Bộ Giáo Dục Và Đào Tạo
Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh
Khoa Công Nghệ Thông Tin

BÁO CÁO KẾT THÚC HỌC PHẦN

QUẢN TRỊ HỆ THỐNG BẢO MẬT

ĐỀ TÀI : CHÍNH SÁCH BẢO MẬT DOANH NGHIỆP

Giảng Viên Hướng Dẫn : ThS. Đinh Xuân Lâm
Học viên thực hiện:

1.	Trương Văn Nghĩa	22DH112378
2.	Nguyễn Vũ Anh Khoa	22DH111684
3.	Phạm Đức Long	22DH114617

Tp. Hồ Chí Minh - Ngày 02 tháng 4 năm 2025

LỜI CẢM ƠN

Lời nói đầu tiên, chúng em xin gửi lời cảm ơn chân thành nhất đến các thầy bộ môn *Quản trị hệ thống bảo mật* đã dành thời gian để truyền đạt những kiến thức quý báu cho chúng em trong quá trình học và làm đồ án. Bài đồ án cuối kỳ là cơ hội để chúng em áp dụng những kiến thức đã được thầy truyền dạy, giúp chúng em hiểu rõ hơn về môn học *Quản trị hệ thống bảo mật* cũng như các *Chính sách bảo mật* và có thêm kỹ năng làm việc nhóm.

Trong quá trình học tập và nghiên cứu, do bản thân em vẫn còn chưa vững kiến thức về chuyên ngành và kinh nghiệm thực tế nên có nhiều khi em còn thiếu sót nhưng nhờ có những lời chỉ dẫn, góp ý của các thầy đã giúp chúng hoàn thành sản phẩm của mình một cách tốt nhất. Chúng em rất biết ơn các thầy vì đã dành thời gian để hướng dẫn chúng em trong quá trình thực hiện đồ án.

Chúng em xin gửi lời cảm ơn đặc biệt đến thầy *Đinh Xuân Lâm* vì đã dành thời gian tận tình hướng dẫn và chia sẻ những kiến thức quý báo giúp chúng em từng bước một thực hiện đồ án, cảm ơn thầy suốt thời gian qua đã luôn góp ý cho chúng em từng chi tiết nhỏ trong đồ án cuối kỳ lần này, giúp đồ án của chúng em có thể hoàn chỉnh nhất.

Cuối cùng, chúng em xin gửi lời cảm ơn sâu sắc đến tất cả các thầy và các bạn đã đồng hành và hỗ trợ chúng em trong suốt quá trình thực hiện đồ án. Chúng em cảm thấy rất may mắn và tự hào khi có cơ hội được học cùng với những người thầy, người cô tận tâm như vậy.

Chúng em xin chân thành cảm ơn!

NHẬN XÉT CỦA GIẢNG VIÊN

(Của ThS Đinh Xuân Lâm)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Điểm: (bằng chữ:)

Đồng ý/Không đồng ý cho sinh viên bảo vệ trước hội đồng chấm đồ án ?

,ngày tháng năm 2024

GIÁO VIÊN HƯỚNG DẪN

(ký, họ tên)

LƯU TRỮ CÁC THAY ĐỔI

*A - Added M - Modified D - Deleted

Ngày tháng	Phần tử thay đổi	A* M, D	Mô tả thay đổi	New Version

BẢNG CHỮ KÝ

Tác giả:

Tên:_____	Chữ ký:_____
Vị trí:_____	Ngày: _____
Tên:	Chữ ký:_____
Vị trí:_____	Ngày: _____
Tên:	Chữ ký:_____
Vị trí:_____	Ngày: _____

Người điều chỉnh:

Tên:_____	Chữ ký:_____
Vị trí:_____	Ngày: _____

Người duyệt:

Tên:_____	Chữ ký:_____
Vị trí:_____	Ngày: _____

MỤC LỤC

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH ẢNH

BẢNG PHÂN CÔNG

Thành viên	Phân công	Đánh giá
Trương Văn Nghĩa		
Nguyễn Vũ Anh Khoa		
Phạm Đức Long		

CHƯƠNG I: GIỚI THIỆU TỔNG QUAN VỀ DOANH NGHIỆP

I. LĨNH VỰC KINH DOANH:

Công ty MoneyS hoạt động trong lĩnh vực kinh doanh điện thoại di động, bao gồm phân phối, bán lẻ và cung cấp các dịch vụ liên quan đến thiết bị di động. MoneyS chuyên cung cấp các sản phẩm từ nhiều thương hiệu nổi tiếng như Apple, Samsung, Xiaomi, Oppo và các hãng công nghệ khác, đáp ứng nhu cầu đa dạng của khách hàng từ phân khúc phổ thông đến cao cấp.

Bên cạnh hoạt động kinh doanh điện thoại, MoneyS còn cung cấp các phụ kiện đi kèm như ốp lưng, sạc, tai nghe, kính cường lực và nhiều sản phẩm hỗ trợ khác. Công ty cũng triển khai các dịch vụ bảo hành, sửa chữa và tư vấn kỹ thuật nhằm mang đến trải nghiệm tốt nhất cho khách hàng.

Để bắt kịp xu hướng mua sắm hiện đại, MoneyS đã phát triển nền tảng thương mại điện tử, cho phép khách hàng dễ dàng mua sắm trực tuyến với dịch vụ giao hàng tận nơi nhanh chóng. Hệ thống công nghệ thông tin của công ty đóng vai trò quan trọng trong việc quản lý kho hàng, xử lý đơn hàng, thanh toán trực tuyến và bảo mật thông tin khách hàng.

Do đó, việc đảm bảo an toàn hệ thống thông tin là ưu tiên hàng đầu của MoneyS. Công ty áp dụng các giải pháp bảo mật tiên tiến nhằm ngăn chặn rủi ro mất mát dữ liệu, bảo vệ thông tin khách hàng và duy trì tính ổn định trong hoạt động kinh doanh.

II. QUI MÔ VÀ TỔ CHỨC CỦA DOANH NGHIỆP:

1. Chi nhánh doanh nghiệp:

Công ty MoneyS hiện có một cơ sở duy nhất, được đặt tại đường Lê Duẩn, Quận 1. Cơ sở này là trung tâm điều hành toàn bộ hoạt động kinh doanh, quản lý và vận hành hệ thống bán hàng.

Tòa nhà của công ty gồm 2 tầng, bố trí như sau:

- Tầng trệt: Bao gồm phòng kinh doanh, phòng kế toán, phòng chăm sóc khách hàng và kho hàng. Đây là nơi diễn ra các hoạt động bán hàng, quản lý tài chính và hỗ trợ khách hàng.
- Lầu 1: Gồm phòng giám đốc và phòng server, nơi điều hành chiến lược công ty và quản lý toàn bộ hệ thống công nghệ thông tin.

2. Bộ phận và nhân viên trong doanh nghiệp:

MoneyS có các bộ phận chính sau, mỗi bộ phận đảm nhận một vai trò cụ thể trong hoạt động kinh doanh:

- **Phòng Kinh doanh**: Chịu trách nhiệm bán hàng, tư vấn khách hàng và triển khai các chiến lược kinh doanh.
- **Phòng Kế toán**: Kiểm soát tài chính, tính lương nhân viên, thực hiện các giao dịch và lập báo cáo tài chính.
- **Phòng Chăm sóc khách hàng**: Tiếp nhận yêu cầu, hỗ trợ bảo hành, giải đáp thắc mắc và xử lý khiếu nại của khách hàng.
- **Phòng Kho**: Quản lý hàng hóa, kiểm kê và cung ứng sản phẩm theo nhu cầu kinh doanh.
- **Phòng Giám đốc**: Định hướng phát triển công ty, giám sát hoạt động và đưa ra các quyết định chiến lược.
- **Phòng Server**: Đảm bảo hoạt động hệ thống IT, bảo mật dữ liệu, vận hành website và hệ thống bán hàng trực tuyến.

3. Chức năng các bộ phận:

Phòng Kinh doanh: Quản lý hoạt động bán hàng, đề xuất chương trình khuyến mãi, tìm kiếm khách hàng mới và mở rộng thị trường.

Phòng Kế toán: Theo dõi thu chi, lập kế hoạch tài chính, đảm bảo các giao dịch diễn ra chính xác và minh bạch.

Phòng Chăm sóc khách hàng: Xử lý khiếu nại, hướng dẫn sử dụng sản phẩm, hỗ trợ bảo hành và nâng cao trải nghiệm khách hàng.

Phòng Kho: Theo dõi số lượng hàng hóa, nhập – xuất kho, đảm bảo nguồn cung sản phẩm ổn định.

Phòng Giám đốc: Giám sát hoạt động của công ty, điều hành các phòng ban và xây dựng chiến lược phát triển dài hạn.

Phòng Server: Quản lý hệ thống công nghệ, bảo vệ dữ liệu và đảm bảo hoạt động kinh doanh trực tuyến luôn ổn định và an toàn.

Với mô hình tổ chức rõ ràng và chặt chẽ, MoneyS đảm bảo hoạt động hiệu quả, phục vụ khách hàng tốt nhất và luôn duy trì mức độ bảo mật cao trong hệ thống.

III. MỤC ĐÍCH TRIỂN KHAI HỆ THỐNG:

1. Lĩnh vực hoạt động kinh doanh:

Công ty MoneyS hoạt động trong lĩnh vực kinh doanh điện thoại di động và các sản phẩm công nghệ liên quan. Công ty chuyên cung cấp điện thoại từ nhiều thương hiệu nổi tiếng như Apple, Samsung, Xiaomi, Oppo,… cùng các phụ kiện như sạc, tai nghe, ốp lưng, kính cường lực. Ngoài ra, MoneyS còn cung cấp dịch vụ bảo hành, sửa chữa và tư vấn kỹ thuật nhằm nâng cao trải nghiệm khách hàng.

Với nhu cầu ngày càng cao về mua sắm trực tuyến, MoneyS cũng triển khai nền tảng thương mại điện tử, cho phép khách hàng đặt hàng và thanh toán trực tuyến, giúp tối ưu hóa quy trình bán hàng và mở rộng thị trường.

2. Yêu cầu cơ bản về kỹ thuật:

Để đảm bảo hoạt động kinh doanh hiệu quả, hệ thống công nghệ thông tin của MoneyS cần đáp ứng các yêu cầu kỹ thuật sau:

- Bảo mật dữ liệu: Đảm bảo an toàn cho thông tin khách hàng, giao dịch và dữ liệu nội bộ.
- Tính ổn định và hiệu suất cao: Hệ thống phải hoạt động liên tục, đảm bảo website và phần mềm bán hàng vận hành trơn tru.
- Hạ tầng mạng và máy chủ: Phòng server cần được trang bị các máy chủ mạnh mẽ để quản lý dữ liệu và hệ thống bán hàng trực tuyến.

- Phân quyền truy cập: Áp dụng cơ chế phân quyền để kiểm soát quyền truy cập của nhân viên vào các phần mềm quản lý.
- Sao lưu và phục hồi dữ liệu: Hệ thống backup tự động để đảm bảo dữ liệu không bị mất trong trường hợp xảy ra sự cố.

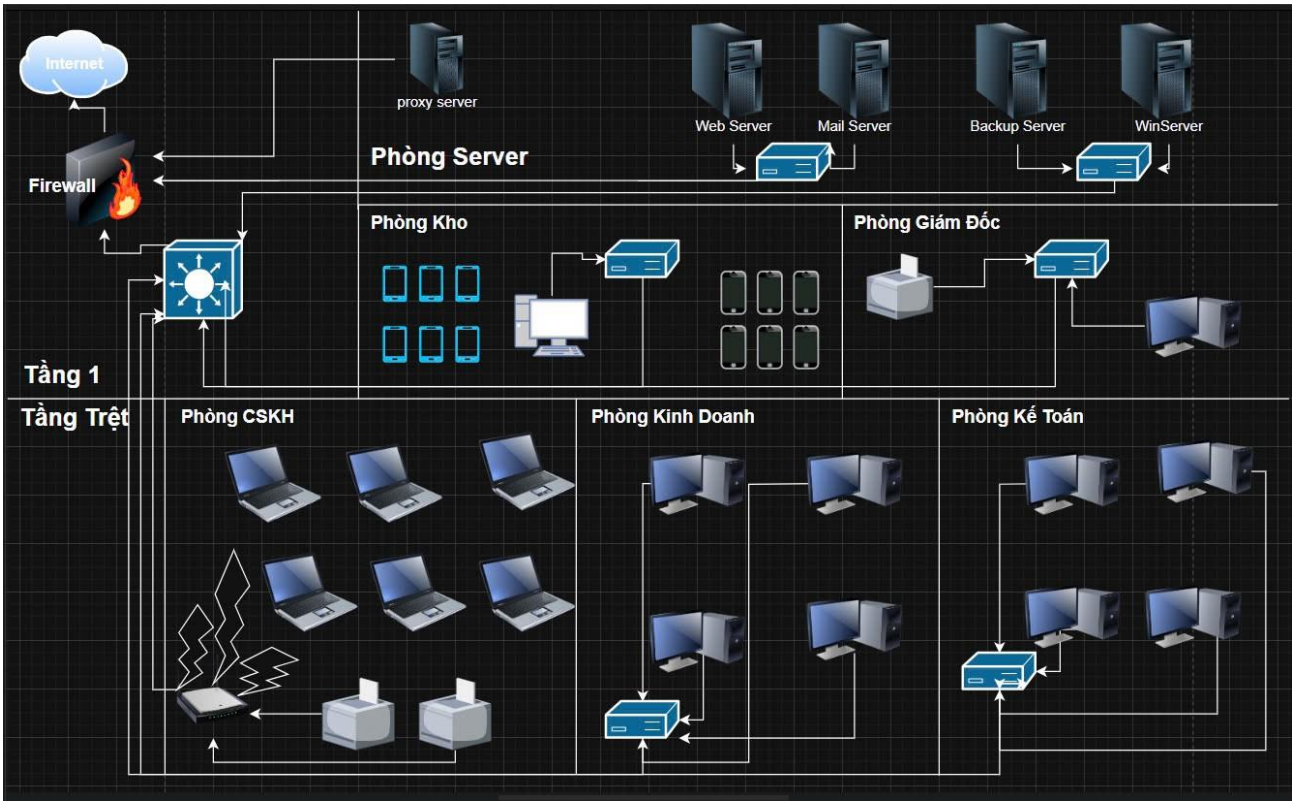
3. Khả năng của doanh nghiệp:

MoneyS có đủ nguồn lực để triển khai và duy trì hệ thống công nghệ thông tin nhờ vào:

- Đội ngũ nhân sự: Công ty có bộ phận IT chuyên trách, đảm bảo vận hành và bảo trì hệ thống.
- Hạ tầng máy chủ: Phòng server được trang bị các máy chủ để lưu trữ dữ liệu và chạy hệ thống quản lý doanh nghiệp.
- Nguồn tài chính: Công ty sẵn sàng đầu tư vào các giải pháp công nghệ hiện đại nhằm nâng cao hiệu quả hoạt động và bảo mật hệ thống.
- Mô hình tổ chức rõ ràng: Với cơ cấu tổ chức chuyên nghiệp, MoneyS có thể phân bổ tài nguyên hợp lý để triển khai và quản lý hệ thống một cách hiệu quả.

Việc triển khai hệ thống không chỉ giúp MoneyS nâng cao năng lực kinh doanh mà còn đảm bảo tính bảo mật, ổn định và khả năng mở rộng trong tương lai.

4. Sơ đồ vật lý tổng thể



Hình 1.1: Sơ đồ vật lý

CHƯƠNG II: LÝ THUYẾT TỔNG QUAN

I. DOMAIN:

Domain Controller (DC) là một máy chủ trung tâm trong hệ thống domain, chịu trách nhiệm xác thực người dùng, quản lý quyền truy cập và thực thi chính sách bảo mật trong mạng doanh nghiệp.

Chức năng của Domain Controller:

- Xác thực người dùng: Kiểm tra danh tính và thông tin đăng nhập khi người dùng truy cập vào hệ thống.
- Quản lý tài khoản tập trung: Tạo, phân quyền và kiểm soát tài khoản người dùng trong toàn bộ hệ thống.
- Thực thi chính sách bảo mật: Áp dụng và giám sát các quy tắc bảo mật, đảm bảo quyền truy cập hợp lệ.
- Quản lý tài nguyên: Cấp hoặc hạn chế quyền truy cập đối với thư mục, máy in, ứng dụng và các dịch vụ mạng trong doanh nghiệp.

1. Active Directory (AD):

Active Directory (AD) là một dịch vụ quan trọng của Microsoft, cung cấp khả năng quản lý tập trung cho toàn bộ hệ thống domain của doanh nghiệp. AD giúp kiểm soát tài khoản người dùng, thiết bị, nhóm và tài nguyên mạng, giúp nâng cao tính bảo mật và hiệu suất vận hành.

Các thành phần chính của Active Directory:

- Domain: Môi trường quản lý tập trung, nơi người dùng và tài nguyên được kiểm soát bởi Domain Controller.
- Users (Người dùng): Tài khoản cá nhân được cấp quyền đăng nhập vào hệ thống.
- Groups (Nhóm): Tập hợp người dùng có cùng quyền truy cập và vai trò trong hệ thống.
- Organizational Units (OU): Các đơn vị tổ chức giúp quản lý nhóm người dùng hoặc tài nguyên theo từng bộ phận của doanh nghiệp.

2. Hệ thống phân giải tên miền (DNS):

Domain Name System (DNS) là một dịch vụ quan trọng giúp chuyển đổi tên miền thành địa chỉ IP, hỗ trợ việc định danh và tìm kiếm tài nguyên trong mạng nội bộ của doanh nghiệp.

Chức năng của DNS trong hệ thống doanh nghiệp:

- Chuyển đổi tên miền thành địa chỉ IP: Giúp các thiết bị trong mạng dễ dàng truy cập tài nguyên nội bộ thông qua tên miền thay vì địa chỉ IP.
- Hỗ trợ truy cập dịch vụ mạng: Định tuyến người dùng đến các dịch vụ nội bộ như máy chủ tệp, email, ứng dụng web.
- Tăng hiệu suất và độ tin cậy: Hệ thống DNS cục bộ giúp cải thiện tốc độ truy cập và giảm tải cho hệ thống mạng doanh nghiệp.

3. DHCP:

Dynamic Host Configuration Protocol (DHCP) là giao thức tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, giúp quản lý tài nguyên mạng hiệu quả và giảm thiểu lỗi cấu hình thủ công.

Lợi ích của DHCP:

- Tự động cấp phát địa chỉ IP: Giúp thiết bị mới kết nối vào hệ thống mà không cần cấu hình thủ công.
- Giảm xung đột IP: Đảm bảo mỗi thiết bị có một địa chỉ IP duy nhất trong mạng.
- Dễ dàng quản lý và giám sát: Giúp bộ phận IT theo dõi và kiểm soát danh sách các địa chỉ IP đang được sử dụng.

4. Group Policy (GPO):

Group Policy Object (GPO) là một tính năng quan trọng của Active Directory, cho phép quản trị viên quản lý tập trung các cài đặt bảo mật, quyền truy cập và chính sách hệ thống trên toàn bộ thiết bị trong domain.

Chức năng của Group Policy:

- Quản lý bảo mật hệ thống: Định cấu hình chính sách mật khẩu mạnh, tự động khóa thiết bị khi không hoạt động.
- Kiểm soát quyền truy cập: Hạn chế người dùng cài đặt phần mềm trái phép hoặc thay đổi cài đặt hệ thống.
- Cấu hình phần mềm tự động: Cài đặt hoặc chặn ứng dụng theo chính sách của doanh nghiệp.
- Thiết lập chính sách mạng: Cấu hình firewall, VPN, quản lý kết nối từ xa và đảm bảo an toàn hệ thống.

II. VPN:

VPN (Virtual Private Network – Mạng riêng ảo) là một công nghệ cho phép thiết lập kết nối an toàn giữa các thiết bị thông qua mạng công cộng như Internet. VPN giúp mã hóa dữ liệu, bảo vệ danh tính người dùng và cho phép truy cập từ xa vào các hệ thống nội bộ của doanh nghiệp, đảm bảo tính bảo mật và toàn vẹn dữ liệu.

1. Các loại VPN phổ biến:

1.1 Site-to-Site VPN:

Site-to-Site VPN được sử dụng để kết nối nhiều hệ thống mạng tại các địa điểm khác nhau, tạo thành một mạng thống nhất. Trong mô hình này, việc xác thực ban đầu được thực hiện giữa các thiết bị đầu cuối (router/firewall) đóng vai trò gateway tại mỗi site. Các chính sách bảo mật được triển khai tại các gateway để đảm bảo dữ liệu được truyền tải an toàn giữa các mạng.

Ứng dụng:

- Kết nối chi nhánh với trụ sở chính.
- Tạo một hệ thống mạng doanh nghiệp thống nhất, bảo mật.
- Đảm bảo kết nối nội bộ ổn định giữa các văn phòng từ xa.

1.2 Remote Access VPN:

Remote Access VPN cho phép người dùng từ xa (như nhân viên làm việc tại nhà hoặc di chuyển) kết nối an toàn vào hệ thống nội bộ của doanh nghiệp thông qua Internet. Người dùng sử dụng phần mềm VPN Client để kết nối với VPN Server và xác thực trước khi được cấp quyền truy cập vào hệ thống.

Ứng dụng:

- Nhân viên làm việc từ xa có thể truy cập hệ thống nội bộ một cách an toàn.
- Hỗ trợ kết nối bảo mật cho văn phòng nhỏ hoặc cá nhân muốn truy cập vào hệ thống chính.
- Bảo vệ dữ liệu truyền tải giữa người dùng và hệ thống doanh nghiệp.

2. OpenVPN:

OpenVPN là một phần mềm VPN mã nguồn mở sử dụng giao thức SSL/TLS để thiết lập kết nối mạng riêng ảo an toàn. Được phát triển từ năm 2001, OpenVPN trở thành một trong những giải pháp VPN đáng tin cậy nhất nhờ tính bảo mật cao, khả năng tương thích với nhiều nền tảng và dễ dàng triển khai.

Chức năng và vai trò của OpenVPN:

- Xác thực và quản lý người dùng: OpenVPN hỗ trợ nhiều phương thức xác thực như pre-shared key, username/password, hoặc chứng chỉ số (certificate-based authentication) để đảm bảo chỉ các thiết bị và người dùng hợp lệ mới có thể truy cập vào hệ thống.
- Quản lý Client-Server hiệu quả: Trong cấu hình multi-client server, OpenVPN cho phép cấp phát chứng chỉ xác thực riêng cho mỗi thiết bị client, giúp quản lý truy cập dễ dàng.
- Mã hóa bảo mật mạnh mẽ: OpenVPN sử dụng các thư viện mã hóa OpenSSL/TLS để đảm bảo dữ liệu được truyền tải an toàn, giảm nguy cơ tấn công trung gian (MITM - Man-in-the-Middle).

- Tính linh hoạt cao: OpenVPN hỗ trợ cả giao thức UDP và TCP, giúp tối ưu hóa hiệu suất kết nối tùy theo yêu cầu sử dụng. UDP thường được dùng để cải thiện tốc độ, trong khi TCP được sử dụng khi yêu cầu độ tin cậy cao.
- Hỗ trợ kết nối nhanh và ổn định: Nhờ sử dụng UDP, OpenVPN cung cấp khả năng kết nối nhanh chóng mà vẫn đảm bảo tính bảo mật.
- Kiểm soát dữ liệu truyền tải: OpenVPN cho phép kiểm soát dữ liệu trong quá trình truyền tải, đảm bảo tính toàn vẹn và tránh mất mát dữ liệu khi truyền qua mạng VPN.

3. OpenVPN Client Export:

OpenVPN Client Export là một công cụ trên pfSense giúp tạo và xuất file cấu hình VPN cho người dùng dễ dàng. Khi sử dụng tiện ích này, người dùng chỉ cần tải file cấu hình và nhập vào ứng dụng OpenVPN Client để kết nối với VPN Server mà không cần thiết lập thủ công.

Lợi ích của OpenVPN Client Export:

- Dễ dàng triển khai: Giúp người dùng nhanh chóng kết nối với VPN Server mà không cần thiết lập thủ công.
- Tăng cường bảo mật: File cấu hình đã được mã hóa và tích hợp sẵn thông tin cần thiết để đảm bảo kết nối an toàn.
- Hỗ trợ đa nền tảng: Hoạt động trên Windows, macOS, Linux, iOS, Android,...

III. PROXY:

Proxy là một máy chủ trung gian hoạt động giữa người dùng và Internet, giúp cải thiện hiệu suất mạng, bảo mật thông tin và kiểm soát truy cập. Proxy có thể lưu trữ nội dung tạm thời để tăng tốc độ truy cập, bảo vệ người dùng khỏi các mối đe dọa trực tuyến và giới hạn quyền truy cập vào các tài nguyên web theo chính sách doanh nghiệp.

1. Squid Proxy Server:

Squid Proxy là một phần mềm mã nguồn mở phổ biến, hoạt động như một máy chủ proxy trung gian giúp quản lý lưu lượng truy cập web hiệu quả. Squid hỗ trợ nhiều giao thức như HTTP, HTTPS, FTP, giúp doanh nghiệp tối ưu hóa băng thông, tăng cường bảo mật và kiểm soát truy cập người dùng.

Tính năng nổi bật của Squid Proxy:

- Caching (Lưu trữ nội dung web): Squid lưu trữ các bản sao của trang web đã truy cập để giảm tải băng thông và tăng tốc độ truy cập trong những lần tiếp theo.
- Kiểm soát truy cập: Quản trị viên có thể thiết lập các chính sách kiểm soát để hạn chế hoặc cho phép truy cập vào các trang web nhất định, giúp bảo vệ mạng nội bộ khỏi các nội dung không phù hợp hoặc độc hại.
- Báo cáo và giám sát: Squid cung cấp các công cụ phân tích lưu lượng truy cập, giúp quản trị viên theo dõi hành vi người dùng và tối ưu hóa hiệu suất mạng.
- Hỗ trợ đa giao thức: Ngoài HTTP và HTTPS, Squid còn hỗ trợ FTP, giúp quản lý lưu lượng truy cập của nhiều loại dịch vụ trực tuyến.
- Bảo mật dữ liệu: Squid có thể ẩn địa chỉ IP của người dùng, giúp tăng cường bảo mật khi duyệt web.

2. SquidGuard:

SquidGuard là một plugin mở rộng của Squid Proxy Server, giúp lọc nội dung web, ngăn chặn truy cập vào các trang web không mong muốn và kiểm soát việc sử dụng Internet trong doanh nghiệp.

Tính năng nổi bật của SquidGuard:

- Lọc nội dung web: SquidGuard cho phép chặn các trang web có nội dung khiêu dâm, bạo lực, độc hại hoặc không phù hợp với chính sách doanh nghiệp.
- Danh sách đen (Blacklist) và danh sách trắng (Whitelist): Quản trị viên có thể tạo blacklist để chặn các trang web cụ thể hoặc whitelist để cho phép truy cập vào những trang web an toàn.
- Tùy chỉnh quy tắc lọc: SquidGuard hỗ trợ thiết lập chính sách lọc theo địa chỉ IP, tên miền, URL hoặc từ khóa, giúp doanh nghiệp linh hoạt trong việc quản lý truy cập web.
- Giám sát và báo cáo: Cung cấp thông tin chi tiết về các trang web bị chặn và lịch sử truy cập, giúp quản trị viên theo dõi và điều chỉnh các chính sách lọc hiệu quả.

- Tăng cường bảo mật: Giúp bảo vệ hệ thống khỏi các trang web độc hại, giảm thiểu nguy cơ lây nhiễm phần mềm độc hại và tấn công mạng.

IV. FIREWALL:

1. Giới thiệu về Firewall:

Firewall (tường lửa) là một hệ thống bảo mật mạng được thiết kế để giám sát, kiểm soát và ngăn chặn các truy cập trái phép vào hoặc ra khỏi mạng nội bộ, dựa trên các chính sách bảo mật được thiết lập. Đây là lớp phòng thủ quan trọng giúp bảo vệ hệ thống khỏi các mối đe dọa từ bên ngoài, bao gồm tấn công từ chối dịch vụ (DDoS), phần mềm độc hại, truy cập trái phép và các nguy cơ bảo mật khác.

Phân loại Firewall tùy vào nhu cầu bảo mật và mô hình của doanh nghiệp

Firewall phần cứng:

- Được triển khai dưới dạng thiết bị vật lý, thường sử dụng trong các công ty lớn hoặc hệ thống mạng cần xử lý lưu lượng cao.
- Cung cấp hiệu suất cao, đảm bảo độ ổn định và khả năng bảo vệ mạnh mẽ.

Firewall phần mềm:

- Là một ứng dụng chạy trên hệ điều hành (Windows, Linux, FreeBSD...) giúp bảo vệ máy chủ hoặc hệ thống mạng.
- Linh hoạt, dễ triển khai, phù hợp với doanh nghiệp nhỏ hoặc văn phòng chi nhánh.

Next-Generation Firewall (NGFW – Tường lửa thế hệ mới):

- Tích hợp công nghệ bảo mật tiên tiến như phát hiện xâm nhập (IDS/IPS), phân tích gói tin sâu (DPI), kiểm soát ứng dụng và bảo vệ trước các mối đe dọa mới.
- Kết hợp với trí tuệ nhận tạo (AI) và machine learning để phát hiện các tấn công tinh vi hơn.

Chức năng chính của Firewall

Lọc gói tin (Packet Filtering):

- Kiểm tra các tiêu đề của gói tin (địa chỉ IP, cổng, giao thức) và quyết định cho phép hoặc từ chối dựa trên chính sách bảo mật.

Kiểm soát truy cập (Access Control):

- Giới hạn hoặc cấp quyền truy cập theo địa chỉ IP, dải mạng, giao thức và cổng kết nối.
- Ngăn chặn truy cập trái phép vào các tài nguyên quan trọng.

Bảo vệ khỏi tấn công DDoS:

- Giới hạn số lượng kết nối đồng thời từ một địa chỉ IP.
- Sử dụng cơ chế phát hiện và giảm thiểu tấn công DDoS.

Hỗ trợ VPN (Virtual Private Network):

- Cung cấp kênh kết nối an toàn cho người dùng từ xa thông qua OpenVPN, IPsec hoặc WireGuard.

Ghi log và giám sát:

- Lưu trữ nhật ký truy cập và hoạt động mạng để giúp phát hiện hành vi bất thường, phân tích các cuộc tấn công và tối ưu hóa hệ thống bảo mật.

2. Giới thiệu về pfSense:

pfSense là một firewall mã nguồn mở, được xây dựng trên hệ điều hành FreeBSD, cung cấp các tính năng bảo mật mạnh mẽ, linh hoạt và dễ triển khai cho mọi mô hình mạng từ nhỏ đến lớn. Với giao diện quản lý web thân thiện, pfSense giúp quản trị viên dễ dàng cấu hình, giám sát và bảo vệ hệ thống mà không cần chuyên sâu về lập trình hoặc mạng.

2.1 Các tính năng nổi bật của pfSense:

Firewall & NAT:

- Kiểm soát truy cập mạng với chính sách linh hoạt.
- Hỗ trợ NAT (Network Address Translation) để chia sẻ kết nối Internet và bảo vệ IP nội bộ.

Hỗ trợ VPN:

- Hỗ trợ các giao thức OpenVPN, IPsec, L2TP giúp thiết lập kết nối an toàn giữa các chi nhánh hoặc cho nhân viên từ xa.

Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS):

- Tích hợp Snort hoặc Suricata để phát hiện và ngăn chặn các mối đe dọa bảo mật như malware, ransomware, tấn công brute-force.

Cân bằng tải (Load Balancing) & Chuyển đổi dự phòng (Failover):

- Hỗ trợ nhiều kết nối Internet và tự động chuyển đổi khi một đường truyền gặp sự cố.

Captive Portal – Xác thực người dùng Wi-Fi:

- Yêu cầu người dùng nhập thông tin đăng nhập khi kết nối Wi-Fi, giúp kiểm soát truy cập mạng công cộng.

Logging & Monitoring:

- Ghi lại toàn bộ hoạt động mạng, giúp theo dõi và phân tích các sự kiện bảo mật quan trọng.

2.2 Ứng dụng của pfSense trong bảo mật hệ thống:

V. IDS:

1. Giới thiệu về IDS:

Hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) là một giải pháp bảo mật giúp phát hiện và cảnh báo về các hoạt động bất thường hoặc tấn công mạng nhằm vào hệ thống. IDS không ngăn chặn tấn công trực tiếp mà giám sát lưu lượng mạng, phân tích gói tin để xác định các mối đe dọa tiềm ẩn.

IDS thường được sử dụng để phát hiện:

- Tấn công từ chối dịch vụ (DDoS)
- Tấn công brute-force (đoán mật khẩu)
- Tấn công khai thác lỗ hổng (exploits)
- Malware, ransomware và phần mềm độc hại
- Các hành vi truy cập trái phép

2. Phân loại IDS:

2.1 Network-based IDS (NIDS – IDS trên mạng)

- Được triển khai tại các điểm quan trọng trong hệ thống mạng để giám sát lưu lượng mạng.
- Phát hiện các mối đe dọa bằng cách phân tích các gói tin theo thời gian thực.

2.2 Host-based IDS (HIDS – IDS trên máy chủ)

- Được cài đặt trên từng thiết bị hoặc máy chủ, giám sát file log, registry, tiến trình đang chạy để phát hiện hành vi đáng ngờ.
- Tích hợp với hệ thống SIEM để quản lý log tập trung.

3. Snort – IDS phổ biến và mạnh mẽ:

Snort là một hệ thống IDS mã nguồn mở mạnh mẽ, được phát triển bởi Cisco, có khả năng phát hiện và phân tích các cuộc tấn công mạng dựa trên luật (rules-based detection).

Tính năng nổi bật của Snort:

- Giám sát lưu lượng mạng: Kiểm tra các gói tin theo thời gian thực.
- Phát hiện xâm nhập: Dựa trên danh sách các quy tắc bảo mật được cập nhật liên tục.
- Ghi log và tạo báo cáo: Lưu lại thông tin tấn công để phục vụ phân tích.
- Hỗ trợ nhiều chế độ hoạt động: Sniffer mode, Packet Logger mode, IDS/IPS mode.

4. Suricata – IDS/ÍP hiệu suất cao:

Suricata là một hệ thống IDS/IPS hiện đại, cung cấp hiệu suất cao hơn Snort do hỗ trợ đa luồng (multi-threading) và tận dụng phần cứng tối ưu hơn.

Tính năng nổi bật của Suricata:

- Phát hiện tấn công theo thời gian thực.
- Hỗ trợ DPI (Deep Packet Inspection) – phân tích sâu gói tin.
- Có thể hoạt động như một IDS hoặc IPS (Intrusion Prevention System).
- Tích hợp với Threat Intelligence để cập nhật danh sách mối đe dọa.

5. So sánh IDS và IPS:

Đặc điểm	IDS	IPS
Chức năng chính	Phát hiện và cảnh báo	Phát hiện và ngăn chặn
Tác động đến lưu lượng mạng	Thụ động (Chỉ giám sát)	Chủ động (có thể chặn)
Ví dụ phần mềm	Snort, Suricata (Chế độ IDS), OSSEC	Snort (chế độ IPS), Suricata (chế độ IPS), pfSense IPS
Ứng dụng phổ biến	Giám sát bảo mật, phân tích log	Ngăn chặn tấn công tự động

6. Ứng dụng của IDS trong bảo mật hệ thống:

- Giám sát lưu lượng mạng và phát hiện hành vi bất thường.
- Cảnh báo sớm về các cuộc tấn công hoặc lỗ hổng bảo mật.
- Hỗ trợ điều tra các sự cố bảo mật bằng log chi tiết.
- Kết hợp với firewall và SIEM để tối ưu hệ thống bảo mật.

CHƯƠNG III: XÂY DỰNG VÀ TRIỂN KHAI HỆ THỐNG BẢO MẬT

I. XÁC ĐỊNH TÀI SẢN CẦN BẢO VỆ:

1. Tài sản vật lý:

- Máy chủ, thiết bị mạng (router, switch, firewall).
- Hệ thống lưu trữ dữ liệu (NAS, SAN).
- Máy tính cá nhân, thiết bị đầu cuối.

2. Tài sản dữ liệu:

- Cơ sở dữ liệu khách hàng, tài liệu nội bộ.
- Mã nguồn phần mềm, thông tin giao dịch.
- Thông tin đăng nhập, dữ liệu quan trọng của tổ chức.

3. Tài sản hệ thống:

- Hệ thống quản lý người dùng (Active Directory, LDAP).
- Hệ thống mạng nội bộ, VPN, firewall.
- Dịch vụ web, email server, hệ thống lưu trữ đám mây.

4. Tài sản con người:

- Nhân sự IT, quản trị viên hệ thống.
- Nhân viên có quyền truy cập vào dữ liệu nhạy cảm.

II. ĐÁNH GIÁ RỦI RO:

1. Xác định các mối đe dọa:

- Tấn công mạng (DDoS, SQL Injection, Malware).
- Truy cập trái phép vào hệ thống.
- Nhân viên nội bộ rò rỉ dữ liệu.
- Thiên tai, mất điện, lỗi phần cứng.

2. Phân tích lỗ hổng:

- Kiểm tra bảo mật hệ thống (pentest, scan lỗ hổng).
- Đánh giá khả năng bị tấn công từ bên ngoài và bên trong.

- Xác định hệ thống nào dễ bị xâm nhập nhất.

3. **Đánh giá tác động và xác suất xảy ra:**
   - Xác định mức độ thiệt hại nếu bị tấn công.
   - Đánh giá khả năng xảy ra của từng rủi ro.

4. **Lập kế hoạch giảm thiểu rủi ro:**
   - Nâng cấp hệ thống bảo mật, sử dụng firewall, IDS/IPS.
   - Áp dụng chính sách bảo mật mạnh mẽ hơn.
   - Đào tạo nhân viên về an toàn thông tin.

III. XÂY DỰNG CHÍNH SÁCH BẢO MẬT VÀ CÁC QUY TRÌNH BẢO MẬT:

1. **Chính sách bảo mật vật lý:**
   - Kiểm soát truy cập vào phòng server, hạn chế quyền ra vào.
   - Sử dụng hệ thống giám sát (camera, cảm biến chuyển động).
   - Đặt máy chủ trong phòng có điều kiện môi trường ổn định.
   - Sử dụng khóa bảo mật, thẻ từ, vân tay để hạn chế truy cập.

2. **Chính sách bảo mật hệ điều hành:**
   - Cập nhật hệ điều hành và phần mềm thường xuyên.
   - Sử dụng phần mềm diệt virus và firewall trên từng máy chủ.
   - Áp dụng nguyên tắc Least Privilege (Chỉ cấp quyền cần thiết).
   - Giám sát và kiểm tra log hệ thống để phát hiện hành vi bất thường.

3. **Chính sách bảo mật mạng:**
   - Cấu hình firewall chặn các truy cập trái phép.
   - Sử dụng VPN để bảo mật kết nối từ xa.
   - Triển khai IDS/IPS để phát hiện và ngăn chặn tấn công.
   - Kiểm soát truy cập mạng bằng VLAN, ACL.

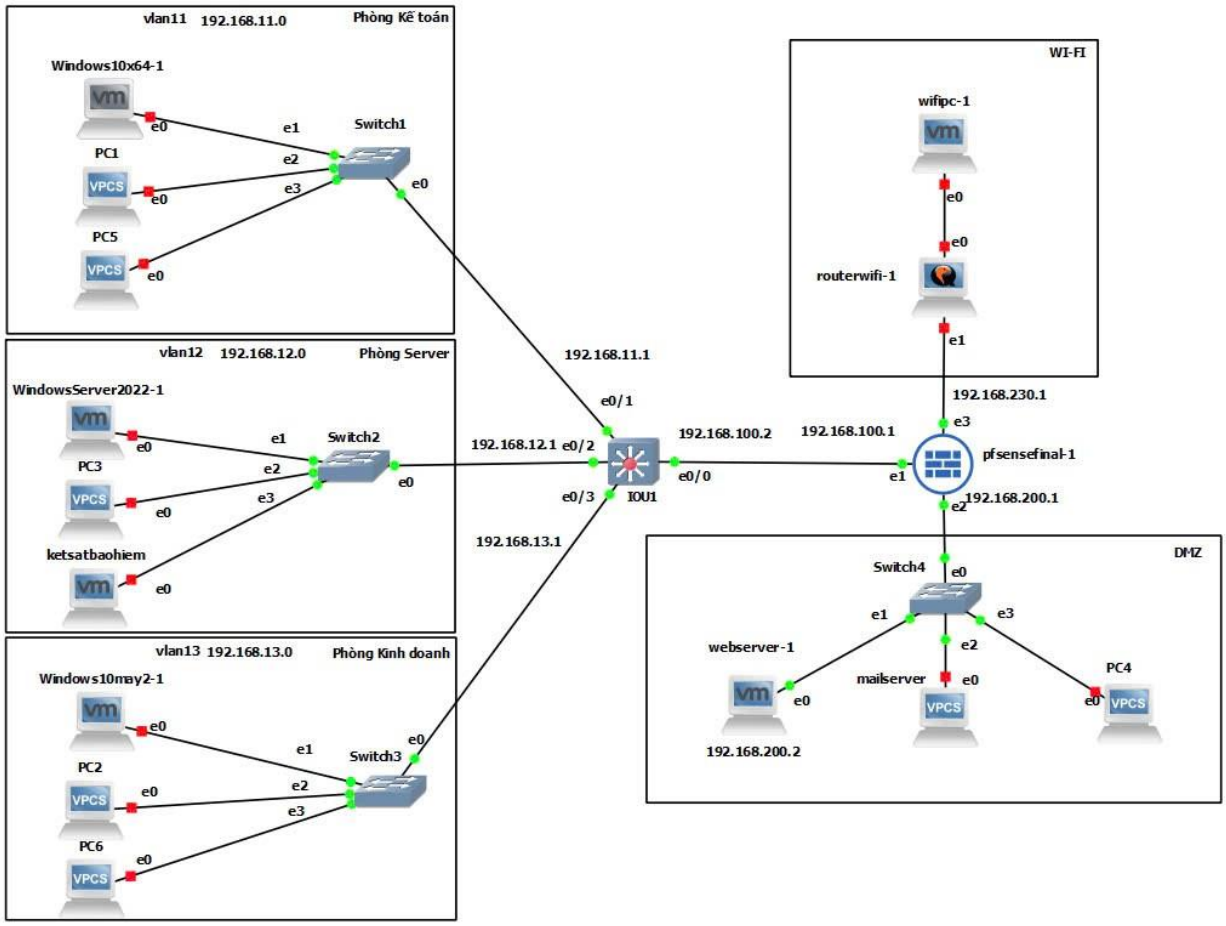
4. **Kế hoạch ứng phó với sự cố:**
   - Xác định các loại sự cố có thể xảy ra (tấn công mạng, mất dữ liệu, lỗi phần cứng).
   - Xây dựng quy trình phản hồi nhanh khi xảy ra sự cố.
   - Chỉ định đội ngũ xử lý sự cố và phân công trách nhiệm cụ thể.

- Ghi log và phân tích nguyên nhân sau sự cố.

5. Kế hoạch khôi phục sau thảm họa:

- Xác định phương pháp sao lưu dữ liệu (backup định kỳ, backup offsite).
- Thiết lập hệ thống dự phòng (Disaster Recovery Site).
- Kiểm tra và diễn tập khôi phục dữ liệu định kỳ.

IV. TRIỂN KHAI GIẢI PHÁP:



Hình 3.1: Sơ đồ GNS3

Phòng Kế Toán (VLAN11 – 192.168.11.0/24):

Thiết bị	IP Address	Subnet Mask
Windows10x61-1	192.168.11.10	255.255.255.0

PC1	192.168.11.1	255.255.255.0
PC5	192.168.11.2	255.255.255.0
Switch1	192.168.11.3	255.255.255.0

Phòng Server (VLAN12 192.168.12.0/24)

Thiết bị	IP Address	Subnet Mask
WindowsServer2022-1	192.168.12.10	255.255.255.0
PC3	192.168.12.1	255.255.255.0
Két sắt bảo hiểm	192.168.12.2	255.255.255.0
Switch2	192.168.12.254	255.255.255.0

Phòng Kinh Doanh (VLAN13 192.168.13.0/24)

Thiết bị	IP Address	Subnet Mask
Windows10may2-1	192.168.13.10	255.255.255.0
PC2	192.168.13.1	255.255.255.0
PC6	192.168.13.2	255.255.255.0
Switch3	192.168.13.254	255.255.255.0

Wi-Fi (192.168.230.0/24)

Thiết bị	IP Address	Subnet Mask
wifipc-1	192.168.230.10	255.255.255.0
routerwifi-1	192.168.230.1	255.255.255.0

DMZ (192.168.200.0/24)

Thiết bị	IP Address	Subnet Mask
webserver-1	192.168.200.2	255.255.255.0
mailserver	192.168.200.3	255.255.255.0
PC4	192.168.200.4	255.255.255.0
Switch4	192.168.200.254	255.255.255.0

pfSense Firewall

Giao diện	IP Address	Subnet Mask
LAN	192.168.100.1	255.255.255.0

WAN	192.168.100.2	255.255.255.0
DMZ	192.168.200.1	255.255.255.0
Wi-Fi	192.168.230.1	255.255.255.0

Clip Demo:

SURICATA:

https://youtu.be/uJpjQ_8hhaY

DMZ Webserver:

https://youtu.be/yeY6TMyZAm0

Proxy:

https://youtu.be/p1ZvVWufUes

Firewall rule test:

https://youtu.be/QENgU1Ilvfo

DemoWinserver:

https://youtu.be/xOgyBm8pXDM

1. **Kiểm soát truy cập:**
   - Áp dụng xác thực hai yếu tố (2FA) cho tài khoản quan trọng.
   - Cấu hình chính sách mật khẩu mạnh.
   - Hạn chế quyền truy cập của người dùng theo nguyên tắc Least Privilege.

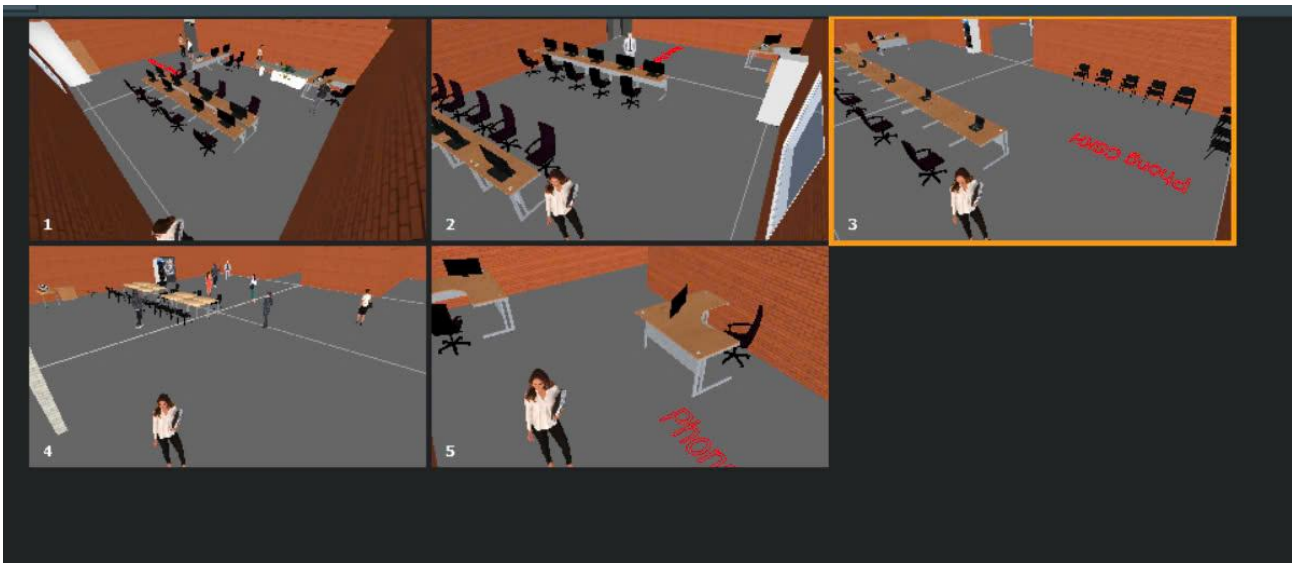
2. **Bảo vệ dữ liệu:**
   - Mã hóa dữ liệu quan trọng (AES, RSA).
   - Triển khai hệ thống DLP (Data Loss Prevention) để ngăn chặn rò rỉ dữ liệu.
   - Hạn chế truy cập vào tài liệu quan trọng theo cấp bậc.

3. **Triển khai các công nghệ bảo mật:**
   - Sử dụng firewall để kiểm soát luồng dữ liệu vào/ra.
   - Cài đặt IDS/IPS để phát hiện và ngăn chặn tấn công.
   - Triển khai SIEM để theo dõi log và phát hiện sự kiện bảo mật.

- Sử dụng phần mềm endpoint security để bảo vệ thiết bị đầu cuối.

4. Triển khai hệ thống giám sát và mạng:

- Cấu hình hệ thống giám sát (Zabbix, Nagios) để theo dõi hiệu suất hệ thống.
- Ghi log tất cả các sự kiện quan trọng và lưu trữ log ít nhất 6 tháng.
- Sử dụng phân tích lưu lượng mạng để phát hiện bất thường.



Hình 3.2: Camera toàn bộ tầng trệt

Hình 3.3: Camera toàn bộ tầng 1

5. Sao lưu và phục hồi:

- Thực hiện backup định kỳ (hàng ngày, hàng tuần, hàng tháng).

- Lưu trữ backup ở nhiều địa điểm khác nhau (on-site và off-site).
- Kiểm tra khả năng khôi phục dữ liệu để đảm bảo tính sẵn sàng.

CHƯƠNG IV: KẾT LUẬN VÀ ĐÁNH GIÁ

I. KẾT LUẬN:

Sau quá trình nghiên cứu và triển khai hệ thống bảo mật, đề tài đã đạt được những mục tiêu đề ra, bao gồm việc xây dựng một hệ thống bảo mật mạng toàn diện, đảm bảo an toàn thông tin cho các phòng ban và hệ thống máy chủ. Các giải pháp bảo mật như Firewall, VPN, IDS/IPS, Proxy và các cơ chế kiểm soát truy cập đã được áp dụng để tăng cường mức độ an toàn và ổn định cho hệ thống.

Việc triển khai các chính sách bảo mật, kế hoạch ứng phó sự cố và khôi phục sau thảm họa cũng giúp giảm thiểu rủi ro, nâng cao khả năng phát hiện và xử lý các mối đe dọa tiềm ẩn. Qua quá trình thực hiện, hệ thống đã chứng minh được tính khả thi và hiệu quả trong việc bảo vệ dữ liệu, kiểm soát truy cập và giám sát hoạt động mạng.

II. ĐÁNH GIÁ :

1. Ưu điểm:

- Hệ thống bảo mật được xây dựng theo mô hình rõ ràng, có khả năng mở rộng và nâng cấp.
- Các công nghệ bảo mật được triển khai linh hoạt, đảm bảo an toàn thông tin mà không ảnh hưởng đến hiệu suất mạng.
- Có sự kết hợp giữa các giải pháp bảo mật phần cứng và phần mềm, giúp tối ưu chi phí và hiệu quả.
- Chính sách bảo mật và quy trình ứng phó được xây dựng chặt chẽ, giảm thiểu rủi ro từ các cuộc tấn công mạng.

Hình 4.1: Ưu điểm

2. **Hạn chế:**
   - Việc triển khai hệ thống yêu cầu kiến thức chuyên môn cao và thời gian cấu hình ban đầu khá lớn.
   - Hệ thống có thể cần được nâng cấp để thích ứng với các mối đe dọa bảo mật mới trong tương lai.
   - Một số thành phần bảo mật như IDS/IPS, giám sát mạng cần được tinh chỉnh và tối ưu hóa để đạt hiệu suất cao nhất.

Hình 4.2: Hạn chế

3. **Hướng phát triển trong tương lai:**
   - Tích hợp trí tuệ nhân tạo (AI) để phát hiện sớm các mối đe dọa và tự động hóa phản ứng bảo mật.
   - Mở rộng hệ thống bảo mật với Zero Trust Model để tăng cường kiểm soát truy cập.
   - Nâng cấp hệ thống giám sát và báo cáo để cải thiện khả năng phân tích dữ liệu bảo mật.
   - Ứng dụng công nghệ blockchain vào bảo mật dữ liệu để đảm bảo tính toàn vẹn và minh bạch.

Hình 4.3: Hướng phát triển

TÀI LIỆU THAM KHẢO

STT	Tên	Link truy cập	Ngày truy cập
1	YouTube	https://www.youtube.com/watch?v=dqlzQXo1wqo	10/3/2025
2	YouTube	https://www.youtube.com/watch?v=Vm98ofYp05g	15/3/2025

3	GitHub	https://github.com/huongbn/Ghi-chep-Suricata-/blob/master/Tong%20quan%20ve%20Suricata.md	17/3/2025
4	YouTube	https://www.youtube.com/watch?v=1-2Q9QigtXY	20/3/2025
5	pfSense	https://docs.netgate.com/pfsense/en/latest/	22/3/2025