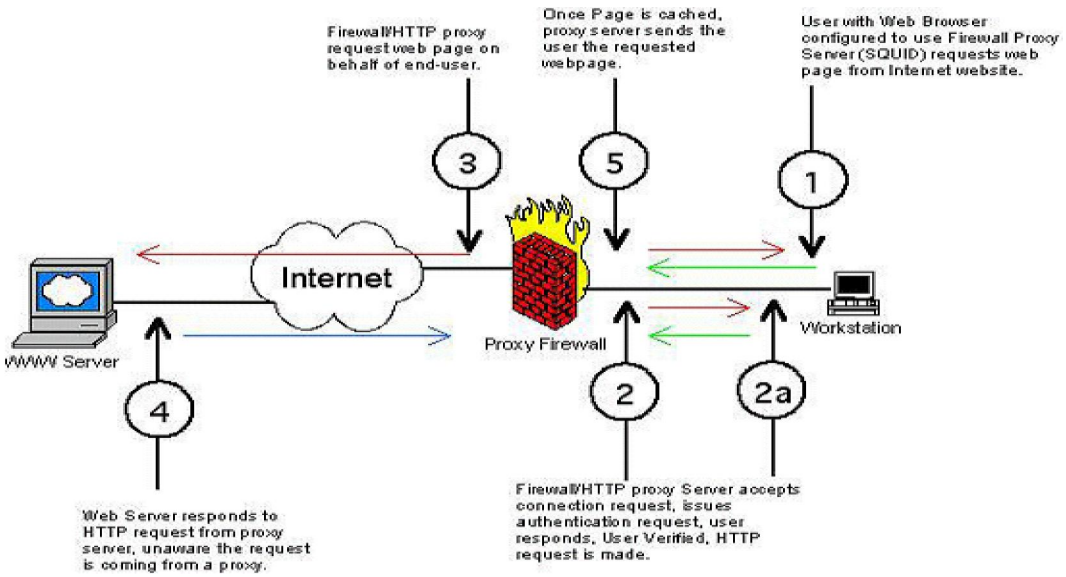
- **Bước 1:** Máy tính nguồn bắt đầu kết nối, sau đó, tường lửa kiểm tra thông tin kết nối dựa trên luật lệ đề ra, nếu kết nối được cho phép, tường lửa cho phép kết nối đi qua.
- **Bước 2:** Thay mặt máy bên trong, tường lửa kết nối đến máy bên ngoài và giám sát chặt chẽ quá trình bắt tay TCP. Quá trình bắt tay liên quan đến việc trao đổi gói tin chứa cờ (SYN hay ACK).
- **Bước 3:** Tường lửa xác thực máy bên trong và máy bên ngoài là thành phần một phiên làm việc. Sau đó, tường lửa sao chép và chuyển tiếp dữ liệu giữa hai kết nối.

Tuy nhiên, máy đích sẽ nhận thấy kết nối này đến từ hệ thống tường lửa, che dấu tất cả thông tin bên trong. Không có bất kì dữ liệu nào được chuyển qua cho đến khi tường lửa xác nhận tính hợp lệ kết nối này. Tường lửa xác định một phiên làm việc hợp lệ nếu cờ SYN, ACK và Sequence Number trong quá trình bắt tay giữa các kết nối là hợp lệ.

- ***Application Level Gateway (ALG)***

Như tên gọi, Proxy Firewall ở lớp ứng dụng (Application Level Proxy Firewall) chủ yếu hoạt động ở lớp Application, dùng để kiểm tra các ứng dụng hay các dịch vụ được chỉ định như HTTP, FTP, DNS, telnet,... Ngoài ra, ALG còn phát hiện những giao thức không mong muốn trên các cổng không nằm trong số cổng tiêu chuẩn (Non-standard Port).

Dựa trên dịch vụ đại diện (Proxy service - chương trình đặc biệt cài trên gateway từng ứng dụng). Quy trình kết nối sử dụng dịch vụ thông qua tường lửa diễn ra theo 5 bước sau đây:



Hình 12 – Quy trình hoạt động của kỹ thuật Application Level Gateway

Bước 1: Máy trạm gửi yêu cầu tới máy chủ ở xa qua tường lửa.

Bước 2: Tường lửa xác thực người dùng. Nếu xác thực thành công chuyển sang bước 3, ngược lại quá trình kết thúc.

Bước 3: Tường lửa chuyển yêu cầu máy trạm đến máy chủ ở xa.

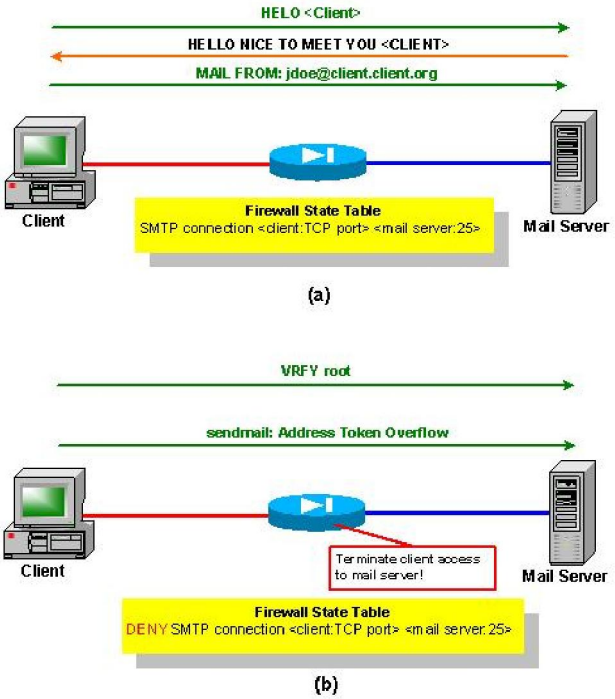
Bước 4: Máy chủ ở xa trả lời chuyển đến tường lửa.

Bước 5: Tường lửa chuyển trả lời của máy chủ ở xa đến máy trạm.

Để nhận biết ứng dụng cần kiểm tra, ALG lưu giữ trạng thái dịch vụ chỉ định từ trước. Khi người dùng kết nối trực tiếp đến Application-Level Proxy yêu cầu các dịch vụ cần thiết như

web (HTTP/HTTPS), mail (SMTP)… proxy lần lượt thay mặt người dùng kết nối các server bên trong. Vì proxy phải lưu thông tin tất cả dịch vụ trong hệ thống nên gây hạn chế trong việc bảo vệ an toàn tất cả ứng dụng.

Cung cấp sự bảo mật và tin cậy hơn so với Packet Filtering bởi vì nó có thể quản lý, giám sát, kiểm tra, đưa ra các chính sách quy định nội dung sâu bên trong luồng dữ liệu đi qua dựa trên kỹ thuật DPI (Deep Packet Inspection). Do đó, việc triển khai ALG trên hệ thống mạng cần xem xét cẩn thận bởi ít nhiều ảnh hưởng hiệu năng hoạt động của mạng. Vì vậy, cần lưu ý là chỉ triển khai proxy khi đặt nặng vấn đề bảo mật an toàn thông tin hơn là hiệu năng mạng.



Hình 13 – Deep Packet Inspection

Nhờ áp dụng DPI, tường lửa có thể kiểm tra các gói tin đi qua. Ở hình 10a, người dùng gửi gói tin HELO cho Mail Server để thiết lập kết nối SMTP. Sau khi kiểm tra tính hợp lệ gói tin, tường lửa thay người dùng truy cập Mail server bên trong và trả lời lại cho người dùng. Khi nhận trả lời từ tường lửa, người dùng tiếp tục gửi các câu lệnh khác.

Ngược lại, ở hình 10b, người dùng đánh lệnh VRFY – lấy thông tin tài khoản trên server. Tường lửa kiểm tra gói tin và nhận thấy không thỏa chính sách nên lập tức từ chối kết nối.

Ưu điểm

- Điều khiển từng dịch vụ trên mạng (quyết định máy chủ nào truy cập dịch vụ nào).
- Xác thực người dùng chứ không phải thiết bị, tường lửa chỉ chuyển tiếp dữ liệu sau khi chứng thực và ủy quyền thành công.

- Khó tấn công giả mạo (Spoofing) và từ chối dịch vụ (Denial of Service – DoS).
- Cho phép giám sát và lọc dữ liệu. Bất cứ yêu cầu nào của người dùng đều được ghi nhận rõ ràng, dễ dàng thống kê ghi nhận nội dung truy cập của bất kì người dùng nào ở mọi thời điểm. Ngoài ra, proxy còn cho phép ủy quyền ai được làm gì, không được làm gì thông qua khả năng xác thực (Authentication) và ủy quyền (Authorization).
- Theo dõi và giám sát chi tiết mỗi luồng thông tin đi qua, thậm chí xác định được kiểu tấn công cũng như mục tiêu bị tấn công. Hơn nữa, còn giám sát thông tin truy cập người dùng như tài nguyên được truy xuất, băng thông sử dụng và thời điểm truy cập.
- Cứ mỗi yêu cầu đến proxy lưu lại thông tin trong bộ nhớ đệm, khi có yêu cầu khác truy cập thông tin này proxy sẽ truy xuất trực tiếp từ bộ nhớ đệm cung cấp cho người dùng, không cần gửi yêu cầu ra bên ngoài, giúp tăng hiệu năng của mạng.
- Thay mặt người dùng truy vấn bên ngoài, che dấu IP và các thông tin nhạy cảm khác.

Nhược điểm

- Tốc độ chậm, hiệu suất thấp do xử lý trên nhiều tầng.
- Khả năng thay đổi mở rộng (scalability) hạn chế.
- Nếu proxy bị tấn công thì mạng bên trong cũng bị ảnh hưởng.
- Các dịch vụ hỗ trợ bị hạn chế, chỉ hỗ trợ việc kiểm soát một số dịch vụ quen thuộc như web (HTTP/HTTPS), FTP… gây khó khăn trong cấu hình thêm dịch vụ khác.
- Kiểm tra tận sâu bên trong gói tin nên ít nhiều làm giảm hiệu năng mạng.
- Cài đặt và bảo trì phức tạp do xử lý gói tin bằng chương trình ứng dụng.
- Hỗ trợ số lượng nhỏ người dùng.

2.3.2.2 Stateful Inspection Firewall (SIF)

Chủ yếu sử dụng kỹ thuật SPI (Stateful Packet Inspection) – thế hệ cải tiến của kỹ thuật lọc gói tin (Packet Filtering), được phát triển bởi Checkpoint vào năm 1993. SPI kết hợp sức mạnh của các kỹ thuật trước đó:

Packet Filtering: hoạt động ở tầng mạng, lọc gói tin đi và đến dựa trên các tham số kết nối như địa chỉ nguồn, địa chỉ đích, cổng nguồn, cổng đích…

Circuit Level Gateway: xác định gói tin trong phiên làm việc hợp lệ dựa trên cờ ACK, SYN và Sequence Number.

Application Level Gateway: SIF đưa gói tin lên tầng ứng dụng và kiểm tra nội dung dữ liệu phù hợp với các chính sách an ninh hệ thống. SFI có thể cấu hình loại bỏ gói tin chứa những

câu lệnh xác định (như FTP PUT, FTP GET...). Ngoài ra, cải thiện tính năng của kỹ thuật Application Level Gateway, SFI cho phép người dùng kết nối trực tiếp với server.

2.4 Triển khai tường lửa trong hệ thống mạng doanh nghiệp

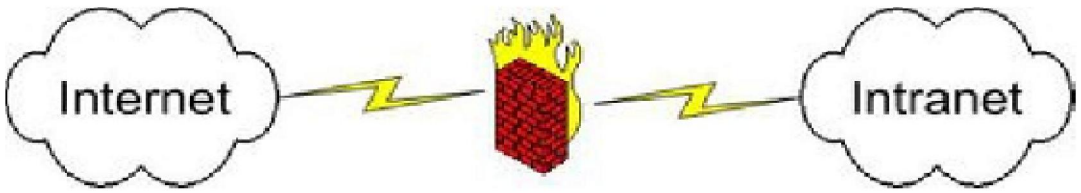
Tùy mục đích, sơ đồ kiến trúc hệ thống mạng mà nhà quản trị lựa chọn mô hình phù hợp, tùy kiến thức, kinh nghiệm người quản trị. Nhìn chung, các mô hình kiến trúc tường lửa vô cùng đa dạng nhưng khái quát lại thì bao gồm ba dạng sau:

2.4.1 Bastion Host

Bation Host, thuật ngữ chung chỉ một hệ thống được xác định bởi người quản trị tường lửa như là một điểm an ninh cực kỳ vững chắc trong hệ thống mạng

Đây là mẫu kiến trúc tường lửa đơn giản nhất, tường lửa đặt giữa mạng nội bộ (Inside Network) và mạng bên ngoài (Outside Network) để lọc các gói tin vào ra thông qua hai cổng giao tiếp: cổng kết nối trực tiếp Internet (Untrusted) và cổng kết nối với Intranet (Trusted), tồn tại hai vùng với độ bảo mật (security level) khác nhau.

Chủ yếu dùng công nghệ cổng ứng dụng (**Application Level Gateway)**, cổng vòng (**Circuit Level Gateway)** hay kết hợp cả hai. Dual – homed host là ví dụ điển hình về Bation Host.



Hình 14 - Bastion Host

Mô hình Bastion Host thích hợp cho hệ thống mạng đơn giản, không có nhu cầu quảng bá các dịch vụ ra Internet, vì như vậy nếu server bị kiểm soát, toàn bộ hệ thống bên trong cũng bị ảnh hưởng. Hơn nữa, mô hình này tạo ranh giới mỏng manh giữa mạng tin cậy và không tin cậy. Nếu ranh giới này phá vỡ, toàn bộ hệ thống mạng, nguồn tài nguyên bên trong bị khai thác.

Ưu điểm

- Chi phí triển khai thấp.
- Dễ quản lý, cấu hình.

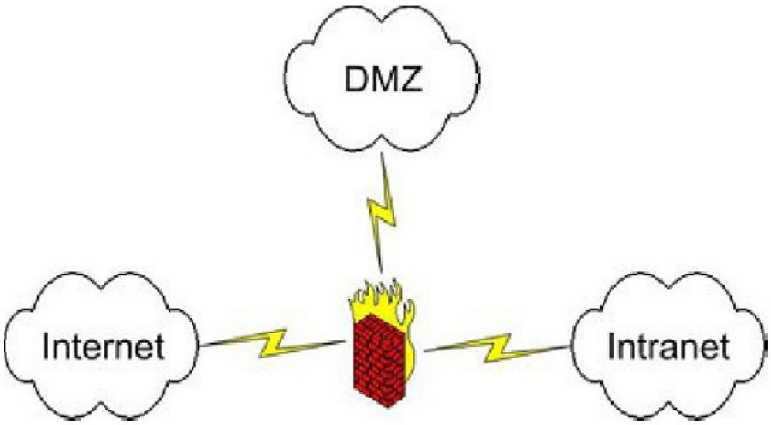
Nhược điểm

- Độ bảo mật thấp, nếu tường lửa bị tấn công, toàn bộ tài nguyện hệ thống mạng bên trong sẽ bị khai thác.

2.4.2 Screened subnet (hay triple homed host firewall)

Mô hình tường lửa cơ bản, so với Bastion Host, hỗ trợ thêm nhu cầu quảng bá dịch vụ ra Internet, nhờ việc định nghĩa vùng phi quân sự (Demilitarized Zone – DMZ) - mạng con biệt lập giữa Internet và mạng nội bộ. Mô hình này thích hợp với công ty vừa và nhỏ, vừa đáp ứng nhu cầu bảo mật hệ thống bên trong vừa cho phép người dùng bên ngoài truy cập các dịch vụ cần thiết và nhất là phù hợp túi tiền nên đây là mô hình được triển khai nhiều nhất.

Giống với Bastion Host, screened subnet chỉ sử dụng một tường lửa duy nhất, với ba card mạng nhằm phân biệt rõ ràng Outside, Inside và DMZ. Như đã nói, mô hình này cung cấp giải pháp cho phép người dùng bên ngoài truy cập các dịch vụ được quảng bá trong vùng DMZ. Độ bảo mật cao hơn so với Bastion Host, khả năng mạng bên trong bị tấn công tương đối thấp vì từ bên ngoài người dùng chỉ có thể truy cập các dịch vụ trong DMZ, mà không thể khởi tạo kết nối vào bên trong.



Hình 15 - Screened subnet

Ưu điểm

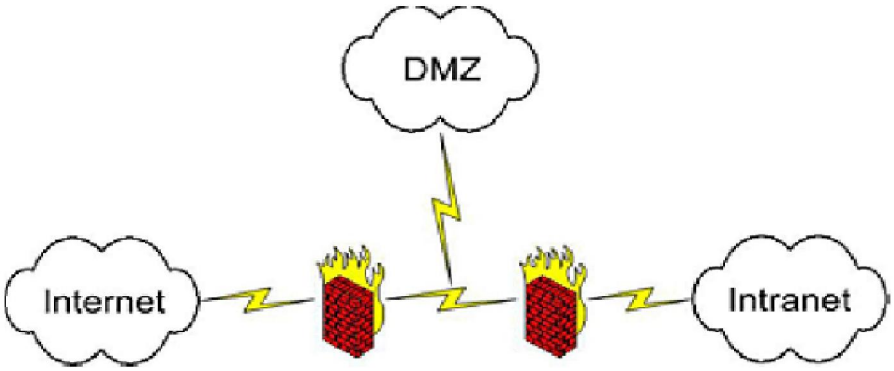
- Nếu vùng DMZ bị tấn công, hệ thống mạng bên trong cũng không bị ảnh hưởng.
- Độ bảo mật tương đối cao so với Bastion Host vì người dùng bên ngoài chỉ truy cập được các dịch vụ quảng bá trong DMZ mà không thể kết nối trực tiếp mạng nội bộ.

Nhược điểm

- Như mô hình Bastion host, nếu lớp bảo vệ duy nhất này bị phá vỡ thì toàn bộ hệ thống mạng bên trong sẽ gặp nguy hiểm.

2.4.3 Dual firewall

Hệ thống bao gồm hai tường lửa, đạt an toàn cao nhất so với hai mô hình trên. Tuy chi phí triển khai cao đồng thời đòi hỏi nhiều sự quan tâm của quản trị viên dành cho hệ thống, việc cấu hình cũng tương đối phức tạp nhưng hệ thống đạt độ tin cậy cao, khó đánh sập.



Hình 16 - Dual Firewall

Cũng giống với mô hình 03 chân, DMZ được tách biệt vào một vùng riêng nên cho dù có bị khai thác thì cũng không tác động đến inside. Việc sử dụng 02 firewall sẽ rất tốn kém, nhưng nếu so sánh giữa việc đầu tư và tầm quan trọng của dữ liệu thì sẽ thấy rất đáng để triển khai. Đặt biệt, mô hình này sẽ có được sự an toàn nhất khi sử dụng mỗi firewall mỗi hảng khác nhau. Nếu firewall vòng ngoài bị xuyên thủng thì hacker cũng không thể xuyên thủng firewall vòng trong, hay ít nhất cũng làm hacker mất một khoảng thời gian để nhận định nó và vượt qua, với khoảng thời gian đó ta đã đủ để dựng lại firewall vòng ngoài và đối phó với hacker.

Ngoài ra, sử dụng nhiều firewall đồng nghĩa với việc có nhiều interface. Điều này có nghĩa là ta có thể có nhiều vùng với nhiều level khác nhau do ta lựa chọn, giúp dễ dàng quảng lý cũng như cấu hình.

Nhìn chung, các mẫu thiết kế trên đều có những ưu và nhược điểm trên. Việc lựa chọn mô hình tường lửa nào chủ yếu phụ thuộc nhu cầu của các tổ chức doanh nghiệp và ngân sách dự trù dành cho việc đầu tư bảo mật ra sao. Từ đó, lựa chọn ra các mô hình phù hợp vừa đáp ứng nhu cầu doanh nghiệp vừa phù hợp chi phí đầu tư của các tổ chức doanh nghiệp.

Ưu điểm

- Mức độ bảo mật cao hơn so với hai mô hình trước. Để xâm nhập hệ thống mạng nội bộ, kẻ tấn công phải vượt qua hai tầng bảo mật: Tường lửa bên ngoài (Outside Firewall) và tường lửa bên trong (Outside Firewall).
- Cho phép người dùng bên ngoài truy cập các dịch vu quảng bá trong vùng DMZ.
- So với screened subnet, nếu vùng DMZ bị tấn công, mạng bên trong vẫn được bảo vệ.

Nhược điểm

- Chi phí triển khai cao.
- Việc quản lý hệ thống tường lửa đòi hỏi nhà quản trị phải có kinh nghiệm cũng như kiến thức nhất định.

PHẦN 3: XÂY DỰNG VPN GIỮA HAI CƠ SỞ CỦA ĐẠI HỌC HOA SEN

3.1 Sự cần thiết của VPN trong doanh nghiệp

3.1.1 Tại sao VPN ra đời

Với sự phát triển nhanh chóng của công nghệ tin học và viễn thông, thế giới ngày càng thu nhỏ và trở nên gần gũi. Nhiều công ty đang vượt qua ranh giới cục bộ và khu vực, vươn ra thị trường thế giới. Nhiều doanh nghiệp trải rộng khắp toàn quốc thậm chí vòng quanh thế giới và tất cả đều đối mặt với một nhu cầu thiết thực: cách thức duy trì những kết nối thông tin kịp thời, an toàn và hiệu quả cho dù văn phòng đặt tại bất cứ nơi đâu.

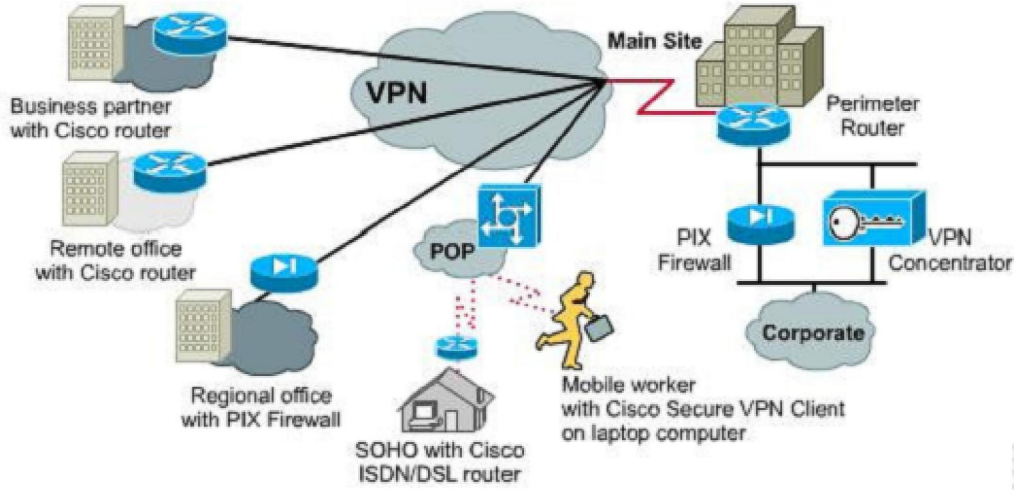
Cùng với sự lớn mạnh của Internet cả về mô hình lẫn công nghệ, đáp ứng phần nào nhu cầu người sử dụng. Internet kết nối nhiều mạng khác nhau và cho phép thông tin chuyển đến người dùng tự do và nhanh chóng mà không xem xét đến tính bảo mật thông tin. Ngày nay, thị trường ngày càng phát triển, kéo theo đó là hàng loạt các công nghệ, kỹ thuật, ứng dụng mới lần lượt ra đời. Các dịch vụ như giáo dục từ xa, mua hàng trực tuyến, tư vấn y tế… dần dần trở nên quen thuộc với hầu hết tất cả mọi người.

Tuy nhiên, chính sự rộng lớn của Internet – thế mạnh đồng thời là điểm yếu duy nhất đã gây ra không ít rủi ro và tổn thất cho doanh nghiệp. Việc quản lý cũng như bảo mật, an toàn dữ liệu trên Internet vô cùng khó khăn bởi Internet có phạm vi toàn cầu, không thuộc sự quản lý của bất kỳ tổ chức nào. Từ đó, với mục đích thoả mãn yêu cầu trên mà vẫn tận dụng cơ sở hạ tầng Internet hiện có, mô hình mạng riêng ảo (Virtual Private Network - VPN) đã ra đời.

3.1.2 VPN thật sự cần thiết đối với doanh nghiệp

Với mô hình mới này, không phải đầu tư thêm nhiều cơ sở hạ tầng mà độ tin cậy vẫn đảm bảo, đồng thời quản lý được hoạt động mạng này. VPN cung cấp cho người sử dụng kết nối bảo mật an toàn khi làm việc tại nhà, trên đường hay ở các văn phòng chi nhánh thông qua Internet. VPN 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.

Trong thị trường cạnh tranh ngày nay, việc xây dựng mạng VPN cho các nhân viên ở xa có thể truy cập dữ liệu các máy bên trong hệ thống thông qua mạng công cộng Internet ngày càng cần thiết đối với các tổ chức doanh nghiệp, giúp tăng năng suất làm việc của nhân viên ở công ty cũng như khi đi công tác. Một mạng VPN điển hình bao gồm mạng LAN chính tại trụ sở (Văn phòng chính), các mạng LAN khác tại những văn phòng từ xa, các điểm kết nối hay người sử dụng (Nhân viên di động) truy cập đến từ bên ngoài.



Hình 17 – Mạng VPN

3.2 Tổng quan VPN

3.2.1 Khái niệm

Sự mở rộng mạng riêng (private network) thông qua mạng công cộng. Về căn bản, VPN là mạng riêng lẻ sử dụng mạng chung (Internet) để kết nối cùng các site (các mạng riêng lẻ) hay nhiều người dùng từ xa. Thay vì sử dụng kết nối thực, chuyên dụng như leased line, mỗi VPN dùng kết nối ảo qua Internet từ mạng riêng của công ty tới các chi nhánh hay nhân viên ở xa.

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 (VPN Tunnel) giống như kết nối point-to-point trên mạng riêng. Để bảo đảm an tòan dữ liệu trong khi truyền dẫn, dữ liệu phải được mã hóa hay che giấu đi chỉ cung cấp thông tin đường đi đến máy đích thông qua Internet. Do đó, nếu các gói tin bị bắt lại trên đường thì kẻ tấn công cũng không thể đọc được nội dung vì không có khóa giải mã.

3.2.2 Lợi ích VPN: So với triển khai các mạng truyền thống, VPN mang lại:

- Chi phí thấp hơn.
- Đơn giản hoá mô hình kiến trúc mạng.
- Cung cấp những cơ hội kết nối toàn cầu.
- Quản lý dễ dàng: so với việc sử dụng các giao thức như Frame Relay và ATM để kết nối các site với nhau, VPN cung cấp giải pháp đơn giản và linh hoạt hơn trong việc quản lý số lượng người dùng (thêm, xoá kênh kết nối liên tục, nhanh chóng).
- Tăng cường an ninh mạng.

- Cung cấp khả năng tương thích với mạng lưới băng thông rộng.
- Hỗ trợ các giao thức mạng thông dụng nhất hiện nay như TCP/IP.
- Bảo mật địa chỉ IP: 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.

3.2.3 Cơ sở hạ tầng kỹ thuật xây dựng VPN

3.2.3.1 Kỹ thuật mật mã

a. Vai trò của kỹ thuật mật mã trong bảo vệ thông tin

Che dấu thông tin mật. Ngày nay, việc nghe trộm hay lấy cắp thông tin trên đường truyền khá phổ biến. Hàng năm, số lượng cuộc tấn công hệ thống mạng doanh ngày càng tăng. Do đó, kỹ thuật mật mã càng quan trọng và cần thiết với hầu hết tổ chức doanh nghiệp, trở thành điều kiện tiên quyết nhằm bảo mật dữ liệu khi truyền dẫn trên các kênh truyền thông công cộng.

b. Các dạng mật mã học

Ngành khoa học mật mã có hai nhánh chính là mật mã học (cryptography) và phân tích mật mã (cryptanalysis). Trong đó, mật mã học nghiên cứu thuật toán, giải pháp mật mã và chia làm hai nhánh con là encryption (mục tiêu confidentiality) và hashing (chức năng authentication, verification); phân tích mật mã nghiên cứu cách phá mật mã (crack).

Không phải mới đây, ngành khoa học mật mã đã ra đời từ lâu vào thế kỷ 18, trải qua thời gian, đi từ thấp đến cao, từ đơn giản đến phức tạp. Bắt đầu bằng việc mã hóa chỉ đơn giản bằng việc thay ký tự này bằng một ký tự, hoặc một số khác; rồi hoán đổi vị trí các ký tự cho nhau, hay dùng ma trận tọa độ. Cho đến nay, các thuật toán mã hóa phức tạp mà cả siêu máy tính cũng phải mất vài tỉ năm để giải mã được đã ra đời, về mặt cơ bản chia làm hai dạng:

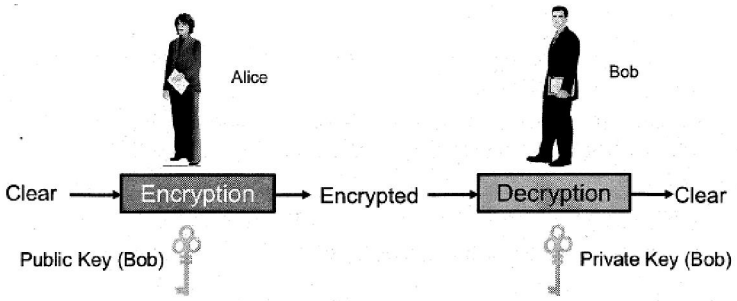
- ***Đồng bộ (Symmetric):*** dùng chung một khóa cho mã hóa, giải mã vì thế người gửi và người nhận yêu cầu phải có khóa giống nhau mới giải mã được. Ngoài ra, thuật toán này hoạt động nhanh hơn, đơn giản hơn, dùng khóa ngắn hơn so với thuật toán bất đồng bộ (Asymmetric) và thường sử dụng khóa có độ dài từ 40 - 256 bit. Ví dụ như DES, 3DES, AES, IDEA, RCx, Blowfish.
- ***Bất Đồng Bộ (Asymmetric):*** còn gọi thuật toán public key, chậm hơn khoảng 1000 lần so với thuật toán đồng bộ (Symmetric) vì phải tiến hành những bước tính toán khó khăn với các con số hàng chục chữ số. Chính vì vậy, thuật toán này thường dùng cho chữ ký số. Tuy nhiên, nó lại đơn giản hơn thuật toán đồng bộ (Symmetric) nhiều trong quản lý khóa bởi thông thường một trong hai khóa được công khai gọi là khóa công khai (public key), còn lại là khóa riêng tư (private key). Việc tính toán chiều dài chính

xác của khóa là không thể, ước lượng từ 512 - 4096 bit và không thể trực tiếp so sánh chiều dài khóa giữa thuật toán đồng bộ (Symmetric) và bất đồng bộ (Asymmetric).

Điểm giống nhau là đều yêu cầu khóa để mã hóa hay giải mã. Tuy nhiên, thuật toán đồng bộ (Symmetric) dùng chung một khóa cho mã hóa và giải mã, còn bất đồng bộ (Asymmetric) dùng một khóa mã hóa và một khóa giải mã, tùy ứng dụng mà hai khóa này được gọi là khóa công khai (public key) hay riêng tư (private key), chủ yếu tùy thuộc hai trường hợp sau:

- ***Public key Confidentiality Scenario:*** khóa công khai (public key) dùng mã hóa và khóa riêng tư (private key) để giải mã. Vì mỗi hệ thống có một khóa riêng tư (private key) khác nhau nên nếu dùng khóa công khai (public key) của hệ thống này để mã hóa thì đảm bảo không hệ thống nào khác giải mã ra được, thường dùng trao đổi khóa.

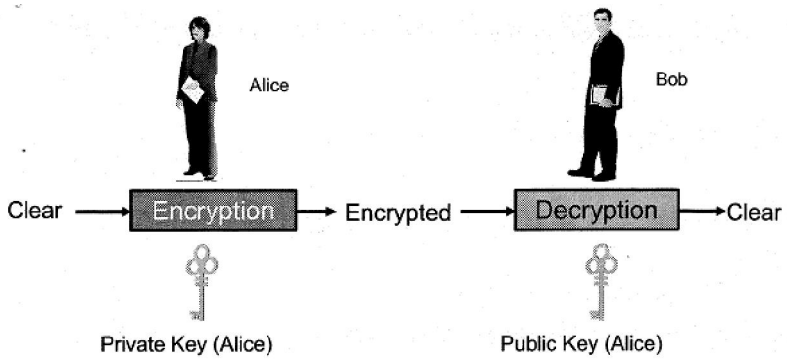
Public key (Encrypt) + Private key (Decrypt) = Confidentiality



Hình 18 – Sơ đồ Public key Confidentiality Scenario

- ***Public key Authentication Scenario:*** khóa riêng tư (private key) dùng mã hóa và khóa công khai (public key) để giải mã. Vì khóa riêng tư (private key) mỗi hệ thống là khác nhau nên khi dùng khóa riêng tư (private key) của hệ thống này mã hóa thì chỉ có khóa công khai (public key) của hệ thống đó mới giải mã ra, thường dùng xác thực.

Private key (Encrypt) + Public key (Decrypt) = Authentication



Hình 19 – Sơ đồ Public key Authentication Scenario

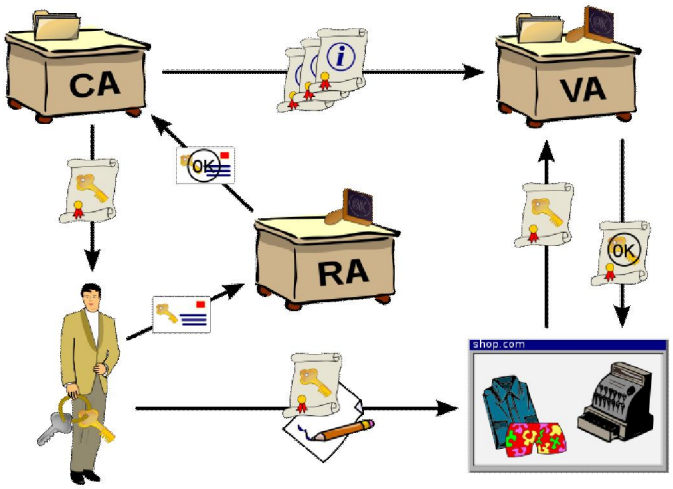
c. Phương thức mã hóa

- ***Mã hóa theo khối (Block cipher):*** dữ liệu được chia làm từng khối có chiều dài cố định và được mã hóa, nếu chiều dài của dữ liệu thô (plaintext) ít hơn so với khối thì dữ liệu rác được thêm vào cho đủ một khối, vì thế thông thường chiều dài của dữ liệu đã mã hóa (ciphertext) lớn hơn chiều dài dữ liệu thô (plaintext). Một số thuật toán ứng dụng cách thức mã hóa này như AES, IDEA....
- ***Mã hóa theo dòng (Stream cipher):*** xử lý trên bit, không thay đổi kích thước dữ liệu mã hóa (ciphertext) so với dữ liệu thô (plaintext) ban đầu và nhanh hơn so với phương thức trên. Một số thuật toán ứng dụng cách thức này như RC4, SEAL…

3.2.3.2 Cơ sở hạ tầng khóa công khai (PKI – Public Key Infrastructure)

a. Giới thiệu

Hệ thống công nghệ mang tính tiêu chuẩn và ứng dụng dùng khởi tạo, lưu trữ và quản lý các chứng thực điện tử (digital certificate) cũng như các mã khoá công khai và riêng tư. PKI ra đời năm 1995, khi các tổ chức công nghiệp và chính phủ xây dựng tiêu chuẩn chung dựa trên phương pháp mã hoá hỗ trợ hạ tầng bảo mật trên mạng Internet. Tại thời điểm đó, mục tiêu là xây dựng bộ tiêu chuẩn bảo mật tổng hợp cùng các công cụ và lý thuyết cho phép người dùng và tổ chức tạo lập, lưu trữ và trao đổi thông tin an toàn trong phạm vi cá nhân và công cộng.



Hình 20 – Sơ đồ Cơ Sở Hạ Tầng Khóa Công Khai (PKI)

Trong mật mã học, PKI là sự sắp xếp gắn các khóa công khai (public key) cho người dùng tương ứng, xác định bởi nhà cung cấp chứng thực số (CA - Certificate Authority) mà định danh mỗi người dùng phải là duy nhất trong toàn CA. Các quá trình này thường được thiết

lập thông qua việc đăng kí và cấp phát chứng nhận tùy vào mức độ đảm bảo mà có thể được thực hiện bởi phần mềm đặt tại trung tâm hoặc là dưới sự giám sát của con người.

- **Public Keys Certificates (Digital Certificate hay Identity Certificate)**

Tài liệu điện tử sử dụng chữ ký số (Digital Siganture) xác thực các bên trao đổi, cấp phát bởi CA, nhằm cấp phát an toàn khoá công khai từ người gửi (mã hoá) đến người nhận (giải mã).

Trước tiên để CA cấp phát public key certificate, người dùng phải đăng ký với CA, gồm các quá trình: đăng ký, kích hoạt và chứng nhận với PKI (CAs và RAs) diễn ra như sau:

- ✓ Người dùng đăng ký với CA hay RA. Trong quá trình đăng ký, đưa ra cách nhận biết đến CA, CA sẽ xác thực đầu cuối, gửi public key của mình đến đầu cuối.
- ✓ Người dùng tạo ra cặp khóa public/private và chuyển khóa công khai (public key) cùng với yêu cầu chứng nhận đến Registration Authority (RA). RA sẽ chịu trách nhiệm chấp nhận hay từ chối yêu cầu người dùng. Sau đó, RA gửi yêu cầu đến CA để xác nhận các chính sách và để xin chữ ký từ CA.
- ✓ CA ký lên public key certificate với khóa riêng tư (private key) của mình để tạo public key certificate cho người dùng
- ✓ Lúc này, người dùng đầu cuối có thể yêu cầu public key certificate cho người khác, sử dụng CAs public key để giải mã nhằm bảo đảm tính hợp lệ của chứng nhận.

b. Các thành phần của PKI: Để bảo đảm các khoá công khai được quản lý an toàn, CA phải quản lý các nhiệm vụ sau:

- Chứng thực và đăng ký mật mã đầu cuối.
- Kiểm tra tính toàn vẹn của khoá công khai.
- Chứng thực yêu cầu trong quá trình bảo quản các khoá công khai.
- Bí mật cấp phát khoá công khai.
- Huỷ bỏ khoá công khai khi nó không có đủ giá trị độ dài.
- Duy trì việc thu hồi các thông tin về khoá công cộng (CRL) và phân bổ thông tin (thông qua CRL cấp phát hoặc đáp ứng đến Online Certificate Status Protocol [OCSP] messages).
- Đảm bảo an toàn về độ lớn của khoá.

Để đơn giản hóa chức năng và giảm bớt việc quản lý khóa cho CA, các chức năng trên lần lượt được chia cho ba bộ phận sau:

- **Registration Authorities**

Trong nhiều trường hợp, CA sẽ cung cấp tất cả các dịch vụ cần thiết của PKI để quản lý các khóa công khai bên trong mạng. Tuy nhiên có nhiều trường hợp CA uỷ nhiệm công việc RA. Một số chức năng CA có thể uỷ nhiệm thay thế RA như:

- ✓ Kiểm tra người dùng đầu cuối đăng ký khóa công khai (public key) với CA để có khóa riêng tư (private key) dùng kết hợp với khóa công khai (public key).
- ✓ Phát cặp khóa công khai và khóa riêng tư (public/private keypairs) dùng khởi tạo quá trình đăng ký.
- ✓ Xác nhận các thông số của khóa công khai (public key).
- ✓ Phát gián tiếp các Certificate Revocation List (CRL).

- **Certificate Authorities**

Cấp phát chứng nhận, xác thực PKI clients và khi cần thiết thu hồi chứng nhận, đại diện nguồn tin cậy chính của PKI. CA là yếu tố duy nhất phát Public Key Certificates đến người dùng đầu cuối đáp ứng sự duy trì CRL và phục vụ CRL Issuer. PKI có thể thiết lập nhiều CA.

Giúp thiết lập việc nhận dạng các thực thể giao tiếp với nhau được đúng đắn. CA không chỉ chứng thực PKI client mà còn cho những CA khác bằng cách cấp phát những chứng nhận số đến chúng. Những CA được chứng thực lần lượt có thể chứng nhận cho những CA khác đến khi mỗi thực thể có thể uỷ nhiệm những thực thể khác có liên quan trong quá trình giao dịch.

- **Validation Authorities:** đảm bảo xác nhận độ an toàn, tin cậy của các chứng nhận số.

Mục đích: cho phép

- ✓ Những người tham gia xác thực lẫn nhau và sử dụng các thông tin từ chứng nhận để mã hoá và giải mã thông tin trong quá trình trao đổi.
- ✓ Các giao dịch điện tử diễn ra bí mật, toàn vẹn và xác thực lẫn nhau mà không cần trao đổi thông tin bảo mật trước.
- ✓ Cung cấp khoá công khai và xác định mối liên hệ giữa khoá và định dạng người dùng. Nhờ vậy, người dùng có thể sử dụng trong một số ứng dụng như:
  - o Mã hoá Email hay xác thực người gửi Email.
  - o Mã hoá hoặc chứng thực văn bản.
  - o Xác thực người dùng ứng dụng.
  - o Các giao thức truyền thông an toàn: trao đổi bằng khoá bất đối xứng, mã hoá bằng khoá đối xứng.

Để cung cấp khả năng mã hóa và xác thực, PKI sử dụng:

- **Thuật toán băm**

Bảo đảm tính toàn vẹn của dữ liệu, nếu có thay đổi nhỏ cũng phát hiện ngay. Nó hoạt động một chiều, với bất kỳ giá trị đầu vào nào thì băm vẫn cho giá trị đầu ra có chiều dài cố định. Tuy nhiên, thuật toán băm không mã hóa dữ liệu, tiêu biểu là MD5 và SHA-1.

Để tăng tính bảo mật, HMAC ra đời. Đối với thuật toán băm, tuy dữ liệu thay đổi bị phát hiện nhưng nếu giá trị băm cũng thay đổi thì không thể nhận ra, HMAC dùng khóa bí mật (secrect key) cho quá trình băm, tăng khả năng xác thực và chống tấn công Man - in - the - middle.

- **Chữ ký số (Digital Signature)**

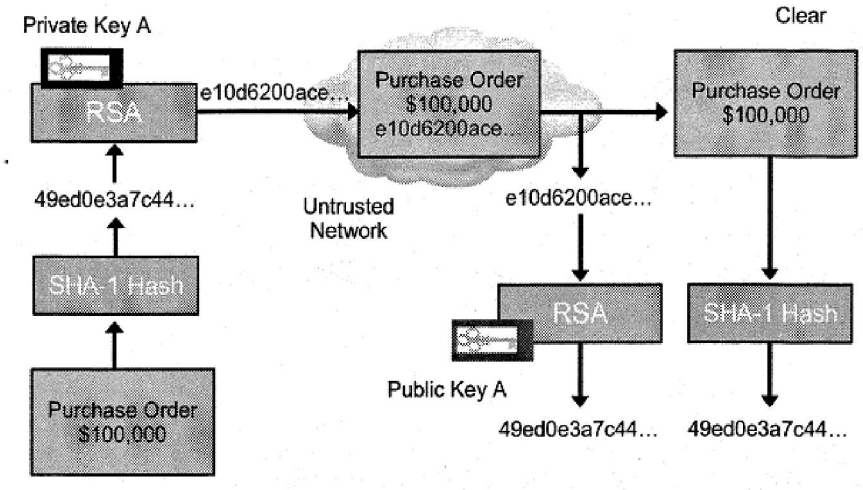
Trong quá trình giao tiếp, không chỉ đảm bảo dữ liệu không thay đổi khi truyền mà còn phải được gửi từ nguồn tin cậy. Chữ ký số cung cấp giải pháp cho vấn đề này bằng việc đưa ra bằng chứng duy nhất dữ liệu gốc, phát hiện nếu có bất cứ thay đổi nào, xác thực bằng khóa riêng tư (private key) ký lên dữ liệu, chứng minh tính xác thực và toàn vẹn chứng nhận.

Về cơ bản chữ ký số hoạt động như sau: khi A gửi tin nhắn cho B, tin nhắn này được ký với khóa riêng tư (private key) của A (signature key) tạo ra chữ ký số mà chỉ có khóa riêng tư (private key) của A mới có thể tạo ra chữ ký này. Sau đó, nó được đính kèm tin nhắn ban đầu và gửi cho B. Sau khi nhận được, B dùng khóa công khai (public key) của A (verification key) giải mã phần chữ ký của A, nếu khác với tin nhắn thì nội dung thông điệp đã thay đổi và ngược lại; đồng thời A không thể thoái thác trách nhiệm khi gửi tin nhắn này, vì chỉ có A mới tạo ra được chữ ký như vậy.

Chữ ký số RSA (RSA Digital Signature): thuật toán bất đồng bộ phổ biến nhất do Ron Rivest, Adi Sharmi và Len Adlemen xây dựng vào 1977. Hoạt động dựa trên những phép tính phức tạp với con số lên đến hàng chục, hàng trăm chữ số. RSA sử dụng khóa công khai (public key) được quảng bá rộng rãi và khóa riêng tư (private key) giữ bí mật tuyệt đối.

Hoạt động

Đầu tiên tin nhắn được băm, tạo ra giá trị băm; giá trị này được ký (mã hóa) với khóa riêng tư (private key) của A tạo ra chữ ký. Chữ ký này đính kèm với tin nhắn gửi cho B. Sau khi B nhận được tiến hành hai công đoạn, lấy chữ ký giải mã với public key của A được giá trị H1 và lấy tin nhắn đem đi băm tạo ra H2. Nếu H1 = H2 tin nhắn không bị chỉnh sửa trên đường đi và gửi từ A; nếu không ngược lại.



Hình 21 – Sơ đồ hoạt động

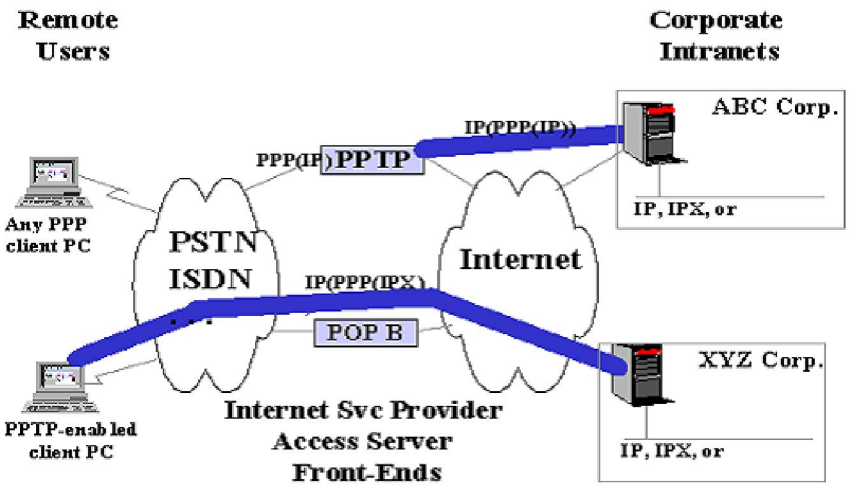
3.2.4 Các giao thức VPN

3.2.4.1 PPTP (Point-to-Point Tunneling Protocol)

Như giao thức L2F (Layer 2 Forwarding), giao thức tạo đường hầm điểm nối điểm (PPTP) ban đầu được thiết kế và phát triển để tạo và duy trì đường hầm VPN trên mạng công cộng dựa vào TCP/IP nhờ sử dụng PPP - kết quả nỗ lực chung của tập đoàn Microsoft và hàng loạt nhà cung cấp gồm Ascend Communications, 3Com/Primary Access, ECI Telematics…

Sử dụng trên các máy người dùng với hệ điều hành Microsoft NT4.0 và Windows 95+, dùng mã hóa dữ liệu lưu thông trên Mạng LAN. PPTP được phát triển dựa trên chuẩn RSA RC4 và hỗ trợ bởi sự mã hóa 40-bit hoặc 128-bit. PPTP được dùng để bao bọc các khung PPP trong các gói IP để truyền trên Internet hoặc bất kỳ mạng khác TCP/IP có thể truy cập công cộng.

- Nếu hệ thống từ xa hỗ trợ PPTP, thì có thể kết nối trực tiếp với VPN Server.
- Ngược lại, có thể sử dụng PPP để nối kết với máy khởi tạo kết nối VPN (L2TP Access Concentrator – LAC) của nhà cung cấp dịch vụ Internet và sau đó sử dụng PPTP để kết nối với VPN Server.

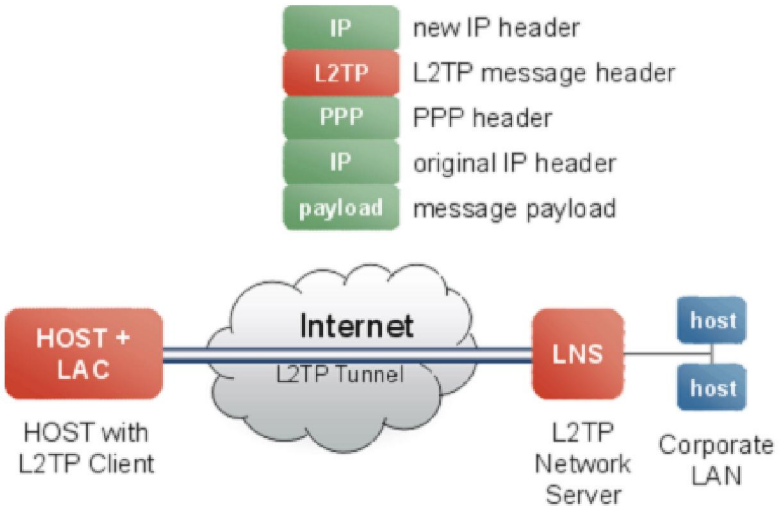


Hình 22 – Kết nối VPN qua giao thức PPTP

PPTP không phát triển trên LAN-to-LAN, giới hạn 255 kết nối tới server và chỉ có một đường hầm VPN trên một kết nối. Ngoài ra, PPTP không cung cấp khả năng mã hóa cho các công việc lớn nhưng lại dễ cài đặt và triển khai và là giải pháp truy cập từ xa chỉ có thể làm được trên mạng Microsoft. Giao thức này thì được dùng tốt trong Window 2000...

3.2.4.2 L2TP (Layer 2 Tunneling Protocol)

Ra đời vào năm 1999 và được định nghĩa trong RFC 2661, xuất phát từ việc kế thừa những điểm mạnh của các giao thức trước đó là L2F (Layer 2 Forwarding) của Cisco và PPTP của Microsoft. Phiên bản mới hơn của giao thức này- L2TPv3 đã được phát hành vào năm 2005, cung cấp những tính năng bảo mật khác như khả năng mã hóa, có thể mang những liên kết dữ liệu khác ngoài kết nối PPP trên mạng IP như là Frame Relay, Ethernet, ATM, …



Hình 23 – L2TP VPN

Tạo kết nối độc lập, đa giao thức cho mạng riêng ảo quay số (Virtual Private Dail-up Network), cho phép người dùng kết nối thông qua chính sách bảo mật (security policies) để tạo VPN hay VPDN. Tuy nhiên, giao thức này không cung cấp mã hóa.

Hiệu quả trong kết nối mạng quay số, ADSL, và các mạng truy cập từ xa khác. Giao thức mở rộng này sử dụng PPP cho phép truy cập VPN bởi những người sử dụng từ xa. Một đường hầm L2TP được thiết lập thông qua ba dạng:

- Voluntary Tunnel.
- Compulsory tunnel (cho các kết nối đi tới và cho dạng quay số từ xa).
- L2TP multi-hop connection.

3.2.4.3 GRE

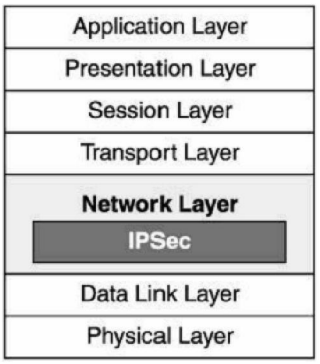
Đa giao thức truyền thông đóng gói IP, CLNP và các gói dữ liệu bên trong đường ống IP (IP tunnel). Với GRE Tunnel, Cisco Router đóng gói mỗi vị trí một giao thức đặc trưng chỉ định trong gói IP header, tạo đường kết nối ảo (virtual point-to-point) tới Cisco Router cần đến và khi gói dữ liệu đến đích IP header sẽ được mở ra.

Bằng việc kết nối nhiều mạng con với các giao thức khác nhau trên giao thức chính. Đường hầm (GRE tunneling) cho phép các giao thức khác thuận lợi trong việc định tuyến cho gói IP.

3.2.4.4 IPSec (Internet Protocol Security)

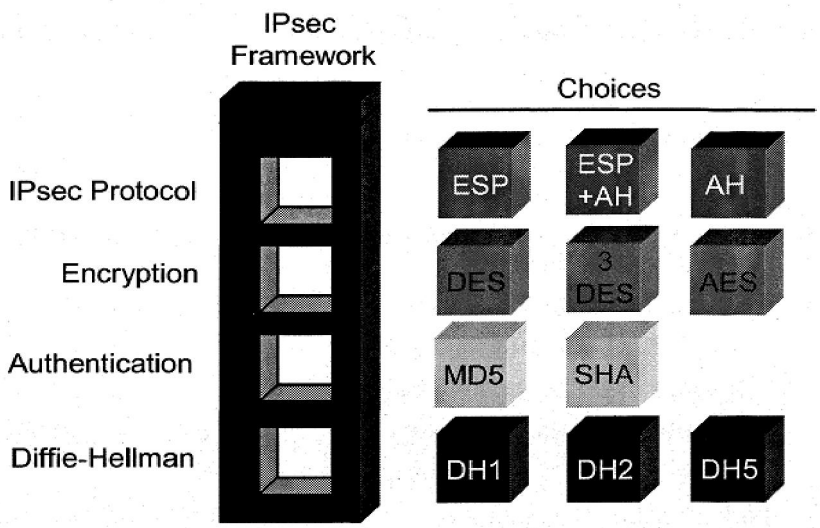
a. Giới thiệu

Phát triển bởi IETF định nghĩa trong RFC 2401 - 2412, quy định phương thức thiết lập VPN (Virtual Private Network) sử dụng IP address protocol nhằm cung cấp cơ cấu bảo mật ở lớp Network. Do đó, IPSec hỗ trợ tất cả ứng dụng, bảo vệ và xác thực gói tin IP giữa các bên. IPSec không ràng buộc bất kỳ thuật toán mã hóa, xác thực cụ thể nào mà là tổ hợp nhiều chuẩn mở.



Hình 24 – IPSec trong mô hình OSI

Nhờ đó, IPSec cho phép ứng dụng các thuật toán mới hơn, tốt hơn mà không cần sửa đổi chuẩn cũ. IPSec cung cấp khả năng bảo mật (Encryption Algorithm), toàn vẹn dữ liệu (Data Integrity), khả năng xác thực (Authentication) các bên ở lớp Network, tạo nên đường truyền bảo mật giữa một cặp Gateway hay cặp Host thậm chí giữa Gateway và Host.



Hình 25 – Các thành phần trong IPSec

Encryption: Mức độ bảo mật, khả thi tùy vào chiều dài khoá mã hóa và thời gian xử lý thuật toán. Do đó, vấn đề đặt ra là chọn lựa thuật toán nào với độ dài khóa như thế nào để hệ thống vừa bảo mật vừa không tiêu tốn quá nhiều hiệu suất xử lý. Sau đây là một số thuật toán và độ lớn của khóa khuyến khích dùng: DES (56 bit), 3DES (112 bit, 168 bit), AES (128 bit, 192 bit, 256 bit), RSA (512 bit, 768 bit, 1024 bit), SEAL (160 bit).

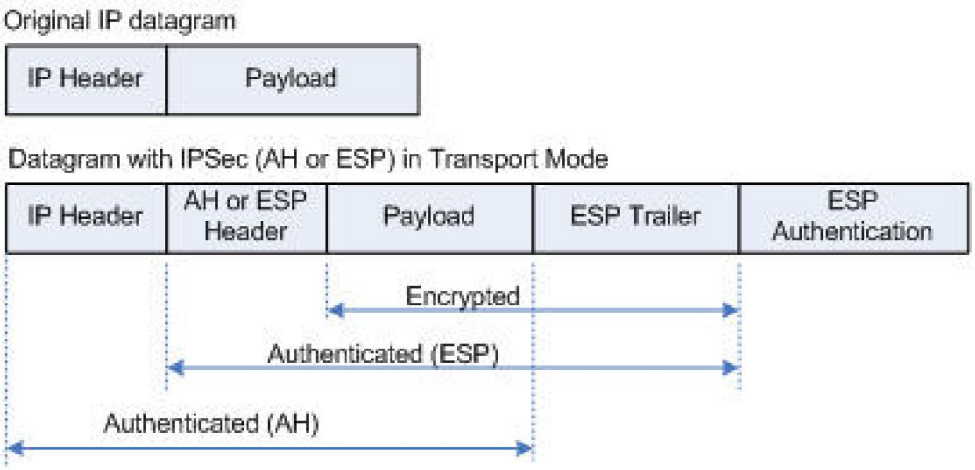
Data Integrity: dữ liệu truyền trên Internet có thể bị chỉnh sửa. Vì thế, IPSec sử dụng thuật toán HMAC - MD5 hoặc HMAC - SHA - 1 để bảo toàn dữ liệu.

Authentication: xác thực đối tượng giao tiếp là điều hết sức quan trọng trước khi bắt đầu thiết lập kết nối giữa hai bên. IPSec cung cấp ba phương thức xác thực:

- **Pre-shared Key:** giá trị nhập bằng tay vào mỗi bên, dùng để xác thực với nhau.
- **RSA signature:** trao đổi nhau chứng nhận, sau đó mỗi bên sinh ra một giá trị băm từ tin nhắn và mã hóa với khóa riêng tư (private key) của mình, đính kèm tin nhắn và gửi cho nhau. Sau khi nhận được, mỗi bên dùng khóa công khai (public key) giải mã giá trị băm đã mã hóa. Nếu trùng giá trị băm tin nhắn nhận được thì xác thực thành công.
- **RSA encrypted nonce:** tương tự RSA signature. Tuy nhiên không dùng chứng nhận (certificate), thay vào đó, khóa công khai (public key) nhập bằng tay ở mỗi bên.

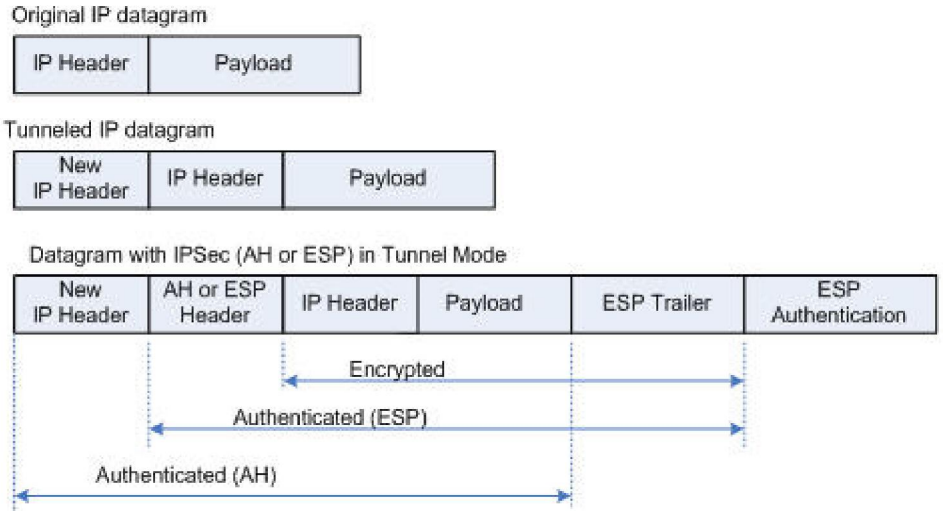
IPSec hoạt động ở hai mode:

- ***Transport mode:*** chỉ bảo vệ payload của gói tin, từ ip header trở đi vẫn không đổi. Tuy nhiên, nếu như AH được sử dụng thì ip header không thể thay đổi. Việc thay đổi ip header sẽ dẫn đến gói tin bị drop. Vì thế chỉ hoạt động tốt giữa host và host. Vấn đề này được giải quyết khi sử dụng NAT – Traversal, sẽ được đề cập sau.



Hình 26 – Transport mode

- ***Tunnel mode:*** bảo mật toàn vẹn gói tin IP định tuyến (Routable IP) trên Internet. So với Transport mode, Tunnel mode hoạt động tốt hơn, hỗ trợ cả Gateway to Gateway. Tuy nhiên, về hiệu năng mạng thì Tunnel mode không bằng Transport mode vì Tunnel mode phát sinh thêm trường IP header mới, còn Transport mode thì không.



Hình 27 – Tunnel Mode

b. Tổng hợp các giao thức và thuật toán được sử dụng

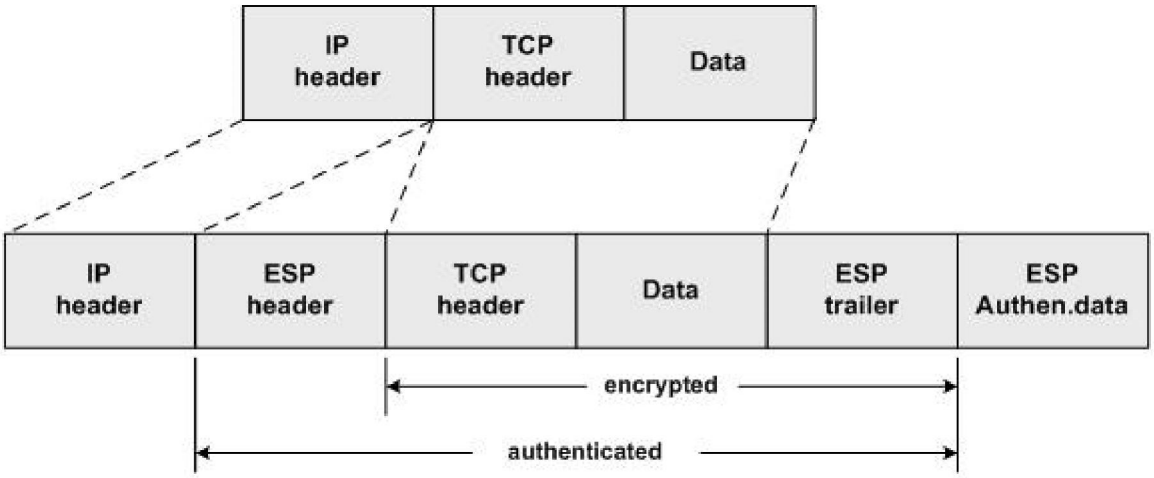
Các giao thức sử dụng

- **ESP (Encapsulating Security Payload)**

Một trong hai giao thức chính cấu thành IPSec. ESP bảo mật cao, hỗ trợ nhiều thuật toán mã hóa đối xứng như DES và 3DES. Ngoài ra, ESP hỗ trợ tính toàn vẹn dữ liệu (Integrity) và chứng thực (Authentication).

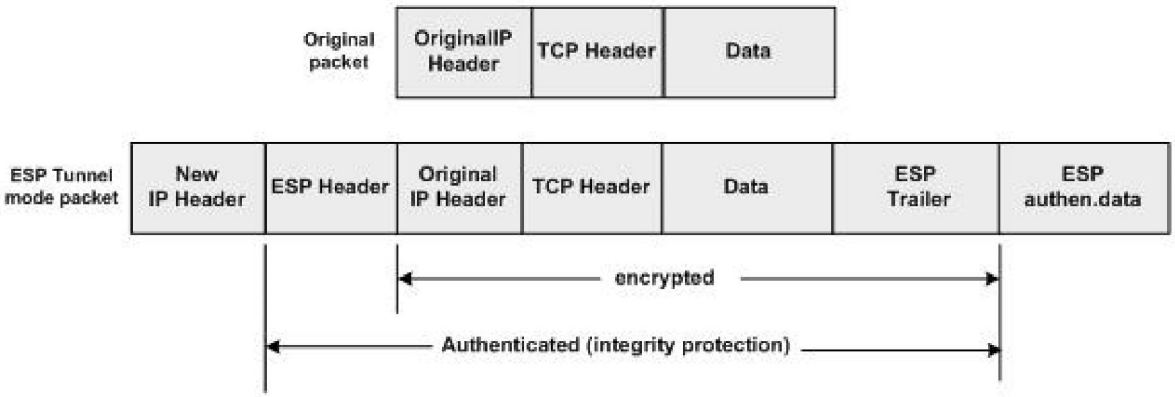
Hoạt động ở hai mode: transport mode và tunnel mode.

Transport mode, ESP chỉ mã hóa và xác thực nội dung của dữ liệu và một số thành phần khác như hình 28.



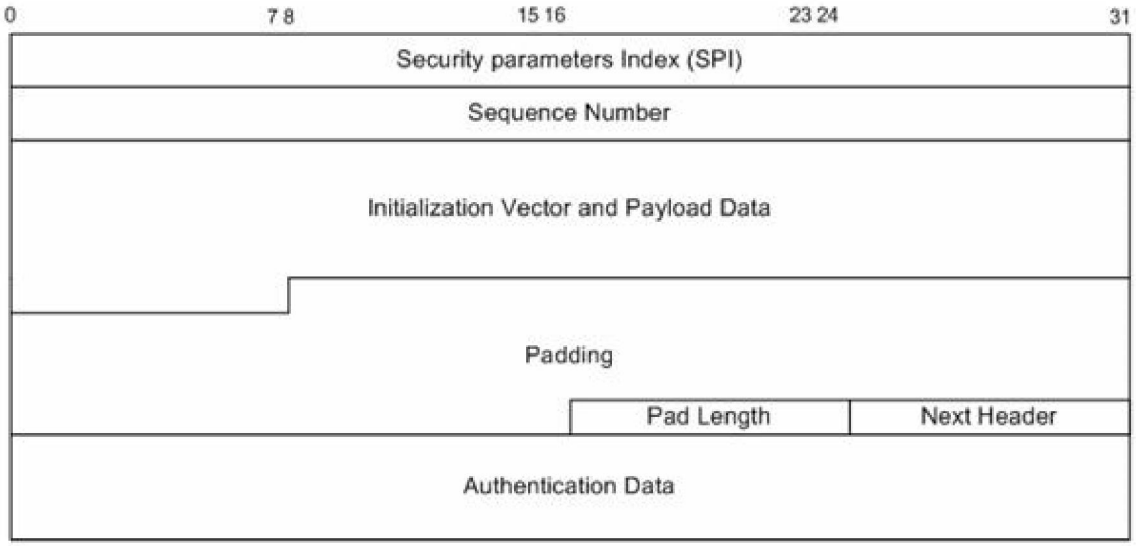
Hình 28 – ESP Transport mode packet

Đối với Tunnel Mode, ESP mã hóa toàn bộ dữ liệu gốc và xác thực phần dữ liệu đã mã hóa này cùng với ESP Header được thêm vào cùng với IP header mới.



Hình 29 – ESP Tunnel mode packet

Các trường trong gói tin ESP



Hình 30 – ESP fields

ESP thêm một header và trailer vào xung quanh nội dung mỗi gói tin. ESP Header được cấu thành bởi hai trường:

- ***SPI (32 bits):*** đầu cuối mỗi kết nối IPSec tuỳ chọn giá trị SPI. Phía nhận dùng giá trị SPI với IP đích và giao thức IPSec để xác định chính sách SA duy nhất mà nó được áp cho gói tin.
- ***Sequence Number:*** cung cấp dịch vụ anti-replay. Khi SA được thiết lập, chỉ số này khởi đầu về 0. Trước khi mỗi gói tin được gửi, chỉ số này tăng lên 1 và đặt trong ESP Header.

Phần kế tiếp của gói tin là Payload, nó được tạo bởi Payload data (được mã hoá) và Initialization Vector (IV) không mã hoá. Giá trị IV trong suốt quá trình mã hoá là khác nhau trong mỗi gói tin.

Phần thứ ba của gói tin là ESP Trailer, nó chứa ít nhất là hai trường:

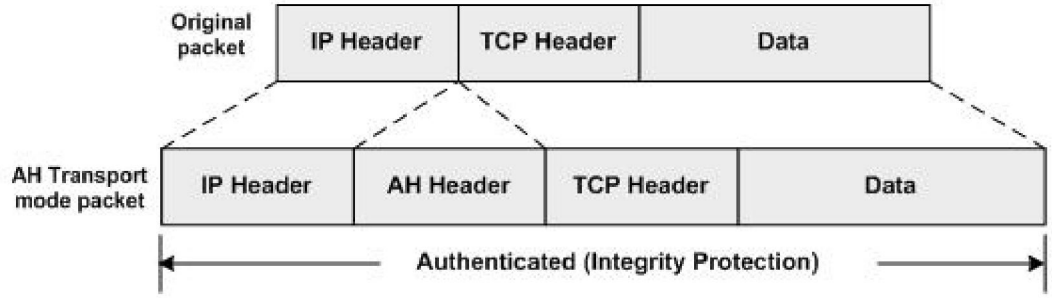
- ***Padding* (0-255 bytes):** *có thể* được thêm vào cho đủ kích thước của mỗi gói tin.
- ***Pad length:*** chiều dài của Padding.
- ***Next header:*** xác định kiểu giao thức chứa trong trường payload. Nếu là IP thì chứa giá trị là 4, nếu là TCP thì 6, UDP thì 17. Mỗi ESP Trailer chứa một giá trị Next Header.

Và cuối cùng là Authentication data chứa giá trị Integrity Check Value (ICV) cho gói tin ESP. ICV được tính lên toàn bộ gói tin ESP công nhận cho trường dữ liệu xác thực của nó. ICV bắt đầu trên ranh giới 4 byte và phải là bội số của 32-bit (đơn vị từ).

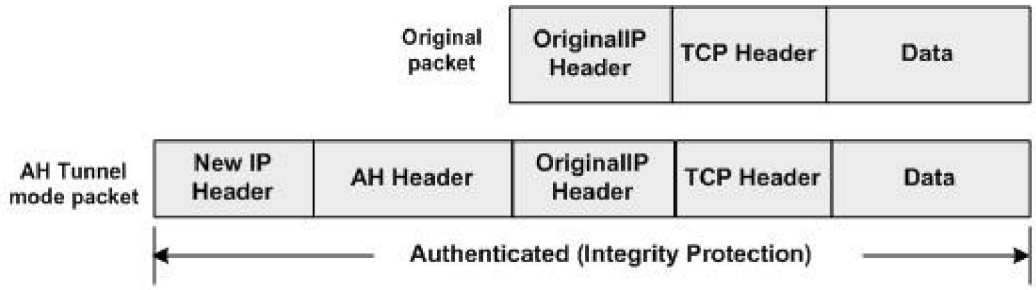
- **AH (Authentication Header)**

Cùng ESP, AH là hai giao thức chính cấu thành IPSEC, cung cấp tính toàn vẹn dữ liệu, xác thực. AH băm các trường dữ liệu trong gói tin kể cả IP header, ngoại trừ những trường thay đổi trên đường đi như TTL (Time – To – Live), trường AH header do hàm băm sinh ra được thêm vào gói tin. Vì trường IP header được băm nên nếu trên đường đi có NAT (Network Address Translation) thì AH không hoạt động được. AH hoạt động như chữ ký số đảm bảo gói tin không bị giả mạo nhưng lại không cung cấp khả năng mã hóa và giải mã.

Cũng như ESP, **AH có hai mode:** transport mode và tunnel mode.



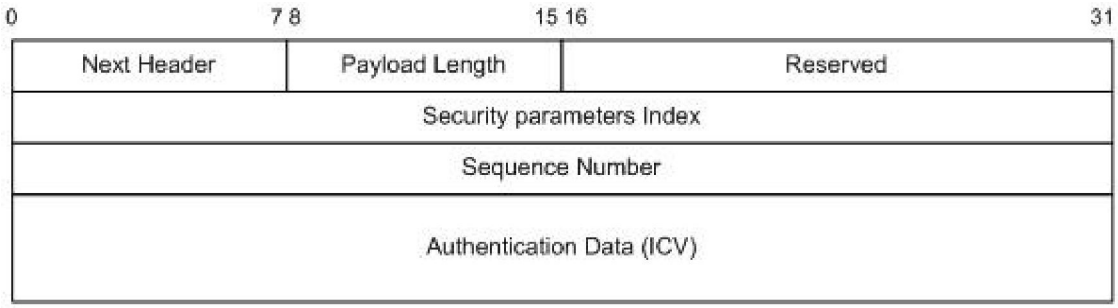
Hình 31 – AH Transport mode



Hình 32 – AH Tunnel mode

Đối với cả hai mode, AH xác thực toàn bộ gói tin (từ data đến IP header). Sự thay đổi ip trên đường truyền dẫn đến AH không hoạt động được.

AH Header gồm các trường sau:



Hình 33 – AH header

- ***Next Header:*** dài 8 bits, xác định kiểu giao thức chứa trong trường payload.
- ***Payload Length:*** chứa chiều dài AH Header.
- ***Reserved*****:** dành sử dụng trong tương lai (cho đến thời điểm này nó được biểu thị bằng các chỉ số 0).
- ***Security parameter Index (SPI):*** đầu cuối mỗi kết nối IPSec tuỳ ý chọn giá trị SPI, dùng nhận dạng kết nối. Bên nhận sử dụng giá trị SPI cùng với địa chỉ IP đích và loại giao thức IPSec (trường hợp này là AH) để xác định chính sách SA dùng cho gói tin (nghĩa là giao thức IPSec và các thuật toán nào được dùng để áp cho gói tin).
- ***Sequence Number:*** tăng lên 1 cho mỗi AH datagram khi một host gửi có liên quan đến chính sách SA. Giá trị bắt đầu của bộ đếm là 1, chuỗi số này không bao giờ cho phép ghi đè lên là 0 vì khi host gửi yêu cầu kiểm tra mà nó không bị ghi đè và nó sẽ thoả thuận chính sách SA mới nếu SA này được thiết lập. Host nhận sẽ dùng chuỗi số để phát hiện replayed datagrams. Nếu kiểm tra bên phía host nhận, bên nhận có thể nói cho bên gửi biết rằng bên nhận không kiểm tra chuỗi số, nhưng đòi hỏi nó phải luôn có trong bên gửi để tăng và gửi chuỗi số.
- ***Authentication Data:*** chứa kết quả của giá trị Integrity Check Value (ICV), luôn là bội của 32-bit (từ) và phải được đệm vào nếu chiều dài ICV trong các bytes chưa đầy.

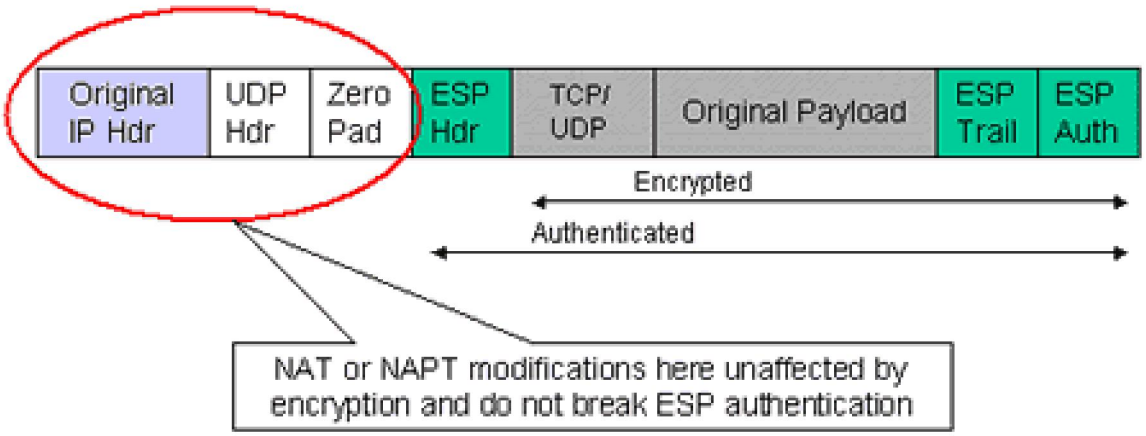
Trong quá trình hoạt động, việc xác thực IPSec mang lại lợi ích rất cao. Tuy nhiên bên cạnh đó, nó cũng mang lại không ít sự phiền toái.

- AH xác thực gói tin dựa vào thông tin IP header. Do vậy, nó sẽ không tương thích với các thay đổi do cơ chế NAT mang lại. Vì giá trị ICV của AH được tính toán trước NAT nên khi gói tin gửi tới đích, việc kiểm tra tính toàn vẹn sẽ thất bại.
- Trong chế độ *transport*, ESP và NAT không tương thích với nhau vì các thông tin của phần header gói tin bị NAT thay đổi. Khi NAT thực hiện thay đổi phần thông tin về IP, nó cũng tính lại giá trị **checksum** trong TCP header và vì TCP checksum được tính toán không chỉ dựa vào TCP header, mà còn dựa vào các thông tin từ IP header,

như địa chỉ nguồn/đích của gói tin nên NAT đã phá vỡ tính toàn vẹn gói tin. Trong chế độ Transport ESP, toàn bộ TCP header được mã hoá, NAT box không thể tính toán lại TCP checksum (tương tự đối với UDP packets khi UDP checksum được tính đến). Kết quả là trước khi giải mã, gói tin sẽ bị hủy vì không bảo đảm tính toàn vẹn.

Để giải quyết các vấn đề trên, **NAT – Traversal** ra đời vào năm 2001, là kết quả đồng ý hợp nhất hai phương pháp tiếp cận cạnh tranh được đề xuất với IETF của SSH Communications và các đồng tác giả F-Secure, Microsoft, Cisco, Nortel.

Giải pháp là gói tin sau khi được mã hóa, xác thực thì được đóng gói theo giao thức UDP với sự xuất hiện của hai trường bổ sung là UDP header và Zeropad.



Hình 34 – Gói tin hỗ trợ NAT-Traversal

Hiện tại, AH không tương thích NAT – Traversal vì không sử dụng rộng rãi nên không được ưu tiên phát triển. SSH Communications cũng đã đề xuất phát triển thêm để hỗ trợ AH.

Tất nhiên, để sử dụng NAT – Traversal, cả hai thiết bị đầu cuối (gateway to gateway, client to gateway, client to client) đều phải hỗ trợ.

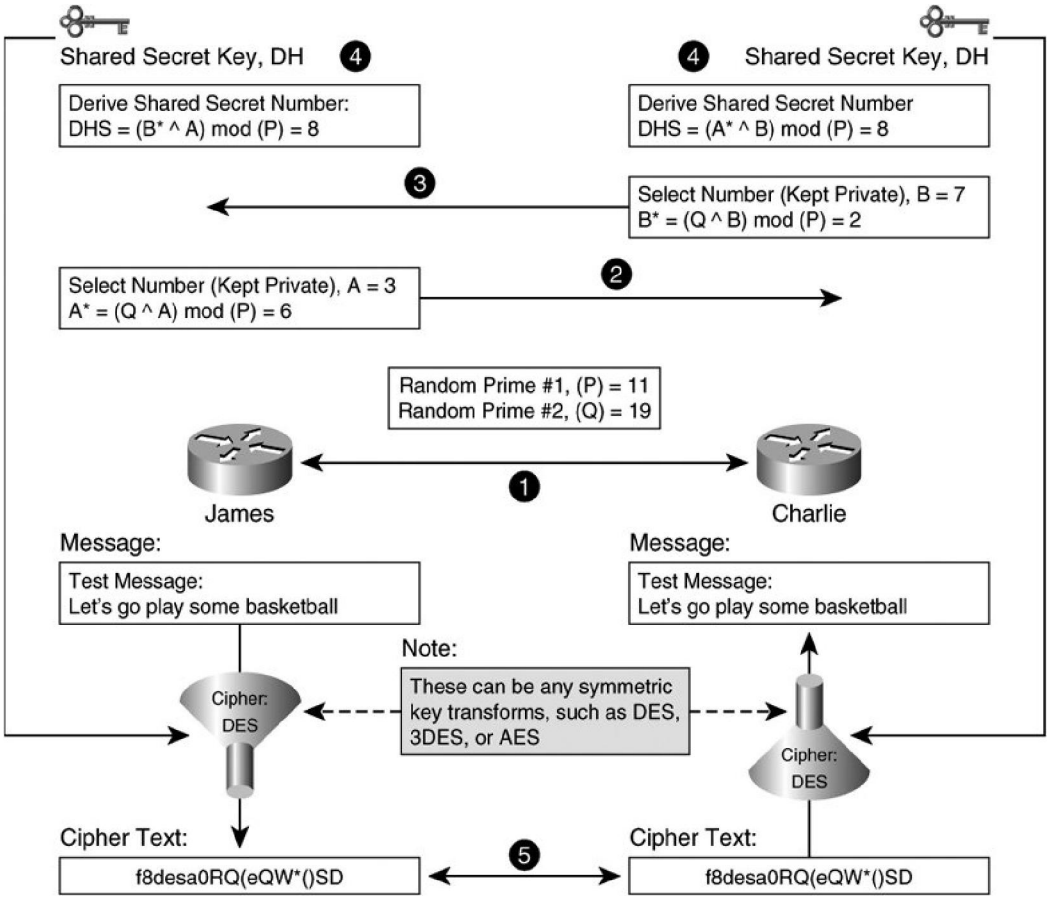
- **IKE (Internet Key Exchange)**

Xác thực hai bên, đàm phán giữa IKE và IPSec SA, tạo các khóa để mã hóa dữ liệu IPSec, có cùng chức năng với ISAKMP (Internet Security Association and Key Management Protocol).

- **DH (Diffie-Hellman)**

Tạo khóa bí mật (secrect key) giữa hai bên trên kênh truyền không bảo mật, dùng bên trong IKE để tạo session key. Hoạt động bằng cách hai bên thống nhất nhau (có thể công khai) 2 số p và q (số nguyên nhỏ hơn p), mỗi bên giữ số bí mật lần lượt a, b. Sau đó A gửi X = (q^a)

mod p cho B, B cũng gửi Y = (q^b) mod p cho A. Bằng phương pháp tính toán riêng, hai bên cùng tính ra giá trị K = ((q^b)^a) mod p = ((q^a)^b) mod p là khóa bí mật (secrect key).



Hình 35 – Cách thức hoạt động của DH

Các thuật toán sử dụng

- **Thuật toán mã hoá**

DES (Data Encryption Standard): còn gọi Lucifer, phát triển bởi IBM vào năm 1975, thuật toán mã hóa đối xứng hoạt động ở dạng mã hóa từng khối (block cipher - 64 bit block). DES là sự trao đổi có trình tự và thay thế các bit dữ liệu, kết hợp khóa mã hóa, hỗ trợ khóa có chiều dài 64 bit trong đó 56 bit mã hóa, 8 bit còn lại kiểm tra parity. Tuy nhiên, nếu dùng khóa có chiều dài nhỏ hơn 56 bit ví dụ 40 bit thì độ mạnh thật sự của khóa chỉ ở 40 bit.

DES dựa trên những tính toán cơ bản nên nó có thể dễ dàng được triển khai trên phần cứng, chú trọng đến tốc độ mã hóa và giải mã, chia làm hai dạng con:

- ***Dạng ECB (Electronic Code Book):*** mỗi dữ liệu thô (plaintext) 64 bit dùng chung khóa 56 bit mã hóa, nếu hai khối dữ liệu thô giống nhau dùng chung khóa mã hóa thì dữ liệu mã hóa (ciphertext) sẽ giống nhau. Vì thế, kẻ tấn công có thể lợi dụng điểm này, bắt lại các gói tin, không quan tâm nội dung bên trong và gửi lại. Ví dụ kẻ tấn

công bắt lại gói tin đăng nhập của người quản trị được bảo vệ bởi DES - ECB, sau đó gửi lại và kẻ tấn công có thể xâm nhập hệ thống. Để chống lại điều này, CBC ra đời.

- ***Dạng CBC (Cipher Block Chaining):*** mỗi khối 64 bit dữ liệu thô (plaintext) đều được XOR với dữ liệu mã hóa (ciphertext) sau đó dữ liệu thô (plaintext) đã XOR mới được mã hóa. Vì thế nếu tất cả khối dữ liệu thô (plaintext) đều giống nhau thi cũng không thể cho ra dữ liệu mã hóa (ciphertext) giống nhau...

3DES (Triple Data Encryption Standard): dạng biến đổi của DES được lặp đi lặp lại ba lần với các khóa khác nhau vì thế 3DES mạnh hơn DES gấp đôi, có thể chống lại tấn công Brute - Force. 3DES sử dụng khóa có chiều dài lên đến 168 bit so với DES (56bit) bao gồm ba khóa có chiều dài 56 bit K1, K2, K3.

- ***Mã hóa:*** dùng K1 mã hóa, dùng K2 giải mã, dùng K3 mã hóa.
- ***Giải mã:*** dùng K3 giải mã, K2 mã hóa, K1 giãi mã.

AES (Advanced Encryption Standard): NIST (The National Institute of Standards and Technology) đưa ra AES thay thế DES trong các thiết bị mã hóa. AES cung cấp tính bảo mật cao hơn nhiều so với DES và hiệu quả hơn so với 3DES. AES dùng khóa 128, 192, 256 bit.

RSA (Rivest, Shamir, and Adleman) signature: mã hóa bất đồng bộ, tùy mục đích sử dụng mà dùng khóa mã hóa giải mã thích hợp, ứng dụng nhiều nhất trong chữ ký điện tử.

- **Thuật toán băm**

MD5 (Message Digest 5): dùng để xác thực gói tin dữ liệu, đảm bảo nếu gói tin bị chỉnh sửa trên đường truyền sẽ phát hiện ra. HMAC (MD5 Hashed Message Authentication Code) là biến thể của MD5, cung cấp tính an toàn cao hơn MD5. Thuật toán băm là thuật toán một chiều. Vì thế, việc chuyển giá trị đã được băm về giá trị ban đầu là không thể. Bất kể giá trị đầu vào là bao nhiêu thì giá trị đầu ra vẫn là cố định. IKE và ESP dùng MD5 để xác thực.

SHA-1 (Secure Hash Algorithm 1): Như MD5, SHA-1 là một thuật toán hash dùng để xác thức dữ liệu gói tin, biến thể là HMAC-SHA-1và dùng để xác thực IKE và ESP.

c. IPSec hoạt động: gồm 5 bước chính

***Bước 1 - Xác định Interesting trafic*:** luồng thông tin được coi là **Interesting trafic** khi nó được nhận ra rằng đây là dữ liệu cần được bảo vệ, tùy thuộc vào chính sách trên thiết bị VPN. Mỗi dữ liệu đi qua thiết bị (Inbound, Outbound) đều có 2 hướng xử lý:

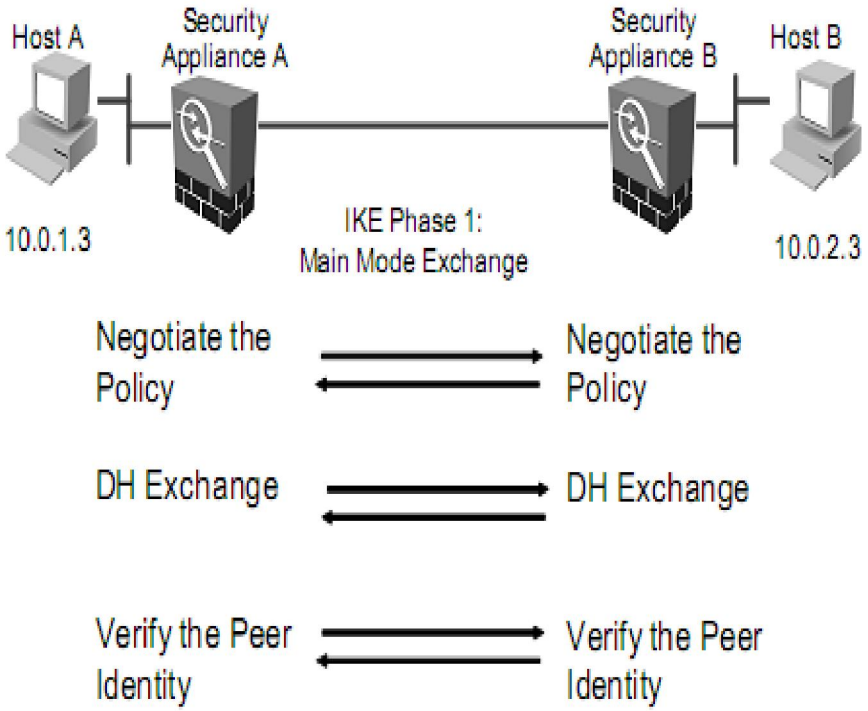
- Bỏ qua IPSec, dữ liệu được gửi dạng cleartext.
- Áp các chính sách IPSec đã được định trước.

Bước 2 - IKE Phase 1: Mục đích cơ bản là đàm phán các chính sách, xác thực peer và thiết lập kênh bảo mật giữa các bên, xảy ra trong hai mode:

- **Aggressive mode:** nhanh hơn nhưng không hỗ trợ khả năng bảo vê tính toàn vẹn của dữ liệu trên đường truyền như main mode. Do đó, hai bên phải trao đổi thông tin xác định trước để thiết lập secure CA, bao gồm hai bước:
  - ✓ **Bước 1:** đàm phán chính sách, DH public key khởi tạo, gửi cho đối tác cùng thông tin xác thực hai bên, sau khi ký thì gói tin trả về và hoàn tất quá trình trao đổi.
  - ✓ **Bước 2:** tái khẳng định quá trình trao đổi.
- **Main mode:** gồm ba bước trao đổi:
  - ✓ **Bước 1:** dùng các thuật toán và hàm băm để bảo mật thông tin IKE được đàm phán và chấp nhận giữa các bên.
  - ✓ **Bước 2:** sử dụng DH để tạo khóa bí mật (secrect key) dùng để sinh ra tất cả khóa cho quá trình mã hóa và xác thực ở bước một kể cả bước hai (nếu cần thiết).
  - ✓ **Bước 3:** xác minh tính xác thực peer còn lại, dùng xác thực remote peer. Nếu không tiến hành xác thực, có khả năng khởi tạo kết nối bảo mật với kẻ tấn công.
- **Policy set:** khi cố gắng thiết lập kênh bảo mật, chính sách đề nghị trao đổi với nhau. Căn cứ chính sách này, lần lượt kiểm tra theo độ ưu tiên từ cao đến thấp (một là cao nhất), đến khi hai bên chọn ra chính sách phù hợp mà cả hai cùng hỗ trợ (cùng thuật toán mã hóa, xác thực, DH và băm) thì qua bước tiếp theo, nếu không kết nối bị ngắt.
- **DH key exchange:** phương thức trao đổi khóa cung cấp giải pháp cho hai bên giúp tạo nên khóa bí mật (secrect key) trên đường truyền không bảo mật mà vẫn đảm bảo độ an toàn của khóa. DH có nhiều nhóm (1 - 7) trong đó nhóm 5 khuyến khích dùng nhất, nhóm 7 chỉ dùng cho các thiết bị cầm tay có vi xử lý yếu. Sau khi việc đàm phán nhóm kết thúc, khóa bí mật (secrect key) được tính toán. Khóa bí mật chia sẻ (Shared secrect key - SKEYID) này được dùng để tính ra ba khóa khác: SKEYID_a, SKEYID_d, SKEYID_e. Mỗi khóa có mục đích sử dụng khác nhau. SKEYID_a dùng cho quá trình xác thực, SKEYID_e dùng cho quá trình mã hóa (bước 1), SKEYID_d dùng sinh khóa cho bước 2. Tất cả khóa trên đều được sinh ra sau khi kết thúc bước 1.
- **Authenticate Peer Identity:** Trên thiết bị nói riêng và cuộc sống nói chung, việc xác định được người đang giao tiếp là điều hết sức quan trọng và không hề dư thừa. Vì thế trước khi qua bước 2 (lập kênh bảo mật cho dữ liệu) thì cần phải có bước xác thực hai bên (peer). Có 2 cách xác thực: Pre-shared key hay RSA signature.

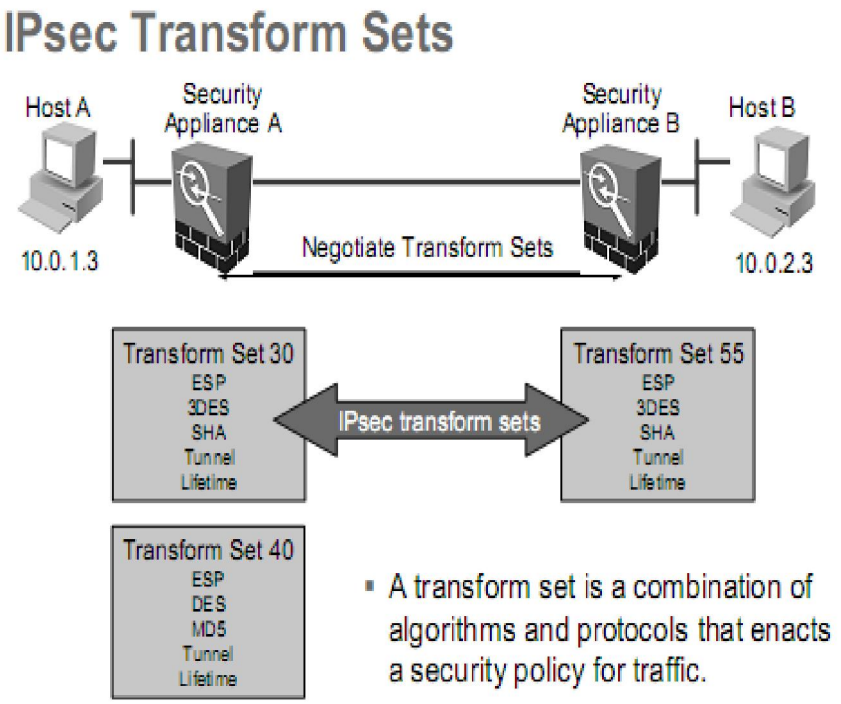
Parameter	Weak	Stronger
Encryption algorithm	DES	3DES or AES
Hash algorithm	MD5	SHA-1
Authentication method	Pre-share	RSA Signature
Key exchange	DH group 1	DH Group 5
IKE SA lifetime	86,4000 seconds	<86,400 seconds

Hình 36 – So sánh chuẩn mã hóa, thuật toán băm, phương thức chứng thực…



Hình 37 – Các bước đàm phán giai đoạn 1

***Bước 3 - IKE Phase 2*:** thỏa thuận tham số bảo mật IPSec (IPSec security parameter) để bảo mật đường hầm IPSec (IPSec tunnel), thành lập IPSec SA, định kỳ đàm phán IPSec SA bảo đảm bảo mật, tạo khóa mới cho quá trình truyền dữ liệu (optional).

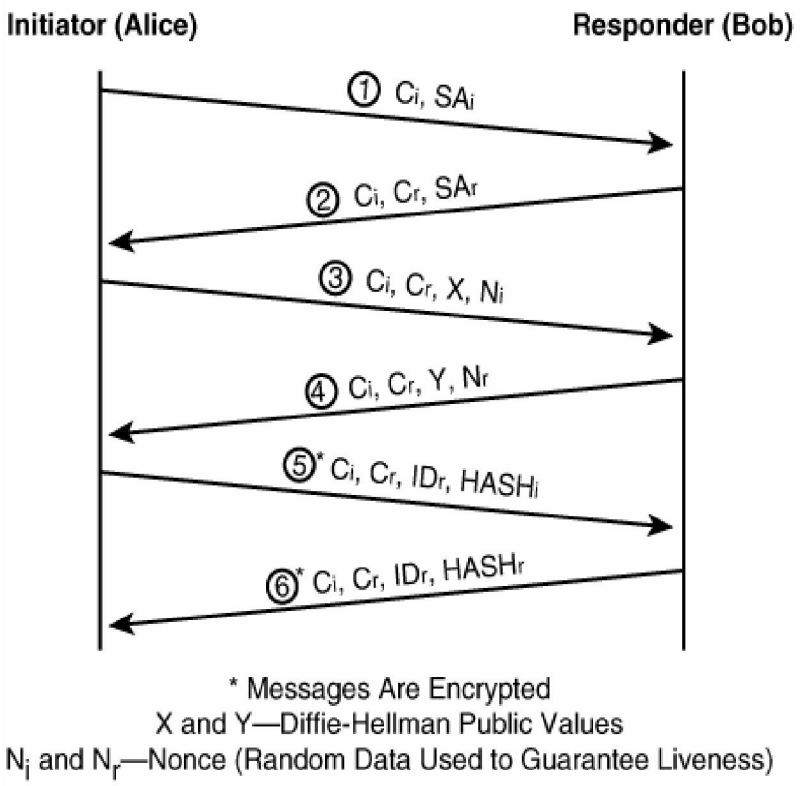


Hình 38 – Đối chiếu các tham số bảo mật

Bước 4 - Data transfer: dữ liệu được truyền giữa 2 peer.

Bước 5 - IPSec tunnel termination: IPSec SA bị xóa hoặc time out.

- **Hoạt động cụ thể**
  - ***Đối với IKE phase 1***
    - ✓ **Pre-shared key**
      - **Với Main Mode**



Hình 39 – IKE giai đoạn 1 sử dụng Pre-shared key trong main mode

Bước (1) Initiator gửi gói ISAKMP có header chứa cookie Ci và policy SAi được định nghĩa trước (phương thức xác thực, thuật toán mã hóa, thuật toán băm, DH, lifetime…)

Bước (2) Responder gửi trả lại gói ISAKMP chứa cookie Ci nhận được kèm theo cookie Cr và SAr. SAr được lựa chọn trong số những chính sách đã được cấu hình mà phù hợp với SAi, nếu tất cả đều không phù hợp thì Responder gửi lại gói tin từ chối.

Bước (3) và (4) xây dựng khóa bí mật (secrect key). Sau quá trình này sinh ra bốn khóa. SKEYID (Shared Key ID) và K được dùng để sinh ra ba khóa còn lại:

SKEYID = hash (Pre-Shared Key, Ni|Nr)

SKEYIDd= hashfunc (SKEYID, K|CI|CR|0)

SKEYIDa hashfunc (SKEYID, SKEYIDd|K|CI|CR|1)

SKEYIDe = hashfunc (SKEYID, SKEYIDa|K|CI|CR|2). Qua hàm hashfunc (key, data) nên khóa được tạo ra là hoàn toàn khác nhau.

SKEYIDd được dùng để sinh ra thêm những khóa khác dùng cho giai đoạn 2 (nếu cần).

SKEYIDa được dùng cho quá trình Integrity của ISAKMP message.

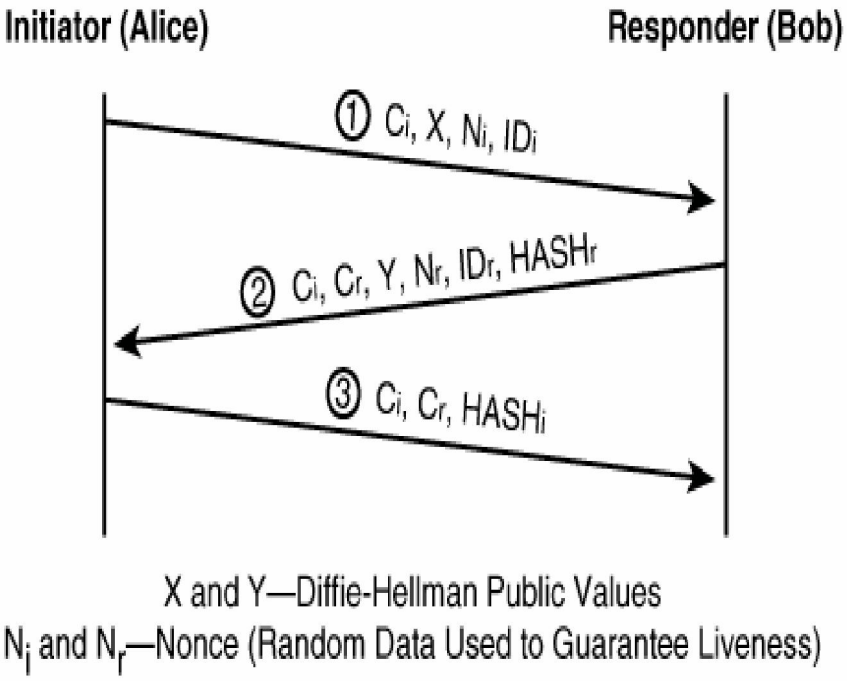
SKEYIDe dùng để encrypt IKE message.

Bước (5) và (6) gói tin mã hóa bằng SKEYIDe, xác thực, kiểm tra toàn vẹn bằng hàm băm:

HASHi = hash (SKEYID, X|Y|Ci|Cr|SAr|IDi)

HASHr = hash (SKEYID, X|Y|Cr|Ci|SAi|IDr)

- ✓ **Với Aggressive Mode**



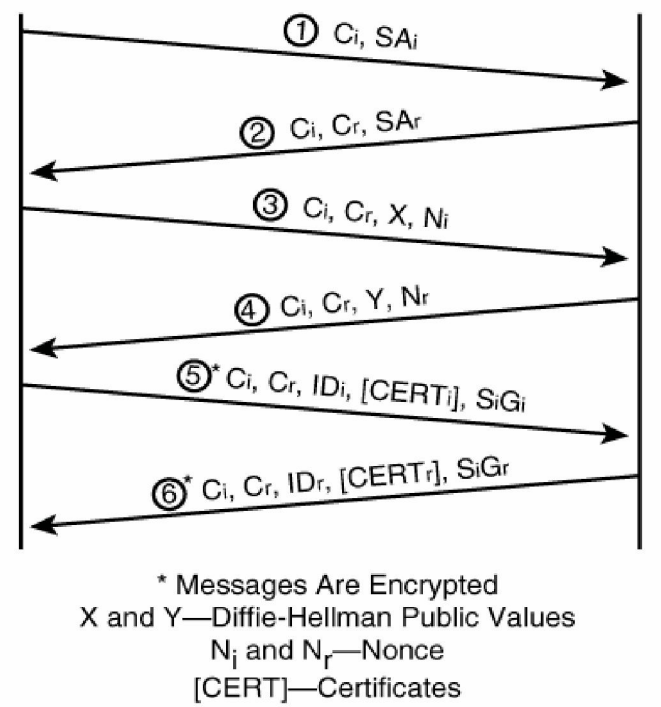
Hình 40 – IKE giai đoạn 1 sử dụng Pre-shared key trong aggressive mode

Bước (1) Initiator gửi gói ISAKMP chứa Ci, giá trị public X của DH… cho Responder.

Bước (2) nhận được X, responder có thể nhanh chóng tìm ra bốn khóa cần thiết: khóa, SKEYIDa, SKEYIDe, SKEYIDd. Sau đó toàn bộ cookie, Y, hash… gửi lại cho Initiator.

Bước (3) Initiator gửi giá trị băm cùng cookie lại cho Responder hoàn tất quá trình xác thực.

- ✓ **Digital Signature**
  - o **Với Main Mode**



Hình 41 – IKE giai đoạn 1 sử dụng Digital Signature trong main mode

Giống Pre-shared key, chỉ khác ở bước (5) và (6). Giá trị ngẫu nhiên được băm và mã hóa bằng khóa riêng tư (private key) của chính mình, đính kèm cùng chứng nhận (certificate) gửi đi. Với SIG được tính như sau:

SIGi= PRIVATEKEY_i (HASHi)

SIGr = PRIVATEKEY_r (HASHr)

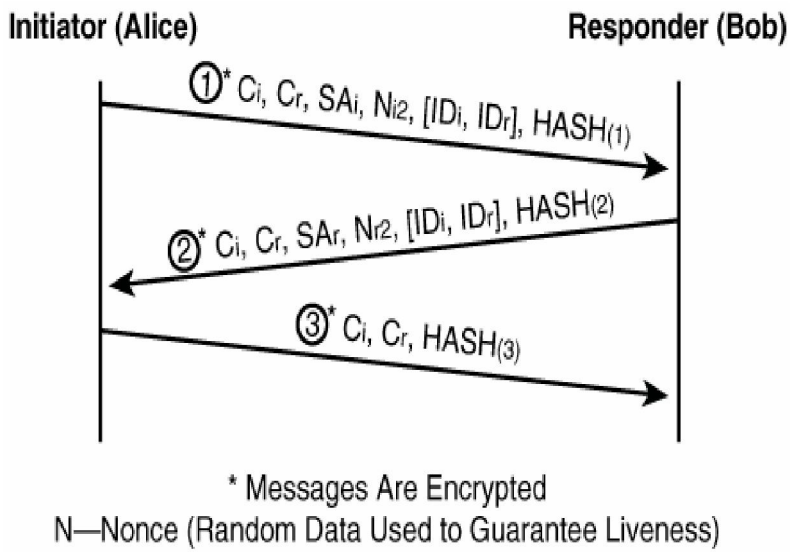
Và khác cách tính SKEYID:

SKEYID = hash (Ni|Nr|K)

Sau khi nhận được, cả hai dùng khóa công khai (public key) của đối phương giải mã chữ ký được giá trị băm, đem giá trị ngẫu nhiên nhận được đi băm, nếu hai giá trị bằng nhau thì xác thực thành công.

- ***Đối với IKE phase 2***

Sau khi thiết lập kênh bảo mật thành công, xét đến giai đoạn **IKE giai đoạn 2,** gồm ba bước:



Hình 42 – IKE giai đoạn 2

Bước (1) Initiator gửi gói tin ISAKMP chứa IPSec SA kèm theo Ni2. Giá trị N này dùng tính toán khóa mới nhằm chống lại tấn công Replay. Bình thường, tất cả khóa của IPSec đều sinh ra từ SKEYIDd của phase 1. Do đó, nếu kẻ tấn công có trình độ hiểu biết về cách DH hoạt động cũng như cơ chế sinh khóa SKEYIDd sẽ có thể tính toán ra các khóa hiện hành và những khóa dùng trong thời gian tới đến khi IKE kết thúc. Vì thế để tăng cường bảo mật, PFS (Perfect Forward Secrecy) dùng để tách biệt mối quan hệ giữa khóa cũ và mới. Nếu kích hoạt, giá trị DH (X, Y) được tính lại từ đó sinh ra khóa bí mật (secrect key) mới từ K:

HASH (1) = hash (SKEYIDa, Mid|SAi|Ni2) không có PFS

HASH (1) = hash (SKEYIDa, Mid|SAi|Ni2|X|IDi|IDr) với PFS

Bước (2) Responder gửi gói tin ISAKMP với nội dung tương tự.

HASH (2) = hash (SKEYIDa, Mid|SAr|Ni2|Nr2) không có PFS

HASH (2) = hash (SKEYIDa, Mid|SAr|Ni2|Nr2|Y|IDi|IDr) với PFS

Bước (3) Tính toán HASH (3) để kiểm tra kênh truyền trước khi thiết lập IPSec.

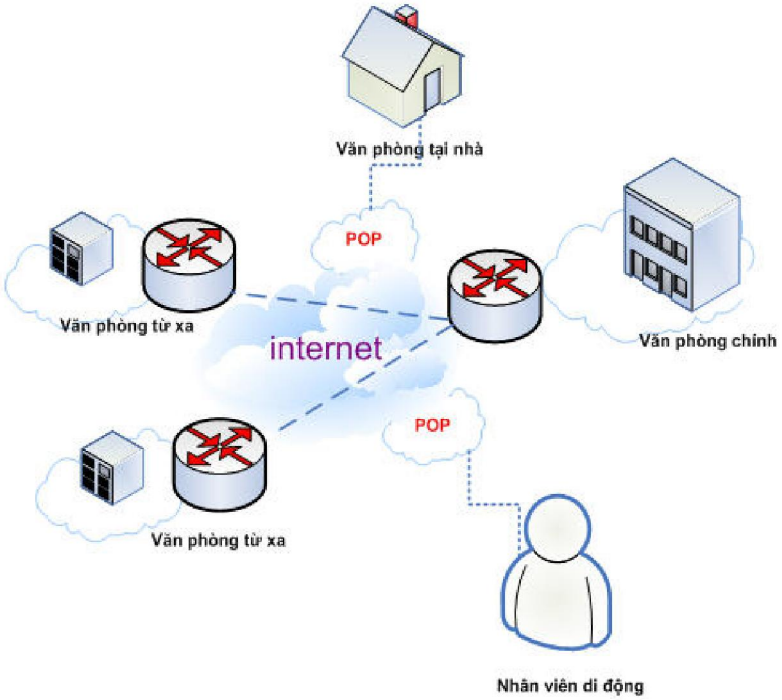
HASH (3) = hash (SKEYIDa, 0|Mid|Ni2|Nr2)

Sau khi gói tin thứ ba được gửi thì bắt đầu truyền IPSec, nếu Responder không nhận được gói tin thứ ba này thì mọi gói IPSec gửi đến đều bị bỏ đi. Để tránh trường hợp này, Responder thiết lập bit cam kết trong quá trình trao đổi gói tin thứ hai. Ở gói tin thứ ba, Responder yêu cầu thiết lập bit cam kết. Một khi xác thực được gói tin thứ ba thì Responder gửi lại thông báo cho Initiator sẵn sàng cho kết nối IPSec.

3.2.5 Các loại VPN

3.2.5.1 Easy VPN

Dựa trên cơ sở IPSec, Easy VPN không khác nhiều so với IPSec VPN. Điểm khác biệt ở chỗ các bước làm việc của client và server.



Hình 43 – Easy VPN

Sơ lượt hoạt động

- VPN client khởi tạo kết nối đến server (IKE Phase 1).
- VPN client thành lập một SA (security association) cho ISAKMP.
- VPN server chấp nhận SA do VPN client đề nghị.
- VPN server yêu cầu username và password.
- Bắt đầu quá trình cấu hình.
- Bắt đầu quá trình RRI (Reverse Route Injection - tính năng giúp cho quá trình thiết kế VPN dễ dàng hơn khi yêu cầu tính năng nâng cao như redundancy hay loadbalancing), tự động thêm các đường định tuyến tĩnh (Static Route) của Remote Client vào server. Mỗi đường này được tạo từ các thuộc tính cơ bản như Network và Netmask với next hop là điểm đầu của tunnel.
- Hoàn tất quá trình kết nối với IPSec quick mode.

Main Mode (hoạt động ở giai đoạn 1) đàm phán IKE nhằm thiết lập kênh bảo mật như ISAKMP Security Association (SA) giữa hai máy tính. ISAKMP SA bảo vệ sự thỏa thuận các tham số bảo mật. Do đó, Main Mode giúp xác định tập hợp các bộ mật mã, trao đổi khóa để thiết lập khóa bảo mật chia sẻ (shared secret key) và xác thực mỗi bên.

Quick Mode (hoạt động sau giai đoạn 1 nhưng không ở giai đoạn 2) thiết lập các thông số bảo mật (SAs) được gọi là IPSec SAs. Trong suốt Mode này, khóa luôn được tính toán lại, nếu cần thiết, có thể sinh ra khóa mới. Một bộ bảo vệ phù hợp cũng được lựa chọn. Quick Mode không được xem là sự trao đổi hoàn chỉnh bởi còn tùy thuộc vào Main Mode.

Bước 1: Người dùng gửi gói tin truy vấn đến server. Nếu pre-shared key được dùng xác thực thì IKE giai đoạn 1 hoạt động ở Aggressive Mode, các tên nhóm dùng phân biệt giữa các nhóm người sử dụng VPN. Còn nếu digital certificate được sử dụng xác thực thì IKE giai đoạn 1 hoạt động ở Main Mode, khi đó trường organization được dùng xác định nhóm.

Bước 2: Người dùng gửi các SA cho Server gồm thuật toán mã hóa, băm, phương thức xác thực và nhóm DH.

Bước 3: Sau khi nhận các SA từ client, server kiểm tra SA phù hợp theo mức độ ưu tiên cao. Sau đó, Server gửi lại cho client SA được chọn (SA được hỗ trợ trên cả client và server).

Bước 4: Hoàn tất ba bước trên, server sẽ yêu cầu client cung cấp username và password xác thực. Khi nhận được thông tin xác thực, server dùng AAA để kiểm tra thông tin xác thực này.

Bước 5: Nếu xác thực thành công, client yêu cầu các thông số cấu hình như IP address, DNS, split tunnel information… trong đó IP là bắt buộc.

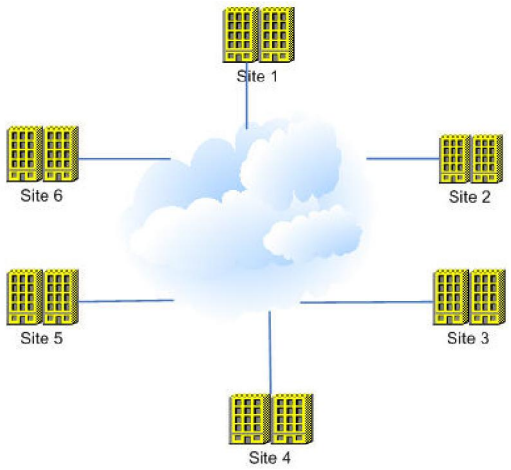
Bước6: Thực hiện quá trình RRI. Khi đó mỗi IP client được ghi nhận vào bảng Routing của server. Tính năng này được khuyến khích sử dụng khi có nhiều hơn một VPN server trong hệ thống và địa chỉ được sử dụng để cấp cho client thay vì dùng IP Pool.

Bước 7: Đến đây, IPSec SA sẽ được thiết lập sau đó VPN connect được hoàn tất.

3.2.5.2 Site to Site VPN

Việc sử dụng mật mã dành riêng cho nhiều người để kết nối nhiều điểm cố định với nhau thông qua mạng Internet, dựa trên:

- **Intranet:** nếu công ty có vài địa điểm từ xa muốn tham gia vào mạng riêng duy nhất, họ có thể tạo ra một VPN Intranet (VPN nội bộ) để nối LAN với LAN.
- **Extranet:** khi công ty có mối quan hệ mật thiết với công ty khác như đối tác cung cấp, khách hàng…họ có thể xây dựng VPN extranet (VPN mở rộng) kết nối LAN với LAN để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung.



Hình 44 – Kết nối các doanh nghiệp qua mạng công cộng

Sự kết nối hai mạng riêng lẻ thông qua đường hầm bảo mật, dùng các giao thức L2TP, hay IPsec. Mục đích chính là kết nối hai mạng lại với nhau, được thiết kế để tạo một kết nối mạng trực tiếp, hiệu quả bất chấp khoảng cách giữa chúng.

3.2.5.3 SSL VPN (hay Web VPN)

Giao thức đa mục đích tạo các giao tiếp giữa hai chương trình ứng dụng trên cổng định trước (socket 443) nhằm mã hoá toàn bộ thông tin đi và đến mà ngày nay sử dụng rộng rãi cho giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet.

Được hình thành và phát triển đầu tiên vào năm 1994 bởi nhóm nghiên cứu Netscape dẫn dắt bởi Elgammal và ngày nay trở thành chuẩn bảo mật thực hành trên mạng Internet. Phiên bản SSL hiện nay là 3.0 và vẫn đang tiếp tục được bổ sung và hoàn thiện. SSL đã kết hợp những yếu tố sau để thiết lập được một giao dịch an toàn nhằm đảm bảo:

- **Xác thực:** tính xác thực của đối tượng bạn làm việc ở đầu kia của kết nối.
- **Mã hoá:** thông tin không thể bị truy cập bởi đối tượng thứ ba. Để loại trừ việc nghe trộm thông tin "nhạy cảm" truyền qua Internet, dữ liệu phải được mã hoá để không thể bị đọc được bởi những người khác ngoài người gửi và người nhận.
- **Toàn vẹn dữ liệu:** thông tin không sai lệch, thể hiện chính xác thông tin gốc gửi đến.

Như IPSec, SSL không phải giao thức đơn lẻ mà là tập thủ tục chuẩn hoá thực hiện nhiệm vụ:

Xác thực server: Cho phép người dùng xác thực server kết nối. Lúc này, phía trình duyệt dùng kỹ thuật mã hoá công khai để chắc chắn chứng nhận và public ID của server là có giá trị và được cấp phát bởi CA (certificate authority) trong danh sách CA đáng tin cậy của người

dùng. Điều này rất quan trọng với người dùng. Ví dụ khi gửi mã số credit card qua mạng người dùng muốn kiểm tra liệu server nhận thông tin này đúng là server họ gửi đến không.

Xác thực người dùng: Cho phép phía server xác thực người dùng muốn kết nối. Phía server dùng các kỹ thuật mã hoá công khai kiểm tra chứng nhận và public ID có giá trị không và được cấp phát bởi CA (certificate authority) trong danh sách các CA đáng tin cậy của server. Điều này rất quan trọng đối với nhà cung cấp. Ví dụ khi ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ muốn kiểm tra định danh của người nhận.

Mã hoá kết nối: Tất cả thông tin trao đổi giữa client và server được mã hoá trên đường truyền để nâng cao khả năng bảo mật. Điều này rất quan trọng với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả dữ liệu gửi đi trên kết nối SSL mã hoá được bảo vệ nhờ cơ chế tự động phát hiện xáo trộn, thay đổi trong dữ liệu (đó là các thuật toán băm).

SSL bao gồm hai giao thức con:

- **SSL record:** xác định các định dạng dùng để truyền dữ liệu.
- **SSL handshake (Giao thức SSL bắt tay):** sử dụng SSL record trao đổi một số thông tin giữa server và client vào lần đầu thiết lập kết nối SSL.

Một số thuật toán được sử dụng: DES, 3DES, KEA, MD5, RSA, SHA-1…

Giao thức SSL handshake: gồm các bước:

- Người dùng sẽ gửi server số phiên bản SSL đang dùng, tham số của thuật toán mã hoá, dữ liệu tạo ra ngẫu nhiên (đó chính là chữ ký số - Digital Signature) và một số thông tin khác mà server cần để thiết lập kết nối với người dùng.
- Ngược lại, server gửi thông tin tương tự cho người dùng. Ngoài ra, còn gửi chứng nhận (certificate) của nó đến người dùng yêu cầu chứng nhận (certificate) người dùng nếu cần.
- Người dùng sử dụng thông tin server gửi đến để xác thực. Nếu server không xác thực thì người dùng sẽ cảnh báo và kết nối không thiết lập. Ngược lại, sẽ thực hiện tiếp.
- Dùng thông tin tạo ra trong giai đoạn bắt tay, người dùng (cùng sự cộng tác của server và phụ thuộc thuật toán sử dụng) tạo ra premaster secret cho phiên làm việc, mã hoá bằng khóa công khai mà server gửi đến trong chứng nhận bước 2 và gửi đến server.
- Nếu server yêu cầu xác thực người dùng thì người dùng đánh dấu vào phần thông tin riêng liên quan quá trình "bắt tay" hai bên đều biết. Khi đó, người dùng gửi cả thông tin đánh dấu và chứng nhận (certificate) cùng với premaster secret mã hoá tới server.
- Server sẽ xác thực người dùng. Trường hợp người dùng không được xác thực, phiên làm việc bị ngắt. Còn nếu người dùng xác thực thành công, server dùng khoá bí mật (private key) giải mã premaster secret, sau đó thực hiện các bước tạo ra master secret.

- Người dùng và server dùng master secret tạo ra session key - khoá đối xứng dùng mã hoá và giải mã thông tin trong phiên làm việc và kiểm tra toàn vẹn dữ liệu.
- Người dùng gửi lời nhắn đến server thông báo message tiếp theo mã hoá bằng session key. Sau đó gửi lời nhắn mã hoá thông báo người dùng kết thúc giai đoạn "bắt tay".
- Server gửi người dùng lời nhắn thông báo các message tiếp theo mã hoá bằng session key. Sau đó, nó gửi lời nhắn mã hoá thông báo server kết thúc giai đoạn "bắt tay".
- Lúc này giai đoạn "bắt tay" đã hoàn thành và phiên làm việc SSL bắt đầu. Cả hai phía người dùng và server sẽ sử dụng các session key để mã hoá và giải mã thông tin.

SSL VPN có ba mode:

- **Clientless:** Cung cấp khả năng bảo mật truy cập tài nguyên cũng như nội dung web, hữu dụng với truy cập tài nguyên, nội dung website thông qua trình duyệt, yêu cầu người dùng sử dụng Windows 2000, Windows XP hay Linux. Trình duyệt sử dụng HTTP hay HTTPS cung cấp các đường link, cho phép người dùng truy cập mạng hay website nội bộ (Internal Website) thông qua liên kết này. Với File Sharing, trình duyệt liệt kê liên kết cho phép người dùng truy cập, tạo mới, sửa xóa tài liệu... cho phép.
- **Thin client (còn gọi port-forwarding):** mở rộng khả năng mã hóa trình duyệt web, cho phép truy cập ứng dụng bằng giao thức TCP: POP3, SMTP, SSH, IMAP.
- **Tunnel mode:** sử dụng đường hầm SSL để chuyển dữ liệu ở lớp Network vì thế Tunnel Mode hỗ trợ hầu hết tất cả các ứng dụng.

So sánh:

Clientless mode	Thin mode	Tunnel mode
• Tùy trình duyệt web (clientless). • Hệ điều hành Microsoft Windows hay Linux. • Hỗ trợ Web-enabled applications, file sharing, Outlook Web Access. • Chuyển đổi IP, giao thức, phân tích và viết lại nội dung để đích đến hiểu.	• Yêu cầu TCP port forwarding. • Sử dụng Java Applet. • Mở rộng hỗ trợ ứng dụng. • Một số ứng dụng được hỗ trợ như Telnet, e-mail, SSH…	• Làm việc giống clientless IPsec VPN. • Tunnel client hoạt động trên JAVA hay ActiveX. • Hỗ trợ tất cả ứng dụng hoạt động ở lớp network. • Có khả năng mở rộng. • Cần phải có quyền admin (local) để cài đặt.

Bảng 1 – Bảng so sánh các dạng SSL VPN

Ngoài ra, để đảm bảo các máy tính người dùng đạt được các tiêu chuẩn tối thiểu đề ra trước khi thiết lập kết nối VPN, chúng tôi cần phải đề cập đến tính năng:

Endpoint Security: tập hợp tính năng nhằm bảo vệ, kiểm tra, đánh giá máy tính người dùng trước khi cho phép gia nhập hệ thống mạng. Các tính năng này hầu hết được hỗ trợ trên các thiết bị tường lửa hay đi kèm với chúng, như Checkpoint, ASA... Cài đặt trên máy tính người dùng, Cisco Secure Desktop (CSD) kiểm tra hệ điều hành (Operating System – OS), antivirus, antispy, process, registry đồng thời bảo vệ dữ liệu các phiên làm việc và cuối cùng sẽ xóa bỏ tất cả history như cookie, ULR history, page cache và những file đã download.

CSD là giải pháp tuyệt vời bảo đảm hệ thống luôn phòng ngừa tốt, nếu phát hiện người dùng có vấn đề, nó bị cách ly ngay lập tức để không ảnh hưởng hệ thống. Khi người dùng kết nối web vpn, trước khi kết nối thiết lập, CSD kiểm tra toàn bộ máy người dùng đảm bảo người dùng không bị vấn đề so với yêu cầu đặt ra.

- ***Host scan****:* kiểm tra thanh ghi (registry), CSD biết được hệ điều hành (Operating System – OS) cũng như service pack. CSD kiểm tra trình antivirus, antispyware cũng như phiên bản của chúng và cả firewall software. Tất cả thông tin lưu trữ trên ASA.
- ***Secure session:*** đảm bảo dữ liệu trong phiên làm việc Web VPN được mã hóa, không bị phân tích, khai thác, lấy cắp nếu người dùng bị chiếm quyền sử dụng hay do thám.
- ***Cache cleaner:*** xóa sạch toàn bộ dấu vết quá trình truy cập người dùng Web VPN.
- ***CSD Onscreen Keyboard (OSK):*** chống lại keylogger phần cứng hay phần mềm khi người dùng đăng nhập hay suốt quá trình dùng Web VPN. Hiện nay, có nhiều bản keylogger CSD phát hiện được. Tuy nhiên, sự phát triển của mối hiểm họa này không lường trước được. Vì thế với những phiên bản mới hơn, CSD vẫn chưa phát hiện được. Do đó, OSK sẽ là giải pháp an toàn nhất cho vấn đề này.

PHẦN 4: XÂY DỰNG IPS VÀ IDS

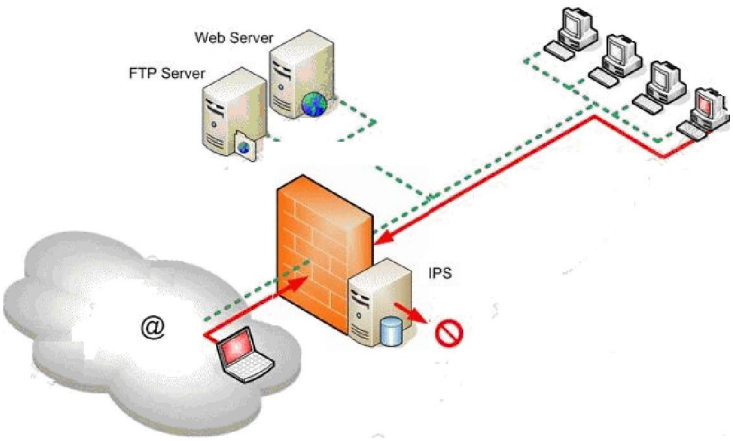
4.1 Tổng quan IDS và IPS

4.1.1 Giới thiệu

Mạng toàn cầu Internet đang phát triển với tốc độ đáng kinh ngạc trên toàn thế giới, nó thay đổi mạnh mẽ cách thức làm việc, trao đổi thông tin, giao tiếp, cuộc sống.. hầu hết các cơ quan, tổ chức, cá nhân. Cùng ưu điểm mà nó mang lại là các mối nguy hiểm ngày càng tăng về mức độ, khả năng lây lan, độ phức tạp trong phương thức tiến hành. Các mối nguy hại làm ảnh hưởng, phá hoại, sai lệch, đánh cắp thông tin, dữ liệu các thành phần hay toàn bộ mạng.

Phần mềm hay thiết bị chuyên dụng giám sát lưu lượng ra vào hệ thống mạng, phân tích dấu hiệu vi phạm chính sách bảo mật hay phát hiện và phòng chống các rủi ro tiềm ẩn, phá hoại hay các hành động như sưu tập, quét cổng đồng thời cung cấp thông tin nhận biết hành động bất thường và đưa ra cảnh báo cho nhà quản trị.

Đây là kỹ thuật an ninh mới, kết hợp ưu điểm tường lửa với hệ thống phát hiện xâm nhập IDS (Intrusion Detection System - IDS) gọi IDPS (Intrusion Detection Prevention System). Cả IDS và IPS đều có nhiều điểm chung thế nhưng hơn hẳn IDS, IPS không đơn giản chỉ theo dõi mà còn ngăn chặn tấn công. Chúng cho phép tổ chức ưu tiên, thực hiện các bước ngăn chặn sự xâm nhập, thường đặt ở vành đai mạng, đủ khả năng bảo vệ các thiết bị trong mạng.



Hình 45 – Hệ thống IPS (Intrusion Prevention System)

IDPS chủ yếu tập trung xác định các nguy cơ xâm nhập, ghi lại thông tin, cố gắng ngăn chặn các nguy cơ xâm hại và đưa ra báo cáo cho quản trị viên mạng. Ngày nay, IDPS đã trở thành một bộ phận không thể thiếu đối với cơ sở hạ tầng an ninh của hầu hết tổ chức doanh nghiệp.

4.1.2 Lịch sử hình thành

Cách đây khoảng 25 năm, khái niệm phát hiện xâm nhập (Intrusion Detection) xuất hiện qua bài báo của James Anderson. Khi đó IDS phát triển với mục đích theo dõi và nghiên cứu hành vi và thái độ bất thường của người dùng nhằm giám sát tài sản hệ thống mạng, nghiên cứu chính thức từ 1983 đến 1988 trước khi dùng trong hệ thống mạng không lực Hoa Kỳ.

Đến năm 1996, các khái niệm IDS vẫn chưa được phổ biến, hầu hết chỉ xuất hiện trong các phòng thí nghiệm và viện nghiên cứu. Tuy nhiên, một số công nghệ IDS đã bắt đầu phát triển dựa trên sự bùng nổ của công nghệ thông tin.

Đến năm 1997, IDS mới được biết đến rộng rãi và thực sự đem lại lợi nhuận với sự đi đầu của công ty ISS. Một năm sau đó, Cisco nhận ra tầm quan trọng của IDS và đã mua lại công ty Wheel – chuyên cung cấp giải pháp IDS.

Vào năm 2003, IPS –thế hệ sau của IDS – ra đời và sau đó phổ biến rộng rãi. Hiện tại, IDS/IPS vẫn là một trong các công nghệ an ninh được sử dụng phổ biến nhất trên thế giới.

4.1.3 Nguyên nhân ra đời

Việc quản trị và vận hành hệ thống IDS ngày càng khó khăn, tốn kém và không đem lại hiệu quả. Đó là nhận định của hầu hết tổ chức doanh nghiệp bấy giờ. Vào năm 2003, Gartner - công ty hàng đầu trong lĩnh vực nghiên cứu và phân tích thị trường công nghệ thông tin trên toàn cầu - đã đưa ra dự đoán gây chấn động trong lĩnh vực bảo mật: "Hệ thống phát hiện xâm nhập (IDS) sẽ không còn nữa vào năm 2005". Phát biểu này xuất phát từ một số kết quả phân tích và đánh giá cho thấy hệ thống IDS đang phải đối mặt với các vấn đề:

- Thường xuyên đưa ra nhiều báo động giả (False Positives).
- Gánh nặng cho quản trị an ninh hệ thống bởi IDS cần được theo dõi liên tục.
- Kèm theo các cảnh báo tấn công là một quy trình xử lý an ninh rất vất vả.
- Không thể theo dõi các luồng dữ liệu được truyền với tốc độ lớn hơn 600 Mbit/s.

Nhìn chung, Gartner đưa ra nhận xét này dựa trên nhiều phản ánh của khách hàng đang sử dụng IDS rằng việc quản trị và vận hành hệ thống IDS rất khó khăn, tốn kém và không đem lại hiệu quả tương xứng so với đầu tư.

Tuy nhiên, một số ý kiến phản đối cho rằng, việc hệ thống IDS không đem lại hiệu quả như mong muốn là do các vấn đề tồn tại trong việc quản lý và vận hành chứ không phải do bản chất công nghệ kiểm soát và phân tích gói tin của IDS. Cụ thể, để hệ thống IDS hoạt động hiệu quả, vai trò công cụ, con người quản trị rất quan trọng, cần đáp ứng được các tiêu chí:

- Thu thập và đánh giá tương quan tất cả các sự kiện an ninh được phát hiện bởi các IDS, tường lửa để tránh các báo động giả.
- Các thành phần quản trị phải tự động hoạt động và phân tích.
- Kết hợp với các biện pháp ngăn chặn tự động

Trước những hạn chế của hệ thống IDS, nhất là sau các cuộc tấn công ồ ạt quy mô lớn như Code Red, NIMDA, SQL Slammer, vấn đề đặt ra là làm sao tự động ngăn chặn được tấn công chứ không chỉ đưa ra cảnh báo, nhằm giảm thiểu công việc của người quản trị hệ thống. Chính những nhu cầu đó, IPS ra đời vào năm 2003 và ngay sau đó, được phổ biến rộng rãi.

Kết hợp nâng cấp thành phần quản trị, IPS dần thay thế IDS bởi nó giảm bớt các yêu cầu tác động của con người cũng như giảm bớt gánh nặng vận hành. Hơn nữa, trong một số trường hợp đặc biệt, IPS hoạt động như IDS bằng việc ngắt bỏ tính năng ngăn chặn xâm nhập.

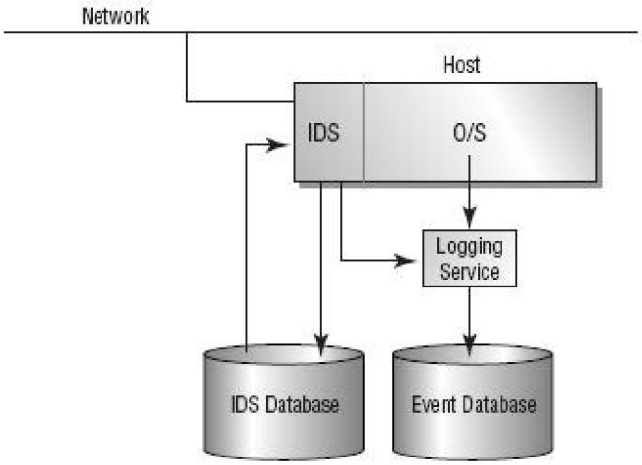
Đến năm 2005, thế hệ sau của IDS-hệ thống tự động phát hiện và ngăn chặn xâm nhập IPS-đã dần khắc phục được các mặt còn hạn chế của IDS và hoạt động hiệu quả hơn nhiều so với thế hệ trước đó. Ngày nay các hệ thống mạng đều hướng tới sử dụng các giải pháp IPS.

4.2 Phân loại

Chức năng chính của IPS là giám sát lưu lượng truyền tải trên mạng nhằm xác định các nguy cơ xâm hại, ghi lại các thông tin cần thiết và đưa ra báo cáo đánh giá hệ thống. Tùy loại hình mạng được giám sát mà lựa chọn các dạng IPS tương ứng, gồm bốn dạng chính:

4.2.1 Host-based Intrusion Prevention System (HIPS)

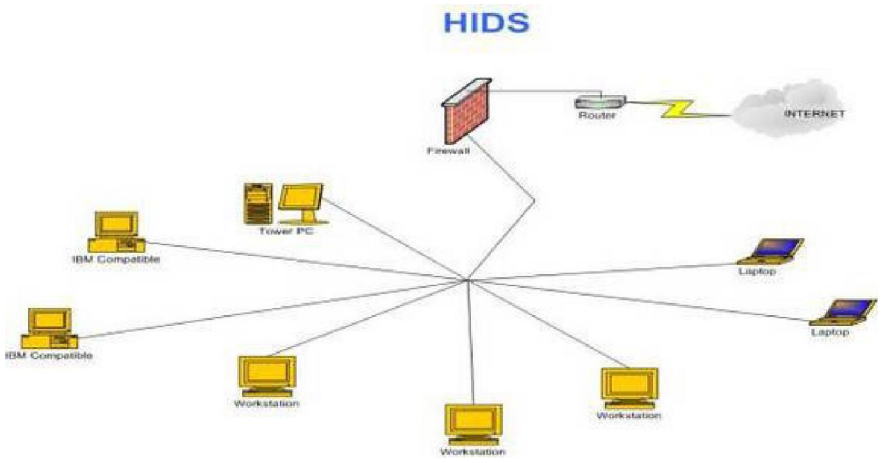
Giám sát và ghi lại toàn bộ khả năng máy trạm (gồm cả hệ điều hành và ứng dụng cũng như toàn bộ dịch vụ). Đây là thiết bị bảo mật phát hiện các tấn công trực tiếp tới máy trạm.



Hình 46 – Hệ thống HIPS

HIPS triển khai dựa trên HIDS (Host-based Intrusion Prevention) - phát triển từ đầu những năm 1980. Ngày nay, HIPS là một trong những công cụ mạnh mẽ chống tấn công và bảo vệ máy trạm hiệu quả. HIPS phân tích file nhật kí (audit logs) giám sát hệ thống, các sự kiện, bản ghi nhận bảo mật (security logs) trên Windows NT và syslog trong Unix. Ngoài ra, HIPS còn can thiệp cuộc gọi hệ điều hành và ứng dụng, bảo mật hệ điều hành và cấu hình ứng dụng, xác nhận yêu cầu dịch vụ đến, phân tích file nhật ký nội bộ cho hoạt động đáng ngờ. Khi phát hiện thay đổi, HIPS so sánh file nhật kí mới với dấu hiệu tấn công được cấu hình trước, nếu phù hợp HIPS tự động thông báo quản trị viên và đưa ra hành động tương ứng.

HIPS dùng các quy luật dựa trên sự kết hợp đặc điểm tấn công và kiến thức chi tiết hệ điều hành và ứng dụng trên máy chủ, giúp HIPS xác định các hoạt động bất thường, từ đó đưa ra hành động ngăn chặn thích hợp. Hơn nữa, HIPS cải thiện tính bảo mật máy chủ bằng các quy tắc kểm soát hành vi hệ điều hành, bộ vi xử lý như tràn bộ đệm, cập nhật thanh ghi (registry), cài đặt chương trình ứng dụng... Các quy chế kiểm tra lưu lượng mạng hạn chế số lượng kết nối truy cập chống tấn công Từ Chối Dịch Vụ (DoS – Denial of Service). HIPS không quan tâm vị trí máy tính trong hệ thống. Sơ đồ sau diễn tả máy tính trong mạng sử dụng HIDS:



Hình 47 – HIDS được cài đặt trên các máy tính

Hệ thống HIPS ngày nay yêu cầu phần mềm Agent phải được cài đặt trên mỗi máy để xem xét những hoat động thực thi trên nó, chống lại tấn công và thực thi những phân tích và bảo vệ phát hiện xâm nhập vào máy.

Ưu điểm

- **Xác minh sự thành công hay thất bại cuộc tấn công:** Vì HIPS chủ yếu phân tích bản ghi nhận sự kiện thực sự xảy ra trong hệ thống nên xác suất phát hiện tấn công cao hơn so với NIPS (Network-based Intrusion Prevention), ít các cảnh báo nhầm.
- **Giám sát các hoạt động hệ thống:** theo dõi người dùng và các hoạt động truy cập tập tin như thay đổi quyền trên tập tin, truy cập các dịch vụ đặc quyền của hệ thống…

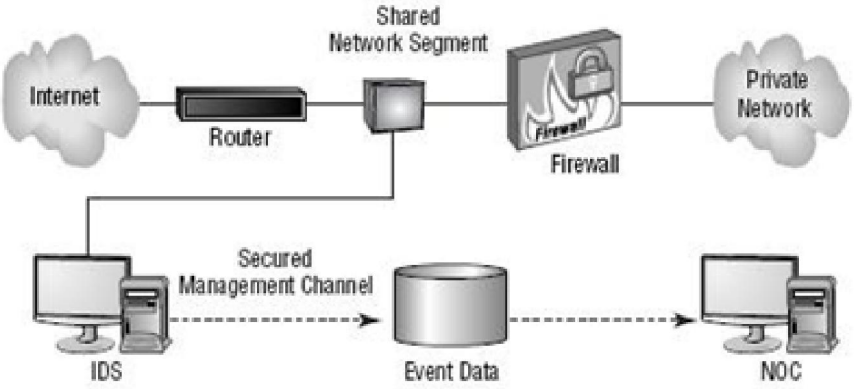
- **Thích hợp sử dụng trong môi trường mã hóa và mạng chuyển mạch:** Switch chia nhỏ mạng lớn thành phân đoạn mạng nhỏ hơn. Do đó, gây khó khăn trong xác định địa điểm tốt nhất triển khai IPS để bao phủ toàn mạng. HIPS cung cấp khả năng hiển thị lớn hơn trong mạng chuyển mạch vì HIPS cài đặt trên nhiều máy tính khác nhau trong hệ thống. Ngoài ra, HIPS cải thiện nhược điểm NIPS đối với gói tin mã hóa vì ngay khi hệ điều hành nhận thấy kết nối đến, các dòng dữ liệu đều được giải mã.
- **Không yêu cầu thêm các thiết bị phần cứng:** xây dựng trên cơ sở hạ tầng sẵn có.
- **Chi phí triển khai thấp:** so với NIPS (Network-based Intrusion Prevention).

Nhược điểm

- **Giới hạn tầm nhìn mạng:** khó xây dựng bức tranh tổng thể hệ thống mạng.
- **Yêu cầu hỗ trợ nhiều hệ điều hành:** HIPS cần chạy trên các máy trong mạng. Do đó, nó đòi hỏi hỗ trợ xác minh cho các hệ điều hành khác nhau dùng trong mạng.

4.2.2 Network-based Intrusion Prevention (NIPS)

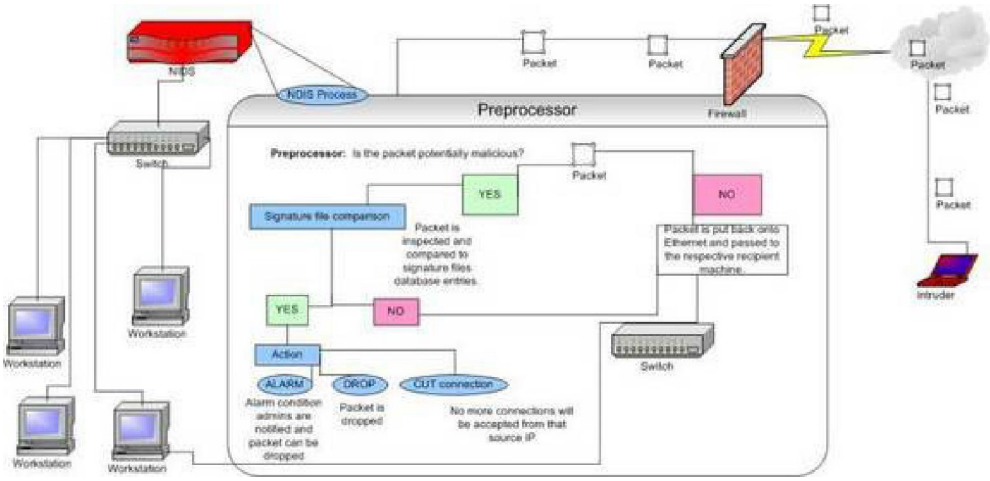
Kiểm tra các cổng giao tiếp trên mạng với thời gian thực (real-time), quét header các gói tin, và kiểm tra nội dung các gói đó để phát hiện các đoạn mã nguy hiểm hay dạng tấn công khác nhau. NIPS hoạt động tin cậy trong việc phát hiện các dạng tấn công trên hệ thống mạng.



Hình 48 – Hệ thống NIPS

NIPS sử dụng các thiết bị theo dõi, cảm biến (sensor) trên toàn mạng nắm bắt và phân tích lưu lượng ra vào hệ thống nhằm phát hiện hoạt động nguy hiểm và xâm nhập trái phép mà đưa ra các hành động phù hợp. Các cảm biến này được triển khai tại các điểm mạng cho phép nhà quản trị giám sát hoạt động mạng, bất kể vị trí mục tiêu tấn công, thường điều chỉnh phân tích phòng chống xâm nhập. Các hệ điều hành cơ bản cài đặt phần mềm IPS cần tắt các dịch vụ mạng không cần thiết và bảo mật các dịch vụ thiết yếu. Về phần cứng gồm thiết bị sau:

- **Card mạng (NIC – Network Interface Card):** NIPS phải có khả năng kết nối với bất kỳ mạng nào (Ethernet, Fast Ethernet, Gigabit Ethernet).
- **Bộ xử lý:** Quá trình phòng chống xâm nhập đòi hỏi sức mạnh của CPU thực hiện phân tích phát hiện xâm nhập và so khớp các dấu hiệu tấn công được cấu hình trước.
- **Bộ nhớ:** trực tiếp ảnh hưởng đến khả năng của NIPS trong việc phát hiện tấn công.



Hình 49 – Hoạt động của NIPS

Bất kể sự mở rộng của hệ thống mạng, các máy tính có thể được thêm vào mạng mà không cần cài thêm bất kì cảm biến nào. Các bộ cảm ứng được yêu cầu chỉ khi hiệu suất của các cảm biến không đáp ứng được nhu cầu hiện tại, khi có bất kì thay đổi nào trong chính sách bảo mật hay mô hình hệ thống mạng đòi hỏi bổ sung các cảm biến.

Ưu điểm

- Dễ dàng nhận thấy các cuộc tấn công đang diễn ra trên toàn bộ mạng.
- Không cần triển khai IDS trên tất cả máy tính trong hệ thống, không phụ thuộc hệ điều hành máy chủ.

Nhược điểm

- Không nhận biết được các luồng thông tin mã hóa.
- Khó xác định vị trí đặt NIPS sao cho nắm bắt tất cả lưu lượng mạng nhất là khi mạng trở nên lớn hơn. Để giải quyết vấn đề này, đòi hỏi sử dụng thêm các cảm biến, tuy nhiên, giải pháp này làm phát sinh thêm chi phí triển khai.

Nhìn chung, HIPS và NIPS đều có thuận lợi cũng như khó khăn khác nhau. Việc lựa chọn tùy mô hình triển khai. Nếu HIDS cho giải pháp hoàn hảo đối với máy trạm thì NIDS bảo vệ mạng LAN hiệu quả. Việc quản lý HIDS yêu cầu ít kiến thức chuyên sâu, còn NIDS yêu cầu nhiều sự quan tâm của nhà quản trị. Sau đây là bảng so sánh chức năng hai hệ thống trên:

Chức năng	**HIDS**	**NIDS**	**Đánh giá**
Bảo vệ trong mạng LAN	****	****	Cả hai đều bảo vệ trong mạng LAN
Bảo vệ ngoài mạng LAN	****	-	Chỉ có HIDS
Dễ dàng quản trị	****	****	Tương đương nhau xét về bối cảnh quản trị chung
Tính linh hoạt	****	**	HIDS là hệ thống linh hoạt hơn
Giá thành	***	*	HIDS tiết kiệm hơn
Dễ dàng bổ sung	****	****	Cả hai tương đương nhau
Đào tạo ngắn hạn cần thiết	****	**	HIDS yêu cầu đào tạo ít hơn NIDS
Tổng giá thành	***	**	HIDS tiêu tốn của bạn ít hơn
Băng tần yêu cầu trong LAN	0	2	NIDS sử dụng băng tần LAN rộng, còn HIDS thì không
Network overhead	1	2	NIDS cần hai yêu cầu băng tần mạng đối với bất kỳ mạng LAN nào
Băng tần yêu cầu (Internet)	**	**	Cả hai đều cần băng tần Internet để cập nhật kịp thời các file mẫu
Các yêu cầu về cổng mở rộng	-	****	NIDS yêu cầu kích hoạt mở rộng cổng để đảm bảo lưu lượng LAN được quét
Chu kỳ nâng cấp cho người dùng	****	-	HIDS nâng cấp tất cả người dùng với file mẫu trung tâm
Khả năng thích nghi trong các nền ứng dụng	**	****	NIDS có khả năng thích nghi trong các nền ứng dụng hơn
Chế độ quét thanh ghi cục bộ	****	-	HIDS mới thực hiện kiểu quét này
Bản ghi	***	***	Cả hai đều có chức năng bản ghi
Chức năng cảnh báo	***	***	Cả hai đều có chức năng cảnh báo từng cá nhân và quản trị viên

Quét PAN	****	-	HIDS mới quét vùng mạng cá nhân
Loại bỏ gói tin	-	****	NIDS mới có phương thức này
Kiến thức chuyên môn	***	****	Cần nhiều kiến thức chuyên môn khi cài đặt và sử dụng NIDS với toàn bộ vấn đề bảo mật mạng
Quản lý tập trung	**	***	NIDS có chiếm ưu thế hơn
Vô hiệu hóa các hệ số rủi ro	*	****	NIDS có hệ số rủi ro nhiều hơn HIDS
Khả năng cập nhật	***	***	Nâng cấp phần mềm dễ hơn phần cứng, thông qua script tập trung
Các nút phát hiện nhiều đoạn mạng LAN	****	**	Phát hiện nhiều đoạn mạng toàn diện hơn

Bảng 2 – Bảng so sánh các chức năng của HIPS và NIPS

Ngoài ra, IPS còn dược triển khai trên các hệ thống mạng sau:

Wireless Intrusion Prevention System (WIPS): phân tích hoạt động các giao thức mạng không dây, nhằm phát hiện các luồng thông tin khả nghi ra vào mạng không dây.

Network Behavior Analysis (NBA): giám sát giao thông mạng xác định các rủi ro tiềm ẩn phát sinh lưu lượng mạng bất thường như DDoS, các dạng malware và xâm phạm chính sách.

Perimeter Intrusion Detection System (PIDS): Phát hiện và chỉ ra vị trí nỗ lực xâm nhập hàng rào biên giới quanh cơ sở hạ tầng quan trọng. Sử dụng cáp quang, PIDS phát hiện rối loạn trên hàng rào, tín hiệu này được theo dõi, kích hoạt cảnh báo khi phát hiện xâm nhập.

VM based Intrusion Detection System (VMIDS): phát hiện xâm nhập nhờ giám sát trên máy ảo. Nhờ đó, triển khai hệ thống phát hiện xâm phạm với Virtual Machine Monitoring. Đây là một trong những phát minh gần đây còn trong giai đoạn nghiên cứu. Không cần xây dựng hệ thống IDS riêng biệt nào, chúng tôi vẫn giám sát được tổng thể hệ thống mạng.

4.3 Nguyên lý hoạt động của hệ thống

Hệ thống IPS thành công nếu đủ yếu tố: thực hiện nhanh, chính xác, đưa ra thông báo hợp lý, phân tích toàn bộ thông lượng, cảm biến tối đa, ngăn chặn thành công và chính sách quản lý mềm dẻo, gồm ba module chính:

4.3.1 Phân tích luồng dữ liệu

Lấy các gói tin đi đến mạng để phân tích, thông thường các gói tin có địa chỉ không phải của card mạng thì sẽ bị card mạng đó hủy bỏ nhưng card mạng IPS đặt ở chế độ thu nhận tất cả. Tất cả gói tin qua chúng được sao chép, xử lý, phân tích đến từng trường thông tin. Bộ phân tích đọc thông tin từng trường trong gói tin, xác định chúng thuộc gói tin nào, dịch vụ gì... Các thông tin này được chuyển đến module phát hiện tấn công.

4.3.2 Phát hiện tấn công

Module quan trọng nhất phát hiện các cuộc tấn công, bao gồm ba phương pháp theo dõi là:

4.3.2.1 Dấu hiệu tấn công (Signature-based Detection hay Misuse Detection)

Tập nguyên tắc sử dụng xác định những hoạt động xâm nhập thông thường, phân tích hoạt động của hệ thống, theo dõi sự kiện và so sánh với mẫu tấn công đã được cấu hình trước:

- ***Dựa trên sự khai thác (exploit-based signature):*** phát hiện công cụ dò tìm lỗ hỏng như đoán password, kịch bản shell tự động tấn công hay thực hiện thủ tục đơn giản tìm kiếm lỗ hỏng hệ thống cũng như đoạn mã thực thi…
- ***Dựa trên các lỗ hỏng chương trình (vulnerability-based signature):*** phân tích lỗ hỏng thực thi chương trình ứng dụng, rủi ro gây hại bảo mật hay chức năng hệ thống như password yếu, xử lý đầu vào không mong muốn hay truyền dẫn không bảo mật…

Việc tạo ra Signature-Based yêu cầu người quản trị các kỹ năng hiểu biết thật rõ về loại hình tấn công, mối nguy hại và phát triển dấu hiệu dò tìm. Khi nhiều phương pháp tấn công và khai thác được khám phá, nhà sản xuất IPS phải cung cấp những bản cập nhật file dấu hiệu.

Nếu có những lưu lượng trùng khớp bất kì dấu hiệu tấn công nào, IPS dựa trên cấu hình trước đó mà đưa ra hành động thích hợp, không cần tác động người dùng. Nhờ đó, phát hiện tấn công nhanh và chính xác, không đưa ra cảnh báo sai làm giảm khả năng hoạt động mạng và giúp các người quản trị xác định các lỗ hỏng bảo mật hệ thống. Tuy nhiên, phương pháp này có nhược điểm là không phát hiện được các cuộc tấn công không có trong cơ sở dữ liệu, các kiểu tấn công mới, do vậy hệ thống luôn phải cập nhật các mẫu tấn công mới.

Lợi ích

- **Ít cảnh báo nhầm:** Những dấu hiệu dựa trên hiểu biết về hoạt động xâm nhập nên xác suất phát hiện tấn công cao.
- **Hệ thống dễ hiểu:** dễ dàng điều chỉnh hành động phù hợp với bất kì tín hiêu cảnh báo nào. Ngoài ra, cũng có thể bật dấu hiệu lên tiến hành kiểm tra toàn mạng.
- **Các tấn công mới cập nhật thường xuyên:** dấu hiệu thay đổi liên tục sau khi cài đặt.

Hạn chế

- **Không thể phát hiện những cuộc tấn công mới hay chưa được biết (false negative):** Do hoạt động dựa trên các mẫu dấu hiệu đã định nghĩa trước, gây khó khăn trong việc nhận ra đợt tấn công mới chưa từng biết hay khám phá trước đây.
- **Không thể phát hiện sự thay đổi những cuộc tấn công đã biết:** Những file dấu hiệu là những file tĩnh do đó không thích nghi với vài hệ thống. Nếu thay đổi cách tấn công, kẻ tấn công có thể xâm nhập mà không bị phát hiện (false negative).
- **Khả năng quản trị cơ sở dữ liệu những dấu hiệu:** Việc bảo đảm cơ sở dữ liệu dấu hiệu luôn cập nhật và hiện hành cần phải đầu tư nhiều thời gian và tiền bạc.
- **Dung lượng bộ nhớ của bộ cảm biến còn hạn chế:** duy trì tình trạng thông tin để nhanh chóng tìm kiếm thông tin. Bộ cảm biến lưu trạng thái thông tin trong bộ nhớ.

4.3.2.2 Dấu hiệu bất thường (Statistical Anomaly-based Detection)

Kỹ thuật dò thông minh, nhận dạng hành động bất thường. Ban đầu, IPS lưu trữ bảng mô tả sơ lược nhóm người dùng hay hoạt động bình thường hệ thống (như phân quyền các nhóm sử dụng theo các hoạt động và nguồn tài nguyên; web server phải có bảng mô tả sơ lược hoạt động của nó dựa trên lưu lượng web, tương tự đối với mail server…). Càng nhiều bảng mô tả sơ lược khác nhau cho mỗi dạng dịch vụ, hệ thống IPS càng đưa ra được các cảnh báo đúng. Sau đó, so sánh với các lưu lượng ra vào hệ thống và nhận dạng hoạt động nào là khác thường, có thể gây hại hệ thống, gồm một số kỹ thuật sau:

- ***Phát hiện mức ngưỡng:*** nhấn mạnh việc vượt quá mức ngưỡng được đặt ra đối với các hoạt động bình thường như đăng nhập với số lần quá quy định, số lượng các tiến trình hoạt động trên CPU, số lượng một loại gói tin được gửi vượt quá mức... thì hệ thống sẽ coi đó là các hoạt động nguy hại.
- ***Phát hiện nhờ quá trình tự học:*** gồm hai bước. Khi bắt đầu thiết lập, hệ thống phát hiện tấn công sẽ chạy ở chế độ tự học và tạo ra một hồ sơ về cách cư xử của mạng với các hoạt động bình thường. Sau thời gian khởi tạo, hệ thống sẽ chạy ở chế độ làm việc, tiến hành theo dõi, phát hiện các hoạt động bất thường của mạng bằng cách so sánh với hồ sơ đã thiết lập. Chế độ tự học có thể chạy song song với chế độ làm việc để cập nhật hồ sơ của mình nhưng nếu dò ra có tín hiệu tấn công thì chế độ tự học phải dừng lại cho tới khi cuộc tấn công kết thúc.
- ***Phát hiện sự không bình thường của các giao thức:*** căn cứ hoạt động của các giao thức, dịch vụ trong hệ thống để tìm ra các gói tin không hợp lệ, các hoạt động bất thường vốn là dấu hiệu xâm nhập, tấn công. Kỹ thuật này hiệu quả trong việc ngăn chặn các hình thức quét mạng, quét cổng để thu thập thông tin của các tin tặc.

Phương pháp này hữu hiệu trong việc phát hiện các cuộc tấn công kiểu từ chối dịch vụ, phát hiện ra các kiểu tấn công mới, cung cấp các thông tin hữu ích bổ sung cho phương pháp trên. Tuy nhiên đôi khi thường tạo ra các cảnh báo sai làm giảm hiệu suất hoạt động của mạng.

Lợi ích

- **Phát hiện kẻ tấn công bên ngoài hay kẻ trộm tài khoản một cách dễ dàng.**
- **Cải thiện những hạn chế của phương pháp theo dõi dấu hiệu tấn công:** Nếu như kẻ tấn công có thể kiểm tra thử các dấu hiệu trên hệ thống IPS mà chọn lựa cách thức cũng như công cụ tấn công phù hợp thì với phương pháp này, điều đó vô cùng khóa khăn do không sử dụng những cơ sở dữ liệu dấu hiệu định dạng trước nên kẻ xâm nhập không thể biết chính xác cái gì gây ra cảnh báo.
- **Phù hợp cho việc phát hiện các cuộc tấn công mới:** không dựa trên tập những dấu hiệu được định dạng hay các đợt tấn công được biết, profile là động và sử dụng trí tuệ nhân tạo để xác định những hoạt động bình thường.

Hạn chế

- **Thời gian chuẩn bị ban đầu cao** đồng thời không có sự bảo vệ suốt thời gian khởi tạo ban đầu.
- **Khó khăn trong việc tạo ra các profile nhóm người dùng:** bảo đảm chất lượng các profile này tương đối phức tạp.
- **Thường xuyên cập nhật profile:** khi thói quen người dùng thay đổi.
- **Khó khăn trong việc định nghĩa cách hành động thông thường:** Hệ IPS chỉ thật sự tốt khi nó định nghĩa những hành động nào là bình thường. Đây là thử thách khi mà môi trường nơi công việc người dùng hay những trách nhiệm thay đổi thường xuyên.
- **Cảnh báo nhầm:** Những hệ thống dựa trên sự bất thường có xu hứng có nhiều false positive bởi vì chúng thường tìm những điều khác thường.
- **Việc định ra các profile người dùng và hoạt động hệ thống tương đối phức tạp:** Lấy mẫu thống kê, dựa trên nguyên tắc, và mạng neural là những phương cách nhằm tạo profile mà thật khó hiểu và giải thích.

4.3.2.3 Giao thức (Stateful Protocol Analysis Detection)

Như Signature-based Detection, thực hiện phân tích chiều sâu giao thức được xác định cụ thể trong gói tin. Ví dụ: Hacker bắt đầu chạy chương trình tấn công Server. Trước tiên hacker phải gửi một gói tin IP cùng với kiểu giao thức, có thể không chứa dữ liệu trong trường payload, phương thức này sẽ theo dõi các kiểu tấn công cơ bản dựa trên một số giao thức:

- Kiểm tra khả năng của giao thức để xác định gói tin đó có hợp pháp hay không.
- Kiểm tra nội dung trong Payload (pattern matching).
- Thực hiện những cảnh cáo không bình thường.

4.3.2.4 Chính sách (Policy-based IPS)

Đưa ra cảnh báo khi có những hành động vi phạm của các chính sách đã được cấu hình trước.

Lợi ích

- **Định ra chính sách riêng biệt:** thiết lập chính sách cho từng thiết bị trong hệ thống.
- **Xác thực và phản ứng nhanh:** rất ít có những cảnh báo sai.

Hạn chế

- **Đòi hỏi kinh nghiệm và kiến thức nhất định:** Việc thiết lập chính sách yêu cầu quản trị viên hệ thống phải có kinh nghiệm và kiến thức nhất định đồng thời để quản lý các chính sách này tương đối phức tạp.
- **Thường xuyên phải cấu hình lại**: khi có các thiết bị mới thêm vào hệ thống.
- **Khó khăn khi quản trị từ xa.**

4.3.3 Phản ứng

Khi có dấu hiệu tấn công hay thâm nhập, module phát hiện tấn công gửi tín hiệu đến module phản ứng. Lúc đó module phản ứng kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo người quản trị. Nếu chỉ đưa ra các cảnh báo thì hệ thống này được gọi là hệ thống phòng thủ bị động. Dưới đây là một số kỹ thuật ngăn chặn:

- ***Kết thúc tiến trình:*** gửi các gói tin phá huỷ tiến trình nghi ngờ. Tuy nhiên, thời gian can thiệp chậm hơn thời điểm tin tặc tấn công, dẫn đến tấn công xong rồi mới bắt đầu can thiệp. Ngoài ra, kỹ thuật này không hiệu quả với giao thức UDP như DNS, hơn nữa gói tin can thiệp phải có trường thứ tự đúng như gói tin trong phiên làm việc tiến trình tấn công. Nếu tiến trình tấn công xảy ra nhanh khó thực hiện phương pháp này.
- ***Huỷ bỏ tấn công:*** hủy bỏ gói tin hay chặn đường gói tin đơn, phiên làm việc hay một luồng thông tin tấn công, an toàn nhất nhưng dễ nhầm với các gói tin hợp lệ.
- ***Thay đổi các chính sách của tường lửa:*** cho phép người quản trị cấu hình lại chính sách bảo mật tấn công xảy ra. Sự cấu hình lại là tạm thời thay đổi các chính sách điều khiển truy nhập bởi người dùng đặc biệt trong khi cảnh báo tới người quản trị.

- ***Cảnh báo thời gian thực:*** Gửi các cảnh báo thời gian thực đến người quản trị để họ nắm được chi tiết các cuộc tấn công, các đặc điểm và thông tin về chúng.
- ***Ghi lại vào tệp tin:*** Các dữ liệu của các gói tin sẽ được lưu trữ trong hệ thống các tệp tin log. Mục đích để người quản trị tiện theo dõi các luồng thông tin và là nguồn thông tin giúp cho module phát hiện tấn công hoạt động.

4.4 Một số thuật ngữ liên quan

Event horizon

Để phát hiện xâm nhập, IPS kiểm tra thông tin so sánh với các dấu hiệu trong cơ sở dữ liệu. Tuy nhiên, thỉnh thoảng thông tin này trải dài qua nhiều gói dữ liệu. Khi dấu hiệu yêu cầu nhiều mảnh dữ liệu, IDS duy trì tình trạng thông tin về dấu hiệu bắt đầu khi nó thấy các mảnh dữ liệu đầu tiên. Tình trạng thông tin duy trì trong khoảng thời gian event horizon, khác nhau đối với từng dạng tấn công. Đối với vài tấn công, đây là khoảng thời gian từ lúc đăng nhập (logon) đến khi rời khỏi hệ thống (logoff), có thể kéo dài cả tuần với các dạng tấn công khác.

False negative

Khi IPS lơ là cảnh báo hành động xâm nhập. False negative miêu tả tấn công thật sự mà IPS bỏ sót khi cấu hình. Hầu hết người phát triển IPS có khuynh hướng thiết kế hệ thống tránh khỏi các false negative này. Tuy nhiên, để loại bỏ toàn bộ false negative, đòi hỏi cập nhật dấu hiệu tấn công thường xuyên, đảm bảo hệ thống luôn nhận biết các dạng tấn công mới.

False positive

Ngược lại false negative, false positive biết đến như việc đưa ra các cảnh báo khi không có bất cứ cuộc tấn công nào diễn ra. Khi IPS đưa ra quá nhiều các báo động giả, gây ảnh hưởng hiệu năng mạng. Việc hạn chế các false negative cũng như false positive luôn là mục tiêu hướng đến của hầu hết các quản trị viên khi triển khai hệ thống IPS.

True Positive

Mô tả việc IPS đưa ra cảnh báo đúng khi phát hiện tấn công hay xâm nhập trái phép vào hệ thống mạng. Đây cũng là mục tiêu hướng đến của các chuyên gia nghiên cứu phát triển IPS.

True Negative

Không đưa ra bất kì cảnh báo nào khi không có tấn công hay xâm nhập trái phép vào hệ thống mạng. Việc bảo đảm hệ thống IPS luôn hướng đến true negative và true positive là mong muốn của nhiều tổ chức doanh nghiệp. Tuy nhiên, điều này đòi hỏi đầu tư nhiều thời gian tiền bạc và sự quan tâm của các nhà quản trị.

PHẦN 5: XÂY DỰNG TƯỜNG LỬA CHO HỆ THỐNG MẠNG TRƯỜNG ĐẠI HỌC HOA SEN

5.1 Giới thiệu

Trường ĐH Hoa Sen có trụ sở chính tại trung tâm TPHCM - trung tâm năng động của Việt Nam và khu vực. hành lập vào năm 1991, giai đoạn nền kinh tế - xã hội chuyển mình hội nhập quốc tế, nhà trường xác định mục tiêu giáo dục và đào tạo thực chất, dấn thân vào thẳng nhu cầu của xã hội, bằng các trường chương trình kỹ thuật viên. Đào tạo đáp ứng nhu cầu xã hội tiếp tục được duy trì và phát triển khi Trường trở thành trường Cao đẳng vào những năm cuối thế kỷ 20. Tầm nhìn, sứ mệnh và triết lý đào tạo hình thành dựa trên giá trị cốt lõi này tiếp tục đưa đại học Hoa Sen phát triển với tư cách trường Đại học bắt đầu từ năm 2006.

5.2 Yêu cầu

Với chủ đề năm học 2010 - 2011 "Cùng nhau vươn cao hơn"nhằm hướng đến việc tăng cường hợp tác thành công hơn nữa giữa Trường ĐH Hoa Sen và các đối tác sư phạm, đối tác doanh nghiệp và xã hội. Trong năm học này nhà trường đón chào 2623 tân sinh viên, do đó, nhằm thỏa mãn nhu cầu học tập cũng như nâng cao hiệu quả làm việc, nhà trường quyết định nâng cấp toàn bộ hệ thống mạng tại các cơ sở hoạt động:

- Xây dựng hệ thống mạng nội bộ gồm phòng làm việc, phòng lab cho sinh viên, cung cấp kết nối Wireless giúp sinh viên tra cứu tài nguyên mạng ngoài giờ học ở trường.
- Cần bảo đảm an toàn thông tin, chống sự xâm nhập hệ thống trái phép bằng việc triển khai hệ thống tường lửa, giải pháp VPN giúp truy cập từ xa giữa các cở sở đồng thời theo dõi và ghi nhận các cuộc tấn công qua IDS/IPS.
- Cung cấp hệ thống dự phòng cho tường lửa khi gặp sự cố, phân chia việc kiểm tra các luồng thông tin qua tường lửa, tân dụng tối đa hiệu suất hoạt động tường lửa đồng thời cân bằng tải kết nối ra Internet nhằm đảm bảo hệ thống hoạt động tốt và liên tục.

Các yêu cầu cụ thể đối với từng phòng ban:

<table>
<tr><th>Thời Gian Làm Việc</th><th>Phòng Ban</th><th>Đối Tượng Truy cập</th><th>Yêu cầu cụ thể</th></tr>
<tr><td rowspan="4">8h30 đến 11h30
13h đến 17h</td><td>Giáo viên</td><td rowspan="4">Nhân viên</td><td rowspan="4">• Cho phép truy cập Web, File Server và gửi mail.
• Chia sẻ file giữa các phòng ban.</td></tr>
<tr><td>Đào Tạo</td></tr>
<tr><td>Tuyển Sinh</td></tr>
<tr><td>Kế Toán – Tài Chính</td></tr>
<tr><td rowspan="3">6h30 đến 12h
13h đến 17h30</td><td>Lab (cho tất cả sinh viên)</td><td rowspan="4">Sinh viên</td><td>• Không cho phép truy cập Internet.</td></tr>
<tr><td>Lab Thực Hành Mạng</td><td>• Cho phép truy cập Internet, mail và các dịch vụ khác giúp sinh viên thực hành thiết kế hệ thống.</td></tr>
<tr><td>Thư viện</td><td rowspan="2">• Chỉ cho phép truy cập Web.</td></tr>
<tr><td>10h đến 14h</td><td>Internet</td></tr>
<tr><td rowspan="3">6h30 đến 17h30</td><td rowspan="3">Wireless</td><td>Sinh viên</td><td rowspan="3">• Cho phép truy cập Internet</td></tr>
<tr><td>Nhân viên</td></tr>
<tr><td>Khách mời</td></tr>
</table>

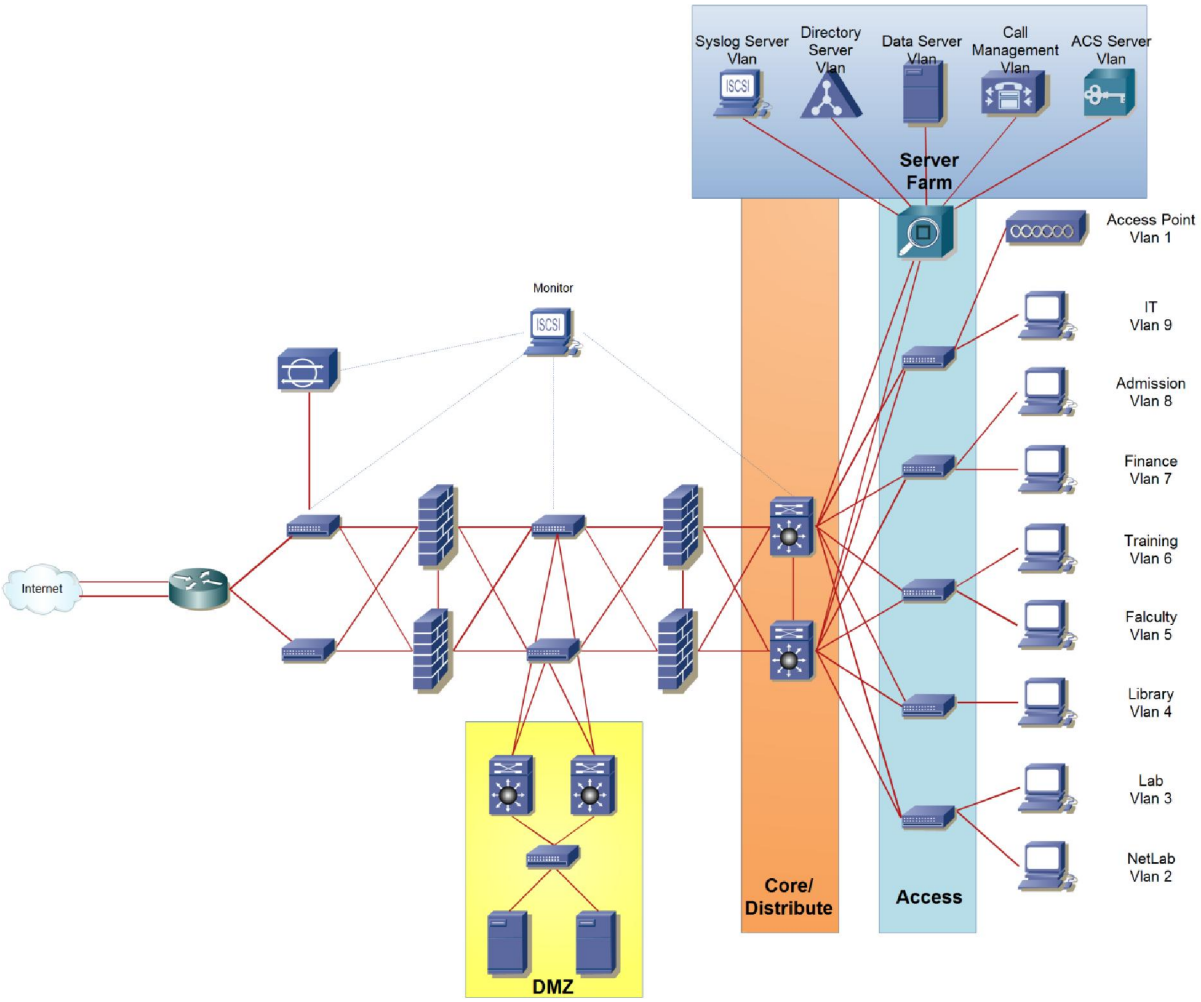
Bảng 3 – Bảng yêu cầu đối với các phòng ban

5.3 Triển khai

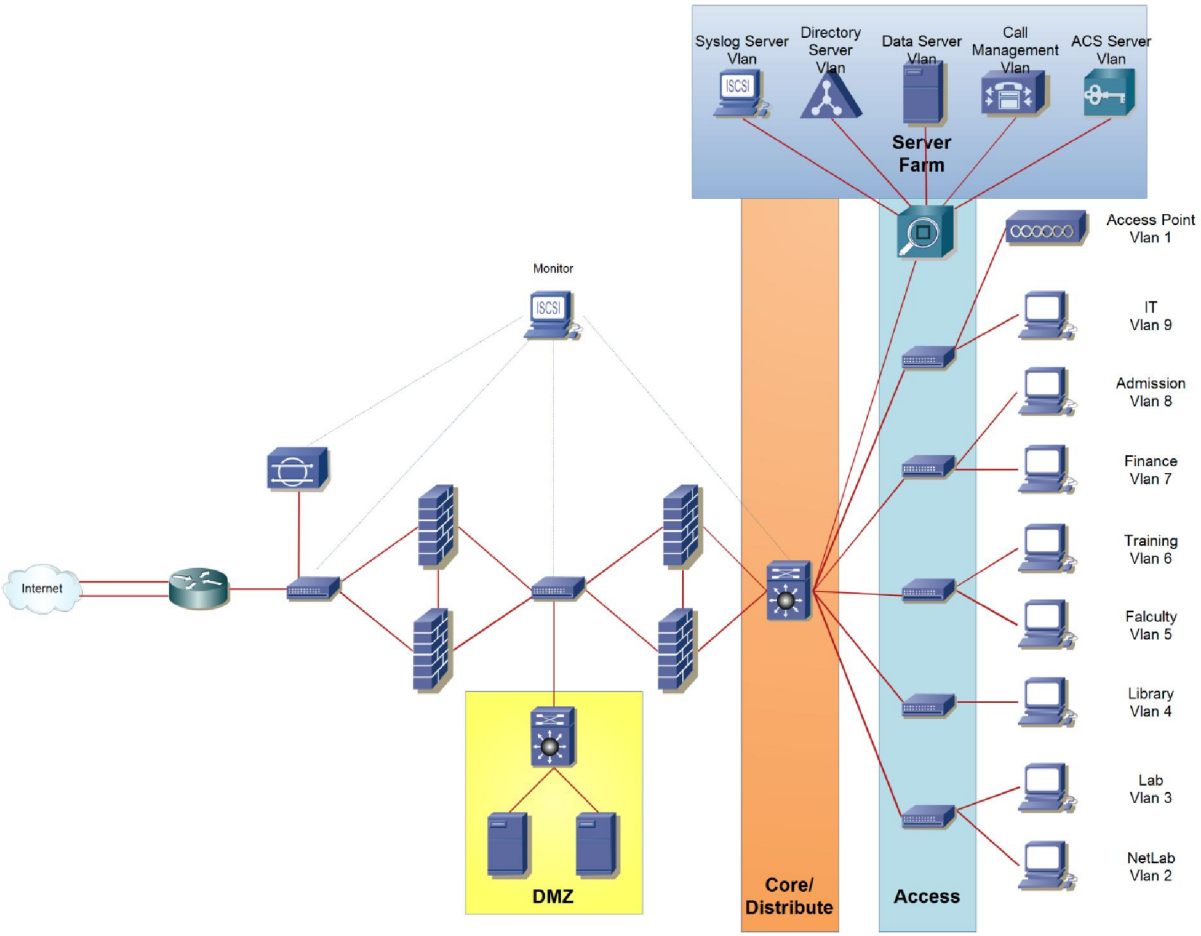
5.3.1 Sơ đồ hệ thống mạng tại trụ sở chính

5.3.1.1 Mô hình mạng

Dựa trên các mẫu kiến trúc tường lửa trên, chúng tôi quyết định triển khai hệ thống tường lửa cho trường Đại Học Hoa Sen theo một trong hai mô hình sau:


Syslog Server Vlan
Directory Server Vlan
Data Server Vlan
Call Management Vlan
ACS Server Vlan
Server Farm
Access Point Vlan 1
IT Vlan 9
Admission Vlan 8
Finance Vlan 7
Training Vlan 6
Falculty Vlan 5
Library Vlan 4
Lab Vlan 3
NetLab Vlan 2
Monitor
Internet
DMZ
Core/ Distribute
Access

(a)



(b)

Hình 50 – Sơ đồ hệ thống mạng trường Đại Học Hoa Sen

Sự khác biệt

- **Với sơ đồ thứ nhất:** Đi kèm việc ứng dụng công nghệ dự phòng tường lửa Active/Active Failover, chúng tôi còn sử dụng HSRP (Hot Standby Router Protocol) – giải pháp ít tốn kém nhất chúng tôi lựa chọn (sẽ có giải pháp khác tối ưu hơn được đề cập trong phần Load Balancing Firewall) nhằm tận dụng tối đa tài nguyên thiết bị. Tuy khai thác hết tài nguyên hệ thống nhưng cũng mang lại một số hạn chế sau:
  - Chi phí đầu tư cao.
  - Đòi hỏi quản tri viên hệ thống mạng phải có kinh nghiệm và trình độ nhất định.
  - Quá trình triển khai cũng như quản trị tương đối phức tạp do việc sử dụng khá nhiều thiết bị (nhất là thiết bị Switch lớp 3).
- **Với sơ đồ thứ hai:** sử dụng công nghệ dự phòng tường lửa Active/Standby Failover. Cùng với việc bỏ bớt các thết bị (Switch lớp 3), chi phí đầu tư được giảm bớt đáng kể. Ngoài ra, việc triển khai theo mô hình thứ hai còn giảm bớt gánh nặng cho nhà quản

trị, không gặp những vấn đề về HSRP hay những giải pháp để loadbalancing cho firewall**.** Tuy nhiên, so với mô hình thứ nhất, mô hình này cũng mắc phải hạn chế:

- Không khai thác toàn bộ tài nguyên hệ thống (cụ thể là hai tường lửa Standby).

Theo hai sơ đồ trên, hệ thống mạng trường Đại học Hoa Sen chủ yếu gồm bốn vùng mạng chính, được sắp xếp theo độ bảo mật giảm dần:

Vùng mạng	**Lớp địa chỉ IP**	**Subnet Mask**	**Mô tả cụ thể**
Mạng bên trong (Inside Network)	172.16.x.0 (x: VLAN tương ứng)	255.255.255.0	Mạng nội bộ tin cậy. Mức độ bảo mật cao nhất (100)
Server Farm	10.0.0.0	255.255.255.0	Đặt Server quan trọng (gồm Database Server…). Mức độ bảo mật 100
Vùng Phi Quân Sự (DMZ – Demilitarized Zone)	11.0.0.0	255.255.255.0	Đặt các Server quảng bá ra Internet (gồm Web Server, Mail Server…). Mức độ bảo mật xếp sau Server Farm (50)
Mạng bên ngoài Internet (Outside Network)	Các lớp IP Public khác dãy địa chỉ trên		Mạng không tin cậy. Mức độ bảo mật thấp nhất (0)

Bảng 4 – Bảng các vùng mạng trong hệ thống trường Đại Học Hoa Sen

Ngoài ra, đối với các kết nối điểm – điểm (point - point) giữa các thiết bị, chúng tôi sử dụng lớp địa chỉ IP 193.1.0.0/16, từ trong ra ngoài được cấu hình địa chỉ IP như sau:

Thiết bị	Kết nối	Lớp địa chỉ IP	Subnet Mask
Cặp tường lửa bên trong (Inside firewall)	Switch lớp 3 với Active Firewall	193.1.1.0	255.255.255.0
	Switch lớp 3 với Standby Firewall (cặp Firewall Inside)	193.1.2.0	255.255.255.0
Giữa hai cặp tường lửa trong và ngoài (Inside & Outside)	Giữa hai cặp tường lửa Active	193.1.4.0	255.255.255.0
	Giữa hai cặp tường lửa Standby	193.1.3.0	255.255.255.0
Cặp tường lửa bên ngoài (Outside firewall)	Router biên với Active Firewall (cặp firewall Outside)	193.1.5.0	255.255.255.0
	Router biên với Stanby Firewall (cặp Firewall Outside)	193.1.6.0	255.255.255.0

Bảng 5 – Lớp địa chỉ IP trên kết nối giữa các thiết bị

5.3.1.2 Xác định các nhóm người dùng

Mỗi phòng ban ứng với từng nhóm người dùng và được phân chia theo các VLAN tương ứng, bao gồm 9 phòng ban như sau:

Phòng ban	**VLAN tương ứng**	**Lớp IP tương ứng**	**Subnet Mask**	**Miêu tả cụ thể**
Access Point	1	172.16.1.0	255.255.255.0	Cung cấp mạng không dây cho khách mời, nhân viên và sinh viên
NetLab	2	172.16.2.0	255.255.255.0	Phòng lab sinh viên mạng
Lab	3	172.16.3.0	255.255.255.0	Phòng thực hành cho tất cả sinh viên
Thư viện (Library)	4	172.16.6.0	255.255.255.0	Thư viện cho sinh viên tự nghiên cứu
Giáo viên (Falculty)	5	172.16.7.0	255.255.255.0	Phòng nghỉ cho giáo viên
Đào Tạo (Training)	6	172.16.8.0	255.255.255.0	Tính toán sổ sách, đưa ra các báo cáo hoạt động
Kế Toán – Tài Chính (Finance)	7	172.16.9.0	255.255.255.0	Quản lý kết quả học tập
Tuyển sinh (Admission)	8	172.16.10.0	255.255.255.0	Cung cấp, xử lý các thông tin tuyển sinh
IT	9	172.16.11.0	255.255.255.0	Quản trị hệ thống

Bảng 6 – Bảng VLAN các phòng ban

Ngoài 9 VLAN được cấu hình trên, chúng tôi còn cấu hình thêm 2 VLAN là Restricted VLAN (được sử dụng khi người dùng đăng nhập sai) và Guest VLAN (được dùng khi cung cấp username và password trống đăng nhập hệ thống).

Ngoài ra, chúng tôi còn triển khai hệ thống thoại VOIP cho từng phòng ban. Ở đây, chúng tôi quy định định dạng số điện thoại tài khoản người dùng là ***xxxx***, trong đó:

- Hai số đầu là số cơ sở.
- Một số tiếp theo là số phòng ban.

- Một số cuối là số thứ tự người dùng.

Số thứ tự các cơ sở, phòng ban và người dùng tương ứng được quy định theo các bảng sau:

Cơ sở	Số thứ tự tương ứng
Quang Trung	11
Nguyễn Văn Tráng	22
Cao Thắng	77

Bảng 7 – Các cơ sở triển khai VOIP

Phòng ban	Số thứ tự tương ứng
Giáo viên (Falculty)	1
Đào Tạo (Training)	2
Kế Toán – Tài Chính (Finance)	3
Tuyển sinh (Admission)	4
Thư viện (Library)	5
NetLab	6
Lab	7

Bảng 8 – Các phòng ban triển khai VOIP

Tài khoản người dùng	Số thứ tự tương ứng
User1	1
User2	2

Bảng 9 – Số thứ tự tài khoản người dùng

5.3.1.3 Các quy định kiểm tra gói tin trên tường lửa

Việc kiểm tra các gói tin ra vào qua hệ thống mạng là vô cùng quan trọng, đóng vai trò quyết định trong việc phát hiện và ngăn chặn các cuộc tấn công vào hệ thống. Do đó, để tăng cường bảo mật an toàn hệ thống mạng, chúng tôi xây dựng quy định kiểm tra, bao gồm hai loại:

Rule ở lớp mạng cho từng phòng ban: gồm ba loại tương ứng với ba vùng mạng, áp dụng cho các luồng thông tin xuất phát từ:

- **Mạng bên trong:** được cấu hình trên tường lửa bên trong

Phòng ban	Hành động	Giao thức	Thời gian áp dụng	Miêu tả
Access Point	ALLOW	HTTPS	6h30 sáng đến 5h30 chiều	Cho phép thiết lập Web VPN để truy cập Internet
Lab	DENY	ALL	0h đến 24h	Cấm tất cả các truy cập ra mạng bên ngoài.
NetLab	ALLOW	ALL	6h30 sáng đến 5h30 chiều	Cho phép truy cập mọi giao thức ra Internet
IT	ALLOW	ALL	6h30 sáng đến 5h30 chiều	Cho phép truy cập web server trong DMZ, truy cập web trên Internet và các giao thức quản lý mạng, hỗ trợ người dùng
Các phòng ban còn lại	ALLOW	HTTP, HTTPS, SMTP, FTP, SMB, SKINNY.	6h30 sáng đến 5h30 chiều	Chỉ cho phép truy cập web, file server mail server và chia sẻ file, VOIP

Bảng 10 – Bảng quy luật cho các phòng ban trong mạng nội bộ

Ngoài thời gian hoạt động trên, tường lửa sẽ khóa tất cả kết nối truy cập từ trong ra ngoài.

- **Vùng Server Farm**

Cấm mọi kết nối từ vùng này vào mạng bên trong hay đi ra mạng bên ngoài. Tuy nhiên, những kết nối đã được chứng thực từ các server có thể đi vào bên trong thông qua ứng dụng web trên các cổng được chỉ định trước, do các kỹ sư lập trình thực hiện.

- **Mạng phi quân sự (DMZ):** Cấm mọi kết nối từ vùng này vào mạng bên trong hay đi ra mạng bên ngoài.
- **Mạng bên ngoài:** được cấu hình trên tường lửa bên ngoài.
  - ✓ Chỉ cho phép truy cập web (HTTP) và mail (SMTP) trên vùng DMZ.

- ✓ Cấm ping (ICMP) trên tất cả cổng giao tiếp của tường lửa.
- ✓ Chống IP Spoofing và ARP Spoofing.

Rule ở lớp ứng dụng dựa vào hướng lưu lượng

- **Từ bên trong ra bên ngoài:** được cấu hình trên tường lửa bên trong.

Giao thức	Các phần kiểm tra	Chi tiết	Miêu tả cụ thể
HTTP	url-length	100	Độ dài địa chỉ truy cập web là 100
	Request (host)	www.tuoitre.vn, www.dantri.com	Cấm truy cập Tuổi Trẻ và Dân Trí
	uri request	union, script, char(…)	Chặn những uri chứa ba chuỗi này
FTP	filename	*.exe, *.wav, *.mpg, *.avi,..	Cấm tải các file audio, video, file nén và file thực thi
IM (Instant Messenger)	protocol	msn, yahoo	Cấm sử dụng phần mềm chat

Bảng 11 – Bảng quy luật ở lớp ứng dụng từ bên trong ra bên ngoài

- **Từ bên ngoài vào mạng DMZ:** được cấu hình trên tường lửa bên ngoài.

Giao thức	Các phần kiểm tra	Chi tiết	Miêu tả cụ thể
HTTP	Max-conn	1000	Quy định số kết nối tối đa
	Embroyic Connection	200	Quy định số kết nối không hoàn tất
	url-length	100	Độ dài địa chỉ truy cập web là 100
	uri request	union, script, char(…)	Chặn những uri chứa ba chuỗi này
	spoof-server	ServerPRO	Chống Server Fingerprinting

Bảng 12 – Bảng quy luật ở lớp ứng dụng từ bên ngoài vào DMZ

Rule đối với kết nối VPN

Loại VPN	Hành động	Giao thức	Miêu tả
Site to Site VPN	ALLOW	H323 SMB FTP HTTP	• Người dùng các chi nhánh gọi điện cho nhau • Cho phép chia sẻ file trên Database Server • Cho phép tải file, truy cập web trên các server trong vùng DMZ
Easy VPN	ALLOW	SKINNY SMB FTP HTTP	• Voice • Cho phép chia sẻ file trên Database Server • Thời gian idle 30 phút • Thời gian kết nối tối đa 5h, sau đó xác thực lại • Thời gian tồn tại của khóa là 1h • Cho phép tải file, truy cập web trên các server trong vùng DMZ
Web VPN		FTP HTTP	• Thời gian idle 30 phút • Thời gian kết nối tối đa 5h, sau đó xác thực lại • Thời gian tồn tại của khóa là 1h

Bảng 13 – Bảng quy luật đối với kết nối VPN

5.3.2 Xây dựng các chính sách

Để bảo mật các thông tin trong hệ thống mạng, việc thiết lập các chính sách kiểm tra trên từng thiết bị vô cùng quan trọng, cụ thể gồm các thiết bị mạng sau:

5.3.2.1 Switch Layer 2

- **Port Security:** đảm bảo sự tường minh các thiết bị đầu cuối. Khi có thiết bị lạ gắn vào thì cổng đó sẽ bị shutdown ngay lập tức.
- **Remote SPAN (Switched Port Analyzer):** cho phép nhà quản trị giám sát hệ thống dễ dàng. Khi tính năng này được bật, thiết bị (Switch) sao chép toàn bộ gói tin đi qua nó và gửi đến cổng hay VLAN cố định. Từ đó, nhà quản trị phân tích, giám sát, đánh giá hệ thống thông qua thiết bị giám sát, hệ thống IDS (Intrusion Detection System)…

- **BPDU guard:** bật trên các cổng ở mode access của Switch, một trong các tính năng Spanning Tree Protocol (STP) nhằm chống những kẻ tấn công bên trong cố tình gửi gói BPDU (PortFast Bridge Protocol Data Unit) để trở thành Root Bridge. Nếu Switch nhận được gói BPDU từ cổng bật tính năng này thì ngay lập tức cổng này rơi vào trạng thái *errdisable*, không thể truyền hay nhận dữ liệu. Muốn sử dụng lại cổng này, cần có sự can thiệp của quản trị viên hay đợi khoảng thời gian *errdisable* hết hạn.
- **IEEE 802.1x (dot1x):** cung cấp mô hình chứng thực client-server nhằm hạn chế người dùng tham gia mạng LAN thông qua cổng vật lí (PNAC - port-based Network Access Control), chỉ triển khai trên Switch được hỗ trợ. Cùng việc cấu hình trên Switch, cần bật tính năng này trên các máy trạm đầu cuối. So với WEP (Wired Equivalent Privacy), 802.1x đảm bảo tính tin cậy, toàn vẹn dữ liệu. Hơn nữa, 802.1x đem lại một số phương pháp tiên tiến, như cơ chế lọc (Filtering). Ngoài thực hiện lọc SSID và MAC, 802.1x còn hỗ trợ khả năng lọc giao thức.

5.3.2.2 Switch Layer 3

Xây dựng ACL theo hướng từ trong ra ngoài với quy định sau:

- Ngăn chặn sự truy cập giữa hai phòng Lab và thư viện tới các phòng ban nhân viên (Phòng Giáo Viên, Kế Toán – Tài Chính, Đào Tạo, Tuyển Sinh) và truy cập lẫn nhau.
- Cho phép các phòng ban nhân viên (Phòng Giáo Viên, Kế Toán – Tài Chính, Đào Tạo, Tuyển Sinh) truy cập giao thức SKINNY (sử dụng dịch vụ VOIP).
- Cho phép phòng NetLab truy cập tất cả giao thức bên ngoài (Outside).
- Thư viện chỉ được phép truy cập HTTP ở bên ngoài (Outside).
- Cấm phòng Lab thường truy cập tất cả giao thức các máy nội bộ và bên ngoài.
- Cho phép các kết nối truy cập giao thức HTTPS từ Access Point (AP) đến Tường lửa bên trong (Firewall Inside).

5.3.2.3 Firewall Inside (Tường lửa bên trong)

Theo hướng lưu lượng

- **Từ trong (Inside) ra ngoài (Outside)**
  - Xây dựng Access Control List (ACL): cho phép các máy tính nội bộ (Inside) truy cập các giao thức HTTP, HTTPS, FTP, SMTP, H323 giữa các CCM server. Ngăn chặn người dung wifi kết nối vào cơ sở khác.

```
time-range NOWORK
 periodic weekdays 0:00 to 06:30
periodic weekdays 17:00 to 24:00
periodic weekend 0:00 to 24:00
!
 access-list IN_OUT extended deny ip 172.16.20.0 255.255.255.0 11.0.0.0 255.0.0.0
 access-list IN_OUT extended deny ip 172.16.20.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list IN_OUT extended permit ospf any any
access-list IN_OUT extended deny ip any any time-range NOWORK
access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 host 10.1.0.2 eq 445
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 any eq http
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 any eq https
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 any eq ftp
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 any eq ftp-data
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 host 11.0.0.2 eq smtp
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 host 11.0.0.2 eq pop3
access-list IN_OUT extended permit tcp host 10.0.0.4 host 10.1.0.4 eq 1720
 access-list IN_OUT extended permit tcp 172.16.0.0 255.255.0.0 any eq domain
 access-list IN_OUT extended permit udp 172.16.0.0 255.255.0.0 any eq domain
```

Bảng 14 – Các ACL từ trong ra ngoài

- Thiết lập chính sách kiểm tra (Inspection Policy) ở lớp Application với giao thức:
  - ✓ **HTTP:** cấm truy cập các trang web có nội dung xấu, hoặc phản động (ví dụ www.tuoitre.com.vn và www.dantri.com); ngăn chặn tải các file có đuôi mở rộng như .exe, .bat, .gif, .vbs), các file nén, file giải trí; chặn các ứng dụng web (có trường header là application); giới hạn chiều dài header phải lớn hơn 100; chặn nội dung tải về không phù hợp với nội dung header, chặn tải các trang web chạy ActiveX, Java Applet; chống CSS (Cross Site Scripting) và SQL Injection.

```
regex URL_TUOITRE ".*[Tt][Uu][Oo][Ii][Tt][Rr][Ee]\.[Vv][Nn]"
regex URL_DANTRI ".*[Dd][Aa][Nn][Tt][Rr][Ii]\.[Cc][Oo][Mm]\.[Vv][Nn]"
regex VIRUS ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt]) HTTP/1.[01]"
regex IMAGE ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh]) HTTP/1.[01]"
regex VIDEO ".*\.([Aa][Vv][Ii]|[Ff][Ll][Vv]|[Ww][Mm][Vv]) HTTP/1.[01]"
regex MUSIC ".*\.([Mm][Pp]3|[Ww][Mm][Aa]|[Ww][Aa][Vv]) HTTP/1.[01]"
regex COMPRESS ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]"
```

```
regex UNION ".*[Uu][Nn][Ii][Oo][Nn].*"
regex SCRIPT ".*[Ss][Cc][Rr][Ii][Pp][Tt].*"
regex CHAR ".*[Cc][H]h[Aa][Rr]\(.*\).*"
regex contenttype "Content-Type"
regex applicationheader "application/.*"
!
class-map HTTP_MAP
 match port tcp eq www
!
 class-map type regex match-any RESTRITED_URLS
  match regex URL_TUOITRE
  match regex URL_DANTRI
!
class-map type inspect http match-any URI_BLOCK
 match request header referer regex UNION
 match request header referer regex SCRIPT
 match request header referer regex CHAR
 match request uri regex VIRUS
 match request uri regex IMAGE
 match request uri regex VIDEO
 match request uri regex MUSIC
 match request uri regex COMPRESS
!
class-map type inspect http match-any RESTRICTED_HTTP
 match request uri length gt 200
 match request header host regex class RESTRITED_URLS
!
class-map type inspect http match-all AppHeaderClass
 match response header regex contenttype regex applicationheader
!
policy-map type inspect http MY_HTTP_MAP
 parameters
  protocol-violation action drop-connection
 class RESTRICTED_HTTP
  reset log
class URI_BLOCK
  reset log
 class AppHeaderClass
```

```
  drop-connection log
!
policy-map IN_OUT
 class HTTP_MAP
  set connection conn-max 1000 embryonic-conn-max 200 per-client-max 10 per-client-
embryonic-max 5
  inspect http MY_HTTP_MAP
!
 service-policy IN_OUT interface inside
```

Bảng 15 – Chính sách HTTP Inspection trên Firewall Inside

- ✓ **FTP:** cấu hình các chính sách tương tự giao thức HTTP.

```
   regex EXT_DOC ".+[Dd][Oc][Cc]"
  regex EXT_DOCX ".+[Dd][Oc][Cc][Xx]"
  regex EXT_XLS ".+[Xx][Ll][Ss]"
  regex EXT_XLSX ".+[Xx][Ll][Ss][Xx]"
  regex EXT_EXE ".+[Ee][Xx][Ee]"
  regex EXT_WAV ".+[Ww][Aa][Vv]"
  regex EXT_MPG ".+[Mm][Pp][Gg]"
  regex EXT_AVI ".+[Aa][Vv][Ii]"
  regex EXT_GIF ".+[Gg][Ii][Ff]"
  regex EXT_MP3 ".+[Mp][Pp]3"
  regex EXT_FLV ".+[Ff][Ll][Vv]"
  regex EXT_ZIP ".+[Zz][Ii][Pp]"
  regex EXT_RAR ".+[Rr][Aa][Rr]"
  !
  class-map type inspect ftp match-any RESTRICTED_EXT
   match filename regex EXT_EXE
   match filename regex EXT_WAV
   match filename regex EXT_MPG
   match filename regex EXT_AVI
   match filename regex EXT_GIF
   match filename regex EXT_MP3
   match filename regex EXT_FLV
   match filename regex EXT_ZIP
```

```
 match filename regex EXT_RAR
!
policy-map type inspect ftp MY_FTP_MAP
 class RESTRICTED_EXT
  reset log
!
class-map FTP_MAP
 match port tcp eq ftp
!
policy-map IN_OUT
 class FTP_MAP
 inspect ftp strict MY_FTP_MAP
 class RESTRICTED_EXT
  reset log
class-map FTP_MAP
 match port tcp eq ftp
!
policy-map IN_OUT
class FTP_MAP
 inspect ftp strict MY_FTP_MAP
!
service-policy IN_OUT interface inside
 !
```

Bảng 16 – Chính sách FTP Inspection trên Firewall Inside

- ✓ **Block Yahoo và MSN messenger**

```
class-map IM
 match any
!
policy-map type inspect im IM
 match protocol yahoo-im msn-im
drop-connection

policy-map IN_OUT
 class IM
  inspect im IM
```

```
!
service-policy IN_OUT interface inside
```

Bảng 17: Block Yahoo Messenger và MSN Messenger

- **Từ bên ngoài (Outside) vào bên trong (Inside)**
  - Cấu hình Access Control List (ACL)
    - ✓ Mở cổng 8000 từ Web Server đến Database Server, xác thực do lập trình viên xử lí.
    - ✓ Cho phép các cơ sở khác truy cập vào Database Server.
    - ✓ Cho phép user (Easy VPN) kết nối vào Call Manager và Call Manager kết nối với nhau
    - ✓ Cho phép các ứng dụng của Web VPN hoạt động.
    - ✓ Cho phép từ firewall outside connect vào ACS để xác thực.

```
access-list OUT_IN extended permit tcp 172.17.0.0 255.255.0.0 host 10.0.0.2 eq 445
access-list OUT_IN extended permit tcp host 10.1.0.4 host 10.0.0.4 eq 1720
access-list OUT_IN extended permit tcp host 11.0.0.2 host 10.0.0.2 eq 8000
access-list OUT_IN extended permit ospf any any
access-list OUT_IN extended permit udp host 193.1.3.1 host 10.0.0.2 eq radius
access-list OUT_IN extended permit tcp host 193.1.3.1 host 10.0.0.2 eq 139
access-list OUT_IN extended permit tcp 12.0.0.0 255.255.255.0 host 10.0.0.4 eq 2000
access-list OUT_IN extended deny ip any any
```

Bảng 18 – Các ACL từ ngoài vào Inside

Kết nối VPN

- **Web VPN:** không cần cài thêm phân mềm, sử dụng trình duyệt web (web browser) thực hiện kết nối VPN. Cho phép các đối tượng sau truy cập Internet thông qua Anyconnect. Tuy nhiên, các đối tượng này không thể truy cập hệ thống mạng nội bộ.
  - ✓ Giáo viên
  - ✓ Sinh viên
  - ✓ Công nhân viên
  - ✓ Khách mời

```
ip local pool WIFI 172.16.20.1-172.16.20.254
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 10.0.0.2 123456
!
webvpn
 enable inside
 tunnel-group-list enable
 onscreen-keyboard logon
 svc image flash:/anyconnect-win-2.4.0202-k9.pkg
 svc enable
 exit
 !
http server enable
!
group-policy WIFI internal
group-policy WIFI attributes
 vpn-tunnel-protocol svc
 webvpn
   svc ask enable
   svc keep-installer installed
   svc rekey method ssl
   svc rekey time 60
 !
tunnel-group WIFI type webvpn
tunnel-group WIFI general-attributes
 address-pool WIFI
 authentication-server-group RADIUS LOCAL
 default-group-policy WIFI
tunnel-group WIFI webvpn-attributes
 group-alias WIFI_GROUP enable
```

Bảng 19 – Các chính sách Web VPN trên Firewall Inside

5.3.2.4 Firewall Outside (Tường lửa bên ngoài)

- ***Theo hướng lưu lượng***
  - **Từ bên ngoài (Outside) vào vùng Phi Quân Sự (DMZ - Demilitarized Zone)**

- ✓ Xây dựng Access Control List (ACL) cho phép các máy tính bên ngoài truy cập HTTP đến Web Server, SMTP đến Mail Server trong vùng DMZ.

```
access-list OUT_IN extended permit tcp any host 193.1.5.2 eq http
access-list OUT_IN extended permit tcp any host 193.1.5.2 eq https
access-list OUT_IN extended permit tcp any host 193.1.5.2 eq smtp
access-list OUT_IN extended permit tcp any host 193.1.5.2 eq pop3
```

Bảng 20 – Các ACL cho phép từ bên ngoài vào DMZ

- ✓ Giới hạn số lượng kết nối truy cập tối đa (Max Connection) là 1000, các kết nối không hoàn tất quá trình bắt tay (Embroyic Connection) là 200.

```
static (inside,outside) tcp interface http 10.0.0.2 http netmask 255.255.255.255 tcp 1000
200
static (inside,outside) tcp interface ftp 10.0.0.2 ftp netmask 255.255.255.255 tcp 1000 200
static (inside,outside) tcp interface ftp-data 10.0.0.2 ftp-data netmask 255.255.255.255 tcp
1000 200
static (inside,outside) tcp interface smtp 10.0.0.2 smtp netmask 255.255.255.255 tcp 1000
200
static (inside,outside) tcp interface pop3 10.0.0.2 pop3 netmask 255.255.255.255 tcp 1000
200
static (inside,outside) tcp interface imap 10.0.0.2 imap netmask 255.255.255.255 tcp 1000
200
```

Bảng 21 – Các chính sách giới hạn kết nối từ ngoài vào DMZ

- ✓ Thiết lập chính sách kiểm tra (Inspection Policy) ở lớp Application với giao thức HTTP nhằm chống tấn công Web Server Fingerprinting, Cross Site Scripting và SQL Injection từ bên ngoài vào web server.

```
regex UNION ".*[uU][nN][iI][oO][nN].*"
 regex SCRIPT ".*[Ss][Cc][Rr][Ii][Pp][Tt].*"
 regex CHAR ".*[Cc][H]h[Aa][Rr]\(.*\).*"
!
class-map type inspect http match-any HACKING
  match request uri regex UNION
  match request uri regex SCRIPT
  match request uri regex CHAR
```

```
!
policy-map type inspect http MY_HTTP
  parameters
   spoof-server ServerPRO
class HACKING
  drop-connection log
!
 policy-map OUT_IN
  class OUT_IN
   inspect http MY_HTTP
!
service-policy OUT_IN interface outside
```

Bảng 22 – Chính sách HTTP Inspection trên Firewall Outside

- ***Kết nối VPN***

  - **Site to Site VPN**

Xây dựng Access List quy định các Interesting traffic, cho phép nhân viên chi nhánh khác có thể kết nối đến Database Server trung tâm cũng như truy cập DMZ. Ngoài ra, cho phép các Call Manager Server liên lạc với nhau giúp người dùng các cơ sở có thể lien lạc với nhau.

```
access-list VPN extended permit tcp 172.16.0.0 255.255.0.0 host 10.1.0.2 eq 445
access-list VPN extended permit tcp host 10.0.0.4 host 10.1.0.4 eq 1720
access-list VPN extended permit tcp host 10.0.0.2 eq 445 172.17.0.0 255.255.0.0
access-list VPN extended permit tcp host 10.0.0.4 eq 1720 host 10.1.0.4
!
access-list NONAT extended permit ip 172.16.0.0 255.255.0.0 10.1.0.0 255.255.255.0
access-list NONAT extended permit ip host 10.0.0.4 host 10.1.0.4
!
nat (inside) 0 access-list NONAT
!
crypto isakmp key 123456 address 192.168.2.3
!
```

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 life 84600
crypto ipsec transform-set TRANFORM esp-aes esp-sha-hmac
!
crypto map IPSEC 10 match address VPN
crypto map IPSEC 10 set peer 192.168.2.3
crypto map IPSEC 10 set transform-set TRANFORM
crypto map IPSEC interface outside
!
crypto isakmp enable outside
```

Bảng 23 – Các chính sách Site to Site VPN trên Firewall Outside

- **Easy VPN:** Cho phép nhân viên truy cập hệ thống mạng nội bộ khi đi công tác, chủ yếu sử dụng ba dịch vụ sau:
  - ✓ Kết nối Database Server trung tâm.
  - ✓ Truy cập web, mail trong DMZ.
  - ✓ Kết nối Call Manager Server để thực hiện các cuộc gọi.

```
ip local pool EASY_VPN 12.0.0.1-12.0.0.254
!
access-list SPLIT stand permit 10.0.0.0 255.255.255.0
access-list NONAT extended permit ip 10.0.0.0 255.255.255.0 12.0.0.0 255.255.255.0
!
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 10.0.0.2 123456
exit
!
```

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 life 84600
crypto ipsec transform-set TRANFORM esp-aes esp-sha-hmac
!
group-policy POLICY_EASY_VPN internal
group-policy POLICY_EASY_VPN attributes
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT
 dns-server value 172.16.5.2 203.113.131.1
 vpn-idle-timeout 15
 default-domain value lotus.edu.vn
!
tunnel-group EASY_VPN type remote-access
tunnel-group EASY_VPN general-attributes
 authentication-server-group RADIUS local
 address-pool EASY_VPN
 default-group-policy POLICY_EASY_VPN
 exit
!
tunnel-group EASY_VPN ipsec-attributes
 pre-shared-key 123456
 exit
!
crypto dynamic-map DYN_MAP_EASY_VPN 20 set transform-set TRANFORM
crypto map IPSEC 60000 ipsec-isakmp dynamic DYN_MAP_EASY_VPN
crypto map IPSEC interface outside
```

Bảng 24 – Các chính sách Easy VPN trên Firewall Outside

- **Web VPN:** Cho phép nhân viên truy cập hệ thống mạng nội bộ khi đi công tác, chủ yếu sử dụng ba dịch vụ sau:

- ✓ Kết nối Database Server trung tâm.
- ✓ Truy cập web, mail trong DMZ. (Port Forwarding).

```
webvpn
 enable outside
 tunnel-group-list enable
 onscreen-keyboard logon
 port-forward APPLICATIONS 23 193.1.1.2 23
 !
http server enable
!
group-policy NHANVIEN internal
group-policy NHANVIEN attributes
 vpn-tunnel-protocol webvpn
 group-lock value NHANVIEN
 webvpn
  functions url-entry file-access file-entry file-browsing
  url-list value URLs
 !
tunnel-group NHANVIEN type webvpn
tunnel-group NHANVIEN general-attributes
 authentication-server-group RADIUS LOCAL
tunnel-group NHANVIEN webvpn-attributes
 group-alias NVGroup enable
group-policy NHANVIEN attributes
 group-lock value NHANVIEN
!
group-policy ADMIN internal
group-policy ADMIN attributes
 group-lock value ADMIN
 vpn-tunnel-protocol webvpn
 webvpn
  functions port-forward
  port-forward value APPLICATIONS
 !
tunnel-group ADMIN type webvpn
tunnel-group ADMIN general-attributes
 authentication-server-group RADIUS LOCAL
tunnel-group ADMIN webvpn-attributes
```

```
 group-alias AdminGroup enable
group-policy ADMIN attributes
 group-lock value ADMIN
```

Bảng 25 – Các chính sách Web VPN trên Firewall Outside

5.3.2.5 Router biên

- Cấu hình chức năng NAT (Network Address Translation) để các máy bên trong hệ thống mạng (Inside) có thể truy cập bên ngoài Internet (Outside)
- Xây dựng Access Control List (ACL) cho phép các kết nối từ ngoài truy cập các giao thức ISAKMP, ESP đi vào Tường lửa bên ngoài (Firewall Outside) và HTTP, HTTPS, SMTP cho các máy Web Server, Mail Server.

5.3.3 Các công nghệ sử dụng

HSRP (Hot Standby Redundancy Protocol): triển khai trên hai Switch Layer 3 nhằm cân bằng tải và dự phòng khi một trong hai Switch gặp bất kì sự cố nào. Ngoài ra, hai Switch này còn đóng vai trò DHCP Server để cung cấp địa chỉ IP tự động cho các máy tính trong hệ thống. Do đó, với sự hỗ trợ cuả HSRP, một số người dùng lấy Switch 1 là Default Gateway của mình, trong khi một số khác nhận thấy Switch 2 mới là Default Gateway. Qua đó, giúp phân chia tải mạng truy cập trên hai Switch đồng thời tăng khả năng chịu lỗi cho hệ thống.

Failover (Dự Phòng): cấu hình trên hai cặp tường lửa (Inside và Outside Firewall) đảm bảo hoạt động liên tục và chính xác đồng thời tận dụng tối đa hiệu năng của cả hai cặp tường lửa.

Load Balancing: chủ yếu triển khai trên hai thiết bị:

- ***Firewall Load Balancing (Cân bằng tải trên tường lửa):*** Việc triển khai hệ thống dự phòng (Failover) trên tường lửa là chưa đủ, cần phải kết hợp thêm tính năng cân bằng tải giúp phân chia kiểm tra các lưu lượng truy cập trong hệ thống. Chỉ như vậy mới đảm bảo thông tin bảo mật an toàn đồng thời tường lửa cũng luôn sẵn sàng hoạt động.
- ***Load balancing ADSL (Cân bằng tải trên Router biên):*** Để cân bằng tải hai hay nhiều kết nối Internet, có nhiều cách khác nhau, tùy nhu cầu và khả năng kinh tế và tất nhiên có sự cân đối giữa chi phí và lợi ích mà nó mang lại.
  - ✓ **HSRP/MHSRP:** là cách đơn giản ít tốn kém nhất tuy nhiên nó không phải là cách cân bằng tải hoàn hảo, vì quá trình phân chia các tải mạng phụ thuộc vào kết nối được khởi tạo từ bên trong ra bên ngoài. Xét ở khía cạnh ngược lại, việc truy cập từ bên ngoài vào sẽ không được cân bằng tải. Chính điều này mà giải pháp

HSRP/MHSRP chỉ mang tính tương đối khi không có điều kiện triển khai những giải pháp khác như BGP hay load balancing bằng Vigor...

- ✓ **Đối với BGP:** dùng trên Internet, quá trình cấu hình tương đối phức tạp đồng thời yêu cầu ISP phải hỗ trợ mới có thể triển khai. So với HSRP/MHSRP, BGP là giải pháp tương đối hoàn hảo hơn. Tuy nhiên, BGP đòi hỏi khả năng xử lý của CPU cũng như RAM của Router.

Ngoài hai cách trên, còn nhiều cách khác nhau. Tuy nhiêu, theo các đánh giá của nhiều chuyên gia, cân bằng tải trên phần cứng (hardware load balancing) sẽ là giải pháp tối ưu nhất so với cân bằng tải trên phần mềm (software load balancing).

- ✓ **Sử dụng thiết bị Vigor:** cho phép gộp chung hai hay ba đường Internet. Chính vì đây là giải pháp phần cứng nên kinh phí đầu tư cao hơn hai cách trên, nhưng so với hiệu quả mà nó mang lại thì rất đáng triển khai.

Vì thế, đây cũng là giải pháp chúng tôi chọn lựa cho mô hình mạng trường Đại Học Hoa Sen.

VOIP: cung cấp hệ thống thoại cho người dùng trong cùng cơ sở hay giữa các chi nhánh với nhau thông qua kết nối leased – line hay triển khai hệ thống VPN (Virtual Private Network).

5.4 Một số công nghệ triển khai thêm

5.4.1 Failover

a. Giới thiệu

Tính năng đặc biệt nhằm cung cấp khả năng dự phòng cho thiết bị, đảm bảo hệ thống luôn hoạt động tốt và liên tục khi gặp sự cố. Một cặp thiết bị, trong đó một đóng vai trò Active, một đóng vai trò Standby, bao gồm hai loại dự phòng:

- **Dự phòng Phần cứng (Hardware failover):** cung cấp khả năng chịu lỗi cho thiết bị phần cứng, chủ yếu đồng bộ cấu hình giữa hai thiết bị. Vì thế, giả sử trong khi kết nối đã thiết lập mà thiết bị Primary bị shutdown thì mọi kết nối đều bị ngắt và phải được khởi tạo lại bên thiết bị secondary, điều không mong muốn khi triển khai hệ thống.
- **Dự phòng Ghi Nhớ Trạng Thái (Stateful failover):** vừa cung cấp khả năng chịu lỗi cho thiết bị phần cứng và khả năng bảo toàn kết nối. Ngoài việc đồng bộ cấu hình, hai thiết bị còn đồng bộ bảng trạng thái kết nối, ngày giờ, MAC address đối với transparent mode, SIP và VPN connection. Vì thế việc bị mất kết nối và phải khởi tạo lại ở thiết bị secondary là điều hiếm khi xảy ra.

b. Hoạt động

Dạng Active/Standby: một trong hai thiết bị ở trạng thái Active, còn lại là Standby tại một thời điểm. Mặc định, Primary sẽ Active, tất cả luồng dữ liệu đi qua thiết bị Active và đồng bộ sang Standby. Standby chỉ giám sát thiết bị Active, nếu nhận thấy Active không hoạt động thì nó tự chuyển sang Active. Mỗi thiết bị có IP và MAC riêng. Nếu xảy ra vấn đề với Active thì Standby tự chuyển IP và MAC của mình thành IP và MAC của active và gửi đi những frame ra các cổng giao tiếp cập nhật bảng MAC của Switch. Chú ý thiết bị active vừa rớt không chuyển sang Standby cho đến khi sửa xong. Cho dù sửa xong, thiết bị này cũng ở trạng thái Standby chứ không lấy lại quyền Active. Tuy nhiên, sử dụng dạng này lãng phí một thiết bị.

Dạng Active/Active: Khắc phục nhược điểm của Active/Standby, Active/Active ra đời dựa trên nền tảng và sự kết hợp của Active/Standby và Context (cho phép xây dựng firewall ảo).Trên mỗi thiết bị sẽ có hai context (CTX1A, CTX1B, CTX2A, CTX2B), mỗi context bên này sẽ kết hợp với context bên kia để tạo nên một Active/Standby, như vậy sẽ có một cặp Active/Standby. Cặp thứ nhất CTX1A là Active, CTX2A là Standby thì cặp thứ hai CTX1B làm Standby, CTX2B làm Active. Ngoài ra, kết hợp với đường định tuyến tĩnh (Static Route), hay động (dynamip route) ở transparent mode thì sẽ có thể cân bằng tải trên hai thiết bị. Tuy nhiên, trong thực tế quan sát thì việc dùng định tuyến tĩnh (Static Route) để cân bằng tải là không tối ưu, vì hầu hết dữ liệu chỉ đi theo một hướng nhất định. Chú ý: multiple mode (hỗ trợ context) không hỗ trợ định tuyến động (dynamip routing).

c. Nguyên nhân

Có nhiều nguyên nhân dẫn đến Failover như mất nguồn, một hay nhiều cổng giao tiếp bị hư, card mạng lỗi hay vấn đề phần mềm như thiếu bộ nhớ, tác nhân trực tiếp của người quản trị với câu lệnh failover active trên tường lửa Standby. Dưới đây là thời gian phát hiện vấn đề:

Failover Condition	Default Time	Minimum Time	Maximum Time
Active unit loses power or stops normal operation	15 seconds	800 ms	45 seconds
Active unit motherboard interface is down	5 seconds	500 ms	15 seconds
Active unit 4-GE card interface is down	5 seconds	2 seconds	15 seconds
Active unit IPS or CSC card fails	2 seconds	2 seconds	2 seconds
Active unit interface is up, but has connection problems that cause interface testing	25 seconds	5 seconds	75 seconds

Hình 51 – Thời gian Failover phát hiện lỗi

d. Giám sát

Về cơ bản, kết nối dự phòng (failover link) và kết nối dữ liệu (data link) giám sát bởi failover. Đối với kết nối dự phòng, tin nhắn hello (failover hello message) tạo ra mỗi 15s (mặt định), nếu ba tin liên tiếp đều không thấy phản hồi từ đối phương thì gói tin ARP được tạo ra và gửi đi trên tất cả cổng giao tiếp. Nếu không nhận được hồi đáp nào từ cổng giao tiếp nào thì failover sẽ làm việc, tự động chuyển thành trạng thái Active. Còn nếu không nhận được hồi đáp từ kết nối dự phòng mà nhận được hồi đáp từ các cổng giao tiếp còn lại thì quá trình chuyển đổi sẽ không xảy ra. Trong trường hợp này, failover kết luận lỗi do kết nối dự phòng.

Đối với kết nối dữ liệu (data link), tin nhắn hello (failover hello message) tạo ra và gửi đi trên tất cả cổng giao tiếp (tối đa là 255), như tin nhắn ở trên và cũng gửi đi mỗi 15s. Nếu quá nữa thời gian hold-down mã vẫn không thấy trả lời thì thiết bị sẽ tiến hành kiểm tra, xác định có vấn đề gì xảy ra với cổng giao tiếp này. Trước mỗi lần kiểm tra, bộ đếm số lượng gói tin nhận được trên cổng giao tiếp sẽ được xóa trắng. Sau đó, thiết bị sẽ kiểm tra xem có nhận được frame hay gói tin nào hợp lệ không, nếu có kết luận cổng giao tiếp hoạt động bình thường, ngược lại chờ đến lần kiểm tra tiếp theo, gồm bốn nội dung:

- ***Link up/down:*** vô hiệu hóa (Disable) và kích hoạt lại (re-enable) để kiểm tra.
- ***Hoạt động mạng:*** giám sát các frame nhận được trong vòng 5s.
- ***ARP:*** tạo hai gói tin truy vấn ARP (ARP Query) cho hai mục mới nhất trong bảng ARP (ARP table) và chờ đợi frame hợp lệ trong vòng 5s.
- ***Broadcast ping test:*** tạo gói ping broadcast và chờ gói tin phản hồi hợp lệ trong 5s

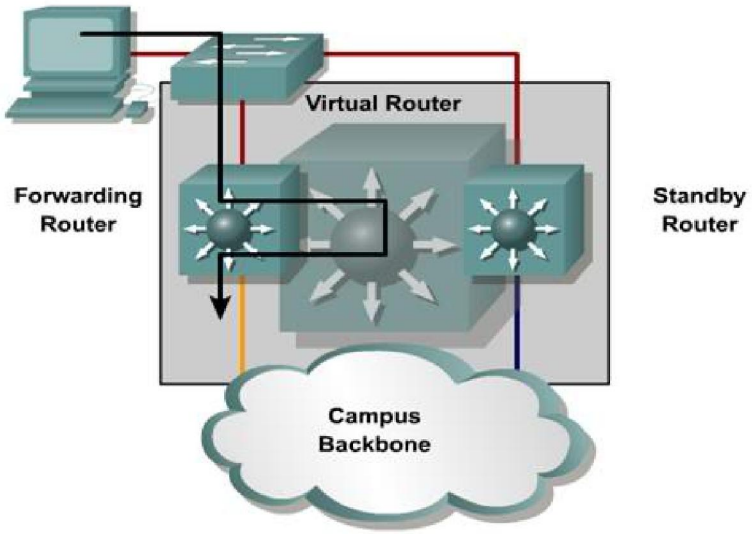
Thông thường thiết bị được kết nối switch layer 2, vì thế để giảm khả năng xảy ra lỗi thì phải đảm bảo các cổng giao tiếp cùng VLAN. Nếu không thì phải vô hiệu hóa giám sát trên cổng giao tiếp đó bằng lệnh **[no] monitor-interface logical_if_name**. Tiếp đến đảm bảo việc vận hành thuật toán STP không tác động hay khóa các cổng này. Ngoài ra nên cấu hình tính năng PortFast nếu dùng sản phẩm của Cisco. Nếu không làm thế, Switch sẽ không sử dụng RSTP mà thay vào đó dùng chuẩn do IEEE đưa ra (802.1d), sau đó STP lại phải tính toán lại, việc này mất khoảng 30 – 45 giây dẫn đến bỏ lỡ ba gói tin hello và ảnh hưởng đến failover.

5.4.2 HSRP (Hot Standby Redundancy Protocol)

a. Giới thiệu

Để bảo đảm hệ thống mạng sẵn sàng hoạt động (High Availability) liên tục khi gặp sự cố, HSRP là một trong số tính năng cung cấp khả năng dự phòng ở lớp Network cho các máy trong hệ thống mạng, giúp tối ưu hóa việc cung cấp các đường kết nối khi phát hiện liên kết

bị hư và cơ chế phục hồi sau khi gặp sự cố. Như HSRP, Virtual Router Redundancy Protocol (VRRP) và Gateway Load Balancing Protocol (GLBP) cũng cung cấp những chức năng tương tự, VRRP là giao thức chuẩn, được hỗ trợ bởi hầu hết Router khác nhau, còn GLBP là chuẩn của Cisco, được cải tiến từ VRRP và bổ sung thêm tính năng cân bằng tải.

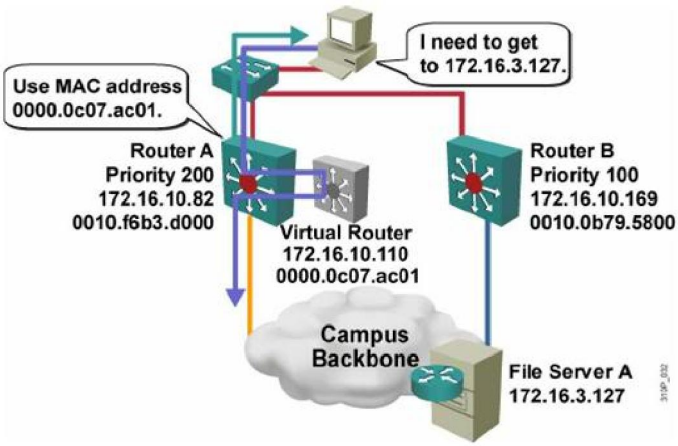


Hình 52 – Giao thức HSRP

HSRP là chuẩn của Cisco, miêu tả cụ thể trong RFC 2281. HSRP cung cấp khả năng dự phòng cho máy trạm dựa trên sự phối hợp của các Router để đưa ra một Router ảo giúp định tuyến lưu lượng ra vào hệ thống. Nhờ dùng chung địa chỉ IP và MAC, Router ảo này đóng vai trò định tuyến các gói tin trong hệ thống. Trên thực tế, Router ảo này hoàn toàn không tồn tại; nó được biểu diễn như thành phần chung các Router vật lý cấu hình tính năng HSRP.

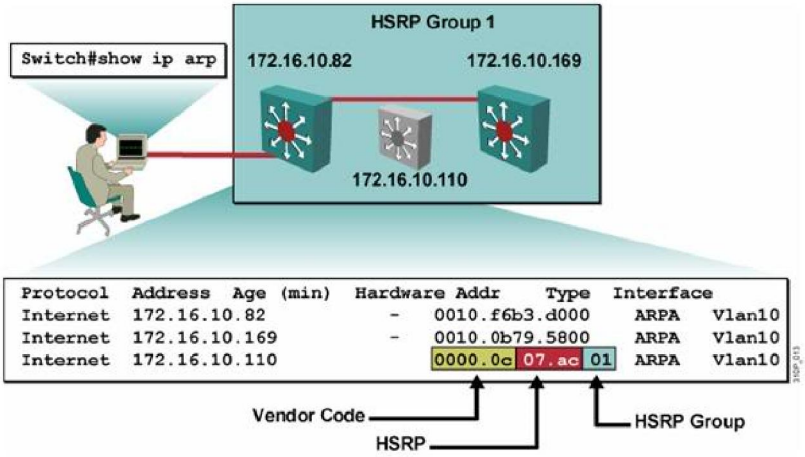
b. Hoạt động

Địa chỉ IP của Router ảo được cấu hình là Default Gateway cho các máy trạm trong mạng. Khi những frame được gửi từ các máy tính đến đến default gateway, chúng dùng cơ chế ARP (Address Resolution Protocol) để phân giải địa chỉ MAC với IP default gateway. Các frame gửi đến địa chỉ MAC này sẽ được xử lý tiếp tục bởi Router chính (Active Router) hay Router dự phòng (Standby Router) thuộc cùng nhóm Router ảo cấu hình. Quá trình này diễn ra hoàn toàn trong suốt với các máy trạm đầu cuối. Nhờ đó, HSRP giúp định tuyến các lưu lượng mà không cần dựa vào tính sẵn sàng của bất kì Router đơn lẻ nào.



Hình 53 – Quá trình hoạt động của HSRP

Trong hình trên Router A đang ở vai trò Active và chuyển tiếp tất cả frame đến địa chỉ MAC là 0000.0c07.acXX với XX là số nhóm dự phòng (standby group). Địa chỉ IP và MAC tương ứng của Router ảo được duy trì trong bảng ARP của mỗi Router trong nhóm.



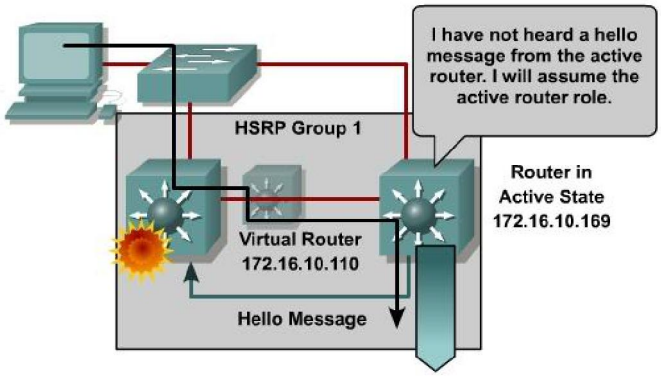
Hình 54 – Bảng ARP của các Router thành viên trong nhóm

Hình trên hiển thị bảng ARP của Router thành viên nhóm dự phòng 1 thuộc VLAN 10. Qua đó, địa chỉ IP của Router ảo là 172.16.10.110 với MAC tương ứng là 0000.0c07.ac01 (01 là số nhóm, hiển thị dưới hệ cơ số thập lục phân).

Các Router dự phòng (Standby Router) trong nhóm luôn theo dõi trạng thái hoạt động của Router chính (Active Router) để nhanh chóng chuyển trạng thái chuyển tiếp gói tin nếu Router chính gặp bất kì sự cố nào. Active và Standby Router sẽ truyền các gói tin hello message để giao tiếp với các Router khác trong nhóm với địa chỉ đích multicast 224.0.0.2, kiểu truyền UDP cổng 1985 và địa chỉ IP nguồn là địa chỉ IP Router gửi đi. Ngoài ra trong nhóm còn chứa một số Router khác không phải Active hay Standby, những Router này sẽ

giám sát các gói tin hello message được gửi bởi Active và Standby Router để chắc chắn Active và Standby Router vẫn đang tồn tại. Hơn nữa, các Router này chỉ chuyển tiếp những gói tin đến chính địa chỉ IP của nó mà không chuyển tiếp chỉ đến Router ảo.

Khi Active Router bị lỗi, những router khác thuộc cùng HSRP group sẽ không còn nhận được message từ active router, Standby Router sẽ giả định vai trò của nó lúc này là Active và điều khiển các lưu lượng mạng, các Router trong nhóm lại bầu chọn ra Standby Router. Lúc này quá trình truyền frame của các máy trạm vẫn không bị ảnh hưởng bởi vì Router ở trạng thái chuyển tiếp vẫn sẽ dùng địa chỉ IP ảo và MAC ảo như lúc đầu.



Hình 55 – Quá trình chuyển đổi khi Active Router gặp sự cố

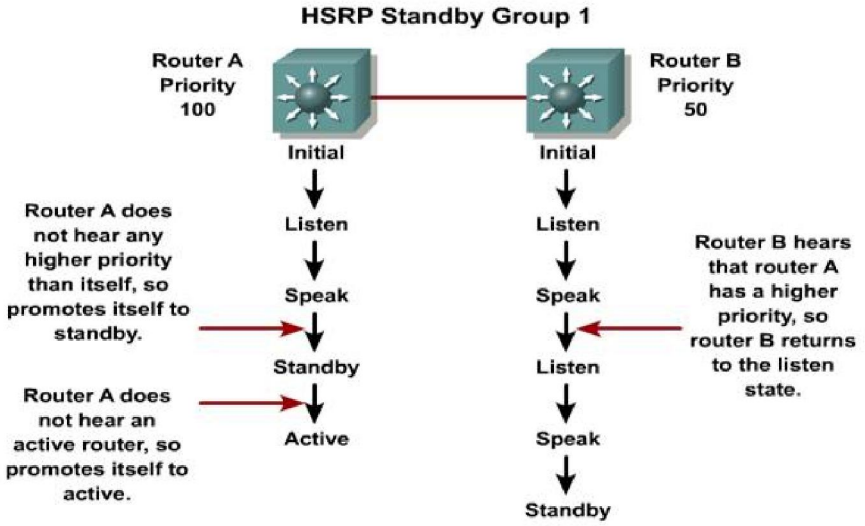
Nếu Active và Standby Router gặp sự cố thì tất cả Router trong nhóm lựa chọn lại Active và Standby Router mới. Active Router mới nhận lấy nhiệm vụ chuyển tiếp gói tin đến các máy trong hệ thống mạng.

Các vai trò của Router trong HSRP

HSRP định nghĩa ra các nhóm dự phòng (Standby Group), các Router sẽ được gán vai trò khác nhau trong nhóm này:

- ***Virtual Router:*** thực tế chỉ là một cặp địa chỉ IP và MAC mà tất cả thiết bị đầu cuối dùng làm IP default gateway. Active router sẽ xử lý tất cả gói tin và frame gửi tới địa chỉ IP hay MAC của Router ảo.
- ***Active Router:*** bầu chọn dựa trên giá trị ưu tiên (1-255, mặc định là 100) cũng như địa chỉ IP cao nhất, chịu trách nhiệm chuyển tiếp gói tin đồng thời gửi địa chỉ MAC ảo đến các thiết bị đầu cuối.
- ***Standby Router:*** dự phòng khi Active Router gặp bất cứ sự cố nào. Khi đó, Standby Router sẽ đóng vai trò Active, tiếp tục định tuyến các lưu lượng trong hệ thống.
- ***Other router:*** các Router khác không tham gia nhóm dự phòng (Standby Group).

Các trạng thái trong giao thức HSRP: Một Router trong nhóm dự phòng có thể ở một trong số trạng thái sau:



Hình 56 – Các trạng thái của HSRP

- ***Initial:*** trạng thái bắt đầu tất cả Router trong nhóm. Ở trạng thái này, HSRP không hoạt động.
- ***Learn:*** Router mong chờ nhận các gói tin HSRP, từ đó nhận thấy địa chỉ IP của Router ảo và xác định Active Router, Standby Router trong nhóm.
- ***Listen:*** Sau khi nhận gói tin HSRP và biết được địa chỉ IP Router ảo, nó tiếp tục chuyển sang trạng thái listen nhằm xác định xem có sự tồn tại Active hay Standby Router trong nhóm không. Nếu như đã có thì nó vẫn giữ nguyên trạng thái, ngược lại chuyển sang trạng thái Speak.
- ***Speak:*** Các Router chủ động tham dự quá trình chọn lựa Active Router, Standby Router dựa vào gói tin Hello.
- ***Standby:*** ứng viên cho vị trí Active Router kế tiếp. Standby Router định kỳ gửi các gói tin hello, đồng thời cũng lắng nghe các hello message từ Active Router. Trong một mạng HSRP chỉ có duy nhất một Standby Router.
- ***Active:*** chuyển tiếp gói tin, gửi địa chỉ MAC ảo của nhóm đồng thời hồi đáp các gói tin ARP request hướng đến IP ảo. Active Router cũng định kỳ gửi ra các hello message. Trong một nhóm dự phòng chỉ tồn tại duy nhất một Active Router.

c. Một số thuật ngữ trong HSRP

Có ba dạng timer dùng trong HSRP. Nếu không có gói tin hello nào được nhận từ Active Router trong khoảng thời gian Active thì Router chuyển sang trạng thái mới.

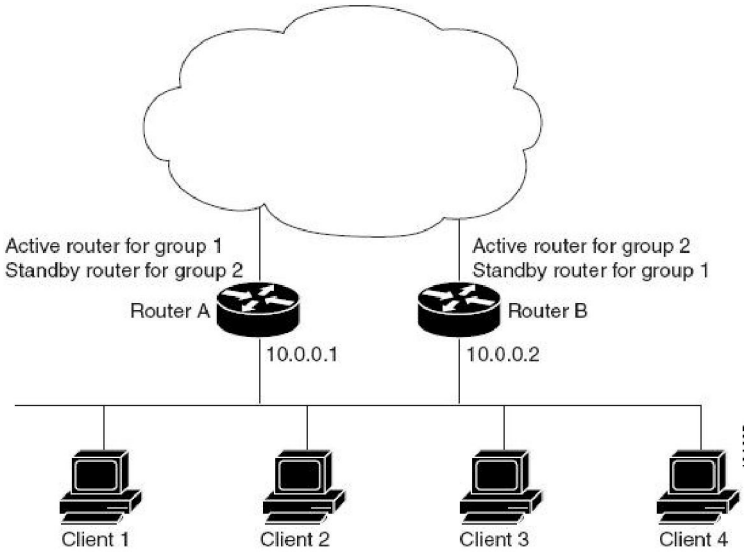
- ***Active timer:*** dùng để giám sát Active Router, tự khởi động lại vào bất kỳ thời điểm nào khi bất kì Router trong nhóm nhận được gói tin hello từ Active Router.
- ***Standby timer:*** dùng để giám sát standby router, tự khởi động lại vào bất kỳ thời điểm nào bất kì Router trong nhóm nhận được gói tin hello từ Standby Router.
- ***Hello timer:*** thời gian của gói tin hello. Tất cả các Router trong nhóm dự phòng ở bất kỳ trạng thái nào của HSRP đều tạo ra gói tin hello khi mà hello timer quá hạn.

Ngoài ra, để xác định khoảng thời gian tối đa gói tin hello, chúng ta quan tân hai giá trị sau:

- ***Hello Interval Time:*** khoảng thời gian giữa hai gói tin hello thành công từ một Router. Mặc định là 3 giây.
- ***Hold Interval Time:*** khoảng thời gian giữa hai gói tin hello được nhận và giả định Router gửi đang gặp sự cố. Mặc định là 10 giây.

d. Multiple HSRP (MHSRP)

Từ phiên bản Cisco IOS Release 12.2(18) SE trở lên đều có khả năng hỗ trợ Multiple HSRP (MHSRP) – được mở rộng từ HSRP cho phép cân bằng tải giữa hai hay nhiều nhóm HSRP từ các máy trạm đến các server trong hệ thống.



Hình 57 – Multiple HSRP

Trong hình trên, ta thấy cả Router A và Router B đều thuộc hai nhóm dự phòng. Đối với nhóm 1, Router A mặc định là Active Router vì nó có giá trị ưu tiên cao nhất và Router B là

Standby Router. Ngược lại nhóm 1, trong nhóm 2, Router B mặc định là Active Router bởi vì nó có giá trị ưu tiên cao nhất và Router A là Standby Router. Trong suốt quá trình hoạt động bình thường, hai Router A và B lần lượt phân chia tải mạng. Khi hai Router không hoạt động, các Router khác trong nhóm sẽ tự bầu chọn Active và Standby bảo đảm hệ thống mạng luôn hoạt động liên tục và cân bằng tải các luồng lưu lượng trong mạng.

5.4.3 Cân bằng tải trên Firewall (Firewall Load Balancing)

Trong môi trường mạng mà bảo mật đóng vai trò sống còn như hiện nay, việc bảo đảm tường lửa luôn sẵn sàng hoạt động (High Availability) rất quan trọng. Ngoài việc cấu hình tính năng dự phòng cho tường lửa (Firewall Failover) – cung cấp khả năng hoạt động liên tục và chính xác, việc phân chia các luồng thông tin kiểm tra trên tường lửa cũng đóng vai trò vô cùng cần thiết. Từ phiên bản ASA 7.0 và FWSM 3.1, Cisco đã đưa ra khái niệm context và hỗ trợ triển khai nhiều context trên các cặp tường lửa dự phòng giúp chia tải kiểm tra các lưu lượng ra vào hệ thống. Tuy nhiên, quá trình này đòi hỏi cấu hình bằng tay và các tường lửa tham gia phải giống nhau về mẫu, phiên bản và các thông số kỹ thuật khác.

a. Tổng quan

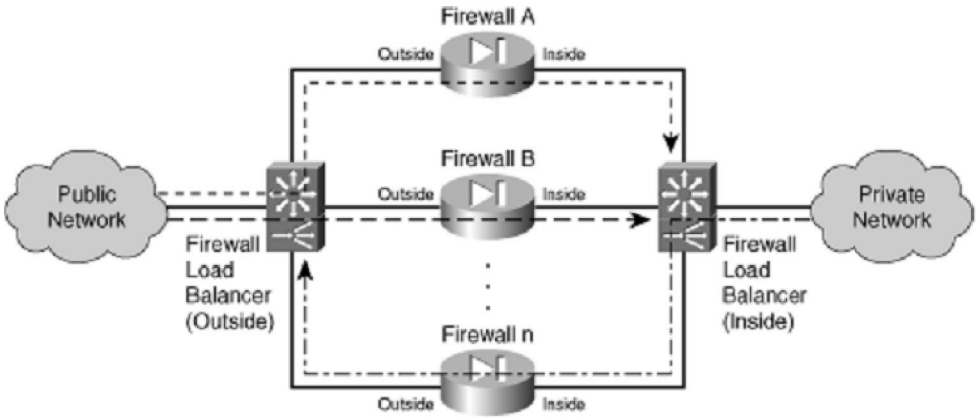
Việc triển khai hệ thống tường lửa có thể thực hiện bằng nhiều cách khác nhau. Dưới đây là bảng so sánh giá thành, các tính năng bảo mật cũng như khả năng dự phòng trên hệ thống triển khai xây dựng một tường lửa đơn lẻ, một cặp tường lửa hay nhóm các tường lửa cấu hình tính năng Firewall Load Balancing (FWLB).

Các tính năng	**Tường lửa đơn lẻ (Single Firewall)**	**Dự phòng tường lửa (Firewall Failover)**	**Cân bằng tải trên tường lửa (FWLB)**
Giá Thành	Thấp, chỉ xây dựng một tường lửa.	Vừa, cần xây dựng hai tường lửa.	Cao, ít nhất hai tường lửa, kèm theo thiết bị cân bằng tải.
Điểm dự phòng (Firewall Point of Failover)	Một: bản thân tường lửa	Không: hai tường lửa vật lý riêng biệt	Không: Tất cả tường lửa gom thành nhóm.

Hiệu năng	Hạn chế đối với hệ thống tường lửa đơn lẻ.	Hạn chế đối với hệ thống tường lửa đơn lẻ. Chỉ một cặp tường lửa chính kiểm soát các lưu lượng tại thời điểm nhất định.	Tỷ lệ thuận số lượng tường lửa. Trên lý thuyết, mỗi tường lửa tận dụng tối đa năng lực với khả năng cân bằng tải lý tưởng.
Cân bằng tải	Không.	Không, tường lửa chính (active) kiểm soát mọi kết nối truy cập.	Kiểm tra kết nối truy cập giao cho các tường lửa, dựa theo thuật toán băm. Cùng một thời điểm, tất cả tường lửa kiểm soát các lưu lượng ra vào.
Phản ứng khi gặp sự cố	Không chuyển tiếp hay kiểm soát bất kì lưu lượng nào.	Tất cả lưu lượng truy cập đẩy qua tường lửa dự phòng (standby) xử lí.	Kết nối truy cập mới giao cho các tường lửa khác xử lí.
Cài đặt thêm các phần cứng bổ sung	Không	Không	Một thiết bị FWLB phải cài đặt mỗi bên nhóm tường lửa. Với Catalyst 6500 Content Switching Module (CSM), CSM thực thi trên cả hai bên nhóm tường lửa.

Bảng 26 – Bảng so sánh các các tính năng tường lửa trên các hệ thống khác nhau

Để phân phối các kết nối giữa các thành viên trong nhóm, FWLB yêu cầu thêm một chức năng cân bằng tải trên mỗi bên nhóm tường lửa. Điều này đảm bảo các kết nối được phân phối trên các bức tường lửa và các lưu lượng ra vào hệ thống luôn gửi đến cùng tường lửa.



Hình 58 – Firewall Load Balancing (FWLB)

b. Một số phương pháp cân bằng tải trên tường lửa

Với việc sử dụng hay kết hợp một trong các cách sau:

- **Phần mềm:** gồm các tính năng sau:
  - ✓ Phần mềm Cisco IOS dùng trên các switch Catalyst 6500 cho IOS Firewall Load Balancing (IOS FWLB), một thành phần của Server Load Balancing (IOS SLB).
  - ✓ Các tường lửa được cấu hình như một trang trại tường lửa (firewall farm).
  - ✓ Khi lưu lượng được định tuyến qua nông trại tường lửa, các kết nối phân phối cho từng tường lửa trong trang trại. Quá trình này diễn ra trong suốt với người dùng.
- **Phần cứng:** Các thiết bị cân bằng tải phân phối các lưu lượng truy cập cho thành viên nông trại tường lửa. Những kết nối qua tường lửa đều được cân bằng tải thông qua các thiết bị phần cứng với các thuộc tính sau:
  - ✓ Cisco Catalyst 6500 Content Switching Module (CSM) dùng cân bằng tải trên tường lửa như là một thành phần của Accelerated Server Load Balancing (ASLB).
  - ✓ Tường lửa được cấu hình như máy chủ trang trại bình thường.
  - ✓ Khi lưu lượng truy cập được nhận trên VLAN ở trong, CSM phân chia các kết nối cho các tường lửa thành viên xử lí.
- **Các thiết bị chuyên dụng**

Thiết bị chuyển nội dung (External content-switching appliances) đặt trên mỗi bên nhóm tường lửa. Các kết nối truy cập phân phối cho các thành viên trong trang trại, dựa theo:

- ✓ Cisco Content Services Switch (CSS) dùng cân bằng tải.
- ✓ Tường lửa được cấu hình riêng, CSS xem chúng như danh sách tường lửa hữu ích hơn là một trang trại tường lửa.

- ✓ CSS phân phối các luồng truy cập đến tường lửa theo đường định tuyến xác định và thuật toán băm trên địa chỉ IP.

5.4.4 Chứng thực 802.1x

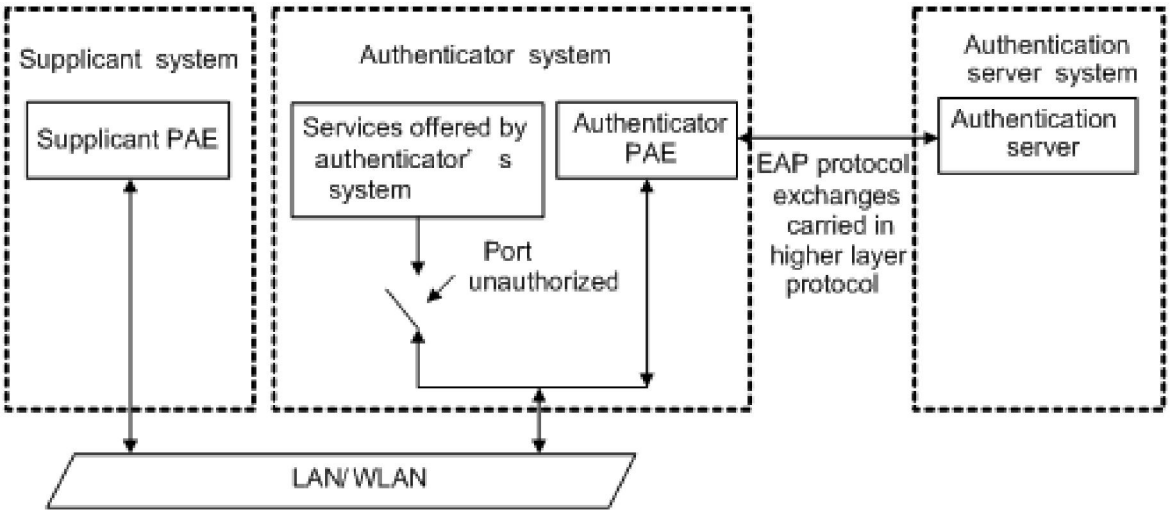
a. Giới thiệu

IEEE 802.1x được phát triển bởi IEEE, một trong số những giao thức mạng IEEE 802.1 nhằm cung cấp khả năng chứng thực cho người dùng trong mạng không dây. Sau đó, nó còn được dùng trong mạng Ethernet như là một cơ chế điều khiển truy cập trên các cổng vật lí.

Chuẩn 802.1x xây dựng dựa trên mô hình chứng thực kiểu client-server giúp hạn chế người dùng tham gia mạng LAN thông qua phương pháp port-based. Bên cạnh đó, 802.1x còn đưa ra hạ tầng cho việc xác nhận và điều khiển lưu thông người dùng trong mạng được bảo vệ cũng như cấp phát động các khóa mã hóa khác nhau.

b. Kiến trúc

Supplicant System (hay Client): máy trạm hoặc các thiết bị có nhu cầu được chứng thực để có đủ thẩm quyền tham gia vào mạng. Quá trình xác thực được kích hoạt khi người dùng thực thi chương trình cung cấp khả năng xác thực 802.1x mà các ứng dụng này thường đòi hỏi phải hỗ trợ giao thức EAPoL (Extensible Authentication Protocol over LAN).



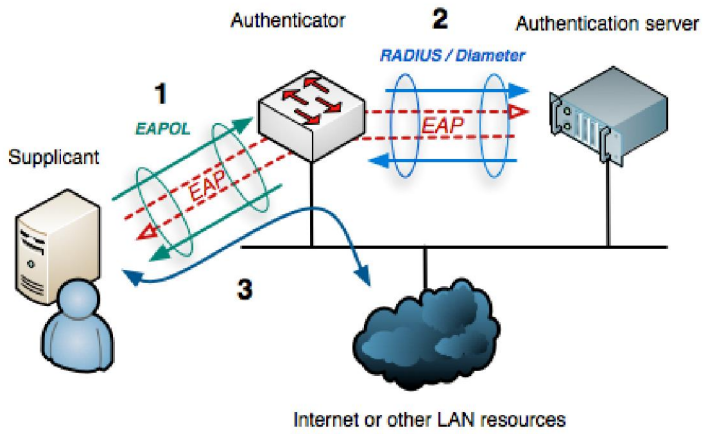
Hình 59 – Kiến trúc 802.1x

Authenticator System (thường là các thiết bị mạng hỗ trợ xác thực 802.1x như Switch…): cung cấp các cổng (vật lý và luận lý) cho máy tính truy cập hệ thống mạng. Ngoài ra, nó còn giúp trung chuyển các thông tin chứng thực qua lại giữa client và server.

Authentication Server System: cung cấp dịch vụ xác thực cho Authenticator System, thông thường là RADIUS server, AAA server. Ngoài ra, nó còn lưu trữ thông tin người dùng như username, password, VLAN phụ thuộc… dùng để so sánh với các thông tin người dùng gửi đến nhằm xác nhận xem đây có phải là người dùng hợp lệ hay không.

Authenticator và Authentication Server được tích hợp chung trên một thiết bị. Tuy nhiên, để tránh trường hợp người dùng tiếp xúc trực tiếp gây tổn hại server, Authentication Server và Authenticator System thường kết nối thông qua Switch và tồn tại trong suốt với người dùng.

c. **Hoạt động:** Quy trình xác thực (authenticate) và ủy quyền (authorize) theo chuẩn 802.1x diễn ra như sau:



Hình 60 – Hoạt động xác thực người dùng theo chuẩn 802.1x

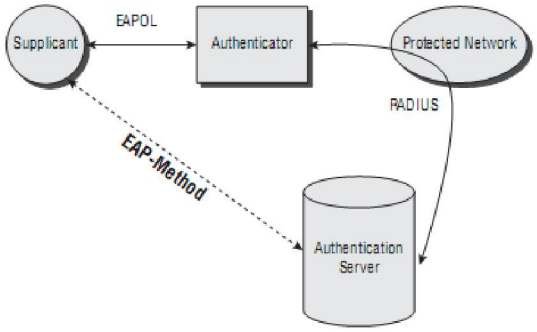
Initialization: Khi phát hiện supplicant mới, cổng trên switch (authenticator) được kích hoạt ở trạng thái chưa được ủy quyền (unauthorized). Ở trạng thái này, chỉ cho phép các lưu lượng 802.1X, ngoài ra những lưu lượng truy cập khác như DHCP, HTTP… đều bị bỏ đi.

Initiation: Để bắt đầu quá trình chứng thực, authenticator sẽ lần lượt chuyển các frame EAP-Request/Identity đến một địa chỉ đặc biệt lớp hai trên phân mạng cục bộ. Supplicant sẽ lắng nghe trên địa chỉ này và khi nhận được frame EAP-Request/Identity, nó sẽ trả lời bằng frame EAP-Response/Identity chứa các thông tin chứng thực của supplicant như tên đăng nhập (User ID), mật mã (password). Sau đó Authenticator sẽ đóng gói các thông tin này trong gói tin RADIUS Access-Request và chuyển tiếp cho Authentication Server. Supplicant cũng có thể bắt đầu hay khởi động lại quá trình chứng thực bằng cách gửi frame EAPOL-Start cho Authenticator, mà sau đó sẽ được trả lời với frame EAP-Request Identity.

Negotiation (hay EAP negotiation): Authentication Server gửi trả lời (đóng gói trong gói tin RADIUS Access-Challenge) cho Authenticator, gồm thông số EAP Method (loại chứng thực dựa trên EAP Supplicant muốn thực hiện). Authenticator đóng gói EAP Request trong frame

EAPOL và chuyển tới Supplicant. Lúc này, Supplicant có thể NAK yêu cầu EAP Method và trả lời với thông số EAP Methods nó muốn thực hiện hay bắt đầu yêu cầu EAP Method.

Authentication: Nếu cả Authentication Server và Supplicant đều đồng ý các thông số EAP Method thì Supplicant và Authentication Server (thông qua Authenticator) sẽ lần lượt trao đổi các bản tin EAP Requests và Responses cho đến khi Authentication Server đáp ứng một trong hai tin EAP-Success (gói gọn trong gói tin RADIUS Access) hay EAP-Failure (gói gọn trong gói tin RADIUS Access-Reject). Nếu chứng thực thành công thì Authenticator sẽ thiết lập trạng thái cổng là "Authorized" và cho phép chuyển tiếp mọi lưu lượng truy cập; ngược lại nếu thất bại, cổng vẫn ở trạng thái "unauthorized". Khi Supplicant thoát khỏi hệ thống, nó gửi bản tin EAPOL-logoff cho Authenticator để lần nữa thiết lập trạng thái cổng là "unauthorized", khóa mọi lưu lượng truy cập ngoại trừ các lưu lượng EAP.



Hình 61 – Cách thức trao đổi giữa Supplicant, Authenticator và Authentication Server

Nhìn chung, quá trình trao đổi bản tin giữa Supplicant và Authentication Server thực hiện thông qua EAP – Method dùng kết nối điểm - điểm, phụ thuộc loại EAP-Method còn Authenticator và Supplicant trao đổi các bản tin thông qua giao thức chứng thực EAPOL (EAP over LAN). Ngoài ra, trước khi chứng thực thành công, chỉ có một số giao thức cơ bản được dùng để trao đổi qua lại giữa Supplicant và Authenticator như STP, CDP, EAPOL... Chỉ sau khi được chứng thực, các frame dữ liệu khác mới được trao đổi bình thường.

d. Ưu và nhược điểm của 802.1x

- ***Ưu điểm***

Đảm bảo tính tin cậy: Hầu hết thông tin trao đổi trong mạng đều mã hóa, cả mật khẩu ban đầu, tránh việc giả mạo thông qua cơ chế chứng thực lẫn nhau giữa Client và Server, áp dụng các phương pháp mã hóa như SSH (Secure Shell), SSL (Secure Sockets Layer) hay IPSec.

Đảm bảo tính toàn vẹn: dùng các phương thức kiểm tra như Checksum hay Cyclic Redundancy Checks (CRCs) để kiểm tra tính toàn vẹn dữ liệu, bên cạnh đó còn dùng các thuật toán hóa MD5 và RC4 để đảm bảo sự toàn vẹn này.

Đảm bảo tính sẵn sàng: cập nhật với sự phát triển thiết bị cũng như các vấn đề phát sinh mới nhất đảm bảo sẵn sàng không gặp phải trở ngại cũng như tương thích thiết bị hiện có.

Cơ chế xác thực: kết hợp giữa cơ chế chứng thực động và quản lí chìa khóa tập trung, 802.1x khắc phục được hầu hết vấn đề của các giao thức khác. EAP - định nghĩa trong RFC 2284, dùng cho kết nối point-to-point (PPP), đưa ra những đặc trưng của phương pháp chứng thực gồm định dạng người dùng như mật mã (password), chứng nhận (certificate), giao thức được sử dụng (MD5, TLS, GMS, OTP…), hỗ trợ sinh khóa tự động và chứng thực lẫn nhau.

Do 802.1x dựa trên cơ sở điều khiển truy cập trên các cổng nên ngoài các phương pháp bảo mật chung, 802.1x còn đem lại một số phương pháp tiên tiến, như cơ chế lọc (Filtering). Ngoài việc thực hiện lọc SSID và MAC như các chuẩn khác, 802.1x còn hỗ trợ khả năng lọc giao thức. Mạng LAN không dây lọc các gói đi qua mạng dựa trên các giao thức lớp 2 đến lớp 7. Trong nhiều trường hợp, các nhà sản xuất làm các bộ lọc giao thức có thể định hình độc lập cho cả những đoạn mạng hữu tuyến và vô tuyến của Access Point (AP).

Nhược điểm

Mặc dù theo nghiên cứu trên thì 802.1x là một chuẩn bảo mật khá an toàn. Tuy nhiên nó vẫn tồn tại những hạn chế:

- Không thể chống lại tấn công "Từ chối dịch vụ (DoS – Denial of Service).
- Một số đặc tính yêu cầu đặc biệt về phần cứng, do đó phải kết hợp các phương pháp bảo mật với nhau, đồng thời đưa ra các chính sách bảo mật hợp lí.

Theo các vấn đề trên, bản thân 802.1x đã đưa ra một số chính sách khắc phục:

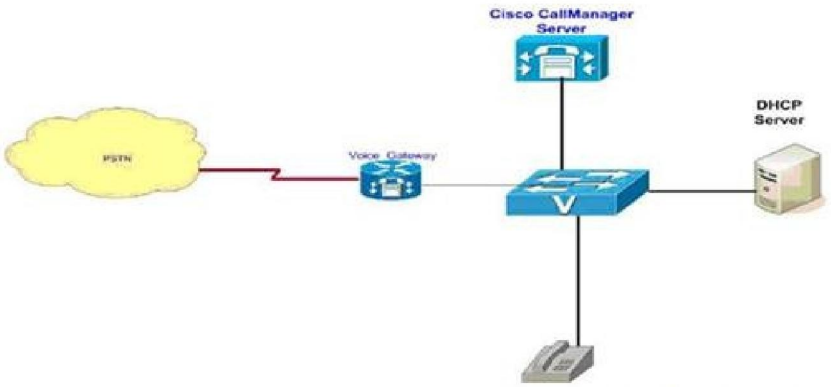
- Bảo mật về mặt thiết bị vật lí, phân cấp quyền hợp lí, luôn bật tính năng tối ưu nhất, do mọi tính năng hầu như đều có thể kích hoạt hay vô hiệu hóa.
- Sử dụng các thiết bị quét phổ để xác định thiết bị nghe trộm, công suất phát hợp lí tránh tín hiệu sóng bị rò rỉ ra ngoài phạm vi cần thiết.
- Tích hợp VPN bảo mật kết nối WLAN. Khi VPN Server tích hợp vào Access Point (AP), người dùng sử dụng phần mềm VPN Client, các giao thức như PPTP hay IPSec để hình thành đường hầm trực tiếp tới Access Point (AP). Trước tiên người dùng kết nối tới điểm truy nhập, sau đó quay số kết nối VPN. Tất cả lưu lượng được qua thông qua đường hầm, và có thể được mã hóa để thêm một lớp an toàn.

5.4.5 Hệ thống thoại VOIP (Voice Over IP)

a. Giới thiệu

Hiện nay, hệ thống voice là yêu cầu cấp thiết mà bất kỳ doanh nghiệp hay tổ chức nào cũng cần đến. Tùy nhu cầu, doanh nghiệp có thể triển khai hệ thống thoại truyền thống hay Voice Over IP (VOIP). Vì vậy, có nhiều giải pháp thoại đưa ra như: hệ thống tổng đài 3CX, hệ thống Asterisk hay CVOICE của Cisco. Là một trong các nhà sản xuất lớn, Cisco cung cấp nhiều giải pháp và thiết bị phục vụ lĩnh vực mạng truyền thông, đặc biệt là giải pháp tích hợp tiếng nói và hình ảnh trên cùng mạng dữ liệu AVVID (Architecture for Voice, Video and Integrated Data), gồm ba thành phần chính cơ bản là cơ sở hạ tầng (Infrastructure), thiết bị đầu cuối (Clients) và chương trình ứng dụng (Applications). Bên cạnh đó, Cisco là hãng đưa ra giải pháp đầy đủ và đồng bộ giữa các thành phần: Định tuyến, Bảo mật và Chuyển mạch.

Về vấn đề đường truyền, VOIP sử dụng hạ tầng mạng IP thông thường gồm LAN, WAN và kết nối PSTN. Đối với LAN, vì hoạt động trên nền IP nên VOIP có thể sử dụng chung hạ tầng có sẵn, không cần đầu tư lại. Đối với kết nối WAN, có thể dùng đường truyền leased-line hay VPN kết nối hai hay nhiều trung tâm. Tuy nhiên, giải pháp nào cũng tồn tại ưu và nhược của nó. Với leased-line, đảm bảo chất lượng cuộc gọi nhưng giá thành cao, còn với VPN khó đảm bảo chất lượng cuộc gọi. Vì thế, tùy nhu cầu mà có sự chọn lựa thích hợp.



Hình 62 – Mô hình VOIP đơn giản

Về thiết bị, các thiết bị sau không thể thiếu trong hệ thống VOIP của Cisco:

- **Call Manager:** hệ thống tích hợp phần cứng và phần mềm do Cisco chế tạo sẵn, hoạt động như Server trong mạng. Tuy nhiên có thể sử dụng Server bình thường do nhà sản xuất khác cung cấp (có trong danh sách hỗ trợ bởi Cisco) cài đặt Call Manager.
- **CCM Server:** xử lý định tuyến cuộc gọi, quản lý điện thoại IP (IP Phone).
- **IP Phone:** thiết bị đầu cuối, chuyển âm thanh thành tín hiệu số, đóng gói vào gói tin và ngược lại. Ngoài ra, Cisco còn đưa ra phần mềm Soft Phone tương tự IP Phone.
- **Voice gateway (hay Voice-enable Router):** chuyển thoại IP thành Analog mạng PSTN. Hiện nay dùng Router 2800 hay 3800 có Card Voice FXO hay Card E1/T1 Pri.

Hơn nữa, Gateway còn làm đảm nhiệm chức năng QoS (Quality of Service) đảm bảo chất lượng đàm thoại.

b. Giải pháp triển khai: bao gồm hai phương án:

- ***Sử dụng Máy chủ Call Manager cho hệ thống có nhiều hơn 96 client***

Trong giải pháp này, tại mỗi điểm sử dụng một Call Manager Server riêng. Mỗi Server chịu trách nhiệm xử lý cuộc gọi ở mỗi chi nhánh. Khi cần thiết người dùng chi nhánh này có thể gọi người dùng ở chi nhánh kia thông qua WAN hay PSTN tùy cấu hình, gồm thiết bị sau:

- Sử dụng hai Voice Gateway độc lập để kết nối đến PSTN.
- Tùy nhu cầu, có thể dùng Card E1 PRI (30 kênh thoại đồng thời) hay n đường FXO (n kênh thoại đồng thời). Khi đó doanh nghiệp thuê dịch vụ tương ứng từ bưu điện.
- Ngoài ra chúng tôi cần thuê thêm đường WAN để kết nối hai chi nhánh lại với nhau để vừa truyền thoại và dữ liệu. Mỗi cuộc gọi cần tối thiểu là 30Kb/s nên khuyến nghị là thuê đường tối thiểu khoảng 128Kb/s.
- IP phone có thể dùng phần cứng hay phần mềm.

Ưu điểm

- Khả năng mở rộng lớn, mỗi Server có thể xử lý cho 1000 máy.
- Nâng cấp, đưa ra các dịch vụ cho IP Phone dễ hơn như: Conference, IP Contact Center, Voice mail….

Nhược điểm: Giá thành cao.

- ***Sử dụng Máy chủ Call Manager cho hệ thống có số máy điện thoại mỗi chi nhánh đều nhỏ hơn 96 Client***

Trong giải pháp này không dùng CCM Server tại hai chi nhánh, việc xử lý cuộc gọi và quản lý IP Phone được thực hiện bởi Voice Gateway. Mọi thông số khác vẫn không đổi.

Ưu điểm: Chi phí thấp.

Nhược điểm:

- Khó mở rộng, tích hợp dịch vụ mới.
- Ít tính năng hơn.

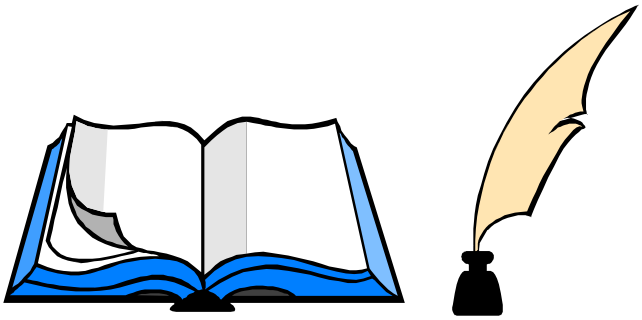
KẾT LUẬN

Trong thời đại khoa học ngày càng phát triển, bảo mật an toàn dữ liệu trong hệ thống mạng ngày càng đóng vai trò quan trọng, khoản chi phí đầu tư không thể thiếu đối với hầu hết tổ chức doanh nghiệp. Báo cáo đề cập đến những công nghệ chung của tường lửa tại các lớp Network, Transport và Application, nghiên cứu triển khai hệ thống VPN và IPS/IDS. Ứng dụng các công nghệ này trên sơ đồ hệ thống mạng trường Đại Học Hoa Sen.

Việc bảo đảm thông tin hoàn toàn bảo mật trên đường truyền là điều không thể, bởi không có giải pháp nào là hoàn hảo trong lĩnh vực bảo mật thông tin, nhất là trong giai đoạn công nghệ kỹ thuật ngày càng phát triển như hiện nay. Phương thức tấn công ngày càng tinh vi, các công cụ mới xâm nhập, đánh cắp dữ liệu ngày càng nhiều và khó phòng chống. Ở đây, nhóm chúng tôi chỉ đưa ra một trong số nhiều lời giải cho bài toán bảo mật hệ thống mạng trường Đại Học Hoa Sen, còn có nhiều cách triển khai khác nhau tùy kiến thức cũng như kinh nghiệm mỗi người. Tuy đây không phải là giải pháp hoàn hảo về mọi mặt nhưng giải pháp này vừa đáp ứng nhu cầu người dùng vừa tận dụng được tối đa tài nguyên hệ thống. Việc thiết kế xây dựng hệ thống VPN cũng như IDS/IPS cũng là điều không thể thiếu đối với các tổ chức doanh nghiệp, góp phần tăng cường an ninh mạng.

Với tốc độ phát triển vượt bậc của khoa học kỹ thuật, việc cập nhật thường xuyên các công nghệ mới phòng chống các cuộc xâm nhập trái phép bảo đảm hệ thống mạng luôn được bảo vệ an toàn. Ngoài ra, cần phải không ngừng hoàn thiện các chính sách bảo mật để duy trì an ninh mạng lâu dài.

Nếu có thêm thời gian cũng như chi phí đầu tư các thiết bị mạng thật, chúng tôi hy vọng có thể nghiên cứu, ứng dụng thêm các công nghệ bảo mật mới. Bởi lẽ, vấn đề bảo mật luôn là đề tài quan tâm hàng đầu của các công ty trong và ngoài nước.



TÀI LIỆU THAM KHẢO

1. Andrew Mason, *CCSP SNAF Quick Reference*, Cisco Press, USA, Dec 2008.
2. Brandon Carroll, *Cisco Access Control Security: AAA Administrative Services*, Cisco Press, USA, May 27, 2004.
3. David Hucaby, *Cisco ASA, PIX, and FWSM Firewall Handbook*, Cisco Press, USA, Aug 2007.
4. *Designing Cisco Network Service Architectures (ARCH) v2.0 Lab Guide*, Cisco Systems, Inc., May 03, 2007.
5. *Designing Cisco Network Service Architectures (ARCH) v2.0 Student Guide*, Cisco Systems, Inc., May 08, 2007.
6. Dr. Thomas W. Shinder, Cherie Amon, Robert J. Shimonski & Debra Littlejohn Shinder, *The Best Damn Firewall Book Period*, Syngress Publishing Inc., United States, 2003.
7. Earl Carter & Jonathan Hogue, *Intrusion Prevention Fundamentals*, Cisco Press, USA, Jan 18, 2006.
8. Edwin Lyle Brown, *802.1x Port-Based Authentication, Auerbach Publication, New York, USA, 2008.*
9. Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, *Building Internet Firewalls Second Edition*, O'Reilly, United States, Jun 2000.
10. *IOS Router: Auth−proxy Authentication Inbound with ACS for IPSec and VPN Client Configuration*, Document ID 14294, Cisco Systems, Inc., Jan 14, 2008.
11. James Henry Carmouche, *IPSec Virtual Private Network*, Cisco Press, USA, Jul 19, 2006.
12. Jazib Frahim & Omar Santos, *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*, Cisco Press, USA, Oct 21, 2005
13. Jeremy Cioara, Michael J. Cavanaugh, Kris A. Krake, *CCNA Voice Official Exam Certification Guide*, Cisco Press, USA, Oct 2004.
14. Jim Geier, *Implementing 802.1X Security Solutions for Wired and Wireless Networks,* Wiley Publishing Inc., Indianapolis, Indiana, 2008.
15. Keith Hutton & Amir Ranjbar, *CCDP Self-Study: Designing Cisco Network Service Architectures (ARCH)*, Cisco Press, USA, 2007.
16. Matt Warnock, *An Evaluation of Firewall Technologies*, Final Term Paper - Bus 503, Jan 02 2005.

17. Ralph Troupe, Vitaly Osipov, Mike Sweeney & Woody Weaver, *Cisco Security Specialist's Guide to PIX Firewall*, Syngress Publishing Inc., United States, 2002.
18. Richard A. Deal, *Cisco ASA Configuration*, The McGraw-Hill Companies, Inc., United States, 2009.
19. Robert Padjen & Todd Lammle, *CCDP: Cisco Internetwork Design Study Guide*, SYBEX Inc., Alameda, CA, 2000.
20. Ryan Lindfield, *CCSP SNAA Quick Reference*, Cisco Press, USA, Feb 2009.
21. *Securing Networks with PIX and ASA (SNPA) Lab Guide*, Cisco System, Inc., May 04 2007.
22. *Securing Networks with PIX and ASA (SNPA) Student Guide*, Cisco System, Inc., May 04, 2007.
23. *Symantec Internet Security Threat Report trends for 2009*, Symantec Corp, April 2010.
24. Wes Noonan & Ido Dubrawsky, *Firewall Fundamentals*, Cisco Press, USA, Jun 02, 2006.