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 ngành: Kỹ thuật viên thông

Mã số: 8.52.02.08

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – 2019

Luận văn được hoàn thành tại:
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS. TS Nguyễn Tiến Ban

Phản biện 1: TS Nguyễn Ngọc Minh

Phản biện 2: TS Dư Đình Viên

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông
Vào lúc: ..... giờ ..... ngày 11 tháng 01năm 2020

Có thể tìm hiểu luận văn tại:
- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

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 các 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.

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

1.1 Các yêu cầu bảo mật chung cho mạng LAN

1.1.1 Yêu cầu bảo mật về mạng

- Yêu cầu về tính sẵn sàng của mạng.
- Yêu cầu về tính bền vững của mạng.
- Yêu cầu về độ tin cậy mạng.

1.1.2Yêu cầu về bảo mật dữ liệu

Yêu cầu về tính sẵn sàng của dữ liệu, yêu cầu về tính toàn vẹn dữ liệu, yêu cầu về bí mật dữ liệu:

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.

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

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.

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

1.3.1. Các mối đe dọa bảo mật mạng LAN

Mối đe dọa không có cấu trúc

Mối đe dọa có cấu trúc

1.3.2 Các phương thức tấn công mạng LAN

- Phương thức ăn cắp thông tin bằng Packet Sniffers
- Phương thức tấn công mật khẩu Password Attack
- Phương thức tấn công bằng Mail Relay
- Phương thức tấn công lớp ứng dụng
- Phương thức tấn công Virus và Trojan Horse

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.

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

Firewall là một công cụ hoạt động ở ranh giới giữa bên trong là mạng LAN với hệ thống Internet bên ngoài.

2.1.2 Tường lửa Cisco

2.1.2.1 Tổng quan về tường lửa của Cisco

2.1.2.2 Nguyên tắc hoạt động của tường lửa Cisco

2.1.2.3 Định tuyến lưu lượng qua tường lửa

2.1.2.4 Truy cập thông qua tường lửa

2.1.2.5 Truy cập ra ngoài thông qua tường lửa

2.1.2.6 Truy cập vào trong thông qua tường lửa

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

2.1.3.2 Công nghệ Cut-Through Proxy

2.1.3.3 Applicatin-Aware Inspection

2.1.3.4 Virtual Private Network

2.1.3.5 Security Context (Virtual Firewall)

2.1.3.6 Khả năng dự phòng - Failover Capabilities

2.1.3.7 Chế độ trong suốt (Transparent Mode)
2.1.3.8 Quản lý thiết bị qua giao diện web
2.1.3.9 Dòng sản phẩm thế hệ mới Cisco ASA

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: LAN, WAN, DMZ.

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.

2.2.1 Hệ thống phát hiện xâm nhập IDS

2.2.2 Hệ thống phòng chống xâm nhập (IPS)

2.3 Giải pháp sử dụng công nghệ VLAN

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.

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.

2.3.2 Phân loại VLAN

VLAN chia thành 5 loại: Data VLAN, Default VLAN, Native VLAN, VLAN quản lý, VLAN voice.

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

VPN (Virtual Private Network) là một mạng riêng 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.

2.4.1 Các đặc tính của VPN
2.4.2 Các loại VPN
2.4.3 Các cách triển khai VPN trên thực tế

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.

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.

2.7 Kết luận chương 2

Trong chương 2, luận văn đã nghiên cứu 6 giải pháp về bảo mật mạng LAN. 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, 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 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.

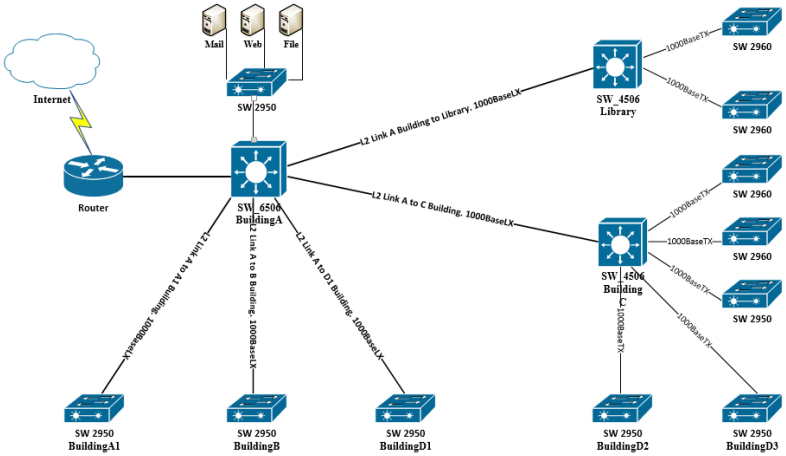
Để có thể xây dựng được những mạng như vậy, người quản trị mạng phải nắm rõ được những kiến thức cơ bản về Firewall, VLAN, Server...

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



Bảng 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 tòa nhà, 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 3 máy chủ DHCP đặt tại 3 trung tâm là Nhà A , Nhà C, Thư viện của

trường và 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.

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 Server 2012, 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 từng cơ sở 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.
- Xây dựng hệ thống Firewall để bảo vệ hệ thống.
- 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 tầng 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

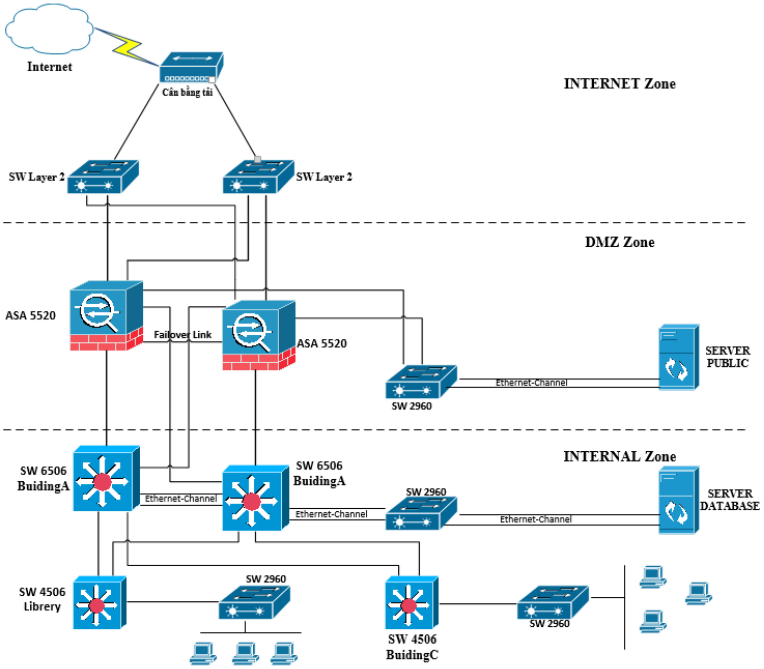
Để quản lý tập trung dữ liệu và các dịch vụ, đồng thời đảm bảo an toàn thông tin cho hệ thống mạng em đề xuất các giải pháp như sau:

3.2.1 Giải pháp mạng

Xây dựng phòng máy chủ tập trung tại nhà A. Sử dụng Firewall cứng Cisco 5520 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
Tổng quan hệ thống:



Bảng 3. 2: Hệ thống mạng với ASA 5520

- Hệ thống bao gồm các thành phần:

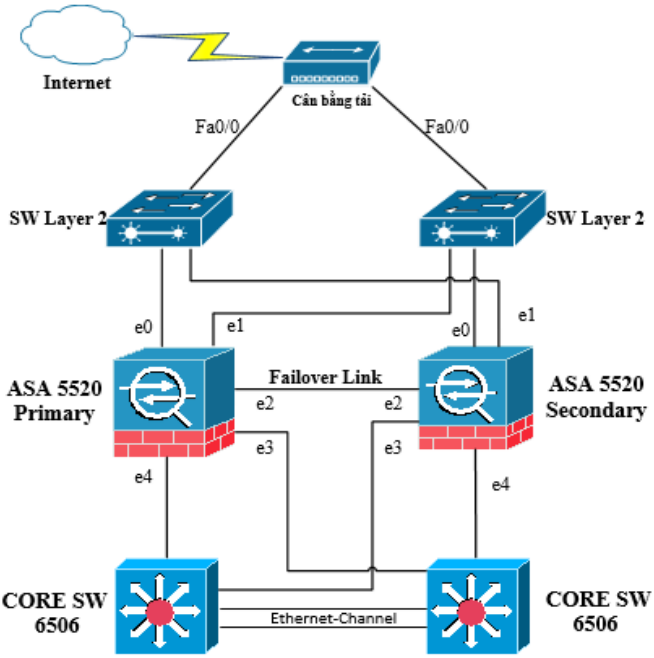
- Vùng Internet sử dụng nhiều đường truyền qua bộ cân bằng tải nhằm đảm bảo tính sẵn sàng cao có thể đáp ứng 24/24 các yêu cầu của người dùng bên trong cũng như các người dùng ở xa truy nhập vào hệ thống của trường. Với đề xuất trên em chủ yếu thiết kế dựa trên các công nghệ ưu việt của hãng Cisco. Với hệ thống nhiều đường truyền internet 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 chuyể 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 tăng 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.



Bảng 3. 3: Mô hình Failover Active/Active trên hệ thống

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.
- Backup File Server.
- 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

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 đề xuất triển khai trong thực tế.

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. 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, hoàn thiện giải pháp bảo mật cho mạng LAN để 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