HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Mạnh Hà

GIẢI PHÁP BẢO MẬT THÔNG TIN MẠNG NỘI BỘ TRƯỜNG ĐẠI HỌC HÀ NỘI

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng nghiên cứu/ ứng dụng)

HÀ NỘI - NĂM 2019

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Mạnh Hà

GIẢI PHÁP BẢO MẬT THÔNG TIN MẠNG NỘI BỘ TRƯỜNG ĐẠI HỌC HÀ NỘI

Chuyên nghành : Kỹ thuật Viễn thông

MÃ SỐ: 8.52.02.08

LUẬN VĂN THẠC SĨ KỸ THUẬT
(Theo định hướng nghiên cứu/ ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS NGUYỄN TIẾN BAN

HÀ NỘI – NĂM 2019

LỜI CAM ĐOAN

Tôi cam đoan đề tài: "***Giải pháp bảo mật thông tin mạng nội bộ trường Đại học Hà Nội***" là công trình nghiên cứu của riêng tôi dưới sự hướng dẫn của **PGS.TS Nguyễn Tiến Ban.**

Các kết quả, phân tích, kết luận trong luận văn thạc sỹ này (ngoài phần được trích dẫn) đều là kết quả làm việc của tác giả, các số liệu nêu trong luận văn là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác.

Nếu sai tôi xin hoàn toàn chịu trách nhiệm.

Hà Nội, ngày 16 tháng 11 năm 2019

Tác giả

Nguyễn Mạnh Hà

LỜI CẢM ƠN

Lời đầu tiên cho em xin gửi lời cảm ơn chân thành đến các thầy, cô giáo thuộc Học Viện công nghệ Bưu chính viễn thông, Khoa ĐT sau đại học thuộc Học viện Công nghệ Bưu chính viễn thông đã tận tình giảng dạy, truyền đạt các nội dung kiến thức, kinh nghiệm quý báu trong suốt quá trình em theo học tại Học viện. Với những bài học quý giá, sự kèm cặp, chỉ bảo và truyền thụ tâm huyết của các thầy, cô đã giúp cá nhân em hoàn thiện hơn nữa hệ thống kiến thức chuyên ngành, phục vụ tốt hơn yêu cầu công tác của đơn vị đồng thời nâng cao hơn vốn tri thức của bản thân.

Đặc biệt, em xin gửi lời cảm ơn trân thành tới thầy hướng dẫn khoa học **PGS.TS Nguyễn Tiến Ban**, Khoa ĐT sau đại học thuộc Học viện Công nghệ Bưu chính viễn thông đã tâm huyết, tận tình chỉ bảo, hướng dẫn, cung cấp tài liệu và các nội dung kiến thức quý báu, đồng thời có sự định hướng đúng đắn giúp em hoàn thành được luận văn này.

Em cũng xin được bày tỏ sự cảm ơn sâu sắc tới các đồng nghiệp và tập thể lớp Cao học kỹ thuật viễn thông – Đợt 1 năm 2018 đã đồng hành, khích lệ và chia sẻ trong suốt quá trình học tập.

Trong quá trình thực hiện luận văn, mặc dù bản thân đã cố gắng, chủ động trong việc sưu tầm tài liệu, củng cố kiến thức… tuy nhiên chắc chắn luận văn vẫn còn nhiều thiếu sót. Em rất mong nhận được sự chỉ dạy, đóng góp tận tình của các thầy, cô để luận văn của em được hoàn thiện hơn nữa và có tính ứng dụng cao hơn trong thực tiễn.

Xin trân trọng cảm ơn!

Hà Nội, ngày 16 tháng 11 năm 2019

Học viên

Nguyễn Mạnh Hà

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Tiếng Việt
GPO	Group Policy Object	Công cụ quản lý quyền người dùng
DLP	Data Loss Prevention	Chống mất dữ liệu
DoS	Denial of Service	Tấn công từ chối dịch vụ
IDS	Intrucsion Detection System	Hệ thống phát hiện xâm nhập
IP	Internet Protocol	Giao thức Internet
IPS	Intrusion Prevention Systems	Hệ thống phòng chống xâm nhập
IT	Information Technology	Công nghệ thông tin
LAN	Local Area Network	Mạng nội bộ
NIC	Network Interface Card	Card mạng
SSL	Secure Sockets Layer	Giao thức an ninh thông tin
TCP	Transmission Control Protocol	Giao thức điều khiển truyền thông tin trên Internet
USB	Universal Serial Bus	Thiết bị lưu trữ ngoài
VLAN	Virtual LAN	Mạng LAN ảo
VPN	Virtual Private Network	Hệ thống mạng riêng ảo

DANH MỤC CÁC HÌNH

MỞ ĐẦU

1. Lý do chọn đề tài

Sự phát triển nhanh của công nghệ thông tin và truyền thông dẫn đến nhiều yêu cầu và thách thức mới đặt ra đối với công tác đảm bảo an toàn thông tin và dữ liệu, hiện nay các biện pháp an toàn thông tin cho máy tính cá nhân cũng như các mạng nội bộ đã được nghiên cứu và triển khai. Tuy nhiên vẫn thường xuyên có các hệ thống mạng bị tấn công, có các tổ chức bị đánh cắp thông tin,…gây nên những hậu quả vô cùng nghiêm trọng. Những vụ tấn công nhằm vào tất cả các máy tính của các công ty lớn như AT&T, IBM, các cơ quan nhà nước, các tổ chức, nhà băng,... Không chỉ các vụ tấn công tăng lên nhanh chóng mà các phương pháp tấn công cũng liên tục được hoàn thiện. Tại Việt Nam, các hệ thống mạng và Website bị tấn công theo chiều hướng gia tăng. Đặc biệt, hãng bảo mật Trend Micro gần đây công bố: Việt Nam đang dẫn đầu Đông Nam Á về tấn công mạng với hơn 86 triệu email có nội dung đe dọa được phát hiện trong nửa đầu năm 2018 và Việt Nam nằm trong số 20 nước bị nhiễm mã độc tống tiền nhiều nhất.

Vì vậy, việc kết nối mạng nội bộ của cơ quan tổ chức mình vào mạng Internet mà không có các biện pháp đảm bảo an ninh sẽ dẫn đến nguy cơ mất an toàn thông tin và dữ liệu cao. Để đảm bảo hệ thống mạng nội bộ phục vụ cho nhu cầu công việc, giảng dạy học tập của trường Đại học Hà Nội. Học viên đã quyết định chọn đề tài: “GIẢI PHÁP BẢO MẬT THÔNG TIN MẠNG NỘI BỘ TRƯỜNG ĐẠI HỌC HÀ NỘI”.

2. Tổng quan vấn đề nghiên cứu

Nội dung chính của luận văn này là quá trình nghiên cứu, tìm hiểu để từ đó đúc kết ra được những yếu tố đảm bảo tính bảo mật cho hệ thống mạng LAN:

- Nắm bắt được một số phương pháp tấn công hệ thống mạng thường gặp và các giải pháp bảo mật để có được cách thức phòng chống, cách xử lý sự cố và khắc phục sau sự cố một cách nhanh nhất.

- Đề xuất giải pháp bảo mật cho hệ thống mạng, cách thức triển khai giải pháp.

3. Mục tiêu nghiên cứu của đề tài

Mục tiêu nghiên cứu của luận văn "Nghiên cứu kỹ thuật tấn công mạng LAN và các giải pháp đảm bảo an toàn mạng LAN" và đề xuất giải pháp bảo mật cho mạng nội bộ tại trường Đại Học Đại Hà Nội triển khai áp dụng trong thực tế.

4. Đối tượng và phạm vi nghiên cứu của đề tài

- Đối tượng nghiên cứu của luận văn là mạng LAN và các vấn đề liên quan đến bảo mật mạng LAN.

- Phạm vi nghiên cứu của luận văn là các giải pháp bảo mật mạng LAN và ứng dụng cho mạng nội bộ tại trường Đại học Hà Nội.

5. Phương pháp nghiên cứu của đề tài

- Về mặt lý thuyết: Thu thập, khảo sát, nghiên cứu các tài liệu và thông tin có liên quan đến bảo mật mạng LAN.

- Về mặt thực nghiệm: Khảo sát hệ thống mạng nội bộ Trường Đại học Hà Nội và đề xuất giải pháp bảo mật cho hệ thống mạng.

6. Bố cục luận văn

Luận văn được trình bày trong 3 chương:

Chương 1: TỔNG QUAN VỀ CÁC MỐI ĐE DỌA VÀ PHƯƠNG THỨC TẤN CÔNG MẠNG LAN

Trong chương đầu tiên này luận văn nghiên cứu các nguy cơ đe dọa bảo mật và phương thức tấn công mạng LAN, đề xuất các yêu cầu bảo mật đối với mạng LAN và các vấn đề bảo mật mạng LAN trong thực tế.

Chương 2*:* NGHIÊN CỨU CÁC GIẢI PHÁP BẢO MẬT CHO MẠNG LAN

Trong chương 2 luận văn nghiên cứu các giải pháp bảo mật mạng LAN nhằm đáp ứng các yêu cầu về bảo mật mạng, bảo mật dữ liệu và bảo mật người dùng.

Chương 3: ĐỀ XUẤT CÁC GIẢI PHÁP BẢO MẬT CHO MẠNG NỘI BỘ TẠI TRƯỜNG ĐẠI HỌC HÀ NỘI.

Chương này luận văn sẽ nghiên cứu về hệ thống mạng nội bộ của trường Đại Học Hà Nội và đề xuất ứng dụng một số giải pháp bảo mật hệ thống mạng LAN đã nghiên cứu trong chương 2 cho hệ thống mạng nội bộ của trường Đại học Hà Nội.

• Khảo sát thực trạng mạng nội bộ trường Đại học Hà Nội

- Mô hình kiến trúc mạng

- Yêu cầu sử dụng

• Đề xuất giải pháp bảo mật cho hệ thống mạng nội bộ trường Đại học Hà Nội

- Giải pháp mạng

+ Sử dụng Firewall cứng để bảo vệ.

+ Chia hệ thống thành các khu vực: LAN, WAN, DMZ.

(Khu vực DMZ sẽ đặt các máy chủ: Web, Mail, File và Phần mềm. Khu vực LAN sẽ sử dụng Switch layer 3 cấu hình VLAN, tách các phòng ban, các tầng ra riêng biệt).

- Giải pháp an toàn dữ liệu

+ Phân quyền truy cập dữ liệu.

+ Backup File Server.

+ Cài đặt phần mềm diệt virus bản quyền trên Server

- Thử nghiệm và đánh giá một số bảo mật đề xuất

Chương 1. TỔNG QUAN VỀ CÁC MỐI ĐE DỌA VÀ PHƯƠNG THỨC TẤN CÔNG MẠNG LAN

Trong chương đầu tiên này luận văn nghiên cứu các nguy cơ đe dọa bảo mật và phương thức tấn công mạng LAN, đề xuất các yêu cầu bảo mật đối với mạng LAN và các vấn đề bảo mật mạng LAN trong thực tế.

1.1. Các yêu cầu bảo mật chung cho mạng LAN

1.1.1. Yêu cầu bảo mật về mạng

Trong vận hành và khai thác mạng LAN sẽ phát sinh các nguy cơ an ninh mạng ngày càng lớn. Không chỉ các kẻ tấn công khám phá ra nhiều lỗ hổng bảo mật mà các công cụ và các kỹ thuật cần thiết để xâm nhập vào một mạng cũng càng trở nên đơn giản hơn. Có sẵn những công cụ được tải về trên Internet cho phép những người không có nhiều kiến thức về mạng cũng có thể thực hiện các cuộc tấn công. Ngoài ra, việc thiết kế, cài đặt sử dụng các tài nguyên mạng không đúng cách cũng góp phần tại ra các lỗ hổng trên mạng cho phép những người có ý đồ xấu có thể xâm nhập vào hệ thống, thực hiện các thao tác phá hoại.

Cùng với sự phát triển của thời gian, các công cụ cho phép tấn công vào mạng ngày càng trở nên phức tạp, khó lường. Một người có thể không có nhiều kiến thức về mạng cũng có thể thực hiện một cuộc tấn công thông qua một công cụ được tải về từ mạng Internet.

Bảo mật và an ninh mạng đã trở thành vấn đề ưu tiên hàng đầu trong thiết kế quản lý và vận hành mạng nhằm đảm bảo các các yêu cầu sau:

- Yêu cầu về tính sẵn sàng của mạng: Mạng phải đảm bảo luôn sẵn sàng cung cấp các dịch vụ cho người dùng mọi lúc, mọi nơi.

- Yêu cầu về tính bền vững của mạng: Trong môi trường đầy những nguy cơ mất an toàn mạng do người dùng giao tiếp với nhiều mạng công cộng và các hệ thống khác nhau, mạng phải chống được các cuộc tấn công mạng như DoS, DDoS, ….

- Yêu cầu về độ tin cậy mạng: Trong quá trình hoạt động, mạng phải đảm bảo các truy cập của người dùng là hợp pháp, tránh các rủi ro làm ảnh hưởng đến an toàn mạng.

Để đáp ứng các yêu cầu trên, thông thường chu trình bảo mật mạng gồm bốn giai đoạn: Bảo mật an ninh mạng *(Secure);* giám sát *(Monitor)*; kiểm tra các lỗ hổng trên mạng (*Test*); cải tiến (*Improve*). Xuyên suốt bốn giai đoạn này là quá trình áp dụng các chính sách an ninh (*Security Policy*).

Chính sách an ninh được xem là các luật lệ chính thức được áp dụng trong mạng qua đó bất kỳ ai khi truy nhập vào mạng đó cũng phải tuân theo. Hay nói cách khác, chính sách bảo mật là một văn bản tổng kết các cách thức mà một tổ chức, một doanh nghiệp, một cá nhân sẽ sử dụng nhằm bảo vệ tài nguyên mạng của mình.

Bốn giai đoạn của chu trình bảo mật mạng được mô tả như sau:

Giai đoạn bảo vệ an ninh mạng: Là một phần trong các hoạt động quản trị mạng của doanh nghiệp. Giai đoạn này là quá trình thiết lập các giải pháp an ninh mạng nhằm ngăn chặn, phòng ngừa các hành động tấn công, các truy nhập trái phép. Có thể đó chỉ là một hoạt động đơn giản như cấu hình bộ định tuyến (*router*) không chấp nhận các dịch vụ, các truy nhập từ các địa chỉ không được chứng thực hay phức tạp hơn là cấu hình các bức tường lửa (*Firewall*), các hệ thống chứng thực (*authentication*), mã hóa (*encryption*)… Các thao tác cài đặt, cấu hình này sẽ tuân theo các chính sách an ninh mà doanh nghiệp lập ra. Các phương pháp sau thường được sử dụng nhằm thiết lập bảo vệ an ninh mạng:

- Chứng thực: Là quá trình công nhận các cá nhân được quyền sử dụng từng loại hình dịch vụ của mạng qua các dấu hiệu nhận dạng của cá nhân.

- Mã hóa: Là phương pháp nhằm đảm bảo truyền dữ liệu an toàn, tin cậy, toàn vẹn, chính xác qua mạng. Dữ liệu trước khi gửi đi được mã hóa theo một thuật toán nào đó và chỉ có bên nhận mới có thể giải mã được.

- Xây dựng tường lửa: Tường lửa là một tập hợp các chương trình liên kết với nhau, được đặt tại các cửa ngõ vào/ra của mạng với chức năng bảo vệ các tài nguyên của mạng trước các truy nhập từ bên ngoài.

- Thực hiện "vá lỗi" (*vulnerability patching*): là quá trình thực hiện xác minh và khắc phục các lỗ hổng của mạng thông qua việc bổ sung các "bản vá", là các phần mềm có tính năng che lấp lỗ hổng của mạng.

Giai đoạn giám sát mạng: Sau khi đã thiết lập nên một hệ thống bảo vệ an ninh mạng, điều cần thiết phải giám sát, theo dõi hoạt động của hệ thống bảo vệ an ninh mạng trước các truy nhập từ bên ngoài vào mạng, nhằm bảo đảm mạng vẫn còn được bảo vệ an toàn. Đây là quá trình phát hiện các vi phạm đối với chính sách bảo mật, phát hiện xâm nhập và kiểm soát hệ thống, xác nhận các thao tác thực hiện bảo vệ an ninh mạng trong giai đoạn 1.

Giai đoạn kiểm tra an ninh mạng: Sự phát triển của công nghệ kéo theo những thay đổi không ngừng về cách thức tấn công xâm nhập mạng. Giai đoạn này tìm kiếm những bất hợp lý trong việc xây dựng chính sách và hệ thống bảo vệ mạng trước đó, tìm ra các điểm yếu mới của mạng mà các giai đoạn trước không nhận ra thông qua các hành động tấn công thử vào các điểm bảo mật của mạng.

Giai đoạn cải tiến: Các giai đoạn giám sát và kiểm tra cung cấp các thông tin cần thiết để tiến hành nâng cấp, cải tiến mức độ bảo vệ an ninh mạng. Các nhà quản trị mạng sử dụng các thông tin này cải tiến các giải pháp bảo vệ, điều chỉnh các chính sách an ninh, bổ sung các điểm yếu trên mạng nhằm đối phó với các nguy cơ mới.

Sau khi đã đưa ra những cải tiến, chu trình lại tiếp tục với giai đoạn bảo vệ an ninh mạng với sự bổ sung mới. Chu trình được tiến hành liên tục nhằm đảm bảo rằng mạng được bảo vệ một cách an toàn nhất.

1.1.2. Yêu cầu về bảo mật dữ liệu

Trong mạng LAN, người dùng thường xuyên truy cập các cơ sở dữ liệu để làm việc nên dễ xảy ra các nguy cơ mất an toàn dữ liệu. Vì vậy, vấn đề bảo mật dữ

liệu phải đảm bảo các yêu cầu sau:

- Yêu cầu về tính sẵn sàng của dữ liệu: Các dữ liệu dùng chung phải luôn trong trạng thái đáp ứng mọi yêu cầu của người dùng mọi lúc, mọi nơi.
- Yêu cầu về tính toàn vẹn dữ liệu: Các dữ liệu không bị chỉnh sửa, thay đổi một cách bất hợp pháp.
- Yêu cầu về bí mật dữ liệu: Các dữ liệu là tài sản quan trọng của đơn vị và cá nhân phải được đảm bảo bí mật, không bị phát tán bất hợp pháp.

1.1.3. Yêu cầu về bảo mật người dùng

Người dùng hợp pháp của mạng LAN là người sử dụng các dịch vụ nhưng đồng thời cũng là một tác nhân gây ra các rủi ro mạng.

Vì vậy, vấn đề bảo mật người dùng phải đảm bảo các yêu cầu sau:

- Yêu cầu về tính hợp pháp: Người dùng hợp pháp phải được đảm bảo truy cập mạng một cách thuận lợi, đáp ứng mọi yêu cầu hợp pháp của người dùng mọi lúc, mọi nơi.
- Yêu cầu về tính riêng tư: Các thông tin cá nhân, lịch sử truy cập mạng là các thông tin riêng tư của người dùng phải được đảm bảo bí mật, không bị đánh cắp hoặc phát tán bất hợp pháp.

Các yêu cầu bảo mật mạng LAN, về mạng, về dữ liệu và người dùng đều có tầm quan trọng và phải được xem xét thấu đáo trong quá trình xây dựng, thiết kế, vận hành và khai thác mạng nội bộ.

1.2. Tình hình triển khai mạng LAN tại Việt Nam và các vấn đề liên quan đến bảo mật mạng LAN trong thực tế.

1.2.1. Tình hình triển khai mạng LAN tại Việt Nam

Ngày nay ở Việt Nam, các tổ chức, doanh nghiệp đều sử dụng, triển khai mạng LAN bên trong hệ thống của họ. Hệ thống mạng nội bộ giúp gia tăng khả năng trao đổi dữ liệu giữa các nhân viên, các ban ngành với nhau, làm gia tăng khả năng làm việc và hoạt động một cách hiệu quả. Tuy nhiên, với nhu cầu trao đổi thông tin, bắt buộc các cơ quan, tổ chức phải kết nối tới mạng Internet. Khi thực hiện kết nối mạng nội bộ của cơ quan, doanh nghiệp, tổ chức với mạng toàn cầu, an

toàn và bảo mật thông tin là một vấn đề cấp bách được đặt ra. Internet có những kỹ thuật cho phép mọi người truy cập, khai thác và chia sẻ thông tin với nhau. Nhưng nó cũng là nguy cơ chính dẫn đến thông tin dễ bị hư hỏng hay bị phá hủy hoàn toàn. Sở dĩ có lí do đó là vì việc truyền thông tin qua mạng Internet hiện nay chủ yếu sử dụng giao thức TCP/IP. TCP/IP cho phép các thông tin từ máy tính này tới máy tính khác phải đi qua một loạt các máy tính trung gian hoặc các mạng riêng biệt trước khi nó tới được đích. Chính vì vậy, giao thức TCP/IP đã tạo cơ hội cho bên thứ ba có thể thực hiện các hành động gây mất an toàn thông tin trong khi thực hiện việc truyền thông tin trên mạng. Thực tế, số vụ tấn công từ bên ngoài vào các cơ quan, tổ chức, trường học,.. đang ngày một tăng lên với quy mô khổng lồ. Nếu chúng ta không có các giải pháp phòng chống và khắc phục, hậu quả và tổn thất sẽ vô cùng nặng nề.

1.2.2. Vấn đề liên quan đến bảo mật mạng LAN trong thực tế

Việt Nam lọt vào top 20 quốc gia có số lượng website bị tấn công lớn nhất thế giới trong quý 3 năm 2018, theo Báo cáo an ninh website quý 3 năm 2018 bởi CyStack. Ở vị trí thứ 19, Việt Nam có 1.183 website bị tấn công, trong đó website doanh nghiệp là đối tượng của đại đa số các tin tặc. Cụ thể, 71,51% số cuộc tấn công nhằm vào các website doanh nghiệp, theo sau bởi website thương mại điện tử với 13,86%.

Theo báo cáo an ninh mạng của Bkav, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017. Đây là kết quả được đưa ra từ chương trình đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện tháng 12/2018.

Trên phạm vi toàn cầu, tội phạm mạng gây thiệt hại lên tới khoảng 600 tỷ USD mỗi năm, tương đương 0,8% GDP toàn cầu. Trong đó, khu vực Đông Á thiệt hại ước tính từ 120 – 200 tỷ USD, tương đương 0,53 – 0,89% GDP khu vực. Mức

thiệt hại 642 triệu USD tương đương 0,26% GDP của Việt Nam tuy chưa phải cao so với khu vực và thế giới, nhưng cũng là kỷ lục đáng báo động.

Phân tích tình trạng mã độc đào tiền ảo tràn lan, theo các chuyên gia của Bkav, nguyên nhân chính là do các cơ quan, doanh nghiệp chưa trang bị giải pháp diệt virus tổng thể, đồng bộ cho tất cả các máy tính trong mạng nội bộ. Do đó, chỉ cần một máy tính trong mạng bị nhiễm mã độc, toàn bộ các máy tính khác trong cùng mạng sẽ bị mã độc tấn công, lây nhiễm. Ngoài việc làm chậm máy, mã độc đào tiền ảo còn có khả năng cập nhật và tải thêm các mã độc khác nhằm xoá dữ liệu, ăn cắp thông tin cá nhân hay thậm chí thực hiện tấn công có chủ đích APT.

Hai dòng mã độc phổ biến tại Việt Nam khiến người dùng bị mất dữ liệu là dòng mã độc mã hóa tống tiền ransomware và dòng virus xóa dữ liệu trên USB. Các mã độc mã hóa tống tiền lây chủ yếu qua email, tuy nhiên có tới 74% người dùng tại Việt Nam vẫn giữ thói quen mở trực tiếp file đính kèm từ email mà không thực hiện mở trong môi trường cách ly an toàn Safe Run, điều này rất nguy hiểm. Trong khi đó, do USB là phương tiện trao đổi dữ liệu phổ biến nhất tại Việt Nam nên số máy tính bị nhiễm mã độc lây qua USB luôn ở mức cao. Thống kê của Bkav cho thấy, có tới 77% USB tại Việt Nam bị nhiễm mã độc ít nhất 1 lần trong năm.

Tấn công nhằm vào lĩnh vực tài chính: Theo ghi nhận của hãng bảo mật Kaspersky (Nga), trong Quý II/2018 đã có hơn 107 triệu cuộc tấn công dạng lừa đảo trực tuyến đã xảy ra. Đáng lưu ý, có tới 35,7% số cuộc tấn công nhắm đến các dịch vụ tài chính. Những cuộc tấn công nhắm vào khách hàng của các tổ chức tài chính như ngân hàng, hệ thống thanh toán và các giao dịch mua bán trực tuyến là một xu hướng lâu dài đối với tội phạm mạng.

Bằng cách tạo ra các trang web giả mạo ngân hàng, trang thanh toán trực tuyến hoặc các trang mua sắm, tin tặc có thể thu thập được các thông tin cá nhân của người dùng như tên, mật khẩu, địa chỉ email, số điện thoại, số thẻ tín dụng và mã PIN mà người dùng không hề hay biết. Các cuộc tấn công mạng nhắm vào lĩnh vực tài chính chiếm hơn 1/3 tổng số các cuộc tấn công trong quý II/2018, cụ thể, các cuộc tấn công nhắm vào các ngân hàng chiếm 21,1%; các cửa hàng trực tuyến

là 8,17% và 6,43% nhắm vào hệ thống thanh toán. Những báo cáo đã đưa ra một bức tranh về tình hình bất ổn của an ninh mạng năm 2018. Cùng với quá trình đẩy mạnh ứng dụng CNTT và hướng tới thế giới kết nối IoT, xu hướng gia tăng tấn công mạng là tất yếu. Bởi vậy, dự đoán được các nguy cơ về ATTT để có biện pháp phòng ngừa phù hợp là trách nhiệm của chủ sở hữu và quản lý các hệ thống thông tin.

Các dạng tấn công hiện nay rất đa dạng. Có thể liệt kê một số như: mã độc tống tiền, tấn công các lỗ hổng hệ thống website, tấn công đánh cắp dữ liệu,… So với các năm trước thì tội phạm mạng tấn công ngày càng thông minh và tinh vi hơn, có sự chuẩn bị với thời gian dài , mức độ nguy hiểm không chỉ đánh cắp thông tin mà còn mang tính phá hủy dữ liệu, lừa đảo, tống tiền người dùng. Hiện nay, an toàn thông tin trên thế giới cũng như ngay tại Việt Nam có những diễn biến phức tạp, các vụ tấn công mạng không chỉ đe dọa trực tiếp đến hoạt động và tài sản của cá nhân, doanh nghiệp mà còn ảnh hưởng đến cả hệ thống hạ tầng mạng của cả một quốc gia. Từ tình hình trên, việc đảm bảo an toàn thông tin cũng như xây dựng hệ thống có tính bảo mật cao cho mạng LAN tại Việt Nam và trên toàn thế giới đang ngày càng trở nên cấp thiết hơn bao giờ hết.

1.3. Các mối đe dọa bảo mật và phương thức tấn công mạng LAN

Trong quá trình vận hành và khai thác mạng LAN, trong môi trường Internet có rất nhiều nguy cơ đe dọa bảo mật mạng. Dưới đây, luận văn liệt kê một số mối đe dọa và phương thức tấn công điển hình đối với bảo mật mạng LAN.

1.3.1. Các mối đe dọa bảo mật mạng LAN

Mối đe dọa không có cấu trúc (Untructured threat) thường là những hành vi xâm nhập mạng trái phép một cách đơn lẻ, không có tổ chức. Công cụ hack và script có rất nhiều trên Internet, vì thế bất cứ ai tò mò có thể tải chúng về và sử dụng thử trên mạng nội bộ. Cũng có những người thích thú với việc xâm nhập vào máy tính và có các hành động vượt khỏi tầm bảo vệ. Hầu hết tấn công không có cấu trúc đều được gây ra bởi Script Kiddies (những kẻ tấn công chỉ sử dụng các công cụ

được cung cấp, không có hoặc có ít khả năng lập trình) hay những người có trình độ vừa phải. Hầu hết các cuộc tấn công đó vì sở thích cá nhân, nhưng cũng có nhiều cuộc tấn công có ý đồ xấu. Những trường hợp đó sẽ có ảnh hưởng xấu đến hệ thống và hình ảnh của các chủ thể sở hữu mạng LAN. Đôi khi, chỉ cần chạy một đoạn mã độc là có thể phá hủy chức năng của mạng LAN.

Mối đe dọa có cấu trúc (Structured threat) là các hành động xâm nhập mạng trái phép cố ý, có động cơ và kỹ thuật cao. Những kẻ tấn công này hoạt động độc lập hoặc theo nhóm. Họ có kỹ năng phát triển và sử dụng các kỹ thuật hack phức tạp nhằm xâm nhập vào mục tiêu, động cơ của các cuộc tấn công này thì có rất nhiều. Một số yếu tố thường thấy có thể vì tiền, hoạt động chính trị, tức giận hay báo thù. Các tổ chức tội phạm, các đối thủ cạnh tranh hay các tổ chức sắc tộc có thể thuê các chuyên gia để thực hiện các cuộc tấn công dạng structured threat. Các cuộc tấn công này thường có mục đích từ trước, như để lấy được mã nguồn của đối thủ cạnh tranh.

Cho dù động cơ là gì, thì các cuộc tấn công như vậy có thể gây hậu quả nghiêm trọng cho mạng LAN. Một cuộc tấn công structured thành công có thể gây nên sự phá hủy cho toàn hệ thống mạng LAN.

Mối đe dọa từ bên ngoài (External threat) là các cuộc tấn công được tạo ra khi không có một quyền nào trong hệ thống. Người dùng trên toàn thế giới thông qua Internet đều có thể thực hiện các cuộc tấn công như vậy vào mạng LAN, mối đe dọa từ bên ngoài là mối đe dọa mà các chủ sở hữu mạng LAN thường phải bỏ nhiều tiền và thời gian để ngăn ngừa.

Mối đe dọa từ bên trong (Internal threat) được sử dụng để mô tả một kiểu tấn công được thực hiện từ một người hoặc một tổ chức có một vài quyền truy cập mạng LAN. Các cách tấn công từ bên trong được thực hiện từ một khu vực được tin cậy trong mạng. Mối đe dọa này có thể khó phòng chống hơn vì các nhân viên có thể truy cập mạng và dữ liệu bí mật của công ty. Mối đe dọa ở bên trong thường được thực hiện bởi các nhân viên bất bình, muốn “quay mặt” lại với công ty. Đôi

khi các cuộc tấn công dạng có cấu trúc vào hệ thống được thực hiện với sự giúp đỡ của người bên trong hệ thống.

1.3.2. Các phương thức tấn công mạng LAN

Phương thức ăn cắp thông tin bằng Packet Sniffers

Đây là một chương trình ứng dụng bắt giữ được tất cả các các gói lưu chuyển trên mạng (trên một collision domain). Sniffer thường được dùng cho troubleshooting network hoặc để phân tích traffic. Tuy nhiên, do một số ứng dụng gởi dữ liệu qua mạng dưới dạng clear text (telnet, FTP, SMTP, POP3,...) nên sniffer cũng là một công cụ cho hacker để bắt các thông tin nhạy cảm như là username, password, và từ đó có thể truy xuất vào các thành phần khác của mạng.

Phương thức tấn công mật khẩu Password Attack

Các hacker tấn công password bằng một số phương pháp như: brute-force attack, chương trình Trojan Horse, IP spoofing và packet sniffer. Mặc dù dùng packet sniffer và IP spoofing có thể lấy được user account và password, nhưng hacker lại thường sử dụng brute-force để lấy user account hơn.

Tấn công brute-force được thực hiện bằng cách dùng một chương trình chạy trên mạng, cố gắng login vào các phần share trên server bằng phương pháp “thử và sai” passwork.

Phương thức tấn công bằng Mail Relay

Đây là phương pháp phổ biến hiện nay. Email server nếu cấu hình không chuẩn hoặc Username/ password của user sử dụng mail bị lộ. Hacker có thể lợi dụng email server để gửi mail gây ngập mạng , phá hoại hệ thống email khác. Ngoài ra với hình thức gắn thêm các đoạn script trong mail hacker có thể gây ra các cuộc tấn công Spam cùng lúc với khả năng tấn công gián tiếp đến các máy chủ Database nội bộ hoặc các cuộc tấn công DoS vào một mục tiêu nào đó.

Phương thức tấn công lớp ứng dụng

Tấn công lớp ứng dụng được thực hiện bằng nhiều cách khác nhau. Một trong những cách thông dụng nhất là tấn công vào các điểm yếu của phần mềm như sendmail, HTTP, hay FTP. Nguyên nhân chủ yếu của các tấn công lớp ứng dụng này là chúng sử dụng những port cho qua bởi firewall. Ví dụ các hacker tấn công Web server bằng cách sử dụng TCP port 80, mail server bằng TCP port 25.

Phương thức tấn công Virus và Trojan Horse

Các nguy hiểm chính cho các workstation và end user là các tấn công virus và ngựa thành Trojan (Trojan horse). Virus là một phần mềm có hại, được đính kèm vào một chương trình thực thi khác để thực hiện một chức năng phá hại nào đó. Trojan horse thì hoạt động khác hơn. Một ví dụ về Trojan horse là một phần mềm ứng dụng để chạy một game đơn giản ở máy workstation. Trong khi người dùng đang mãi mê chơi game, Trojan horse sẽ gởi một bản copy đến tất cả các user trong address book. Khi user khác nhận và chơi trò chơi, thì nó lại tiếp tục làm như vậy, gởi đến tất cả các địa chỉ mail có trong address book của user đó.

1.4. Giải pháp phòng chống chung

Để phòng chống tấn công mạng, người dùng cần thực hiện nhiều biện pháp phòng thủ, bảo vệ và đồng thời nâng cao hiểu biết về cách sử dụng internet an toàn. Những phương pháp chống lại tấn công mạng được tổng hợp dưới đây:

Sử dụng một phần mềm diệt virus/malware uy tín.

Bảo vệ các mật khẩu của mình bằng cách sử dụng xác thực 2 bước khi đăng nhập; đặt mật khẩu khó (bao gồm chữ in hoa, số và ký tự đặc biệt)

Không nên sử dụng các thiết bị ngoại vi không rõ nguồn gốc (USB, ổ đĩa cứng, đĩa CD). Nếu bắt buộc phải sử dụng, hãy quét virus trước.

Không nên click vào đường link lạ, trang web đáng ngờ, không tải file đính kèm không rõ nguồn gốc.

Nâng cấp, cập nhật các phần mềm, hệ điều hành, công cụ thường xuyên.

Đối với doanh nghiệp, cần xây dựng một chiến lược tổng thể để phòng chống những cuộc tấn công mạng phức tạp có thể xảy ra.

1.5. Kết luận chương 1

Với xu hướng phát triển của các công nghệ mạng và Internet, tình hình mất an ninh mạng đang diễn biến phức tạp và xuất hiện nhiều nguy cơ đe dọa nghiêm trọng đến việc ứng dụng công nghệ thông tin phục vụ phát triển kinh tế xã hội và đảm bảo quốc phòng, an ninh. Số vụ tấn công trên mạng và các vụ xâm nhập hệ thống công nghệ thông tin nhằm do thám, trục lợi, phá hoại dữ liệu, ăn cắp tài sản, cạnh tranh không lành mạnh và một số vụ việc mất an toàn thông tin đang gia tăng ở mức báo động về số lượng, đa dạng về hình thức, tinh vi về công nghệ...Tấn công mạng đang dần trở nên phổ biến nhất là trong bối cảnh Việt Nam lọt vào top 20 quốc gia có số lượng website bị tấn công lớn nhất thế giới trong quý 3 năm 2018. Việc triển khai giải pháp bảo mật cho hệ thống mạng nội bộ mang tính cấp thiết.

Trong chương 1, luận văn đã nghiên cứu tổng quan về các nguy cơ đe dọa bảo mật và tấn công mạng LAN. Từ đó đã đưa ra các yêu cầu bảo mật cho mạng LAN, cũng như các vấn đề liên quan đến bảo mật mạng LAN trong thực tế.

Trên cơ sở các nội dung đã trình bày trong chương 1, các giải pháp bảo mật mạng LAN đáp ứng các yêu cầu đề ra sẽ được nghiên cứu trong chương 2 của luận văn.

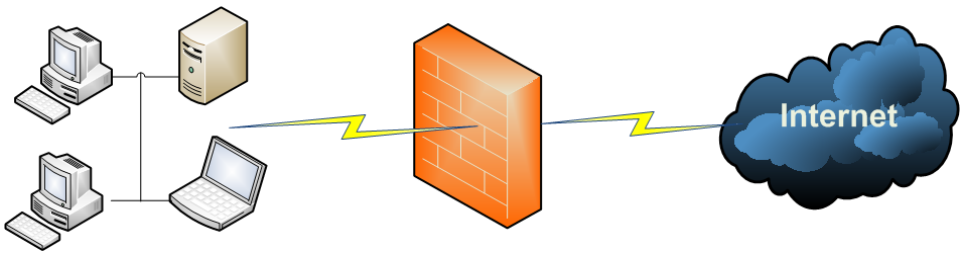
Chương II: NGHIÊN CỨU CÁC GIẢI PHÁP BẢO MẬT CHO MẠNG LAN

Trong chương 2 luận văn nghiên cứu các giải pháp bảo mật cho mạng LAN nhằm đáp ứng các yêu cầu về bảo mật mạng, bảo mật dữ liệu và bảo mật người dùng.

2.1. Giải pháp sử dụng hệ thống tường lửa

2.1.1. Giới thiệu chung

Một trong các giải pháp bảo mật mạng LAN nhằm tránh các cuộc tấn công từ bên ngoài hay ngăn chặn truy cập các trang web từ bên trong là sử dụng tường lửa (Firewall).



Hình 2. 1: Firewall bảo mật mạng LAN[14]

Tường lửa (firewall) là rào chắn mà các tổ chức, doanh nghiệp, cơ quan nhà nước, hay cá nhân lập ra nhằm ngăn chặn các truy cập thông tin không mong muốn từ ngoài vào hệ thống mạng nội bộ, cũng như ngăn chặn các thông tin bảo mật nằm trong mạng nội bộ xuất ra ngoài Internet mà không được cho phép.

Firewall là một công cụ hoạt động ở ranh giới giữa bên trong là mạng LAN với hệ thống Internet bên ngoài. Firewall cung cấp cơ chế phòng thủ từ vành đai, nó hạn chế việc truyền thông của hệ thống với những kẻ xâm nhập tiềm tàng và làm giảm rủi ro cho hệ thống. Đây là một công cụ không thể thiếu trong một giải pháp bảo mật tổng thể.

Nhiệm vụ cơ bản của tường lửa là kiểm soát truyền thông dữ liệu giữa hai vùng có độ tin cậy khác nhau. Các vùng tin cậy (zone of trust) điển hình bao gồm:

mạng Internet (vùng không đáng tin cậy) và mạng LAN (một vùng có độ tin cậy cao). Mục đích cuối cùng là cung cấp kết nối có kiểm soát giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc quyền tối thiểu (principle of least privilege).

Tường lửa là một thiết bị phần cứng hoặc một phần mềm. Cấu hình đúng đắn cho các tường lửa đòi hỏi kỹ năng của người quản trị hệ thống. Việc này yêu cầu hiểu biết đáng kể về các giao thức mạng và về an ninh máy tính. Những lỗi nhỏ có thể biến tường lửa thành một công cụ an ninh vô dụng.

Có hai loại tường lửa thông dụng là tường lửa bảo vệ, để bảo vệ an ninh cho máy tính cá nhân hay mạng cục bộ, tránh sự xâm nhập, tấn công từ bên ngoài. Tường lửa ngăn chặn thường do các nhà cung cấp dịch vụ Internet thiết lập và có nhiệm vụ ngăn chặn không cho máy tính truy cập một số trang web hay máy chủ nhất định, thường dùng với mục đích kiểm duyệt Internet.

Trên thị trường có rất nhiều loại Firewall nhưng hiện nay Firewall cứng Cisco đang được các doanh nghiệp tin dùng vì có khả năng bảo mật mạnh cũng như dễ dàng sử dụng. Dưới đây, luận văn sẽ khảo sát chi tiết về hệ thống Firewall cứng Cisco.

2.1.2. Tường lửa Cisco

2.1.2.1. Tổng quan về tường lửa của Cisco:

Cisco ASA Firewalls đã luôn luôn đóng vai trò quan trọng trong chiến lược bảo mật của Cisco.Các mô hình tường lửa khác nhau của Cisco cung cấp các giải pháp bảo mật cho các doanh nghiệp vừa và nhỏ.

Các sản phẩm tường lửa trước đây của Cisco bao gồm:

- Cisco PIX Firewalls.
- Cisco FWSM(Firewall Service Module)
- Cisco IOS Firewall.

ASA/PIX firewall là một yếu tố chính trong toàn bộ giải pháp an ninh end-to-end của Cisco. ASA/PIX Firewall là một giải pháp an ninh phần cứng và phần

mềm chuyên dụng và mức độ bảo mật cao hơn mà không ảnh hưởng đến sự thực thi của hệ thống mạng. Nó là một hệ thống được lai ghép bởi vì nó sử dụng cả hai kỹ thuật packet filtering và proxy server.

ASA/PIX Firewall cung cấp các đặc tính và các chứ năng sau:

- Apdaptive Security Algorithm (ASA) – thực hiện việc điều khiển các kết nối stateful thông qua ASA/PIX Firewall
- Cut – through proxy – Một người sử dụng phải dựa trên phương pháp chứng thực của các kết nối vào và ra cung cấp một hiệu suất cải thiện khi so sánh nó với proxy server
- Stateful failover – ASA/PIX Firewall cho phép bạn cấu hình hai thiết bị ASA/PIX Firewall trong một topo mạng nhằm đảm bảo tính dự phòng.
- Stateful packet filtering – Một phương pháp bảo mật phân tích các gói dữ liệu mà thông tin nằm trải rộng sang một bảng. Để một phiên được thiết lập thông tin về các kết nối phải kết hợp được với thông tin trong bảng

ASA/PIX Firewall có thể vận hành và mở rộng cấp độ được với các ISPes, các ISPec bao gồm một lưới an ninh và các giao thức chứng thực như là internet Key Exchange (IKE) và Public Key Infrastructure (PKI). Các máy clients ở xa có thể truy cập một cách an toàn đến mạng của công ty thông qua các ISPs của họ.

2.1.2.2. Nguyên tắc hoạt động của tường lửa Cisco

Nguyên tắc chung của firewall (kể cả firewall dạng phần mềm như proxy hay dạng thiết bị cứng như là ASA/PIX) là bắt gói dữ liệu đi ngang qua nó và so sánh với các luật đã thiết lập. Nếu thấy không vi phạm luật nào thì cho đi qua, ngược lại thì hủy gói dữ liệu. ASA/PIX firewall hoạt động dựa trên giải thuật bảo mật thích hợp ASA (Adaptive Security Algorithm) sử dụng Security level (cấp độ bảo mật). Giữa hai cổng thì một sẽ có Security level cao hơn, một có Security level thấp hơn.

Vấn đề cốt lõi của các thiết bị an ninh là thuật toán bảo mật thích hợp (Adaptive Security Algorithm - ASA). Giải thuật ASA duy trì vành đai an toàn giữa các mạng điều khiển bởi thiết bị an ninh. ASA tuân theo các quy luật sau:

- Không gói tin nào đi qua ASA/PIX mà không có một kết nối và trạng thái.

- Cho phép các kết nối ra bên ngoài, trừ những kết nối bị cấm bởi danh sách điều khiển truy nhập ACLs. Một kết nối ra bên ngoài có thể là một nguồn hoặc một client ở cổng có mức bảo mật cao hơn nơi nhận hoặc server. Cổng có mức bảo mật cao nhất là inside với giá trị là 100, cổng có mức bảo mật thấp nhất là outside với giá trị là 0. Bất kỳ cổng nào khác cũng có thể có mức bảo mật nhận giá trị từ 1 đến 99.

- Cấm các kết nối vào bên trong, ngoại trừ những kết nối được phép. Một kết nối vào bên trong là một nguồn hoặc client ở cổng hay mạng có mức bảo mật thấp hơn nơi nhận hoặc server.

- Tất cả các gói ICMP đều bị cấm, trừ những gói được phép

- Mọi sự thử nghiệm nhằm phá vỡ các quy tắc trên đều bị hủy bỏ

Trên mỗi cổng của ASA/PIX có các cấp độ bảo mật (Security-level), xác định một giao tiếp (interface) là tin cậy, được bảo vệ hay không tin cậy, được bảo vệ ít và tương quan với các giao tiếp khác như thế nào. Một giao tiếp được xem là tin cậy trong mối quan hệ với các giao tiếp khác nếu nó có mức độ bảo mật cao hơn.

Quy tắc cơ bản về mức độ bảo mật là: Dữ liệu có thể đi vào ASA/PIX thông qua một interface với Security level cao hơn, đi qua ASA/PIX và đi ra ngoài thông qua interface có Security level thấp hơn. Ngược lại, dữ liệu đi vào interface có Security level thấp hơn không thể đi qua ASA/PIX và đi ra ngoài thông qua interface có Security level cao hơn nếu trên ASA/PIX không có cấu hình conduit hoặc access-list để cho phép nó thực hiện điều này. Các mức bảo mật đánh số từ 0 đến 100.

- Mức 0: Là mức thấp nhất, thiết lập mặc định cho outside interface (cổng ra) của ASA/PIX, thường dành cho cổng kết nối ra internet. Vì 0 là mức bảo mật ít an toàn nhất nên các untrusted network thường ở sau interface này. Các thiết bị ở outside chỉ được phép truy nhập vào ASA/PIX khi nó được cấu hình để làm điều đó.

- Mức 100: Là mức cao nhất cho một interface. Nó được sử dụng cho inside interface (cổng vào) của ASA/PIX, là cấu hình mặc định cho ASA/PIX và không thể thay đổi. Vì vậy mạng của tổ chức thường ở sau interface này, không ai có thể truy nhập vào mạng này trừ khi được phép thực hiện điều đó. Việc cho phép đó phải được cấu hình trên ASA/PIX; các thiết bị trong mạng này có thể truy nhập ra mạng outside.

- Mức từ 1 đến 99: Được dành cho những mạng xung quanh kết nối tới ASA/PIX, đăng ký dựa trên kiểu của truy nhập của mỗi thiết bị, thông thường là kết nối đến một mạng hoạt động như là Demilitarized zone (DMZ).

Khi có nhiều kết nối giữa ASA/PIX và các thiết bị xung quanh thì:

- Dữ liệu đi từ interface có Security level cao hơn đến interface có Security level thấp hơn: Cần phải có một translation (static hay dynamic) để cho phép giao thông từ interface có Security level cao hơn đến interface có Security level thấp hơn. Khi đã có translation này, giao thông bắt đầu từ inside interface đến outside interface sẽ được phép, trừ khi nó bị chặn bởi access-list, authentication hay authorization.

- Dữ liệu đi từ interface có Security level thấp hơn đến interface có Security level cao hơn: 2 điều quan trọng cần phải được cấu hình để cho giao thông từ interface có Security level thấp hơn đến interface có Security level cao hơn là static translation và conduit hoặc access-list.

- Dữ liệu đi qua hai interface có Security level như nhau: Không có giao thông đi giữa hai interface có Security level như nhau.

2.1.2.3. Định tuyến lưu lượng qua tường lửa

Mặc định thì ASA/PIX Firewall đóng vai trò như một thiết bị lớp 3 trong hệ thống mạng. Nghĩa là nó phải định tuyến cho các lưu lượng đi qua nó. Khi gói tin đến ASA/PIX Firewall, nó cần xác định xem phải đẩy gói tin ra interface nào (nếu được phép). Tương tự như Router, ASA/PIX Firewall định tuyến cho các lưu lượng dựa vào địa chỉ IP đích. ASA/PIX tách phần địa chỉ IP đích trong IP Header của gói tin và tra trong bảng định tuyến (routing Table) của nó để ra quyết định. Nếu nó biết

được địa chỉ đích tương ứng với interface nào thì sẽ đẩy gói tin ra interface đó; nếu không tìm thấy thông tin thích hợp trong bảng định tuyến, nó sẽ hủy gói tin. Vì vậy, để Firewall có thể định tuyến cho các lưu lượng qua nó, người quan trị cần phải cấu hình định tuyến cho các mạng ở các vùng mà Firewall cần biết.

Khi cấu hình định tuyến cho Firewall, ta có thể sử dụng định tuyến tĩnh (Static) hoặc định tuyến động (RIP, IGRP, EIGRP, OSPF...).

2.1.2.4. Truy cập thông qua tường lửa

ASA/PIX Firewall có thể được cấu hình với nhiều interface. Mỗi interface có một cấp độ bảo mật riêng. Một interface được coi là bên trong (Inside) - tin cậy, hay bên ngoài (Outside) - không tin cậy, còn phụ thuộc vào mối quan hệ của nó với interface nào. Nghĩa là trong mối quan hệ với interface này nó có thể là Inside nhưng trong mối quan hệ khác nó lại là Outside. Interface được coi là Inside đối với interface khác nếu như nó có cấp độ bảo mật cao hơn, và ngược lại nếu cấp độ bảo mật của nó thấp hơn thì nó được coi là Outside.

Chính sách bảo mật mặc định của ASA/PIX Firewall cho phép lưu lượng từ interface có cấp độ bảo mật cao (Inside) truy cập vào interface có cấp độ bảo mật thấp hơn (Outside). Kết nối từ Inside đến Outside gọi là kết nối ra ngoài (Outbound Connection). Các kết nối này mặc định là luôn được phép trừ khi người quản trị (Admin) đưa ra chính sách bảo mật ngăn cản kết nối.

Kết nối từ interface có cấp độ bảo mật thấp đến interface có cấp độ bảo mật cao hơn (từ Outside vào Inside) được gọi là kết nối vào trong (Inbound Connection). Kết nối này mặc định là không được phép trừ khi người quản trị thiết lập một cặp gồm: chuyển đổi địa chỉ tĩnh (Static Translation) và Access List.

2.1.2.5. Truy cập ra ngoài thông qua tường lửa

Các kết nối ra ngoài (Outbound Connection) luôn được cho phép bởi chính sách bảo mật mặc định. Tuy nhiên, ta vẫn cần phải thiết lập chuyển đổi địa chỉ cho ASA/PIX Firewall đối với các kết nối kiểu này. Vì mục đích an toàn, để tránh mạng ngoài (Outside) biết được cấu trúc mạng bên trong (Inside), công nghệ chuyển đổi

địa chỉ được sử dụng với ASA/PIX Firewall, giúp nó che dấu được cấu trúc mạng bên trong mà vẫn đảm bảo kết nối hoạt động tốt. Có hai kiểu chuyển đổi địa chỉ:

- Chuyển đổi địa chỉ động (Dynamic Address Translation): chuyển đổi nhiều địa chỉ cục bộ (Local Address) ra một hoặc nhiều địa chỉ toàn cục (Global Address). Chuyển đổi địa chỉ động được chia làm hai loại:

+ Chuyển đổi địa chỉ mạng (Network Address Translation - NAT): chuyển đổi nhiều địa chỉ cục bộ ra một dải (Pool) địa chỉ toàn cục.

+ Chuyển đổi địa chỉ cổng (Port Address Translation - PAT): chuyển đổi nhiều địa chỉ cục bộ ra một hay một số địa chỉ toàn cục. Sau khi chuyển đổi, các địa chỉ toàn cục có thể giống nhau nhưng khác về số hiệu cổng. Nói cách khác, đây không đơn thuần là chuyển đổi một địa chỉ mà là chuyển đổi một cặp địa chỉ IP/số hiệu cổng (IP Address/Port).

- Chuyển đổi địa chỉ tĩnh (Static Address Translation): là ánh xạ một-một giữa địa chỉ cục bộ và địa chỉ toàn cục.

Với NAT và PAT, mỗi khi có một chuyển đổi, ASA/PIX Firewall sẽ ghi nó vào bảng chuyển đổi (Xlate Table). Khi hết thời gian dành cho chuyển đổi (timeout) mà không có lưu lượng nào của chuyển đổi này đi qua thì ASA/PIX Firewall sẽ xóa nó khỏi bảng chuyển đổi. Cơ chế này ngoài việc giúp che giấu cấu trúc mạng bên trong còn tránh mạng ngoài có thể dò và tấn công ngược lại địa chỉ đã chuyển đổi bởi các chuyển đổi chỉ là tạm thời.

Để cho phép các host bên trong (Inside) truy cập ra ngoài, ta thiết lập chuyển đổi địa chỉ động với hai câu lệnh nat cho interface bên trong và Global cho interface ngoài.

2.1.2.6. Truy cập vào trong thông qua tường lửa

Chính sách bảo mật mặc định của ASA/PIX Firewall không cho phép các truy cập từ mạng ngoài (Outside) và trong (Inside). Để cho phép kết nối này, ta phải thiết lập hai thành phần sau:

- Danh sách điều khiển truy cập (Access Control List - ACL)

- Chuyển đổi địa chỉ tĩnh (Static Address Translation)

Tuy nhiên, cần lưu ý là chỉ thiết lập chuyển đổi tĩnh không cho phép kết nối được khởi tạo từ mạng ngoài mà phải kết hợp với Access List. Danh sách điều khiển truy cập là thành phần quan trọng được sử dụng trong các thiết bị của Cisco. Đối với ASA/PIX Firewall, ACL được dùng để hạn chế lưu lượng ra ngoài (Outbound Traffic), và cho phép lưu lượng đi theo chiều ngược lại. Một ACL là một danh sách tuần tự các câu điều kiện "Permit" và "Deny" để chỉ ra cho Firewall biết lưu lượng nào được chấp nhận (Permit) hoặc loại bỏ (Deny).

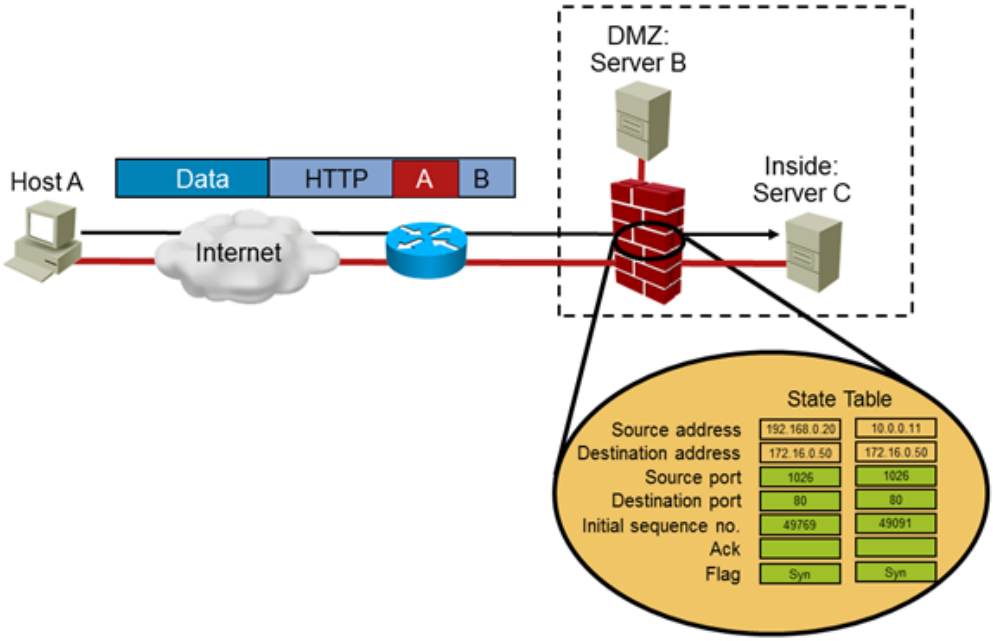
Cơ chế kiểm tra Access-List tuân theo nguyên tắc tuần tự từ trên xuống. Vì vậy thứ tự các câu lệnh trong Access-List. Trong quá trình kiểm tra, nếu khớp (match) với câu lệnh nào thì gói tin sẽ được xử lý (Permit hay Deny) ngay và không phải kiểm tra các câu lệnh tiếp theo nữa. Lưu ý là trong mỗi Access-List đều luôn có câu lệnh từ chối ẩn (Implicit Deny) ở cuối cùng (cho dù nó có được thiết lập hay không) với mục đích từ chối tất cả các gói tin.

Sau khi thiết lập ACL cho phép truy cập vào trong, ta cần một chuyển đổi tĩnh. Chuyển đổi tĩnh cho phép host ở mạng ngoài truy cập vào host bên trong qua địa chỉ toàn cục. Khi gói tin bên ngoài đến ASA/PIX Firewall và thông qua chính sách bảo mật, Firewall sẽ kiểm tra xem có chuyển đổi tĩnh phù hợp không. Nếu có, nó chuyển đổi địa chỉ toàn cục ra địa chỉ cục bộ và đẩy gói tin đến đích.

2.1.3. Công nghệ tích hợp trên tường lửa Cisco

Công nghệ tưởng lửa Cisco dựa trên công nghệ Statefaul Inspection được tổng hợp từ các công nghệ Packet filtering(lọc gói), Proxy Server và Stateful packet filtering.

2.1.3.1. Công nghệ Stateful Inspection



Hình 2. 2: Công nghệ Stateful Inspection[13]

Công nghệ Stateful Inspection là sự tổng hợp tính năng của 3 loại công nghệ trên. Nó được xem là chuẩn công nghệ cho các giải pháp bảo mật mạng dành cho các doanh nghiệp. Công nghệ Stateful Inspection đáp ứng được tất cả các yêu cầu về bảo mật trong khi các công nghệ tường lửa truyền thống, như lọc gói hoặc các gateway lớp ứng dụng thường không đáp ứng được đầy đủ các yêu cầu về bảo mật.

Có nhiều hãng tường lửa sử dụng công nghệ Stateful Inspection như: CheckPoint, Cisco, Netscreen, 3COM Secure Gateway…

Đối với công nghệ Stateful Inspection, các gói tin được ngăn chặn từ tầng mạng (tương tự như trong công nghệ lọc gói), tuy nhiên dữ liệu bắt nguồn từ tất cả các tầng đều được xem xét và phân tích phục vụ cho mục đích đảm bảo an ninh (đối với các gateway lớp ứng dụng thì đối tượng xem xét từ tầng 4 đến tầng 7). Công nghệ Stateful Inspection giới thiệu giải pháp có độ bảo mật cao hơn nhờ việc kết hợp chặt chẽ các thông tin kết nối, trạng thái application-derived và nội dung thông tin được lưu trữ và cập nhật tự động. Nó dựa vào các thông tin trước để lượng giá các kết nối sau đấy.

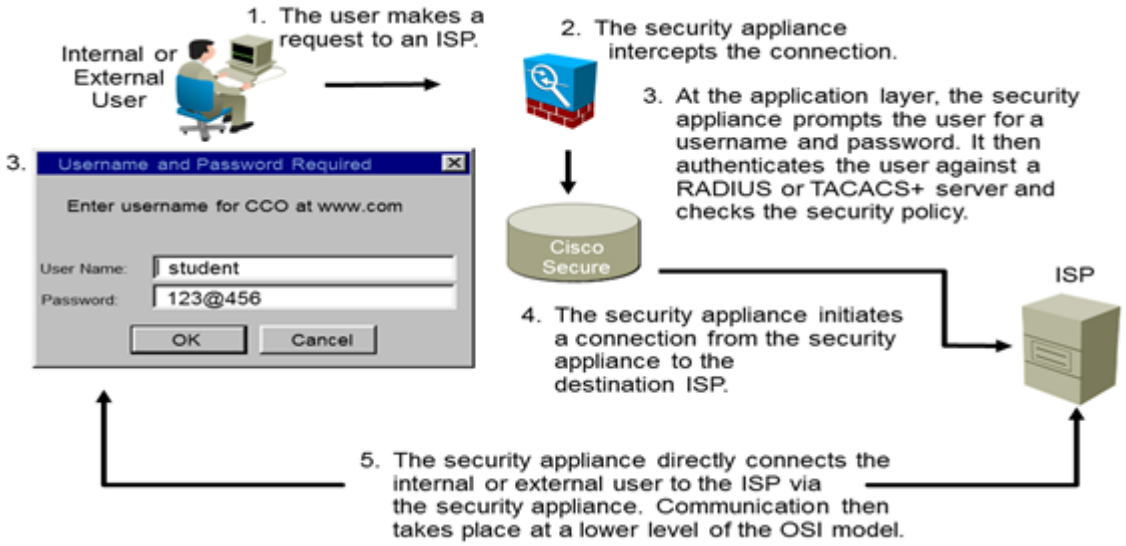
Nó cũng cung cấp khả năng tạo ra các thông tin phiên làm việc ảo cho việc theo dõi các giao thức không kết nối (ví dụ các ứng dụng dựa trên các giao thức

RPC và UDP), đấy là những điều mà các công nghệ tường lửa khác không làm được.

Không như công nghệ lọc gói chỉ kiểm tra thông thông tin header của gói tin, công nghệ Stateful Inspection theo kiểm soát, theo dõi các kết nối trên tất cả các cổng của tường lửa và đảm bảo các kết nối đó là hợp pháp. Tường lửa sử dụng công nghệ Stateful Inspection không chỉ kiểm tra thông tin header của gói tin mà còn kiểm tra nội dung của gói tin ở tầng ứng dụng. Tường lửa Stateful Inspection có khả năng theo dõi trạng thái của kết nối và đưa các thông tin trạng thái vào bảng trạng thái. Vì thế, tường lửa sử dụng công nghệ Stateful Inspection kiểm soát không chỉ dựa trên tập luật (chính sách) mà còn dựa theo ngữ cảnh đã được thiết lập ưu tiên của các gói tin trước đó đã đi qua tường lửa.

Hơn thế nữa, các cổng của tường lửa luôn ở trong trạng thái đóng (close off) nó chỉ được mở khi có yêu cầu kết nối. Điều này giúp đảm bảo an toàn cho tường lửa và hệ thống.

2.1.3.2. Công nghệ Cut-Through Proxy



Hình 2. 3: Công nghệ Cut – Though Proxy[13]

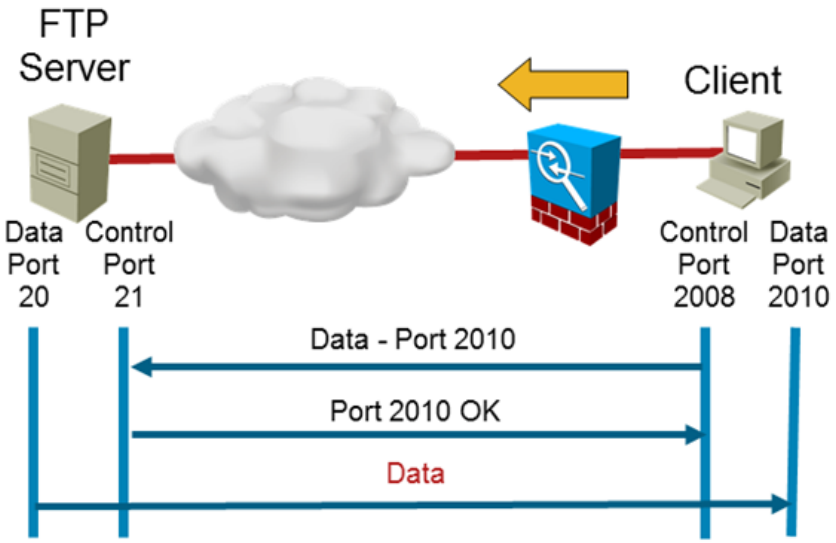
Tính năng Cut-Through Proxy giúp tưởng lửa Cisco hoạt động hiệu quả hơn tường lửa Proxy, vì nó thực hiện quá trình xác minh người tại tầng ứng dụng, kiểm

tra phân quyền tới chính sách bảo mật, rồi sau đó mới mở kết nối như là được phân quyền bởi chính sách bảo mật. Các lưu lượng đến sau của kết nối này không bị quản lý tại tầng ứng dụng nữa nhưng vẫn được kiểm tra trạng thái. Việc này giúp PIX Firewall hoạt động nhanh hơn, và không bị quá tải so với tường lửa Proxy.

Mô tả quá trình hoạt động của Cut-Through.

1. Người dùng có nhu cầu sẽ tạo một yêu cầu gửi tới ISP.
2. Tường lửa Cisco sẽ tạm chặn yêu cầu lại.
3. Tại lớp ứng dụng sẽ bắt buộc người dùng nhập username và mật khẩu. Mật khẩu có thể sẽ được xác thực tại Local hay một server xác thực Radius, TACACS+ ..
4. Xác thực thành công sẽ được chuyển tiếp tới ISP.
5. ISP hồi đạp lại yêu cầu của người dùng thông qua tường lửa.

2.1.3.3. Applicatin-Aware Inspection

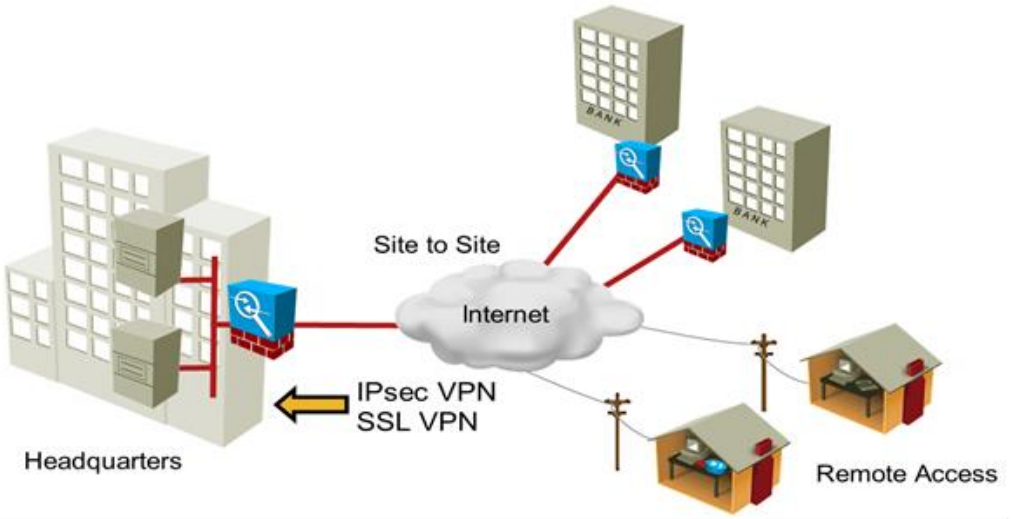


Hình 2. 4: Công nghệ Application – Aware Inspection[13]

Với tính năng này, các dịch vụ như FTP ,HTTP .. sẽ được tự động gán địa chỉ Port nguồn và Port đích thông qua firewall. Tường lửa sẽ làm nhiệm vụ thanh tra các gói tin từ lớp 3 – lớp network.

Tường lửa sẽ chịu trách nhiệm mở và đóng port cho các ứng dụng kết nối thông qua nó.

2.1.3.4. Virtual Private Network



Hình 2. 5: Công nghệ mạng riêng ảo VPN[13]

Dòng sản phẩm Cisco ASA 5500 Series hỗ trợ tính năng VPN, cho phép thiết lập kết nối từ xa giữa các chi nhánh hoặc từ người dùng ở xa.

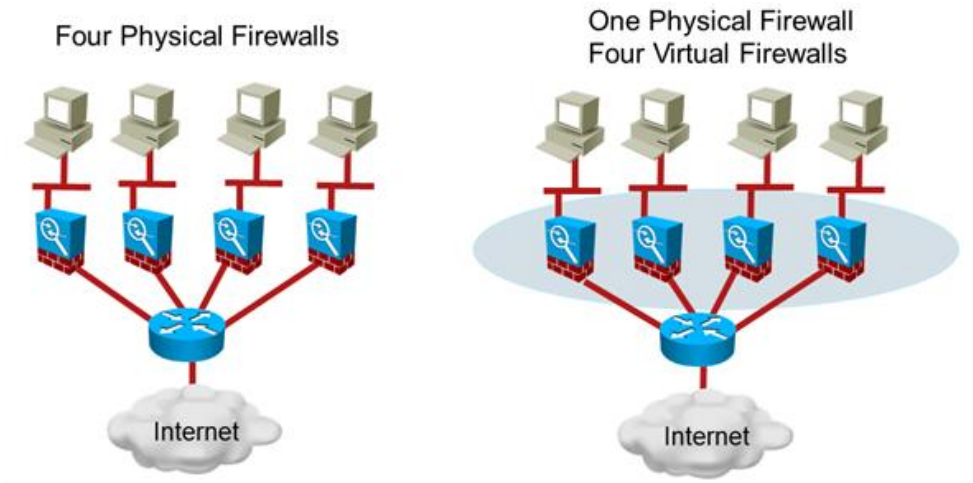
• Site – to – Site : Cung cấp kết nối từ xa giữa các chi nhanh

• IPsec VPN : Dựa trên nền tảng ipsec, người dùng ở xa sẽ sử dụng phần mềm Cisco VPN client để kết nối với hệ thống.

• SSL VPN: Đây là tính năng cho phép người dùng ở xa kết nối tới hệ thống thông qua trình duyệt web.

Các tài khoản sử dụng VPN sẽ được xác thực ngay tại tường lửa hoặc sẽ được xác thực tại máy chủ chuyên dụng Radius, AAA, TACACS+..

2.1.3.5. Security Context (Virtual Firewall)



Hình 2. 6: Công nghệ tường lửa ảo[13]

Việc xuất hiện ngày một nhiều các Hacker mới am hiểu kỹ thuật hơn, các cuộc tấn công ngày một nguy hiểm hơn, đã khiến cho các quản trị viên gặp rất nhiều khó khăn trong việc điều khiển và quản lý các hoạt động của người dùng trên mạng. Trước đây, khi một tổ chức đặt ra yêu cầu phải có các chính sách bảo mật riêng biệt cho từng phòng ban thì đi kèm với nó cũng là việc phải có thêm nhiều tường lửa riêng biệt, mỗi thiết bị cho một phòng. Do đó, sẽ làm tăng độ phức tạp, gây khó khăn trong quản lý hệ thống mạng của công ty, và làm tăng chi phí đầu tư thiết bị. Để giải quyết vấn đề này, tập đoàn Cisco đã đưa ra giải pháp tạo tường lửa ảo (Virtual Firewall) trong phiên bản hệ điều hành 7.0.

Với tính năng Virtual Firewall hay còn được gọi là Security Context (ngữ cảnh bảo mật), người quản trị có thể tạo ra nhiều Security Context trong một thiết bị tường lửa. Mỗi Context có một file cấu hình riêng cho chính sách bảo mật, áp đặt các Interface, và các lựa chọn quản lý Security Context. Tính năng này làm giảm số lượng thiết bị, chi phí đầu tư, và khối lượng công việc của quản trị viên.

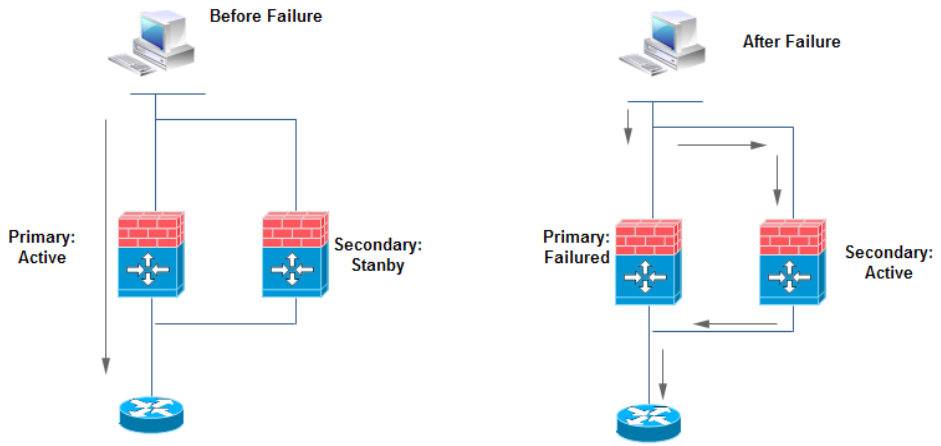
Mặc định thì ASA/PIX Firewall hoạt động ở chế đơn độ ngữ cảnh (Single Context). Để sử dụng tính năng Virtual Firewall ta cần chuyển sang chế độ đa ngữ cảnh (Multiple Context). Khi đó, mỗi Context sẽ là một tường lửa độc lập với chính sách bảo mật và các interface của nó.

Mặc dù Security Context tạo ra khả năng mềm dẻo cho thiết kế của thiết bị bảo mật, tuy nhiên khi thiết lập ở chế độ đa ngữ cảnh (Multiple Context) thì Firewall sẽ không hỗ trợ một số tính năng sau:

- Các giao thức định tuyến động như RIP, OSPF (chỉ hỗ trợ định tuyến tĩnh)
- Mạng riêng ảo (VPN)
- Multicast

2.1.3.6. Khả năng dự phòng - Failover Capabilities

Khả năng dự phòng là một đặc điểm nổi bật của các thiết bị Cisco nói chung và của ASA nói riêng. Khả năng dự phòng giúp cho hệ thống vẫn có thể hoạt động được ngay cả khi gặp các sự cố nghiêm trọng mà không bị sụp đổ như các hệ thống đơn lẻ. Có nhiều nguyên nhân có thể gây ra sự cố đối với một hệ thống đang vận hành như: mất điện, cáp bị lỗi, đứt dây cáp, lỗi phần cứng thiết bị, hay các lỗi kết nối mạng... Bất kỳ một lỗi nào cũng có thể gây ra sự ngừng trệ, thậm chí tê liệt hệ thống. Một hệ thống hoạt động tốt không chỉ phải đảm bảo an ninh, thuận tiện mà còn phải đảm bảo tính sẵn sàng (Available). Vì vậy, khả năng dự phòng cũng như vượt lỗi (Failover) là cần thiết đối với bất cứ một hệ thống nào.



Hình 2. 7: Công nghệ failover[13]

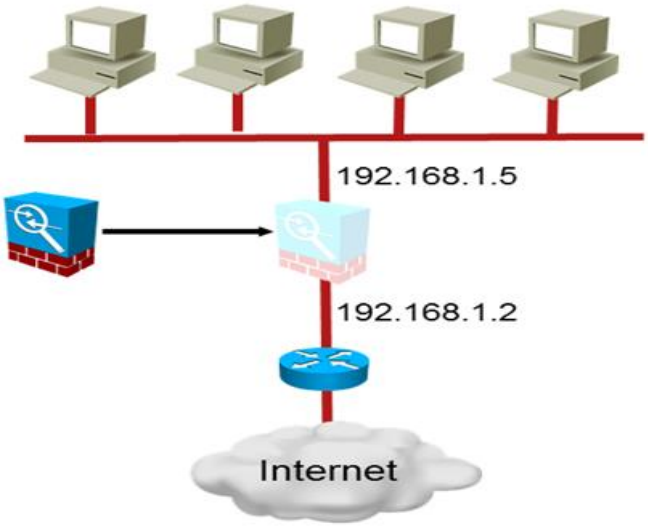
Một hệ thống triển khai dự phòng cần ít nhất hai thiết bị ASA/PIX Firewall, một thiết bị hoạt động chính (Active) và một thiết bị dự phòng nóng (Hot Standby).

Bình thường thì các hoạt động mạng sẽ được thực hiện bởi thiết bị chính (Primary). Thiết bị thứ cấp (Secondary) không tham gia điều khiển các hoạt động mạng mà chỉ đóng vai trò dự phòng. Nếu có một sự cố xảy ra khiến thiết bị chính không hoạt động được thì thiết bị dự phòng sẽ chuyển từ trạng thái Standby sang trạng thái Active và các hoạt động mạng sẽ chuyển sang thiết bị dự phòng để xử lý. Với thiết kế như trên thì các hoạt động của mạng sau khi bị lỗi sẽ trở lại hoạt động bình thường một cách nhanh chóng, tuy nhiên ta có thể thấy nhược điểm của nó là các kết nối ngay trước khi xảy ra sự cố sẽ bị hủy và các ứng dụng của người dùng sẽ phải khởi tạo lại. Để giải quyết vấn đề này, Cisco đã đưa ra thiết kế vượt lỗi trạng thái (Stateful Failover). Trong thiết kế dự phòng đơn giản thì chỉ cần thiết lập kết nối LAN-based Failover (kết nối qua cổng Ethernet) hoặc serial-based Failover (kết nối qua cổng serial) cho hai thiết bị. Đối với thiết kế Stateful Failover, cần thiết lập thêm đường kết nối trạng thái (Stateful Link) giữa hai thiết bị. Đường kết nối này sẽ làm nhiệm vụ chuyển tiếp các thông tin về kết nối cũng như các hoạt động khác của thiết bị chính cho thiết bị dự phòng để khi sự cố xảy ra với thiết bị chính thì thiết bị dự phòng vẫn có thể đảm nhiệm tiếp công việc của thiết bị chính mà không phải hủy các kết nối trước khi xảy ra sự cố. Hình 2.1 mô tả hệ thống được thiết kế dự phòng kiểu Stateful Failover.

Lưu ý: để có thể triển khai được hệ thống dự phòng, phải thỏa mãn những yêu cầu sau:

- Các thiết bị phải cùng nhóm (Series).
- Các thiết bị có chung tính năng Failover.
- Các thiết bị phải chạy trên cùng phiên bản hệ điều hành.
- Các thiết bị phải có cùng số lượng cũng như kiểu của Interface.
- Các thiết bị phải có dung lượng bộ nhớ flash và RAM như nhau.

2.1.3.7. Chế độ trong suốt (Transparent Mode)



Hình 2. 8: Firewall hoạt động ở chế độ Transparent[13]

Mặc định thì Cisco Firewall hoạt động như một thiết bị lớp 3. Nó định tuyến (routing) và chuyển đổi địa chỉ (Translation) các lưu lượng đi qua nó. Tuy nhiên, cấu hình mặc định này có thể yêu cầu phải thay đổi các thành phần của mạng khi Firewall được triển khai trong hệ thống mạng có từ trước (như hệ thống địa chỉ IP, cấu hình NAT). Vấn đề này có thể được khắc phục bằng cách cấu hình Cisco Firewall hoạt động ở chế độ trong suốt (transparent mode).

Với cấu hình transparent mode, Cisco Firewall sẽ hoạt động như một thiết bị ở lớp 2. Nó sẽ chuyển mạch (switching) các gói tin thay vì định tuyến chúng. Cisco Firewall chuyển mạch các gói tin từ Interface này sang một Interface khác. Các Interface này thường nằm trong cùng một VLAN (Virtual Local Area Network - mạng nội bộ ảo) hay mạng con.

Trong chế độ này, Cisco Firewall quản lý các lưu lượng đi qua nó dựa trên địa chỉ MAC thay vì địa chỉ IP. Mặc định thì Cisco Firewall sẽ tự động học địa chỉ MAC. Tuy nhiên cấu hình này có thể bị Hacker khai thác bằng cách đóng giả địa chỉ MAC đã kết nối đến mạng hoặc sử dụng địa chỉ MAC ngẫu nhiên để truy cập vào mạng. Để đảm bảo an toàn cho hệ thống mạng, người quản trị có thể tắt bỏ chế độ học địa chỉ MAC tự động, và chỉ sử dụng các địa chỉ MAC được cấu hình tĩnh bởi quản trị viên.

Lưu ý là khi thay đổi sang chế độ trong suốt thì sẽ loại bỏ hoặc hạn chế một số tính năng sau của Cisco Firewall:

Giới hạn interface (Interface limit): tường lửa trong suốt (transparent Firewall) chỉ có thể hoạt động với 2 interface cho mỗi ngữ cảnh đơn (Single Context). Nếu có đa ngữ cảnh (Multiple Context) thì mỗi Context sẽ được sử dụng 2 interface. Các interface này chỉ được sử dụng bởi một Context duy nhất và không thể chia sẻ giữa các Context.

NAT: cấu hình NAT không được hỗ trợ trong chế độ này. NAT chỉ được hỗ trợ với chế độ hoạt động ở lớp 3.

Các giao thức định tuyến động (dynamic routing Protocol): ASA/PIX Firewall trong chế độ này hoạt động như là thiết bị lớp 2. Nó chuyển mạch gói tin thay vì định tuyến chúng. Vì vậy, chế độ trong suốt không hỗ trợ các giao thức định tuyến động.

DHCP: transparent Firewall không thể hoạt động với chức năng là DHCP relay (DHCP chuyển tiếp), mặc dù có thể cấu hình làm DHCP Server.

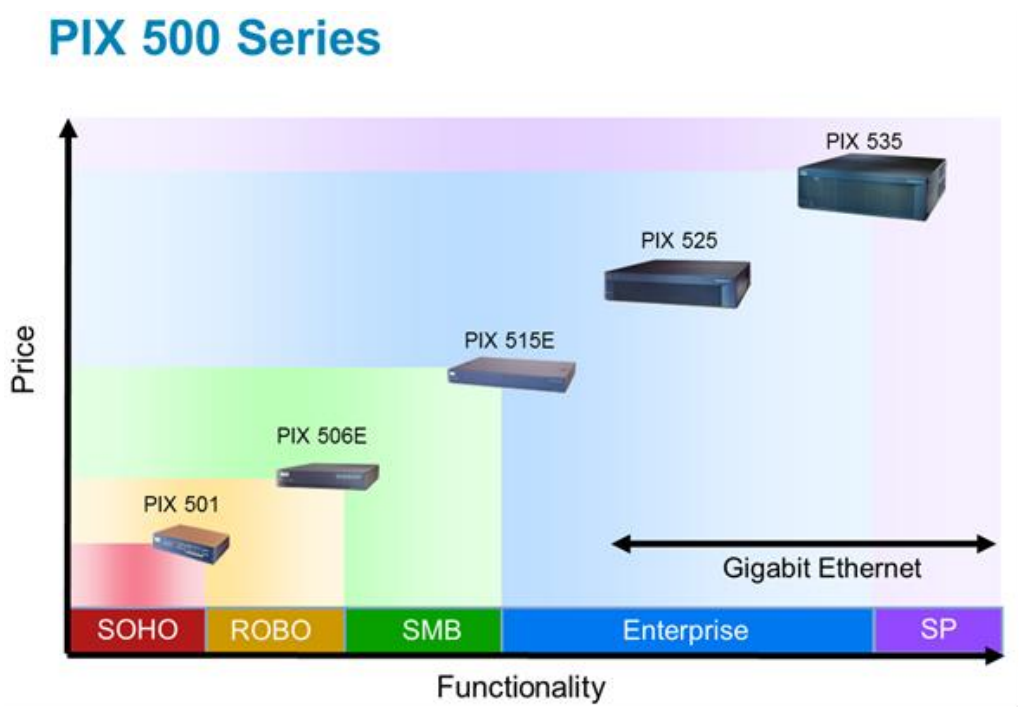
Multicast: mặc định thì chế độ này không hỗ trợ lưu lượng multicast. Để cho phép lưu lượng multicast đi qua, phải sử dụng danh sách truy cập mở rộng (extended Access List).

2.1.3.8. Quản lý thiết bị qua giao diện web

Với việc cài đặt phần mềm Adaptive Security Device Manager (ASDM) cung cấp giao diện cho người quản trị. Đơn giản hóa việc cấu hình một số tính năng thay vì phải dùng giao diện dòng lệnh hơi phức tạp.

Tuy nhiên hạn chế là việc cấu hình, giám sát và quản lý chỉ trên một thiết bị, hơi thiếu tính chuyên nghiệp. Không mềm dẻo trong việc cấu hình và kiểm soát lỗi.

2.1.3.9. Dòng sản phẩm thế hệ mới Cisco ASA Firewall



Hình 2.9 Các dòng sản phẩm ASA[13]

Dòng sản Cisco ASA 5500 Series ra đời nhằm khắc phục các hạn chế mắc phải ở dòng sản phẩm trước Pix Firewall. Cisco ASA 5500 Series tích hợp các tính năng cao cấp, đáp ứng được những yếu cầu khắt khe nhất từ phía người dùng, các doanh nghiệp. Dòng sản phẩm này có hiệu năng, băng thông xử lý cao, phù hợp với các mạng doanh nghiệp và các hệ thống lớn như của các nhà cung cấp dịch vụ ISP. Dòng sản phẩm ASA 5500 Series bao gồm: ASA 5505, ASA 5510, ASA 5520, ASA 5540… được tích hợp các cổng giao tiếp tốc độ cao fastethernet(10/100 Mbps) và gigaethernet(1Gbps) đảm bảo việc xử lý nhanh hơn và đáp ứng tốt băng thông cho hệ thống.

Cisco ASA 5500 Series đã tích hợp Secure Socket Layer (SSL) VPNs, cho phép người dùng ở xa truy nhập an toàn vào hệ thống. Bên cạnh đó còn hỗ trợ tính năng Site – To – Site VPN cho phép tạo kết nối ảo giữa các chi nhánh ở xa nhau. Tính năng Webvpn cho phép người dùng dễ dàng thiết lập một kết nối VPN vào hệ thống thống qua trình duyệt web browser. Thêm đó là tính Anyconnect VPN cho phép kết nối VPN được thực hiện từ bất kỳ VPN client nào. Kết hợp với Advance

Inspection and Prevention Security Services Moudle (AIP-SSM) sẽ cung cấp tính năng phát hiện và ngăn chặn xâm nhập bất hợp pháp IPS/IDS.

2.1.4. Tách hệ thống, tối ưu hóa tường lửa

Tuy nhiên, để có thể nâng cao khả năng của firewall, ở các doanh nghiệp hay trường học, nên phân hệ thống mạng ra thành 3 khu vực, gồm:

- Internal: Gồm các máy client bên trong nội bộ.
- Perimeter: Gồm các máy chủ của nội bộ như máy chủ web, mail, database,..
- External: Mạng bên ngoài nội bộ.

Tại sao lại phải phân ra thành 3 khu vực này. Đó là bởi vì nếu xếp chung các máy chủ và client cùng một khu vực, khi xảy ra sự cố tấn công từ bên ngoài hay phát tán virus từ bên trong, sự cố sẽ lây sang các máy chủ và làm hỏng cả hệ thống mạng.

Firewall sẽ đặt ở trung tâm, như một cầu nối điều khiển các luồng thông tin cho phép truy cập hay không truy cập.

- Ở Internal, ta sẽ mở firewall cho phép máy bên trong truy cập ra bên ngoài External và Perimeter để lấy thông tin.
- Ở Perimeter, ta sẽ mở cho phép truy cập ra bên ngoài External.

Sau khi cấu hình như trên, có thể giúp hệ thống tránh việc bị tấn công vào server, hay tránh lây nhiễm virus từ các máy client sang server.

Giả dụ, khi trong client gửi một gói tin ra bên ngoài mạng, Firewall sẽ mở cổng cho gói tin đó ra ngoài. Sau khi đến server bên ngoài và họ gửi lại một gói tin, firewall sẽ mở cổng để cho gói tin đó đến được máy client vừa mới gửi ra ngoài. Đó là để cho bên trong kết nối ra ngoài mạng bình thường. Nhưng khi xảy ra tấn công, họ sẽ chỉ có thể tấn công vào trong client, nhưng không thể tấn công vào server do ta không có kết nối nào cho phép các gói tin bên ngoài External được truy cập vào trong Perimeter. Việc lây lan virus thông qua các gói tin bên trong mạng nội bộ cũng vậy, do ở khu vực riêng biệt nên sự lây lan sẽ bị giảm thiểu hoặc có thể tránh được nếu phát hiện và xử lý đúng phương pháp.

Tuy nhiên, giải pháp Firewall cũng có những điểm yếu sau:

• Firewall không quản lý các hoạt động của người dùng khi đã vào được hệ thống, và không thể chống lại sự đe dọa từ trong hệ thống.

• Firewall cần phải đảm bảo một mức độ truy cập nào đó tới hệ thống, việc này có thể cho phép việc thăm dò điểm yếu.

• Chính sách của Firewall có thể chậm trễ so với sự thay đổi của môi trường, điều này cũng có thể tạo nên cơ hội cho việc xâm nhập và tấn công.

• Hacker có thể sử dụng phương thức tác động đến yếu tố con người để được truy nhập một cách tin cậy và loại bỏ được cơ chế firewall.

• Firewall không ngăn được việc sử dụng các tài khoản không được xác thực hoặc không an toàn gia nhập hoặc rời khỏi hệ thống.

Vì vậy, cần phải nghiên cứu bổ sung các giải pháp khác nhằm đảm bảo yêu cầu bảo mật cho mạng LAN.

2.2. Giải pháp sử dụng hệ thống phát hiện và ngăn chặn xâm nhập mạng IDS/IPS.

Nếu không có hệ thống cảnh báo, kẻ xấu có thể xâm nhập vào hệ thống và đạt được mục tiêu xâm nhập, trước khi có người phát hiện ra. Người quản trị nên nắm được những thay đổi của hệ thống hoặc các nguy cơ xâm nhập.

2.2.1. Hệ thống phát hiện xâm nhập IDS

IDS là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Khác với tường lửa, IDS không thực hiện các thao tác ngăn chặn truy xuất mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng. Một điểm khác biệt khác đó là mặc dù cả hai đều liên quan đến bảo mật mạng, nhưng tường lửa theo dõi sự xâm nhập từ bên ngoài và ngăn chặn chúng xảy ra, nó giới hạn truy nhập giữa các mạng để ngăn chặn sự xâm nhập nhưng không phát hiện được cuộc tấn công từ bên trong mạng. Bên cạnh đó IDS sẽ đánh giá sự

xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được các cuộc tấn công có nguồn gốc từ bên trong một hệ thống.

Chức năng ban đầu của IDS chỉ là phát hiện các dấu hiện xâm nhập, do đó IDS chỉ có thể tạo ra các cảnh báo tấn công khi tấn công đang diễn ra hoặc thậm chí sau khi tấn công đã hoàn tất. Càng về sau, nhiều kỹ thuật mới được tích hợp vào IDS, giúp nó có khả năng dự đoán được tấn công (Prediction) và thậm chí phản ứng lại các tấn công đang diễn ra (Active response).

Một trong những phần mềm IDS phổ biến hiện nay là Snort. Đây là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (được gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet. Trong thực tế, IDS là một kỹ thuật mới so với firewall, tuy nhiên, cho đến thời điểm này, với sự phát triển khá mạnh mẽ của kỹ thuật tấn công thì IDS vẫn chưa thật sự chứng tỏ được tính hiệu quả của nó trong việc đảm bảo an toàn cho các hệ thống. Xu hướng hiện nay là chuyển dịch dần sang các hệ thống IPS có khả năng phát hiện và ngăn chặn một cách hiệu quả các cuộc tấn công mạng, đồng thời giảm thiểu thời gian chết và các chi phí ảnh hưởng đến hiệu quả hoạt động của mạng.

2.2.2. Hệ thống phòng chống xâm nhập (IPS)

Hệ thống phòng chống xâm nhập (IPS) là một kỹ thuật, kết hợp các ưu điểm của kỹ thuật tường lửa với hệ thống phát hiện xâm nhập IDS, có khả năng phát hiện các cuộc tấn công và tự động ngăn chặn các cuộc tấn công nhằm vào điểm yếu của hệ thống.

Ý tưởng của công nghệ IPS là mọi cuộc tấn công chống lại bất cứ thành phần nào của môi trường được bảo vệ sẽ bị làm chệch hướng bằng các giải pháp ngăn ngừa xâm nhập. Với “quyền tối thượng”, các hệ thống phòng chống xâm nhập có thể “nắm” lấy bất cứ lưu lượng nào của các gói tin mạng và đưa ra quyết định có chủ ý – liệu đây có phải là một cuộc tấn công hay một sự sử dụng hợp pháp – sau đó thực hiện hành động thích hợp để hoàn thành tác vụ một cách trọn vẹn. Kết quả cuối

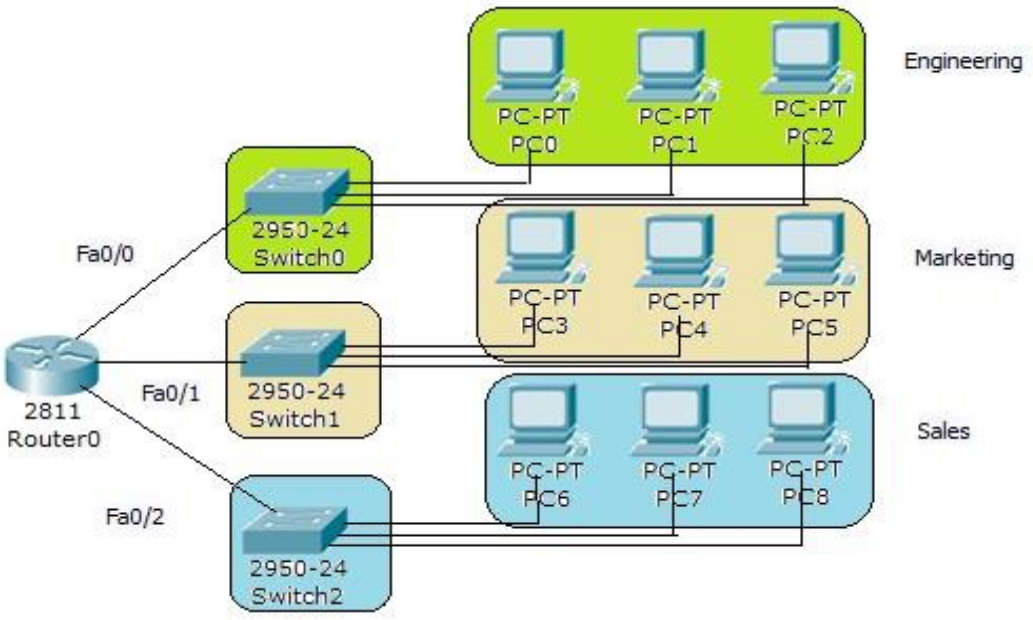
cùng là một nhu cầu có hạn định cho các giải pháp phát hiện hay giám sát xâm nhập một khi tất cả những gì liên quan đến mối đe doạ đều bị ngăn chặn.

2.3. Giải pháp sử dụng công nghệ VLAN

VLAN là cụm từ viết tắt của virtual local area network (virtual LAN) hay còn được gọi là mạng LAN ảo. VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ (giữa các khoa trong một trường học, giữa các phòng ban,...) giúp giảm thiểu bão broadcast cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. VLAN tương đương như mạng con (subnet).

2.3.1. Các miền quảng bá của mạng LAN ảo

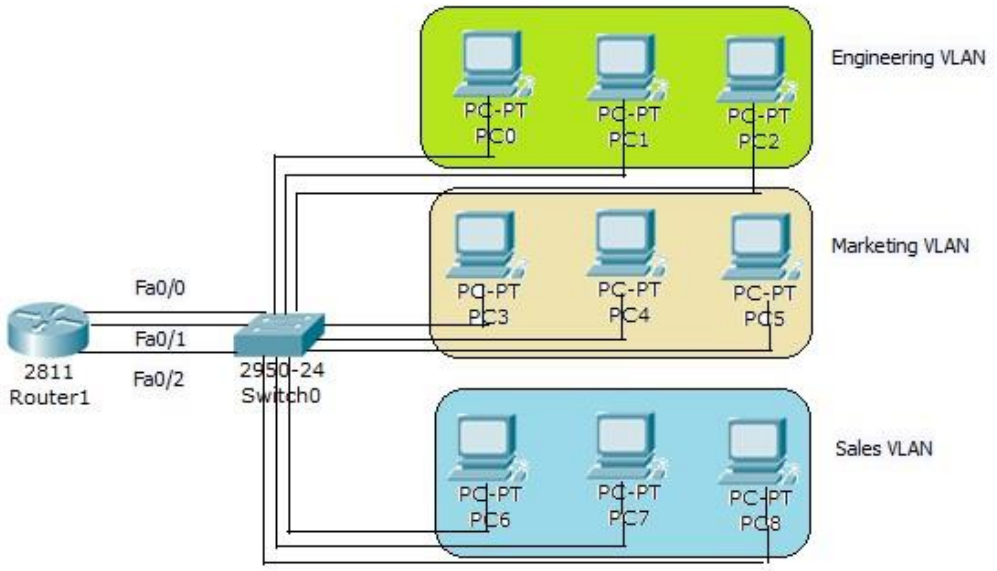
Về mặt kỹ thuật, một VLAN là một miền quảng bá được tạo nên bởi một hay nhiều Switch. Bình thường thì router đóng vai trò tạo ra miền quảng bá. Đối với VLAN, switch có thể tạo ra miền quảng bá. Trong hình 2.9, ba miền quảng bá riêng biệt trên 3 Switch, định tuyến mạng cho phép Router chuyển gói giữa các miền quảng bá với nhau.



Hình 2. 9: Miền quảng bá khi chưa chia VLAN[10]

Còn ở hình 2.10, ta thấy 3 VLAN tức là 3 miền quảng bá khác nhau được tạo ra trên một Switch và trên một Router. Router sử dụng định tuyến mạng để chuyển lưu lượng giữa 3 VLAN. Switch trong hình này sẽ truyền frame lên cổng giao tiếp của Router khi:

- Gói dữ liệu là gói quảng bá.
- Gói dữ liệu có địa chỉ MAC đích là một trong các địa chỉ MAC của Router.



Hình 2. 10: Miền quảng bá khi đã chia VLAN[10]

Nếu máy trạm 1 trong Engineering VLAN muốn gửi dữ liệu cho máy trạm 2 trong Marketing VLAN, vì hai máy này nằm trong 2 miền quảng bá khác nhau, thuộc hai mạng khác nhau, nên địa chỉ MAC đích trong gói dữ liệu sẽ là địa chỉ MAC của default gateway của máy trạm 1. Vì vậy địa chỉ MAC đích của gói dữ liệu sẽ là địa chỉ MAC của cổng Fa0/0 trên Router. Gói dữ liệu được chuyển đến Router bằng định tuyến IP, Router sẽ chuyển gói đúng đến Marketing VLAN. Nếu máy trạm 1 trong Engineering VLAN muốn gửi gói dữ liệu cho máy trạm 2 trong cùng VLAN này thì địa chỉ MAC đích của gói dữ liệu sẽ chính là địa chỉ MAC của máy trạm 2.

Tóm lại, Switch sẽ xử lý chuyển mạch gói dữ liệu khi có chia VLAN như sau:

Đối với mỗi VLAN, Switch có một bảng chuyển mạch riêng tương ứng. Nếu

Switch nhận được gói dữ liệu từ một port nằm trong một VLAN nào đó, thì Switch sẽ tìm địa chỉ MAC đích trong bảng chuyển mạch của VLAN đó mà thôi. Đồng thời Switch sẽ lọc địa chỉ MAC nguồn trong gói dữ liệu và ghi vào bảng chuyển mạch của VLAN đó nếu địa chỉ này chưa được biết. Sau đó Switch quyết định chuyển gói dữ liệu. Switch nhận frame vào từ VLAN nào thì Switch chỉ lọc địa chỉ nguồn của frame và tìm địa chỉ đích cho frame trong một bảng chuyển mạch tương ứng với VLAN đó.

2.3.2. Phân loại VLAN

VLAN chia thành 5 loại:

- **Data VLAN**: là VLAN phổ biến nhất, được dùng cho các kết nối của người dùng.

- **Default VLAN**: là VLAN mặc định tất cả các Switch đều có và khởi tạo tất cả các cổng của Switch đều nằm trong VLAN này. VLAN mặc định của Switch Cisco là VLAN 1 và chúng ta không thể thay đổi tên hay xóa VLAN này.

- **Native VLAN**: là VLAN duy nhất trên Switch mà Frame xuất phát từ nó khi đi qua đường truyền chung cho các VLAN (đường Trunk) không phải đóng gói thêm trường VLAN ID. Mặc định Native VLAN trên mỗi Switch cisco là VLAN1.

- **VLAN quản lý**: là bất cứ VLAN nào mà chúng ta cấu hình địa chỉ IP cho interface VLAN tương ứng. Địa chỉ IP này được sử dụng để telnet tới Switch và điều hành hoạt động của Switch từ xa.

- **VLAN voice**: là một VLAN có độ ưu tiên cao nhất vì Voice là một VLAN ứng dụng thời gian thực. (mạng nghẽn voice vẫn chạy được).

Từ 5 loại trên, các VLAN được chia thành 3 kiểu:

- **Static VLAN**: là VLAN tĩnh phân chia theo cổng. Cắm máy vào cổng nào thì nó sẽ theo VLAN đó.

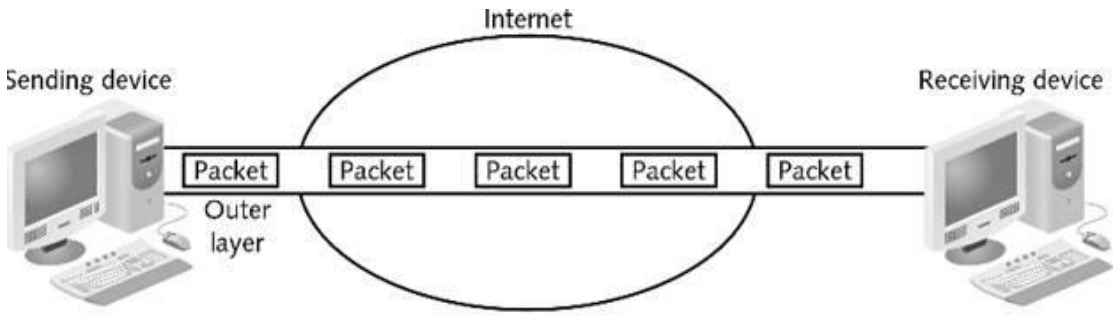
- **Dynamic VLAN**: quy định theo địa chỉ MAC, trên Switch gán MAC: 111111 là của PC1 thuộc VLAN 10 thì PC1 có cắm vào bất kì cổng nào trên Switch

nó vẫn thuộc VLAN 10. Để gán được MAC vào VLAN thì ta phải có một VMPS Server (VLAN Mangerment Policy Server).

- **Voice VLAN**: chỉ dành riêng cho dữ liệu Voice.

2.4. Giải pháp áp dụng công nghệ mạng riêng ảo (VPN)

VPN (Virtual Private Network) là một mạng riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các địa điểm hoặc người sử dụng từ xa với một mạng LAN ở trụ sở trung tâm (Hình 2.5). Thay vì dùng kết nối thật khá phức tạp như đường dây thuê bao số, VPN tạo ra các liên kết ảo được truyền qua Internet giữa mạng riêng của một tổ chức với địa điểm hoặc người sử dụng ở xa.Virtual Private Network sử dụng kỹ thuật Tunneling Protocols. Đây là kỹ thuật đóng gói một gói tin dữ liệu bên trong một gói tin khác để tạo ra một kênh truyền an toàn.



Hình 2. 11: Mô hình hệ thống VPN[14]

2.4.1. Các đặc tính của VPN

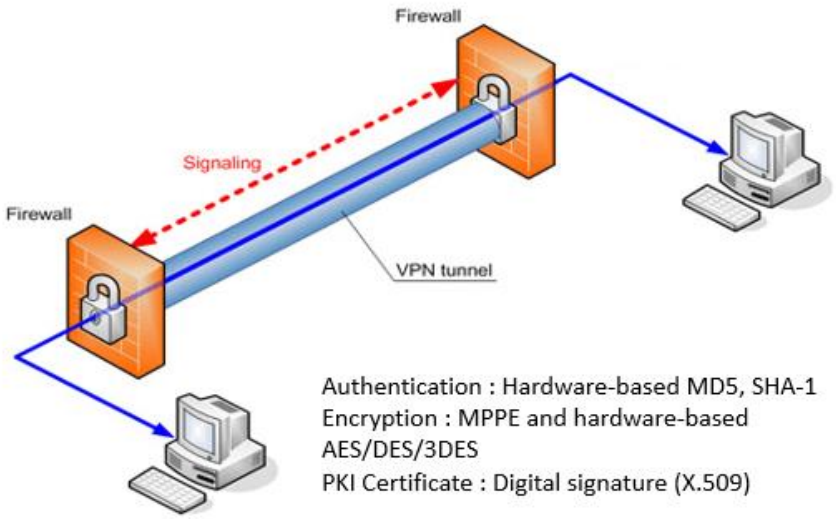
VPN có các đặc tính hữu ích gồm:

- Chi phí thiết lập mạng VPN thấp do sử dụng chung hạ tầng Internet.

- Tính linh hoạt: VPN đã xóa bỏ rào cản về mặt địa lý cho hệ thống mạng, sẵn sàng kết nối các mạng riêng lại với nhau một cách dễ dàng thông qua môi trường Internet.

- Tăng tính bảo mật: các dữ liệu quan trọng sẽ được che giấu đối với những người không có quyền truy cập và cho phép truy cập đối với những người dùng có quyền truy cập. Sử dụng các giao thức đóng gói, các thuật toán mã hóa và các phương pháp chứng thực để bảo mật dữ liệu trong quá trình truyền.

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



Hình 2. 12: Các đặc tính của hệ thống VPN[14]

2.4.2. Các loại VPN

Có hai loại phổ biến hiện nay là VPN truy cập từ xa (Remote-Access) và VPN điểm-nối-điểm (site-to-site)

- **VPN truy cập từ xa** (Remote): còn được gọi là mạng Dial-up riêng ảo (VPDN), là một kết nối người dùng-đến-LAN, thường là nhu cầu của một tổ chức có nhiều nhân viên cần liên hệ với mạng riêng của mình từ rất nhiều địa điểm ở xa. Ví dụ như công ty muốn thiết lập một VPN lớn phải cần đến một nhà cung cấp dịch vụ doanh nghiệp (ESP). ESP này tạo ra một máy chủ truy cập mạng (NAS) và cung cấp cho những người sử dụng từ xa một phần mềm máy khách cho máy tính của họ. Sau đó, người sử dụng có thể gọi một số miễn phí để liên hệ với NAS và dùng phần mềm VPN máy khách để truy cập vào mạng riêng của công ty. Loại VPN này cho phép các kết nối an toàn, có mật mã.

- **VPN điểm-nối-điểm** (site-to-site): là việc sử dụng mật mã dành cho nhiều người để kết nối nhiều điểm cố định với nhau thông qua một mạng công cộng như Internet. Loại này có thể dựa trên Intranet hoặc Extranet. Loại dựa trên Intranet:

Nếu một công ty có vài địa điểm từ xa muốn tham gia vào một mạng riêng duy nhất, họ có thể tạo ra một VPN intranet (VPN nội bộ) để nối LAN với LAN. Loại dựa trên Extranet: Khi một công ty có mối quan hệ mật thiết với một công ty khác (ví dụ như đối tác cung cấp, khách hàng...), họ có thể xây dựng một 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.

2.4.3. Các cách triển khai VPN trên thực tế

Mạng VPN an toàn bảo vệ sự lưu thông trên mạng và cung cấp sự riêng tư, sự chứng thực và toàn vẹn dữ liệu thông qua các giải thuật mã hoá. Tùy vào từng nhu cầu và mục đích sử dụng, ta có thể chọn 1 trong 3 cách sau:

- **Site to site:** Áp dụng cho các tổ chức có nhiều văn phòng chi nhánh, giữa các văn phòng cần trao đổi dữ liệu với nhau.

- **Remote-Access:** Hay cũng được gọi là Virtual Private Dial-up Network (VPDN), đây là dạng kết nối Remote-Access VPN áp dụng cho các cơ quan mà các nhân viên có nhu cầu kết nối tới mạng riêng (private network) từ các địa điểm từ xa.

- **Intranet/ Internal VPN:** Trong một số tổ chức, quá trình truyền dữ liệu giữa một số bộ phận cần bảo đảm tính riêng tư, không cho phép những bộ phận khác truy cập. Hệ thống Intranet VPN có thể đáp ứng tình huống này.

Mỗi cách đều tùy từng thiết bị mà ta sử dụng ở các doanh nghiệp mà có cách cấu hình khác nhau.

2.5. Giải pháp phân quyền truy cập dữ liệu

Việc xây dựng tài khoản người dùng của mỗi công ty, doanh nghiệp cho phép quản lý việc truy cập và phân phối các dữ liệu tùy vào từng mục đích cá nhân của những người sử dụng, tránh trường hợp rò rỉ các thông tin quan trọng hay các hoạt động phá hoại dữ liệu khác.

Người dùng muốn truy cập vào hệ thống cần khai báo: Tên người dùng và Password. Dựa vào thông tin tài khoản mà hệ quản trị cơ sở dữ liệu sẽ xác minh để cho phép hay từ chối quyền được truy cập vào cơ sở dữ liệu.

Sau khi xây dựng danh sách tài khoản người dùng, chúng ta cần phân tài khoản ra các phòng ban khác nhau tùy vào từng phòng ban một. Việc phân chia vào các phòng ban giúp quản lý các thông tin mà từng nhân viên trong phòng ban đó được phép truy cập hay không. Chẳng hạn ta phân ra 2 phòng ban là IT và Sale, sau đó trên máy chủ ta tạo 2 thư mục cũng là IT và Sale, rồi ta phân quyền cho phép các tài khoản ở 2 phòng ban này truy cập vào thư mục của phòng ban đó nhưng không được truy cập vào phòng ban còn lại. Đó là cách hiệu quả để quản lý dữ liệu, tránh việc thất thoát và các trường hợp không mong muốn.

Do phân theo phòng ban nên các thư mục chứa dữ liệu cũng cần phải được lọc kĩ nội dung để đưa vào các thư mục thích hợp, có hệ thống nhằm dễ quản lý, kiểm soát các đầu mục thông tin theo từng phòng ban.

Ngoài ra hệ thống cơ sở dữ liệu còn xây dựng thêm bản phân quyền truy cập dữ liệu, tùy vào chức vụ như trưởng phòng, giám đốc, giáo viên,… mà ta cho phép các quyền cơ bản đối với dữ liệu là: Đọc, sửa, xóa, bổ sung hoặc không cho phép truy cập. Chẳng hạn nhân viên chỉ được phép xem, bổ sung dữ liệu, còn trưởng phòng mới có quyền sửa, xóa các dữ liệu đó. Đây gọi là phân tầng quyền truy cập cơ sở dữ liệu.

2.6. Xây dựng chính sách an ninh cho hệ thống

Một chính sách an ninh cho hệ thống (hay còn gọi là yếu tố con người) phải gồm nhiều các chính sách được kết hợp với nhau và được tuân thủ nghiêm ngặt để có thể tạo hiệu quả cao nhất. Các chính sách thường có trong một chính sách an ninh hệ thống là:

Chính sách con người:

- Việc đưa ra các chính sách cho các hành động cụ thể với hệ thống là việc tối quan trọng để đặt ra các khuôn khổ kiểm soát chặt chẽ yếu tố con người. Các khuôn khổ này chỉ ra những hoạt động cụ thể mà từng cá nhân có thể thực hiện trong hệ thống. Bên cạnh đó, có biện pháp thích hợp với các hành vi không tuân thủ các quy tắc, chính sách hoạt động trong mạng.

- Đào tạo nâng cao nhận thức, năng lực. Nhiều tổ chức, công ty thường xuyên bỏ qua các hoạt động đào tạo và nâng cao nhận thức về an ninh mà không biết được rằng, đây con người mới là điểm yếu nhất của hệ thống mạng. Chỉ một sai sót nhỏ của con người trong hệ thống cũng có thể dẫn tới gián đoạn toàn hệ thống. Thường xuyên tổ chức đào tạo, nâng cao, rèn luyện trình độ cho các cá nhân trong hệ thống mạng LAN để nâng cao nhận thức, khả năng bảo vệ mạng. Từ đó, giảm thiểu các nguy cơ sự cố từ bên trong, đồng thời có kiến thức nền tảng khắc phục sự cố tấn công từ bên ngoài cho toàn bộ thành viên trong hệ thống. Giúp hệ thống hoạt động ổn định hơn.

2.7. Kết luận chương 2

Trong chương 2, luận văn đã nghiên cứu 6 giải pháp về bảo mật mạng LAN, trong đó đã trình bày khá chi tiết về Firewall và những giải pháp khác liên quan đến bảo vệ thông tin cho các mạng nội bộ. Mỗi giải pháp đều có một mục đích riêng và tăng khả năng bảo mật cho mạng LAN. Để đạt hiệu quả cao nhất, trong thực tế cần kết hợp tất cả các giải pháp nhằm giúp cho mạng nội bộ có thể hoạt động an toàn, tránh được các cuộc tấn công từ bên ngoài hay bên trong cũng như có thể phát hiện và có các biện pháp xử lý nhanh chóng nhất có thể khi xảy ra sự cố ngoài ý muốn.

Firewall luôn là mối quan tâm hàng đầu của các nhà quản trị mạng trong hệ thống bảo mật. Để có thể xây dựng được những mạng như vậy, người quản trị mạng phải nắm rõ được những kiến thức cơ bản về Firewall, VLAN, Server...

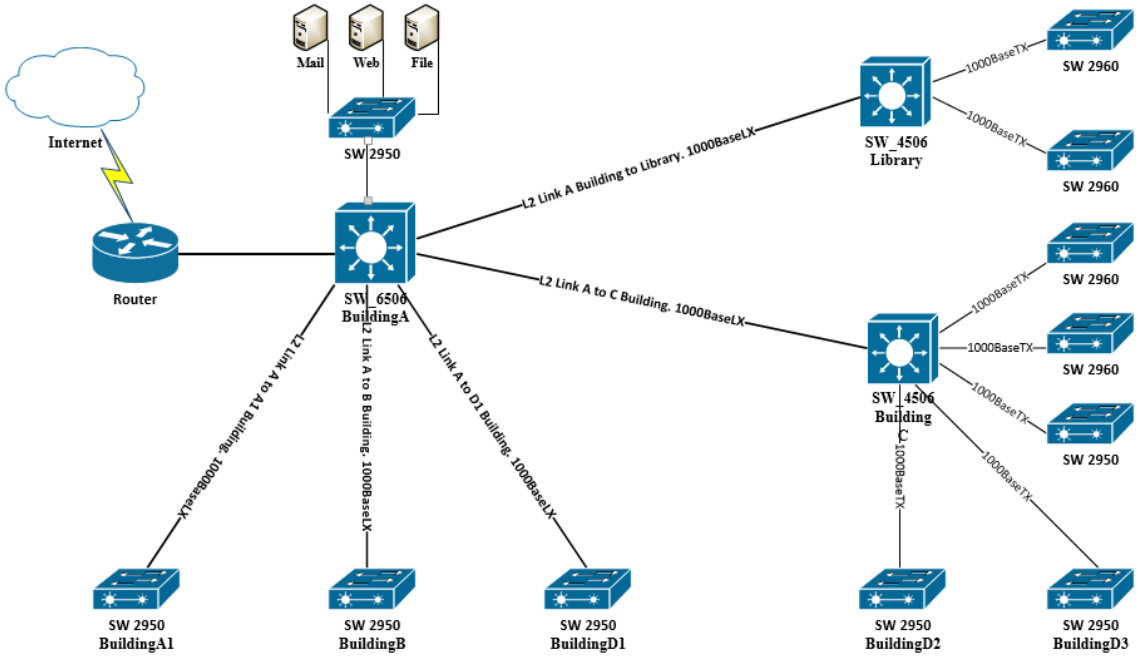
Để xây dựng được một mạng riêng mà có thể tránh khỏi mọi sự tấn công là không thể, nhưng chúng ta có thể xây dựng được những mạng có tính an toàn cao theo những yêu cầu cụ thể.

Chương III: ĐỀ XUẤT GIẢI PHÁP BẢO MẬT CHO MẠNG NỘI BỘ TRƯỜNG ĐẠI HỌC HÀ NỘI

Chương 3 của luận văn sẽ nghiên cứu đề xuất một số giải pháp bảo mật phù hợp cho mạng LAN tại trường Đại học Hà Nội.

3.1. Khảo sát mạng nội bộ trường Đại Học Hà Nội

3.1.1. Hiện trạng kiến trúc, các chức năng và trang thiết bị mạng hiện có trong mạng LAN trường Đại học Hà nội



Hình 3. 1: Mô hình kết nối mạng nội bộ của trường Đại học Hà Nội

Hệ thống mạng máy tính tại trường Đại học Hà nội được xây dựng theo mô hình client server, đồng thời với kiến trúc mạng hình sao ở các tầng, ta sẽ đạt được tốc độ nhanh nhất có thể và kiểm soát tốt khi xảy ra lỗi cũng như mở rộng tùy ý muốn. Hiện nay tại trường Đại học Hà nội đang sử dụng hệ thống máy chủ đặt tại 3 trung tâm là Nhà A , Nhà C, Thư viện của trường và khoảng 1100 máy trạm. Tại khu vực mạng nội bộ, ở mỗi tòa nhà trong trường Đại học Hà Nội đều có các Switch được kết nối thẳng tới Switch tổng để đi ra ngoài mạng cũng như đi vào khu

vực máy chủ nội bộ, các máy chủ được kết nối với nhau thông qua switch Cisco 48 port đường 1000Base LX và 1000 Base TX, các máy trạm kết nối với máy chủ thông qua các Switch Cisco 24 port.

Các máy trạm được phân bổ như sau:

- 100 máy sử dụng tại nhà A dùng cho các phòng ban và trung tâm.

- 50 máy sử dụng tại nhà B dùng cho văn phòng La Trobe và các dự án.

- 150 máy sử dụng tại nhà C dùng cho các khoa và bộ môn.

- 150 máy sử dụng tại Thư viện.

- 650 máy dùng cho các phòng LAP tại nhà A1,C, D1.

Toàn bộ các máy tính trong trường đều được kết nối ra internet thông qua các máy chủ đặt tại nhà A, nhà C, và Thư viện các máy chủ này chạy hệ điều hành windown 2008 Server, hệ điều hành Linux…. Các máy chủ nội bộ có chức năng chứa dịch vụ của nhà trường: Mail, Web, File, cung cấp DHCP cho các máy trạm theo các Vlan đã định quản lý việc truy cập internet của các máy trạm.

Máy chủ kết nối ra internet thông qua các modem cáp quang tốc độ cao của các nhà cung cấp dịch vụ internet như : FPT, VDC, VNPT… . Khoảng cách từ máy chủ của các tòa nhà tới máy xa nhất là 100m.

Một số Switch được sử dụng tại trường đại học hà nội: Switch Cisco 6506, Switch Cisco 4506, Catalyst 2950, Catalyst 2960.

3.1.2. Ứng dụng mạng máy tính trong trường Đại học Hà nội.

- Tra cứu tài liệu phục vụ công việc học tập của sinh viên và công việc của cán bộ trong toàn trường.

- Sinh viên có thể theo dõi thông tin và tình hình học tập của mình trong thời gian học tại trường thông qua cổng thông tin của nhà trường (http://hanu.vn).

- Việc trao đổi thông tin trong toàn trường dễ dàng hơn, khi có những thông báo, quyết định mới đều được phổ cập cho toàn bộ CB trong toàn trường thông qua trang tác nghiệp của trường (http://tacnghiep.hanu.vn)

3.1.3. Yêu cầu sử dụng

- Hệ thống phải luôn kết nối được Internet.

- Hệ thống phải luôn được giám sát và bảo đảm an toàn thông tin.

- VPS, các dịch vụ File, Mail, Server luôn phải ổn định để học sinh cũng như các cán bộ trong trường có thể sử dụng.

- Dữ liệu tại các phòng ban phải được tập trung, không phân tán, dễ quản lý, được phân quyền phù hợp với chức trách.

- Khả năng cung ứng cao, đáp ứng được một lượng lớn kết nối vào trong hay ra ngoài mạng mà vẫn giữ được sự ổn định.

- Có khả năng mở rộng trong tương lai.

3.1.4. Hiện trạng các vấn đề liên quan đến bảo mật trong quá trình vận hành, khai thác mạng nội bộ tại trường Đại học Hà Nội

Thực trạng :

- Các máy chủ DHCP đặt ở 3 nơi.

- Dù có ISA bảo vệ Mail và Web nhưng là firewall mềm nên khả năng cung cấp các phiên làm việc bị hạn chế, khả năng ngăn chặn các cuộc tấn công mạng rất thấp, ngoài ra toàn bộ hệ thống mạng còn lại chưa có firewall bảo vệ.

- Các Switch tại các tòa nhà chưa được quy hoạch, khó quản lý.

- Sử dụng nhiều đường Internet riêng biệt nhưng chưa chuyên hóa mục đích sử dụng.

Nguy cơ :

- Các nguy cơ đến từ bên ngoài:

+ Các cuộc tấn công Dos, Ddos vào hệ thống nhà trường.

+ Các virus, spam email được gửi từ bên ngoài vào.

+ Các cuộc tấn công bằng social engineering.

- Các nguy cơ từ bên trong:

+ Các lỗ hổng từ hệ điều hành, phần mềm cài đặt trên máy do chưa được update.

+ Các spam, virus lây lan bên trong mạng.

+ Các hành vi vô tình hay cố tình nhằm đánh cắp, phá hủy dữ liệu

+ Các sự cố gây ảnh hưởng đến dữ liệu

3.2. Đề xuất các giải pháp bảo mật cho mạng nội bộ tại trường đại học Hà Nội

Để quản lý tập trung dữ liệu và các dịch vụ, đồng thời đảm bảo an toàn thông tin cho hệ thống mạng học viên đề xuất một số giải pháp như sau:

3.2.1. Giải pháp mạng

Xây dựng phòng máy chủ tập trung tại nhà A. Sử dụng Firewall cứng Cisco để bảo vệ. Đồng thời tách hệ thống thành 3 khu vực: LAN, WAN, DMZ. Khu vực DMZ sẽ đặt các máy chủ: Web, Mail, File. Phần mềm quản lý nhân sự, cách ly hoàn toàn với khu vực người dùng. Tránh lây nhiễm Virus và lỗi do phía máy Client của người dùng gây ra.

Khu vực LAN sẽ sử dụng Switch layer 3 Cisco cấu hình VLAN, tách các khoa, phòng ban và các phòng máy ra riêng biệt.

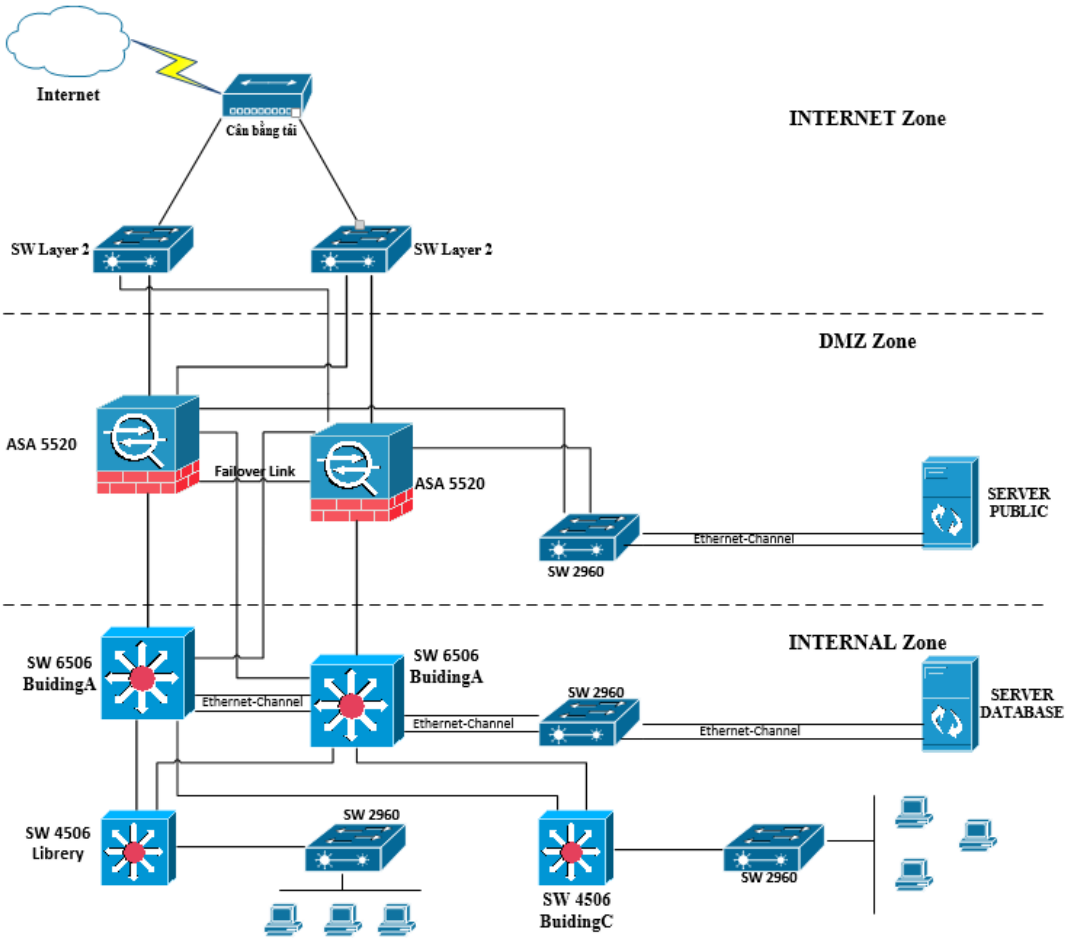
Đề xuất giải pháp thiết kế hệ thống mạng với tính dự phòng và tính sẵn sàng cao với Firewall Cisco ASA5520

Cisco ASA5520 có thể giúp bảo vệ một hoặc nhiều mạng từ những kẻ xâm nhập và tấn công. Kết nối giữa các mạng này có thể được kiểm soát và theo dõi bằng cách sử dụng các tính năng mạnh mẽ mà Cisco ASA cung cấp có thể đảm bảo rằng tất cả lưu lượng truy cập từ các mạng tin cậy cho đến mạng không tin cậy(và ngược lại) đi qua các tường lửa dựa trên chính sách an ninh của tổ chức.

Giao thức AAA và dịch vụ hỗ trợ của Cisco ASA. AAA cung cấp các giải pháp khác nhau để điều khiển kiểm soát truy cập đến các thiết bị mạng

Kiểm tra ứng dụng: Cơ chế kiểm tra ứng dụng của Cisco sử dụng để kiểm tra độ an ninh của các ứng dụng và dịch vụ trong hệ thống. Các công cụ kiểm tra trạng thái thông tin về mỗi kết nối đi qua các interface của thiết bị an ninh và đảm bảo chúng là hợp lệ.

Tổng quan hệ thống:



Hình 3. 2: Hệ thống mạng với ASA 5520

Hệ thống bao gồm các thành phần:

- Vùng Internet sử dụng nhiều đường truyền qua bộ cân bằng tải nhằm đảm bảo tính sẵn sàng cao có thể đáp ứng 24/24 các yêu cầu của người dùng bên trong cũng như các người dùng ở xa truy nhập vào hệ thống của trường. Với đề xuất trên em chủ yếu thiết kế dựa trên các công nghệ ưu việt của hãng Cisco. Với hệ thống cân bằng tải, cùng với tính năng Failover được triển khai trên hai thiết bị ASA 5520 sẽ cung cấp cho hệ thống độ an toàn cao và khả năng dự phòng linh hoạt. Hệ thống firewall hỗ trợ bảo mật, mã hóa, antivirus, lọc web, IPS/IDS …

- Vùng DMZ Zone chứa máy chủ hỗ trợ các dịch vụ mail, web, ftp .. có thể public ra ngoài cho người dùng ở ngoài và cả người dùng bên trong.

- Vùng Ineternal Zone, với hai Switch layer 3 đảm nhiệm luôn vai trò vừa là Core layer và Distribution layer nhằm tiết kiệm chi phí cũng như việc cấu hình và vận hành hệ thống. Lớp Core chịu trách nhiệm vận chuyển khối lượng lớn dữ liệu mà vẫn đảm bảo độ tin cậy và sự sẵn sàng cao. Trên hai Switch lớp Core này ta có thể cấu hình tính năng cluster switch hay High Availability.

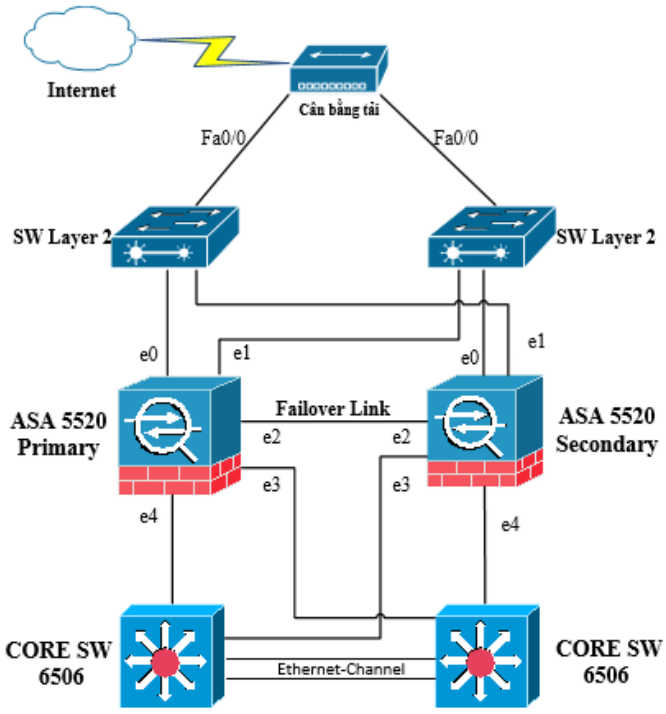
Các giải pháp ứng dụng để xây dựng hệ thống :

- Tính năng Failover : Ở đây ta sẽ sử dụng tính năng Failover theo mô hình Actvie/Active để tang hiệu năng xử lý cũng như tận dụng tối đa hoạt động của thiết bị. Ở chế độ Active/Active thì hai thiết bị ASA/PIX hoạt động cùng lúc và theo kịch bản mà người quản trị định trước.

- Công nghệ Etherchannel là công nghệ của Cisco cho phép kết hợp các kết nối Ethernet thành mộ bó (bundle) để tăng băng thông. Mỗi bundle có thể bao gồm từ hai đến tám kết nối FastEthernet hay Gigabit Ethernet tạo thành mội kết nối logic gọi là FastEthernet Channel hay Gigabit Ethernet Channel. Kết nối này cung cấp băng thông lên đến 1600Mbps (16Gbps).

- Áp dụng công nghệ Etherchannel trên giao tiếp giữa các máy chủ và switch để tăng băng thông. Trên các máy chủ sử dụng card mạng hỗ trợ công nghệ Etherchannel và sử dụng phần mềm đi kèm theo máy chủ, như HP Auto Port Aggregation ..

Mô hình Failover Active/Active trên hệ thống



Hình 3. 3: Mô hình Failover Active/Active

Bảng 3. 1. Bảng phân chia địa chỉ

STT	Loại TB	Tên Port	Chức năng	IP Address	Subnetmask
1	PRIMARY	E0	Outside(admin)	192.168.0.1	/29
		E1	Outside(ctx1)	192.168.0.10	/29
		E2	Folink	172.16.1.1	/30
		E3	Inside(ctx1)	10.10.20.2	/24
		E4	Inside(admin)	10.10.10.1	/24
2	SECONDARY	E0	Outside(ctx1)	192.168.0.9	/29
		E1	Outside(admin)	192.168.0.2	/29
		E2	Folink	172.16.1.2	/30
		E3	Inside(admin)	10.10.10.2	/24
		E4	Inside(ctx1)	10.10.20.1	/24
3	RJ1	Fa0/0		192.168.0.3	/29
4	RJ2	Fa0/0		192.168.0.11	/29

3.2.2. Giải pháp an toàn bảo mật dữ liệu

Đối với vấn đề an toàn bảo mật dữ liệu em dùng các phương pháp sau:

- Phân quyền truy cập: Ta sẽ phân quyền truy cập cho các phòng ban. Tùy theo yêu cầu của từng đối tượng sau khi khảo sát chi tiết phía người dùng sẽ đưa ra chính sách phân quyền.

- Backup File Server: Ta sử dụng Service Backup File Server có sẵn trên nền tảng Window Server nhằm tạo một bản sao lưu trữ dữ liệu đề phòng các trường hợp hỏng hóc làm mất mát dữ liệu ngoài ý muốn.

- Cài đặt phần mềm diệt virus bản quyền trên các máy tính client cũng như trên server để tránh virus tấn công gây hại đến dữ liệu.

3.2.3. Giải pháp về người sử dụng

Về người sử dụng, đề xuất một số giải pháp sau:

- Mỗi người sử dụng cần phải chịu hoàn toàn trách nhiệm với tài khoản đăng nhập vào hệ thống máy tính (Domain Server).

- Cần phải xây dựng và tuân thủ nghiêm ngặt chính sách an ninh hệ thống, kết hợp với các hình thức kỉ luật trong nhà trường khi xảy ra các lỗi đến từ phía người dùng.

3.3. Triển khai thử nghiệm và đánh giá một số giải pháp bảo mật đề xuất

3.3.1. Nội dung thử nghiệm

Luận văn thực hiện thử nghiệm một số nội dung sau đây.

- Cấu hình một số dịch vụ trên tường lửa Cisco ASA 5520.
- Chia Vlan trên các Switch Cisco.
- Phân quyền truy cập dữ liệu trên File Server, Domain.
- Backup File Server.
- Xây dựng chính sách bảo mật cho hệ thống trường.

Từ đó có cơ sở để đề xuất triển khai trong thực tế.

(1) Triển khai thử nghiệm ASA 5520 và cấu hình một số dịch vụ

Sau khi lắp đặt ASA ở vị trí phù hợp trong hệ thống như đã thiết kế, ta sẽ triển khai các luật sau cho ASA:

Học viên thực hiện cấu hình chia hệ thống ra làm 3 khu vực: WAN (2 đường mạng), LAN và DMZ và thiết lập các Rules cần thiết.

- Cho phép vùng inside và DMZ ra ngoài internet
- Cho phép mạng inside truy cập vào DMZ.
- Thực hiện cấm mạng bên ngoài (vùng internet) truy cập vào hệ thống mạng của công ty.

Có 6 lệnh cấu hình cơ bản cho ASA/PIX Firewall:

1. Nameif – Gán tên đến mỗi giao diện mạng vành đai và chỉ định mức an ninh cho nó

2. Interface – Cấu hình kiểu và khả năng của mỗi giao diện vành đai

3. Ip address – gán một địa chỉ ip cho mỗi cổng

4. Nat – che dấu địa chỉ trên mạng inside từ mạng outside

5. Global – Che dấu địa chỉ IP trên mạng inside từ mạng outside sử dụng một pool (một dải địa chỉ public) của địa chỉ IP

6. Route – định nghĩa một tuyến đường tĩnh hoặc tuyến đường mặc định cho một interface.

Kết quả cần đạt: Cisco ASA5520 có thể giúp bảo vệ một hoặc nhiều mạng từ những kẻ xâm nhập và tấn công. Thông qua Rules sẽ cho phép các khu vực có thể kết nối được với nhau. Ngoài ra, hệ thống cần public web từ trong khu vực DMZ ra ngoài WAN để bên ngoài mạng có thể truy cập được web. Quá trình chia ra làm 3 khu vực giúp hệ thống dễ dàng quản lý, tránh lây lan mã độc và chống lại các cuộc tấn công từ bên trong cũng như bên ngoài.

(2) Chia Vlan trên các Switch

Học viên thực hiện cấu hình Switch (ở đây là switch cisco), tạo ra các Vlan (C1 – Vlan 11, C2 – Vlan 12,...) và kết nối chúng tới Switch tổng. Kết quả cần đạt được: Sau khi chia các VLAN, các đường truyền mạng hoạt động ổn định. Các Vlan tách biệt nhau giúp dễ dàng kiểm soát.

(3) Phân quyền truy cập dữ liệu trên File Server, Domain

Học viên thực hiện quá trình tạo ra các folder chứa các dữ liệu của từng phòng ban cũng như các tài khoản của từng phòng ban trong trường Đại học Hà Nội.

Kết quả cần đạt: Chỉ có tài khoản của phòng ban được cấp quyền mới có quyền truy cập vào folder chứa dữ liệu của họ, cũng như không thể truy cập vào dữ liệu phòng ban khác, nhằm chống ăn cắp dữ liệu, các hành vi phá hoại cố ý hoặc vô ý, khoanh vùng kịp thời để phát hiện thủ phạm nếu có vấn đề xảy ra.

(4) Backup File Server

Học viên sử dụng công cụ Backup File Server trên Window Server để có thể backup dữ liệu. Sau khi cài đặt Backup File Server và thông qua giao diện để có thể dễ dàng backup lại những dữ liệu cần thiết.

Kết quả cần đạt: Khi xảy ra sự cố về mất mát hay hỏng hóc dữ liệu, hệ thống có thể dễ dàng khôi phục lại bằng khả năng recovery của công cụ đã cài đặt.

(5) Xây dựng chính sách bảo mật cho hệ thống trường

Học viên đề xuất xây dựng một chính sách bảo mật cho hệ thống của trường, từ đó học sinh và nhân viên có thể tuân theo các quy tắc để đảm bảo an toàn được hệ thống mạng nội bộ của trường.

Kết quả cần đạt: Chính sách bảo mật phải chặt chẽ, phù hợp với hiện trạng của trường Đại học Hà Nội.

3.3.2. Kết quả thử nghiệm và đánh giá

Chi tiết kết quả thử nghiệm trình bày trong phần phụ lục. Tất cả các thử nghiệm trên đều cho kết quả khả quan cũng như vận hành tốt, ổn định, đáp ứng được các yêu cầu bảo mật mạng LAN.

Các giải pháp đã thử nghiệm có thể ứng dụng cho mạng nội bộ tại trường Đại học Hà Nội và đáp ứng được các nhu cầu của quá trình đào tạo, quản lý trong nhà trường.

3.4. Kết luận chương 3

Chương 3 của luận văn đã khảo sát mạng nội bộ tại trường Đại học Hà Nội, các vấn đề nảy sinh trong quá trình sử dụng và các yêu cầu bảo mật mạng nhằm đáp ứng nhu cầu đào tạo của nhà trường.

Luận văn cũng đề xuất một số giải pháp bảo mật cho mạng nội bộ của trường Đại học Hà Nội. Qua thử nghiệm cho thấy Cisco ASA5520 có thể giúp bảo vệ một hoặc nhiều mạng từ những kẻ xâm nhập và tấn công. Kết nối giữa các mạng này có thể được kiểm soát và theo dõi bằng cách sử dụng các tính năng mạnh mẽ mà Cisco ASA cung cấp có thể đảm bảo rằng tất cả lưu lượng truy cập từ các mạng tin cậy cho dến mạng không tin cậy(và ngược lại). Các giải pháp bảo mật đề xuất có thể triển khai trong thực tế và phù hợp với các yêu cầu đề ra.

Trên thực tế, không có một giải pháp toàn diện nào cho việc phòng chống các loại hình tấn công trên mạng. Phòng chống các nguy cơ tấn công mạng không phải trách nhiệm của một cá nhân hay tổ chức, mà là của cộng đồng.

Các giải pháp cơ bản phòng chống:

- Đào tạo nâng cao nhận thức và kỹ năng khai thác dịch vụ cho người sử dụng.

- Thay đổi quan điểm phòng chống tấn công: phòng chống không chỉ từ bên ngoài mà ngay cả từ bên trong nội bộ.

- Triển khai các hệ thống giám sát bảo vệ toàn mạng nhằm tự động phát hiện và cô lập các truy cập, hoạt động trái phép trên mạng nội.

- Xây dựng chính sách phòng chống APT (Advanced persistent threat) ngay từ bên trong mạng nội bộ.

Bảo mật mạng máy tính là một công việc khó và có tính chất nhạy cảm trong một tổ chức. Bên cạnh việc đầu tư các trang thiết bị phần cứng cho cơ sở hạ tầng mạng, còn phải có một đội ngũ quản trị viên có kiến thức sâu rộng trong việc vận hành, khai thác các dịch vụ trong mạng LAN cũng như trên mạng Internet có hiệu quả.

KẾT LUẬN

Các kết quả đạt được của luận văn:

Với mục tiêu nghiên cứu giải pháp bảo mật cho mạng LAN và ứng dụng tại Trường Đại học Hà nội, Luận văn đã đạt được một số kết quả sau đây:

- Nghiên cứu các yêu cầu bảo mật cho mạng LAN.

- Nghiên cứu các giải pháp bảo mật cho mạng LAN.

- Về giải pháp luận văn đề xuất một số giải pháp bảo mật có thể triển khai cho mạng nội bộ tại Trường Đại học Hà nội gồm:

+ Hiểu được tổng quan, các khái niệm và công nghệ cũng như kiến trúc xây dựng hệ thống firewall.

+ Ứng dụng, triển khai các tính năng của Cisco Firewall.

+ Đưa ra đề xuất giải pháp mô hình mạng sử dụng firewall ASA 5520 có tính bảo mật, sẵn sàng và độ dự phòng cao.

+ Chia các VLAN trên các Switch.

+ Phân quyền truy cập dữ liệu trên File Server.

+ Backup dữ liệu Server.

- Kết quả của việc sử dụng Firewall, VLAN và kết hợp với phân quyền truy cập để bảo vệ mạng nội bộ. Cho phép người quản trị mạng xác định một điểm khống chế ngăn chặn để phòng ngừa tin tặc, kẻ phá hoại, xâm nhập mạng nội bộ. Cấm không cho các loại dịch vụ kém an toàn ra vào mạng, đồng thời chống trả sự công kích đến từ các đường khác. Tính an toàn mạng được củng cố trên hệ thống Firewall mà không phải phân bố trên tất cả máy chủ của mạng. Bảo vệ những dịch vụ yếu kém trong mạng.

Hướng phát triển tiếp theo:

Học viên sẽ tiếp tục nghiên cứu, kết hợp thêm phương pháp bảo mật khác để hoàn thiện giải pháp bảo mật cho mạng LAN và có thể triển khai một cách hiệu quả trong thực tế.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Nguyễn Tiến Ban (2011) – "Công nghệ IP/MPLS và các mạng riêng ảo" - Học viện Công nghệ Bưu chính Viễn thông.

[2] Hoàng Xuân Dậu (2007) – "Bài giảng an toàn bảo mật hệ thống thông tin" - Học viện Công nghệ Bưu chính Viễn thông.

[3] Hoàng Đăng Hải (2018) – "Quản lý an toàn thông tin" - Học viện Công nghệ Bưu chính Viễn thông.

[4] Phương Minh Nam (2010) - "Nguy cơ mất an ninh, an toàn thông tin, dữ liệu và một số giải pháp khắc phục" – Bộ Công An.

Tiếng Anh

[5] M. Bishop (2005) – "Introduction to Computer Security".

[6] Earl Carter (2002) - "Introduction to Network Security" - Cisco Secure Intrusion Detection System, Cisco Press.

[7] IEEE std. 802 IQ. (2005) – "Virtual Bridged Local Area Networks".

[8] K.R. Karthikeyan, A. Indra (2010) – "Intrusion Detection Tools and Techniques: A Survey" - International Journal of Computer Theory and Engineering, Vol.2, No.6.

[9] Rinat Khoussainov, Ahmed Patel (2000) – "LAN security: Problems and Solutions" – Computer Standard & Interface, V. 22, pp. 191-202.

[10] Timo Kiravuo, Mikko Sarela, Jukka Maner (2013) – "A Survey of Ethernet LAN Security" – IEEE, V. 15, pp. 1477-1491.

Trang WEB

[11] http://searchsecurity.com/

[12] http://www.cisco.com/go/vpn

[13] https://www.oreilly.com/library/view/cisco-asa-and/1587051583/

[14]https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_ri%C3%AAng_%E1%BA%A3o

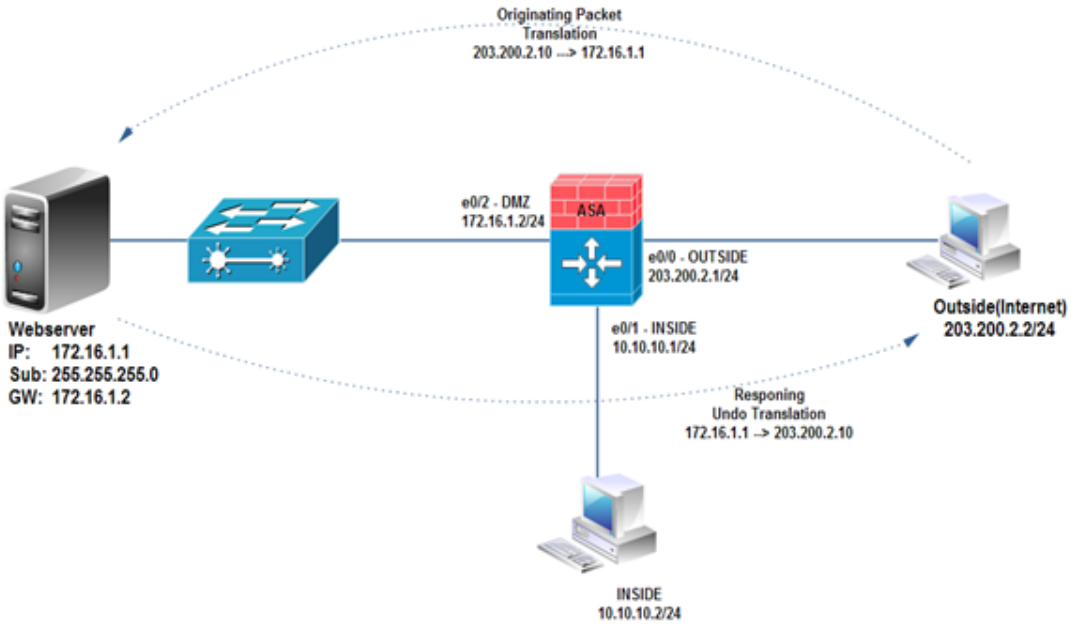
PHỤ LỤC

Trong phần phụ lục, Học viên trình bày chi tiết một số thử nghiệm các giải pháp bảo mật triển khai tại Trường Đại học Hà Nội bao gồm:

- Triển khai thử nghiệm Cisco 5520 và cấu hình một số dịch vụ
- Chia Vlan trên các Switch

Cấu hình một số dịch vụ trên Firewall Cisco ASA 5520

1. Publich website qua tường lửa Cisco



Hình 1: Mô hình demo NAT và PAT

Mô tả:

− Cho phép người dùng ngoài internet có thể truy nhập vào website của trường và quản trị viên có thể dùng Remote Desktop vào Webserver để quản lý.

− Cho phép người dùng trong vùng INSIDE có thể truy nhập Webserver và sử dụng các dịch vụ trên đó.

Chuẩn bị:

− Máy chủ cài Windows Server 2012.

− Các thiết bị được cấu hình địa chỉ như hình vẽ.

Cấu hình trên ASA:

Định nghĩa thông tin cổng inside

ASA(config)# interface e0/0

ASA(config-if)# ip address 203.200.2.1 255.255.255.0

ASA(config-if)# nameif outside

ASA(config-if)# no shut

Định nghĩa thông tin cổng outsde

ASA(config)# interface e0/1

ASA(config-if)# ip address 10.10.10.1 255.255.255.0

ASA(config-if)# nameif inside

ASA(config-if)# no shut

Định nghĩa thông tin cổng dmz

ASA(config)# interface e0/2

ASA(config-if)# ip address 172.16.1.2 255.255.255.0

ASA(config-if)# nameif dmz

ASA(config-if)# no shut

Thực hiện Nat tĩnh

ASA(config)# static (dmz,outside) tcp 203.200.2.10 80 172.16.1.1 80

ASA(config)# static (dmz,outside) tcp 203.200.2.10 3389 172.16.1.1 3389

Tạo ACL cho phép truy cập dịch vụ trong DMZ

ASA(config)# access-list AL_WEB permit tcp any host 203.200.2.10 eq 80

ASA(config)# access-list AL_WEB permit tcp any host 203.200.2.10 eq 3389

ASA(config)# access-group AL_WEB in interface outside

Cho phép vùng INSIDE truy nhập vào Webserver không cần NAT

ASA(config)# access-list IN_DMZ permit ip 10.10.10.0 255.255.255.0 host 172.16.1.1

ASA(config)# nat (inside) 0 access-list IN_DMZ

2. Cấu hình PAT cho phép vùng INSIDE ra ngoài INTERNET

Mô tả:

Cho phép người dùng trong vùng INSIDE có thể sử dụng các dịch vụ ngoài vùng INTERNET và được ánh xạ ngay tại địa chỉ cổng của ASA.

Cấu hình trên ASA:

Định nghĩa tuyến mặc định

ASA(config)# route outside 0 0 203.200.2.2

Xác định mạng được NAT hoặc PAT

ASA(config)# nat (inside) 1 10.10.10.0 255.255.255.0

Xác định NAT hoặc PAT trên cổng outside

ASA(config)# global (outside) 1 interface

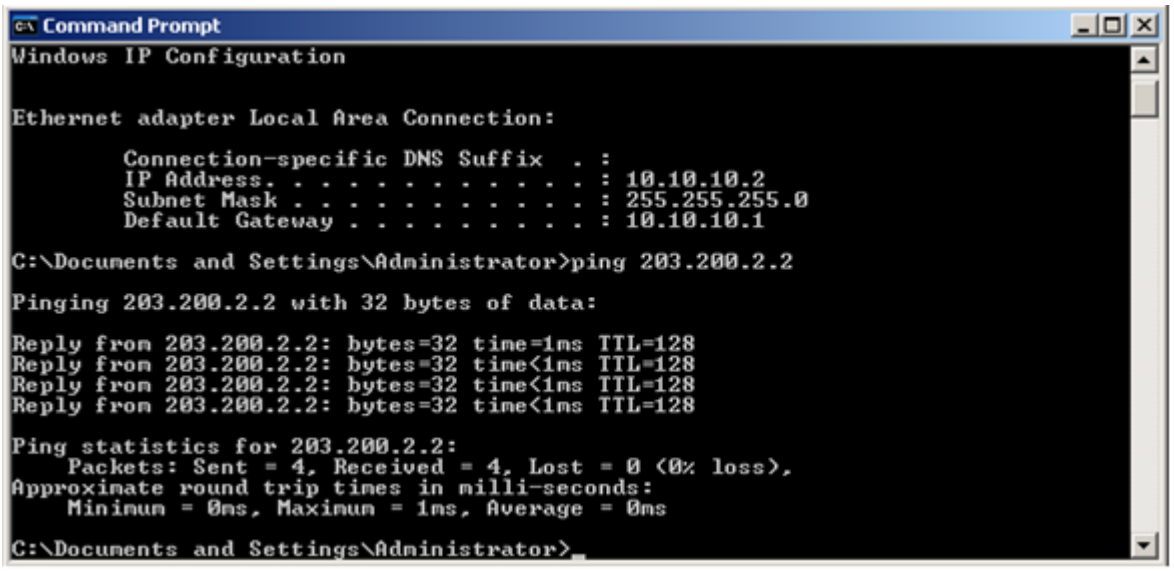
INFO: outside interface address added to PAT pool

Mặc dù có thể truy phần lớn những dịch vị cần thiết ngoài Internet như http, pop3, smtp, ftp... Nhưng với icmp thì ASA không cho phép gói echo-reply được trả về. Để giải quyết trường hợp này cần tạo chính sách cho echo-reply được trả về:

ASA(config)# access-list PING permit icmp any any echo-reply

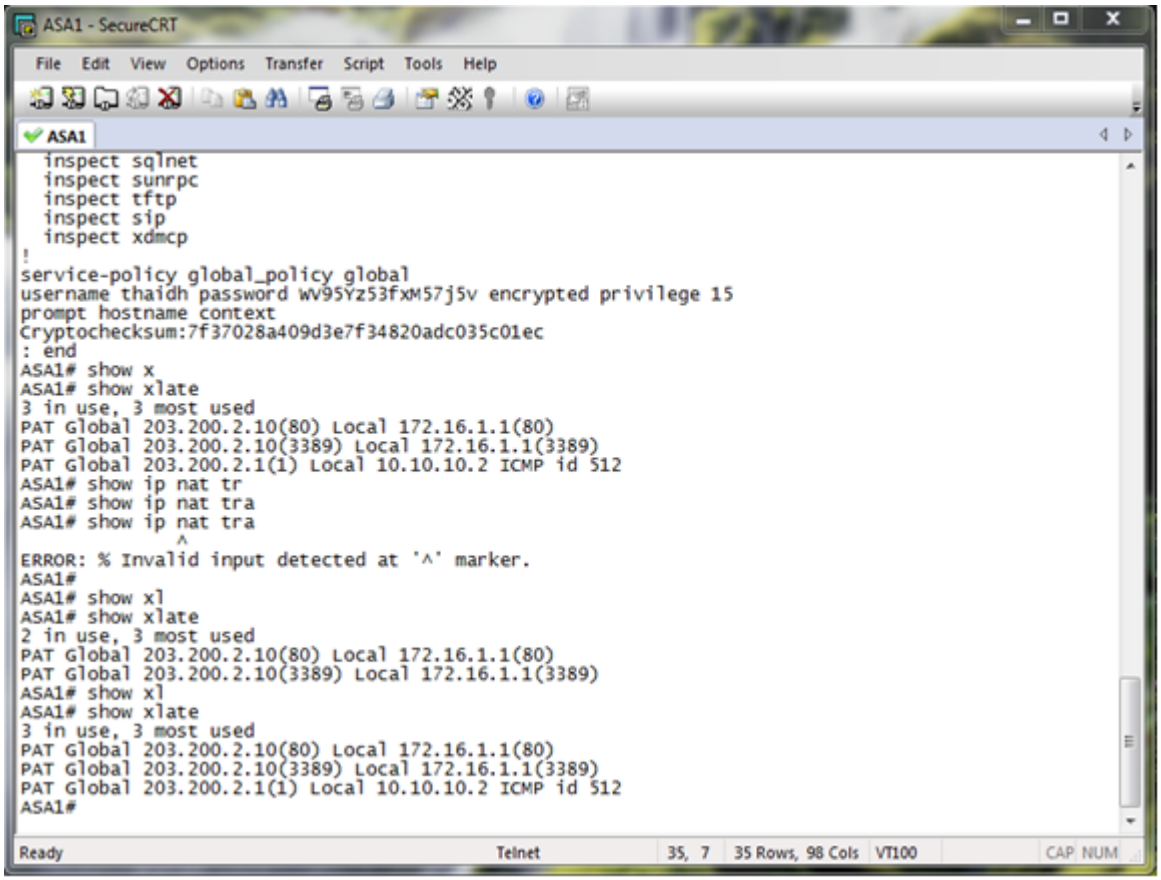
ASA(config)# access-group PING in interface outside

Kiểm tra từ máy trong vùng INSIDE:



Hình 2: Kết quả Ping thành công

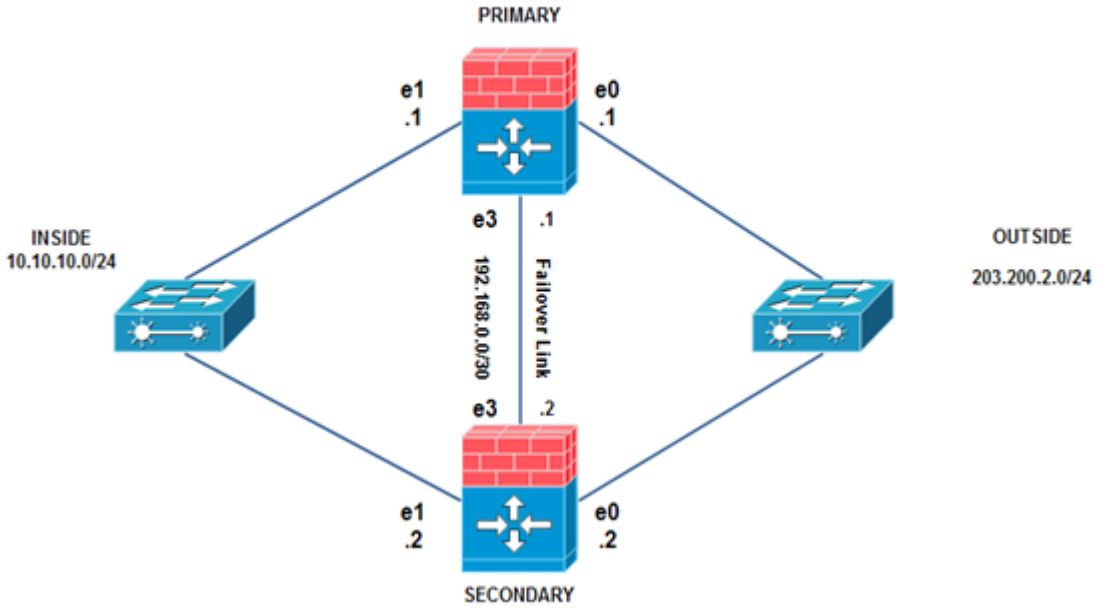
Kết quả là từ máy tính trong vùng INSIDE đã ping thành công ra ngoài vùng OUTSIDE.



Hình 3: Bảng ánh xạ địa chỉ PAT

Khi thực hiện Ping thành công, địa chỉ máy trong vùng INSIDE 10.10.10.2 đã được ánh xạ sang địa chỉ vùng OUTSIDE.

3. Cấu hình dự phòng Failover Active/Stanby



Hình 4: Mô hình Failover Active/Standby

Mô tả : Với tính năng Failover sẽ cho phép hệ thống có tính dự phòng, khi thiết bị chính (Primary) có vấn đề thì thiết bị phụ đóng vai trò là Secondary sẽ từ chế độ chờ (Standby) chuyển sang chế độ hoạt động (Active) để đảm nhiệm thay vai trò của Primary. Và khi Primary hoạt động trở lại thì nó lại chuyển về đúng vai trò như ban đầu.

Cấu hình :

Trên ASA đóng vai trò làm PRIMARY

Định nghĩa thông tin cổng OUTSIDE và cổng dự phòng cho cổng này.

ASA(config)# int Ethernet 0/0

ASA(config)# no shutdown

ASA(config)# ip add 203.200.2.1 255.255.255.0 standby 203.200.2.2

ASA(config)# nameif outside

Định nghĩa thong tin cổng INSIDE và cổng dự phòng cho cổng này.

ASA(config)# int Ethernet 0/1

ASA(config)# no shutdown

ASA(config)# ip add 10.10.10.1 255.255.255.0 standby 10.10.10.2

ASA(config)# nameif inside

Active cổng đóng vai trò làm Failover link

ASA(config)# int Ethernet 0/3

ASA(config)# no shutdown

Kích hoạt tính năng failover trên Primay

ASA(config)# failover

ASA(config)# failover lan unit primary

ASA(config)# failover lan interface lolink Ethernet0/3

ASA(config)# failover polltime unit msec 500

ASA(config)# failover link lolink Ethernet0/3

ASA(config)# failover interface ip lolink 192.168.0.1 255.255.255.252 standby 192.168.0.2

ASA(config)# failover

Trên ASA đóng vai trò làm SECONDARY

Active cổng đóng vai trò làm Failover link

ASA(config)# int Ethernet 0/3

ASA(config)# no shutdown

Kích hoạt tính năng failover trên Secondary

ASA(config)# failover

ASA(config)# failover lan unit secondary

ASA(config)# failover lan interface lolink Ethernet0/3

ASA(config)# failover link lolink Ethernet0/3

ASA(config)# failover interface ip lolink 192.168.0.1 255.255.255.252 standby 192.168.0.2

ASA(config)# failover

Kiểm tra tính năng Failover trên Primary

PRIMARY# show failover

Failover On

Failover unit Primary

Failover LAN Interface: lolink Ethernet0/3 (up)

Unit Poll frequency 500 milliseconds, holdtime 2 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 2 of 250 maximum

Version: Ours 8.0(2), Mate 8.0(2)

This host: Primary - Active

Active time: 690 (sec)

slot 0: empty

Interface outside (203.200.2.1): Normal

Interface inside (10.10.10.1): Normal

slot 1: empty

Other host: Secondary - Standby Ready

Active time: 0 (sec)

slot 0: empty

Interface outside (203.200.2.2): Normal

Interface inside (10.10.10.2): Normal

slot 1: empty

Stateful Failover Logical Update Statistics

Link : lolink Ethernet0/3 (up)

PRIMARY#

Kiểm tra tính năng Failover trên Secondary

PRIMARY# show failover

Failover On

Failover unit Secondary

Failover LAN Interface: lolink Ethernet0/3 (up)

Unit Poll frequency 500 milliseconds, holdtime 2 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 2 of 250 maximum

Version: Ours 8.0(2), Mate 8.0(2)

This host: Secondary - Standby Ready

Active time: 0 (sec)

slot 0: empty

Interface outside (203.200.2.2): Normal

Interface inside (10.10.10.2): Normal

slot 1: empty

Other host: Primary - Active

Active time: 768 (sec)

slot 0: empty

Interface outside (203.200.2.1): Normal

Interface inside (10.10.10.1): Normal

slot 1: empty

Stateful Failover Logical Update Statistics

Link : lolink Ethernet0/3 (up)

PRIMARY#

4. Chia Vlan trên Switch

(*Có tham khảo mã nguồn Cisco Certified Network Associate – Cisco Academy*)

- Cấu hình cơ bản tại tất cả các Switch:

Switch>enable

Switch#configure terminal

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#login

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#login

Switch(config-line)#exit

Switch(config)#banner motd "Xinchao"

Switch(config)#enable secret cisco

Switch(config)#service password-encryption

- Cấu hình các Switch con (tại các tòa nhà):

Switch(config)#hostname C1

C1(config)#vlan 11 //ID Vlan, mỗi phòng ban/tầng có một ID riêng

C1(config-vlan)#name C //Tên Vlan

C1(config)#interface range f0/1-20 //Chọn cổng từ 1 đến 20

C1(config-if-range)#switchport access vlan 11

C1(config-if-range)#exit

C1(config)#interface vlan 1 //Đặt IP Vlan1 để manage

C1(config-if)#no shutdown

C1(config-if)#ip address 100.0.0.5 255.255.255.0

C1(config-if)#end

C1#wr

(Làm tương tự, tạo ra các vlan 12 – C2, 13 – C3,… và đặt IP vlan 1 để manage)

- Cấu hình Switch 4650

Switch(config)#hostname SW4650

SW4650(config)#interface vlan 1 // Đặt IP Vlan1

SW4650(config-if)#no shutdown

SW4650(config-if)#ip address 100.0.0.2 255.255.255.0

SW4650(config-if)#exit

SW4650(config)#vlan 11 // Add các Vlan ở các SW

SW4650(config-vlan)#name C1

SW4650(config-vlan)#vlan 12

SW4650(config-vlan)#name C2

SW4650(config-vlan)#vlan 13

SW4650(config-vlan)#name C3

(…)

SW4650(config-vlan)#exit

SW4650(config)#interface range f0/1-10

SW4650(config-if-range)#switchport mode trunk

SW4650(config-if-range)#end

SW465#wr

5. Triển khai File server kết hợp với DC và phân quyền

File Server: Ở đây ta sẽ cài đặt Window Server 2012 lên Server. Sau đó ta cài đặt một số dịch vụ: DC, DNS, Web,... (có thể thêm tùy nhu cầu)

Riêng dịch vụ File Server đã được cài mặc định sau khi cài Window Server 2012

Sau khi cài đặt xong, ta vào trong ổ cứng và tạo các Folder chứa dữ liệu của các phòng ban...ở bên trong Folder Data.

Trong Folder sẽ chứa các tài nguyên ở các khoa.

DC + Phân quyền truy cập: Giờ ta cần tạo ra các User và Group trong Domain để phân quyền truy cập dữ liệu cho từng phòng ban cũng như cá nhân. Ta vào Active Directory User and Computers và tạo User cũng như Group.

Sau khi tạo cũng như add User vào trong Group. Ta trở lại các Folder, ấn chuột trái vào Properties, chọn Sharing và add các Group (hoặc User).

Ở đây ta add những Group vào trong Folder Data để cho phép các User trong Group được phép truy cập vào trong Folder Data. Tiếp theo vào trong Folder Data và phân quyền hẹp đi cho từng Folder một.

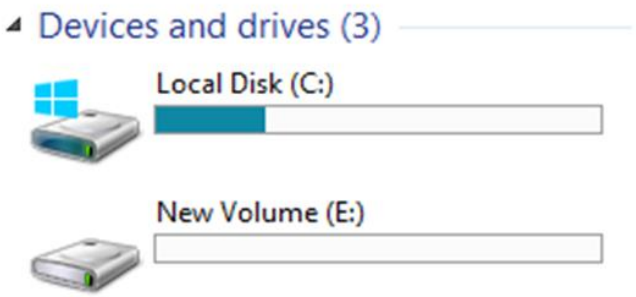
Sau khi đã phân quyền truy cập File, ta sẽ test bằng cách đăng nhập vào tài khoản ở máy Client đã Join Domain của máy chủ.

Vào Window + R ->\\(IP Server), ta thấy nó đã hiện Folder Data

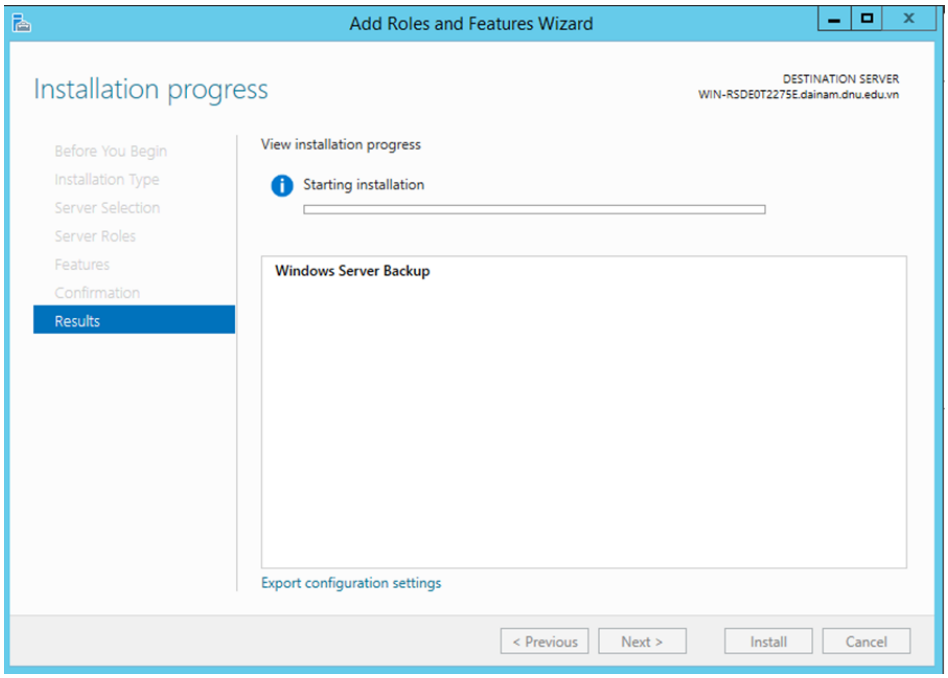
Vậy là ta đã hoàn thành việc tạo File Server cũng như phân quyền truy cập dữ liệu kết hợp DC.

6. Backup File trên Server

Đầu tiên ta cần phải có một phân vùng hoặc một ổ cứng khác để làm nhiệm vụ backup (Ở đây là ổ E), sau đó ta cài Window Server Backup lên Server.

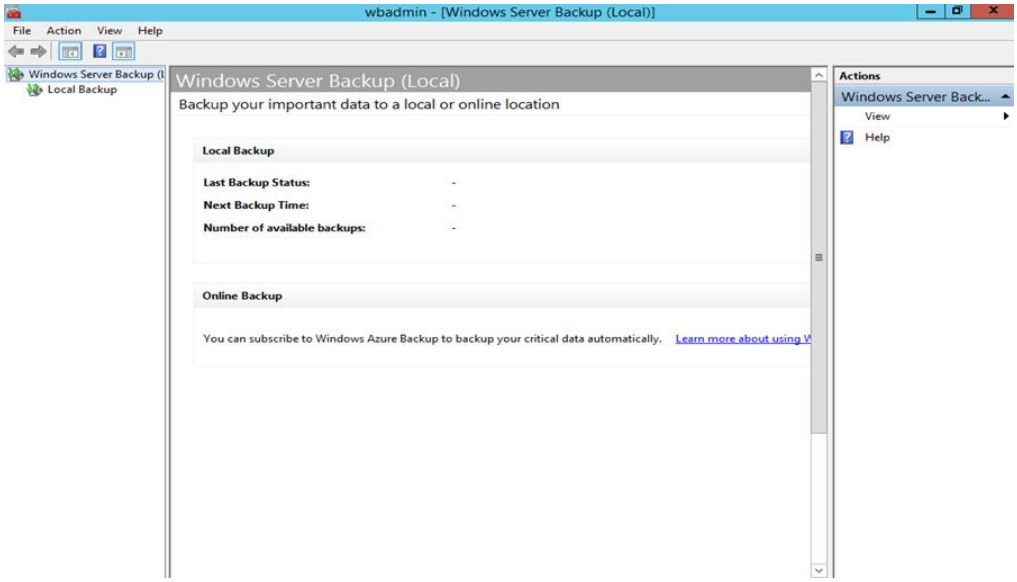


Hình 5: Tạo phân vùng mới lưu trữ Backup



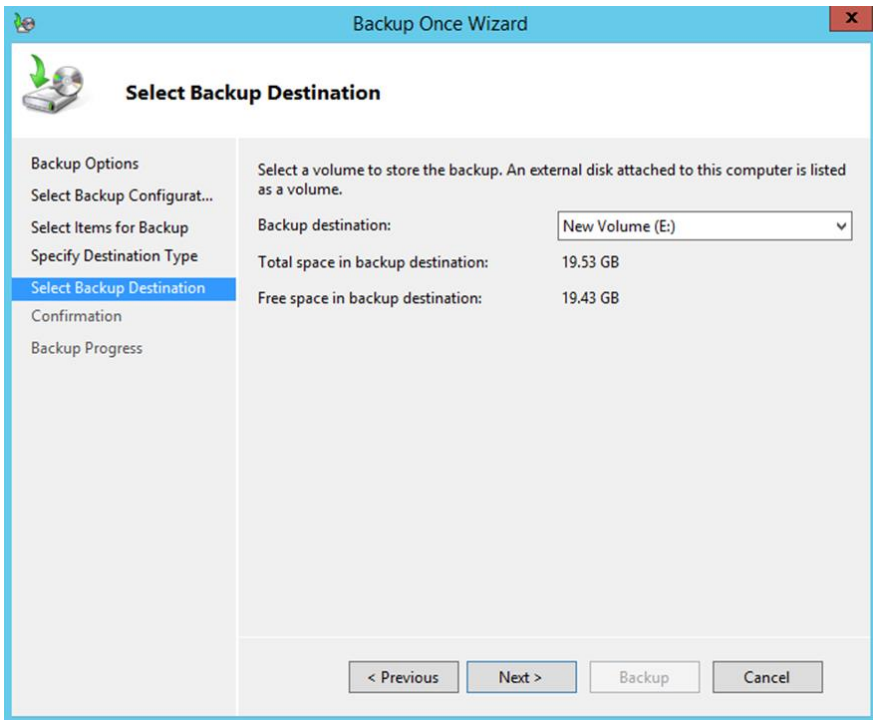
Hình 6: Cài đặt Window Server Backup

Sau đó ta khởi động Window Server Backup.



Hình 7: Giao diện Window Server Backup

Ở phần Local Backup, ta ấn Backup Once. Trong Backup Once Wizard, có 2 lựa chọn Backup là Full Server là backup toàn bộ và Custom là backup những file ta chọn. Tùy nhu cầu, ở đây ta sẽ chọn Custom để backup Folder Data chứa dữ liệu của các khoa mà ta vừa tạo ở trên. Sau đó ta chọn ổ lưu trữ bản Backup (Ổ E) rồi ấn Backup.



Hình 8: Chọn ổ đĩa lưu trữ Backup

Vậy là ta đã hoàn thành việc Backup dữ liệu để Recovery lại dữ liệu khi xảy ra sự cố.

7. Xây dựng chính sách bảo mật cho hệ thống mạng trường Đại học Hà Nội

Chính sách nội bộ

- Xây dựng được một "document" mô tả toàn bộ hệ thống mạng của Trường Đại học Hà Nội. (đã nói trong chương 3)

- Hệ thống mạng phải được bảo mật. Điều này thực hiện thông qua các giải pháp mà ta vừa áp dụng ở trên.

- Chính sách đảm bảo an toàn cho vùng server nội bộ: Các server nội bộ public ra bên ngoài thông qua firewall. Ngoài ra ta cũng kiểm soát được bên trong thông qua phân quyền truy cập dữ liệu.

- Sao lưu dữ liệu thường xuyên: Đặt một giờ cố định (12h đêm mỗi ngày)

- Quản lý các file cấu hình của các thiết bị trong mạng : các file cấu hình trên router, switch trong trường cần phải được quản lý sao lưu.

- Quản lý các đường định tuyến, các bảng routing table trên router cũng như switch nhằm tránh bị loop.

Chính sách Quản lý tài sản

Tất cả các học sinh và nhân viên có quyền truy nhập vào hệ thống máy tính trong trường phải tuân thủ các chính sách được đề ra nhằm bảo vệ hệ thống máy tính, mạng máy tính, sự toàn vẹn dữ liệu và an toàn thông tin của trường.

Chính sách Quản lý con người

- Mỗi học sinh, nhân viên sẽ được cấp một tài khoản để đăng nhập vào hệ thống máy tính. Password để đăng nhập vào tài khoản máy tính phải có độ phức tạp (bao gồm chữ in hoa, các ký tự đặt biệt… do các nhân viên IT cấp) và học sinh, nhân viên phải tự bảo quản không để mất mát, rò rỉ. Nếu bị mất hoặc bị lộ phải báo với nhân viên IT để giải quyết. Nếu học sinh, nhân viên không còn sử dụng tài khoản nữa thì tài khoản của học sinh, nhân viên đó sẽ bị xóa khỏi hệ thống.

- Mỗi học sinh, nhân viên phải có nghĩa vụ và trách nhiệm bảo quản các thiết bị được ủy quyền sử dụng, nếu có vấn đề xảy ra phải báo ngay với bộ phận IT để kịp thời xử lý.

- Học sinh, nhân viên không được cài đặt phần mềm không rõ nguồn gốc hoặc không có bản quyền ngoài các phần mềm phục vụ công việc được cài sẵn trên máy.

- Mỗi học sinh, nhân viên cần nghiêm túc thực hiện các chính sách của nhà trường đưa ra, nếu vi phạm phải chịu trách.

Học sinh, nhân viên bình thường

- Được cấp tài khoản cho phép truy cập các dữ liệu thông thường.

- Chỉ được phép sử dụng thiết bị khi đến giờ hành chính hoặc được sự cho phép.

- Không cố ý truy cập tài nguyên không thuộc thẩm quyền.

- Không sử dụng thiết bị vào mục đích khác

Nhân viên IT

- Có trách nhiệm giám sát, theo dõi hoạt động của các nhân viên khác trong nhà trường sử dụng máy tính vào công việc mà không làm chuyện riêng. Đảm bảo dữ liệu của nhà trường được bảo mật tránh thất thoát ra ngoài.

- Khi xảy ra sự cố phải báo cáo tình hình và mức độ thiệt hại cho cấp trên được biết. Phải khắc phục sự cố với thời gian nhanh nhất có thể để đảm bảo hệ thống hoạt động thông suốt.

- Chịu sự quản lý và nghiêm chỉnh chấp hành yêu cầu của cấp trên.

- Quản lý các tài nguyên của nhà trường, chịu trách nhiệm backup dữ liệu của nhà trường theo định.

- Nếu nhân viên IT nghỉ làm việc nhà trường phải thông báo trước với nhà trường và bàn giao toàn bộ công việc hiện thời đang làm và các thiết bị do mình quản lý cho nhân viên khác có cùng chuyên môn hoặc cho cấp trên...

Ban lãnh đạo

- Có toàn quyền quyết định các chính sách an ninh thông tin cho nhà trường

- Không được truy xuất vào dữ liệu, tài nguyên nội bộ của các nhân viên khác ngoại trừ những trường hợp đặt biệt.

- Có trách nhiệm tự bảo quản tài nguyên của nhà trường, các tài liệu cá nhân tránh để xảy ra tình trạng thất thoát dữ liệu.

- Có trách nhiệm giám sát các nhân viên cấp dưới